www.ip-com.com.cn

配置指导

G5528X-EI交换机命令行配置手册

IP-COM
无线网络解决方案专家

命令配置

1 访问命令行

我们可以使用此界面来配置和管理交换机。通过直连到服务器的控制台端口、Telnet 或 Secure Shellconnection（SSH）访问交换机的管理界面时，可以通过在提示符下输入命令行关键字符和参数来管理交换机。

要通过控制台端口访问交换机，请执行以下步骤：

1. 在控制台提示符下，输入用户名和密码（默认用户名为“admin”和“guest”，对应的密码为“admin”和“guest”。）输入管理员用户名和密码后，控制界面将显示“Console＃”提示符并进入特权访问模式（即特权操作）。但是当输入“guest”用户名和密码时，控制界面将显示“控制台>”提示进入普通访问模式（即普通操作）。
2. 输入必要的命令以完成所需的任务。
3. 完成后，使用“quit”或“exit”命令退出会话。

通过控制台端口连接到系统后，屏幕显示登陆界面：

```
User Access Verification
Username: admin
Password:
CLI session with the XXXX is opened.
To end the CLI session, enter [Exit].
Console#
```

要通过 Telnet 会话访问交换机，必须先设置该设备的 IP 主单元的地址，如果要从不同的 IP 子网管理交换机则需要设置该 IP 地址的默认网关。 其他步骤与控制台操作相同 。

2 普通命令

普通命令是一些基本功能。

2.1.1 quit

这个命令是退出配置模式。

缺省配置

无

命令模式

普通模式，特权模式

命令用法

在 **quit** 和 **exit** 命令都可以退出配置模式。

范例

这个示例显示如何退出命令操作会话：

```
Console#quit

Press ENTER to start session

User Access Verification

Username:
```

2.1.2 show history

此命令显示命令历史记录缓冲区的内容。

缺省配置

无

命令模式

普通模式，特权模式

命令用法

历史缓冲区大小固定为 10 个执行命令和 10 个配置命令。

范例

在此示例中，show history 命令列出了命令历史记录缓冲区的内容：

```
Console#show history

Execution command history:

2 config

1 show history

Configuration command history:

4 interface vlan 1

3 exit

2 interface vlan 1

1 end

Console#
```

当处于普通模式或特权模式时，“!”命令会重复执行命令历史记录缓冲区中的命令。当您处于任何配置模式时，命令会从配置命令历史记录缓冲区中调出对应的命令进行执行。在此示例中**!2** 命令在执行历史记录缓冲区（**config**）中重复第二个命令 。

```
Console#!2

Console#config

Console(config)#
```

2.1.3 configure

此命令激活全局配置模式。您必须输入此模式才能修改交换机上的任何设置。 在启用某些其他配置模式（例如，接口配置，线路配置和 VLAN 数据配置）之前，还必须进入全局配置模式。

缺省配置

无

命令模式

特权模式

范例

```
Console#configure

Console(config)#
```

2.1.4 restart (PrivilegedExec)

此命令将重新启动设备系统。

注释:当系统重新启动，它总是会运行加电自检。 还可以通过 copy running-config startup-config 命令保留所有的配置信息在存储器中。

缺省配置

无

命令模式

特权模式

命令用法

此命令重置整个系统。

范例

此示例显示如何重置交换机：

```
Console#restart

System will be restarted, continue <y/n>? y
```

2.1.5 end

此命令返回特权模式。

缺省配置

无

命令模式

全局配置，接口配置，线路配置，VLAN 数据库配置和多实例生成树配置.

范例

此示例显示如何从“接口配置”模式返回到特权模式：

```
Console(config-if)#end

Console#
```

2.1.6 exit

此命令返回先前的配置模式或退出配置程序。

缺省配置

无

命令模式

任一模式

范例

此示例显示如何从全局配置模式返回到特权模式模式，然后退出 CLI 会话：

```
Console(config)#exit

Console#exit

Press ENTER to start session

User Access Verification

Username:
```

3 系统管理命令

系统管理命令用于控制系统日志，密码，用户名，管理选项，以及显示或配置各种其他系统信息。

3.1 设备名称

本节介绍用于配置唯一标识交换机的信息的命令。

3.1.1 hostname

此命令指定或修改此设备的主机名。使用“no”命令还原默认主机名。

语法

hostname name

no hostname

name - 主机的名称. (最大字符长度: 255)

缺省配置

无

命令模式

全局模式

范例

```
Console(config)#hostname RD#1

Console(config)#
```

3.2 系统状况

本节介绍用于显示系统信息的命令。

3.2.1 show memory

此命令显示内存利用率参数。

命令模式

普通模式，特权模式

命令用法

此命令显示当前可以自由使用的内存量，分配给活动进程的内存量以及系统内存总量。

范例

```
Console#show memory

Status Bytes %

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

Free 42348544 31

Used 91869184 69

Total 134217728

Alarm Configuration

Rising Threshold : 90%

Falling Threshold : 70%

Console#
```

3.2.2 show process cpu

此命令显示 CPU 利用率参数，警报状态和警报配置。

命令模式

普通模式, 特权模式

范例

```
Console#show process cpu
CPU Utilization in the past 5 seconds : 18%
CPU Utilization in the past 60 seconds
Average Utilization : 16%
Maximum Utilization : 19%
Alarm Status
Current Alarm Status : Off
Last Alarm Start Time : Sep 26 01:39:04 2011
Last Alarm Duration Time : 4 seconds
Alarm Configuration
Rising Threshold : 90%
Falling Threshold : 70%
Console#
```

3.2.3 show running-config

此命令显示当前正在使用的配置信息。

参数

show running-config [**interface** *interface*]

interface

ethernet *单元 / 端口*

unit - 单位标识符. (范围: 1)

port - 端口号. (范围: 1-52)

port-channel *通道标识* (范围: 1-12)

vlan *vlan-id* (范围: 1-4093)

命令模式

特权模式

命令用法

◆ 使用 **interface** 关键字显示指定接口的配置数据。

◆ 将此命令与 **show startup-config** 命令结合使用，将运行内存中的信息与存储在非易失性内存中的信息进行比较。

◆ 此命令显示键命令模式的设置。每个模式组由“!”符号分隔，并包括配置模式命令和相应的命令。此命令显示以下信息：

■ 交换机的 MAC 地址

- SNMP 共用体字符串
- 用户（名称，访问级别和 加密密码）
- VLAN 数据库（VLAN ID，名称和状态）
- 每个接口的 VLAN 配置设置
- 多个生成树实例（名称和接口）
- 为管理 VLAN 配置的 IP 地址
- 接口设置
- 控制台端口和 Telnet 的任意设置

范例

```
Console#show running-config
Building startup configuration. Please wait...
!<stackingDB>00</stackingDB>
!<stackingMac>01_00-e0-0c-00-00-fd_00</stackingMac>
!
snmp-server community public ro
snmp-server community private rw
!
snmp-server enable traps authentication
!
username admin access-level 15
username admin password 7 21232f297a57a5a743894a0e4a801fc3
username guest access-level 0
username guest password 7 084e0343a0486ff05530df6c705c8bb4
enable password level 15 7 1b3231655cebb7a1f783eddf27d254ca
!
vlan database
VLAN 1 name default Vlan media ethernet state active
!
spanning-tree mst configuration
!
interface ethernet 1/1
switchport allowed vlan add 1 untagged
switchport native vlan 1
switchport allowed vlan add 4093 tagged
!

interface vlan 1

ip address dhcp

ip dhcp client class-id text Edge-Core

!

line console
```

```
!
line vty
!
end
!
Console#
```

3.2.4 show startup-config

此命令显示存储在用于启动系统的存储器中的配置文件。

命令模式

特权模式

命令用法

◆ 将此命令与 **show running-config** 命令结合使用，可将运行内存中的信息与存储的信息进行比较。

◆ 此命令显示键命令模式的设置。每个模式组由“!”符号分隔，并包括配置模式命令和相应的命令。此命令显示以下信息：

- 交换机的 MAC 地址
- SNMP 共用体字符串
- SNMP 陷阱身份验证
- 用户（名称和访问级别）
- VLAN 数据库（VLAN ID，名称和状态）
- 多个生成树实例（名称和接口）
- 每个接口的接口设置和 VLAN 配置设置
- 管理 VLAN 的 IP 地址
- console 端口和 Telnet 的 任何已配置设置

范例

有关正在运行的配置文件，请参阅示例。

3.2.5 show system

此命令显示系统信息。

缺省配置

无

命令模式

普通模式，特权模式

命令用法

有关此命令显示系统相关信息的说明　。

范例

```
Console#show system

System Description : DG-GS4628T

System OID String : 1.3.6.1.4.1.259.10.1.24.1

System Information

System Up Time : 0 days, 0 hours, 52 minutes, and 2.21 seconds

System Name :

System Location :

System Contact :

MAC Address (Unit 1) : 00-E0-00-00-00-01

Web Server : enabled

Web Server Port : 80

Web Secure Server : enabled

Web Secure Server Port : 443

Telnet Server : enabled

Telnet Server Port : 23

Jumbo Frame : disabled

Console#
```

3.2.6 show users

显示所有活动的控制台和 Telnet 会话，包括 Telnet 客户端的用户名，空闲时间和 IP 地址。

缺省配置

无

命令模式

普通模式，特权模式

命令用法

用于执行此命令的会话由行旁边的“*”符号表示（即会话）索引号。

范例

```
Console#show users

User Name Accounts:

User Name Privilege Public-Key

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

admin 15 无

guest 0 无

steve 15 RSA

Online Users:

Line Username Idle time (h:m:s) Remote IP addr.

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

0 console admin 0:14:14

* 1 VTY 0 admin 0:00:00 192.168.1.19

2 SSH 1 steve 0:00:06 192.168.1.19

Web Online Users:

Line Remote IP Addr User Name Idle time (h:m:s)

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

1 HTTP 192.168.1.19 admin 0:00:00

Console#
```

3.2.7 show version

此命令显示系统的硬件和软件版本信息。

命令模式

普通模式，特权模式

命令用法

无

范例

```
Console#show version

Unit 1

Serial Number : A35018426

Number of Ports : 28

Main Power Status : Up

Loader Version : 111.9.21.1

Operation Code Version : 10.28.09.50

Console#
```

3.3 帧长度管理

本节介绍用于在交换机上配置以太网帧大小的命令。

3.3.1 jumbo frame

此命令用于启用千兆以太网端口的 2 层超大帧的配置。 使用 no 形式可以关闭这个功能。

语法

[no] jumbo frame

缺省配置

禁用

命令模式

全局配置

命令用法

◆ 此交换机允许千兆以太网端口上的 2 层超大帧到 10240 字节，为大型数据传输提供更高效的吞吐量。与 1.5 KB 的标准以太网帧相比，使用超大帧可明显降低处理协议封装字段所需的开销。

◆ 要使用超大帧，源端节点和目标端节点（如计算机或服务器）必须支持此功能。 此外，当连接以全双工模式运行时，两个端节点之间的网络中的所有交换机必须能够接受扩展的帧大小。 对于半双工连接，冲突域中的所有设备都需要支持超大帧。

◆ 超大帧的当前设置可以使用 show system 命令进行显示。

范例

```
Console(config)#jumbo frame

Console(config)#
```

3.4 文件管理

固件管理

固件可以上传到 FTP / TFTP 服务器或从 FTP / TFTP 服务器下载。通过将运行时代码保存到 FTP / TFTP 服务器上的文件，该文件可以随后下载到交换机以恢复操作。该开关还可以设置为使用新固件而不覆盖以前的版本。

下载运行时代码时，可以指定目标文件名来替换当前映像，或者可以使用当前运行时代码文件中的不同名称首先下载文件，然后将新文件设置为启动文件。

下载运行时代码时，可以指定目标文件名来替换当前映像，或者可以使用当前运行时代码文件中的不同名称首先下载文件，然后将新文件设置为启动文件。

保存或恢复配置设置

可以从 FTP/ TFTP 服务器上载和下载设备配置文件。稍后可以将这个配置文件做为系统重启后的配置文件。

可以使用新文件名下载配置文件，然后将其设置为启动文件，或者可以将当前启动配置文件指定为目标文件以直接替换它。请注意，文件“Factory_缺省配置_Config.cfg”可以复制到 FTP / TFTP 服务器，但不能用作交换机上的目标。

3.4.1 boot system

此命令指定用于启动系统的文件或映像。

语法

boot system {**boot-rom** | **config** | **opcode**}: *filename*

boot-rom* - 启动 ROM.

config* - 配置文件.

opcode* - 当前运行程序.

filename - 配置文件或者系统文件的名字.

* The colon (:) is required.

缺省配置

无

命令模式

全局配置

命令用法

- 指定的文件类型后需要冒号（:）。
- 如果文件包含错误，则无法将其设置为默认文件。

范例

```
Console(config)#boot system config: startup

Console(config)#
```

3.4.2 boot system

此命令指定用于启动系统的文件或映像。

语法

boot system {**boot-rom** | **config** | **opcode**}: *filename*

boot-rom* - 启动 ROM.

config* - 配置文件.

opcode* - 当前运行程序.

filename - 配置文件或者系统文件的名字.

* The colon (:) is required.

缺省配置

无

命令模式

全局配置

命令用法

- 指定的文件类型后需要冒号（:）。
- 如果文件包含错误，则无法将其设置为默认文件。

范例

```
Console(config)#boot system config: startup

Console(config)#
```

3.4.3 delete

此命令删除文件或图像。

语法

delete *filename*

filename -配置文件或代码映像的名称。

缺省配置

无

命令模式

特权模式

命令用法

- 如果文件用于系统启动，则无法删除此文件。
- 无法删除“Factory_缺省配置_Config.cfg”。

范例

此示例显示如何从闪存中删除 test2.cfg 配置文件。

```
Console#delete test2.cfg

Console#
```

3.4.4 whichboot

此命令显示系统启动时引导的文件。

语法

whichboot

缺省配置

无

命令模式

特权模式

范例

此示例显示 **whichboot** 命令显示的信息。有关此命令显示的文件信息的说明， 请参阅 **dir** 命令下的表 。

```
Console#whichboot
```

```
File Name Type Startup Modify Time Size(bytes)

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

Unit 1:

DG-GS4628T_V1.0.0.0.bix OpCode Y 1970-01-01 00:00:00 12509804

startup1.cfg Config Y 2011-11-08 07:34:33 1547

Console#
```

3.4.5 upgrade opcode auto

当在 upgrade opcode path 命令指示的服务器上检测到新版本时，此命令会自动升级当前操作代码。使用此命令的 no 形式恢复默认设置。

语法

[no] upgrade opcode auto

缺省配置

禁用

命令模式

全局配置

命令用法

◆此命令用于启用或禁用操作代码的自动升级。当交换机启动并通过此命令启用自动系统更新时，交换机将在启动时按照以下步骤操作：

1. 它将在 upgrade opcode path 命令指定的位置搜索新版本的映像。TFTP 服务器上存储的新映像的名称必须为指定的文件名。如果交换机检测到的代码版本比当前使用的代码版本更新，则会下载新映像。如果交换机中已存储了两个代码映像，则未设置为启动系统的映像将被新版本覆盖。
2. 下载映像后，交换机将发送陷阱消息，以记录升级操作是否有效。
3. 它将新版本设置为启动映像。
4. 然后重新启动系统以开始使用新图像。

◆可以使用 show running-config 或 show startup-config 命令显示对默认设置所做的任何更改 。

范例

```
Console(config)#upgrade opcode auto

Console(config)#upgrade opcode path tftp://192.168.0.1/sm24/

Console(config)#
```

如果在指定位置找到新映像，则在启动期间将显示以下类型的消息。

```
...
```

```
Automatic Upgrade is looking for a new image

New image detected: current version 1.1.1.0; new version 1.1.1.2

Image upgrade in progress

The switch will restart after upgrade succeeds

Downloading new image

Flash programming started

Flash programming completed

The switch will now restart

...
```

3.4.6 upgrade opcode path

此命令指定存储 new opcode 的 TFTP 服务器和目录。使用此命令的 no 形式清除当前设置。

语法

upgrade opcode path *opcode-dir-url*

no upgrade opcode path

opcode-dir-url - The location of the new code.

缺省配置

无

命令模式

全局配置

命令用法

◆此命令与 upgrade opcode auto 命令一起使用，以便于自动升级在此命令指示的位置存储的新操作代码 。

◆存储在 TFTP 服务器上的新映像的名称必须为指定的文件名。但请注意，此命令不包含文件名。

◆指定 TFTP 服务器时，必须使用以下语法，其中 *filedir* 指示包含新的映像文件的目录的路径：TFTP：//192.168.0.1 [/ FILEDIR] /

◆指定 FTP 服务器时，必须使用以下语法，其中 *filedir* 指示包含新的映像文件的目录的路径：

ftp：// [username [：password @]] 192.168.0.1 [/ filed ir] /

如果省略用户名，则“anonymous”将用于连接。如果省略密码，则将使用空字符串（“”）进行连接。

范例

这显示了如何指定存储新代码的 TFTP 服务器。

```
Console(config)#upgrade opcode path tftp://192.168.0.1/sm24/

Console(config)#
```

这显示了如何指定存储新代码的 FTP 服务器。

```
Console(config)#upgrade opcode path ftp://admin:billy@192.168.0.1/sm24/

Console(config)#
```

3.4.7 upgrade opcode reload

此命令在操作码升级后自动重新加载交换机完成。使用 no 形式禁用此功能。

语法

[no] upgrade opcode reload

缺省配置

禁用

命令模式

全局配置

范例

这显示了如何指定存储新代码的 TFTP 服务器。

```
Console(config)#upgrade opcode reload

Console(config)#
```

3.4.8 show upgrade

此命令显示操作码升级配置设置。

命令模式

特权模式

范例

```
Console#show upgrade

Auto Image Upgrade Global Settings:

Status : Disable

Reload Status : Disable

Path :
```

```
File Name : xxxx-Series.bix

Console#
```

3.5 事件记录

本节介绍用于在交换机上配置事件日志记录的命令。

3.5.1 logging facility

此命令设置远程记录 syslog 消息的设施类型。使用 no 形式将类型返回到默认值。

语法

logging facility *type*

no logging facility

type --一个数字，指示 syslog serverto 调度日志消息使用的工具到适当的服务。 （范围：16-23）

缺省配置

23

命令模式

全局配置

命令用法

该命令指定 syslog 消息中发送的设施类型标记。（请参阅 RFC 3164。）此类型对交换机报告的消息类型没有影响。但是，syslog 服务器可以使用它来对消息进行排序，以将消息存储在相应的数据库中。

范例

```
Console(config)#logging facility 19

Console(config)#
```

3.5.2 logging history

此命令根据严重性限制保存到交换机内存的系统日志消息。no 形式返回系统日志消息的缺省等级的记录。

语法

logging history {**flash** | **ram**} *level*

no logging history {**flash** | **ram**}

flash -存储在闪存中的事件历史记录（即永久存储器）。

ram -存储在临时 RAM 中的事件历史记录（即，电源复位时的内存刷新）。

level -下面列出的级别之一。 发送的消息包括所选级别至级别 0.（范围：0-7）

级别严重性名称描述

7 调试调试消息

6 仅供参考。仅供参考

5 通知正常但重要的条件，例如冷启动

4 警告警告条件（例如，返回错误，意外返回）

3 错误错误条件（例如，无效输入，默认使用）

2 个关键临界条件（例如，内存分配或 freememory 错误）

1 警报需要立即采取行动

0 紧急情况系统无法使用

缺省配置

Flash: errors (level 3 - 0)

RAM: debugging (level 7 - 0)

命令模式

全局配置

命令用法

为闪存指定的消息级别必须具有更高的优先级（即数值较低），而不是 RAM 指定的值。

范例

```
Console(config)#logging history ram 0

Console(config)#
```

3.5.3 logging host

此命令添加将接收记录消息的系统日志服务器主机 IP 地址。使用 **no** 形式删除 syslog 服务器主机。

语法

[no] **logging host** *host-ip-address*

host-ip-address -系统日志服务器的 IP 地址。

缺省配置

无

命令模式

全局配置

命令用法

◆多次使用此命令构建主机 IP 地址列表。

◆允许的最大主机 IP 地址数为 5。

范例

```
Console(config)#logging host 10.1.0.3
Console(config)#
```

3.5.4 logging on

此命令控制错误消息的记录，将调试或错误消息发送到日志记录过程。no 形式禁用日志进程。

语法

[no] **logging on**

缺省配置

无

命令模式

全局配置

命令用法

日志记录过程控制保存到切换内存或者发送到远程 syslog 服务器的错误消息。您可以使用 logging history 命令控制存储在内存中的错误消息的类型。您可以使用 logging trap 命令来控制指定的 syslog 服务器上发送的错误消息的类型。

范例

```
Console(config)#logging on
Console(config)
```

3.5.5 logging trap

此命令可以将系统消息记录到远程服务器，或者根据严重性限制保存到远程服务器的系统日志消息。使用此命令不带指定级别来启用远程日志记录。使用 no 形式禁用远程日志记录。

语法

logging trap [**level** *level*]

no logging trap [**level**]

level -系统日志严重性级别之一。发送的消息包括通过级别 0 的所选级别。

缺省配置

禁用

等级 7

命令模式

全局配置

命令用法

◆使用具有指定级别的此命令可启用远程日志记录并设置要保存的最低严重性级别。

◆使用不带指定级别的此命令也会启用远程 logging，但会将最低级别恢复为默认级别。

范例

```
Console(config)#logging trap 4

Console(config)#
```

3.5.6 clear log

此命令清除日志缓冲区中的消息。

语法

clear log [**flash** | **ram**]

flash -存储在闪存中的事件历史记录（即永久性的记忆）。

ram -存储在临时 RAM 中的事件历史记录（即内存刷新关于电源复位）。

缺省配置

Flash and RAM

命令模式

特权模式

范例

```
Console#clear log

Console#
```

3.5.7 show log

此命令显示存储在本地内存中的日志消息。

语法

show log {**flash** | **ram**}

flash -存储在闪存中的事件历史记录（即永久存储器）。

ram -存储在临时 RAM 中的事件历史记录（即电源复位时的内存刷新）。

缺省配置

无

命令模式

特权模式

命令用法

◆热启动后（即通过命令界面重置电源），所有日志消息都保留在 RAM 和 Flash 中。

◆所有日志消息都保留在 Flash 中，并在重新启动后从 RAM 中清除（即关闭电源然后通过电源打开）。

范例

以下示例显示了存储在 RAM 中的事件消息。

```
Console#show log ram

[1] 00:01:30 2001-01-01

"VLAN 1 link-up notification."

level: 6, module: 5, function: 1, and event no.: 1

[0] 00:01:30 2001-01-01

"Unit 1, Port 1 link-up notification."

level: 6, module: 5, function: 1, and event no.: 1

Console#
```

3.5.8 show logging

此命令显示将邮件记录到本地交换机内存,SMTP 事件处理程序或远程 syslog 服务器的配置设置。

语法

show logging {**flash** | **ram** | **sendmail** | **trap**}

flash -显示用于在 flashmemory（即永久内存）中存储事件消息的设置。

ram -显示用于在临时 **RAM** 中存储事件消息的设置（即在电源复位时刷新的内存）。

sendmail -显示 SMTP 事件处理程序的设置。

trap -显示陷阱功能的设置。

缺省配置

无

命令模式

特权模式

范例

以下示例显示启用了系统日志记录，闪存的消息级别为“错误”（即默认级别 3 - 0），RAM 的主题级别为“调试”（即默认级别 7 - 0）。

```
Console#show logging flash

Syslog logging: Enabled

History logging in FLASH: level errors

Console#show logging ram

Syslog logging: Enabled

History logging in RAM: level debugging

Console#
```

3.6 SMTP 告警

这些命令配置 SMTP 事件处理，并将警报消息转发到指定的 SMTP 服务器和电子邮件收件人。

3.6.1 logging sendmail

此命令启用 SMTP 事件处理。使用 no 形式禁用此功能。

语法

[no] logging sendmail

缺省配置

启用

命令模式

全局配置

范例

```
Console(config)#logging sendmail
Console(config)#
```

3.6.2 logging sendmail host

此命令指定将发送警报消息的 SMTP 服务器。使用 no 形式删除 SMTP 服务器。

语法

[no] logging sendmail host *ip-address*

ip-address -将发送事件处理警报消息的 SMTP 服务器的 IPv4 或 IPv6 地址。

缺省配置

无

命令模式

全局配置

命令用法

◆您最多可以指定三个 SMTP 服务器进行事件处理。但是您必须输入单独的命令来指定每个服务器。

◆要发送电子邮件警报，交换机首先打开一个连接，逐个发送队列中等待的所有电子邮件警报，然后关闭连接。

◆要打开连接，交换机首先选择在上次连接期间成功发送邮件的服务器，或者此命令配置的第一台服务器。如果无法发送邮件交换机将选择列表中的下一个服务器并尝试再次发送邮件。如果仍然失败，系统将以定期间隔重复该过程。（如果交换机无法成功打开连接，则会触发陷阱。）

范例

```
Console(config)#logging sendmail host 192.168.1.19

Console(config)#
```

3.6.3 logging sendmail level

此命令设置用于触发警报消息的严重性阈值。使用 no 形式恢复默认设置。

语法

logging sendmail level *level*

no logging sendmail level

level -系统消息级别之一。消息发送包括将所选级别降低到级别 0.（范围：0-7;默认值：7）

缺省配置

等级 7

命令模式

全局配置

命令用法

指定的级别表示事件阈值。此级别或更高级别的所有事件都将发送给已配置的电子邮件收件人。

（例如使用 Level 7 将报告从级别 7 到级别 0 的所有事件。）

范例

此示例将从 3 级到 0 级发送系统错误的电子邮件警报。

```
Console(config)#logging sendmail level 3

Console(config)#
```

3.6.4 logging sendmail destination-email

此命令指定警报消息的电子邮件收件人。使用 no 形式删除收件人。

语法

[no] **logging sendmail destination-email** *email-address*

email-address -警报消息中使用的源电子邮件地址。（范围：1-41 个字符）

缺省配置

无

命令模式

全局配置

命令用法

您最多可以为警报消息指定五个收件人。但是您可以使用单独的命令来指定每个收件人。

范例

```
Console(config)#logging sendmail destination-email ted@this-company.com

Console(config)#
```

3.6.5 logging sendmail source-email

此命令设置用于告警信息中“From”字段的电子邮件地址。使用 no 形式恢复默认值。

语法

logging sendmail source-email *email-address*

no logging sendmail source-email

email-address -警报消息中使用的源电子邮件地址。（范围：1-41 个字符）

缺省配置

无

命令模式

全局配置

命令用法

您可以使用标识交换机的符号电子邮件地址或负责交换机的管理员的地址。

范例

```
Console(config)#logging sendmail source-email bill@this-company.com

Console(config)#
```

3.6.6 show logging sendmail

此命令显示 SMTP 事件处理程序的设置。

命令模式

普通模式，特权模式

范例

```
Console#show logging sendmail

SMTP servers

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

192.168.1.19

SMTP Minimum Severity Level: 7

SMTP destination email addresses

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

ted@this-company.com

SMTP Source Email Address: bill@this-company.com

SMTP Status: Enabled

Console#
```

3.7 时间

可以通过轮询一组指定的时间服务器（NTP 或 SNTP）来动态设置系统时钟。在交换机上保持准确的时间使系统日志能够记录事件条目的有意义的日期和时间。如果未设置时钟，则交换机将仅记录上次启动时设置的出厂默认设置的时间。

3.7.1 sntp client

此命令启用 SNTP 客户端对　使用 sntp server 命令指定的时间同步从 NTP 或 SNTP 时间服务器的请求。使用 no 形式禁用 SNTP 客户端请求。

语法

[no] sntp client

缺省配置

禁用

命令模式

全局配置

命令用法

◆从时间服务器获取的时间用于记录日志事件的准确日期和时间。如果没有 SNTP，交换机仅记

录从上次启动时设置的出厂默认值开始的时间（即 2001 年 1 月 1 日 00：00：00）。

◆ 此命令启用客户端时间请求以使用 sntp server 命令指定的服务器时间。它基于通过 sntp poll 命令设置的间隔发出时间同步请求 。

范例

```
Console(config)#sntp server 10.1.0.19

Console(config)#sntp poll 60

Console(config)#sntp client

Console(config)#end

Console#show sntp

Current Time: Dec 23 02:52:44 2002

Poll Interval: 60

Current Mode: unicast

SNTP Status : Enabled

SNTP Server 137.92.140.80 0.0.0.0 0.0.0.0

Current Server: 137.92.140.80

Console#
```

3.7.2 sntp poll

此命令设置当交换机设置为 SNTP 客户端模式时发送时间请求之间的间隔。使用 no 形式还原到默认值。

语法

sntp poll *seconds*

no sntp poll

seconds -时间请求之间的间隔。（范围：16-16384 秒）

缺省配置

16 秒

命令模式

全局配置

范例

```
Console(config)#sntp poll 60

Console#
```

3.7.3 sntp server

此命令设置发出 SNTP 时间请求的服务器的 IP 地址。使用不带参数的这个命令清除当前列表中的所有时间服务器。使用 no 形式清除当前列表中的所有时间服务器或清除特定服务器。

语法

sntp server [*ip1* [*ip2* [*ip3*]]]

no sntp server [*ip1* [*ip2* [*ip3*]]]

ip -时间服务器的 IP 地址(NTP or SNTP).(Range: 1 - 3 addresses)

缺省配置

无

命令模式

全局配置

命令用法

此命令设置发布 SNTP 时间请求的服务器的 IP 地址。使用此命令参数来清除当前列表中的所有时间服务器。使用“no”窗体清除当前列表中的所有时间服务器，或清除特定服务器。

范例

```
Console(config)#sntp server 10.1.0.19

Console#
```

3.7.4 show sntp

此命令显示 SNMP 客户端的当前时间和配置设置，并指示本地时间是否已正确更新。

命令模式

普通模式, 特权模式

命令用法

此命令显示当前时间，用于发送时间同步请求的轮询间隔以及当前 SNTP 模式（即单播）。

范例

```
Console#show sntp
```

```
Current Time : Nov 5 18:51:22 2006

Poll Interval : 16 seconds

Current Mode : Unicast

SNTP Status : Enabled

SNTP Server : 137.92.140.80 0.0.0.0 0.0.0.0

Current Server : 137.92.140.80

Console#
```

3.7.5 ntp authenticate

此命令启用 NTP 客户端 – 服务器通信的身份验证。 使用 no 形式禁用身份验证。

语法

[no] ntp authenticate

缺省配置

禁用

命令模式

全局配置

命令用法

可以启用 NTP 身份验证，以确保只从授权的 NTP 服务器接收可靠的更新。身份验证密钥及其相关的密钥号必须集中管理，并手动分发到 NTP 服务器和客户端。密钥号和键值必须在服务器和客户端上匹配。

范例

```
Console(config)#ntp authenticate

Console(config)#
```

3.7.6 ntp authentication-key

此命令配置了在 NTP 身份验证被使用时使用的身份验证密钥和密钥号。使用命令的 no 形式来清除当前列表中的特定身份验证密钥或所有密钥。

语法

ntp authentication-key *number* md5 *key*

no ntp authentication-key [*number*]

number - The NTP authentication key ID number. (Range: 1-65535)

md5 -指定使用消息摘要算法 5 提供身份验证。

key - 一个认证密钥的 MD5 字符串。关键字最多可达到 32 个大小敏感的可打印 ASCII 字符。(没有空格)。

缺省配置

无

命令模式

全局配置

命令用法

◆关键号指定 NTP 认证密钥列表中的键值。在交换机上可以配置多达 255 个关键字。为要配置的每个服务器重新输入此命令。

◆注意，NTP 认证密钥号和值必须匹配服务器和客户端两者。

◆NTP 认证是可选的。当使用 NTP 认证命令启用时，还必须使用此命令配置至少一个密钥号。

◆使用此命令的 no 形式，而无需参数来清除列表中的所有身份验证密钥。

范例

```
Console(config)#ntp authentication-key 45 md5 thisiskey45
Console(config)#
```

3.7.7 ntp client

此命令允许 NTP 客户端从 NTP 服务器命令指定的 NTP 时间服务器中进行时间同步请求。使用 no 形式禁用 NTP 客户端请求。

语法

[no] ntp client

缺省配置

禁用

命令模式

全局配置

命令用法

◆SNTP 和 NTP 客户端不能同时进行加密。首先在使用此命令之前禁用 SNTP 客户端。

◆从时间服务器获取的时间用于记录日志事件的精确日期和时间。没有 NTP，开关只记录从上次引导时设置的工厂默认值开始的时间（即，00:00:00,2001 年 1 月 1 日）。

◆此命令允许客户端时间请求到时间服务器指定的 VIAE-NTP 服务器命令。它通过 NTP 轮询命令基于时间间隔发出时间同步请求。

范例

```
Console(config)#ntp client
Console(config)#
```

3.7.8 ntp server

此命令设置向其发出 NTP 时间请求的服务器的 IP 地址。使用 no 形式清除当前列表中的特定时间服务器或所有服务器。

语法

ntp server *ip-address* [**key** *key-number*]

no ntp server [*ip-address*]

ip-address - NTP 时间服务器的 IP 地址。

key-number -与服务器使用通信的身份验证密钥的编号。（范围：1-65535）

缺省配置

版本号：3

命令模式

全局配置

命令用法

◆此命令指定当设置为 NTP 客户端模式时交换机将轮询时间更新的时间服务器。它根据使用 **ntp poll** 命令设置的时间间隔发出时间同步**请求**。客户端将轮询所有配置的服务器，对收到的响应进行过滤和比较，以确定交换机的最可靠和准确的时间更新。

◆您最多可以在交换机上配置 50 个 NTP 服务器。 为要配置的每个服务器重新输入这个命令。

◆NTP 身份验证是可选的。如果使用 **ntp authenticate** 命令启用，则还必须使用 **ntp authentication-key** 命令配置至少一个密钥编号。

◆ 如果**没有**参数，请使用此命令的 no 形式清除列表中的所有配置服务器。

范例

```
Console(config)#ntp server 192.168.10.20

Console(config)#ntp server 192.168.10.11

Console(config)#ntp server 192.168.5.25 key 21

Console(config)#
```

3.7.9 show ntp

此命令显示 NTP 客户端的当前时间和配置设置，并指示本地时间是否已正确更新。

命令模式

普通模式，特权模式

命令用法

此命令显示当前时间，用于发送时间同步请求的轮询间隔以及当前 NTP 模式（即单播）。

范例

```
Console#show ntp

Current Time : Apr 20 18:37:34 2015

Polling : 1024 seconds

Current Mode : unicast

NTP Status : Disabled

NTP Authenticate Status : Enabled

Last Update NTP Server : 0.0.0.0 Port: 0

Last Update Time : Jan 1 00:00:00 1970 UTC

NTP Server 192.168.10.20 version 3

NTP Server 192.168.10.21 version 3

NTP Server 192.168.3.22 version 3 key 3

NTP Authentication Key 19 md5 42V68751663T6K11P2J307210R885

Console#
```

3.7.10 clock timezone

此命令设置交换机内部时钟的时区。

语法

clock timezone *name* **hour** *hours* **minute** *minutes*{**before-utc** | **after-utc**}

name -时区名称，通常是首字母缩写词。 （范围：1-30 个字符）

hours - UTC 之前/之后的小时数。 （范围：UTC 前 0-12 小时，UTC 后 0-13 小时）

minutes - UTC 之前/之后的分钟数。 （范围：0-59 分钟）

before-utc -设置 UTC 之前（东）的本地时区。

after-utc -设置 UTC（西）之后的本地时区。

缺省配置

无

命令模式

全局配置

命令用法

此命令根据地球的本初子午线，零度经度设置相对于 CoordinatedUniversal Time（UTC，以前的格林威治标准时间或 GMT）的本地时区。 要显示与当地时间相对应的时间，您必须指明您的时区在 UTC 的东（之前）或之前（之后）的小时数和分钟数。

范例

```
Console(config)#clock timezone Japan hours 8 minute 0 after-UTC
Console(config)#
```

3.7.11 calendar set

该命令用于设置系统时钟。如果您的网络上没有时间服务器，或者您没有将交换机配置为从时间服务器接收信号，则可以使用它。

语法

calendar set *hour min sec* {*day month year* | *month day year*}

hour - 24 小时制的小时。 （范围：0 - 23）

min -分钟。 （范围：0 - 59）

sec -秒。 （范围：0 - 59）

day -月的一天。 （范围：1 - 31）

month -一月 | 二月 | 三月 | 四月 | 可能 | 六月 | 七月 | 八月 | 九月 | 十月 | 十一月 | 十二月

year -年（4 位数）。 （范围：1970 - 2037）

缺省配置

无

命令模式

特权模式

命令用法

请注意，启用 SNTP 时，无法手动配置系统时钟。

范例

此示例显示如何将系统时钟设置为 1 6 ：1 7 ：3 5 ，February1st，201 6 。

```
Console#calendar set 16:17:35 1 February 2016

Console#
```

3.7.12 show calendar

此命令显示系统时钟。

缺省配置

无

命令模式

普通模式，特权模式

范例

```
Console#show calendar

16:17:35 1 February 2016

Console#
```

3.8 时间范围

本节介绍用于设置其他功能（如访问控制列表）使用的时间范围的命令。

3.8.1 time-range

此命令指定时间范围的名称，并进入时间范围配置模式。使用 no 形式删除以前指定的时间范围。

语法

[no] time-range *name*

name -时间范围的名称。（范围：1-16 个字符）

缺省配置

无

命令模式

全局配置

命令用法

此命令设置其他功能使用的时间范围，比如访问控制列表。

范例

```
Console(config)#time-range r&d

Console(config-time- range)#
```

3.8.2 absolute

此命令设置执行命令的时间范围。使用 no 形式删除先前指定的时间。

语法

absolute start *hour minute day month year*[end *hour minutes day month year*]

absolute end *hour minutes day month year*

no absolute

hour - 24 小时制的小时。 （范围：0-23）

minute -分钟。（范围：0-59）

day -月的一天。（范围：1-31）

month -一月 | 二月 | 三月 | 四月 | 可能 | 六月 | 七月 | 八月 | 九月 | 十月 | 十一月| 十二月

year -年（4 位数）。（范围：2009-2109）

缺省配置

无

命令模式

时间范围配置

命令用法

◆ 如果已配置时间范围，则必须使用此命令的 no 形式在配置新时间范围之前删除当前条目 。

◆ 如果为相同的时间范围（即命名条目）配置了绝对规则和一个或多个周期性规则，则只有当前时间在绝对时间范围和周期性时间范围之一时，该条目才会生效。

范例

此示例配置单次事件发生的时间。

```
Console(config)#time-range r&d
Console(config-time-range)#absolute start 1 23 april 2014 end 2 3 1 april
2014
Console(config-time-range)#
```

3.8.3 periodic

此命令设置定期执行某一命令的时间范围。 使用 no 形式删除先前指定的时间范围。

语法

[no] periodic {daily | friday | monday | saturday | sunday |thursday | tuesday | wednesday | weekdays | weekend} *hour minute* to {daily | friday | monday | saturday | sunday |thursday | tuesday | wednesday | weekdays | weekend |*hour minute*}

daily - 每日

friday -星期五

monday -星期一

saturday -星期六

sunday -星期天

thursday -星期四

tuesday -星期二

wednesday -星期三

weekdays -工作日

weekend -周末

hour - 24 小时制的小时。 （范围：0-23）

minute -分钟。 （范围：0-59）

缺省配置

无

命令模式

时间范围配置

命令用法

- 如果已配置时间范围，则必须使用此命令的 no 形式在配置新时间范围之前删除当前条目。
- 如果为相同的时间范围（即命名条目）配置了绝对规则和一个或多个周期性规则，则只有当前时间在绝对时间范围和周期性时间范围之一时，该条目才会生效。

范例

此示例配置定期发生事件的时间范围。

```
Console(config)#time-range sales
Console(config-time-range)#periodic daily 2 1 to 3 1
Console(config-time-range)#
```

3.8.4 show time-range

此命令显示已配置的时间范围。

语法

show time-range [*name*]

name -**语法**

缺省配置

无

命令模式

特权模式

范例

```
Console#show time-range r&d
Time-range r&d:
absolute start 01:01 01 April 2009
periodic Daily 01:01 to Daily 02:01
```

```
periodic Daily 02:01 to Daily 03:01
Console#
```

4 SNMP 命令

SNMP 命令使用简单网络管理协议（SNMP）控制从管理站访问此交换机，以及发送到陷阱管理器的错误类型。

SNMP 版本 3 还提供涵盖消息的安全功能完整性，身份验证和加密;以及控制用户访问 MIB 树的特定区域。要使用 SNMPv3，首先设置 SNMP engineID（或接受默认值），为 MIBtree 指定读写访问视图，使用所需的安全模型（即 SNMP v1，v2c 或 v3）和安全级别配置 SNMP 用户组（即身份验证和隐私），然后将 SNMP 用户及其特定的身份验证和隐私密码分配给这些组。

4.1 常规 SNMP 命令

4.1.1 snmp-server

此命令为所有管理客户端（即版本 1,2c，3）启用 SNMPv3 引擎和服务。使用 no 形式禁用服务器。

语法

[no] snmp-server

缺省配置

启用

命令模式

全局配置

范例

```
Console(config)#snmp-server
Console(config)#
```

4.1.2 snmp-servercommunity

此命令定义用于授权客户端使用 SNMPv1 或 v2c 进行管理访问的社区访问字符串。使用 **no** 形式删除指定的社区字符串。

语法

snmp-server community *string* [**ro** | **rw**]

no snmp-server community *string*

string - 共用体字符串，其作用类似于密码并允许访问 SNMP 协议。（最大长度：32 个字符，区分大小写;最大字符串数：5）

ro -指定只读访问权限。授权管理站只能检索 MIB 对象。

rw -指定读/写访问权限。授权管理站能够检索和修改 MIB 对象。

缺省配置

◆public -只读访问权限。授权管理站仅能检索 MIB 对象。

◆private -读/写访问权限。授权管理站能够检索和修改 MIB 对象。

命令模式

全局配置

范例

```
Console(config)#snmp-server community alpha rw

Console(config)#
```

4.1.3 snmp-server contact

此命令设置系统联系人字符串。使用 **no** 形式删除系统联系信息。

语法

snmp-server contact *string*

no snmp-server contact

string -描述系统联系信息的字符串。（最大长度：255 个字符）

缺省配置

无

命令模式

全局配置

范例

```
Console(config)#snmp-server contact Paul

Console(config)#
```

4.1.4 snmp-server location

此命令设置系统位置字符串。使用 no 形式删除位置字符串。

语法

snmp-server location *text*

no snmp-server location

text -描述系统位置的字符串。(最大长度：255 个字符)

缺省配置

无

命令模式

全局配置

范例

```
Console(config)#snmp-server location WC-19

Console(config)#
```

4.1.5 show snmp

此命令可用于检查 SNMP 通信的状态。

缺省配置

无

命令模式

普通模式，特权模式

命令用法

此命令提供有关共用体字符串，SNMP 输入和输出协议数据单元的计数器以及是否已使用 **snmp-server enable traps** 命令**启用 SNMP** 日志记录的信息 。

范例

```
Console#show snmp
```

```
SNMP Agent : Enabled

SNMP Traps :

Authentication : Enabled

Link-up-down : Enabled

SNMP Communities :

1. public, and the access level is read-only

2. private, and the access level is read/write

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

0 No such name errors

0 Bad values errors

0 General errors

0 Response PDUs

0 Trap PDUs

SNMP Logging: Disabled

Console#
```

4.2 SNMP Target Host Commands

4.2.1 snmp-server enable traps

此命令使此设备能够发送简单网络管理协议陷阱或通知（即 SNMP 通知）。 使用 no 形式去禁用 SNMP 通知。

语法

[no] snmp-server enable traps [authentication | link-up-down |ethernet cfm]

authentication -发出身份验证失败通知的关键字。

link-up-down -发出链接或链接断开通知的关键字。

ethernet cfm -连接故障管理陷阱。

缺省配置

发出身份验证和链接向上陷阱

命令模式

全局配置

命令用法

◆如果未输入 snmp-server enable traps 命令，则会发送此命令控制的非通知。要将此设备配置为发送 SNMP 通知，您必须至少输入一个 snmp-server enable traps 命令。如果输入逗号为 no 的关键字，则启用身份验证和链接向上通知。如果输入带有关键字的命令，则仅启用与该关键字相关的语言类型。

◆本 SNMP 服务器启用陷阱指令是结合任意不等阶小号 SNMP-服务器主机命令中使用。使用 snmp-server host 命令指定哪些主机接收 SNMP 通知。在发送通知中，您必须至少配置一个 snmp-server host 命令。

◆身份验证，链接和链接断开陷阱是一种错误，因此当用于 SNMP 版本 3 主机时，必须与 snmp-server group 命令分配的“通知视图”中的相应条目一起启用它们 。

范例

```
Console(config)#snmp-server enable traps link-up-down
Console(config)#
```

4.2.2 snmp-server host

此命令指定简单网络管理协议通知操作的收件人。使用 no 形式删除指定的主机。

语法

snmp-server host *host-addr* [**inform** [**retry** *retries* |**timeout** *seconds*]] *community-string*[**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**} [**udp-port** *port*]}

no snmp-server host *host-addr*

host-addr -*主机的* Internet 地址（目标收件人）。（最大主机地址：5 个陷阱目标 IP 地址条目）

inform -通知作为通知消息发送。请注意此选项仅适用于版本 2c 和 3 主机。（默认值：使用陷阱）

retries-如果收件人未确认收到，则重新发送通知消息的最大次数。（范围：0-255;默认值：3）

seconds -重新发送通知消息之前等待确认的秒数。（范围：0-2147483647 厘秒;默认值：1500 厘秒）

community-string-与通知操作一起发送到 SNMP V1 和 V2C 主机的密码类共用体字符串。虽然您可以单独使用 snmp-server 主机命令设置这个字符串，但我们建议在使用 snmp-server 主机命令之前使用 snmp-server 共用体命令定义它。（最大长度：32 个字符）

version -指定是否将通知作为 SNMP Version1,2c 或 3 陷阱发送。（范围：1,2c，3;默认值：1）

auth | **noauth** | **priv** -该组使用 SNMPv3 身份验证，无身份验证或身份验证和隐私。

port - 要使用的主机 UDP 端口。（范围：1-65535;默认值：162）

缺省配置

主机地址：无

通知类型：陷阱

SNMP 版本：1

UDP 端口：162

命令模式

全局配置

命令用法

◆如果未输入 **snmp-server host** 命令，则不会发送任何通知。要将交换机配置为发送 SNMP 通知，必须至少输入一个 **snmp-server host** 命令。要启用多个主机，必须为每个主机发出单独的 **snmp-server 主机**命令。

◆本 **snmp-server host** 命令与 SNMP-server 一起使用 enable traps 命令。使用 snmp-server enable traps 命令启用陷阱或通知的发送，并指定全局发送哪些 SNMP 通知。要使主机接收通知，必须至少启用一个 snmp-server enable traps 命令，并且必须启用该主机的 **snmp-server host** 命令。

◆使用 snmp-serverenable traps 命令无法控制某些通知类型。例如某些通知类型始终启用。

◆默认情况下，交换机将通知作为陷阱消息发出。陷阱消息的接收者不会向交换机发送响应。因此跟踪消息不如通知消息可靠，其中包括确认接收的请求。通知可用于确保主机接收关键信息。但是请注意，它会消耗更多的系统资源，因为它们必须保持在内存中，直到收到响应。通知还添加到网络交通。在决定是否将通知作为陷阱或通知时，您应该考虑这些影响。

要向 SNMPv2c 主机发送通知，请完成以下步骤：

1. 启用 SNMP 代理。
2. 使用所需的通知消息创建视图。
3. 创建包含所需通知视图的组。
4. 允许交换机发送 SNMP 陷阱； 即通知。
5. 使用 **snmp-server host** 命令 指定将接收通知消息的目标主机， 如本节所述。

要向 SNMPv3 主机发送通知，请完成以下步骤：

1. 启用 SNMP 代理。
2. 创建要在消息交换过程中使用的本地 SNMPv3 用户。
3. 使用所需的通知消息创建视图。
4. 创建包含所需通知视图的组。
5. 允许交换机发送 SNMP 陷阱，即通知。
6. 使用 **snmp-server host** 命令 指定将接收通知消息的目标主机，如本节所述。

◆交换机可以向主机 IP 地址发送 SNMP 版本 1, 2c 或 3 通知，具体取决于管理站支持的 SNMP 版本。如果 **snmp-server host** 命令未指定 SNMP 版本，则默认为发送 SNMP 版本 1 通知。

◆如果指定 SNMP 版本 3 主机，则将通信字符串解释为 SNMP 用户名。必须首先使用 snmp-server user 命令定义用户名。否则 **snmp-server host** 命令将使用指定的社区字符串的名称以及读取，写入和通知视图的默认设置自动创建 SNMPv3 组。

范例

```
Console(config)#snmp-server host 10.1.19.23 batman
Console(config)#
```

4.3 SNMPv3 命令

4.3.1 snmp-serverengine-id

此命令配置 SNMPv3 引擎的标识字符串。使用 no 形式恢复默认值。

语法

snmp-server engine-id {**local** | **remote** {*ip-address*}} *engineid-string*

no snmp-server engine-id {**local** | **remote** {*ip-address*}}

local -远程设备的 Internet 地址。

remote -指定远程设备上的 SNMP 引擎。

ip-address -标识引擎 ID 的字符串。（范围：1-26 十六进制字符）

engineid-string -标识引擎 ID 的字符串。（范围：1-26 十六进制字符）

缺省配置

交换机根据其 MAC 地址自动生成唯一的引擎 ID

命令模式

全局配置

命令用法

◆SNMP 引擎是一个独立的 SNMP 代理，驻留在此交换机上或远程设备上。此引擎可防止消息重放、延迟和重定向。引擎 ID 还与用户密码结合使用，以生成用于验证和加密 SNMPv3 数据包的安全密钥。

◆使用 SNMPv3 的 INFORMS 当需要一个远程引擎 ID。 （请参阅 snmp-server host 命令。）远程引擎 ID 用于计算安全摘要，以验证交换机与远程主机上的用户之间传递的数据包的身份验证和加密。SNMP 密码使用权威代理的引擎 ID 进行本地化。权威的 SNMP 代理是远程代理。 因此，您需要先配置远程代理的 SNMP 引擎 ID，然后才能发送代理请求或通知它。

◆无需输入尾随零来唯一指定引擎 ID。 换句话说，值“0123456789”等效于“0123456789”，后跟本地引擎 ID 的 16 个零。

◆自动生成本地引擎 ID，该引擎 ID 对于交换机是唯一的。这称为默认引擎 ID。如果删除或更改本地 engineID，则将清除所有 SNMP 用户。您需要重新配置所有现有用户。

范例

```
Console(config)#snmp-server engine-id local 1234567890
```

```
Console(config)#snmp-server engineID remote 9876543210 192.168.1.19
Console(config)#
```

4.3.2 snmp-server group

此命令添加 SNMP 组，将 SNMP 用户映射到 SNMP 视图。使用 **no** 形式删除 SNMP 组。

语法

snmp-server group *groupname*{**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}}

[**read** *readview*] [**write** *writeview*] [**notify** *notifyview*]

no snmp-server group *groupname*

groupname - Name of an SNMP group. (Range: 1-32 characters)

v1 | **v2c** | **v3** - Use SNMP version 1, 2c or 3.

auth | **noauth** | **priv** - This group uses SNMPv3 withauthentication, no authentication, or with authentication and

privacy.

readview - 定义读访问的视图。(1-32 个字符)

writeview - 定义写访问的视图。(1-32 个字符)

notifyview - 定义通知视图。(1-32 个字符)

缺省配置

默认组：public 15 (只读)，private 16 (读/写)

readview - 属于 Internet OID 空间的每个对象 (1)。

writeview - 没有定义。

notifyview - 没有定义任何内容。

命令模式

全局配置

命令用法

◆组为分配的用户设置访问策略。

◆选择身份验证时，将使用 snmp-server user 命令中指定的 MD5 或 SHA 算法 。

◆选择隐私时，DES 56 位算法用于数据加密。

范例

```
Console(config)#snmp-server group r&d v3 auth write daily
Console(config)#
```

4.3.3 snmp-server user

此命令将用户添加 SNMP 组，将用户限制为特定的 SNMP 读取，写入或通知视图。 使用 no 形式从 SNMP 组中删除一个用户。

语法

snmp-server user *username groupname* [**remote** *ip-address*]{**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password*[**priv des56** *priv-password*]]

no snmp-server user *username* {**v1** | **v2c** | **v3** | **remote**}

username - 连接 SNMP 代理的用户名。（范围：1-32 个字符）

groupname - 为其分配用户的 SNMP 组的名称。（范围：1-32 个字符）

remote - 指定远程设备上的 SNMP 引擎。

ip-address - 远程设备的 Internet 地址。

v1 | **v2c** | **v3** - 使用 SNMP 版本 1,2c 或 3。

encrypted - 接受密码作为加密输入。

auth - 使用 SNMPv3 进行身份验证。

md5 | **sha** - 使用 MD5 或 SHA 身份验证。

auth-password -认证密码。如果未使用加密选项，则输入纯文本。否则输入加密的密码。（最少需要八个字符。）

priv des56 - 使用带有 DES56 加密的隐私的 SNMPv3。

priv-password -隐私密码。如果未使用加密选项，则输入纯文本。否则输入加密的密码。。

缺省配置

无

命令模式

全局配置

命令用法

◆必须将本地用户（即该命令不指定远程工程师权限。）配置为授权 SNMPv3 客户端的管理访问权限，或者识别本地交换机中的 SNMPv3 陷阱消息的来源。

◆必须配置远程用户（即命令指定远程引擎标识符）以识别来自本地交换机的 SNMPv3 通知消息的来源。

◆SNMP 引擎 ID 用于根据密码计算身份验证/隐私文摘。因此在使用此配置命令之前，应使用 snmp-server engine-id 命令配置 engineID 。

◆在配置远程用户之前，请使用 snmp-server engine-id 命令指定用户所在的远程设备的引擎 ID。 然后使用 **snmp-server user** 命令指定用户所在的远程设备的用户和 IP 地址。远程代理的 SNMP 引擎 ID 用于根据用户密码计算身份验证/隐私摘要。 如果未首先配置远程引擎 ID，则指定远程用户的 **snmp-server user** 命令将失败。

◆ 使用授权人的引擎 ID 本地化 SNMP 密码。对于通知，权威 SNMP 代理是远程代理。因此，您需要先配置远程代理的 SNMP 引擎 ID，然后才能发送代理请求或通知它。

范例

```
Console(config)#snmp-server user steve group r&d v3 auth md5 greenpeace priv
des56 einstien
Console(config)#snmp-server user mark group r&d remote 192.168.1.19 v3 auth
md5 greenpeace priv des56 einstien
Console(config)#
```

4.3.4 snmp-server view

此命令添加一个 SNMP 视图，用于控制用户对 MIB 的访问。使用 **no** 形式删除 SNMP 视图。

语法

snmp-server view *view-name oid-tree* {**included** | **excluded**}

no snmp-server view *view-name*

view-name - SNMP 视图的名称。（范围：1-32 个字符）

oid-tree - MIB 树中分支的对象标识符。通配符可用于屏蔽 OID 字符串的特定部分。（请参阅示例。）

included -定义包含的视图。

excluded -定义排除的视图。

缺省配置

缺省视图（包括对整个 MIB 树的访问）

命令模式

全局配置

命令用法

◆snmp-server group 命令中使用视图将用户访问限制为 MIB 树的指定部分。

◆预定义视图“缺省配置 view”包括对整个 MIB 树的访问。

范例

该视图包括 MIB-2。

```
Console(config)#snmp-server view mib-2 1.3.6.1.2.1 included

Console(config)#
```

该视图包括 MIB-2 接口表。通配符用于选择此表中的所有索引值。

```
Console(config)#snmp-server view ifEntry.2 1.3.6.1.2.1.2.2.1.*.2 included

Console(config)#
```

该视图包括 MIB-2 接口表，掩码选择 allindex 条目。

```
Console(config)#snmp-server view ifEntry.a 1.3.6.1.2.1.2.2.1.1.* included

Console(config)#
```

4.3.5 show snmp engine-id

此命令显示 SNMP 引擎 ID。

命令模式

特权模式

范例

此示例显示默认引擎 ID。

```
Console#show snmp engine-id

Local SNMP EngineID: 8000002a8000000000e8666672

Local SNMP EngineBoots: 1

Remote SNMP EngineID IP address

80000000030004e2b316c54321 192.168.1.19

Console#
```

4.3.6 show snmp group

提供了四个默认组 - SNMPv1 只读访问和读/写访问，以及 SNMPv2c 只读访问和读/写访问。

命令模式

特权模式

范例

```
Console#show snmp group

Group Name: r&d

Security Model: v3

Read View: defaultview

Write View: daily

Notify View: Disabled

Storage Type: permanent

Row Status: active

Group Name: public

Security Model: v1

Read View: defaultview

Write View: Disabled

Notify View: Disabled

Storage Type: volatile

Row Status: active

Group Name: public

Security Model: v2c

Read View: defaultview

Write View: Disabled

Notify View: Disabled

Storage Type: volatile

Row Status: active

Group Name: private

Security Model: v1
```

```
Read View: defaultview

Write View: defaultview

Notify View: Disabled

Storage Type: volatile

Row Status: active

Group Name: private

Security Model: v2c

Read View: defaultview

Write View: defaultview

Notify View: Disabled

Storage Type: volatile

Row Status: active

Console#
```

4.3.7 show snmp user

此命令显示有关 SNMP 用户的信息。

命令模式

特权模式

范例

```
Console#show snmp user

EngineId: 800000ca030030f1df9ca00000

User Name: steve

Authentication Protocol: md5

Privacy Protocol: des56

Storage Type: nonvolatile

Row Status: active
```

4.3.8 show snmp view

此命令显示有关 SNMP 视图的信息。

命令模式

特权模式

范例

```
Console#show snmp view

View Name: mib-2

Subtree OID: 1.2.2.3.6.2.1

View Type: included

Storage Type: permanent

Row Status: active

View Name: defaultview

Subtree OID: 1

View Type: included

Storage Type: volatile

Row Status: active

Console#
```

4.4 其他 Trap 命令

4.4.1 memory

此命令根据配置的内存利用率阈值设置 SNMP 陷阱。使用 no 形式恢复默认设置。

语法

memory {**rising** *rising-threshold* | **falling** *falling-threshold*}

no memory {**rising** | **falling**}

上升阈值 - 内存利用率上升阈值以百分比表示。（范围：1-100）

下降阈值 - 内存利用率下降阈值以百分比表示。（范围：1-100）

缺省配置

上升门槛：90%

下降门槛：70%

命令模式

全局配置

命令用法

一旦超过警报阈值，在警报终止之前，利用率必须低于下降阈值，然后在触发另一个警报之前再次超过阈值阈值。

范例

```
Console(config)#memory rising 80
Console(config)#memory falling 60
Console#
```

4.4.2 process cpu

此命令根据 CPU 利用的已配置阈值设置 SNMP 陷阱。使用 no 形式恢复默认设置。

语法

process cpu {**rising** *rising-threshold* | **falling** *falling-threshold*}

no process cpu {**rising** | **falling**}

上升阈值 - CPU 利用率的上升阈值以百分比表示。 （范围：1-100）

下降阈值 - CPU 利用率下降阈值以百分比表示。 （范围：1-100）

缺省配置

上升门槛：90%

下降门槛：70%

命令模式

全局配置

命令用法

一旦超过警报阈值，在警报终止之前，利用率必须低于下降阈值，然后在触发另一个警报之前再次超过阈值阈值。

范例

```
Console(config)#process cpu rising 80
```

```
Console(config)#process cpu falling 60

Console#
```

5 RMON 命令

远程监控允许远程设备独立收集信息或响应指定事件。这个开关是一个支持 RMON 的设备，可以独立执行各种任务，显着减少网络管理流量。它可以连续运行诊断并记录网络性能信息。如果触发事件，它可以自动通知网络管理员故障并提供有关事件的历史信息。如果它无法连接到管理代理程序，它将继续执行任何指定的任务，并在下次联系时将数据传回管理站。此交换机支持 mini-RMON，包括统计、历史、事件和警报组。 启用 RMON 后，系统会逐步建立有关其物理接口的信息，并将此信息存储在相关的 RMON 数据库组中。然后管理代理使用 SNMP 协议与交换机进行周期性通信。但是如果交换机遇到严重事件，它可以自动向管理代理发送陷阱消息，然后管理代理可以响应事件（如果已配置）。

5.1.1 rmon alarm

此命令设置受监视变量的阈值边界。使用 no 形式删除警报。

语法

rmon alarm *index variable interval* {**absolute** | **delta**}**rising-threshold** *threshold* [*event-index*]**falling-threshold** *threshold* [*event-index*][**owner** *name*]

no rmon alarm *index*

ndex - 此条目的索引。（范围：1-65535）

variable - 要采样的 MIB 变量的对象标识符。只能采样其它的统计条目类型的变量。注意，其它的统计条目唯一地定义 MIB 变量，其它的统计条目定义 MIB 变量，以及其它的统计索引。例如，1.3.61.2.1.16.1.1.1.61 表示统计广播 PKT，加上计指数为 1。

interval - 轮询间隔。（范围：1-31622400 秒）

absolute - 将变量直接与采样周期结束时的阈值进行比较。

delta - 从当前值中减去最后一个样本，然后将差值与阈值进行比较。

threshold - 采样变量的警报阈值。（范围：0-2147483647）

event-index - 触发警报时使用的事件的索引。如果事件控制表中没有相应的条目，则将生成无事件。（范围：0-65535）

name - 创建此条目的人员的姓名。（范围：1-127 个字符）

缺省配置

1.3.6.1.2.1.16.1.1.1.6.1 - 1.3.6.1.2.1.16.1.1.1.6.28

每隔 30 秒取样本，

上升阈值为 892800，分配给前夕 0

下降阈值为 446400，分配给事件 0

命令模式

全局配置

命令用法

◆如果已为索引定义了事件，则必须先删除该条目，然后才能使用此命令进行任何更改。

◆ 如果当前值大于或等于上升阈值，并且最后一个样本值小于此阈值，则将生成警报。在生成上升事件之后，在采样值低于上升阈值，达到下降阈值，并再次向上移动到上升阈值之前，将不会生成另一个此类事件。

◆如果当前值小于或等于下降阈值，并且最后一个样本值大于此阈值，则将生成警报。在生成下降事件之后在样本值已经超过下降阈值，达到上升阈值，并再次向下移动到失败阈值之前，不会产生其他事件。

范例

```
Console(config)#rmon alarm 1 1.3.6.1.2.1.16.1.1.1.6.1 15 delta

rising-threshold 100 1 falling-threshold 30 1 owner mike

Console(config)#
```

5.1.2 rmon event

此命令为警报创建响应事件。使用 no 形式删除事件。

语法

rmon event *index* [**log**] | [**trap** *community*] | [**description** *string*] |[**owner** *name*]

no rmon event *index*

index - 此条目的索引。（范围：1-65535）

log - 触发事件时生成 RMON 日志条目。根据事件日志记录的当前配置设置处理日志消息。

trap - 向所有已配置的陷阱管理器发送陷阱消息。

community - 一起发送到 SNMP v1 和 v2c 主机的类似密码的共用体字符串。尽管可以使用 **rmon event** 命令自行设置此字符串，但建议使用 snmp-server community 命令定义字符串，以使用 **rmon event** 命令。（范围：1-32 个字符）

string - 描述此事件的注释。（范围：1-127 个字符）

name - 创建此条目的人员的姓名。（范围：1-127 个字符）

缺省配置

无

命令模式

全局配置

命令用法

◆如果已为索引定义了事件，则必须先删除该条目，然后才能使用此命令进行任何更改。

◆　指定的事件确定警报触发此事件时要执行的操作。对警报的响应可以包括记录警报或向消息管理器发送消息。

范例

```
Console(config)#rmon event 2 log description urgent owner mike

Console(config)#
```

5.1.3 rmon collection history

此命令定期对物理接口的统计信息进行采样。使用 no 形式禁用定期采样。

语法

rmon collection history controlEntry *index*[[**owner** *name*] [**buckets** *number*] [**interval** *seconds*]] |[**buckets** *number*] [**interval** *seconds*] | **interval** *seconds*

no rmon collection history controlEntry *index*

index - 此条目的索引。（范围：1-65535）

number - 此条目请求的桶数。（范围：1-65536）

seconds - 轮询间隔。（范围：1-3600 秒）

name - 创建此条目的人员的姓名。（范围：1-127 个字符）

缺省配置

1.3.6.1.2.1.16.1.1.1.6.1 - 1.3.6.1.2.1.16.1.1.1.6.28

取样容计：50

间隔：偶数条目的 30 秒，

奇数条目的 1800 秒

命令模式

接口配置（Ethernet）

命令用法

◆默认情况下，每个索引号等于交换机上的端口，但可以更改为当前未使用的任何数字。

◆如果已在接口上启用了定期采样，则必须先删除该条目，然后才能使用此命令进行任何更改。

◆为每个样本收集的信息包括：输入八位字节、数据包、广播数据包、多播数据包、尺寸过小的

数据包、超大数据包、片段、CRC 校准错误、冲突、丢弃事件和网络利用率等。

◆交换机为每个端口保留两个控制项索引条目。如果通过此命令将添加缺省索引条目重新分配给另一个端口，则 show running-config 命令将显示一条消息，指示此索引不适用于通常分配给的端口。例如，如果将控制条目 15 分配给端口 5 如下所示 show running-config 命令将指示此条目不适用于端口 8。

```
Console(config)#interface ethernet 1/5

Console(config-if)#rmon collection history controlEntry 15

Console(config-if)#end

Console#show running-config

!

interface ethernet 1/5

rmon collection history controlEntry 15 buckets 50 interval 1800

...

interface ethernet 1/8

no rmon collection history controlEntry 15
```

范例

```
Console(config)#interface ethernet 1/1

Console(config-if)#rmon collection history controlentry 21 owner mike buckets

24 interval 60

Console(config-if)#
```

5.1.4 rmon collection rmon1

此命令用于在物理接口上收集统计信息。使用 no 形式禁用统计信息收集。

语法

rmon collection rmon1 controlEntry *index* [**owner** *name*]

no rmon collection rmon1 controlEntry *index*

index - 此条目的索引。（范围：1-65535）

name - 创建此条目的人员的姓名。（范围：1-127 个字符）

缺省配置

启用

命令模式

接口配置(Ethernet)

命令用法

◆默认情况下，每个索引号等于交换机上的端口，但可以更改为当前未使用的任何数字。

◆如果已在接口上启用统计信息收集，则必须先删除该条目，然后才能使用此命令进行任何更改。

◆为每个条目收集的信息包括：输入八位字节、数据包、广播数据包、多播数据包、尺寸不足数据包、超大数据包、片段、CRC 校准错误、冲突、丢弃事件和指定长度的数据包等。

范例

```
Console(config)#interface ethernet 1/1

Console(config-if)#rmon collection rmon1 controlEntry 1 owner mike

Console(config-if)#
```

5.1.5 show rmon alarms

此命令显示所有已配置警报的设置。

命令模式

特权模式

范例

```
Console#show rmon alarms

Alarm 1 is valid, owned by

Monitors 1.3.6.1.2.1.16.1.1.1.6.1 every 30 seconds

Taking delta samples, last value was 0

Rising threshold is 892800, assigned to event 0

Falling threshold is 446400, assigned to event 0

..
```

5.1.6 show rmon events

此命令显示所有已配置事件的设置。

命令模式

特权模式

范例

```
Console#show rmon events

Event 2 is valid, owned by mike

Description is urgent

Event firing causes log and trap to community , last fired 00:00:00

Console#
```

5.1.7 show rmon history

此命令显示为历史记录组中的每个条目配置的采样参数。

命令模式

特权模式

范例

```
Console#show rmon history

Entry 1 is valid, and owned by

Monitors 1.3.6.1.2.1.2.2.1.1.1 every 1800 seconds

Requested # of time intervals, ie buckets, is 8

Granted # of time intervals, ie buckets, is 8

Sample # 1 began measuring at 00:00:01

Received 77671 octets, 1077 packets,

61 broadcast and 978 multicast packets,

0 undersized and 0 oversized packets,

0 fragments and 0 jabbers packets,

0 CRC alignment errors and 0 collisions.

# of dropped packet events is 0
```

```
Network utilization is estimated at 0

...
```

5.1.8 show rmon statistics

此命令显示为统计组中的所有已配置条目收集的信息。

命令模式

特权模式

范例

```
Console#show rmon statistics

Interface 1 is valid, and owned by

Monitors 1.3.6.1.2.1.2.2.1.1.1 which has

Received 164289 octets, 2372 packets,

120 broadcast and 2211 multicast packets,

0 undersized and 0 oversized packets,

0 fragments and 0 jabbers,

0 CRC alignment errors and 0 collisions.

# of dropped packet events (due to lack of resources): 0

# of packets received of length (in octets):

64: 2245, 65-127: 87, 128-255: 31,

256-511: 5, 512-1023: 2, 1024-1518: 2

..
```

6 流量采样命令

流采样（sFlow）可与远程 sFlow 收集器一起使用，提供对网络上存在的流量类型和水平的准确、详细和实时概述。sFlow Agent 从遍历交换机的所有数据中采样 n 个包中的 1，将采样重新封装为 sFlow 数据报并将它们发送到 sFlow Collector。这种采样发生在内部硬件级别，其中可以看到所有通信量，其中异常探测只具有通信量的部分视图，因为它是在主题接口上采样的。此外，由于不发生局部分析，由 SFROM 代理所施加的处理器和内存负载是最小的。

6.1.1 sflow

该命令为交换机全局启用 sFlow。使用 no 形式禁用此功能。

语法

[no] sflow

缺省配置

禁用

命令模式

全局配置

命令用法

必须在交换机上全局启用流采样，以及需要它的那些端口（请参阅 sflow 源 命令）。

范例

```
Console(config)#sflow
Console(config)#
```

6.1.2 sflow destination

此命令配置集合器使用的 IP 地址和 UDP 端口。使用 no 形式恢复默认设置。

语法

sflow destination {**ipv4** *ipv4-address* | **ipv6** *ipv6-address*}[*destination-udp-port*]

no sflow destination

ipv4-address - sFlow Collector 的 IPv4 地址。有效的 IPv4 地址由四个十进制数组成，0 到 255，由句点分隔。

ipv6-address - sFlow Collector 的 IPv6 地址。一个完整的 IPv6 地址，包括网络前缀和主机地址位。IPv6 地址由 8 个以冒号分隔的 16 位十六进制值组成。一个双冒号可用于指示填充未定义字段所需的适当零数。

destination-udp-port -收集器为 sFlow 流监视的 UDP 端口。（范围：0-65534）

缺省配置

IP Address: 空

UDP Port: 6343

命令模式

接口配置 (Ethernet)

范例

此示例配置收集器的 IP 地址，并使用缺省 UDP 端口。

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow destination ipv4 192.168.0.4
Console(config-if)#
```

6.1.3 sflow max-datagram-size

此命令配置 sFlow 数据报有效载荷的最大尺寸。使用 no 形式恢复默认设置。

语法

sflow max-datagram-size *max-datagram-size*

no max-datagram-size

max-datagram-size - sFlow datagrampayload 的最大尺寸。（范围：200-1500 字节）

缺省配置

1400 bytes

命令模式

接口配置 (Ethernet)

范例

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow max-datagram-size 1500
Console(config-if)#
```

6.1.4 sflow max-header-size

此命令配置 sFlow 数据报头的最大尺寸。使用 no 形式恢复默认设置。

语法

sflow max-header-size *max-header-size*

no max-header-size

max-header-size - sFlow 数据报头的最大尺寸。(范围：64-256 字节)

缺省配置

128 bytes

命令模式

接口配置(Ethernet)

范例

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow max-header-size 256
Console(config-if)#
```

6.1.5 sflow owner

此命令配置接收方的名称（即 sFlow Collector)。使用 no 形式删除此名称。

语法

sflow owner *name*

no sflow owner

name -接收者的名称。(范围：1-256 个字符)

缺省配置

无

命令模式

接口配置(Ethernet)

范例

此示例将所有者的名称设置为 Lamar。

```
Console(config)#interface ethernet 1/9

Console(config-if)#sflow owner Lamer

Console(config-if)#
```

6.1.6 sflow polling-interval

此命令配置将计数器添加到样本数据报的时间间隔。使用 no 形式还原默认轮询间隔。

语法

sflow polling-interval *seconds*

no sflow polling-interval

seconds - sFlow 进程向样本数据报添加计数器的时间间隔。（范围：0-10,000,000 秒，其中 0 表示禁用此功能）

缺省配置

禁用

命令模式

接口配置 (Ethernet)

范例

此示例将轮询间隔设置为 10 秒。

```
Console(config)#interface ethernet 1/9

Console(config-if)#sflow polling-interval 10

Console(config-if)#
```

6.1.7 sflow sample

此命令配置数据包采样率。使用 no 形式恢复默认费率。

语法

sflow sample *rate*

no sflow sample

rate -数据包采样率，或者采样的数据包数量。（范围：256-16777215 包）

缺省配置

禁用

命令模式

接口配置 (Ethernet)

范例

此示例将采样率设置为每 100 个数据包中的 1 个。

```
Console(config)#interface ethernet 1/9

Console(config-if)#sflow sample 100

Console(config-if)#
```

6.1.8 sflow source

此命令可以监视源端口上的 sFlow。使用 no 形式禁用指定端口上的 sFlow。

语法

[no] **sflow source**

缺省配置

禁用

命令模式

接口配置 (Ethernet)

范例

此示例在端口 9 到 16 上启用流控制。

```
Console(config)#interface ethernet 1/9

Console(config-if)#sflow source

Console(config-if)#
```

6.1.9 sflow timeout

此命令配置在重置所有 sFlow 端口参数之前将样本发送到收集器的时间长度。使用 no 形式恢复默认超时。

语法

sflow timeout *seconds*

no sflow timeout

seconds - sFlow 进程在重置所有 sFlow 端口参数之前连续向采集器发送采样的时间长度。（范围：0-10000000 秒，其中 0 表示没有超时）

缺省配置

禁用

命令模式

接口配置 (Ethernet)

命令用法

受此命令影响的 sFlow 参数包括采样间隔，接收方名称，地址和 UDP 端口、超时、最大标头大小和最大数据报大小。

范例

此示例将超时设置为 1000 秒。

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow timeout 10000
Console(config-if)#
```

6.1.10 show sflow

此命令显示 sFlowprocess 的全局和接口设置。

语法

show sflow interface [*interface*]

interface

ethernet *unit/port*

单位 - 堆叠单位。（范围：1）

端口 - 端口号。（范围：1-28）

命令模式

特权模式

范例

```
Console#show sflow interface ethernet 1/9

Interface of Ethernet 1/9 :

Interface status : Enabled

Owner name : Lamar

Owner destination : 192.168.0.4

Owner socket port : 6343

Time out : 9994

Maximum header size : 256

Maximum datagram size : 1500

Sample rate : 1/256

Polling interval : 10

Console#
```

7 认证命令

您可以将此交换机配置为使用本地或远程身份验证方法对登录系统以进行管理访问的用户进行身份验证。还可以配置使用 IEEE 802.1X 的基于端口的身份验证，以控制对上行链路端口的管理访问或对数据端口的客户端访问。

7.1 用户帐户和特权级别

本节列出了管理访问和分配命令权限级别所需的基本命令。

7.1.1 enable password

在最初登录系统后，您应该设置特权模式密码。请记住将其记录在安全的地方。此命令控制从普通模式级别访问特权模式级别。使用 **no** 形式重置默认密码。

语法

enable password [**level** *level*] {**0** | **7**} *password*

no enable password [**level** *level*]

level *level* -为特权用户级别 15。（未使用 0-14 级。）

{**0** | **7**} - 0 表示普通密码，7 表示加密密码。

password -此权限级别的密码。（最大长度：32 个字符纯文本或加密，区分大小写）

缺省配置

缺省等级：15

缺省密码：super

命令模式

全局配置模式

命令用法

◆您无法设置空密码。您必须输入密码，使用 enable 命令将命令模式从普通模式更改为特权模式。

◆在系统启动期间或从 TFTP 服务器下载配置文件时，读取配置文件时，需要使用加密密码以与遗留密码设置（即纯文本或加密）兼容。您无需手动配置加密密码。

范例

```
Console(config)#enable password level 15 0 admin

Console(config)#
```

7.1.2 username

此命令添加命名用户,要求在登录时进行身份验证,指定或更改用户的密码(或指定不需要密码),或指定或更改用户的访问级别。使用 **no** 形式删除用户名。

语法

username *name* {**access-level** *level* | **nopassword** |**password** {**0** | **7**} *password*}

no username *name*

name -用户名。(最大长度：32 个字符，区分大小写。最大用户数：16)

access-level *level*-指定用户级别。设备有两个预定义的权限级别： **0** ：正常执行， **15** ：特权执行。

nopassword -此用户无需密码即可登录。{ **0** | **7** } - 0 表示普通密码，7 表示加密密码。

password *password* -用户的验证密码。(最大长度：32 个字符纯文本或加密，区分大小写)

缺省配置

默认访问级别为普通模式。

用户名和密码的出厂默认值为：

```
username access-level password

guest            0                guest

admin        15            admin
```

命令模式

全局配置

命令用法

在读取配置文件系统启动时或从FTP/ TFTP 服务器下载配置文件时,加密密码是与旧密码设置(即纯文本或加密）兼容所必需的。您无需手动配置加密密码。

范例

此示例显示如何设置用户的访问级别和密码。

```
Console(config)#username bob access-level 15
Console(config)#username bob password 0 smith
Console(config)#
```

7.1.3 privilege

此命令为指定的命令组或单个命令分配权限级别。使用 no 形式恢复默认设置。

语法

privilege *mode* [**all**] **level** *level command*

no privilege *mode* [**all**] *command*

mode - 这个配置模式包含指定的命令。

all -在指定命令下修改所有子命令的特权级别。

level *level* -指定指定*命*令的权限级别。此设备具有三个预定义权限级别： **0** ：正常执行， **8** ：管理， **15** ：特权执行。（范围：0-15）

command - 在特定模式下的任意指令。

缺省配置

权限级别 0 提供对有限数量的命令的访问，这些命令显示交换机的当前状态，以及多个数据库清除和重置功能。级别 8 提供对所有显示状态和配置命令的访问，但控制各种身份验证和安全功能的命令除外。15 级提供对所有命令的完全访问权限。

命令模式

全局配置

范例

此示例将 ping 命令的权限级别设置为特权模式。

```
Console(config)#privilege exec level 15 ping
Console(config)#
```

7.1.4 show privilege

此命令显示当前用户的特权级别，或特权命令修改的命令的特权级别。

语法

show privilege [command]

command -显示特权命令修改的所有命令的特权级别。

命令模式

特权模式

范例

此示例显示特权命令修改的任何命令的特权级别。

```
Console#show privilege command

privilege line all level 0 accounting

privilege exec level 15 ping

Console(config)#
```

7.2 认证序列

可以指定三种身份验证方法来验证用户登录系统以进行管理访问。本节中的命令可用于定义身份验证方法和序列。

7.2.1 Authentication enable

此命令定义使 enable 命令从执行命令模式更改为特权模式命令模式时使用的身份验证方法和优先级。使用 no 形式恢复默认值。

语法

authentication enable {[**local**] [**radius**] [**tacacs**]}

no authentication enable

local - 仅使用本地密码。

radius - 仅使用 RADIUS 服务器密码。

tacacs - 使用 TACACS 服务器密码。

缺省配置

本地

命令模式

全局配置

命令用法

◆RADIUS 使用 UDP 而 TACACS +使用 TCP。 UDP 仅提供尽力而为的交付，而 TCP 提供面向连接的传输。 此外，请注意，RADIUS 仅加密从客户端到服务器的访问请求数据包中的密码，而 TACACS +加密 数据包的整个主体。

◆ RADIUS 和 TACACS +登录身份验证为每个用户名和密码对分配特定的权限级别。 必须在身份验证服务器上配置用户名，密码和权限级别。

◆ 您可以在单个命令中指定 三种身份验证方法来指示身份验证序列。例如，如果输入“ **authentication enable radius tacacs local** ”，则首先验证 RADIUS 服务器上的用户名和密码。如果 RADIUS 服务器不可用，则尝试在 TACACS +服务器上进行身份验证。如果 TACACS + 服务器不可用，则使用本地用户名和密码已检查。

范例

```
Console(config)#authentication enable radius
Console(config)#
```

7.2.2 authentication login

此命令定义登录验证方法和优先级。使用 no 形式恢复默认值。

语法

authentication login {[**local**] [**radius**] [**tacacs**]}

no authentication login

local - 使用本地密码。

radius - 使用 RADIUS 服务器密码。

tacacs - 使用 TACACS 服务器密码。

缺省配置

本地

命令模式

全局配置

命令用法

◆RADIUS 使用 UDP 而 TACACS +使用 TCP。UDP 仅提供尽力而为的交付，而 TCP 提供面向连接的传输。此外请注意，RADIUS 仅加密从客户端到服务器的访问请求数据包中的密码，而 TACACS +加

密数据包的整个主体。

◆ RADIUS 和 TACACS +登录身份验证为每个用户名和密码对分配特定的权限级别。必须在身份验证服务器上配置用户名，密码和权限级别。

◆ 您可以在单个命令中指定 三种身份验证方法来指示身份验证序列。例如如果输入“ **authentication login radius tacacs local** ”，则首先验证 RADIUS 服务器上的用户名和密码。如果 RADIUS 服务器不可用，则尝试在 TACACS +服务器上进行身份验证。如果 TACACS + 服务器不可用，则使用本地用户名和密码已检查。

范例

```
Console(config)#authentication login radius
Console(config)#
```

7.3 RADIUS CLIENT

远程身份验证拨入用户服务（RADIUS）是一种身份验证协议，它使用在中央服务器上运行的软件来控制对网络上支持 RADIUS 的设备的访问。 身份验证服务器包含多个用户名/密码对的数据库，其中包含需要管理访问交换机的每个用户或组的相关权限级别。

7.3.1 radius-server acct-port

此命令为统计信息设置 RADIUS 服务器网络端口。使用 no 形式恢复默认值。

语法

radius-server acct-port *port-number*

no radius-server acct-port

port-number -用于统计信息的 RADIUS 服务器 UDP 端口。（范围：1-65535）

缺省配置

1813

命令模式

全局配置

范例

```
Console(config)#radius-server acct-port 181

Console(config)#
```

7.3.2 radius-server auth-port

此命令设置 RADIUS 服务器网络端口。使用 no 形式恢复默认值。

语法

radius-server auth-port *port-number*

no radius-server auth-port

port-number -用于认证信息的 RADIUS 服务器 UDP 端口。 （范围：1-65535

缺省配置

1812

命令模式

全局配置

范例

```
Console(config)#radius-server auth-port 181

Console(config)#
```

7.3.3 radius-server host

此命令指定主 RADIUS 服务器和备份 RADIUS 服务器，以及适用于每个服务器的身份验证和记帐参数。使用 no 形式删除指定的服务器，或恢复默认值。

语法

[no] **radius-server** *index* **host** *host-ip-address* [**acct-port** *acct-port*][**auth-port** *auth-port*] [**key** *key*] [**retransmit** *retransmit*][**timeout** *timeout*]

index - 允许您指定最多五个服务器。这些服务器按顺序执行，直到服务器响应或重新传输 periodexxire。

host-ip-address - 服务器的 IP 地址。

acct-port - 用于计费消息的 RADIUS 服务器 UDP 端口。（范围：1-65535）

auth-port - 用于身份验证消息的 RADIUS 服务器 UDP 端口。（范围：1-65535）

key - 用于验证客户端登录访问权限的加密密钥。不要在字符串中使用空格。（最大长度：48

个字符）

retransmit - 交换机尝试通过 RADIUS 服务器验证登录访问的次数。（范围：1-30）

timeout - 交换机在发送请求之前等待回复的秒数。（范围：1-65535）

缺省配置

auth-port - 1812

acct-port - 1813

超时 - 5 秒

转发 - 2

命令模式

全局配置

范例

```
Console(config)#radius-server 1 host 192.168.1.20 port 181 timeout 10
retransmit 5 key green
Console(config)#
```

7.3.4 radius-server key

此命令设置 RADIUS 加密密钥。使用 no 形式恢复默认值。

语法

radius-server key *key-string*

no radius-server key

key-string-用于验证客户端登录访问权限的加密密钥。不要在字符串中使用空格。（最大长度：48 个字符）

缺省配置

无

命令模式

全局配置

范例

```
Console(config)#radius-server key green
Console(config)#
```

7.3.5 radius-server retransmit

此命令设置重试次数。使用 no 形式恢复默认值。

语法

radius-server retransmit *number-of-retries*

no radius-server retransmit

number-of-retries -交换机尝试通过 RADIUS 服务器验证登录访问的次数。 （范围：1 - 30）

缺省配置

2

命令模式

全局配置

范例

```
Console(config)#radius-server retransmit 5

Console(config)#
```

7.3.6 radius-server timeout

此命令设置将身份验证请求发送到 RADIUS 服务器之间的时间间隔。 使用 no 形式恢复默认值。

语法

radius-server timeout *number-of-seconds*

no radius-server timeout

number-of-seconds -交换机在重新发送请求之前等待的秒数。（范围：1-65535

缺省配置

5

命令模式

全局配置

范例

```
Console(config)#radius-server timeout 10

Console(config)#
```

7.3.7 show radius-server

此命令显示 RADIUS 服务器的当前设置。

缺省配置

无

命令模式

特权模式

范例

```
Console#show radius-server

Remote RADIUS Server Configuration:

Global Settings:

Authentication Port Number : 1812

Accounting Port Number : 1813

Retransmit Times : 2

Request Timeout : 5

Server 1:

Server IP Address : 192.168.1.1

Authentication Port Number : 1812

Accounting Port Number : 1813

Retransmit Times : 2

Request Timeout : 5

RADIUS Server Group:

Group Name Member Index

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

radius 1

Console#
```

7.4 TACACS +客户端

终端访问控制器访问控制系统（TACACS +）是一种逻辑身份验证协议，它使用在中央服务器上运行的软件来控制对网络上的 TACACS 感知设备的访问。 身份验证服务器包含多个用户名/密码对的数据库，其中包含需要管理访问交换机的每个用户或组的相关权限级别。

7.4.1 tacacs-server host

此命令指定 TACACS +服务器和其他可选参数。使用 no 形式删除服务器或恢复默认值。

语法

tacacs-server *index* **host** *host-ip-address* [**key** *key*][**port** *port-number*] [**retransmit** *retransmit*] [**timeout** *timeout*]

no tacacs-server *index*

index - 此服务器的索引。（范围：1）

host-ip-address - TACACS +服务器的 IP 地址。

key - 用于验证客户端登录访问权限的加密密钥。不要在字符串中使用空格。（最大长度：48 个字符）

port-number - 用于身份验证消息的 TACACS +服务器 TCP 端口。（范围：1-65535）

retransmit - 交换机尝试通过 TACACS +服务器验证登录访问的次数。（范围：1-30）

timeout - 交换机在发送请求之前等待回复的秒数。（范围：1-540）

缺省配置

身份验证端口 - 49

超时 - 5 秒

转发 - 2

命令模式

全局配置

范例

```
Console(config)#tacacs-server 1 host 192.168.1.25 port 181 timeout 10

retransmit 5 key green

Console(config)#
```

7.4.2 tacacs-server key

此命令设置 TACACS +加密密钥。使用 no 形式恢复默认值。

语法

tacacs-server key *key-string*

no tacacs-server key

key-string -用于验证客户端登录访问权限的加密密钥。 不要在字符串中使用空格。(最大长度：48 个字符)

缺省配置

无

命令模式

全局配置

范例

```
Console(config)#tacacs-server key green
Console(config)#
```

7.4.3 tacacs-server port

此命令指定 TACACS +服务器网络端口。 使用 no 形式恢复默认值。

语法

tacacs-server port *port-number*

no tacacs-server port

port-number -用于身份验证消息的 TACACS+服务器 TCP 端口。(范围：1-65535)

缺省配置

49

命令模式

全局配置

范例

```
Console(config)#tacacs-server port 181
Console(config)#
```

7.4.4 tacacs-server retransmit

此命令设置重试次数。使用 no 形式恢复默认值。

语法

tacacs-server retransmit *number-of-retries*

no tacacs-server retransmit

number-of-retries -交换机尝试通过 TACACS +服务器验证登录访问的次数。 （范围：1 - 30）

缺省配置

2

命令模式

全局配置

范例

```
Console(config)#tacacs-server retransmit 5

Console(config)#
```

7.4.5 tacacs-server timeout

此命令设置将身份验证请求发送到 TACACS+服务器之间的时间间隔。使用 no 形式恢复默认值。

语法

tacacs-server timeout *number-of-seconds*

no tacacs-server timeout

number-of-seconds -交换机在重新发送请求之前等待的秒数。（范围：1-540）

缺省配置

5

命令模式

全局配置

范例

```
Console(config)#tacacs-server timeout 10

Console(config)#
```

7.4.6 show tacacs-server

此命令显示 TACACS+服务器的当前设置。

缺省配置

无

命令模式

特权模式

范例

```
Console#show tacacs-server

Remote TACACS+ Server Configuration:

Global Settings:

Server Port Number : 49

Retransmit Times : 2

Timeout : 5

Server 1:

Server IP Address : 10.11.12.13

Server Port Number : 49

Retransmit Times : 2

Timeout : 4

TACACS+ Server Group:

Group Name Member Index

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

tacacs+ 1

Console#
```

7.5 AAA

身份验证，授权和记帐（AAA）功能提供了在交换机上配置访问控制的主要框架。AAA 功能需要在网络中使用已配置的 RADIUS 或 TACACS +服务器。

7.5.1 aaa accounting commands

此命令用于记录执行模式命令。使用 no 形式禁用记帐服务。

语法

aaa accounting commands *level* {**缺省配置** | *method-name*} **start-stop group** {**tacacs+** | *server-group*}

no aaa accounting commands *level* {**缺省配置** | *method-name*}

level -执行命令的权限级别。（范围：0-15）

缺省配置 -指定服务请求的缺省记帐方法。

method-name -指定服务请求的记帐方法。（范围：1-64 个字符）

start-stop -从起点和终点记录会计

group -指定要使用的服务器组。

tacacs+ -指定使用 tacacs-server host 命令配置的所有 TACACS +主机 。

server-group -指定使用 aaa group server 命令配置的服务器组的名称。（范围：1-64 个字符）

缺省配置

Accounting is not Enabled

No servers are specified

命令模式

全局配置

命令用法

◆只有 TACACS +服务器支持 Exec 模式命令的计费。

◆ 请注意**缺省配置**和 *method-name* 字段仅用于描述在指定的 TACACS +服务器上配置的计费方法，并且实际上不会向服务器发送 有关要使用的方法的任何信息 。

范例

```
Console(config)#aaa accounting commands 15 default start-stop group tacacs+
Console(config)#
```

7.5.2 aaa accounting dot1x

此命令可以计算所请求的 802.1X 服务以进行网络访问。 使用 no 表单禁用记帐服务。

语法

aaa accounting dot1x {**缺省配置** | *method-name*} **start-stop group** {**radius** | |*server-group*}

no aaa accounting dot1x {**缺省配置** | *method-name*}

缺省配置 -指定 servicerequests 的缺省记帐方法.

method-name -指定 servicerequests 的记帐方法。 （范围：1-64 个字符）

start-stop -从起点和终点记录会计。

group -指定要使用的服务器组。

radius -指定使用 radius server host 命令配置的所有 RADIUS 主机。

server-group -指定使用 aaa group server 命令配置的服务器组的名称。（范围：1-64 个字符）

缺省配置

统计未启用

未指定服务器

命令模式

全局配置

命令用法

请注意**缺省配置**和 *method-name* 字段仅用于描述在指定 RADIUS 服务器上配置的记帐方法，并且实际上不会向服务器发送有关要使用的方法的任何信息。

范例

```
Console(config)#aaa accounting dot1x default start-stop group radius

Console(config)#
```

7.5.3 aaa accounting exec

此命令可以计算所请求的 Exec 服务以进行网络访问。使用 no 形式禁用记帐服务。

语法

aaa accounting exec {**缺省配置** | *method-name*} **start-stop group** {**radius** | **tacacs+** |*server-group*}

no aaa accounting exec {**缺省配置** | *method-name*}

缺省配置 -指定 servicerequests 的缺省记帐方法。

method-name - 指定 servicerequests 的记帐方法。 （范围：1-64 个字符）

start-stop - 从起点和终点记录会计。

group - 指定要使用的服务器组。

radius - 指定使用 radiusserver host 命令配置的所有 RADIUS 主机。

tacacs + – 指定使用 tacacs-server host 命令配置的所有 TACACS +主机。

server-group – 指定使用 aaa group server 命令配置的服务器组的名称。（范围：1-64 个字符）

缺省配置

统计未启用

未指定服务器

命令模式

全局配置

命令用法

◆此命令运行对本地控制台和 Telnet 连接的 Exec 服务请求的计费。

◆ 请注意**缺省配置**和 *method-name* 字段仅用于描述在指定的 RADIUS 或 TACACS +服务器上配置的计费方法，并且实际上并不向服务器发送有关要使用的方法的任何信息。

范例

```
Console(config)#aaa accounting exec default start-stop group tacacs+

Console(config)#
```

7.5.4 aaa accounting update

此命令允许向统计服务器发送定期更新。使用 no 形式禁用记帐更新。

语法

aaa accounting update [**periodic** *interval*]

no aaa accounting update

interval -在此*间隔*向服务器发送临时记帐记录。（范围：1-2147483647 分钟）

缺省配置

1 分钟

命令模式

全局配置

命令用法

◆启用记帐更新后，交换机会为系统上的所有用户发出暂时记帐记录。

◆ 使用命令而不指定中间间隔启用升级，但不更改当前间隔设置。

范例

```
Console(config)#aaa accounting update periodic 30

Console(config)#
```

7.5.5 aaa authorization exec

此命令启用 Exec 访问权限。使用 no 形式禁用授权服务。

语法

aaa authorization exec {**缺省配置** | *method-name*}**group** {**tacacs+** | *server-group*}

no aaa authorization exec {**缺省配置** | *method-name*}

缺省配置 -指定 Execaccess 的默认授权方法。

method-name - 指定 Exec 访问的授权方法。（范围：1-64 个字符）

group - 指定要使用的服务器组。

tacacs + - 指定使用 tacacs-server host 命令配置的所有 TACACS+主机。

server-group - 指定使用 aaa group server 命令配置的服务器组的名称。（范围：1-64 个字符）

缺省配置

认证未启用

未指定服务器

命令模式

全局配置

命令用法

◆此命令执行授权以确定是否允许用户运行 Exec shell。

◆ 在启用授权之前，必须启用 AAA 身份验证。

◆ 如果在没有指定命名方法的情况下发出此命令，则默认方法列表将应用于 所有接口或行（应用此授权类型），但具有已命名的 methodex 明确定义的接口或行除外。

范例

```
Console(config)#aaa authorization exec default group tacacs+
Console(config)#
```

7.5.6 aaa group server

使用此命令命名一组安全服务器主机。要从配置列表中删除服务器组，请输入此命令的 no 形式。

语法

[no] **aaa group server** {**radius** | **tacacs+**} *group-name*

radius – 定义 RADIUS 服务器组。

tacacs + – 定义 TACACS +服务器组。

group-name – 命名安全服务器组的文本字符串。(范围：1-64 个字符)

缺省配置

无

命令模式

全局配置

范例

```
Console(config)#aaa group server radius tps
Console(config-sg-radius)#
```

7.5.7 server

此命令将安全服务器添加到 AAA 服务器组。使用 **no** 形式从组中删除关联的服务器。

语法

[**no**] **server** {*index* | *ip-address*}

index – 指定服务器索引。(范围：RADIUS 1-5，TACACS + 1)

ip-address – 指定服务器的主机 IP 地址 。

缺省配置

无

命令模式

服务组配置

命令用法

◆指定 RADIUS 服务器的索引时,必须已由 radius-server host 命令定义该服务器索引 。

◆指定 TACACS +服务器的索引时，该服务器索引必须已由 tacacs-server host 命令定义 。

范例

```
Console(config)#aaa group server radius tps
Console(config-sg-radius)#server 10.2.68.120
Console(config-sg-radius)#
```

7.5.8 accounting dot1x

此命令在接口上应用 802.1X 服务请求的计费方法。使用 no 形式禁用接口上的记帐。

语法

accounting dot1x {**缺省配置** | *list-name*}

no accounting dot1x

缺省配置 -指定使用 aaaaccounting dot1x 命令创建的默认方法列表 。

list-name - 指定使用 aaa accountingdot1x 命令创建的方法列表 。

缺省配置

无

命令模式

接口配置

范例

```
Console(config)#interface ethernet 1/2

Console(config-if)#accounting dot1x tps

Console(config-if)#
```

7.5.9 show accounting

此命令显示每个功能和端口的当前记帐设置。

语法

show accounting [**commands** [*level*]] |[[**dot1x** [**statistics** [**username** *user-name* | **interface** *interface*]]| **exec** [**statistics**] | **statistics**]

命令 - 显示命令记帐信息。

level - 显示指定级别的命令记帐信息。

dot1x - 显示 dot1x 会计信息。

exec - 显示 Exec 记帐记录。

statistics - 显示记帐记录。

user - *name* - 显示可指定 *用户* *名的* 记帐记录。

接口

以太网 *单元* / *端口*

unit - 单位标识符。 （范围：1）

端口 - 端口号。 （范围：1-28）

缺省配置

无

命令模式

特权模式

范例

```
Console#show accounting

Accounting Type : dot1x

Method List : default

Group List : radius

Interface : Eth 1/1

Method List : tps

Group List : radius

Interface : Eth 1/2

Console#
```

7.6 网络服务器

本节介绍用于配置对交换机的 Web 浏览器管理访问的命令。

7.6.1 ip http port

此命令指定 Web 浏览器界面使用的 TCP 端口号。使用 no 形式使用默认端口。

语法

ip http port *port-number*

no ip http port

port-number -浏览器界面使用的 TCP 端口。（范围：1-65535）

缺省配置

80

命令模式

全局配置

范例

```
Console(config)#ip http port 769

Console(config)#
```

7.6.2 ip http server

此命令允许从浏览器监视或配置该设备。使用 no 形式禁用此功能。

语法

[no] ip http server

缺省配置

启用

命令模式

全局配置

范例

```
Console(config)#ip http server

Console(config)#
```

7.6.3 ip http secure-port

此命令指定用于 HTTPS 连接的 UDP 端口号到交换机的 Web 界面。 使用 **no** 形式还原缺省端口。

语法

ip http secure-port *port_number*

no ip http secure-port

port_number - 用于 HTTPS 的 UDP 端口。（范围：1-65535）

缺省配置

443

命令模式

全局配置

命令用法

◆ 您无法将 HTTP 和 HTTPS 服务器配置为使用同一端口。

◆ 如果更改 HTTPS 端口号，尝试连接到 HTTPS 服务器的客户端必须在 URL 中指定端口号，格式为： **https：//***device*：*port_number*

范例

```
Console(config)#ip http secure-port 1000

Console(config)#
```

7.6.4 ip http secure-server

此命令在安全套接字层（SSL）上启用安全超文本传输协议（HTTPS），为交换机的 Web 界面提供安全访问（即加密连接）。使用 **no** 形式禁用此功能。

语法

[no] ip http secure-server

缺省配置

启用

命令模式

全局配置

命令用法

◆ 可以在交换机上独立启用 HTTP 和 HTTPS 服务。但是您无法将 HTTP 和 HTTPS 服务器配置为使用相同的 UDP 端口。

◆ 如果启用 HTTPS，则必须在浏览器中指定的 URL 中指明此内容：**https：//***device*[：*port number*

范例

```
Console(config)#ip http secure-server

Console(config)#
```

7.7 远程登陆服务器

本节介绍用于配置 Telnet 管理访问交换机的命令。 此交换机还支持 Telnet 客户端功能。 通过在特权模式配置级别输入 telnet 命令，可以从此交换机到另一台设备建立 Telnet 连接。

7.7.1 ip telnet max-sessions

此命令指定可以同时连接到此系统的最大 Telnet 会话数。使用 no 形式恢复默认设置。

语法

ip telnet max-sessions *session-count*

no ip telnet max-sessions

session-count -允许的 Telnet 会话的最大数量。（范围：0-8）

缺省配置

4 会话

命令模式

全局配置

命令用法

对于 Telnet 和 Secure Shell，最多可以同时打开八个会话（Telnet 和 SSH 共享最多一个或八个会话）。

范例

```
Console(config)#ip telnet max-sessions 1
Console(config)#
```

7.7.2 ip telnet port

此命令指定 Telnet 接口使用的 TCP 端口号。使用 no 形式使用默认端口。

语法

ip telnet port *port-number*

no telnet port

port-number -浏览器界面使用的 TCP 端口号。（范围：1-65535）

缺省配置

23

命令模式

全局配置

范例

```
Console(config)#ip telnet port 123
Console(config)#
```

7.7.3 ip telnet server

此命令允许从 Telnet 监视或配置此设备。使用 no 形式禁用此功能。

语法

[no] ip telnet server

缺省配置

启用

命令模式

全局配置

范例

```
Console(config)#ip telnet server
Console(config)#
```

7.7.4 show ip telnet

此命令显示 Telnet 服务器的配置设置。

命令模式

普通模式, 特权模式

范例

```
Console#show ip telnet
IP Telnet Configuration:
Telnet Status: Enabled
Telnet Service Port: 23
Telnet Max Session: 4
Console#
```

7.8 安全壳

本节介绍用于配置 SSH 服务器的命令。请注意，在使用此协议配置交换机时，还需要在管理站上安装 SSH 客户端。交换机支持 SSH 版本 1.5 和 2.0 客户端。

配置指南

此交换机上的 SSH 服务器同时支持密码和公钥身份验证。如果 SSH 客户端指定了密码验证，则可以在本地或通过 RADIUS 或 TCP /远程验证服务器验证密码，如 authenticationlogin 命令所指定。如果客户端指定了公钥验证，则必须在客户端和下一节中描述的交换机上配置验证密钥。请注意，无论您是使用公钥还是密码身份验证，您仍然必须在交换机上生成身份验证密钥并启用 SSH 服务器。

要使用 SSH 服务器，请完成以下步骤：

1. 生成主机密钥对 - 使用 ip ssh crypto host-key generate 命令创建主机公钥/私钥对。

2. 为客户端提供主机公钥 - 许多 SSH 客户端程序在与交换机的初始连接设置期

间自动导入主机公钥。否则您需要在 Management Station 上手动创建一个 knownhosts 文件，并将主机公钥设置为 init。已知主机文件中的公钥条目将类似于以下示例：

10.1.0.54 1024 35

15684995401867669259333946775054617325313674890836547254

15020245593199868544358361651999923329781766065830956

10825913212890233765468017262725714134287629413011961955667825

95664104869574278881462065194174677298486546861571773939016477

93559423035774130980227370877945452408397175264635805817671670

9574804776117

3.将客户端的公钥导入交换机 - 使用 copy tftp public-key 命令将包含公钥的文件复制到交换机的所有 SSH 客户端的管理访问权限。（请注意，必须使用 username 命令在交换机上本地配置这些客户端。）随后使用这些密钥对客户端进行身份验证。 当前固件仅接受基于标准 UNIX 格式的公钥文件，如以下 RSA 密钥示例所示：

1024 3 6

13410816856098939210409449201554253476316419218729589211431738

80055536161631051775940838686311092912322268285192543746031009

37187721199696317813662774141689851320491172048303392543241016

37997592371449011938006090253948408482717819437228840253311595

21348610229029789827213532671316294325328189150453063939166 43

4.设置可选参数 - 设置其他可选参数，包括身份验证超时，重试次数和服务器密钥大小。

5.启用 SSH 服务 - 使用 ip ssh server 命令在交换机上启用 SHS 服务器。

6.身份验证 - 使用以下身份验证方法之一：

密码验证（适用于 SSH v1.5 或 V2 客户端）

a.客户端将其密码发送到服务器。

b.交换机将客户端的密码与存储在内存中的密码进行比较。

c.如果找到匹配项，则允许连接。

注意： 要仅使用密码身份验证的 SSH，主机公钥仍必须在初始连接期间或手动输入到已知主机文件中时提供给客户端。 但是，您无需配置客户端密钥。

公钥验证 - 当 SSH 客户端尝试联系该交换机时，SSH 服务器使用主机密钥对来协商会话密钥和加密方法。只有具有与存储在交换机上的公钥相对应的私钥的客户端才能访问它。在此过程中进行以下交换：

验证 SSH v1.5 客户端

a. 客户端将其 RSA 公钥发送给交换机。

b.交换机将客户端的公钥与存储在内存中的公钥进行比较。

C.如果找到匹配项，则交换机使用其密钥生成随机 256 位字符串作为质询，使用

用户的公钥加密此字符串，并将其发送到客户端。
d. 客户端使用其私钥解密质询字符串，计算 MD5 校验和，并将校验和发送回交换机。
e. 交换机将从客户端发送的校验和与为其发送的原始字符串计算的校验和进行比较。如果两次检验总和匹配，则意味着客户端的私钥对应于授权的公钥，并且客户端是经过身份验证的。
验证 SSH v2 客户端
a. 客户端首先查询交换机以确定使用首选算法的 DSA 公钥认证是否可接受。
b. 如果交换机支持指定的算法，则通知客户端继续进行身份验证过程。否则，它会拒绝该请求。
C. 客户端使用私钥将生成的签名发送到交换机。
d. 当服务器收到此消息时，它会检查提供的密钥是否可用于身份验证，如果是，则检查签名是否正确。如果两者都检查，则客户端已通过身份验证。

注意： SSH 服务器最多支持四个客户端会话。 最大数量的客户端会话包括当前的 Telnet 会话和 SSH 会话。

注意： 可以使用交换机上任何已配置的 IPv4 或 IPv6 接口地址访问 SSH 服务器。

7.8.1 ip sshauthentication-retries

此命令用于配置 SSH 服务器尝试验证用户的次数。使用 no 形式恢复默认设置。

语法

ip ssh authentication-retries *count*

no ip ssh authentication-retries

count - 重置接口后允许的身份验证尝试次数。（范围：1-5）

缺省配置

3

命令模式

全局配置

范例

```
Console(config)#ip ssh authentication-retires 2

Console(config)#
```

7.8.2 ip ssh server

此命令在此交换机上启用 Secure Shell（SSH）服务器。使用 no 形式禁用此服务。

语法

[no] ip ssh server

缺省配置

禁用

命令模式

全局配置

命令用法

◆SSH 服务器最多支持四个客户端会话。 客户会话的最大数量包括当前的 Telnet 会话和 SSH 会话。

◆当客户端第一次与交换机建立连接时，SSH 服务器使用 DSA 或 RSA 进行密钥交换，并且 n 与客户端协商选择 DES（56 位）或 3DES（168 位）进行数据加密。

◆在启用 SSH 服务器之前，必须生成 DSA 和 RSA 主机密钥。

范例

```
Console#ip ssh crypto host-key generate dsa

Console#configure

Console(config)#ip ssh server

Console(config)#
```

7.8.3 ip ssh server-key size

此命令设置 SSH 服务器密钥大小。使用 no 形式恢复默认设置。

语法

ip ssh server-key size *key-size*

no ip ssh server-key size

key-size - 服务器密钥的大小。（范围：512-896 位）

缺省配置

768 bits

命令模式

全局配置

命令用法

服务器密钥是永远不会在交换机外共享的私钥。主机密钥与 SSH 客户端共享，并固定为 1024 位。

范例

```
Console(config)#ip ssh server-key size 512

Console(config)#
```

7.8.4 ip ssh timeout

此命令用于配置 SSH 服务器的超时时间。使用 no 形式恢复默认设置。

语法

ip ssh timeout *seconds*

no ip ssh timeout

seconds – SSH 协商期间客户端响应的超时时间（范围：1-120）

缺省配置

10 秒

命令模式

全局配置

命令用法

超时 指定的时间间隔的开关将等待期间 SSH 协商阶段 fromthe 客户端的响应。 一旦 SSH 会话成为可能 ，用户输入的超时由 vty 会话的 exec-timeout 命令控制 。

范例

```
Console(config)#ip ssh timeout 60

Console(config)#
```

7.8.5 delete public-key

此命令删除指定用户的公钥。

语法

delete public-key *username* [**dsa** | **rsa**]

username – SSH 用户的名称。（范围：1-8 个字符）

dsa - DSA 公钥类型。

rsa - RSA 公钥类型。

缺省配置

删除 DSA 和 RSA 密钥

命令模式

特权模式

范例

```
Console#delete public-key admin dsa

Console#
```

7.8.6 ip ssh crypto host-key generate

此命令生成主机密钥对（即公共密钥和私有密钥对）。

语法

ip ssh crypto host-key generate [**dsa** | **rsa**]

dsa - DSA（版本 2）密钥类型。

rsa - RSA（版本 1）密钥类型。

缺省配置

生成 DSA 和 RSA 密钥对。

命令模式

特权模式

命令用法

◆交换机仅对 SSHv1.5 客户端使用 RSA 版本 1，对 SSHv2 客户端使用 DSAVersion 2。

◆ 此命令将主机密钥对存储在内存（即 RAM）中。使用 ip ssh save host-key 命令将主机密钥保存。

◆作为配置过程的一部分，某些 SSH 客户端程序会自动将公钥添加到已知主机文件中。否则，您必须手动创建已知的主机文件并将主机公钥放入其中。

◆SSH 服务器使用此主机密钥与尝试连接到它的客户端协商会话密钥和加密方法。

范例

```
Console#ip ssh crypto host-key generate dsa

Console#
```

7.8.7 ip ssh crypto zeroize

此命令从内存（即 RAM）清除主机密钥。

语法

ip ssh crypto zeroize [**dsa** | **rsa**]

dsa - DSA 密钥类型。

rsa - RSA 密钥类型。

缺省配置

清除 DSA 和 RSA 密钥

命令模式

特权模式

命令用法

◆此命令从易失性存储器（RAM）中清除主机密钥。使用 no ip ssh save host-key 命令清除保存过的主机密钥。

◆必须先禁用 SSH 服务器，然后才能执行此命令。

范例

```
Console#ip ssh crypto zeroize dsa

Console#
```

7.8.8 ip ssh save host-key

此命令将主机密钥从 RAM 保存到闪存。

语法

ip ssh save host-key

缺省配置

保存 DSA 和 RSA 密钥。

命令模式

特权模式

范例

```
Console#ip ssh save host-key dsa

Console#
```

7.8.9 show ip ssh

此命令显示验证客户端访问 SSH 服务器时使用的连接设置。

命令模式

特权模式

范例

```
Console#show ip ssh

SSH Enabled - Version 2.0

Negotiation Timeout : 120 seconds; Authentication Retries : 3

Server Key Size : 768 bits

Console#
```

7.8.10 show public-key

此命令显示指定用户或主机的公钥。

语法

show public-key [**user** [*username*]| **host**]

username - 此命令显示指定用户或主机的公钥。

缺省配置

显示所有公钥

命令模式

特权模式

命令用法

◆如果未输入参数，则显示所有键。如果输入了用户关键字，但未指定用户名，则显示所有用户的公钥。

◆当显示 RSA 密钥时，第一个字段指示主机密钥的大小（例如，10　24），第二个字段是编码的公共指数（例如，35），最后一个字符串是编码的模数。当显示 DSA 密钥时，第一个字段指示 SHS

使用的加密方法基于数字签名标准（DSS），并且持续字符串是编码模数。

范例

```
Console#show public-key host

Host:

RSA:

1024 65537 13236940658254764031382795526536375927835525327972629521130241

07194210616557594245909392360969540503627752575562510038661309893938345231 0

33280214988866192159556859887989191950588394018138744046890877916030583776 8

18549000283134162500834871844952208742921225569166565529632816351696404083 1

5547660664151657116381

DSA:

ssh-dss AAAB3NzaC1kc3MAAACBAPWKZTPbsRIB8ydEXcxM3dyV/yrDbKStIlnzD/DgOh2Hxc

YV44sXZ2JXhamLK6P8bvuiyacWbUW/a4PAtp1KMSdqsKeh3hKoA3vRRSy1N2XFfAKxl5fwFfv

JlPdOkFgzLGMinvSNYQwiQXbKTBHOZ4mUZpE85PWxDZMaCNBPjBrRAAAAFQChb4vsdfQGNIjwbv

wrNLaQ77isiwAAAIEAsy5YWDC99ebYHNRj5kh47wY4i8cZvH+/p9cnrfwFTMUO1VFDly3IR

2G395NLy5Qd7ZDxfA9mCOfT/yyEfbobMJZi8oGCstSNOxrZZVnMqWrTYfdrKX7YKBw/Kjw6Bm

iFq7O+jAhf1Dg45loAc27s6TLdtny1wRq/ow2eTCD5nekAAACBAJ8rMccXTxHLFAczWS7EjOy

DbsloBfPuSAb4oAsyjKXKVYNLQkTLZfcFRu41bS2KV5LAwecsigF/+DjKGWtPNIQqabKgYCw2

o/dVzX4Gg+yqdTlYmGA7fHGm8ARGeiG4ssFKy4Z6DmYPXFum1Yg0fhLwuHpOSKdxT3kk475S7

wOW

Console#
```

7.8.11 show ssh

此命令显示当前的 SSH 服务器连接。

命令模式

特权模式

范例

```
Console#show ssh

Connection Version State Username Encryption
```

0 2.0 Session-Started admin ctos aes128-cbc-hmac-md5

stoc aes128-cbc-hmac-md5

Console#

7.9 802.1X 端口认证

该交换机支持基于 IEEE 802.1X（dot1x）端口的访问控制，通过要求用户首先提交凭据进行身份验证，防止对网络进行未经授权的访问。客户端身份验证由 RADIUS 服务器使用 EAP（可扩展身份验证协议）进行控制。

7.9.1 dot1x 缺省配置

此命令将所有可配置的 dot1x 全局和端口设置设置为其默认值。

命令模式

全局配置

范例

Console(config)#dot1x default

Console(config)#

dot1x eapol-pass-through

当全局禁用 dot1x 时，此命令将 EAPOL 帧传递到 STP 转发状态中的所有端口。使用 no 形式恢复默认值。

语法

[no] dot1x eapol-pass-through

缺省配置

当全局禁用 dot1x 时，丢弃所有 EAPOL 帧

命令模式

全局配置

命令用法

◆ 当此设备作为网络中的中间节点并且不需要执行 dot1x 身份验证时，dot1x eapolpass-through 命令可用于将 EAPOL 帧转发到使用身份验证服务器进行身份验证的其他交换

机，从而允许身份验证过程仍然由位于网络边缘的交换机执行。

◆当此设备用作边缘交换机但不需要对任何连接的客户端进行身份验证时，可以使用 no dot1x eapol-pas sthrough 命令来丢弃不必要的 EAPOL 流量。

范例

此示例指示交换机将所有 EAPOL 帧传递到 STP 转发状态中的任何端口。

```
Console(config)#dot1x eapol-pass-through
Console(config)#
```

7.9.2 dot1x system-auth-control

此命令在交换机上全局启用 IEEE 802.1X 端口验证。使用 no 形式恢复默认值。

语法

[no] dot1x system-auth-control

缺省配置

禁用

命令模式

全局配置

范例

```
Console(config)#dot1x system-auth-control
Console(config)#
```

7.9.3 dot1x intrusion-action

此命令设置端口对失败的身份验证的响应，或者阻止所有流量，或者将端口的所有流量分配给访客 VLAN。使用 no 形式重置默认值。

语法

dot1x intrusion-action {block-traffic | guest-vlan}

no dot1x intrusion-action

block-traffic -阻止此端口上的流量。

guest-vlan -将用户分配给 Guest VLAN。

缺省配置

块传输

命令模式

接口配置

命令用法

要使 guest VLAN 分配成功，必须配置 VLAN 并将其设置为 active（请参阅 vlan database 命令）并将其指定为端口的最新 VLAN（请参阅 network-access guest-vlan 命令）。

范例

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x intrusion-action guest-vlan
Console(config-if)#
```

7.9.4 dot1x max-reauth-req

此命令设置交换机在重新启动身份验证过程之前向客户端发送 EAP 请求/标识帧的最大次数。使用 no 形式恢复默认值。

语法

dot1x max-reauth-req *count*

no dot1x max-reauth-req

count -最大请求数（范围：1-10）

缺省配置

2

命令模式

接口配置

范例

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x max-reauth-req 2
Console(config-if)#
```

7.9.5 dot1x max-req

此命令设置交换机端口在超出身份验证会话之前将 EAP 请求/身份数据包传输到客户端的最大次数。使用 no 形式恢复默认值。

语法

dot1x max-req *count*

no dot1x max-req

count - The maximum number of requests (Range: 1-10)

缺省配置

2

命令模式

接口配置

范例

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x max-req 2
Console(config-if)#
```

7.9.6 dot1x operation-mode

此命令允许主机（客户端）连接到 802.1X 授权端口。使用**不**带关键字的 no 形式将默认值恢复为单个主机。 使用带有**多主机** max-count 关键字的 no 形式来恢复默认的最大计数。

语法

dot1x operation-mode {**single-host** |**multi-host** [**max-count** *count*] | **mac-based-auth**}

no dot1x operation-mode [**multi-host max-count**]

单主机 - 仅允许单个主机连接到此端口。

多主机 - 允许多个主机连接到此端口。

max-count - 最大主机数的关键字。

count - 可以连接到端口的最大主机数。（范围：1-1024;默认值：5）

基于 mac - 允许多个主机连接到此端口，需要对主机进行身份验证。

缺省配置

单主机

命令模式

接口配置

命令用法

◆此命令指定的“max-count”参数仅在 dot1x port-control 命令将 dot1x 模式设置为“auto”时有效 。

◆ 在“多主机”模式下，只有一个连接到端口的主机需要通过认证才能为所有其他主机授予网络访问权限。同样如果一个附属主机无法重新验证或发送一个端口，则所有主机的端口都可能未经授权 EAPOL 注销消息。

◆ 在“基于 mac-auth”模式下，连接到端口的每台主机都需要通过认证。允许访问此模式下的端口操作的主机数量仅受这些固定地址表中的可用空间（即最多 1024 个地址）的限制。

范例

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x operation-mode multi-host max-count 10
Console(config-if)#
```

7.9.7 dot1x port-control

此命令在端口接口上设置 dot1x 模式。使用 no 形式恢复默认值。

语法

dot1x port-control {**auto** | **force-authorized** |**force-unauthorized**}

no dot1x port-control

auto - 需要 RADIUS 服务器授权支持 dot1x 的连接客户端。 不支持 dot1x 的客户端将被拒绝访问。

force-authorized - 配置端口以授予对所有客户端的访问权限，无论是 dot1x 还是其他。

force-unauthorized - 配置端口拒绝访问所有客户端，无论是 dot1x 感知还是其他方式。

缺省配置

强制授权

命令模式

接口配置

范例

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x port-control auto
Console(config-if)#
```

7.9.8 dot1x re-authentication

此命令启用对指定端口的定期重新身份验证。使用 no 形式禁用重新身份验证。

语法

[no] dot1x re-authentication

命令模式

接口配置

命令用法

◆重新验证过程　验证 RADIUS 服务器上连接的客户端的用户 ID 和密码。在重新认证期间，客户端仍然与网络连接，并且 dot1x 客户端软件可以处理该过程。只有重新验证失败才会阻止端口。

◆在 dot1x timeout re-authperiod 命令指定的时间间隔后，重新验证连接的客户端。默认值为 3600 秒。

范例

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x re-authentication
Console(config-if)#
```

7.9.9 dot1x timeout quiet-period

此命令设置在尝试获取新客户端之前，在超过最大请求计数后交换机端口等待的时间。使用 no 形式重置默认值。

语法

dot1x timeout quiet-period *seconds*

no dot1x timeout quiet-period

seconds -秒数。（范围：1-65535）

缺省配置

60 秒

命令模式

接口配置

范例

```
Console(config)#interface eth 1/2

Console(config-if)#dot1x timeout quiet-period 350

Console(config-if)#
```

7.9.10 dot1x timeout re-authperiod

此命令设置必须对连接的客户端进行身份验证的时间段。使用此命令的 no 形式重置默认值。

语法

dot1x timeout re-authperiod *seconds*

no dot1x timeout re-authperiod

seconds -秒数。（范围：1-65535）

缺省配置

3600 秒

命令模式

接口配置

范例

```
Console(config)#interface eth 1/2

Console(config-if)#dot1x timeout re-authperiod 300

Console(config-if)#
```

7.9.11 dot1x timeout supp-timeout

此命令设置交换机上的接口在重新传输 EAP 协议包之前等待来自客户端的 EAP 请求的时间。使用 no 形式重置为默认值。

语法

dot1x timeout supp-timeout *seconds*

no dot1x timeout supp-timeout

seconds -秒数。 （范围：1-65535）

缺省配置

30 秒

命令模式

接口配置

命令用法

此命令设置除 EAP 之外的 EAP 请求帧的超时-请求/标识帧。如果在端口上启用了 dot1x 身份验证，则当端口链路状态出现时，交换机将启动身份验证。它将向客户端发送 EAP 请求/身份帧以请求其身份，然后是一个或多个身份验证信息请求。它还可以根据重新认证的需要在主动连接期间向客户端发送其他 EAP 请求帧。

范例

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout supp-timeout 300
Console(config-if)#
```

7.9.12 dot1x timeout tx-period

此命令设置在重新传输 EAP 数据包之前，交换机上的接口在认证会话期间等待的时间。使用 no 形式重置为默认值。

语法

dot1x timeout tx-period *seconds*

no dot1x timeout tx-period

seconds -秒数。（范围：1-65535）

缺省配置

30 秒

命令模式

接口配置

范例

```
Console(config)#interface eth 1/2
```

```
Console(config-if)#dot1x timeout tx-period 300

Console(config-if)#
```

7.9.13 dot1x re-authenticate

此命令强制在所有端口或特定接口上重新进行身份验证。

语法

dot1x re-authenticate [*interface*]

interface

ethernet *unit/port*

unit - 单位标识符。 （范围：1）

端口 - 端口号。 （范围：1-28）

命令模式

特权模式

命令用法

重新验证过程验证连接的客户端的用户 ID 和 RADIUS 服务器上的密码。 在重新验证期间，客户端保持连接网络，透明处理过程通过 dot1x 客户端软件。只有重新认证失败才是端口受阻。

范例

```
Console#dot1x re-authenticate

Console#
```

7.9.14 dot1x identity profile

此命令设置 dot1x 请求者用户名和密码。使用 **no** 形式删除标识设置。

语法

dot1x identity profile {**username** *username* | **password** *password*}

no dot1x identity profile {**username** | **password**}

username - 指定请求者用户名。（范围：1-8 个字符）

password - 指定请求者密码。（范围：1-8 个字符）

缺省配置

无

命令模式

全局配置

命令用法

全局请求者用户名和密码用于在响应来自该客户端的 MD5 质询时将此交换机识别为请求者。当此交换机将客户端身份验证请求传递给网络上的另一个身份验证器时，必须设置这些参数。

范例

```
Console(config)#dot1x identity profile username steve
Console(config)#dot1x identity profile password excess
Console(config)#
```

7.9.15 dot1x max-start

此命令设置端口请求者在假定客户端为802.1X不知道之前向客户端发送EAP开始帧的最大次数。使用 no 形式恢复默认值。

语法

dot1x max-start *count*

no dot1x max-start

count -指定 EAP 起始帧的最大数量。（范围：1-65535）

缺省配置

3

命令模式

接口配置

范例

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x max-start 10
Console(config-if)#
```

7.9.16 dot1x pae supplicant

此命令在端口上启用 dot1x 请求方模式。使用 no 形式禁用端口上的 dot1x 请求方模式。

语法

[no] dot1x pae supplicant

缺省配置

禁用

命令模式

接口配置

命令用法

◆当连接到端口的设备必须向网络上的另一个验证器提交请求时，请配置标识此开关的身份配置文件参数作为请求者，并为必须通过远程验证者使用此命令验证客户端的端口启用 dot1x 请求者模式。在此模式下，端口不会响应用于验证者的 dot1x 信息。

◆ 通过将控制模式设置为“auto”， 可以将此交换机配置为在选定端口上作为可靠的，并通过将控制模式设置为“强制授权”并使用此命令启用 dot1x 请求者模式，将其配置为其他端口上的请求者。

◆如果某个端口是聚合组的成员或端口上启用了 LACP，则该端口不能配置为 dot1x 请求者 。

范例

```
Console(config)#interface ethernet 1/2
Console(config-if)#dot1x pae supplicant
Console(config-if)#
```

7.9.17 dot1x timeout auth-period

此命令设置请求方端口等待来自验证方的响应的时间。使用 no 形式恢复默认设置。

语法

dot1x timeout auth-period *seconds*

no dot1x timeout auth-period

seconds -秒数。 （范围：1-65535）

缺省配置

30 秒

命令模式

接口配置

命令用法

此命令设置请求者等待来自 EAPOL-Start 以外的数据包的验证者响应的时间。

范例

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout auth-period 60
Console(config-if)#
```

7.9.18 dot1x timeout held-period

此命令设置请求方端口在重新发送凭据以查找新的身份验证器之前等待的时间。使用 no 形式重置默认值。

语法

dot1x timeout held-period *seconds*

no dot1x timeout held-period

seconds -秒数。（范围：1-65535）

缺省配置

60 秒

命令模式

接口配置

范例

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout held-period 120
Console(config-if)#
```

7.9.19 dot1x timeout start-period

此命令设置请求方端口在将 EAPOL 开始帧重新发送到验证方之前等待的时间。使用 no 形式恢复默认设置。

语法

dot1x timeout start-period *seconds*

no dot1x timeout start-period

seconds -秒数。（范围：1-65535）

缺省配置

30 秒

命令模式

接口配置

范例

```
Console(config)#interface eth 1/2

Console(config-if)#dot1x timeout start-period 60

Console(config-if)#
```

7.9.20 show dot1x

此命令显示交换机或特定接口上的常规端口验证相关设置。

语法

show dot1x [**statistics**] [**interface** *interface*]

statistics - Displays dot1x status for each port.

interface

ethernet *unit/port*

unit - 单位标识符。 （范围：1）

端口 - 端口号。 （范围：1-28）

命令模式

特权模式

命令用法

此命令显示 dot1x 信息。

范例

```
Console#show dot1x

Global 802.1X Parameters

System Auth Control : Enabled

Authenticator Parameters:

EAPOL Pass Through : Disabled

Supplicant Parameters:
```

```
Identity Profile Username : steve

802.1X Port Summary

Port Type Operation Mode Control Mode Authorized

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

Eth 1/ 1 禁用 Single-Host Force-Authorized Yes

Eth 1/ 2 禁用 Single-Host Force-Authorized Yes

...

Eth 1/27 禁用 Single-Host Force-Authorized Yes

Eth 1/28 启用 Single-Host Auto Yes

802.1X Port Details

802.1X Authenticator is Enabled on port 1/1

802.1X Supplicant is Disabled on port 1/1

...

802.1X Authenticator is Enabled on port 28

Reauthentication : Enabled

Reauth Period : 3600

Quiet Period : 60

TX Period : 30

Supplicant Timeout : 30

Server Timeout : 10

Reauth Max Retries : 2

Max Request : 2

Operation Mode : Multi-host

Port Control : Auto

Intrusion Action : Block traffic

Supplicant : 00-e0-29-94-34-65

Authenticator PAE State Machine

State : Authenticated

Reauth Count : 0

Current Identifier : 3
```

```
Backend State Machine

State : Idle

Request Count : 0

Identifier(Server) : 2

Reauthentication State Machine

State : Initialize

Console#
```

7.10 管理 IP 过滤器

本节介绍用于配置对交换机的 IP 管理访问的命令。

7.10.1 management

此命令指定允许通过各种协议访问交换机的客户端 IP 地址。使用 no 形式恢复默认设置。

语法

[no] management {all-client | http-client | snmp-client |telnet-client} *start-address* [*end-address*]

all-client - 为所有组添加 IP 地址。

http-client - 将 IP 地址添加到 Web 组。

snmp-client - 将 IP 地址添加到 SNMP 组。

telnet-client - 将 IP 地址添加到 Telnet 组。

start-address - 单个 IP 地址或范围的起始地址。

end-address - 范围的结束地址。

缺省配置

所有地址

命令模式

全局配置

命令用法

◆如果有人尝试从无效地址访问交换机上的管理接口，交换机将拒绝连接，在系统日志中输入事件信息，并向陷井管理者发送陷阱消息。

◆可以分别为 SNMP，Web 和 Telnet 访问 配置 IP 地址。这些组中的每一个都可以包括最多五个不同的地址集，单独的地址或地址范围。

◆输入同一组（即 SNMP，Web 或 Telnet）的地址时，交换机将不接受超出应用的地址范围。 对于不同组的轮换地址，交换机将接受重写地址范围。

◆您无法从指定范围中删除单个地址。您必须删除整个范围，然后重新输入地址。

◆你可以只通过指定起始地址，或者从同时指定起始地址和结束地址删除的地址范围。

范例

此示例限制对指定地址的管理访问。

```
Console(config)#management all-client 192.168.1.19

Console(config)#management all-client 192.168.1.25 192.168.1.30

Console#
```

7.10.2 show management

此命令显示允许通过各种协议访问交换机的客户端 IP 地址。

语法

show management {**all-client** | **http-client** | **snmp-client** |**telnet-client**}

all-client - 显示所有组的 IP 地址。

http-client - 显示 Web 组的 IP 地址。

snmp-client - 显示 SNMP 组的 IP 地址。

telnet-client - 显示 Telnet 组的 IP 地址。

命令模式

特权模式

范例

```
Console#show management all-client

Management Ip Filter

HTTP-Client:

Start IP address End IP address

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

1. 192.168.1.19 192.168.1.19

2. 192.168.1.25 192.168.1.30

SNMP-Client:

Start IP address End IP address

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

1. 192.168.1.19 192.168.1.19

2. 192.168.1.25 192.168.1.30

TELNET-Client:

Start IP address End IP address

---

1. 192.168.1.19 192.168.1.19

2. 192.168.1.25 192.168.1.30

Console#

7.11 PPPOE 中间代理

本节介绍用于配置在客户端和宽带远程访问服务器之间传递身份验证消息所需的 PPPoE IA 中继参数的命令。

7.11.1 pppoe intermediate-agent

此命令在交换机上全局启用 PPPoE 中间代理。使用 no 形式禁用此功能。

语法

[no] pppoe intermediate-agent

缺省配置

禁用

命令模式

全局配置

命令用法

◆交换机插入标签标识本身作为 PPPoE 中间体的附加客户端之间请求网络接入和连接到宽带远程接入服务器（BRAS）的端口。这个交换机从客户端的 PPPoE 活跃发现请求中提取访问循环信息，并将此信息转发到由 pppoe intermediate-agent trust 命令指定的所有可信端口。BRAS 在 PPPoE 发现期间检测到由交换机插入的用户的 circuit-Id 标签的存在，并将该标签作为 PPP 认证中的 NASport-Id 属性和 AAA 计费请求发送给 RADIUS 服务器。

◆必须先使用此命令启用 PPPoE IA，然后才能使这条命令在接口上启用此功能 。

范例

```
Console(config)#pppoe intermediate-agent

Console(config)#
```

7.11.2 pppoe intermediate-agent format-type

此命令设置交换机的访问节点标识符和一般错误消息。使用 no 形式恢复默认设置。

语法

pppoe intermediate-agent format-type {**access-node-identifier** *id-string* | **generic-error-message** *error-message*}

no pppoe intermediate-agent format-type {**access-nodeidentifier** | **generic-error-message**}

id-string -将此交换机标识为 PPPoEserver 的 P PPoE IA 的字符串。 （范围：1-48 个 ASCII 字符）

error-message - 一条错误消息，通知发件人 PPPoE Discovery 数据包太大。

缺省配置

◆Access Node Identifier: 管理接口的 IP 地址

◆Generic Error Message: PPPoE 发现数据包太大而无法处理。尝试减少添加的标签数量。

命令模式

全局配置

命令用法

◆交换机使用 access-node-identifier 生成发送给 BRAS 的 PPPoE 发现阶段报文的 circuit-id，但不修改这些 PPPoE 发现报文的源 MAC 地址或目的 MAC 地址。

◆这些消息将转发到 pppoe intermediate-agent trust 命令指定的所有可信端口 。

范例

```
Console(config)#pppoe intermediate-agent format-type access-node-identifierbillibong

Console(config)#
```

7.11.3 pppoe intermediate-agent port-enable

此命令在接口上启用 PPPoE IA。 使用 no 形式禁用此功能。

语法

[no] pppoe intermediate-agent port-enable

缺省配置

禁用

命令模式

接口配置（Ethernet，Port Channel）

命令用法

还必须在交换机上全局启用 PPPoE IA 以实现此命令的转换效果。

范例

```
Console(config)#int ethernet 1/5

Console(config-if)#pppoe intermediate-agent port-enable

Console(config-if)#
```

7.11.4 pppoe intermediate-agent port-format-type

此命令设置接口的 circuit-id 或 remote-id。使用 no 形式恢复默认设置。

语法

pppoe intermediate-agent port-format-type {**circuit-id** |**remote-id**} *id-string*

circuit-id -标识用户所连接的交换机上的电路标识符（或接口）的字符串。 （范围：1-10 个 ASCII 字符）

remote-id -标识用户所 连接的 此交换机上的远程标识符（或接口）的字符串 。 （范围：1-63 个 ASCII 字符）

缺省配置

circuit-id: unit / port：vlan-id 或 0 / trunk-id：vlan-id

remote-id: 端口 MAC 地址

命令模式

接口配置（Ethernet，Port Channel）

命令用法

◆PPPoE 服务器从 PPPoE 发现阶段消息中提取 Line-Id 标记，并使用该标记的 Circuit-Id 字段作为 AAA 访问和记帐请求中的 NAS-Port-Idattribute。

◆ 交换机拦截来自客户端的 PPPoE 发现帧，并使用 PPPoE Ve ndor-Specific 标记（0x0105）将唯一的线路标识符插入 PPPoE Active Discovery Initiation（PADI）和 Request（PADR）数据包。然后交换机将这些数据包转发到 PPPoEserver。 标签包含接收发现数据包的客户线路的 Line-Id，进入交换机（或接入节点）

中间代理所在的位置。

◆ 来自 PPPoE 服务器的传出 PAD 提供（PADO）和会话确认（PADS）数据包包括由交换机插入的 Circuit-Id 标签，应该从 PADO 和 PADS 数据包中删除，以便直接传递给端节点客户端使用所述的这条命令。

范例

```
Console(config)#int ethernet 1/5
Console(config-if)#pppoe intermediate-agent port-format-type circuit-id
ECS4500-28
Console(config-if)#
```

7.11.5 pppoe intermediate-agent trust

此命令将接口设置为受信任模式，以指示它已连接到 PPPoE 服务器。 使用 no 形式设置接口可信模式。

语法

[no] **pppoe intermediate-agent trust**

缺省配置

非信任

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

◆将交换机连接到 PPPoE Server 的任何接口设置为信任。将交换机连接到用户（PPPoE 客户端）的接口应设置为不可信。

◆交换机上必须至少配置一个可信任接口才能使 PPPoE IA 正常运行。

范例

```
Console(config)#int ethernet 1/5
Console(config-if)#pppoe intermediate-agent trust
Console(config-if)#
```

7.11.6 pppoe intermediate-agent vendor-tagstrip

此命令允许从 PPPoE 服务器发送的 PPPoE 发现协议包中剥离供应商标签。使用 no 形式禁用此功能。

语法

[no] pppoe intermediate-agent vendor-tag strip

缺省配置

禁用

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

此命令仅适用于可信任接口。 它用于在从上游 PPPoE 服务器接收的 PPPoE 发现数据包中剥离特定于发送者的标签（其中包含用户和线路识别信息），然后再将其转发给用户。

范例

```
Console(config)#int ethernet 1/5
Console(config-if)#pppoe intermediate-agent vendor-tag strip
Console(config-if)#
```

7.11.7 clear pppoe intermediate-agent statistics

此命令清除 PPPoE 中间代理的统计计数器。

语法

clear pppoe intermediate-agent statistics [**interface**[*interface*]]

interface

ethernet *unit/port*

单位 - 堆叠单位。 （范围：1）

端口 - 端口号。 （范围：1-28）

port-channel *channel-id* （范围：1-12）

命令模式

特权模式

范例

```
Console#clear pppoe intermediate-agent statistics

Console#
```

7.11.8 show pppoe intermediate-agent info

此命令显示 PPPoE IntermediateAgent 的配置设置。

语法

show pppoe intermediate-agent info [**interface** [*interface*]]

interface

ethernet *unit/port*

unit -堆叠单位。 （范围：1）

port -端口号。 （范围：1-28）

port-channel *channel-id*（范围：1-12）

命令模式

特权模式

范例

```
Console#show pppoe intermediate-agent info

PPPoE Intermediate Agent Global Status : Enabled

PPPoE Intermediate Agent Admin Access Node Identifier : 192.168.0.2

PPPoE Intermediate Agent Oper Access Node Identifier : 192.168.0.2

PPPoE Intermediate Agent Admin Generic Error Message :

PPPoE Discover packet too large to process. Try reducing the number of tags

added.

PPPoE Intermediate Agent Oper Generic Error Message :

PPPoE Discover packet too large to process. Try reducing the number of tags

added.

Consoleshow pppoe intermediate-agent info interface ethernet 1/1
```

```
Interface PPPoE IA Trusted Vendor-Tag Strip Admin Circuit-ID Admin Remote-ID
Oper Circuit-ID Oper Remote-ID
--------- -------- ------- ---------------- ------------ ----------------
Eth 1/2 Yes No Yes ECS4510-28T ECS4510-28T
ECS4510-28T ECS4510-28T
Console#
```

7.11.9 show pppoe intermediate-agent statistics

此命令显示 PPPoE 中间代理的统计信息。

语法

show pppoe intermediate-agent statistics interface [*interface*]

interface

ethernet *unit/port*

unit -单位标识符。 （范围：1）

port -端口号。 （范围：1-28）

port-channel *channel-id* （范围：1-12）

命令模式

特权模式

范例

```
Console#show pppoe intermediate-agent statistics interface ethernet 1/1
Eth 1/1 statistics
------------------------------------------------------------------------------
Received : All PADI PADO PADR PADS PADT
---------- ---------- ---------- ---------- ---------- ----------
3 0 0 0 0 3
Dropped : Response from untrusted Request towards untrusted Malformed
---------------------- ------------------------ ---------
0 0 0
Console#
```

8 全局安全措施

此交换机支持许多方法，用于隔离连接到每个数据端口的客户端的流量，并确保只有授权客户才能访问网络。 使用 IEEE802.1X 的基于端口的身份验证通常用于这些目的。 除了这些方法之外，本章还介绍了提供客户端安全性的其他几个选项。 这些包括基于端口的身份验证，可以通过指定一组固定的 MAC 地址来配置允许网络客户端访问。也可以使用 IP Source Guard 和 DHCP Snooping 命令仔细控制分配给 DHCP 客户端的地址。

8.1 端口安全

这些命令可用于在端口上启用端口安全性。使用端口安全性时，交换机会停止学习新的 MAC 地址达到配置的最大数量时指定的端口。
只有具有已存储在此端口的动态或静态地址表中的源地址的传入流量才有权访问该网络。 端口将丢弃任何传入帧，其源 MAC 地址未知或之前已从其他端口获知。如果具有未授权 MAC 地址的设备尝试使用交换机端口，则将检测到入侵并且交换机可以通过禁用自动执行操作端口并发送陷阱消息。

8.1.1 port security

此命令启用或配置端口安全性。使用不带任何关键字的 no 形式禁用端口安全性。 使用带有适当关键字的 no 形式可以恢复响应安全违规的默认设置或最大允许地址数。

语法

port security [action {shutdown | trap | trap-and-shutdown}| max-mac-count *address-count*]

no port security [action | max-mac-count]

action -违反端口安全性时的响应。

shutdown -违反端口安全性时的响应。

trap -仅发出 SNMP 陷阱消息。

trap-and-shutdown -发出 SNMP 陷阱消息和禁用端口。

max-mac-count

address-count -端口可以学习的最大 MAC 地址数。（范围：0 - 1024，其中 0 表示禁用）

缺省配置

状态：禁用

应用：无

最大地址：0

命令模式

接口配置 (Ethernet)

命令用法

◆ 安全端口上允许的默认最大 MAC 地址数为零（即禁用端口安全性）。要使用端口安全性，您必须使用端口安全的 **max-mac-count** 命令配置端口上允许的最大地址数 。

◆ 当端口安全使用的 **port security** 命令，在启用端口安全之后，将最大允许数或允许地址设置为低于当前限制值，交换机首先从地址表中清除所有动态学习的条目。然后启动在指定端口上学习新的 MAC 地址，并在达到配置的最大数量时停止学习地址。只有已存储在动态或静态地址表中的源地址的传入流量才会被接受。

◆ 要配置可在端口上学习的最大地址条目数，请指定允许的最大动态地址数。交换机将学习最大数量的允许地址对<源 MAC 地址,VLAN>用于在端口上接收的帧数。(启用或禁用端口安全时，指定的最大地址计数有效。）请注意，您可以手动添加使用 mac-address-tablestatic 命令为端口添加其他安全地址。当端口达到最大 MAC 地址数时，端口将停止学习新地址。已保留在地址表中的 MAC 地址将被保留，不会被删除。

◆ 如果启用了端口安全性，并且最大允许地址数设置为非零值，则将阻止任何不在地址表的 MAC 地址尝试使用该端口的设备访问该交换机。

◆ 如果由于安全性违规而禁用端口，则必须使用 no shutdown 命令手动重新启用该端口 。

◆ 安全端口具有以下限制：

- 无法连接到网络互连设备。
- 不能是中继端口。

范例

下面的示例启用端口 5 的端口安全性，并设置安全漏洞的响应以发出陷阱消息：

```
Console(config)#interface ethernet 1/5

Console(config-if)#port security action trap
```

8.1.2 show port security

此命令显示端口安全状态和安全地址计数。

语法

show port security [**interface** *interface*]

interface -指定端口接口。

ethernet *单元 / 端口*

unit -单位标识符。 （范围：1）

port -端口号。 （范围：1-28）

端口号。 （范围：1-28）

特权模式

范例

此示例显示端口安全设置和安全数量所有端口的地址。

```
Console#show port security

Global Port Security Parameters

Secure MAC Aging Mode : Disabled

Port Security Port Summary

Port Port Security Port Status Intrusion Action MaxMacCnt CurrMacCnt

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

Eth 1/ 1 Disabled Secure/Down None 0 2

Eth 1/ 2 Enabled Secure/Up None 10 0

Eth 1/ 3 Disabled Secure/Down None 0 0

Eth 1/ 4 Disabled Secure/Down None 0 0

Eth 1/ 5 Disabled Secure/Down None 0 0
```

8.2 网络访问

网络访问身份验证通过验证尝试连接到aswitch端口的每个主机的MAC地址来控制对网络的访问。仅当源 MAC 地址由中央 RADIUS 服务器成功验证时，才从交换机转发从特定 MAC 地址接收的流量。 虽然 MAC 地址的身份验证正在进行，但在身份验证完成之前，所有流量都会被阻止。成功通过身份验证后，RADIUS 服务器可以选择为交换机端口分配 VLAN 和 QoS 设置。

8.2.1 network-accessaging

使用此命令为存储在安全 MAC 地址表中的已认证 MAC 地址启用老化。 使用此命令的 no 形式禁用地址老化。

语法

[no] network-access aging

缺省配置

禁用

命令模式

全局配置

命令用法

◆经过身份验证的 MAC 地址作为动态条目存储在交换机的安全 MAC 地址表中，并在老化时间到期时被删除。地址老化时间由 mac address-table aging-time 命令决定。

◆此参数适用于本节所述的 MAC 地址认证过程配置的认证 MAC 地址，以及 802.1X 认证的任何安全 MAC 地址，无论 802.1X 操作模式（单主机，多主机或基于 MAC）认证）。

◆交换机系统支持的最大安全 MAC 地址数为 1024。

范例

```
Console(config-if)#network-access aging
Console(config-if)#
```

8.2.2 network-accessmac-filter

使用此命令将 MAC 地址添加到过滤器表中。使用 no 形式删除指定的 MAC 地址。

语法

[no] **network-access mac-filter** *filter-id***mac-address** *mac-address* [**mask** *mask-address*]

filter-id -指定 MAC 地址过滤表。（范围：1-64）

mac-address -指定 MAC 地址条目。（格式：xx-xx-xx-xx-xx-xx

mask -指定一系列地址的 MAC 地址位掩码。

缺省配置

禁用

命令模式

全局配置

命令用法

◆指定的地址免于网络访问身份验证。

◆此命令与使用 mac-address-table static 命令配置静态地址不同，它允许您在使用掩码时配置一组地址，然后使用 network-access port-mac 将这些地址分配给一个或多个端口 -filter 命令。

◆最多可以定义 64 个过滤表。

◆对过滤表中输入的条目数没有限制。

范例

```
Console(config)#network-access mac-filter 1 mac-address 11-22-33-44-55-66
Console(config)#
```

8.2.3 mac-authentication reauth-time

使用此命令设置必须重新验证连接的 MAC 地址的时间段。使用此命令的 no 形式来恢复默认值。

语法

mac-authentication reauth-time *seconds*

no mac-authentication reauth-time

seconds -认证时间周期（范围：120-1000000 秒）。

缺省配置

1800

命令模式

全局配置

命令用法

◆重新 - 认证时间是一个全局设置，适用于所有端口。

◆当再 - 认证到期时间为安全 MAC 地址是 ISRE - 与 RADIUS 服务器进行验证。在重新 - 通过端口认证处理交通不受影响。

范例

```
Console(config)#mac-authentication reauth-time 300

Console(config)#
```

8.2.4 network-access dynamic-qos

使用此命令为认证端口启用动态 QoS 功能。使用 no 形式恢复默认值。

语法

[no] network-access dynamic-qos

缺省配置

禁用

命令模式

接口配置

命令用法

◆RADIUS 服务器可以选择性地返回动态 QoS 分配，以应用于经过身份验证的用户的交换机端口。

◆ 当最后一个用户使用动态 QoS 分配注销端口时，交换机将恢复端口的原始 QoS 配置。

◆ 当用户尝试使用与已登录到同一端口的用户不同的返回 dynamicQoS 配置文件登录网络时，将拒绝用户访问。

◆ 虽然端口具有已分配的动态 QoS 配置文件，但任何手动 QoS 配置更改仅在所有用户都已注销端口后生效。

注意 ：用于动态 QoS 的任何配置变化将不会保存到换精计划配置文件。

范例

以下示例在端口 1 上启用动态 QoS 功能。

```
Console(config)#interface ethernet 1/1

Console(config-if)#network-access dynamic-qos

Console(config-if)#
```

8.2.5 network-accessdynamic-vlan

使用此命令为经过身份验证的端口启用动态 VLAN 分配。使用 no 形式禁用动态 VLAN 分配。

语法

[no] network-access dynamic-vlan

缺省配置

启用

命令模式

接口配置

命令用法

◆启用后，RADIUS 服务器返回的 VLAN 标识符将通过 802.1X 身份验证过程应用于该端口，前提是已在交换机上创建了 VLAN。GVRP 不用于创建 VLAN。

◆ 为端口实现第一个经过身份验证的 MAC 地址规范的 VLAN 设置。 该端口上的其他经过身份验证的 MAC 地址必须具有相同的 VLAN 配置，否则它们将被视为身份验证失败。

◆ 如果在端口上启用了动态 VLAN 分配，并且 RADIUS 服务器未返回 VLAN 配置，则仍会认为身份验证成功，并且主机已分配给默认的未标记 VLAN。

◆ 在端口上更改动态 VLAN 分配状态时，将从安全 MAC 地址清所有认证地址 。

范例

以下示例在端口 1 上启用动态 VLAN 分配。

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access dynamic-vlan
Console(config-if)#
```

8.2.6 network-accessguest-vlan

当拒绝 802.1x 身份验证时，使用此命令将端口上的所有流量分配给访客 VLAN。 使用此命令的 no 形式禁用 guest VLAN 分配。

语法

network-access guest-vlan *vlan-id*

no network-access guest-vlan

vlan-id - VLAN ID (Range: 1-4093)

缺省配置

禁用

命令模式

接口配置

命令用法

◆必须定义要用作访客 VLAN 的 VLAN 并将其设置为活跃（请参阅 vlan database 命令）。

◆ 与 802.1X 身份验证一起使用时，必须设置入侵操作以使“guest-vlan”生效（请参阅 dot1x intrusion-action 命令）。

范例

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access guest-vlan 25
Console(config-if)#
```

8.2.7 network-access link-detection

使用此命令启用所选端口的链路检测。使用此命令的 no 形式恢复默认值。

语法

[no] network-access link-detection

缺省配置

禁用

命令模式

接口配置

范例

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access link-detection
Console(config-if)#
```

8.2.8 network-accesslink-detection link-down

使用此命令检测链接断开事件。检测到后交换机可以关闭端口，发送 SNMP 陷阱或两者。使用此命令的 no 形式禁用此功能。

语法

network-access link-detection link-downaction [shutdown | trap | trap-and-shutdown]

no network-access link-detection

action - 违反端口安全性时的响应。

shutdown - 仅禁用端口。

trap - 仅发出 SNMP 陷阱消息。

trap-and-shutdown - 发出 SNMP 陷阱消息并禁用端口。

缺省配置

禁用

命令模式

接口配置

范例

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access link-detection link-down action trap
Console(config-if)#
```

8.2.9 network-accesslink-detection link-up

使用此命令检测链接事件。 检测到时交换机可以关闭端口，发送 SNMP 陷阱或两者。使用此命令的 no 形式禁用此功能。

语法

network-access link-detection link-upaction [shutdown | trap | trap-and-shutdown]

no network-access link-detection

action - 违反端口安全性时的响应。

shutdown - 仅禁用端口。

trap - 仅发出 SNMP 陷阱消息。

trap-and-shutdown - 发出 SNMP 陷阱消息并禁用端口。

缺省配置

禁用

命令模式

接口配置

```
Console(config)#interface ethernet 1/1

Console(config-if)#network-access link-detection link-up action trap

Console(config-if)#
```

8.2.10 network-accesslink-detection link-up-down

使用此命令可以检测链接和链接断开事件。 检测到 eitherevent 时，交换机可以关闭端口，发送 SNMP 陷阱或两者。 使用此命令的 no 形式禁用此功能。

语法

network-access link-detection link-up-downaction [shutdown | trap | trap-and-shutdown]

no network-access link-detection

action - 违反端口安全性时的响应。

shutdown - 仅禁用端口。

trap - 仅发出 SNMP 陷阱消息。

trap-and-shutdown - 发出 SNMP 陷阱消息并禁用端口。

缺省配置

禁用

命令模式

接口配置

范例

```
Console(config)#interface ethernet 1/1

Console(config-if)#network-access link-detection link-up-down action trap

Console(config-if)#
```

8.2.11 network-access max-mac-count

使用此命令设置可通过所有形式的身份验证在端口接口上进行身份验证的最大 MAC 地址数。 使

用此命令的 no 形式恢复默认值。

语法

network-access max-mac-count *count*

no network-access max-mac-count

count -允许的最大认证 IEEE 802.1X 和 MAC 地址数。（范围：0-2048；0 表示无限制）

缺省配置

1024

命令模式

接口配置

命令用法

每个端口的最大 MAC 地址数为 1024，并且交换机系统支持的最大安全 MAC 地址数为 1024.达到限制时，所有新 MAC 地址都将作为身份验证失败进行处理。

范例

```
Console(config-if)#network-access max-mac-count 5

Console(config-if)#
```

8.2.12 network-accessmode mac-authentication

使用此命令在端口上启用网络访问身份验证。使用此命令的 no 形式禁用网络访问身份验证。

语法

[no] **network-access mode mac-authentication**

缺省配置

禁用

命令模式

接口配置

命令用法

◆在端口上启用时，身份验证过程会向已配置的 RADIUS 服务器发送 PAP 请求。用户名和密码都等于正在验证的 MAC 地址。

◆在 RADIUS 服务器上，必须以 MAC 地址格式 XX-XX-XX-XX-XX-XX（全部为大写）配置 PAP 用户名和密码。

◆经过身份验证的 MAC 地址作为动态条目存储在交换机安全 MAC 地址表中，并在老化时间过后删除。交换机系统支持的最大安全 MAC 地址数为 1024。

◆配置的静态 MAC 地址在交换机端口上显示时会添加到安全地址表中。静态地址被视为未经身份验证，而不向 RADIUS 服务器发送请求。

◆不能在同一端口上配置 MAC 认证，802.1X 和端口安全。只能应用一种安全机制。

◆无法在 Trunk 端口上配置 MAC 认证。

◆当端口状态变为 down 时，将从安全 MAC 地址表中清除所有 MAC 地址。静态 VLAN 分配未恢复。

◆RADIUS 服务器可以选择返回 VLAN 标识符列表。VLAN 标识符列表在“Tunnel-Private-Group-ID”属性中携带。VLAN 列表可以包含多个 VLAN 标识符，格式为“1u，2t”，其中“u”表示未标记的 VLAN 和“t”标记的 VLAN。 “Tunnel - Type”属性应设置为“VLAN”，“Tunnel-Medium-Type”属性设置为“802”。

范例

```
Console(config-if)#network-access mode mac-authentication

Console(config-if)#
```

8.2.13 network-access port-mac-filter

使用此命令启用指定的 MAC 地址过滤器。使用此命令的 no 形式禁用指定的 MAC 地址过滤器。

语法

network-access port-mac-filter *filter-id*

no network-access port-mac-filter

filter-id - Specifies a MAC address filter table. (Range: 1-64)

缺省配置

无

命令模式

接口配置

命令模式

◆可以使用 network-access mac-filter 命令配置 MAC 地址过滤表中的条目 。

◆只能为端口分配一个过滤器表。

范例

```
Console(config)#interface ethernet 1/1

Console(config-if)#network-access port-mac-filter 1

Console(config-if)#
```

8.2.14 mac-authentication intrusion-action

使用此命令配置对主机 MAC 身份验证失败的端口响应。 使用此命令的 no 形式来恢复默认值。

语法

mac-authentication intrusion-action {**block traffic** | **pass traffic**}

no mac-authentication intrusion-action

缺省配置

阻止流量

命令模式

接口配置

范例

```
Console(config-if)#mac-authentication intrusion-action block-traffic

Console(config-if)#
```

8.2.15 mac-authentication max-mac-count

使用此命令设置可通过 MAC 身份验证在端口上进行身份验证的最大 MAC 地址数。 使用此命令的 no 形式恢复默认值。

语法

mac-authentication max-mac-count *count*

no mac-authentication max-mac-count

count -允许的 MAC 认证 MACaddresses 的最大数量。（范围：1-1024）

缺省配置

1024

命令模式

接口配置

范例

```
Console(config-if)#mac-authentication max-mac-count 32

Console(config-if)#
```

8.2.16 clear network-access

使用此命令清除安全 MAC 地址表中的条目。

语法

clear network-access mac-address-table [**static** | **dynamic**][**address** *mac-address*] [**interface** *interface*]

static -指定静态地址条目。

dynamic -指定动态地址条目。

mac-address -指定 MAC 地址条目。 （格式：xx-xx-xxxx-xx-xx）

interface -指定端口接口。

ethernet *unit/port*

unit -单位标识符。 （范围：1）

port -端口号。 （范围：1-28）

缺省配置

无

命令模式

特权模式

范例

```
Console#clear network-access mac-address-table interface ethernet 1/1
Console#
```

8.2.17 show network-access

使用此命令可显示端口接口的 MAC 身份验证设置。

语法

show network-access [**interface** *interface*]

interface - Specifies a port interface.

ethernet *unit/port*

unit -单位标识符。 （范围：1）

port -端口号。 （范围：1-28）

缺省配置

显示所有接口的设置。

命令模式

特权模式

范例

```
Console#show network-access interface ethernet 1/1

Global secure port information

Reauthentication Time : 1800

MAC Address Aging : Disabled

Port : 1/1

MAC Authentication : Disabled

MAC Authentication Intrusion Action : Block traffic

MAC Authentication Maximum MAC Counts : 1024

Maximum MAC Counts : 1024

Dynamic VLAN Assignment : Enabled

Dynamic QoS Assignment : Disabled

MAC Filter ID : Disabled

Guest VLAN : Disabled

Link Detection : Disabled

Detection Mode : Link-down

Detection Action : Trap

Console#
```

8.2.18 show network-access mac-address-table

使用此命令可显示安全 MAC 地址表条目。

语法

show network-access mac-address-table [**static** | **dynamic**][**address** *mac-address* [*mask*]]

[**interface** *interface*][**sort** {**address** | **interface**}]

static -指定静态地址条目。

dynamic -指定动态地址条目。

mac-address -指定 MAC 地址条目。（格式：xx-xx-xx-xx-xx-xx）

mask -指定用于过滤 displayaddresses 的 MAC 地址位掩码。

interface -指定端口接口。

ethernet *unit/port*

unit -单位标识符。 （范围：1）

port -端口号。 （范围：1-28）

sort -按 MAC 地址或接口对显示的条目进行排序。

缺省配置

显示所有过滤器

命令模式

特权模式

命令用法

使用位掩码过滤显示的 MAC 地址时，1 表示“小心”，0 表示“不关心”。 例如，MAC 为 00-00-01-02-03-04 和掩码 FF-FF-FF-00-00-00 将导致所有 MAC 在 00-00-01- 00-00-00 到 00 范围内 -00-01-FF-FF-FF 显示。 所有其他 MAC 都将被过滤掉。

范例

```
Console#show network-access mac-address-table

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

Port MAC-Address RADIUS-Server Attribute Time

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

1/1 00-00-01-02-03-04 172.155.120.17 Static 00d06h32m50s

1/1 00-00-01-02-03-05 172.155.120.17 Dynamic 00d06h33m20s

1/1 00-00-01-02-03-06 172.155.120.17 Static 00d06h35m10s

1/3 00-00-01-02-03-07 172.155.120.17 Dynamic 00d06h34m20s

Console#
```

8.2.19 show network-access mac-filter

使用此命令显示 MAC 过滤表中条目的信息。

语法

show network-access mac-filter [*filter-id*]

filter-id -指定 MAC 地址过滤表。 （范围：1-64）

缺省配置

显示所有过滤器

命令模式

特权模式

范例

```
Console#show network-access mac-filter

Filter ID MAC Address MAC Mask

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

1 00-00-01-02-03-08 FF-FF-FF-FF-FF-FF

Console#
```

8.3 WEB 认证

Web 身份验证允许站点在 802.1X 或网络访问身份验证不可行或不切实际的情况下对网络进行身份验证和访问。 Web 身份验证功能允许未经身份验证的主机部门请求和接收 DHCP 分配的 IP 地址并执行 DNS 查询。除 HTTP 协议流量外，所有其他流量都被阻止。换精计划截取 HTTP 协议流量，并将其重定向到一个开关-生成的网页，其经由 RADIUS 便于用户名和的密码认证。 验证成功后，Web 浏览器将转发到最初请求的网页。 成功认证后对连接到该端口的所有主机都有效。

注： 必须激活并配置 RADIUS 身份验证才能使 Web 身份验证功能正常工作。

注意： 无法在中继端口上配置 Web 身份验证。

8.3.1 web-auth login-attempts

此命令定义失败的 Web 身份验证 loginattempts 的限制。达到限制后，交换机拒绝进一步登录尝试，直到安静时间到期。使用 no 形式恢复默认值。

语法

web-auth login-attempts *count*

no web-auth login-attempts

count -允许的失败登录尝试次数限制。 （范围：1-3）

缺省配置

3 次登录尝试

命令模式

全局配置

范例

```
Console(config)#web-auth login-attempts 2

Console(config)#
```

8.3.2 web-auth quiet-period

此命令定义主机在超过登录尝试失败限制之后必须等待的时间，然后才能再次尝试进行 Web 身份验证。使用 no 形式恢复默认值。

语法

web-auth quiet-period *time*

no web-auth quiet period

time -主机在再次尝试身份验证之前必须等待的时间。（范围：1-180 秒）

缺省配置

60 秒

命令模式

全局配置

范例

```
Console(config)#web-auth quiet-period 120

Console(config)#
```

8.3.3 web-auth session-timeout

此命令定义 Web 身份验证会话保持有效的时间量。达到会话超时后，主机将被注销，并且必须在下次数据传输到位时重新进行身份验证。使用 no 形式恢复默认值。

语法

web-auth session-timeout *timeout*

no web-auth session timeout

timeout -经过身份验证的会话保持有效的时间量。（范围：300-3600 秒）

缺省配置

3600 秒

命令模式

全局配置

范例

```
Console(config)#web-auth session-timeout 1800

Console(config)#
```

8.3.4 web-auth system-auth-control

此命令全局启用交换机的 Web 身份验证。使用 no 形式恢复默认值。

语法

[no] **web-auth system-auth-control**

缺省配置

禁用

命令模式

全局配置

命令用法

这两个**网络身份验证系统认证- 控制**开关和网络身份验证的接口必须为 Web 认证功能被启用活跃。

范例

```
Console(config)#web-auth system-auth-control

Console(config)#
```

8.3.5 web-auth

此命令启用接口的 Web 身份验证。使用 no 形式恢复默认值。

语法

[no] **web-auth**

缺省配置

禁用

命令模式

接口配置

命令用法

这两个网络身份验证系统认证- 控制开关和**网络身份验证**的端口必须为 Web 认证功能被启用活跃。

范例

```
Console(config-if)#web-auth
Console(config-if)#
```

8.3.6 web-authre-authenticate(Port)

此命令结束连接到端口的所有 Web 身份验证会话，并强制用户重新进行身份验证。

语法

web-auth re-authenticate interface *interface*

interface -指定端口接口。

ethernet *unit/port*

unit -单位标识符。 （范围：1）

port -端口号。 （范围：1-28）

缺省配置

无

命令模式

特权模式

范例

```
Console#web-auth re-authenticate interface ethernet 1/2
Console#
```

8.3.7 web-authre-authenticate (IP)

此命令结束与指定 IP 地址关联的 Web 身份验证会话，并强制用户重新进行身份验证。

语法

web-auth re-authenticate interface *interface ip*

interface -指定端口接口。

ethernet *unit/port*

unit -单位标识符。 （范围：1）

port -端口号。 （范围：1-28）

ip - IPv4 格式的 IP 地址

缺省配置

无

命令模式

特权模式

范例

```
Console#web-auth re-authenticate interface ethernet 1/2 192.168.1.5
Console#
```

8.3.8 show web-auth

此命令显示全局 Web 身份验证参数。

命令模式

特权模式

范例

```
Console#show web-auth
Global Web-Auth Parameters
System Auth Control : enabled
Session Timeout : 3600
Quiet Period : 60
Max Login Attempts : 3
Console#
```

8.3.9 show web-auth interface

此命令显示特定于接口的 Web 身份验证参数和统计信息。

语法

show web-auth interface *interface*

interface -指定端口接口。

ethernet *unit/port*

unit -单位标识符。 （范围：1）

port -端口号。 （范围：1-28）

命令模式

特权模式

范例

```
Console#show web-auth interface ethernet 1/2

Web Auth Status : Enabled

Host Summary

IP address Web-Auth-State Remaining-Session-Time

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

1.1.1.1 Authenticated 295

1.1.1.2 Authenticated 111

Console#
```

8.3.10 show web-auth summary

此命令显示 Web 身份验证端口参数和统计信息的摘要。

命令模式

特权模式

范例

```
Console#show web-auth summary

Global Web-Auth Parameters

System Auth Control : Enabled

Port Status Authenticated Host Count
```

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

1/ 1 Disabled 0

1/ 2 Enabled 8

1/ 3 Disabled 0

1/ 4 Disabled 0

1/ 5 Disabled 0

..

8.4 DHCPv4 侦听

DHCPv4 Snooping 允许交换机保护网络免受恶意 DHCPv4 服务器或其他将端口相关信息发送到 DHCPv4 服务器的设备的影响。 此信息可用于跟踪返回物理端口的 IP 地址。本节介绍用于配置 DHCPv4snooping 的命令。

8.4.1 ip dhcp snooping

该命令用来全局使能 DHCP Snooping 功能。使用 no 形式恢复默认设置。

语法

[no] ip dhcp snooping

缺省配置

禁用

命令模式

全局模式

命令用法

◆ 当恶意的 DHCP 消息从外部来源获得时，网络流量可能被中断。DHCP 侦听用于过滤从网络或防火墙之外的不安全接口上接收的 DHCP 消息。当 DHCP 窥探通过该命令全局启用，并且通过 IP DHCP 窥探 VLAN 命令在 VLAN 接口上启用时，将从 DHCP 窥探表中列出的设备上不接收的不可信接口（As）上接收的 DHCP 消息从 DHCP 窥探表中列出的设备中删除。

◆ 当启用时，基于通过 DHCP 窥探学习的动态条目，过滤进入不可信接口的 DHCP 消息。

◆ 表条目仅为可信接口学习。每个入口包括 MAC 地址、IP 地址、租约时间、VLAN 标识符和端口标识符。

◆ 当启用 DHCP 侦听时，交换机可以处理的 DHCP 消息数量的速率限制是每秒 100 个分组。超过此限制的任何 DHCP 包都会被丢弃。

◆ 过滤规则如下实现：

■ 如果全局 DHCP 侦听被禁用，则转发所有 DHCP 数据包。

■ 如果 DHCP 侦听是全局启用的，并且在接收 DHCP 分组的 VLAN 上也启用了，则所有 DHCP 分组

都被转发给可信端口。如果接收到的分组是 DHCP ACK 消息，则也将增强的 DHCP 窥探条目添加到绑定表中。

■ 如果 DHCP 侦听是全局启用的，并且在接收 DHCP 分组的 VLAN 上也启用，但是端口不可信，则其处理如下：

※ 如果 DHCP 分组是来自 DHCP 服务器（包括提供、ACK 或 NACK 消息）的应答分组，则丢弃该分组。

※ 如果 DHCP 数据包来自客户端，例如 DECLINE 或 RELEASE 消息，则只有在绑定表中找到相应的条目时，交换机才转发数据包。

※ 如果 DHCP 数据包来自客户端，例如 DISCOVER、REQUEST、INFORM、DECLINE 或 RELEASE 消息，则如果禁用 MAC 地址验证（如 ip dhcp 侦听验证 mac-address 命令所指定的），则转发数据包。但是，如果启用了 MAC 地址验证，则只有在存储在 DHCP 包中的客户端硬件地址与以太网报头中的源 MAC 地址相同的情况下，才转发包集。

※ 如果 DHCP 包不是可识别类型，则丢弃它。

■ 如果来自客户端的 DHCP 包通过上面的过滤标准，它将只转发到同一个 VLAN 中的可信端口。

■ 如果一个 DHCP 数据包是从服务器上收到的，那么它将被转发到同一 VLAN 中的可信端口和不可信端口。

◆ 如果 DHCP 侦听被全局禁用，则所有绑定绑定都将从绑定表中删除。

◆ *当交换机本身是 DHCP 客户机时需要考虑的其他事项——交换机向 DHCPserver 提交客户机请求的端口必须配置为可信的（使用 ip dhcp 侦听信任命令）。注意，当交换机从 DHCPserver 接收到 ACK 消息时，它不会在绑定表中为其自身添加动态条目。此外，当交换机为自己发送 DHCP 客户端分组时，不发生过滤。然而，当交换机从 DHCP 服务器接收到任何消息时，从 UntrutrudDe 端口接收的任何数据包都会被丢弃。*

范例

此示例为交换机全局启用 DHCP 侦听。

```
Console(config)#ip dhcp snooping
Console(config)#
```

8.4.2 ip dhcp snooping information option

该命令用于为交换机使用 DHCP Option 82 信息，并指定交换机生成 Option 82 信息时用于 remote-id 的帧格式。 使用没有任何关键字的 no 形式来禁用此函数，使用没有子类型编码的

关键字的 **no** 形式可以 CID/RID 域中使用子类型和子长度，或者使用带有 **remote-id** 关键字的 **no** 形式来设置远程 ID 用于以十六进制编码的交换机 MAC 地址。

语法

ip dhcp snooping information option[**encode no-subtype**][**remote-id** {**ip-address** [**encode** {**ascii** | **hex**}] |**mac-address** [**encode** {**ascii** | **hex**}] |

string *string*}]

no ip dhcp snooping information option [**encode no-subtype**][**remote-id** [**ip-address encode**] | [**mac-address encode**]]

encode no-subtype - Disables use of sub-type and sub-lengthfields in circuit-ID (CID) and remote-ID (RID) in Option 82information.

mac-address - Inserts a MAC address in the remote ID sub-optionfor the DHCP snooping agent (that is, the MAC address of theswitch’s CPU).

ip-address - Inserts an IP address in the remote ID sub-option forthe DHCP snooping agent (that is, the IP address of themanagement interface).

encode - Indicates encoding in ASCII or hexadecimal.

string - An arbitrary string inserted into the remote identifier field.(范围: 1-32 characters)

缺省配置

Option 82: 禁用

CID/RID sub-type: 启用

Remote ID: MAC 地址(十六进制)

命令模式

全局配置

命令用法

◆DHCP 提供了一种中继机制，用于将有关交换机及其 DHCP 客户端的信息发送到 DHCP 服务器。它被称为 DHCP Option82，它允许兼容的 DHCP 服务器在分配 IP 地址时使用该信息，或为客户端设置其他服务或策略。

◆当启用 DHCP 侦听信息选项 82 时，可以在交换机转发的 DHCP 请求数据包和从 DHCP 服务器发回的应答数据包中识别请求客户端（或使用信息字段描述自身的中间中继代理） 。

◆启用 DHCP 侦听信息选项后，客户端可以通过它们所连接的交换机端口进行识别，而不是仅仅调整其 MAC 地址。然后，DHCP 客户端-服务器交换消息直接在服务器和客户端之间转发，而不必将它们共享到整个 VLAN。

◆必须启用 DHCP Snooping 才能将 DHCP Option 82 信息插入到数据包中。启用后，交换机将仅在传入的 DCHP 数据包中添加/删除选项 82 信息，但不会传输它们。数据包按如下方式处理：

■如果传入数据包是带有选项 82 信息的 DHCP 请求数据包，它将根据 ip dhcp snooping information policy 命令指定的设置修改选项 82 信息 。

■如果传入数据包是没有选项 82 信息的 DHCP 请求数据包，则为数据包启用 DHCP 侦听信息选项将添加选项 82 信息。

■如果传入数据包是带有选项 82 信息的 DHCP 应答数据包，则启用 DHCP 侦听信息选项将从数据包中删除选项 82 信息。

◆DHCP Snooping Information Option 82 和 DHCP Relay InformationOption 82 不能同时启用。

范例

此示例启用 DHCP S nooping 信息选项。

```
Console(config)#ip dhcp snooping information option
Console(config)#
```

8.4.3 ip dhcp snooping information policy

此命令为包含 Option 82 信息的 DHCP 客户端数据包设置 DHCP 侦听信息选项策略。

语法

ip dhcp snooping information policy {**drop** | **keep** | **replace**}

drop -丢弃客户端的请求数据包而不是中继它。

keep -保留客户端请求中的 Option82 信息，并将报文转发给可信端口。

replace -使用有关连接代理本身的信息替换客户端请求中的 Option 82 信息 circuit-id 和 remote-id 字段，插入中继代理的地址（启用 DHCPsnooping 时），并将数据包转发到可信端口。

缺省配置

代替

命令模式

全局配置

命令用法

当交换机从已包含 DHCP Option 82 信息的客户端收到 DHCP 数据包时，可以配置交换机为这些数据包设置应用策略。交换机可以丢弃 DHCP 数据包，保留现有信息或者用交换机的中继信息替换它。

范例

```
Console(config)#ip dhcp snooping information policy drop

Console(config)#
```

8.4.4 ip dhcp snooping verify mac-address

此命令根据以太网报头中的源 MAC 地址验证存储在 DHCP 数据包中的客户端硬件地址。 使用 no 形式禁用此功能。

语法

[no] **ip dhcp binding verify mac-address**

缺省配置

启用

命令模式

全局配置

命令用法

如果启用了 MAC 地址验证，并且数据包的以太网报头中的源 MAC 地址与 DHCP 数据包中客户端的硬件地址不同，则丢弃该数据包。

范例

此示例启用 MAC 地址验证。

```
Console(config)#ip dhcp snooping verify mac-address

Console(config)#
```

8.4.5 ip dhcp snooping vlan

该命令用来在指定 VLAN 上进行 DHCP Snooping 功能。使用 no 形式恢复默认设置。

语法

[no] **ip dhcp snooping vlan** *vlan-id*

vlan-id - ID of a configured VLAN (范围: 1-4093)

缺省配置

禁用

命令模式

全局配置

命令用法

◆使用 ip dhcp snooping 命令全局启用 DHCP Snooping，并使用此命令在 VLAN 上启用时，将在 ip dhcp snooping trust 命令指定的 VLAN 中的任何不受信任的端口上执行 DHCP 数据包过滤。

◆全局禁用 DHCP Snooping 时，仍然可以为特定 VLAN 配置 DHCP Snooping，但更改不会生效，直到全局重新启用 DHCP Snooping。

◆当全局启用 DHCP 侦听，然后在 VLAN 上禁用时，将从绑定表中删除为此 VLAN 学习的所有动态绑定。

范例

此示例为 VLAN 1 启用 DHCP 侦听。

```
Console(config)#ip dhcp snooping vlan 1
Console(config)#
```

8.4.6 ip dhcp snooping information option circuit-id

此命令指定 DHCP Option 82 circuit-id 子选项信息。使用 no 形式使用默认设置。

语法

ip dhcp snooping information option circuit-id string *string*

no dhcp snooping information option circuit-id

string -插入电路标识符字段的任意字符串。(范围：1-32 个字符)

缺省配置

VLAN-Unit-Port

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

DHCP 提供了一种中继机制，用于将有关其 DHCP 客户端的交换机信息发送到 DHCP 服务器。DHCP Option 82 允许兼容的DHCP服务器在分配IP地址时使用该信息,为客户端设置其他服务或策略。有关此过程的更多信息，请参阅 ip dhcp snoopinginformation 选项命令下的“命令用法”部分 。

范例

此示例设置 DHCP 侦听信息 circuit-id 子选项串。

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip dhcp snooping information option circuit-id string mv2
Console(config-if)#
```

8.4.7 ip dhcp snooping trust

此命令将指定的接口配置为受信任。 使用 no 形式恢复默认设置。

语法

[no] ip dhcp snooping trust

缺省配置

非信任

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

◆可信任接口是配置为仅从网络内接收消息的接口。不受信任的接口是一个接口，配置为从网络或防火墙外部接收消息。

◆将连接到本地网络或防火墙内的 DHCP 服务器的所有端口设置为受信任，将本地网络外部的所有其他端口或防火墙设置为不受信任。

◆当 DHCP Snooping 功能使用 ip DHCP snooping 命令，并与 IP DHCP 一个 VLAN 启用 监听 vlan 命令，DHCP 包过滤将在 VLAN 内的任何 untrustedports 根据缺省状态进行，或作为 specificallyconfigured 为接口使用 no ip dhcp snooping trust 命令。

◆当不受信任的端口更改为受信任端口时，将删除与此端口关联的所有 dynamicDHCP snooping 绑定。

◆*交换机本身是 DHCP 客户端时的其他注意事项* - 通过其向 DHCP 服务器提交客户端请求的

端口必须配置为受信任。

范例

此示例将端口 5 设置为不可信。

```
Console(config)#interface ethernet 1/5

Console(config-if)#no ip dhcp snooping trust

Console(config-if)#
```

8.4.8 clear ip dhcp snooping binding

该命令用于清除 RAM 中的 DHCP Snooping 绑定表项。 使用此命令不带任何可选关键字来清除绑定表中的所有条目。

语法

clear ip dhcp snooping binding [*mac-address* **vlan** *vlan-id*]

mac-address -指定 MAC 地址条目。(格式：xx-xx-xx-xx-xx-xx)

vlan-id -配置的 VLAN ID（范围：1-4093）

命令模式

特权模式

范例

```
Console(config)#clear ip dhcp snooping binding 11-22-33-44-55-66 vlan 1

Console(config)#
```

8.4.9 clear ip dhcp snooping database flash

此命令从 flashmemory 中删除所有动态学习的监听条目。

命令模式

特权模式

范例

```
Console(config)#clear ip dhcp snooping database flash

Console(config)#
```

8.4.10 ip dhcp snooping database flash

此命令将所有动态学习的监听条目写入存储器。

命令模式

特权模式

命令用法

此命令可用于将当前学习的动态 DHCPsnooping 条目存储到闪存中。重置开关时，这些条目将恢复到指定表。但请注意，已从闪存恢复的动态条目的租约时间显示将不再有效。

范例

```
Console(config)#ip dhcp snooping database flash

Console(config)#
```

8.4.11 show ip dhcp snooping

此命令显示 DHCP 侦听配置设置。

命令模式

特权模式

范例

```
Console#show ip dhcp snooping

Global DHCP Snooping status: disabled

DHCP Snooping Information Option Status: disabled

DHCP Snooping Information Policy: replace

DHCP Snooping is configured on the following VLANs:

1

Verify Source Mac-Address: enable

Interface Trusted

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

Eth 1/1 No

Eth 1/2 No

Eth 1/3 No

Eth 1/4 No
```

```
Eth 1/5 Yes

...
```

8.4.12 show ip dhcp snooping binding

此命令显示 DHCP Snooping 绑定表条目。

命令模式

特权模式

范例

```
Console#show ip dhcp snooping binding

MAC Address IP Address Lease(sec) Type VLAN Interface

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

11-22-33-44-55-66 192.168.0.99 0 Dynamic-DHCPSNP 1 Eth 1/5

Console#
```

8.5 DHCPv6 侦听

DHCPv6 Snooping 允许交换机保护网络免受恶意 DHCPv6 服务器或其他将端口相关信息发送到 DHCPv6 服务器的设备的影响。此信息可用于跟踪返回物理端口的 IP 地址。本节介绍用于配置 DHCPv6snooping 的命令 。

8.5.1 ipv6 dhcp snooping

该命令用来全局使能 DHCPv6 Snooping。使用 no 形式恢复默认设置。

语法

[no] **ipv6 dhcp snooping**

缺省配置

禁用

命令模式

全局配置

命令用法

◆从外部源接收恶意 DHCPv6 消息时，可能会中断网络故障。DHCPv6 snooping 用于过滤从网络

或防火墙外部的不安全接口上接收的 DHCPCP6 消息。当该命令全局启用 DHCPv6 Snooping，并通过 ipv6 dhcp snoopingvlan 命令在 VLAN 接口上启用时，从 DHCPv6 侦听表中未列出的设备中指定的（由 no ipv6 dhcp snooping trust 命令指定）上收到的 DHCP 消息将被丢弃。

◆启用后进入不受信任接口的 DHCPv6 消息将根据通过 DHCPv6 监听获知的动态条目进行过滤。

◆仅为可信接口学习表条目。每个条目包括 MAC 地址，IPv6 地址，租用时间，绑定类型，VLAN 标识符和端口标识符。

◆启用 DHCPv6 Snooping 时，交换机可以处理的 DHCPCP6 消息数的速率限制为每秒 100 个数据包。 超过此限制的任何 DHCPv6 数据包都将被丢弃。

◆过滤规则实现如下：

■如果禁用全局 DHCPv6 侦听，则会转发所有 DHCPv6 数据包。

■如果全局启用了 DHCPv6 侦听，并且在接收到 DHCPv6 数据包的 VLAN 上也启用了■ DHCPv6 侦听，则会为*可信*端口转发 DHCPv6 数据包，如下所述。

■如果全局启用了 DHCPv6 侦听，并且在接收到 DHCP 数据包的 VLAN 上启用了 DHCPv6 侦听 ，但该端口*不受信任*，则根据消息类型处理 DHCP 数据包，如下所示：

DHCP 客户端数据包

※Request：更新绑定缓存中的条目，记录客户端的 DHCPCP6 唯一标识符（DUID），服务器的 DUID，Identity Association（IA）类型，IA 标识符和地址（4 个消息交换以获取 IPv6 地址），并转发到可信端口。

※Solicit：在绑定缓存中添加新条目，记录客户端的 DUID，IA 类型，IA ID（2 个消息交换以获取 IPv6 地址 withrapid commit 选项，否则 4 个消息交换），并转发到可信端口。

※Decline：如果在绑定缓存中找不到匹配的条目，则删除该数据包。

※Renew, Rebind, Release, Confirm：如果在绑定缓存中找不到匹配的条目，则丢弃该数据包。

※如果 DHCPv6 包 不是可识别的类型，则将其删除。

如果来自客户端的 DHCPv6 数据包通过上述过滤条件，则只会转发到同一 VLAN 中的信任端口。

DHCP 服务器数据包

※如果在*不受信任的*端口上收到 DHCP 服务器数据包，请删除该数据包并在系统中添加日志条目。

※如果从*受信任*端口上的服务器收到 DHCPv6 Reply 报文，将按以下方式处理：

A. 检查绑定表中是否找到 IA 选项中的 IPv6 地址：

■如果是，请继续执行 C。

■如果没有，继续 B。

B. 检查绑定缓存中是否找到 IA 选项中的 IPv6 地址：

■如果是，请继续执行 C。

■如果不是，请检查失败，并将数据包转发到受信任端口。

C. 检查 IA 选项中的状态代码：

■如果成功，并且条目在绑定表中，则 u pdate leasetime 并转发到原始目标。

■如果成功，并且条目在绑定缓存中，则将条目从绑定缓存移动到绑定表，更新租约时间并转发到原始目标。

■否则，删除绑定条目，并检查失败。

※ 如果收到 DHCPv6 中继报文，请检查 Relay-Forward 或 Relay-Reply 报文中的中继 messageoption，并按上述方法处理客户端和服务器报文。

◆如果全局禁用 DHCPv6 监听，则从绑定表中删除所有动态绑定 。

◆*当交换机本身是 DHCPv6 客户端时的其他注意事项* - 交换机通过其向 DHCPCPv6 服务器提交客户端请求的端口必须配置为受信任（使用 ipv6 dhcpsnooping trust 命令）。 请注意， 当从 DHCPv6 服务器收到 ACK 消息时，交换机不会向绑定表添加动态条件。此外，当交换机发出 DHCPv6 客户端时数据包本身，不会发生过滤。 但是，当交换机接收来自 DHCPv6 服务器的任何消息时，从不可信端口接收的任何数据包都将被丢弃。

范例

此示例为交换机全局启用 DHCPv6 侦听。

```
Console(config)#ipv6 dhcp snooping

Console(config)#
```

8.5.2 ipv6 dhcp snooping vlan

该命令在指定 VLAN 上使能 DHCPv6 Snooping 功能。 使用 no 形式恢复默认设置。

语法

[no] **ipv6 dhcp snooping vlan** {*vlan-id* | *vlan-范围*}

vlan-id -配置的 VLAN ID（范围：1-4093）

vlan-范围 -使用 ahyphen 指示的连续 VLAN 范围，或随机的 VLAN 组，每个条目用逗号分隔。

缺省配置

禁用

命令模式

全局配置

命令用法

◆使用 ipv6 dhcp snooping 命令全局启用 DHCPv6 Snooping，并使用此命令在 VLAN 上启用时，将在 ipv6 dhcp snooping trust 命令指定的 VLAN 内的任何不可信端口上执行 DHCPv6 数据包过滤。

◆当 DHCPv6 功能在全局禁用，DHCPv6 Snooping 功能仍然可以配置为特定 VLAN，但变化不会生效到的 DHCPv6 功能在全局重新启用。

◆当全局启用 DHCPv6 侦听，然后一个 VLAN 上禁用时，将从绑定表中删除为此 VLAN 学习的动态绑定。

范例

此示例为 VLAN 1 启用 DHCP6 侦听。

```
Console(config)#ipv6 dhcp snooping vlan 1
Console(config)#
```

8.5.3 ipv6 dhcp snooping max-binding

此命令设置可以在接口的绑定数据库中存储的最大条目数。使用 no 形式恢复默认设置。

语法

ipv6 dhcp snooping max-binding *count*

no ipv6 dhcp snooping max-binding

count - Maximum number of entries. (范围: 1-5)

缺省配置

无

命令模式

接口配置 (Ethernet, Port Channel)

范例

此示例将绑定条目的最大数量设置为 1。

```
Console(config)#interface ethernet 1/1
```

```
Console(config-if)#ipv6 dhcp snooping max-binding 1

Console(config-if)#
```

8.5.4 ipv6 dhcp snooping trust

此命令将指定的接口配置为受信任。使用 no 形式恢复默认设置。

语法

[no] **ipv6 dhcp snooping trust**

缺省配置

非信任

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

◆可信任接口是配置为仅从网络内接收消息的接口。不受信任的接口是一个接口，配置为从网络或防火墙外部接收消息。

◆将连接到本地网络或防火墙内的 DHCv6 服务器的所有端口设置为可信，并将本地网络或防火墙外的所有其他端口设置为不可信。

◆使用 ipv6 dhcpsnooping 命令 全局启用 DHCPv6 Snooping ，并 使用 ipv6 dhcp snoopingvlan 命令在 VLAN 上启用时 ，将根据默认状态在 VLAN 内的任何不可信端口上执行 DHCPv6 数据包过滤，或者为具有特定配置的接口配置 DHCPv6 数据包过滤。在 **no iPv6 dhcp snooping trust** 命令。

◆当未使用的端口更改为可信端口时，将删除与此端口关联的所有动态 DHCPv6 侦听绑定。

◆*交换机本身是 DHCPv6 客户端时的其他注意事项*-通过其向 DHCPv6 server 提交客户端请求的端口必须配置为受信任。

范例

此示例将端口 5 设置为不可信。

```
Console(config)#interface ethernet 1/5

Console(config-if)#no ipv6 dhcp snooping trust

Console(config-if)#
```

8.5.5 clear ipv6 dhcp snooping binding

此命令清除 RAM 中的 DHCPv6 监听绑定表条目。使用此命令时不带任何可选关键字，以清除绑定表中的所有条目。

语法

clear ipv6 dhcp snooping binding [*mac-address ipv6-address*]

mac-address -指定 MAC 地址条目。（格式：xx-xx-xx-xx-xx-xx）

ipv6-address -相应的 IPv6 地址。这个地址必须按照 RFC 2373“IPv6 地址结构”输入，使用 8 冒号分隔的 16 位十六进制值。可以在地址中使用一个双冒号来指示填充未定义字段所需的适当数目的零值。

命令模式

特权模式

范例

```
Console(config)#clear ipv6 dhcp snooping binding 00-12-cf-01-02-03 2001::1
Console(config)#
```

8.5.6 clear ipv6 dhcp snooping database flash

此命令从存储器中删除所有动态学习的监听条目。

命令模式

特权模式

范例

```
Console(config)#clear ipv6 dhcp snooping database flash
Console(config)#
```

8.5.7 show ipv6 dhcp snooping

此命令显示 DHCPv6 监听配置设置。

命令模式

特权模式

范例

```
Console#show ipv6 dhcp snooping

Global DHCPv6 Snooping status: disabled

DHCPv6 Snooping is configured on the following VLANs:

1,

Interface Trusted Max-binding Current-binding

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

Eth 1/1 No 5 0

Eth 1/2 No 5 0

Eth 1/3 No 5 0

Eth 1/4 No 5 0

Eth 1/5 Yes 5 0

...
```

8.5.8 show ipv6 dhcp snooping binding

此命令显示 DHCPv6 监听绑定表条目。

命令模式

特权模式

范例

```
Console#show ipv6 dhcp snooping binding

NA - Non-temporary address

TA - Temporary address

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

Link-layer Address: 00-13-49-aa-39-26

IPv6 Address Lifetime VLAN Port Type

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

2001:b021:1435:5612:ab3c:6792:a452:6712 2591998 1 Eth 1/5 NA

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

Link-layer Address: 00-12-cf-01-02-03

IPv6 Address Lifetime VLAN Port Type
```

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

2001:b000::1 2591912 1 Eth 1/3 NA

Console#
```

8.5.9 show ipv6 dhcp snooping statistics

此命令显示 DHCPv6 Snooping 客户端，服务器和中继数据包的统计信息。

命令模式

特权模式

范例

```
Console#show ipv6 dhcp snooping statistics

DHCPv6 Snooping Statistics:

Client Packet: Solicit, Request, Confirm, Renew, Rebind,

Decline, Release, Information-request

Server Packet: Advertise, Reply, Reconfigure

Relay Packet: Relay-forward, Relay-reply

State Client Server Relay Total

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

Received 10 9 0 19

Sent 9 9 0 18

Droped 1 0 0 1

Console#
```

8.6 IP 源守护

IP Source Guard 是一种安全功能，可根据 IP Source Guard table 中手动配置的条目过滤网络接口上的 IP 流量，或者在启用时过滤 DHCP Snooping 表中的动态条目（请参阅“DHCPv4 Snooping”）。 IP 源防护可用于防止主机尝试使用邻居的 IP 地址访问网络时导致的流量攻击。本节介绍用于配置 IP Source Guard 的命令。

8.6.1 ip source-guard binding

此命令将静态地址添加到源保护绑定表。使用 no 形式删除静态条目。

语法

ip source-guard binding *mac-address* **vlan** *vlan-id ip-address***interface ethernet** *单元 / 端口*

no ip source-guard binding *mac-address* **vlan** *vlan-id*

mac-address -有效的单播 MAC 地址。

vlan-id -配置的 VLAN ID（范围：1-4093）

ip-address -有效的单播 IP 地址，包括有类型的类型 A，Bor C.

unit -单位标识符。（范围：1）

port -端口号。（范围：1-28）

缺省配置

无

命令模式

全局配置

命令用法

◆表条目包括 MAC 地址，IP 地址，租用时间，条目类型（Static-IP-SG-Binding，Dynamic-DHCP-Binding），VLAN 标识符和端口标识符。

◆所有静态条目都配置了无限租约时间，show ip source-guard 命令 使用值 zero 表示。

◆启用源防护后，将根据通过 DHCP 侦听获取的动态条目或使用此命令在源防护绑定表中配置的静态地址来过滤流量。

◆静态绑定按如下方式处理 ：

■如果没有具有相同 VLAN ID 和 MAC 地址的条目，则使用静态 IP Sourceguard 绑定的类型将新条目添加到绑定表。

■如果存在具有相同 VLAN ID 和 MAC 地址的条目，并且条目类型是静态 IP 源文件 绑定，则新条目将替换旧条目。

■如果存在具有相同 VLAN ID 和 MAC 地址的条目，并且条目的类型是动态 DHCP 侦听绑定，则新条目将替换旧条目，并且条目类型将更改为源 IP 防护绑定。

范例

此示例在端口 5 上配置静态源防护绑定。

```
Console(config)#ip source-guard binding 11-22-33-44-55-66 vlan 1 192.168.0.99
interface ethernet 1/5
Console(config-if)#
```

8.6.2 ip source-guard

此命令用于配置交换机根据源 IP 地址或源 IP 地址和相应的 MAC 地址过滤入站流量。使用 **no** 形式禁用此功能。

语法

ip source-guard {**sip** | **sip-mac**}

no ip source-guard

sip - Filters traffic based on IP addresses stored in the bindingtable.

sip-mac - Filters traffic based on IP addresses and correspondingMAC addresses stored in the binding table.

缺省配置

关闭

命令模式

接口配置 (Ethernet)

命令用法

◆源防护用于在不安全的端口上传输流量，该端口接收来自网络外部或防火墙的消息，因此可能受到主机试图使用邻居的 IP 地址引起的流量攻击。

◆将源保护模式设置为“sip”或“sip-mac” 在所选端口上 启用此功能。 使用“sip”选项检查绑定表中所有条目的 VLAN ID，sourceIP 地址和端口号。使用“sip-mac”选项检查这些相同的参数以及源 MAC 地址。使用 **no ip source guard** 命令禁用所选端口上的此功能。

◆启用后，将根据通过 DHCP 监听获得的动态条目或源保护绑定表中配置的静态地址过滤流量。

◆表条目包括 MAC 地址，IP 地址，租用时间，条目类型（Static-IP-SG-Binding，Dynamic-DHCP-Binding，VLAN 标识符和端口标识符）。

◆使用 ip source-guard binding 命令在源防护绑定表中输入的静态地址将自动配置为无限租约时间。通过 DHCP 窥探获知的动态条目由 DHCP 服务器本身配置。

◆如果启用了 IP 源防护，将根据绑定表检查入站数据包的 IP 地址（sipoption）或其 IP 地址和相应的 MAC 地址（sip-macoption）。如果未找到匹配的条目，则将丢弃该数据包。

◆过滤规则实现如下：

■如果禁用 DHCP 侦听，IP 源防护将检查 VLAN ID，源 IP 地址，端口号和 sourceMAC 地址（对于 sip-mac 选项）。 如果在绑定表中找到 匹配的条目，并且条目类型是静态 IP 源保护绑定，则将转发该分组。

■如果启用了 DHCP 侦听，IP 源防护将检查 VLAN ID，源 IP 地址，端口号和源 MAC 地址（对于 sip-mac 选项）。 如果在绑定表中找到匹配的条目，并且条目类型是静态 IP 源保护绑定或者动态的 DHCP snooping 绑定，则将转发该数据包。

■如果在尚未配置 IP 源绑定（通过 DHCP 侦听或手动配置动态学习）的接口上启用了 IP 源防护，则交换机将丢弃该端口上的所有 IP 流量，DHCP 数据包除外。

范例

此示例在端口 5 上启用 IP 源保护。

```
Console(config)#interface ethernet 1/5
Console(config-if)#ip source-guard sip
Console(config-if)#
```

8.6.3 ip source-guard max-binding

此命令设置可绑定到接口的最大条目数。使用 no 形式恢复默认设置。

语法

ip source-guard max-binding *number*

no ip source-guard max-binding

number - The maximum number of IP addresses that can bemapped to an interface in the binding table. (范围: 1-5)

缺省配置

无

命令模式

接口配置 (Ethernet)

命令用法

◆该命令用来设置绑定表中可以映射到接口的最大地址表项数，包括 DHCP Snooping 发现的动态条目和 ipsource-guard 命令设置的静态条目 。

范例

此示例将端口 5 的可绑定表中允许的最大条目数设置为一个条目。

```
Console(config)#interface ethernet 1/5

Console(config-if)#ip source-guard max-binding 1

Console(config-if)#
```

8.6.4 show ip source-guard

此命令显示是否在每个接口上启用或禁用源保护。

命令模式

特权模式

范例

```
Console#show ip source-guard

Interface Filter-type Max-binding

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

Eth 1/1 DISABLED 5

Eth 1/2 DISABLED 5

Eth 1/3 DISABLED 5

Eth 1/4 DISABLED 5

Eth 1/5 SIP 1

Eth 1/6 DISABLED 5

.
```

8.6.5 show ip source-guard binding

此命令显示源保护绑定表。

语法

show ip source-guard binding [dhcp-snooping | static]

dhcp-snooping -显示使用 DHCPSnooping 命令配置的动态条目 。

static -显示使用 ip source-guardbinding 命令配置的静态条目。

命令模式

特权模式

范例

```
Console#show ip source-guard binding

MacAddress IpAddress Lease(sec) Type VLAN Interface

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

11-22-33-44-55-66 192.168.0.99 0 Static 1 Eth 1/5

Console#
```

8.7 ARP 检查

ARP 检查验证 AddressResolution Protocol（ARP）数据包中的 MAC 到 IP 地址绑定。 它能防止 ARP 通信 withinvalid 地址绑定，形成基础的某些“人在这方面的 - 中间”的攻击。 这是通过拦截所有 ARP 请求和响应并在更新本地 ARP 缓存或将数据包转发到适当的目标之前验证每个数据包来实现的，从而丢弃任何无效的 ARP 数据包。

ARP 检测确定基于有效的 IP ARP 分组的有效性 - 和 MAC 地址存储在一个可信数据库地址绑定-的 DHCP snoopingbinding 数据库。 ARP 检测还可以针对具有静态配置的 IP 地址的主机，针对用户配置的 ARP 访问控制列表（ACL）验证 ARP 数据包。

本节介绍用于配置 ARP 检测的命令。

8.7.1 ip arp inspection

此命令在交换机上全局启用 ARP 检测。使用 no 形式禁用此功能。

语法

[no] ip arp inspection

缺省配置

关闭

命令模式

全局配置

命令用法

◆当使用此命令全局启用 ARP 检查时，它仅在那些通过 ip arp 检查 vlan 命令启用 ARP 检查的 VLAN 上变为活动。

◆当 ARP 检查被全局启用并在所选 VLAN 上启用时，这些 VLAN 上的所有 ARP 请求和应答包被重定向到 CPU，并且它们的切换由 ARP 检查引擎处理。

◆当 ARP 检查在全局禁用时，它对所有 VLAN 都无效，包括启用 ARP 检查的那些。

◆当 ARP 检查被禁用时，所有 ARP 请求和回复分组绕过 ARP 检查引擎，并且它们的切换方式与所有其他分组的切换方式匹配。

◆禁用和再启用全局 ARP 检查不会影响任何 VLAN 的 ARP 检查配置。

◆当 ARP 检查在全局禁用时，仍然可以为单个 VLAN 配置 ARP 检查。在 ARP 检查重新启用后，这些配置变化才会变得活跃。

范例

```
Console(config)#ip arp inspection

Console(config)#
```

8.7.2 ip arp inspection filter

此命令指定要应用于一个或多个 VLAN 的 ARP ACL。使用 **no** 形式删除 ACL 绑定。

语法

ip arp inspection filter *arp-acl-name* **vlan** {*vlan-id* | *vlan-范围*}[**static**]

arp-acl-name - ARP ACL 的名称。（最大长度：16 个字符）

vlan-id - （范围：1-4093）

vlan-范围 -使用连字符指示的连续 VLAN 范围，或随机的 VLAN 组，每个条目用逗号分隔。

static -只对指定的 ACL 验证 ARP 报文，不检查 DHCP Snooping 数据库中的地址绑定。

缺省配置

不绑定

静态模式未启用

命令模式

全局配置

命令用法

◆ARP ACL 配置命令。

◆如果启用静态模式，交换机会将 ARP 数据包与指定的 ARP ACL 进行比较。匹配在允许或拒绝规则中的 IP 到 MAC 地址绑定的分组被相应地处理。不匹配任何 ACL 规则的数据包将被删除。不检查 DHCPsnooping 数据库中的地址绑定。

◆如果未启用静态模式，则首先根据指定的 ARP ACL 验证数据包。匹配拒绝规则的数据包将被删除。所有剩余数据包都会再次通过 DHCP 侦听数据库中的地址绑定进行验证 。

范例

```
Console(config)#ip arp inspection filter sales vlan 1
Console(config)#
```

8.7.3 ip arp inspection log-buffer logs

此命令设置日志信息中保存的最大条目数以及这些消息的发送速率。使用 no 形式恢复默认设置。

语法

ip arp inspection log-buffer logs *message-number* **interval** *seconds*

no ip arp inspection log-buffer logs

message-number - logmessage 中保存的最大条目数。(范围：0-256，其中 0 表示不保存任何事件)

seconds -发送日志消息的时间间隔。(范围：0-86400)

缺省配置

条目数 5

间隔 1 秒

命令模式

全局配置

命令用法

◆ARP 检查必须通过 IP ARP 检查命令来启用，然后才能接受该命令。

◆ 默认情况下，ARP 检查的日志记录处于活动状态，无法禁用。

◆ 当交换机丢弃数据包时，它会在日志缓冲区中放置一个条目。每个条目都包含流信息，例如接收 VLAN，端口号，源和目标 IP 地址以及源和目标 MAC 地址。

◆ 如果在同一 VLAN 上连续接收到多个相同的无效 ARP 数据包，则日志记录工具只会在日志缓

冲区和一个相应的系统消息中生成一个条目。

◆ 日志缓冲区中可以存储的最大条目数由消息号参数决定。如果日志缓冲区在发送消息之前填满，则最旧的条目将被替换为最新的条目。

◆ 交换机在由*秒*值确定的速率控制的基础上生成系统消息。生成系统消息后，将从日志缓冲区中清除所有条目。

范例

```
Console(config)#ip arp inspection log-buffer logs 1 interval 10
Console(config)#
```

8.7.4 ip arp inspection validate

此命令指定一个 ARP 数据包中地址组件的附加验证。使用 no 形式恢复默认设置。

语法

ip arp inspection validate {**dst-mac** [**ip**] [**src-mac**] |**ip** [**src-mac**] | **src-mac**}

no ip arp inspection validate

dst-mac -根据 ARP 主体中的目标 MAC 地址检查以太网头中的目标 MAC 地址。 此检查是针对 ARP 响应执行的。启用后，具有不同 MAC 地址的数据包将被归类为无效并被丢弃。

ip -检查 ARP 正文中的无效和意外 IP 地址。地址包括 0.0.0.0,255.255.255.255 和所有 IP 多播地址。在所有 ARP 请求和响应中检查发件人 IP 地址，而仅在 ARP 响应中检查目标 IP 地址。

src-mac -检查以太网中的源 MAC 地址，然后检查 ARP 主体中的发送方 MAC 地址。 此检查在 ARP 请求和响应上执行。 启用后，具有不同 MAC 地址的数据包将被归类为无效并丢弃。

缺省配置

无

命令模式

全局配置

命令用法

缺省情况下，ARP Inspection 仅检查 ARP ACL 或 DHCP Snooping 数据库中指定的 IP-MAC 地址绑定。

范例

```
Console(config)#ip arp inspection validate dst-mac

Console(config)#
```

8.7.5 ip arp inspection vlan

此命令启用指定 VLAN 或范围的 VLAN 的 ARP 检测。使用 no 形式禁用此功能。

语法

[no] **ip arp inspection vlan** {*vlan-id* | *vlan-范围*}

vlan-id - VLAN ID。 （范围：1-4093）

vlan-范围 -使用连字符指示的连续 VLAN 范围，或随机的 VLAN 组，每个条目用逗号分隔。

缺省配置

禁用

命令模式

全局配置

命令用法

◆使用 ip arp inspection 命令全局启用 ARP 检测时，它仅在已使用此命令启用的 VLAN 上变为活动状态。

◆ 当全局启用 ARP 检测并在选择 VLAN 上启用时，这些 VLAN 上的所有 ARP 请求和回复请求都将被转发到 CPU，并且它们的切换由 ARPInspection 引擎处理。

◆ 全局禁用 ARP 检测时，对所有 VLAN（包括启用了 ARP 检查的 VLAN）将变为非活动状态。

◆ 当禁用 ARP 检测时，所有 ARP 请求和应答包都通过 ARP 检测引擎，并且它们的切换方式与所有其他数据包的方式匹配。

◆ 禁用然后重新启用全局 ARP 检查不会影响任何 VLAN 的 ARP 检查配置 。

◆ 全局禁用 ARP 检测时，仍可以为各个 VLAN 配置 ARP 检查。 在再次全局启用 ARP 检查后，这些配置更改将仅激活。

范例

```
Console(config)#ip arp inspection vlan 1,2

Console(config)#
```

8.7.6 ip arp inspection limit

此命令设置端口上接收的 ARP 数据包的速率限制。使用 no 形式恢复默认设置。

语法

ip arp inspection limit {**rate** *pps* | **none**}

no ip arp inspection limit

pps -*每秒* CPU 可处理的最大 ARP 数据包数。(范围：0-2048，其中 0 表示可以转发 no ARP 数据包)

none - CPU 可以处理的 ARP 数据包数量没有限制。

缺省配置

15

命令模式

接口配置 (Port, Static Aggregation)

命令用法

◆此命令适用于受信任和不受信任的端口。

◆ 当入局 ARP 报文的速率超过配置的限制时，交换机将丢弃超过限制的所有 ARP 报文。

范例

```
Console(config)#interface ethernet 1/1

Console(config-if)#ip arp inspection limit rate 150

Console(config-if)#
```

8.7.7 ip arp inspection trust

此命令将端口设置为受信任，因此免于 ARPInspection。使用 no 形式恢复默认设置。

语法

[no] **ip arp inspection trust**

缺省配置

非信任

命令模式

接口配置 (Port, Static Aggregation)

命令用法

到达不受信任端口的数据包需要进行任何已配置的 ARPInspection 和其他验证检查。到达受信端口的数据包会绕过所有这些检查，并根据正常切换规则进行转发。

范例

```
Console(config)#interface ethernet 1/1

Console(config-if)#ip arp inspection trust

Console(config-if)#
```

8.7.8 show ip arp inspection configuration

此命令显示 ARP inspection 的全局配置设置。

命令模式

特权模式

范例

```
Console#show ip arp inspection configuration

ARP inspection global information:

Global IP ARP Inspection status : disabled

Log Message Interval : 10 s

Log Message Number : 1

Need Additional Validation(s) : Yes

Additional Validation Type : Destination MAC address

Console#
```

8.7.9 show ip arp inspection interface

此命令显示端口的信任状态和 ARP 检查速率限制。

语法

show ip arp inspection interface [*interface*]

interface

ethernet *单元 / 端口*

unit -单位标识符。（范围：1）

port - 端口号。 （范围：1-28）

命令模式

特权模式

范例

```
Console#show ip arp inspection interface ethernet 1/1

Port Number Trust Status Rate Limit (pps)

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

Eth 1/1 Trusted 150

Console#
```

8.7.10 show ip arp inspection log

此命令显示有关存储在日志中的条目的信息，包括关联的 VLAN，端口和地址组件。

命令模式

特权模式

范例

```
Console#show ip arp inspection log

Total log entries number is 1

Num VLAN Port Src IP Address Dst IP Address Src MAC Address Dst MAC Address

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

1 1 11 192.168.2.2 192.168.2.1 00-04-E2-A0-E2-7C FF-FF-FF-FF-FF-FF

Console#
```

8.7.11 show ip arp inspection statistics

此命令显示有关由于各种原因处理或丢弃的 ARP 数据包的统计信息。

命令模式

特权模式

范例

```
Console#Console#show ip arp inspection statistics

ARP packets received before rate limit : 150

ARP packets dropped due to rate limt : 5
```

```
Total ARP packets processed by ARP Inspection : 150

ARP packets dropped by additional validation (source MAC address) : 0

ARP packets dropped by additional validation (destination MAC address): 0

ARP packets dropped by additional validation (IP address) : 0

ARP packets dropped by ARP ACLs : 0

ARP packets dropped by DHCP snooping : 0

Console#
```

8.7.12 show ip arp inspection vlan

此命令显示 VLAN 的配置设置，包括 ARP 检查的状态，ARP ACL 名称以及 ARP ACL 验证完成后是否使用 DHCP 侦听数据库。

语法

show ip arp inspection vlan [*vlan-id* | *vlan-范围*]

vlan-id - VLAN ID。 （范围：1-4093）

vlan-范围 -使用连字符指示的连续 VLAN 范围，或随机的 VLAN 组，每个条目用逗号分隔。

命令模式

特权模式

范例

```
Console#show ip arp inspection vlan 1

VLAN ID DAI Status ACL Name ACL Status

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

1 disabled sales static

Console#
```

8.8 DoS 保护

拒绝服务攻击（DoS 攻击）是阻止计算机或网络资源提供的服务的尝试。 这种攻击试图阻止 Internet 站点或服务高效运行或根本不运行。 通常，DoS 攻击是通过强制目标重置，消耗其大部分资源以使其无法再提供其预期服务，或者阻碍目标用户与目标之间的通信媒体来实现的，这样它们就不能长时间地进行通

信。
本节介绍用于防范 DoS 攻击的命令。

8.8.1 dos-protection echo-chargen

此命令可防止 DoS echo/chargen 攻击，其中每一个服务重复发送给它的任何内容，而字符发生器服务生成连续的数据流。当一起使用时，它们会创建一个无限循环并导致拒绝服务。使用 no 形式禁用此功能。

语法

dos-protection echo-chargen [**bit-rate-in-kilo** *rate*]

no dos-protection echo-chargen

rate - 允许的最大速率。（范围：64-2000 千位/秒）

缺省配置

禁用 ,1000 kbits/秒

命令模式

全局配置

范例

```
Console(config)#dos-protection echo-chargen 65
Console(config)#
```

8.8.2 dos-protection murf

此命令可防止 DoS smurf 攻击，其中犯罪者将大量欺骗性 ICMP 回应请求流量生成到广播目标 IP 地址(255.255.255.255)，所有这些都使用预期受害者的 aspoofed 源地址。受害者应该发送 ICMP Echo 响应数据包所需的许多中断。使用 no 形式禁用此功能。

语法

[no] **dos-protection smurf**

缺省配置

启用

命令模式

全局配置

范例

```
Console(config)#dos-protection smurf

Console(config)#
```

8.8.3 dos-protection tcp-flooding

此命令可防止 Doper TCP-flooding 攻击，其中一个破坏者将一连串 TCP SYN 请求（带或不带 aspoofed-Source IP）发送到目标，并且永远不会返回 ACK 数据包。这些半开放连接将绑定目标上的资源，并且不能建立新连接，从而导致拒绝服务。使用 no 形式禁用此功能。

语法

dos-protection tcp-flooding [**bit-rate-in-kilo** *rate*]

no dos-protection tcp-flooding

rate - 允许的最大速率。（范围：64-2000 千位/秒）

缺省配置

禁用，1000 kbits/秒

命令模式

全局配置

范例

```
Console(config)#dos-protection tcp-flooding 65

Console(config)#
```

8.8.4 dos-protection tcp-null-scan

此命令可防止 DoS TCP-null 扫描攻击，其中 TCPNULL 扫描消息用于标识侦听 TCP 端口。 扫描使用一系列奇怪配置的 TCP 数据包，其中包含序列号 0 和无标志。 如果目标的 TCP 端口关闭，则目标将使用 TCP RST(重置)数据包。 如果目标 TCP 端口打开，它只会丢弃 TCP NULL 扫描。 使用 no 形式禁用此功能。

语法

[no] **dos-protection tcp-null-scan**

缺省配置

启用

命令模式

全局配置

范例

```
Console(config)#dos-protection tcp-null-scan
Console(config)#
```

8.8.5 dos-protection tcp-syn-fin-scan

此命令可防止 DoS TCP-SYN/FIN 扫描攻击，其中 TCP SYN / FIN 扫描消息用于标识侦听 TCP 端口。扫描使用一系列奇怪配置的 TCP 数据包，其中包含 SYN（同步）和 FIN（完成）标志。如果目标的 TCP 端口关闭，则目标会回复 TCP RST（重置）数据包。如果目标 TCP 端口打开，它只会丢弃 TCP SYN/FIN 扫描。使用 no 形式禁用此功能。

语法

[no] dos-protection syn-fin-scan

缺省配置

启用

命令模式

全局配置

范例

```
Console(config)#dos-protection syn-fin-scan
Console(config)#
```

dos-protection tcp-xmas-scan

此命令可防止 DoS TCP-xmas 扫描，其中使用所谓的 TCP XMAS 扫描消息来识别侦听 TCP 端口。此扫描使用一系列奇怪配置的 TCP 数据包，其中包含序列号 0 和 URG，PSH 和 FIN 标志。如果目标的 TCP 端口已关闭，则目标将使用 TCP RST 数据包进行回复。如果目标 TCP 端口打开，它只是丢弃 TCP XMAS 扫描。使用 no 形式此功能。

语法

[no] dos-protection tcp-xmas-scan

缺省配置

启用

命令模式

全局配置

范例

```
Console(config)#dos-protection tcp-xmas-scan

Console(config)#
```

8.8.6 dos-protection udp-flooding

此命令可防止 Doper UDP 泛洪攻击，其中 aperpetrator 将大量 UDP 数据包（带或不带有 aspoofed-Source IP）发送到远程主机上的随机端口。 目标将确定应用程序正在该端口上侦听，并使用 ICMPDestination Unreachable 数据包进行回复。 它将被迫发送许多 ICMP 包，最终导致其他客户无法访问它。使用 no 形式禁用此功能。

语法

dos-protection udp-flooding [**bit-rate-in-kilo** *rate*]

no dos-protection udp-flooding

rate - Maximum allowed rate. (范围: 64-2000 kbits/second)

缺省配置

禁用, 1000 kbits/秒

命令模式

全局配置

范例

```
Console(config)#dos-protection udp-flooding 65

Console(config)#
```

8.8.7 dos-protection win-nuke

此命令可防止影响 Microsoft Windows 3.1x / 95 / NT 操作系统的 DoS WinNuke 攻击。 在这种类型的攻击中，犯罪者将包含 TCP URG 标志的 OOB 带外（OOB）数据包字符串发送到 TCP 端口 139（NetBIOS）上的目标计算机，将其封锁并显示“蓝屏”死亡。“这不会对计算机的硬盘造成

任何损害或更改数据，但任何未保存的数据都将丢失。 微软制作补丁以防止 WinNuke 攻击，但是 OOB 数据包仍然将服务置于紧密的循环中，从而消耗了所有可用的 CPU 时间。 使用 **no** 形式禁用此功能特征。

语法

dos-protection win-nuke [**bit-rate-in-kilo** *rate*]

no dos-protection udp-flooding

rate - 允许的最大速率。（范围：64-2000 千位/秒）

缺省配置

禁用，1000 kbits/秒

命令模式

全局配置

范例

```
Console(config)#dos-protection win-nuke 65

Console(config)#
```

8.8.8 show dos-protection

此命令显示 DoS 保护命令的配置设置。

命令模式

特权模式

范例

```
Console#show dos-protection

Global DoS Protection:

Echo-Chargen Attack : Disabled, 1000 kilobits per second

Smurf Attack : Enabled

TCP Flooding Attack : Disabled, 1000 kilobits per second

TCP Null Scan : Enabled

TCP SYN/FIN Scan : Enabled

TCP XMAS Scan : Enabled

UDP Flooding Attack : Disabled, 1000 kilobits per second
```

```
WinNuke Attack : Disabled, 1000 kilobits per second

Console#
```

9 访问控制列表

访问控制列表（ACL）为 IPv4 帧（基于地址，协议，第 4 层协议端口号或 TCP 控制代码），IPv6 帧（基于地址，DSCP 流量类或下一个头类型），orany 帧（基于）提供数据包过滤在 MAC 地址或以太网类型上）。要过滤数据包，首先要创建一个访问列表，添加所需的规则，然后将列表绑定到特定端口。本节介绍“访问控制列表”命令。

9.1 IPV4 ACLs

本节中的命令根据 IPv4 地址，TCP / UDP 端口号，协议类型和 TCP 控制代码配置 ACL。要配置 IPv4 ACL，请首先创建包含所需许可或拒绝规则的访问列表，然后将访问列表绑定到一个或多个端口。

9.1.1 access-list ip

此命令添加 IP 访问列表，并进入配置模式标准或扩展 IPv4 ACL。使用 no 形式删除指定的 ACL。

语法

[no] access-list ip {standard | extended} *acl-name*

standard - 指定根据源 IP 地址过滤数据包的 ACL。

extended - 指定根据源或目标 IP 地址以及其他更具体的条件过滤数据包的 ACL。

acl-name - ACL 的名称。（最大长度：32 个字符，nospace 或其他特殊字符）

缺省配置

无

命令模式

全局配置

命令用法

◆为现有 ACL 创建新 ACL 或进入配置模式时，请使用 **permit** 或 **deny** 命令将新规则添加到列表底部。

◆ 要删除规则，请使用 **no permit** 或 **no deny** 命令，后跟精确先前配置的规则的文本。

◆ ACL 最多可包含 64 条规则。

范例

```
Console(config)#access-list ip standard david
Console(config-std-acl)#
```

9.1.2 permit, deny(Standard)

此命令将规则添加到标准 IPv4 ACL。该规则为从指定源发出的数据包设置过滤条件。使用 no 形式删除规则。

语法

{**permit** | **deny**} {**any** | *source bitmask* / **host** *source*}[**time-range** *time-range-name*]

no {**permit** | **deny**} {**any** | *source bitmask* / **host** *source*}

any - 任何源 IP 地址。

source - 源 IP 地址。

bitmask - 表示地址位匹配的虚线十进制数。

host - 关键字后跟特定的 IP 地址。

time-range-name - *时间段的名称* 。（范围：1-30 个字符）

缺省配置

无

命令模式

标准 IPv4 ACL

命令用法

◆新规则将附加到列表末尾。

◆地址位掩码类似于子网掩码，包含从 0 到 255 的四个整数，每个整数由句点分隔。二进制掩码

使用 1 位表示“匹配”，0 位指示“忽略”。位掩码与指定的源 IP 地址进行按位 AND 运算，然后与进入此 ACL 的端口的每个 IP 数据包的地址进行比较。已被分配。

范例

此示例为特定地址 10.1.1.21 配置一个允许规则，为地址范围 168.92.16.x - 168.92.31.x 配置另一个规则。

```
Console(config-std-acl)#permit host 10.1.1.21
Console(config-std-acl)#permit 168.92.16.0 255.255.240.0
Console(config-std-acl)#
```

9.1.3 permit, deny(Extended)

此命令将规则添加到扩展 IPv4 ACL。该规则为具有特定源或目标 IP 地址，协议类型，源或目标协议端口或 TCP 控制代码的数据包设置过滤条件。使用 no 形式删除规则。

语法

{**permit** | **deny**} [*protocol-number* / **udp**]{**any** | *source address-bitmask* / **host** *source*} {**any** | *destination address-bitmask* / **host** *destination*}[**precedence** *precedence*] [**dscp** *dscp*][**source**-port *sport* [*bitmask*]][**destination**-port *dport* [*port-bitmask*]][**time-range** *time-range-name*]

no {**permit** | **deny**} [*protocol-number* / **udp**]{**any** | *source address-bitmask* / **host** *source*}{**any** | *destination address-bitmask* / **host** *destination*}[**precedence** *precedence*] **dscp** *dscp*][**source**-port *sport* [*bitmask*]][**destination**-port *dport* [*port-bitmask*]]

{**permit** | **deny**} **tcp**{**any** | *source address-bitmask* / **host** *source*}{**any** | *destination address-bitmask* / **host** *destination*}[**precedence** *precedence*] [**dscp** *dscp*][**source-port** *sport* [*bitmask*]][**destination-port** *dport* [*port-bitmask*]][**control-flag** *control-flags flag-bitmask*][**time-range** *time-range-name*]

no {**permit** | **deny**} **tcp**{**any** | *source address-bitmask* / **host** *source*}{**any** | *destination address-bitmask* / **host** *destination*}[**precedence** *precedence*] [**dscp** *dscp*][**source-port** *sport* [*bitmask*]][**destination-port** *dport* [*port-bitmask*]][**control-flag** *control-flags flag-bitmask*]

protocol-number - 特定的协议号。 （范围：0-255）

source - 源 IP 地址。

destination - 目标 IP 地址。

address-bitmask - 表示匹配的地址位的十进制数。

host - 关键字后跟特定的 IP 地址。

优先级 - IP 优先级。 （范围：0-7）

dscp - DSCP 优先级。 （范围：0-63）
sport - 协议 18 源端口号。 （范围：0-65535）
dport - 协议 18 目标端口号。 （范围：0-65535）
port-bitmask - 表示要匹配的端口位的十进制数。（范围：0-65535）
control-flags - 指定 TCP 头的字节 14 中的标志位的十进制数(表示位串)。（范围:0-63）
flag-bitmask - 表示匹配的代码位的十进制数。
time-range-name - *时间段的名称* 。（范围：1-30 个字符）

缺省配置

无

命令模式

扩展 IPv4 ACL

命令用法

◆所有新规则都附加到列表的末尾。

◆ 地址位掩码类似于子网掩码，包含 从 0 到 255 的 四个整数 ，每个 整数 由句点分隔。 二进制掩码使用 1 位指示“匹配”，使用 0 位指示“忽略”。位掩码与指定的源 IP 地址进行按位 AND 运算，然后与进入此 ACL 的端口的每个 IP 数据包的地址进行比较。已被分配。

◆ 您可以在同一规则中指定 Precedence 和 ToS。 但是，如果使用了 DSCP，则既不能指定 Precedence 也不能指定 ToS。

◆ 控制代码位掩码是应用于控制代码的十进制数（表示等效位掩码）。 其中，所述等效的二进制位“1”是指以匹配位和“0”表示忽略位。 可以指定以下位：

- 1（fin） - 完成
- 2（syn） - 同步
- 4（rst） - 重置
- 8（psh） - 推
- 16（ack） - 致谢
- 32（urg） - 紧急指针

例如，使用下面的代码值和掩码来捕获具有以下标志集的数据包：

- SYN 标志有效，使用“control-code 2 2”
- SYN 和 ACK 都有效，使用“control-code 18 18”
- SYN 有效且 ACK 无效，请使用“control-code 2 18”

范例

如果源地址是 withubnet 10.7.1.x，此示例接受任何传入的数据包。 例如，如果规则匹配； 即规则（10.7.1.0 和 255.255.255.0）等于屏蔽地址（10.7.1.2 和 255.255.255.0），数据包通过。

```
Console(config-ext-acl)#permit 10.7.1.1 255.255.255.0 any
Console(config-ext-acl)#
```

当为目标 TCP 端口 80（即 HTTP）设置时，这允许来自 C 类地址 192.168.1.0 的 TCP 数据包到任何目的地地址。

```
Console(config-ext-acl)#permit 192.168.1.0 255.255.255.0 any destination-port
80
Console(config-ext-acl)#
```

这允许来自 C 类地址 192.168.1.0 的所有 TCP 数据包，并将 TCP 控制代码设置为“SYN”。

```
Console(config-ext-acl)#permit tcp 192.168.1.0 255.255.255.0 any controlflag 2 2
Console(config-ext-acl)#
```

9.1.4 ip access-group

此命令将 IPv4 ACL 绑定到端口。使用 no 形式删除该端口。

语法

ip access-group *acl-name* {**in** | **out**}[**time-range** *time-range-name*] [**counter**]

no ip access-group *acl-name* **in**

acl-name - Name of the ACL. (Maximum length: 16 characters)

in - 表示此列表适用于入口数据包。

out - 表示此列表适用于出口数据包。

time-range-name - *时间段的名称* 。（范围：1-30 个字符）

counter - 启用 ACL 统计信息的计数器。

缺省配置

无

命令模式

接口配置 (Ethernet)

◆如果 ACL 已绑定到端口并且您为其绑定了不同的 ACL，则交换机将使用新绑定替换旧绑定。

范例

```
Console(config)#int eth 1/2

Console(config-if)#ip access-group david in

Console(config-if)#
```

9.1.5 show ip access-group

此命令显示分配给 IP ACL 的端口。

命令模式

特权模式

范例

```
Console#show ip access-group

Interface ethernet 1/2

IP access-list david in

Console#
```

9.1.6 show ip access-list

此命令显示已配置的 IPv4 ACL 的规则。

语法

show ip access-list {**standard** | **extended**} [*acl-name*]

standard - 指定标准 IP ACL。

extended - 指定扩展 IP ACL。

acl-name - ACL 的名称。 （最大长度：16 个字符）

命令模式

特权模式

范例

```
Console#show ip access-list standard

IP standard access-list david:

permit host 10.1.1.21
```

```
permit 168.92.0.0 255.255.15.0

Console#
```

9.2 IPV6 ACLs

本节中的命令根据 IPv6 地址，DSCP 流量类或下一个报头类型配置 ACL。 要配置 IPv6 ACL，请首先创建包含所需许可或拒绝规则的访问列表，然后将访问列表绑定到一个或多个端口。

9.2.1 access-list ipv6

此命令添加 IP 访问列表,并进入配置模式标准或扩展 IPv6 ACL。 使用 no 形式删除指定的 ACL。

语法

[no] **access-list ipv6** {**standard** | **extended**} *acl-name*

standard - 指定根据源 IP 地址过滤数据包的 ACL。

extended - 指定根据目标 IP 地址和其他更具体的条件过滤数据包的 ACL。

acl-name - ACL 的名称。 （最大长度：32 个字符）

缺省配置

无

命令模式

全局配置

命令用法

◆为现有 ACL 创建新 ACL 或进入配置模式时，请使用 **permit** 或 **deny** 命令将新规则添加到列表底部。 要创建 ACL，您必须至少向列表添加一个规则。

◆ 要删除规则，请使用 **no permit** 或 **no de ny** 命令，后跟先前配置的规则的确切文本。

◆ ACL 最多可包含 64 条规则。

范例

```
Console(config)#access-list ipv6 standard david

Console(config-std-ipv6-acl)#
```

9.2.2 permit, deny(Standard)

此命令将规则添加到标准 IP v6 ACL。该规则为从指定源发出的数据包设置过滤条件。使用 no 形式删除规则。

语法

{**permit** | **deny**} {**any** / **host** *source-ipv6-address* | *source-ipv6-address*[*/prefix-length*]}[**time-range** *time-range-name*]

no {**permit** | **deny**} {**any** / **host** *source-ipv6-address* | *source-ipv6-address*[*/prefix-length*]}

any - 任何源 IP 地址。

host - 关键字后跟特定的 IP 地址。

source-ipv6-address - IPv6 源地址或网络类。 地址必须根据 RFC 2373 “IPv6 AddressingArchitecture”进行格式化，使用 8 个冒号分隔的 16 位十六进制值。地址中可以使用一个双冒号来表示填充未定义字段所需的零数。

prefix-length - 一个十进制值，表示地址的多少个连续位（左起）构成前缀； 即，地址的网络部分。 （范围：0-128）

time-range-name - *时间段的名称* 。（范围：1-30 个字符）

缺省配置

无

命令模式

标准 IPv6 ACL

命令用法

新规则附加到列表的末尾。

范例

此示例为特定 address2009 配置一个许可规则：DB9：2229 :: 79，以及具有 networkprefix 2009 的地址的另一个规则：DB9：2229：5 :: / 64。

```
Console(config-std-ipv6-acl)#permit host 2009:DB9:2229::79

Console(config-std-ipv6-acl)#permit 2009:DB9:2229:5::/64

Console(config-std-ipv6-acl)#
```

9.2.3 permit, deny(Extended)

此命令将规则添加到扩展 IPv6 ACL。该规则为具有特定目标 IP 地址或下一个 headertype 的数据包设置过滤条件。使用 no 形式删除规则。

语法

{**permit** | **deny**} {**any** | **host** *source-ipv6-address* | *source-ipv6-address*[*/prefix-length*]} {**any** | *destination-ipv6-address*[*/prefix-length*]} [**dscp** *dscp*][**next-header** *next-header*][**time-range** *time-range-name*]

no {**permit** | **deny**} {**any** | **host** *source-ipv6-address* | *source-ipv6-address*[*/prefix-length*]} [**dscp** *dscp*][**next-header** *next-header*]

any - 任何 IP 地址（IPv6 前缀:: / 0 的缩写）。

host - 关键字后跟特定的源 IP 地址。

source-ipv6-address - IPv6 源地址或网络类。 必须根据 RFC 2373 “IPv6 AddressingArchitecture”使用 8 个以冒号分隔的 16 位十六进制值格式化地址。可以在地址中使用一个双冒号来指示填充未定义字段所需的零数。

destination-ipv6-address - IPv6 目标地址或网络类。 必须使用 8 个冒号分隔的 16 位十六进制值根据 RFC 2373“IPv6Addressing Architecture”格式化地址。 可以在地址中使用一个双冒号 来指示填充未定义字段所需的适当数量的零。

prefix-length - 一个十进制值，表示地址的多少个连续位（左起）构成前缀； 即，地址的网络部分。 （范围：源前缀 0-128，目的地前缀 0-8）

dscp - DSCP 流量类。 （范围：0-63）

next-header - 标识紧跟 IPv6 标头之后的标头类型。 （范围： 0-255）

time-range-name - *时间段的名称* 。（范围：1-30 个字符）

缺省配置

无

命令模式

扩展的 IPv6 ACL

命令用法

◆所有新规则都附加到列表的末尾。

◆ 可选的互联网层信息在单独 的标题中 编码，可以放在 IPv6 标头和数据包中的上层标头

之间。存在少量此类扩展标头，每个标头由不同的 Next Header 值标识。IPv6 支持 RFC 1700 中为 IPv4 协议字段定义的值，包括这些常用的标头：

0：逐跳选项（RFC 2460）

6：TCP 上层头（RFC 1700）

17：UDP 上层头（RFC 1700）

43：路由（RFC 2460）

44：片段（RFC 2460）

51：身份验证（RFC 2402）

50：封装安全负载（RFC 2406）

60：目标选项（RFC 2460）

范例

如果目标地址是 2009：DB9：2229 :: 79/8，此示例接受任何传入的数据包。

```
Console(config-ext-ipv6-acl)#permit 2009:DB9:2229::79/8
Console(config-ext-ipv6-acl)#
```

当 DSCP 值为 5 时，这允许数据包到达任何目标地址。

```
Console(config-ext-ipv6-acl)#permit any dscp 5
Console(config-ext-ipv6-acl)#
```

这允许　在下一个标头为 43 时　发送到目标 2009：DB9：2229 :: 79/48 的任何数据包　。

```
Console(config-ext-ipv6-acl)#permit 2009:DB9:2229::79/48 next-header 43
Console(config-ext-ipv6-acl)#
```

9.2.4 show ipv6 access-list

此命令显示已配置的 IPv6 ACL 的规则。

语法

show ipv6 access-list {**standard** | **extended**} [*acl-name*]

standard - 指定标准 IPv6 ACL。

extended - 指定扩展 IPv6 ACL。

acl-name - ACL 的名称。　（最大长度：16 个字符）

命令模式

特权模式

范例

```
Console#show ipv6 access-list standard

IPv6 standard access-list david:

permit host 2009:DB9:2229::79

permit 2009:DB9:2229:5::/64

Console#
```

9.2.5 ipv6 access-group

此命令将端口绑定到 IPv6 ACL。 使用 no 形式删除该端口。

语法

ipv6 access-group *acl-name* {**in** | **out**}[**time-range** *time-range-name*] [**counter**]

no ipv6 access-group *acl-name* {**in** | **out**}

acl-name - ACL 的名称。(最大长度：16 个字符)

in - 表示此列表适用于入口数据包。

out - 表示此列表适用于出口数据包。

time-range-name - *时间段的名称* 。(范围：1-30 个字符)

counter - 启用 ACL 统计信息的计数器。

缺省配置

无

命令模式

接口配置 (Ethernet)

命令用法

如果端口已绑定到 ACL 并将其绑定到不同的 ACL，则该交换机将使用新绑定替换旧绑定。

范例

```
Console(config)#interface ethernet 1/2

Console(config-if)#ipv6 access-group standard david in

Console(config-if)#
```

9.2.6 show ipv6 access-group

此命令显示分配给 IPv6 ACL 的端口。

命令模式

特权模式

范例

```
Console#show ipv6 access-group

Interface ethernet 1/2

IPv6 standard access-list david in

Console#
```

9.3 MAC ACLs

本节中的命令根据硬件地址，数据包格式和以太网类型配置 ACL。 要配置 MAC ACL，请首先创建包含所需许可或拒绝规则的访问列表，然后将访问列表绑定到一个或多个端口。

9.3.1 access-list mac

此命令添加 MAC 访问列表并输入 MAC ACL 配置模式。使用 no 形式删除指定的 ACL。

语法

[no] **access-list mac** *acl-name*

acl-name - ACL 的 名称。（最大长度：16 个字符，没有空格或其他特殊字符）

缺省配置

无

命令模式

全局配置

命令用法

◆为现有 ACL 创建新 ACL 或进入配置模式时，请使用 **permit** 或 **deny** 命令 将新规则添加到列表底部。

◆ 要删除规则，请使用 **no permit** 或 **no deny** 命令，后跟先前配置的规则的确切文

本。

◆ ACL 最多可包含 64 条规则。

范例

```
Console(config)#access-list mac jerry

Console(config-mac-acl)#
```

9.3.2 permit, deny(MAC)

此命令将规则添加到 MAC ACL。该规则过滤与指定的 MAC 源或目标地址（即物理层地址）或以太网协议类型匹配的数据包。使用 no 形式删除规则。

语法

{**permit** | **deny**}{**any** | **host** *source* | *source address-bitmask*}{**any** | **host** *destination* | *destination address-bitmask*}[**vid** *vid vid-bitmask*] [**ethertype** *protocol* [*protocol-bitmask*]][**time-range** *time-range-name*]

no {**permit** | **deny**}{**any** | **host** *source* | *source address-bitmask*}{**any** | **host** *destination* | *destination address-bitmask*}[**vid** *vid vid-bitmask*] [**ethertype** *protocol* [*protocol-bitmask*]]

注意: 默认是用于以太网 II 数据包。

{**permit** | **deny**} **tagged-eth2**{**any** | **host** *source* | *source address-bitmask*}{**any** | **host** *destination* | *destination address-bitmask*}[**vid** *vid vid-bitmask*] [**ethertype** *protocol* [*protocol-bitmask*]][**time-range** *time-range-name*]

no {**permit** | **deny**} **tagged-eth2**{**any** | **host** *source* | *source address-bitmask*} {**any** | **host** *destination* | *destination address-bitmask*}[**vid** *vid vid-bitmask*] [**ethertype** *protocol* [*protocol-bitmask*]]

{**permit** | **deny**} **untagged-eth2**{**any** | **host** *source* | *source address-bitmask*} {**any** | **host** *destination* | *destination address-bitmask*}[**ethertype** *protocol* [*protocol-bitmask*]][**time-range** *time-range-name*]

no {**permit** | **deny**} **untagged-eth2**{**any** | **host** *source* | *source address-bitmask*}{**any** | **host** *destination* | *destination address-bitmask*}[**ethertype** *protocol* [*protocol-bitmask*]]

{**permit** | **deny**} **tagged-802.3**{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}[**vid** *vid vid-bitmask*] [**time-range** *time-range-name*]
no {**permit** | **deny**} **tagged-802.3**{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}[**vid** *vid vid-bitmask*]
{**permit** | **deny**} **untagged-802.3**{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}[**time-range** *time-range-name*]
no {**permit** | **deny**} **untagged-802.3**{**any** | **host** *source* | *source address-bitmask*}{**any** | **host** *destination* | *destination address-bitmask*}
tagged-eth2 - 标记以太网 II 数据包。
untagged-eth2 - Untagged Ethernet II 数据包。
tagged-802.3 - 标记以太网 802.3 数据包。
untagged-802.3 - 未 标记的以太网 802.3 数据包。
any - 任何 MAC 源或目标地址。
host - 特定的 MAC 地址。
source - 源 MAC 地址。
destination - 具有位掩码的目标 MAC 地址范围。
address-bitmask 19 - MAC 地址的 位掩码 （十六进制 格式）。
vid - VLAN ID。 （范围：1-4093）
vid-bitmask 19 - VLAN 位掩码。 （范围：1-4095）
协议 - 特定的以太网协议号。 （范围：600-ffff hex。）
protocol - *bitmask* - 协议位掩码。 （范围：600-ffff hex。）
time-range-name - *时间范围的名称* 。 （范围：1-30 个字符）

缺省配置

无

命令模式

MAC ACL

命令用法

◆新规则将添加到列表的末尾。

◆**以太网类型** 选项只能用于过滤以太网 II 格式充许的数据包。

◆RFC 1060 中提供了以太网协议类型的详细列表。一些较常见的类型包括：

- 0800 - IP
- 0806 - RP
- 8137 - IPX

范例

此规则允许从任何源 MAC 地址到目标地址 00-e0-29-94-34-de 的数据包，其中以太网类型为 0800。

```
Console(config-mac-acl)#permit any host 00-e0-29-94-34-de ethertype 0800

Console(config-mac-acl)#
```

9.3.3 mac access-group

此命令将 MAC ACL 绑定到端口。 使用 no 形式删除端口。

语法

mac access-group *acl-name* {**in** | **out**}[**time-range** *time-range-name*] [**counter**]

acl-name - ACL 的名称。 （最大长度：16 个字符）

in - 表示此列表适用于入口数据包。

out - 表示此列表适用于出口数据包。

time-range-name - *时间段的名称* 。（范围：1-30 个字符）

counter - 启用 ACL 统计信息的计数器。

缺省配置

无

命令模式

接口配置 (Ethernet)

命令用法

如果 ACL 已绑定到端口并且您将其绑定到不同的 ACL，则该交换机将使用新绑定替换旧绑定。

范例

```
Console(config)#interface ethernet 1/2

Console(config-if)#mac access-group jerry in

Console(config-if)#
```

9.3.4 show mac access-group

此命令显示分配给 MAC ACL 的端口。

命令模式

特权模式

范例

```
Console#show mac access-group

Interface ethernet 1/5

MAC access-list M5 in

Console#
```

9.3.5 show mac access-list

此命令显示已配置的 MAC ACL 的规则。

语法

show mac access-list [*acl-name*]

acl-name - ACL 的名称。 （最大长度：16 个字符）

命令模式

特权模式

范例

```
Console#show mac access-list

MAC access-list jerry:

permit any 00-e0-29-94-34-de ethertype 0800

Console#
```

9.4 ARP ACLs

本节中的命令基于包含在 ARP 请求和应答消息中的 IP 地址或 MAC 地址来配置 ACL。要配置 ARP ACL，请首先创建包含所需许可或拒绝规则的访问列表，然后将访问列表绑定到一个或多个 VLAN。

9.4.1 access-list arp

此命令添加 ARP 访问列表并进入 ARP ACL 配置模式。使用 no 形式删除指定的 ACL。

语法

[no] **access-list arp** *acl-name*

acl-name - ACL 的名称。（最大长度：16 个字符）

缺省配置

无

命令模式

全局配置

命令用法

◆为现有 ACL 创建新 ACL 或进入配置模式时，请使用 **permit** 或 **deny** 命令将新规则添加到列表底部。 要创建 ACL，您必须至少向列表添加一个规则。

◆ 要删除规则，请使用 **no permit** 或 **no de ny** 命令，后跟先前配置的规则的确切文本。

◆ ACL 最多可包含 128 条规则。

范例

```
Console(config)#access-list arp factory
Console(config-arp-acl)#
```

9.4.2 permit, deny (ARP)

此命令将规则添加到 ARP ACL。该规则过滤与 ARP 消息中指定的源或目标地址匹配的数据包。使用 no 形式删除规则。

语法

[no] {**permit** | **deny**}**ip** {**any** | **host** *source-ip* | *source-ip ip-address-bitmask*}

mac {**any** | **host** *source-mac* | *source-mac mac-address-bitmask*}[**log**]

This form indicates either request or response packets.

[no] {**permit** | **deny**} **requestip** {**any** | **host** *source-ip* | *source-ip ip-address-bitmask*}**mac** {**any** | **host** *source-mac* | *source-mac mac-address-bitmask*}[**log**]

[no] {**permit** | **deny**} **responseip** {**any** | **host** *source-ip* | *source-ip ip-address-bitmask*}{**any** | **host** *destination-ip* / *destination-ip ip-address-bitmask*}**mac** {**any** | **host** *source-mac* | *source-mac mac-address-bitmask*}[**any** | **host** *destination-mac* | *destination-mac mac-addressbitmask*] [**log**]

source-ip - 源 IP 地址。

destination-ip - 带位掩码的目标 IP 地址。

ip-address-bitmask - 表示地址 bitsto 匹配的 IPv4 号。

source-mac - 源 MAC 地址。

destination-mac - 带位掩码的目标 MAC 地址范围。

mac-address-bitmask 20 - MAC 地址的位掩码（十六进制格式）。

log - 在与访问控制条目匹配时记录数据包。

缺省配置

无

命令模式

ARP ACL

命令用法

新规则将添加到列表的末尾。

范例

此规则允许从任何源 IP 和 MAC 地址到目标子网地址 192.168.0.0 的数据包。

```
Console(config-arp-acl)#$permit response ip any 192.168.0.0 255.255.0.0 macany any

Console(config-mac-acl)#
```

9.4.3 show arp access-list

此命令显示已配置的 ARP ACL 的规则。

语法

show arp access-list [*acl-name*]

acl-name -ACL 的名称。 （最大长度：16 个字符）

命令模式

特权模式

范例

```
Console#show arp access-list

ARP access-list factory:

permit response ip any 192.168.0.0 255.255.0.0 mac any any

Console#
```

9.5 ACL 信息

本节介绍用于显示 ACL 信息的命令。

9.5.1 clear access-list hardware counters

此命令清除所有 ACL 中规则的命中计数器，或清除指定 ACL 中规则的命中计数器。

语法

clear access-list hardware counters [*acl-name*]

acl-name - ACL 的名称。（最大长度：16 个字符）

命令模式

特权模式

范例

```
Console#clear access-list hardware counters

Console#
```

9.5.2 show access-group

此命令显示 ACL 的端口分配。

命令模式

特权模式

范例

```
Console#show access-group

Interface ethernet 1/2

IP access-list david

MAC access-list jerry

Console#
```

9.5.3 show access-list

此命令显示所有 ACL 和关联规则。

语法

show access-list[[**arp** [*acl-name*]] |[**ip** [**extended** [*acl-name*] | **standard** [*acl-name*]] |[**ipv6** [**extended** [*acl-name*] | **standard** [*acl-name*]] |[**mac** [*acl-name*]] | [**tcam-utilization**] | [**hardware counters**]]

arp - 显示 ARP ACL 的入口或出口规则。

hardware counters - 显示所有 ACL 的统计信息。

ip extended - 显示扩展 IPv4ACL 的入口或出口规则。

ip standard - 显示标准 IPv4ACL 的入口或出口规则。

ipv6 extended - 显示扩展 IPv6ACL 的入口或出口规则。

ipv6 standard - 显示标准 IPv6ACL 的入口或出口规则。

mac - 显示 MAC ACL 的入口或出口规则。

tcam-utilization - 显示用户配置的 ACL 规则占总 ACL 规则百分比的百分比

acl-name - ACL 的名称。 （最大长度：16 个字符）

命令模式

特权模式

范例

```
Console#show access-list

IP standard access-list david:

permit host 10.1.1.21

permit 168.92.0.0 255.255.15.0

IP extended access-list bob:

permit 10.7.1.1 255.255.255.0 any

permit 192.168.1.0 255.255.255.0 any destination-port 80 80

permit 192.168.1.0 255.255.255.0 any protocol tcp control-code 2 2

MAC access-list jerry:

permit any host 00-30-29-94-34-de ethertype 800 800

IP extended access-list A6:

deny tcp any any control-flag 2 2

permit any any

Console#
```

10 接口命令

这些命令用于显示或设置以太网端口，聚合链路或 VLAN 的通信参数； 或在指定的接口上执行电缆诊断。

10.1 接口配置

10.1.1 Interface

此命令配置接口类型并进入接口配置模式。 使用带有主干的 no 形式删除非活动接口。

语法

[no] **interface** *interface*

interface

ethernet *单元 / 端口*

unit -单位标识符。 （范围：1）

port -端口号。 （范围：1-28）

port-channel *channel-id* （范围：1-12）

vlan *vlan-id* （范围：1-4093）

缺省配置

无

命令模式

全局配置

范例

要指定端口 4，请输入以下命令：

```
Console(config)#interface ethernet 1/4
Console(config-if)#
```

10.1.2 capabilities

此命令在自动协商期间通告给定接口的端口功能。使用带有参数的 no 形式来删除无法使用的功能，或使用不带参数的 no 形式来恢复默认值。

语法

[no] capabilities {1000full | 100full | 100half | 10full | 10half |flowcontrol | symmetric}

1000full - 支持 1 Gbps 全双工操作

100full - 支持 100 Mbps 全双工操作

100half - 支持 100 Mbps 半双工操作

10full - 支持 10 Mbps 全双工操作

10half - 支持 10 Mbps 半双工操作

flowcontrol - 支持流量控制

symmetric - 指定时，端口发送和接收对称暂停帧。

缺省配置

1000BASE-T: 10half, 10full, 100half, 100full, 1000full

1000BASE-SX/LX/ZX (SFP+): 1000full

10GBASE-SR/LR/ER (SFP+): 10Gfull

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

◆10GBASE-SFP +连接固定为 10G，完全双工。当自动-启动谈判，唯一的属性，它可以是 advertisedinclude 流量控制和对称暂停帧。

◆ 1000BASE-T 标准不支持强制模式。

◆ 使用 negotiation 命令 启用自动协商时，交换机将根据命令协商链路的最佳设置。禁用

自动协商时，必须使用 speed-duplex 和 flowcontrol 命令手动指定链接属性 。

范例

以下示例将以太网端口 5 功能配置为包含 100half 和 100full。

```
Console(config)#interface ethernet 1/5

Console(config-if)#capabilities 100half

Console(config-if)#capabilities 100full

Console(config-if)#capabilities flowcontrol

Console(config-if)#
```

10.1.3 description

此命令将向接口添加说明。使用 no 形式删除描述。

语法

description *string*

no description

string -注释或描述，以帮助您记住此接口的附加内容。（范围：1-64 个字符）

缺省配置

无

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

描述由 show interfaces status 命令和 running-configuration 文件显示。 网络管理员可能在此对象中存储的值的示例是制造商的名称和产品名称。

范例

以下示例将描述添加到端口 4。

```
Console(config)#interface ethernet 1/4

Console(config-if)#description RD-SW#3

Console(config-if)#
```

10.1.4 flowcontrol

此命令启用流量控制。使用 no 形禁用流量控制。

语法

[no] flowcontrol

缺省配置

禁用

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

◆1000BASE-T 不支持强制模式。应始终使用自动协商通过任何 1000BASE-T 端口 ortrunk 建立连接。

◆ 流量控制可以通过 在缓冲区填充时 “阻塞”来自直接连接到 交换机的 终端站或段的流量来消除帧丢失。启用后，背压用于半双工操作，而背压用于全双工操作，IEEE 802.3-2002（正式为 IEEE 802.3x）。

◆ 要强制的流量控制或关（与**流量控制**或**流量控制没有**命令）时，使用**没有负** otiation 命令禁用自动-协商选定接口上。

◆ 使用 negotiation 命令启用自动协商时，最佳设置将由 capabilities 命令确定。自动协商下的启用流量控制，“flowcontrol”必须包含在任何端口的功能列表中。

范例

以下示例启用端口 5 上的流控制。

```
Console(config)#interface ethernet 1/5
Console(config-if)#flowcontrol
Console(config-if)#no negotiation
Console(config-if)#
```

10.1.5 negotiation

此命令启用给定接口的自动协商。使用 no 形式禁用自动协商。

语法

[no] negotiation

缺省配置

启用

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

◆1000BASE-T 不支持强制模式。应始终使用自动协商通过任何 1000BASE-T 端口 ortrunk 建立连接。

◆ 启用自动协商后，交换机将根据 capabilities 命令 协商链路的最佳设置。当自动-协商被禁用，您必须手动指定速度，双工和流量控制命令的链接 。

◆ 如果禁用自动协商，则 RJ-45 端口也将禁用自动 MDI / MDI-X 引脚信号配置。

范例

以下示例将端口 10 配置为使用自动协商。

```
Console(config)#interface ethernet 1/10
Console(config-if)#negotiation
Console(config-if)#
```

10.1.6 shutdown

此命令禁用接口。要重新启动已禁用的接口，请使用 no 形式。

语法

[no] shutdown

缺省配置

启用

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

此命令允许您由于异常行为(例如,过度冲突)而禁用端口,然后在问题得到解决后重新启用它。出于安全原因，您可能还希望禁用端口。

范例

以下示例禁用端口 5。

```
Console(config)#interface ethernet 1/5

Console(config-if)#shutdown

Console(config-if)#
```

10.1.7 speed-duplex

当禁用自动协商时，此命令配置给定接口的速度和双工模式。使用 no 形式恢复默认值。

语法

speed-duplex {**1000full** | **100full** | **100half** | **10full** | **10half**}

no speed-duplex

1000full - 强制 1000 Mbps 全双工操作

100full - 强制 100 Mbps 全双工操作

100half - 强制 100 Mbps 半双工操作

10full - 强制 10 Mbps 全双工操作

10half - 强制 10 Mbps 半双工操作

缺省配置

◆默认情况下启用自动协商。

◆ 禁用自动协商时 ，1000BASE-T 端口 的默认速度双工设置为 **100full**。

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

◆1000BASE-T 标准不支持强制模式。自动-谈判应始终被用来建立在 any1000BASE-T 端口或主干的连接。如果不使用，连接到其他类型的交换机时无法保证链接过程的成功。

◆ 要强制操作，以在**速度**指定的速度和双工模式**-双工**命令，使用没有协商命令禁用自动-在所选接口上的协商。

◆ 使用 negotiation 命令启用自动协商时，最佳设置将由命令确定。要在自动协商下设置速度/双工模式，可在接口的功能列表中指定所需的调制解调器。

范例

以下示例将端口 5 配置为 100 Mbps，半双工操作。

```
Console(config)#interface ethernet 1/5

Console(config-if)#speed-duplex 100half

Console(config-if)#no negotiation

Console(config-if)#
```

10.1.8 switchport packet-rate

此命令用于配置广播，组播和未知单播风暴控制。使用 no 形式恢复默认设置。

语法

switchport {**broadcast** | **multicast** | **unicast**} **packet-rate** *rate*

no switchport {**broadcast** | **multicast** | **unicast**}

broadcast - 指定广播流量的风暴控制。

multicast - 指定组播流量的风暴控制。

unicast - 指定未知单播流量的风暴控制。

rate - 阈值级别，单位为 Kilobits /秒。(范围：范围：64-10,000,000 Kbps;默认值：64 Kbps)

缺省配置

Broadcast Storm 控制: 启用, packet-rate limit: 64 kbps

Multicast Storm 控制: 禁用

Unknown Unicast 控制: 禁用

命令模式

接口配置 (Ethernet)

命令用法

◆当流量超过为广播和多播或未知单播流量指定的阈值时，超过阈值的数据包将丢弃，直到速率降低到阈值以下。

◆ 可以使用此 命令在硬件级别控制流量风暴，也可以使用 auto-traffic-control 命令在软件级别控制流量风暴。但是，这些控件类型中只有一种可以应用于 aport。在端口上启用硬件级风暴控制将禁用该端口上的自动风暴控制。

◆ 当通过 auto - traffic-control action 命令将控制响应设置为速率限制时，自动 stormcontrol 也会使用此命令设置的速率限制。

◆ 在同一界面上同时使用速率限制和风暴控制可能会导致意外结果。例如，假设通过命令“switchport broadcastpacket-rate 500”将广播风暴控制设置为 500 Kbps，并且通过快速以太网端口上的命令“速率限制输入 20000”将速率限制设置为 20000 Kbps。由于 20000Kbps 是 1 / 5 线速（100 Mbps），接收速率实际上是

100 Kbps，或风暴控制命令设置的 500 Kbps 限制的 1/5。因此不建议在同一接口上同时使用这两个命令。

范例

以下显示如何以每秒 600 千比特的速度配置广播风暴控制：

```
Console(config)#interface ethernet 1/5

Console(config-if)#switchport broadcast packet-rate 600

Console(config-if)#
```

10.1.9 clear counters

该命令用于清除接口的统计信息。

语法

clear counters *interface*

interface

ethernet *单元 / 端口*

unit - 单位标识符。 （范围：1）

端口 - 端口号。 （范围：1-28）

port-channel *channel-id*（范围：1-12）

缺省配置

无

命令模式

特权模式

命令用法

统计信息仅针对电源重置进行初始化。此命令将当前管理会话的显示统计信息的基值设置为零。

但是，如果您注销并返回管理界面，则显示的统计信息将显示自上次重置电源后累积的绝对值。

范例

以下示例清除端口 5 上的统计信息

```
Console#clear counters ethernet 1/5

Console#
```

10.1.10 show interfaces brief

此命令显示所有端口的关键信息摘要，包括操作状态，本机 VLAN ID，默认优先级，速度/双工模式和端口类型。

命令模式

特权模式

范例

```
Console#show interfaces brief

Interface Name Status PVID Pri Speed/Duplex Type Trunk

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

--

Eth 1/ 1 Down 1 0 Auto 1000BASE-T None

Eth 1/ 2 Down 1 0 Auto 1000BASE-T None

Eth 1/ 3 Down 1 0 Auto 1000BASE-T None

Eth 1/ 4 Down 1 0 Auto 1000BASE-T None

Eth 1/ 5 Down 1 0 Auto 1000BASE-T None

Eth 1/ 6 Down 1 0 Auto 1000BASE-T None
```

10.1.11 show interfaces counters

此命令显示接口统计信息。

语法

show interfaces counters [*interface*]

interface

ethernet *单元 / 端口*

unit -单位标识符。（范围：1）

port -端口号。（范围：1-28）

port-channel *channel-id* (范围: 1-12)

缺省配置

所有端口

命令模式

普通模式，特权模式

命令用法

如果未指定接口，则显示所有接口的信息。

范例

```
Console#show interfaces counters ethernet 1/1

Ethernet 1/ 1

===== IF table Stats =====

2166458 Octets Input

14734059 Octets Output

14707 Unicast Input

19806 Unicast Output

0 Discard Input

0 Discard Output

0 Error Input

0 Error Output

0 Unknown Protocols Input

0 QLen Output

===== Extended Iftable Stats =====

23 Multi-cast Input

5525 Multi-cast Output

170 Broadcast Input

11 Broadcast Output

===== Ether-like Stats =====

0 Alignment Errors

0 FCS Errors

0 Single Collision Frames

0 Multiple Collision Frames

0 SQE Test Errors

0 Deferred Transmissions

0 Late Collisions
```

0 Excessive Collisions

0 Internal Mac Transmit Errors

0 Internal Mac Receive Errors

0 Frames Too Long

0 Carrier Sense Errors

0 Symbol Errors

0 Pause Frames Input

0 Pause Frames Output

===== RMON Stats =====

0 Drop Events

16900558 Octets

40243 Packets

170 Broadcast PKTS

23 Multi-cast PKTS

0 Undersize PKTS

0 Oversize PKTS

0 Fragments

0 Jabbers

0 CRC Align Errors

0 Collisions

21065 Packet Size <= 64 Octets

3805 Packet Size 65 to 127 Octets

2448 Packet Size 128 to 255 Octets

797 Packet Size 256 to 511 Octets

2941 Packet Size 512 to 1023 Octets

9187 Packet Size 1024 to 1518 Octets

===== Port Utilization =====

111 Octets Input in kbits per second

0 Packets Input per second

0.00 % Input Utilization

606 Octets Output in kbits per second

1 Packets Output per second

0.00 % Output Utilization

Console#

10.1.12 show interfaces status

此命令显示接口的状态。

语法

show interfaces status [*interface*]

interface

ethernet *单元 / 端口*

unit -单位标识符。(范围：1)

port -端口号。(范围：1-28)

port-channel *channel-id* (范围：1-12)

vlan *vlan-id* (范围：1-4093)

缺省配置

所有端口

命令模式

普通模式，特权模式

命令用法

如果未指定接口，则显示所有接口的信息。

范例

Console#show interfaces status ethernet 1/1

Information of Eth 1/1

Basic Information:

Port Type : 1000BASE-T

MAC Address : 00-E0-0C-00-00-FE

Configuration:

Name :

```
Port Admin : Up

Speed-duplex : Auto

Capabilities : 10half, 10full, 100half, 100full

Broadcast Storm : Enabled

Broadcast Storm Limit : 64 Kbits/second

Multicast Storm : Disabled

Multicast Storm Limit : 64 Kbits/second

Unknown Unicast Storm : Disabled

Unknown Unicast Storm Limit : 64 Kbits/second

Flow Control : Disabled

VLAN Trunking : Disabled

LACP : Disabled

Media Type : Copper forced

Current Status:

Link Status : Up

Port Operation Status : Up

Operation Speed-duplex : 100full

Up Time : 0w 0d 1h 11m 2s (4262 seconds)

Flow Control Type : None

Max Frame Size : 1518 bytes (1522 bytes for tagged frames)

Console#
```

10.1.13 show interfaces switchport

此命令显示指定接口的管理和操作状态。

语法

show interfaces switchport [*interface*]

interface

ethernet *单元 / 端口*

unit -单位标识符。 （范围：1）

port -端口号。 （范围：1-28）

port-channel *channel-id*（范围：1-12）

缺省配置

所有端口

命令模式

普通模式，特权模式

命令用法

如果未指定接口，则显示所有接口的信息。

范例

此示例显示端口 1 的配置设置。

```
Console#show interfaces switchport ethernet 1/1

Information of Eth 1/1

Broadcast Threshold : Enabled, 500 packets/second

Multicast Threshold : Disabled

Unknown Unicast Threshold : Disabled

LACP Status : Disabled

Ingress Rate Limit : Disabled, 1000M bits per second

Egress Rate Limit : Disabled, 1000M bits per second

VLAN Membership Mode : Hybrid

Ingress Rule : Disabled

Acceptable Frame Type : All frames

Native VLAN : 1

Priority for Untagged Traffic : 0

GVRP Status : Disabled

Allowed VLAN : 1(u)

Forbidden VLAN :

802.1Q Tunnel Status : Disabled

802.1Q Tunnel Mode : Normal

802.1Q Tunnel TPID : 8100 (Hex)
```

```
Layer 2 Protocol Tunnel : None

Console#
```

10.1.14 show interfaces transceiver

此命令显示指定收发器的识别信息，包括连接器类型和供应商相关参数，以及温度，电压，偏置电流，发射功率和接收功率。

语法

show interfaces transceiver [*interface*]

interface

ethernet *单元 / 端口*

unit -单位标识符。（范围：1）

port -端口号。（范围：SFP 端口 25-28）

缺省配置

所有的光端口

命令模式

特权模式

命令用法

交换机可以显示 SFP 模块的诊断信息，该模块支持 SFF-8472 光学收发器诊断监控接口规范。此信息允许管理员远程诊断光学设备的问题。此功能在命令显示中称为数字诊断监控（DDM），可提供收发器参数信息，包括温度，电源电压，激光电流，激光功率和接收光功率。

范例

```
Console#show interfaces transceiver ethernet 1/25

Information of Eth 1/10

Connector Type : LC

Fiber Type : [0x00]

Eth Compliance Codes : 1000BASE-ZX

Baud Rate : 1300 MBd

Vendor OUI : 00-00-5F
```

```
Vendor Name : SumitomoElectric

Vendor PN : SCP6G94-FN-BWH


Vendor Rev : Z
Vendor SN : SE08T712Z00006
Date Code : 10-09-14
DDM Info
Temperature : 35.64 degree C
Vcc : 3.25 V
Bias Current : 12.13 mA
TX Power : 2.36 dBm
RX Power : -24.20 dBm
Console#
```

10.2 电缆诊断

10.2.1 test cable-diagnostics

此命令在指定端口上执行电缆诊断，以诊断电缆故障（短路，开路等）并报告电缆长度。

语法

test cable-diagnostics interface *interface*

interface

ethernet *unit/port*

unit -单位标识符。 （范围：1）

port -端口号。 （范围：1-28）

命令模式

特权模式

命令用法

◆使用数字信号处理（DSP）测试方法执行电缆诊断。 DSP 通过在电缆中发送脉冲信号，然后检查该脉冲的反射来分析电缆。

◆ 此电缆测试仅适用于 7 - 140 米 长的 电缆 。

◆ 测试大约需要 5 秒钟。 交换机在完成后立即显示测试结果，包括常见的电缆故障，以及每个电缆对的状态和大致长度。

◆ 诊断 可能列出的潜在条件 包括：

■ 确定：正确终止对

■ 打开：打开对，没有链接伙伴

■ 短：对短

■ 不支持：此消息显示为链接的任何快速以太网端口，或者连接到 低于 1000 Mbps 的 任何千兆以太网端口 。

- 阻抗不匹配：终端阻抗不在参考范围内。

◆ 运行电缆诊断时，端口已链接。

◆ 为了确保长度的更准确的测量到的故障,firstdisable 省电模式(使用 无省电 命令）上 thelink 伙伴运行电缆诊断之前。

范例

```
Console#test cable-diagnostics interface ethernet 1/25

Port Type Link Status Pair A (meters) Pair B (meters) Last Update

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

Eth 1/25 GE Up OK (21) OK (21) 2009-11-13 09:44:19

Console#
```

10.2.2 show cable-diagnostics

此命令显示电缆诊断测试的结果。

语法

show cable-diagnostics interface [*interface*]

interface

ethernet *unit/port*

unit -单位标识符。 （范围：1）

port -端口号。 （范围：1-28）

命令模式

特权模式

命令用法

◆结果包括常见的电缆故障，以及故障的状态和近似距离，或者如果 发现 nofault， 则显示 大致的电缆长度 。

◆ 为了确保更准确地测量故障长度，在运行 cablediagnostics 之前，首先在链路伙伴上禁用省电模式。

◆ 对于链路断开端口，报告的故障距离精确到+/- 2 米。 对于链接 端口，精度为+/- 10 米。

范例

```
Console#show cable-diagnostics interface ethernet 1/26
```

```
Port Type Link Status Pair A (meters) Pair B (meters) Last Update
-------- ---- ----------- --------------- --------------- -----------------
Eth 1/26 GE Up OK (21) OK (21) 2009-11-13 09:44:19
Console#
```

10.3 省电

10.3.1 power-save

此命令在指定端口上启用节能模式。

语法

[no] power-save

命令模式

接口配置 (Ethernet)

命令用法

◆IEEE 802.3 定义了基于 100 米工作的电缆连接的以太网标准和后续电源要求。启用省电模式可以减少 60 米或更短的电缆长度所用的电力，对于 20 米或更小的电缆 进行 更大幅度的减少 ，并继续确保信号完整性。

◆ 省电模式仅适用于使用铜介质的千兆以太网端口。

◆ 可以在千兆以太网 RJ-45 端口上实现节能。

◆ 此开关提供的省电方法 包括：

■ 没有链接伙伴时节省电量：

在正常操作下,交换机不断自动协商链接伙伴,即使存在 nolink 连接,也保持 MAC 接口通电。 当使用省电模式时，开关 在电路上吸收能量以确定是否存在 linkpartner。 如果没有检测到，则开关自动关闭发射器和大部分接收电路（进入睡眠模式）。在此模式下，低功率能量检测电路不断检查电缆上的能量。 如果没有检测到，则 MAC 接口也会断电以节省额外的能量。 如果检测到能量，则交换机立即打开发送器和接收器功能，并启动 MAC 接口。

■ 存在链接伙伴时节省电量：

传统的以太网连接通常以足够的功率运行，以支持至少 100 米的电缆，即使平均网络电缆长度较短。 当电缆长度较短时， 由于信号衰减与电缆长度成比例 ，因此可以 降低 功耗 。 启用省电模式后，switchanalyzes 电缆长度，以确定它是否可以减少电源
在特定链路上使用的信号幅度。

注意： 一个主链路上的节电模式，只有当 theconnection 速度为 100 Mbps 或在衔接更高，和线路长度是每种不超过 60 米工作。

注意： 电源节省只能在千兆位以太网实现 portsusing 双绞线电缆。 仅当连接速度为 1 Gbps 且线路长度小于 60 米时，活动链路上的省电模式才有效。

范例

```
Console(config)#interface ethernet 1/28

Console(config-if)#power-save

Console(config-if)#
```

10.3.2 show power-save

此命令显示节能的配置设置。

语法

show power-save [**interface** *interface*]

interface

ethernet *unit/port*

unit -单位标识符。 （范围：1）

port -端口号。 （范围：1-28）

命令模式

特权模式

范例

```
Console#show power-save interface ethernet 1/28

Power Saving Status:

Ethernet 1/28 : Enabled

Console#
```

11 链接聚合命令

端口可以静态分组为聚合链路（即主干）增加网络连接的带宽或确保故障恢复。或者，您可以使用链路聚合控制协议（LACP）自动协商此交换机与另一个网络设备之间的中继链路。 对于静态干线，交换机必须符合思科以太网 - 通道标准。对于动态中继，交换机与 LACP 紧密相关。此开关最多支持 12 个中继线。例如，当以全双工模式运行时，由两个 1000 Mbps 端口组成的 trunk 可支持 4 Gbps 的聚合带宽。

11.1 手动配置命令

11.1.1 port channel load-balance

此命令在聚合链接（用于静态和动态中继）的端口之间设置负载分配方法。使用 no 形式恢复默认设置。

语法

port channel load-balance {dst-ip | dst-mac | src-dst-ip |src-dst-mac | src-ip | src-mac}

no port channel load-balance

dst-ip - 基于目标 IP 地址的负载均衡。

dst-mac - 基于目标 MAC 地址的负载均衡。

src-dst-ip - 基于源和目标 IP 地址的 负载均衡。

src-dst-mac - 基于源和目标 MAC 地址的负载平衡。

src-ip - 基于源 IP 地址的负载均衡。

src-mac - 基于源 MAC 地址的负载均衡。

缺省配置

src-dst-ip

命令模式

全局配置

命令用法

◆此命令适用于交换机上的所有静态和动态中继。

◆ 要确保交换机流量负载均匀分布在中继的 alllink 中，请选择负载平衡计算中使用的源地址和目标地址，以便 为 trunk 连接提供最佳 结果：

■ **dst-ip** ：具有相同目标 IP 地址的所有流量都在中继的同一链路上输出。 此模式最适用于交换机到路由器的链路，其中通过交换机的流量发往不同的主机。 不要 将此模式用于交换机到服务器的中继链路，其中目标 IP 地址对于所有流量都相同。

■ **dst-mac** ：具有相同目标 MAC 地址的所有流量都是在中继的同一链路上输出。 此模式适用于最佳的交换机到交换机中继 链路，其中通过交换机的流量适用于许多不同的主机。 不要将此模式用于目的 MAC 地址对所有流量都相同的交换机路由器中继链路。

■ **src-dst-ip** ：具有相同源和目标 IPa 地址的 所有流量都 在中继的同一链路上输出。 此模式最适用于交换机到路由器中继链路，其中通过交换机的流量接收并发往许多不同的主机。

■ **src-dst-mac** ：具有相同源和目标 MACadd 的所有流量都 在中继的同一链路上输出。 此模式最适用于交换机到交换机中继链路，其中通过交换机的流量接收并发往许多不同的主机。

■ **src-ip** ：具有相同源 IP 地址的所有流量都 在中继的 the me me 链路 上输出 。 此模式最适用于交换机到路由器或交换机到服务器中继链路，其中通过交换机的流量从许多不同的主机接收。

■ **src-mac** ：具有相同源 MAC 地址的所有流量都在中继的同一链路上输出。 此模式最适用于从不同主机接收通过交换机的流量的交换机到交换机链路。

范例

```
Console(config)#port-channel load-balance dst-ip
Console(config)#
```

11.1.2 channel-group

此命令将端口添加到中继。 使用 no 形式从 trunk 中删除端口。

语法

channel-group *channel-id*

no channel-group

channel-id - Trunk 索引（范围：1-12）

缺省配置

当前端口将添加到此中继。

命令模式

接口配置 (Ethernet)

命令用法

◆配置静态中继时，交换机必须符合 Cisco Ether - Channel 标准。

◆不使用**通道**组从主干中删除端口组。

◆不使用接口端口通道从交换机中删除中继。

范例

以下示例创建 trunk 1，然后添加端口 10：

```
Console(config)#interface port-channel 1

Console(config-if)#exit

Console(config)#interface ethernet 1/10

Console(config-if)#channel-group 1

Console(config-if)#
```

11.2 动态配置命令

11.2.1 lacp

此命令为当前接口启用 802.3ad 链路聚合控制协议（LACP）。 使用 no 形式禁用它。

语法

[no] lacp

缺省配置

禁用

命令模式

接口配置 (Ethernet)

命令用法

◆必须通过强制模式或自动协商将 LACP 中继两端的端口配置为 fullduplex。

◆ 使用 LACP 与另一台交换机形成的中继将自动分配下一个可用的端口通道 ID。

◆ 如果目标交换机在连接的端口上也启用了 LACP，则会自动激活该路由器。

◆ 如果连接到同一目标交换机的八个以上端口具有 LACP 启用，则其他端口将处于待机模式，并且只有其中一个活动链路发生故障时才会启用 。

范例

以下显示端口 1-3 上启用 LACP。由于 LACP 也已在链路另一端的端口上启用，因此 show interfacesstatus port-channel 1 命令显示已建立 Trunk1。

```
Console(config)#interface ethernet 1/1

Console(config-if)#lacp

Console(config-if)#interface ethernet 1/2

Console(config-if)#lacp

Console(config-if)#interface ethernet 1/3

Console(config-if)#lacp

Console(config-if)#end

Console#show interfaces status port-channel 1

Information of Trunk 1

Basic Information:

Port Type : 1000BASE-T

MAC Address : 12-34-12-34-12-3F

Configuration:

Name :

Port Admin : Up

Speed-duplex : Auto

Capabilities : 10half, 10full, 100half, 100full

Broadcast Storm : Enabled

Broadcast Storm Limit : 64 Kbits/second
```

```
Multicast Storm : Disabled

Multicast Storm Limit : 64 Kbits/second

Unknown Unicast Storm : Disabled

Unknown Unicast Storm Limit : 64 Kbits/second

Flow Control : Disabled

VLAN Trunking : Disabled

Current status:

Created By : LACP

Link Status : Up

Port Operation Status : Up

Operation speed-duplex : 100full

Up Time : 0w 0d 0h 0m 53s (53 seconds)

Flow Control Type : None

Max Frame Size : 1518 bytes (1522 bytes for tagged frames)

Member Ports : Eth1/1, Eth1/2, Eth1/3,

Console#
```

11.2.2 lacp admin-key(Ethernet Interface)

此命令配置端口的 LACP 管理密钥。使用 no 形式恢复默认设置。

语法

lacp {**actor** | **partner**} **admin-key** *key*

no lacp {**actor** | **partner**} **admin-key**

actor - 本地方面的聚合链接。

partner - 聚合链接的远程端。

key - 端口管理密钥必须设置为属于同一链路聚合组(LAG)的端口的相同值。(范围:0-65535)

缺省配置

Actor: 1, Partner: 0

命令模式

接口配置 (Ethernet)

命令用法

◆如果（1）LACP 系统优先级匹配，（2）LACP 端口管理密钥匹配，以及（3）LACP 端口通道密钥匹配（如果已配置），则仅允许端口加入相同的 LAG。

◆ 如果未设置端口通道管理密钥（ lacp 管理密钥 - 端口通道），则 形成通道组（即，其空值为 0），此键设置为与端口管理密钥相同的值（ lacp admin 密钥 - 以太网接口）由加入该组的接口使用。

◆ 一旦建立了链路的远程端， LACP 操作设置就已在该端使用。 为伙伴配置 LACP 设置仅适用于其管理状态，而不适用于其操作状态。

范例

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor admin-key 120
Console(config-if)#
```

11.2.3 lacp port-priority

该命令用来配置 LACP 端口优先级。使用 no 形式恢复默认设置。

语法

lacp {**actor** | **partner**} **port-priority** *priority*

no lacp {**actor** | **partner**} **port-priority**

actor -当地一侧的聚合。

partner -聚合链接的远程端。

priority - LACP 端口优先级用于选择备份链路。（范围：0-65535）

缺省配置

32768

命令模式

接口配置 (Ethernet)

命令用法

◆设置较低的值表示 更高的有效优先级。

◆ 如果活动端口链路断开，则选择具有最高优先级的备用端口来替换已关闭的链路。但是，如果两个或多个端口具有相同的 LACP 端口优先级，则将选择具有最低物理端口号 的端口作为

备份端口。

◆ 如果已存在具有最大允许端口成员数的 LAG，并且随后使用比现有成员更高的优先级在另一个端口上启用 LACP，则新配置的端口将替换 具有较低优先级的现有 port 成员。

◆ 一旦建立了链路的远程端，LACP 操作设置就已在该端使用。为合作伙伴配置 LACP 设置仅适用于其管理状态，而不适用于其操作状态，并且仅在下次与合作伙伴建立聚合链接时生效。

范例

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor port-priority 128
```

11.2.4 lacp system-priority

此命令用于配置端口的 LACP 系统优先级。使用 no 形式恢复默认设置。

语法

lacp {**actor** | **partner**} **system-priority** *priority*

no lacp {**actor** | **partner**} **system-priority**

actor -本地方面的聚合链接。

partner -聚合链接的远程端。

priority -此优先级用于确定链路聚合组（LAG）成员资格，并在 LAG 协商期间将此设备标识给其他交换机。（范围：0-65535）

缺省配置

32768

命令模式

接口配置 (Ethernet)

命令用法

◆必须为端口 配置相同的系统优先级才能加入 sameLAG。

◆系统优先级与交换机的 MAC 地址组合以形成 LAG 标识符。该标识符用于在与其他系统的 LACP 协商期间指示特定 LAG。

◆一旦建立了链接的远程端，LACP 操作设置就已经在该侧使用。为合作伙伴配置 LACP 设置仅适用于其管理状态，而不适用于其操作状态，并且仅在下次与合作伙伴建立聚合链接时生效。

范例

```
Console(config)#interface ethernet 1/5

Console(config-if)#lacp actor system-priority 3

Console(config-if)#
```

11.2.5 lacp admin-key(Port Channel)

此命令配置端口通道的 LACP 管理密钥字符串。使用 no 形式恢复默认设置。

语法

lacp admin-key *key*

no lacp admin-key

key -端口通道管理密钥用于在此交换机上的本地 LACP 设置期间识别特定的链路聚合组（LAG）。（范围：0-65535）

缺省配置

0

命令模式

接口配置 (Port Channel)

命令用法

◆如果（1）LACP 系统优先级匹配，（2）LACP 端口管理密钥匹配，以及（3）LACP 端口通道密钥匹配（如果已配置），则仅允许端口加入相同的 LAG。

◆ 如果未设置端口通道管理密钥（ **lacp 管理密钥** - 端口通道） ，则表示已形成通道组（即，其空值为 0），此键设置为与端口管理密钥相同的值（ lacp admin 密钥 - 以太网接口）由加入该组的接口使用。 请注意，当不再使用 LAG 时，端口通道管理密钥将重置为 0。

范例

```
Console(config)#interface port-channel 1

Console(config-if)#lacp admin-key 3

Console(config-if)#
```

11.3 中继状态显示命令

11.3.1 show lacp

此命令显示 LACP 信息。

语法

show lacp [*port-channel*] {**counters** | **internal** | **neighbors** |**sys-id**}

port-channel -链路聚合组的本地标识符。（范围：1-12）

counters - LACP 协议消息的统计信息。

internal - 本地端的配置设置和操作状态。

neighbors -远程端的配置设置和操作状态。

sys-id -所有通道组的系统优先级和 MAC 地址摘要。

缺省配置

全部

命令模式

特权模式

范例

```
Console#show lacp 1 counters

Port Channel: 1

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

Eth 1/ 2

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

LACPDUs Sent : 12

LACPDUs Received : 6

Marker Sent : 0

Marker Received : 0

LACPDUs Unknown Pkts : 0

LACPDUs Illegal Pkts : 0

...
```

```
Console#show lacp 1 internal

Port Channel : 1

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

Oper Key : 3

Admin Key : 0

Eth 1/ 1

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

LACPDUs Internal : 30 seconds

LACP System Priority : 32768

LACP Port Priority : 32768

Admin Key : 3

Oper Key : 3

Admin State : defaulted, aggregation, long timeout, LACP-activity

Oper State : distributing, collecting, synchronization,

aggregation, long timeout, LACP-activity

...

Console#show lacp 1 neighbors

Port Channel 1 neighbors

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

Eth 1/ 1

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

Partner Admin System ID : 32768, 00-00-00-00-00-00

Partner Oper System ID : 32768, 00-12-CF-61-24-2F

Partner Admin Port Number : 1

Partner Oper Port Number : 1

Port Admin Priority : 32768

Port Oper Priority : 32768

Admin Key : 0

Oper Key : 3

Admin State: defaulted, distributing, collecting,
```

```
synchronization, long timeout,

Oper State: distributing, collecting, synchronization,

aggregation, long timeout, LACP-activity

...

Console#show lacp sysid

Port Channel System Priority System MAC Address

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

1 32768 00-30-F1-8F-2C-A7

2 32768 00-30-F1-8F-2C-A7

3 32768 00-30-F1-8F-2C-A7

4 32768 00-30-F1-8F-2C-A7

5 32768 00-30-F1-8F-2C-A7

6 32768 00-30-F1-8F-2C-A7

7 32768 00-30-F1-D4-73-A0

8 32768 00-30-F1-D4-73-A0

9 32768 00-30-F1-D4-73-A0

10 32768 00-30-F1-D4-73-A0

11 32768 00-30-F1-D4-73-A0

12 32768 00-30-F1-D4-73-A0

...
```

11.3.2 show port-channelload-balance

此命令显示聚合链接上使用的负载分配方法。

命令模式

特权模式

范例

```
Console#show port-channel load-balance

Trunk Load Balance Mode: Destination IP address

Console#
```

12 端口镜像命令

可以使用软件监视工具或硬件探测器从同一交换机上的本地端口或另一台交换机上的远程端口镜像数据，以便在目标端口进行分析。此开关支持以下镜像模式。

12.1 本地端口镜像指令

本节介绍如何从本地设备的源端口到目标端口镜像流量。

12.1.1 port monitor

本节介绍如何镜像从源端口到目标端口的流量。

语法

port monitor {*interface* [**rx** | **tx** | **both**] | **vlan** *vlan-id* |

mac-address *mac-address* | **access-list** *acl-name*}

no port monitor {*interface* | **vlan** *vlan-id* |

mac-address *mac-address* | **access-list** *acl-name*}

interface -**以太网** *单元* / *端口* （源端口）

unit -单位标识符。 （范围：1）

port -端口号。 （范围：1-28）

rx -镜像收到的数据包。

tx -镜像传输的数据包。

both -镜像接收和发送的数据包。

vlan-id - VLAN ID（范围：1-4093）

mac-address - xx-xx-xx-xx-xx-xx 或 xxxxxxxxxxx 形式的 MAC 地址 。

acl-name - ACL 的名称。 （最大长度：16 个字符，不带空格或其他特殊字符）

缺省配置

◆无

◆启用接口时，默认镜像用于 接收和传输的数据包。

◆ 启用 VLAN 或 MAC 地址时，镜像仅限于接收的数据包。

命令模式

接口配置 (Ethernet, destination port)

命令用法

◆您可以将来自任何源端口的流量镜像到目标端口以进行实时分析。然后，您可以将逻辑分析仪或 RMON 安装在目标端口上，并以完全不引人注目的方式研究穿过源端口的流量。

◆ 通过指定与接口配置命令以太网接口设定目的地端口，然后使用 **port mirror** 命令指定流量的源进行镜像。

◆ 镜像来自端口的流量时，镜像端口和监视端口应该匹配，否则可能会从该端口丢弃流量。镜像来自 VLAN 的流量时，流量也可能在重负载下进行。

◆ 当启用 VLAN 镜像和端口镜像时，目标端口可以接收两次镜像数据包； 一次从源镜像端口再次从这样的镜像 VLAN。

◆ 镜像来自 MAC 地址的流量时，具有指定源地址的入口流量进入交换机中除目标端口之外的任何端口，将镜像到目标端口。

◆ 请注意，生成树 BPDU 数据包不会镜像到目标端口。

◆ 基于源 MACaddress 镜像 VLAN 流量或数据包时，目标端口不能设置为与基本端口镜像相同的目标端口。

◆ 您可以创建多个镜像会话，但所有会话必须共享同一目标端口。

◆ 目标端口不能是中继或中继成员端口。

◆ 基于 ACL 的镜像仅用于入口流量。 要镜像 ACL，请按照下列步骤操作：

1. 使用 **access-list** 命令添加 ACL。
2. 使用 **access-group** 命令将镜像端口添加到访问控制列表。
3. 使用 **port monitor access-list** 命令并指定将镜像匹配 ACL 的流量的目标端口。

范例

以下示例将交换机配置为镜像来自端口的所有数据包 6 to 5:

```
Console(config)#interface ethernet 1/5

Console(config-if)#port monitor ethernet 1/6 both

Console(config-if)#
```

12.1.2 show port monitor

此命令显示镜像信息。

语法

show port monitor [*interface* | **vlan** *vlan-id* |

mac-address *mac-address*]

interface -**以太网** *单元* / *端口* （源端口）

unit -单位标识符。 （范围：1）

port -端口号。 （范围：1-28）

vlan-id - VLAN ID（范围：1-4093）

mac-address - xx-xx-xx-xx-xx-xx 或 xxxxxxxxxxx 形式的 MAC 地址。

缺省配置

全部

命令模式

特权模式

命令用法

此命令显示当前配置的源端口，目标端口和镜像模式（即 RX，TX，RX / TX）。

范例

以下显示从端口 6 到端口 5 配置的镜像：

```
Console(config)#interface ethernet 1/5
```

```
Console(config-if)#port monitor ethernet 1/6

Console(config-if)#end

Console#show port monitor

Port Mirroring

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

Destination Port (listen port):Eth1/5

Source Port (monitored port) :Eth1/6

Mode :RX/TX

Console#
```

12.2 远程端口镜像命令

远程交换端口分析器（RSPAN）允许您镜像来自远程交换机的流量，以便在本地目标端口上进行分析。

配置指南

执行以下步骤以配置 RSPAN 会话：

1. 使用 vlan rspan 命令配置用于 RSPAN 的 VLAN（禁止使用缺省 VLAN 1 和交换机集群 VLAN 4093）。
2. 使用 rspan source 命令指定要监视的接口和 traffictype（RX，TX 或两者）。
3. 使用 rspan destination 命令为 RSPAN 会话镜像的流量指定目标端口。
4. 使用 rspan remote vlan 命令指定要在 RSPAN 会话中使用的 VLAN，指定交换机作为镜像流量的源，中间中继或目标的角色，以及配置指定承载此流量的上行链路端口。

RSP AN 限制

以下限制适用于在此交换机上使用 RSPAN：

◆ *RSPAN 端口* - 只能将端口配置为 RSPAN 源，目标或上行链路； 不允许使用静态和动态中继。 Aport 只能配置为一种 RSPAN 接口 - 源，目标或上行链路。 另请注意，源端口和目标端口不能在同一台交换机上配置。只能将 802.1Q 中继或混合（即通用）端口配置为 RSPAN 上行链路或目标端口 - 不允许访问端口（请参阅 switchport 模式 ）。

◆ *本地/远程镜像* - 本地镜像会话的目标（使用 port monitor 命令创建）不能用作 RSPAN 流量的目标。只允许一个镜像会话，包括本地镜像和远程镜像。 如果 启用了 本地镜像 ，则无法为 RSPAN 配置任何会话。

◆ *生成树* - 如果禁用生成树，则 BPDU 不会流入 RSPAN VLAN。当交换机上启用了 RSPAN 时，RSPAN 上行链路端口不支持 MAC 地址学习。 因此如果在配置 RSPAN 后启用了生成树，则不会在

RSPAN 上行链路端口上重新启动 MAC 地址学习。

◆ *IEEE 802.1X* - RSPAN 和 802.1X 是互斥功能。当全局启用 802.1X 时 ，即使仍可配置 RSPAN 源端口和目标端口，也无法配置 RSPAN 上行链路端口。在交换机上启用 RSPAN 上行链路端口时，无法全局启用 802.1X .RSPAN 上行链路端口不能配置为使用 IEEE 802.1X 端口认证，但可以配置 RSPAN 源端口和目标端口以使用它。

◆ *端口安全性* - 如果在任何端口上启用了端口安全性，则该端口无法设置为 RSPAN 上行链路端口，即使它仍可配置为 RSPAN 源或目标端口。 此外当端口配置为 RSPAN 上行链路端口时， 不会在该端口上启用端口安全性 。

12.2.1 rspan source

使用此命令可以指定要镜像的源端口和流量类型。使用 no 形式在指定端口上禁用 RSPAN，或使用无效型关键字禁用指定类型的镜像。

语法

[no] **rspan session** *session-id* **source interface** *interface-list*[**rx** | **tx** | **both**]

session-id - 标识这个 RSPAN 会话的数字。（范围：1）

只允许两个镜像会话，包括本地镜像和远程镜像。如果使用端口监视器命令启用本地镜像，则只有一个会话可用于 RSPAN。

interface-list - 一个或多个源端口。使用连字符表示连续的端口列表或非连续端口之间的逗号。

ethernet *单元* / *端口*

unit - 单位标识符。 （范围：1）

port - 端口号。 （范围：1-28）

rx - 镜像收到的数据包。

tx - 镜像传输的数据包。

both - 镜像接收和发送的数据包。

缺省配置

双向镜像

命令模式

全局配置

命令用法

◆可以在同一台交换机上或不同交换机上将一个或多个源端口分配给同一 RSPAN 会话。

◆ 只能将端口配置为 RSPAN 源-不允许使用静/动态链路聚合端口。

◆ 无法在同一交换机上配置源端口和目标端口。

范例

以下示例将交换机配置为镜像接收的数据包从端口 2 和 3：

```
Console(config)#rspan session 1 source interface ethernet 1/2

Console(config)#rspan session 1 source interface ethernet 1/3

Console(config)#
```

12.2.2 rspan destination

使用此命令指定要监视镜像流的目标端口。使用 no 形式禁用指定端口上的 RSPAN。

语法

rspan session *session-id* **destination interface** *interface* [**tagged** |**untagged**]

no rspan session *session-id* **destination interface** *interface*

session-id - 标识此 RSPAN 会话的数字。（范围：1）

只允许两个镜像会话，包括本地镜像和远程镜像。 如果使用 port monitor 命令 启用了本地镜像 ，则只有一个会话可用于 RSPAN。

interface - **以太网** *单元* / *端口*

unit - 单位标识符。（范围：1）

port - 端口号。（范围：1-28）

tagged - 退出目标端口的流量带有 RSPAN VLANtag。

untagged - 退出目标端口的流量未标记。

缺省配置

未标记

命令模式

全局配置

命令用法

◆在同一交换机上只能配置一个目标端口，但可以在同一会话的多个交换机上配置目标端

口 。

- 只能将 802.1Q 中继或混合（即通用）端口配置为 RSPAN 目标端口-不允许访问端口（请参阅 switchport 模式 ）。
- 只能将端口配置为 RSPAN 目标-不允许使用静态和动态中继。
- 无法在同一交换机上配置源端口和目标端口。
- 目标端口仍然可以发送和接收交换流量，并参与任何第 2 层协议，以便分配它。

范例

以下示例将端口 4 配置为接收镜像 RSPAN 流量：

```
Console(config)#rspan session 1 destination interface ethernet 1/2

Console(config)#
```

12.2.3 rspan remote vlan

使用此命令指定 RSPAN VLAN，交换机角色（源、中间或目标）和上行链路端口。在指定的 VLAN 上 使用**无**表格的 RSPAN。

语法

[no] **rspan session** *session-id* **remote vlan** *vlan-id*
{**source** | **intermediate** | **destination**} **uplink** *interface*

session-id - 标识此 RSPAN 会话的数字。（范围：1）
只允许两个镜像会话，包括本地镜像和远程镜像。 如果使用 port monitor 命令启用了本地镜像 ，则只有一个会话可用于 RSPAN。
vlan-id-配置的 RSPAN VLAN 的 ID。 （范围：2-4092）在使用 此命令启用 RSPAN 之前， 使用 vlan rspan 命令为 RSPANmirroring 保留 VLAN。
source -将此设备指定为 remote mirroredtraffic 的源。
intermediate -将此设备指定为中间交换机，将镜像流量从一个或多个源透明地传递到一个或多个目标。
destination -将此设备指定为配置了 adestination 端口的交换机，该端口用于接收此会话的镜像流量。
uplink -配置为远程接收或传输镜像流量的端口。
interface -**以太网** *单元* / *端口*
ethernet *单元* / *端口*
unit -单位标识符。 （范围：1）
port -端口号。 （范围：1-28）

缺省配置

无

命令模式

全局配置

命令用法

◆只能将 802.1Q 中继或混合（即通用）端口配置为 RSPAN 上行链路端口-不允许访问端口（请参阅 switchportmode ）。

◆ 源交换机上只能配置一个上行端口，但中间或目的交换机上配置的上行端口数量没有限制 。

◆ 交换机仅为此 VLAN 分配目标和上行链路端口。 无法使用 switchport allowed vlan 命令将端口手动分配给 RSPANVLAN。也不是 GVRP 动态地将端口成员添加到 RSPAN VLAN。另请注意，show vlan 命令不会显示 RSPAN VLAN 的任何成员，但仅显示已配置的 RSPAN VLAN 标识符。

范例

以下示例在 VLAN 2 上启用 RSPAN，将此设备指定为 RSPAN 目标交换机，将上行链路接口指定为端口 3：

```
Console(config)#rspan session 1 remote vlan 2 destination uplink ethernet 1/3
Console(config)#
```

12.2.4 no rspan session

使用此命令删除已配置的 RSPAN 会话。

语法

no rspan session *session-id*

session-id - 标识此 RSPAN 会话的数字。（范围：1）

只允许两个镜像会话，包括本地镜像和远程镜像。如果使用 port monitor 命令启用了本地镜像 ，则只有一个会话可用于 RSPAN。

命令模式

全局配置

命令用法

在**没有 RSPAN 会话**命令必须使用禁用 RSPAN VLAN 之前它可以从 VLAN 数据库（见 vlan 命令）被删除 。

范例

```
Console(config)#no rspan session 1
Console(config)#
```

12.2.5 show rspan

使用此命令可显示 RSPAN 会话的配置设置。

语法

show rspan session [*session-id*]

session-id - 标识此 RSPAN 会话的数字。（范围：1）

只允许两个镜像会话，包括本地镜像和远程镜像。如果使用 port monitor 命令启用了本地镜像 ，则只有一个会话可用于 RSPAN。

命令模式

特权模式

范例

```
Console#show rspan session

RSPAN Session ID : 1

Source Ports (mirrored ports) : None

RX Only : None

TX Only : None

BOTH : None

Destination Port (monitor port) : Eth 1/2

Destination Tagged Mode : Untagged

Switch Role : Destination

RSPAN VLAN : 2

RSPAN Uplink Ports : Eth 1/3

Operation Status : Up

Console#
```

13 速率限制命令

此功能允许网络管理员控制在接口上发送或接收的最大速率。在网络边缘的接口上配置速率限制，以限制流入或流出网络的流量。超出可接受流量的数据包将被丢弃。
速率限制可以应用于单个端口或中继。使用此功能配置接口时，将通过硬件监控流量速率以验证是否符合要求。不合规的流量被丢弃。

13.1.1 rate-limit

此命令定义特定接口的速率限制。使用此命令而不指定恢复默认速率的速率。使用 no 形式恢复已禁用的默认状态。

语法

rate-limit {**input** | **output**} [*rate*]

no rate-limit {**input** | **output**}

input - 指定接口的输入速率

output - 指定接口的输出速率

rate - 以 Kbps 为单位的最大值。(范围：千兆以太网端口为 64 - 1,000,000 kbits /秒; 10 - 千兆以太网端口为 64 - 10,000,000 kbits /秒)

缺省配置

禁用

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

在同一界面上同时使用速率限制和风暴控制可能会导致意外结果。例如，假设通过命令“switchport broadcast packet-rate 500”将广播风暴控制设置为 500 Kbps，并且通过快速

以太网端口上的“速率限制输入 20000”命令将速率限制设置为 20000 Kbps。自 20000 Kbps 以来是速度的 1/5（100 Mbps），接收速率实际上是 100 Kbps，或　风暴控制命令设置的 500 Kbps 限制的 1/5　。因此不建议同时使用这两个命令接口。

范例

```
Console(config)#interface ethernet 1/1

Console(config-if)#rate-limit input 64

Console(config-if)#
```

14 自动流量控制命令

自动流量控制（ATC）为广播和多播风暴配置边界阈值，可用于触发配置限制或关闭端口。

14.1 阈值命令

14.1.1 auto-traffic-controlapply-timer

此命令设置应用控制响应后续流量超过上限阈值的时间。使用 no 形式恢复默认设置。

语法

auto-traffic-control {**broadcast** | **multicast**} **apply-timer** *seconds*

no auto-traffic-control {**broadcast** | **multicast**} **apply-timer**

broadcast - 指定广播流量的自动风暴控制。

multicast - 指定组播流量的自动风暴控制。

seconds - 超出上限阈值后应用控制响应的时间间隔。（范围：1-300 秒）

缺省配置

300 秒

命令模式

全局配置

命令用法

应用定时器超时后，可以触发 auto-traffic-control 动作 命令 指定的 控制动作， 并发送 snmp-server enable port-traps atc broadcast-control-apply 命令或 snmp-server enable 端口发送的告警消息 -traps atc multicast-control-apply 命令。

范例

此示例将所有端口的应用计时器设置为 200 秒。

```
Console(config)#auto-traffic-control broadcast apply-timer 200

Console(config)#
```

14.1.2 auto-traffic-controlrelease-timer

此命令设置释放控制响应的时间，后续流量低于下限阈值。使用 no 形式恢复默认设置。

语法

auto-traffic-control {**broadcast** | **multicast**}**release-timer** *seconds*

no auto-traffic-control {**broadcast** | **multicast**} **release-timer**

broadcast - 指定广播流量的自动风暴控制。

multicast - 指定组播流量的自动风暴控制。

秒 - 释放控制响应后续流量低于下限阈值的时间。（范围：1-900 秒）

缺省配置

900 秒

命令模式

全局配置

命令用法

此命令设置延迟，在此之后可以终止控制响应。必须使用 auto-traffic-control auto-control-release 命令来启用或禁用控制响应的速率限制的自动释放。 要重新启用已通过 automatictraffic 控制关闭的端口，必须使用 auto-traffic - control control-release 命令 手动重新启用端口 。

范例

此示例将所有端口的释放计时器设置为 800 秒。

```
Console(config)#auto-traffic-control broadcast release-timer 800

Console(config)#
```

14.1.3 auto-traffic-control

此命令启用广播或多播风暴的自动流量控制。使用 no 形式禁用此功能。

语法

[no] auto-traffic-control {broadcast | multicast}

broadcast - 指定广播流量的自动风暴控制。

multicast - 指定组播流量的自动风暴控制。

缺省配置

禁用

命令模式

接口配置 (Ethernet)

命令用法

◆可以为广播或多播流量启用自动风暴控制。它不能同时为这两种流量类型启用。

◆自动风暴控制是一种软件级控制功能。也可以使用 switchport packet-rate 命令在硬件级别控制 Trafficstorms。但是这些控制类型中只有一个可以应用于端口。在端口上启用自动风暴控制将禁用该端口上的硬件级风暴控制。

范例

此示例为 port1 上的广播流量启用自动风暴控制。

```
Console(config)#interface ethernet 1/1

Console(config-if)#auto-traffic-control broadcast

Console(config-if)#
```

14.1.4 auto-traffic-controlaction

此命令设置控制操作以限制入口流量或关闭违规端口。使用 no 形式恢复默认设置。

语法

auto-traffic-control {broadcast | multicast}action {rate-control | shutdown}

no auto-traffic-control {broadcast | multicast} action

broadcast -指定广播流量的自动风暴控制。

multicast - 指定组播流量的自动风暴控制。

rate-control -如果触发控制响应,则根据 auto - traffic-control alarm-clear-threshold 命令配置的阈值限制流入限制的速率 。

shutdown -如果触发控制响应，则管理端口被禁用。通过自动流量控制禁用的端口只能手动重新启用。

缺省配置

速率控制

命令模式

接口配置（Ethernet）

命令用法

◆超过上限阈值且应用定时器超时时，将根据此命令触发 acontrol 响应。

◆当控制响应通过此命令设置为速率限制时，速率限制由 auto-traffic-control alarm-clear-threshold 命令确定。

◆如果控制响应是限制入口流量的速率，则一旦流量速率低于较低阈值并且释放定时器已到期，它就可以自动终止。

◆如果端口已被控制响应停机，也不会被重新-通过自动交通控制功能。它只能使用 auto-traffic-control control-release 命令手动重新启用 。

范例

此示例设置端口 1 上广播流量的控制响应。

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast action shutdown
Console(config-if)#
```

14.1.5 auto-traffic-controlalarm-clear-threshold

此命令设置入口流量的下限阈值，如果由 auto-traffic-control auto-control-release 命令配置，则在释放 Timerexpires 之后将释放速率限制的 acontrol 响应。使用 no 形式恢复默认设置。

语法

auto-traffic-control {**broadcast** | **multicast**}**alarm-clear-threshold** *threshold*

no auto-traffic-control {**broadcast** | **multicast**}**alarm-clear-threshold**

broadcast - 指定广播流量的自动风暴控制。

multicast - 指定组播流量的自动风暴控制。

threshold - 发送 acleared 风暴控制陷阱的入口流量的下限阈值。（范围：1-255 千包秒）

缺省配置

每秒 128 千包

命令模式

接口配置（Ethernet）

命令用法

◆ 一旦流量速率低于下限保持，如果由 snmp-server enable port-traps atcbroadcast-alarm-clear 命令或 snmp-server enable port-traps atcmulticast-alarm-clear 命令配置，则可能会发送陷阱消息 。

◆ 如果将速率限制配置为控制响应，则在流量速率低于低阈值后，它将停止运行，并且释放计时器已到期。请注意，如果某个端口已被控制响应关闭，则不会通过自动流量控制重新启用该端口。它只能使用 auto-traffic-control control-release 命令手动重新启用 。

范例

此示例为端口 1 上的广播流量设置自动风暴控制的清除阈值。

```
Console(config)#interface ethernet 1/1

Console(config-if)#auto-traffic-control broadcast alarm-clear-threshold 155

Console(config-if)#
```

14.1.6 auto-traffic-controlalarm-fire-threshold

此命令设置入口流量的上限阈值，超过该阈值，应用定时器到期后将触发控制响应。 使用 no 形式恢复默认设置。

语法

auto-traffic-control {**broadcast** | **multicast**}**alarm-fire-threshold** *threshold*

no auto-traffic-control {**broadcast** | **multicast**}**alarm-fire-threshold**

broadcast - 指定广播流量的自动风暴控制。

multicast - 指定组播流量的自动风暴控制。

threshold - 应用定时器到期后触发 astorm 控制响应的入口流量上限阈值（范围：每秒 1-255 千包）

缺省配置

每秒 128 千包

命令模式

接口配置（Ethernet）

命令用法

◆一旦超过上限阈值，如果由 snmp-server enable port-traps atc broadcast-alarm - fire 命令或 snmp-server enable port-traps atc multicast-alarmfire 命令配置，则可能会发送陷阱消息 。

◆超过上限阈值后，如果 auto-traffic - control action 命令配置了控制响应，则控制定时器必须按照 auto-traffic-control apply-timer 命令配置为首次过期。

范例

此示例为端口 1 上的广播流量设置自动风暴控制的触发阈值。

```
Console(config)#interface ethernet 1/1

Console(config-if)#auto-traffic-control broadcast alarm-fire-threshold 255

Console(config-if)#
```

14.1.7 auto-traffic-controlauto-control-release

此命令会在 auto-traffic-control release-timer 命令指定的时间到期后自动释放限速控制响应 。

语法

auto-traffic-control {broadcast | multicast}auto-control-release

broadcast - 指定广播流量的自动风暴控制。

multicast - 指定组播流量的自动风暴控制。

命令模式

接口配置（Ethernet）

命令用法

◆此命令可用于在触发指定操作并且计时器已过期后自动停止控制响应限制。

◆要释放在触发指定操作并且释放计时器已过期后已关闭端口的控制响应，请使用 auto-traffic-control control-release 命令。

范例

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast auto-control-release
Console(config-if)#
```

14.1.8 auto-traffic-controlcontrol-release

此命令手动释放控制响应。

语法

auto-traffic-control {broadcast | multicast} control-release

broadcast - 指定广播流量的自动风暴控制。

multicast - 指定组播流量的自动风暴控制。

命令模式

接口配置 (Ethernet)

命令用法

该命令可以用于手动停止率的控制响应 - 限制或端口的关闭的任何时间指定的动作已被触发之后。

范例

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast control-release
Console(config-if)#
```

14.2 SNMP 陷阱命令

14.2.1 snmp-server enableport-traps atcbroadcast-alarm-clear

在触发风暴控制响应后，当广播流量低于低阈值时，此命令发送陷阱。使用 no 形式禁用此陷阱。

语法

[no] snmp-server enable port-traps atc broadcast-alarm-clear

缺省配置

禁用

命令模式

接口配置（Ethernet）

范例

```
Console(config)#interface ethernet 1/1

Console(config-if)#snmp-server enable port-traps atc broadcast-alarm-clear

Console(config-if)#
```

14.2.2 snmp-server enableport-traps atcbroadcast-alarm-fire

当广播流量超过自动风暴控制的上阈值时，此命令发送陷阱。使用 no 形式禁用此陷阱。

语法

[no] snmp-server enable port-traps atc broadcast-alarm-fire

缺省配置

禁用

命令模式

接口配置（Ethernet）

范例

```
Console(config)#interface ethernet 1/1

Console(config-if)#snmp-server enable port-traps atc broadcast-alarm-fire

Console(config-if)#
```

14.2.3 snmp-server enableport-traps atcbroadcast-control-apply

当广播流量超过自动风暴控制的上阈值且应用定时器到期时，此命令发送陷阱。使用 no 形式禁用此陷阱。

语法

[no] snmp-server enable port-traps atc broadcast-control-apply

缺省配置

禁用

命令模式

接口配置（Ethernet）

范例

```
Console(config)#interface ethernet 1/1

Console(config-if)#snmp-server enable port-traps atc broadcast-control-apply

Console(config-if)#
```

14.2.4 snmp-server enableport-traps atcbroadcast-control-release

在触发风暴控制响应并且计时器到期后，当广播流量低于低阈值时，此命令发送陷阱。使用 no 形式禁用此陷阱。

语法

[no] snmp-server enable port-traps atc

broadcast-control-release

缺省配置

禁用

命令模式

接口配置（Ethernet）

范例

```
Console(config)#interface ethernet 1/1

Console(config-if)#snmp-server enable port-traps atc broadcast-control-release

Console(config-if)#
```

14.2.5 snmp-server enableport-traps atcmulticast-alarm-clear

在触发风暴控制响应后，当组播流量低于低阈值时，此命令发送陷阱。使用 no 形式禁用此陷阱。

语法

[no] snmp-server enable port-traps atc multicast-alarm-clear

缺省配置

禁用

命令模式

接口配置（Ethernet）

范例

```
Console(config)#interface ethernet 1/1

Console(config-if)#snmp-server enable port-traps atc multicast-alarm-clear

Console(config-if)#
```

14.2.6 snmp-server enableport-traps atcmulticast-alarm-fire

当组播流量超过自动风暴控制的上限阈值时，此命令发送陷阱。使用 no 形式禁用此陷阱。

语法

[no] snmp-server enable port-traps atc multicast-alarm-fire

缺省配置

禁用

命令模式

接口配置（Ethernet）

范例

```
Console(config)#interface ethernet 1/1

Console(config-if)#snmp-server enable port-traps atc multicast-alarm-fire

Console(config-if)#
```

14.2.7 snmp-server enableport-traps atcmulticast-control-apply

当组播流量超过自动风暴控制的上限阈值且应用定时器到期时，此命令发送陷阱。使用 no 形式禁用此陷阱。

语法

[no] snmp-server enable port-traps atc multicast-control-apply

缺省配置

禁用

命令模式

接口配置（Ethernet）

范例

```
Console(config)#interface ethernet 1/1

Console(config-if)#snmp-server enable port-traps atc multicast-control-apply

Console(config-if)#
```

14.2.8 snmp-server enableport-traps atcmulticast-control-release

在触发风暴控制响应并且计时器到期后，当组播流量低于低阈值时，此命令发送陷阱。使用 no 形式禁用此陷阱。

语法

[no] snmp-server enable port-traps atcmulticast-control-release

缺省配置

禁用

命令模式

接口配置（Ethernet）

范例

```
Console(config)#interface ethernet 1/1

Console(config-if)#snmp-server enable port-traps atc multicast-control-release

Console(config-if)#
```

14.3 ATC 显示命令

14.3.1 show auto-traffic-control

此命令显示自动目前暴控制的全局配置设置。

命令模式

特权模式

范例

```
Console#show auto-traffic-control

Storm Control Broadcast

Apply Timer (sec) : 300

Release Timer (sec) : 900

Storm Control Multicast

Apply Timer (sec) : 300

Release Timer (sec) : 900

Console#
```

14.3.2 show auto-traffic-control interface

此命令显示指定端口的接口配置设置和风暴控制状态。

语法

show auto-traffic-control interface [*interface*]

interface

ethernet *unit/port*

unit -单位标识符。 （范围：1）

port -端口号。 （范围：1-28）

命令模式

特权模式

范例

```
Console#show auto-traffic-control interface ethernet 1/1
```

```
Eth 1/1 Information
--------------------------------------------------------------------------
Storm Control: Broadcast Multicast
State: Disabled Disabled
Action: Rate Control Rate Control
Auto Release Control: Disabled Disabled
Alarm Fire Threshold(Kpps): 128 128
Alarm Clear Threshold(Kpps):128 128
Trap Storm Fire: Disabled Disabled
Trap Storm Clear: Disabled Disabled
Trap Traffic Apply: Disabled Disabled
Trap Traffic Release: Disabled Disabled
--------------------------------------------------------------------------
Console#
```

15 回路检测命令

可以将交换机配置为检测由硬件问题或协议设置错误引起的一般环回条件。 启用后，将在参与端口上传输控制帧，并且交换机监视入站流量以查看帧是否已循环回来。

使用指南

◆可以调整控制帧发送间隔和恢复的默认设置，以提高特定环境的性能。一旦确定要回送哪种类型的数据包，也可能需要更改关闭模式。

◆本节描述的命令提供的一般环回检测和生成树协议提供的环回检测不能同时启用。如果对生成树协议启用环回检测，则不能在同一接口上启用常规环回检测。

◆当在接口上检测到环回事件或者由于环回事件导致接口从关闭状态释放时，将发送陷阱消息并将事件记录在系统日志中。

◆必须在全局和接口上启用环回检测才能使 环回检测生效。

15.1.1 loopback-detection

此命令在交换机或指定接口上全局启用环回检测。使用 no 形式禁用环回检测。

语法

[no] loopback-detection

缺省配置

禁用

命令模式

全局配置

接口配置 (Ethernet, Port Channel)

命令用法

必须通过此命令为交换机全局启用环回检测，并启用此特定接口以使此功能生效。

范例

此示例启用交换机上的常规环回检测，为端口 1 上的生成树协议提供禁用回路检测，然后启用该端口的常规环回检测。

```
Console(config)#loopback-detection

Console(config)#interface ethernet 1/1

Console(config-if)#no spanning-tree loopback-detection

Console(config-if)#loopback-detection

Console(config)#
```

15.1.2 loopback-detection mode

此命令通过丢弃在环回状态下检测到的端口的数据包或通过丢弃属于在环回状态下检测到的 VLAN 的数据包来指定关闭。使用 no 形式恢复默认设置。

语法

loopback-detection mode {**port-based** | **vlan-based**}

no loopback-detection mode

port-based -在端口上检测到环回时，端口会自动关闭。

vlan-based -当在特定 VLAN 成员的端口上检测到环回时，属于该 VLAN 的数据包将被丢弃到端口。

缺省配置

基于端口

命令模式

全局配置

命令用法

◆使用基于 vlan 的模式时，根据端口的 VLAN 成员资格类型，环回检测控制帧被标记或标记。

◆ 使用基于 vlan 的模式时，如果 switchport ingress-filtering 命令尚未启用，则会自动启用端口的入口过滤。当禁用环回检测时，将恢复端口的入口过滤原始设置。

◆当环回检测模式改变时，无论剩余的恢复时间如何，通过环回检测过程置于关闭状态的任何端口都将立即恢复运行。

范例

此示例将环回检测模式设置为基于 VLAN。

```
Console(config)#loopback-detection mode vlan-based

Console(config)#
```

15.1.3 loopback-detection recover-time

此命令指定交换机自动从关闭状态释放接口之前要等待的时间间隔。使用 no 形式恢复默认设置。

语法

loopback-detection recover-time *seconds*

no loopback-detection recover-time

seconds -关闭状态的恢复时间。（范围：60-1,000,000 秒，或 0 表示禁用自动恢复）

缺省配置

60 秒

命令模式

全局配置

命令用法

◆当环回检测模式改变时，无论剩余的恢复时间如何，环回检测过程中任何处于关闭状态的端口都将立即恢复运行。

◆如果恢复时间设置为零，则可以使用 loopback-detection release 命令将处于关闭状态的所有端口恢复为运行状态。要还原特定端口，请使用 no shutdown 命令。

范例

```
Console(config)#loopback-detection recover-time 120

Console(config-if)#
```

15.1.4 loopback-detection transmit-interval

此命令指定传输环回检测控制帧的时间间隔。使用 no 形式恢复默认设置。

语法

loopback-detection transmit-interval *seconds*

[no] loopback-detection transmit-interval

seconds - 环回检测控制帧的传输间隔。（范围：1-32767 秒）

缺省配置

10 秒

命令模式

全局配置

范例

```
Console(config)#loopback-detection transmit-interval 60

Console(config)#
```

15.1.5 loopback-detection release

此命令释放当前由环回检测功能关闭的所有接口。

语法

loopback-detection release

命令模式

特权模式

范例

```
Console#loopback-detection release

Console(config)#
```

15.1.6 show loopback-detection

此命令显示交换机或指定接口的环回检测配置设置。

语法

show loopback-detection [*interface*]

interface

ethernet *unit/port*

unit -单位标识符。（范围：1）

port -端口号。（范围：1-28）

命令模式

特权模式

范例

```
Console#show loopback-detection

Loopback Detection Global Information

Global Status : Enabled

Transmit Interval : 10

Recover Time : 60

Mode : Port-based

Loopback Detection Port Information

Port Admin State Oper State

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

Eth 1/ 1 Enabled Normal

Eth 1/ 2 Disabled Disabled

Eth 1/ 3 Disabled Disabled

...

Console#show loopback-detection ethernet 1/1

Loopback Detection Information of Eth 1/1

Admin State : Enabled

Oper State : Normal

Console#
```

16 单向链接检测

交换机可配置为检测和禁用单向以太网光纤或铜缆链路。启用后，协议会通告端口的身份并了解特定 LAN 网段上的邻居； 并存储有关缓存中其邻居的信息。 它还可以在需要快速通知或重新同步缓存信息的情况下发送回声消息的响应。

16.1.1 udld message-interval

此命令配置 UDLD 探测消息之间的消息间隔，用于广告阶段中的端口并确定为双向性。 使用 no 形式恢复默认设置。

语法

udld message-interval *message-interval*

no message-interval

message-interval - 端口发送 UDLD 探测的间隔链接或检测阶段后的消息。（范围：7-90 秒）

缺省配置

15 秒

命令模式

全局配置

命令用法

在检测阶段，消息以每秒一个的最大速率进行交换。之后如果协议达到稳定状态并确定链路是双向的，则消息间隔基于称为 M1（t）的曲线增加到可配置值，该曲线是 RFC 5171 中描述的基于时间的函数。

如果在检测阶段结束时认为链路不是双向的,则该曲线变为具有固定值 Mfast(7 秒)的扁平线。

如果链路被认为是双向的，则曲线将使用 Mfast 用于前四个后续消息传输，然后转换为用于所有其他稳态传输的 Mlowlow 值。Mslow 是此命令配置的值。

范例

此示例将消息间隔设置为 10 秒。

```
Console(config)#udld message-interval 10

Console(config)#
```

16.1.2 udld aggressive

此命令将 UDLD 设置为接口上的主动模式。使用 no 形式恢复默认设置。

语法

[no] udld aggressive

缺省配置

禁用

命令模式

接口配置 (Ethernet Port)

命令用法

UDLD 可以在两种模式下运行：正常模式和积极模式。

◆ 在正常模式下，在检测过程结束时确定链接状态始终基于 UDLD 消息中收到的信息：是否有关于正确邻居识别交换的信息或缺少此类信息。 因此，虽然通过 atimer 确定，正常模式确定总是基于收集信息，因此是“基于事件的”。如果不能获得这样的信息（例如，由于双向连接丢失），UDLD 遵循保守的方法最小化在检测过程中误报并认为端口处于“未确定”状态。换句话说，正常模式只有在可以长时间明确确定关联链路出现故障时才会关闭端口。

◆ 在主动模式下，如果 UDLD 在相同的延长时间内失去与邻居的双向连接（如上面针对正常模式所述的那样），UDLD 也将关闭端口，并且随后重复最后尝试重新建立与另一端的通信的链接。 这种操作模式假设与邻居的通信丢失本身就是一个有意义的网络事件，并且是严重连接 问题 的症状。因为这种类型的检测可以是无事件的，并且缺乏信息并不总是与链路的实际故障相关联，所以此模式是可选的，仅建议在某些情况下（通常仅在两点之间的通信失败的点对点链路上）。邻居是可以接受的）。

范例

此示例在端口 1 上启用 UDLD 主动模式。

```
Console(config)#interface ethernet 1/1
Console(config-if)#udld aggressive
Console(config-if)#
```

16.1.3 udld port

此命令在接口上启用 UDLD。使用 no 形式在接口上禁用 UDLD。

语法

[no] udld port

缺省配置

禁用

命令模式

接口配置 (Ethernet Port)

命令用法

◆UDLD 要求所有连接到同一 LAN 的设备 segmentbe 运行协议，以便为潜在的错误 S- 构型，以被检测到的和采取迅速的纠正措施。

◆ 每当 UDLD 设备获知新邻居或接收来自不同步邻居的同步请求时，它（重新）启动连接侧的检测过程并发送 N 个回应消息。（这种机制隐含地假设 N 个数据包足以通过链路到达另一端，尽管它们中的一些可能在传输过程中被丢弃。）

由于此行为在所有邻居上必须相同，因此回声的发送方期望在回复中接收回声。如果检测过程结束而没有接收到适当的回波信息，则认为链路是单向的。

范例

```
Console(config)#interface ethernet 1/1

Console(config-if)#udld port

Console(config-if)#
```

16.1.4 show udld

此命令显示交换机或指定接口的 UDLD 配置设置和操作状态。

语法

show udld [**interface** *interface*]

interface

ethernet *unit/port*

unit -单位标识符。（范围：1）

port -端口号。（范围：1-28）

命令模式

特权模式

范例

```
Console#show udld
```

```
Message Interval : 15
Interface UDLD Mode Oper State Msg Invl
Port State Timeout
--------- -------- ---------- ---------------------------------- --------
Eth 1/ 1 Enabled Aggressive Advertisement 15 s
Bidirectional 5 s
Eth 1/ 2 Disabled Normal Disabled 7 s
Unknown 5 s
Eth 1/ 3 Disabled Normal Disabled 7 s
Unknown 5 s
Eth 1/ 4 Disabled Normal Disabled 7 s
Unknown 5 s
Eth 1/ 5 Disabled Normal Disabled 7 s
Unknown 5 s
...
Console#show udld interface ethernet 1/1
Interface UDLD Mode Oper State Msg Invl
Port State Timeout
--------- -------- ---------- ---------------------------------- --------
Eth 1/ 1 Enabled Aggressive Advertisement 15 s
Bidirectional 5 s
Console#
```

17 地址表管理命令

这些命令用于配置过滤器指定地址的地址表，显示当前条目，清除表，以及老化时间。

17.1.1 mac-address-table aging-time

此命令设置地址表中条目的老化时间。使用 no 形式恢复默认的老化时间。

语法

mac-address-table aging-time *seconds*

no mac-address-table aging-time

seconds -老化时间。 （范围：6-672 秒；0 表示禁用老化）

缺省配置

300 秒

命令模式

全局配置

命令用法

老化时间用于老化动态学习的转发信息。

范例

```
Console(config)#mac-address-table aging-time 100
Console(config)#
```

17.1.2 mac-address-table static

此命令将静态地址映射到 VLAN 中的目标端口。使用 no 表格删除地址。

语法

mac-address-table static *mac-address* **interface** *interface***vlan** *vlan-id* [*action*]

no mac-address-table static *mac-address* **vlan** *vlan-id*

mac-address - MAC address.

interface

ethernet *单元 / 端口*

unit -单位标识符。(范围：1)

port -端口号。(范围：1-28)

port-channel *channel-id*(范围：1-12)

vlan-id - VLAN ID(范围：1-4093)

action - 响应。

delete-on-reset -分配持续到重置开关。

permanent -作业是永久性的。

缺省配置

没有定义静态地址。默认模式是**永久性的**。

命令模式

全局配置

命令用法

可以将主机设备的静态地址分配给特定 VLAN 中的特定端口。使用此命令将静态地址添加到 MAC 地址表。静态地址具有以下特征：

- 当 agiven 接口链路断开时，静态地址不会从地址表中删除。
- 静态地址绑定到指定的接口，不会被移动。当在另一个接口上看到静态地址时，将忽略该地址，并且不会将该地址写入该地址。
- 在使用 no 命令删除地址之前，无法在另一个端口上学习静态地址 。

范例

```
Console(config)#mac-address-table static 00-e0-29-94-34-de interface ethernet
```

```
1/1 vlan 1 delete-on-reset

Console(config)#
```

17.1.3 clear mac-address-table dynamic

此命令从转发数据库中删除所有已学习的条目。

缺省配置

无

命令模式

特权模式

范例

```
Console#clear mac-address-table dynamic

Console#
```

17.1.4 show mac-address-table

此命令显示桥转发数据库中的条目类。

语法

show mac-address-table [**address** *mac-address* [*mask*]][**interface** *interface*] [**vlan** *vlan-id*][**sort** {**address** | **vlan** | **interface**}]

mac-address - MAC 地址。

mask -要在地址中匹配的位。

interface

ethernet *单元* / *端口*

unit -单位标识符。（范围：1）

port -端口号。（范围：1-28）

port-channel *channel-id* （范围：1-12）

vlan-id - VLAN ID (范围: 1-4093)

sort -按地址，vlan 或接口排序。

缺省配置

无

命令模式

特权模式

命令用法

◆MAC 地址表包含与接口关联的 MAC 地址。请注意，“类型”字段可能包含以下类型：

- 学习-动态地址条目
- 配置-静态输入

◆ 掩码应为 xx-xx-xx-xx-xx-xx 形式的 十六进制数字（表示等价 物质掩码），应用于指定的 MAC 地址。 输入十六进制数，其中等效的二进制位“0”表示匹配一位，“1”表示忽略一位。 例如，00-00-00-00-00-00 的掩码表示完全匹配，FF-FF-FF-FF-FF-FF 的掩码表示“任何”。

◆ 最大地址条目数为 16K。

范例

```
Console#show mac-address-table

Total entry in system: 3

Interface MAC Address VLAN Type Life Time

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

CPU 00-E0-00-00-00-01 1 CPU Delete on Reset

Eth 1/ 1 00-E0-0C-10-90-09 1 Learn Delete on Timeout

Eth 1/ 1 00-E0-29-94-34-64 1 Learn Delete on Timeout

Console#
```

17.1.5 show mac-address-table aging-time

此命令显示地址表中条目的老化时间。

缺省配置

无

命令模式

特权模式

范例

```
Console#show mac-address-table aging-time

Aging Status : Enabled
```

```
Aging Time: 300 sec.

Console#
```

17.1.6 show mac-address-table count

此命令显示已使用的 MAC 地址数以及整个系统或接口的可用 MAC 地址数。

语法

show mac-address-table count interface *interface*

interface

ethernet *单元 / 端口*

unit -单位标识符。(范围: 1)

port -端口号。(范围: 1-28)

port-channel *channel-id* (范围: 1-12)

缺省配置

无

命令模式

特权模式

范例

```
Console#show mac-address-table count interface ethernet 1/1

MAC Entries for Port ID :1

Dynamic Address Count :2

Total MAC Addresses :2

Total MAC Address Space Available: 16384

Console#
```

18 生成树命令

本节包括为交换机全局配置 Spanning Tree Algorithm（STA）的命令，以及为所选接口配置 STA 的命令。

18.1.1 spanning-tree

此命令为交换机全局启用生成树算法。使用 no 形式禁用它。

语法

[no] spanning-tree

缺省配置

启用

命令模式

全局配置

命令用法

生成树算法（STA）可用于检测和禁用网络环路，并提供交换机，网桥或路由器之间的备份链路。 这允许交换机与网络中的其他桥接设备（即，符合 STA 的交换机，网桥或路由器）进行交互，以确保网络上任意两个站之间只存在一条路由，并提供备用链路，这些链路在主网络上自动接管链接下来。

范例

此示例显示如何为切换启用生成树算法：

```
Console(config)#spanning-tree
Console(config)#
```

18.1.2 spanning-tree cisco-prestandard

此命令将生成树操作配置为与 Cisco 预标准版本兼容。使用 no 形式恢复默认设置。

语法

[no] spanning-tree cisco-prestandard

缺省配置

禁用

命令模式

全局配置

命令用法

Cisco IOS 版本 12.2（25）SEC 之前的思科预标准版本不符合 IEEE 标准，导致某些状态机程序功能不正确。该命令以与 Cisco 预标准版本兼容的方式强制生成树协议功能。

范例

```
Console(config)#spanning-tree cisco-prestandard

Console(config)#
```

18.1.3 spanning-tree forward-time

此命令用于为此交换机全局配置生成树网桥转发时间。使用 no 形式恢复默认值。

语法

spanning-tree forward-time *seconds*

no spanning-tree forward-time

seconds -以秒为单位的时间。（范围：4 - 30 秒）。最小值是 4 或[（max-age / 2）+ 1]中的较高者。

缺省配置

15 秒

命令模式

全局配置

命令用法

此命令设置端口在更改状态之前等待的最长时间（以秒为单位）（即，丢弃到学习转发）。需要此延迟是因为每个设备必须在开始转发帧之前接收有关拓扑更改的信息。此外，每个端口都需要时

间来监听会使其返回到灾难状态的冲突信息;否则可能会导致临时数据循环。

范例

```
Console(config)#spanning-tree forward-time 20
Console(config)#
```

18.1.4 spanning-tree hello-time

此命令用于配置全局生成的生成树网桥 hello 时间。使用 no 形式恢复默认值。

语法

spanning-tree hello-time *time*

no spanning-tree hello-time

time -以秒为单位的时间。(范围：1-10 秒)。最大值是 10 或[(max-age / 2) - 1]中的较低值。

缺省配置

2 秒

命令模式

全局配置

命令用法

此命令设置根设备发送配置消息的时间间隔（以秒为单位)。

范例

```
Console(config)#spanning-tree hello-time 5
Console(config)#
```

18.1.5 spanning-tree max-age

此命令用于为此交换机全局配置生成树网桥最大使用期限。使用 no 形式恢复默认值。

语法

spanning-tree max-age *seconds*

no spanning-tree max-age

seconds -以秒为单位的时间。(范围：6-40 秒)

最小值是 6 或[2 x (hello-time + 1)]中的较高者。

最大值是 40 或[2 x（前进时间 - 1）]中的较低值。

缺省配置

20 秒

命令模式

全局配置

命令用法

此命令设置设备在尝试收敛-收敛之前可以等待而不接收配置消息的最长时间（以秒为单位）。所有设备端口（指定端口除外）应定期接收配置消息。任何使 STA 信息老化的端口（在最后一个配置消息中提供）成为连接 LAN 的指定端口。如果是根端口，则从连接到网络的设备端口中选择新的根端口。

范例

```
Console(config)#spanning-tree max-age 40

Console(config)#
```

18.1.6 spanning-tree mode

此命令选择此交换机的生成树模式。使用 no 形式恢复默认值。

语法

spanning-tree mode {**stp** | **rstp** | **mstp**}

no spanning-tree mode

stp - Spanning Tree Protocol (IEEE 802.1D)

rstp - Rapid Spanning Tree Protocol (IEEE 802.1w)

mstp - Multiple Spanning Tree (IEEE 802.1s)

缺省配置

rstp

命令模式

全局配置

命令用法

◆生成树

此选项使用RSTP 设置为STP 强制兼容模式。它使用RSTP 作为内部状态机，但是只发送802.1DBPDU，

这为整个网络创建了一个生成树实例。如果在网络上实现多个 VLAN，则可能会不经意地禁用特定 VLAN 成员之间的路径以防止网络循环，从而隔离组成员。在操作多路复用器时，我们建议选择 MSTP 选项。

◆快速生成树

RSTP 通过监视传入的协议消息并动态调整 RSTP 节点发送的协议消息的类型，支持到 STP 或 RSTP 节点的连接，如下所述：

■STP Mode – 如果交换机在端口迁移延迟定时器过期后接收到 802.1DBPDU，则交换机假定它连接到 802.1D 桥上，并开始仅使用 802.1D BPDU。

■RSTP Mode – 如果 RSTP 在端口上使用 802.1D BPDU，并且在迁移延迟期满后接收到 RSTP BPDU，则 RSTP 重新启动标记延迟计时器，并开始在该端口上使用 RSTP BPDU。

◆多实例生成树

■为了允许多个生成树在网络上操作，必须配置具有相同 MSTP 配置的相关桥集，允许它们参与特定的生成树实例集。

■生成树实例只能存在于兼容 VLAN 实例赋值的桥上。

■在生成树模式之间切换时要小心。更改模式将停止先前模式的所有生成树实例，并在新模式下重新启动系统，从而暂时中断用户通信量。

范例

以下示例将交换机配置为使用快速生成树：

```
Console(config)#spanning-tree mode rstp
Console(config)#
```

18.1.7 spanning-tree pathcost method

此命令配置用于快速生成树和多实例生成树的路径成本方法。使用 no 形式恢复默认值。

语法

spanning-tree pathcost method {**long** | **short**}

no spanning-tree pathcost method

long -指定基于 32 位的值，范围为 1-200,000,000。该方法基于 IEEE 802.1w RapidSpanning 树协议。

short -指定基于 16 位的值，范围为 1-65535。此方法基于 IEEE 802.1 生成树协议。

缺省配置

长算法

命令模式

全局配置

命令用法

◆路径成本法用于确定设备之间的最佳路径。因此应将较低的值分配给连接到较快介质的端口，将较高的值分配给具有较慢介质的端口。

◆路径开销方法适用于所有生成树模型（STP，RSTP 和 MSTP）。具体地长方法可以应用于 STP，因为该模式由 RSTP 的后向兼容模式支持。

范例

```
Console(config)#spanning-tree pathcost method long

Console(config)#
```

18.1.8 spanning-tree priority

此命令为此交换机全局配置生成树优先级。使用 no 形式恢复默认值。

语法

spanning-tree priority *priority*

no spanning-tree priority

priority - 桥梁的优先级。（范围 -0-61440，步长为 4096; 选项：0, 4096, 8192, 12288, 16384, 20480, 24576, 28673, 22768, 36864, 40960, 45056, 49152, 53248, 57344, 61440）

缺省配置

32768

命令模式

全局配置

命令用法

网桥优先级用于选择根设备，根端口和指定端口。具有最高优先级的设备（即较低的数值）成为 STA 根设备。但是如果所有设备具有相同的优先级，则具有最低 MAC 地址的设备将成为根设备。

范例

```
Console(config)#spanning-tree priority 40000

Console(config)#
```

18.1.9 spanning-tree mst configuration

此命令将更改为多生成树（MST）配置模式。

缺省配置

没有 VLAN 映射到任何 MST 实例。

区域名称设置为交换机的 MAC 地址。

命令模式

全局配置

范例

```
Console(config)#spanning-tree mst configuration

Console(config-mstp)#
```

18.1.10 spanning-tree system-bpdu-flooding

此命令将系统配置为在交换机上全局禁用生成树或在特定端口上禁用生成树时，将 BPDU 泛洪到交换机上的所有其他端口，或仅扩散到同一 VLAN 中的所有其他端口。使用 no 形式恢复默认值。

语法

spanning-tree system-bpdu-flooding {**to-all** | **to-vlan**}

no spanning-tree system-bpdu-flooding

to-all -将 BPDU 泛洪到交换机上的所有其他端口。

to-vlan -将 BPDU 泛洪到接收端口的 VLAN 内的所有其他端口（即由端口的 PVID 确定）。

缺省配置

洪泛到同一 VLAN 中的所有其他端口。

命令模式

全局配置

命令用法

如果在端口上禁用了 BPDU 泛洪，则 **spanning-tree system-bpdu-flooding** 命令无效（请参阅 spanning-tree port-bpduflooding 命令）。

范例

```
Console(config)#spanning-tree system-bpdu-flooding

Console(config)#
```

18.1.11 spanning-tree transmission-limit

该命令用来配置连续 RSTP / MSTP BPDU 传输的最小时间间隔。 使用 no 形式恢复默认值。

语法

spanning-tree transmission-limit *count*

no spanning-tree transmission-limit

count -以秒为单位的传输限制。（范围：1-10）

缺省配置

3

命令模式

全局配置

命令用法

此命令限制 BPDU 的最大传输速率。

范例

```
Console(config)#spanning-tree transmission-limit 4

Console(config)#
```

18.1.12 max-hops

此命令用于配置丢弃 BPDU 之前区域内的最大跳数。 使用 no 表单恢复默认值。

语法

max-hops *hop-number*

hop-number -多生成树的最大跳数。（范围：1-40）

缺省配置

20

命令模式

MST 配置

命令用法

通过 STP 和 RSTP 协议将 MSTI 区域视为单个节点。因此，MSTI 区域内 BPDU 的消息时间永远不会改变。 但是，区域内的每个生成树实例以及连接这些实例的内部生成树（IST）使用跳数来指定将传播 BPDU 的最大桥数。每个桥在传递 BPDU 之前将跳数减 1 。当跳数达到零时，消息将被丢弃。

范例

```
Console(config-mstp)#max-hops 30

Console(config-mstp)#
```

18.1.13 mst priority

此命令用于配置生成树实例的优先级。使用 no 形式恢复默认值。

语法

mst *instance-id* **priority** *priority*

no mst *instance-id* **priority**

instance-id -生成树的实例标识符。（范围：0-4094）

priority - 生成树实例的优先级。（范围：0-61440，步长为 4096；选项：0,4096,8192,12288,16384,20480,24576,28673,22768,36864,40960,45056,49152,53248,57344,61440）

缺省配置

32768

命令模式

MST 配置

命令用法

◆MST 优先级用于选择指定实例的根桥和备用桥。具有最高优先级(即最低数值)的设备成为 MSTI 根设备。但是如果所有设备都具有相同的优先级，则具有最低 MAC 地址的设备将成为根设备。

◆ 您可以通过指定优先级为 0 来将此交换机设置为 MSTI 根设备，或者通过指定优先级 16384 将其设置为 MSTI 备用设备 。

范例

```
Console(config-mstp)#mst 1 priority 4096

Console(config-mstp)#
```

18.1.14 mst vlan

此命令将 VLAN 添加到生成树实例。使用 no 形式删除指定的 VLAN。使用没有任何 VLAN 参数的 no 形式删除所有 VLAN。

语法

[no] **mst** *instance-id* **vlan** *vlan-范围*

instance-id -生成树的实例标识符。（范围：0-4094）

vlan-范围 - VLAN 范围。（范围：1-4093）

缺省配置

无

命令模式

MST 配置

命令用法

◆使用此命令将 VLAN 分组为生成树实例。MSTP 为每个实例生成唯一的生成树。这提供了跨网络的多个路径，从而平衡了流量负载，防止了单个实例中的网桥节点发生故障时的大规模中断，并允许新故障实例的更快收敛。

◆ 默认情况下，所有 VLAN 都分配给连接 MST 区域内所有网桥和 LAN 的内部生成树（MSTI0）。这个交换机最多支持 32 个实例。 您应该尝试对覆盖网络的同一区域的 VLAN 进行分组。但是，请记住，必须使用相同的实例集配置同一 MSTI Region 中的所有网桥，并使用相同的 VLAN 集配置相同实例（在每个网桥上）。另请注意，RSTP 将每个 MSTI 区域视为单个节点，将所有区域连接到公共生成树。

范例

```
Console(config-mstp)#mst 1 vlan 2-5

Console(config-mstp)#
```

18.1.15 name

此命令配置此交换机所在的多生成树区域的名称。使用 no 表单清除名称。

语法

name *name*

name -生成树的名称。

缺省配置

交换机的 MAC 地址

命令模式

MST 配置

命令用法

MST 区域名称和修订号用于指定唯一的 MST 区域。桥（即，诸如此交换机的生成树兼容设备）只能属于一个 MST 区域。并且必须在同一区域中的所有桥接器配置相同的 MST 实例。

范例

```
Console(config-mstp)#name R&D
Console(config-mstp)#
```

18.1.16 revision

此命令配置此交换机的此多跨域配置的修订号。使用 no 形式恢复默认值。

语法

revision *number*

number -生成树的修订号。（范围：0-65535）

缺省配置

0

命令模式

MST 配置

命令用法

MST 区域名称和修订号用于指定唯一的 MST 区域。 桥（即诸如此交换机的生成树兼容设备）只能属于一个 MST 区域。并且必须在同一区域中的所有桥接器配置相同的 MST 实例。

范例

```
Console(config-mstp)#revision 1

Console(config-mstp)#
```

18.1.17 spanning-tree bpdu-filter

此命令过滤边缘端口上接收的所有 BPDU。使用 no 形式禁用此功能。

语法

[no] spanning-tree bpdu-filter

缺省配置

禁用

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

◆此命令过滤接口上接收的所有网桥协议数据单元（BPDU），以节省 CPU 处理时间。此功能设计为到工作站与边缘端口相结合，边缘端口只应将终端连接到交换机，因此不需要处理 BPDU。但是请注意，如果连接到另一个交换机或桥接设备的中继端口被错误地配置为边缘端口，并且在此端口上启用了 BPDU 过滤功能，这可能会导致生成树中出现循环。

◆ 在启用 BPDU Filter 之前，必须首先使用 spanning-tree edge-port 命令将接口配置为一个 edge 端口 。

范例

```
Console(config)#interface ethernet 1/5

Console(config-if)#spanning-tree edge-port

Console(config-if)#spanning-tree bpdu-filter

Console(config-if)#
```

18.1.18 spanning-tree bpdu-guard

如果接收到 BPDU，则此命令将关闭边缘端口（即用于快速转发的接口集）。 使用没有任何关键字的 no 形式可以使用此功能，或使用关键字恢复默认设置。

语法

spanning-tree bpdu-guard [auto-recovery [interval *interval*]]

no spanning-tree bpdu-guard [**auto-recovery** [*interval*]]

auto-recovery -在指定的时间间隔后自动重新启用接口。

interval -重新启用接口之前等待的时间。（范围：30-86400 秒）

缺省配置

BPDU Guard: 禁用

Auto-Recovery: 禁用

Auto-Recovery Interval: 300 秒

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

◆边缘端口只应连接到不生成 BPDU 的端节点。如果在边缘端口上收到 BPDU，则表示网络配置无效，或者交换机可能未被黑客攻击。如果接口被 BPDU Guard 关闭，则必须使用 no spanning-tree spanning-disabled 命令手动重新启用它，如果未指定自动恢复间隔。

◆ 在启用 BPDU Guard 之前，必须使用 spanning-tree edge-port 命令将接口配置为 anedge 端口。另请注意，如果在接口上禁用了边缘端口属性，则还会在该接口上禁用 BPDU Guard。

范例

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#spanning-tree bpdu-guard
Console(config-if)#
```

18.1.19 spanning-tree cost

此命令用于配置指定接口的生成树路径开销。使用 no 形式恢复默认自动配置模式。

语法

spanning-tree cost *cost*

no spanning-tree cost

cost -端口的路径开销。 （范围：0 表示自动配置，1-65535 表示短路径成本法，1-200,000,000 表示长路径成本法）

推荐的 STA 路径成本范围

Port Type	Short Path Cost (IEEE 802.1D-1998)	Long Path Cost (802.1D-2004)
Ethernet	50-600	200,000-20,000,000
Fast Ethernet	10-60	20,000-2,000,000
Gigabit Ethernet	3-10	2,000-200,000
10G Ethernet	1-5	200-20,000

缺省配置

默认情况下，系统会自动检测每个端口上使用的速度和双工模式，并根据下面的值配置路径开销。　路径成本“0”用于指示自动配置模式。当选择短路径成本方法并且 IEEE8021w 标准推荐的默认路径成本超过 65,535 时，默认设置为 65,535。

默认 STA 路径成本

Port Type	Short Path Cost (IEEE 802.1D-1998)	Long Path Cost (802.1D-2004)
Ethernet	65,535	1,000,000
Fast Ethernet	65,535	100,000
Gigabit Ethernet	10,000	10,000
10G Ethernet	1,000	1,000

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

◆生成树算法使用此命令确定设备之间的最佳路径。因此应将较低的值分配给连接到较快介质的端口，将较高的值分配给具有较慢介质的端口。

◆　路径开销优先于端口优先级。

◆　当路径成本法设置为 short 时，路径成本的最大值为 65,535。

范例

```
Console(config)#interface ethernet 1/5

Console(config-if)#spanning-tree cost 50

Console(config-if)#
```

18.1.20 spanning-tree edge-port

此命令将接口指定为边缘端口。使用 no 形式恢复默认值。

语法

spanning-tree edge-port [auto]

no spanning-tree edge-port

auto -自动确定接口是否为边缘端口。

缺省配置

自动

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

如果接口连接到位于桥接 LAN 末端或端节点的 LAN 段，则可以启用此选项。由于端节点不能导致转发循环，因此它们可以直接传递到生成树转发状态。指定边缘端口为工作站或服务器等设备提供更快的收敛，保留当前转发数据库以减少重新配置事件期间重建地址表所需的帧泛滥量，不会导致生成树在接口更改状态时启动重新配置，并且还会覆盖其他 STA 相关的超时问题。 但是请记住，只应为连接到端节点设备的端口启用 Edge 端口。

范例

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#
```

18.1.21 spanning-tree link-type

此命令配置快速生成树和多生成树的链接类型。使用 no 形式恢复默认值。

语法

spanning-tree link-type {auto | point-to-point | shared}

no spanning-tree link-type

auto -自动从双工模式设置派生。

point-to-point -点对点链接。

shared -共享媒体。

缺省配置

自动

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

◆如果接口只能连接到另一个桥接器，则指定点对点链接;如果可以连接到另外两个桥接器，则指定共享链接。

◆ 选择自动检测时，交换机从双工模式导出链路类型。全双工接口被认为是一个点对-点链接，而半双工接口被假定为一个共享链接。

◆ RSTP 仅适用于两个网桥之间的点对点链路。如果您将端口作为共享链接加入，则禁止使用 RSTP。由于 MSTP 是 RSTP 的延伸，因此同样的限制也适用。

范例

```
Console(config)#interface ethernet 1/5

Console(config-if)#spanning-tree link-type point-to-point
```

18.1.22 spanning-tree loopback-detection

此命令用于在端口上检测和响应生成树 loopback BPDU 数据包。使用 no 形式禁用此功能特征。

语法

[no] spanning-tree loopback-detection

缺省配置

启用

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

◆如果未启用端口环回检测且端口收到自己的 BPDU，则端口将根据 IEEES 标准 802.1W-2001 9.3.4（注 1）丢弃环回 BPDU。

◆ 如果在交换机上禁用了 Spanning Tree，则端口环回检测不会处于活动状态 。

范例

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree loopback-detection
```

18.1.23 spanning-tree loopback-detection action

此命令配置环回检测的响应以阻止 usertraffic 或关闭接口。使用 no 形式恢复默认值。

语法

spanning-tree loopback-detection action{**block** | **shutdown** *duration*}

no spanning-tree loopback-detection action

block -阻止用户流量。

shutdown -关闭界面。

duration -关闭接口的持续时间。（范围：60-86400 秒）

缺省配置

阻塞

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

◆如果通过此命令关闭接口，并且使用 spanning-tree loopback-detection release-mode 命令将释放模式设置为“auto”，则在关闭间隔到期时，将自动启用所选接口。

◆ 如果此命令关闭接口，并且释放模式设置为“手动”，则可以使用 spanning - tree loopback-detection release 命令重新启用该接口 。

范例

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree loopback-detection action shutdown 600
```

18.1.24 spanning-tree loopback-detection release-mode

此命令配置放置在丢弃状态的端口的释放模式,因为收到了环回 BPDU。使用 no 形式恢复默认值。

语法

spanning-tree loopback-detection release-mode{auto | manual}

no spanning-tree loopback-detection release-mode

auto -允许端口在环回状态结束时自动从缓存状态释放。

manual -该端口只能通过**手动**释放丢弃状态。

缺省配置

自动

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

◆如果端口配置为自动环回释放，则只有满足以下条件之一时，才会将端口返回到转发状态：

- 端口接收除自己的 BPDU 之外的任何其他 BPDU;
- 端口的链接状态更改为链接，然后再次链接;
- 端口在前向延迟间隔中停止接收自己的 BPDU。

◆ 如果未启用端口环回检测且端口收到自己的 BPDU，则端口将根据 IEEES 标准 802.1W-2001 9.3.4（注 1）丢弃环回 BPDU 。

◆ 如果在交换机上禁用了生成树，则端口环回检测不会处于活动状态。

◆ 当配置为手动释放模式时，链接向下/向上事件将不会从丢弃状态释放端口。它只能使用 spanning-tree loopback-detection release 命令进行处理。

范例

```
Console(config)#interface ethernet 1/5

Console(config-if)#spanning-tree loopback-detection release-mode manual

Console(config-if)#
```

18.1.25 spanning-tree loopback-detection trap

此命令为生成树 loopback BPDU 检测启用 SNMP 陷阱通知。使用 no 形式恢复默认值。

语法

[no] spanning-tree loopback-detection trap

缺省配置

禁用

命令模式

接口配置 (Ethernet, Port Channel)

范例

```
Console(config)#interface ethernet 1/5

Console(config-if)#spanning-tree loopback-detection trap
```

18.1.26 spanning-tree mst cost

此命令在多个生成树中配置生成实例上的路径开销。使用 no 形式恢复到默认的自动-配置模式。

语法

spanning-tree mst *instance-id* **cost** *cost*

no spanning-tree mst *instance-id* **cost**

instance-id -生成树的实例标识符。（范围：0-4094）

cost-接口的路径开销。 （范围：0 表示自动配置，1-65535 表示短路径成本法，1-200,000,000 表示长路径成本法）

缺省配置

默认情况下，系统会自动检测每个端口上使用的速度和双工模式，并根据下面的值配置路径开销。 路径成本“0”用于指示自动配置模式。当选择短路径成本方法并且 IEEE802.1w 标准推荐的默认路径成本超过 65,535 时。

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

◆每个生成树实例都与一组唯一的 VLANID 相关联。

◆ 多生成树算法使用此命令来确定设备之间的最佳路径。因此，应将较低的值分配给附加到较快介质的接口，并将较高的值分配给具有较慢介质的接口。

◆ 使用 **no spanning-tree mst cost** 命令来指定自动-配置模式。

◆ 路径开销优先于接口优先级。

范例

```
Console(config)#interface Ethernet 1/5

Console(config-if)#spanning-tree mst 1 cost 50

Console(config-if)#
```

18.1.27 spanning-tree mst port-priority

此命令配置多生成树中生成实例的接口优先级。使用 no 形式恢复默认值。

语法

spanning-tree mst *instance-id* **port-priority** *priority*

no spanning-tree mst *instance-id* **port-priority**

instance-id -生成树的实例标识符。（范围：0-4094）

priority -接口的*优先* 级。 （范围：0-240，步长为 16）

缺省配置

128

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

◆此命令定义在多个生成树中使用接口的优先级。如果交换机上所有接口的路径开销相同，则优先级最高的接口（即最低值）将被配置为生成树中的活动链路。

◆ 如果为多个接口分配了最高优先级，则将启用具有最低数字标识符的接口。

范例

```
Console(config)#interface Ethernet 1/5
Console(config-if)#spanning-tree mst 1 port-priority 0
Console(config-if)#
```

18.1.28 spanning-tree port-bpdu-flooding

当在特定端口上禁用生成树或禁用生成树时，此命令会将 BPDU 泛洪到其他端口。 使用 no 形式恢复默认设置。

语法

[no] **spanning-tree port-bpdu-flooding**

缺省配置

启用

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

◆启用后，BPDU 将溢出到交换机上的所有其他端口，或者扩展到接收端口的本地 VLAN 中的所有其他端口，如 spanning-tree system-bpdu-flooding 命令所指定。

◆ 如果通过 **spanning-tree port-bpdu - flooding** 命令在端口上禁用了 BPDU 泛洪，则 spanning-tree system-bpdu-flooding 命令无效 。

范例

```
Console(config)#interface ethernet 1/5

Console(config-if)#spanning-tree port-bpdu-flooding

Console(config-if)#
```

18.1.29 spanning-tree port-priority

此命令配置指定接口的优先级。使用 **no** 形式恢复默认值。

语法

spanning-tree port-priority *priority*

no spanning-tree port-priority

priority -端口的优先级。（范围：0-240，步长为 16）

缺省配置

128

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

◆此命令定义在 SpanningTree 算法中使用端口的优先级。 如果交换机上所有端口的路径开销相同，则优先级最高的端口（即最低值）将被配置为生成树中的活动链路。

◆ 如果为多个端口分配了最高优先级，则将启用具有最低数字标识符的端口。

范例

```
Console(config)#interface ethernet 1/5

Console(config-if)#spanning-tree port-priority 0
```

18.1.30 spanning-tree root-guard

此命令可防止指定端口将高级 BPDU 记入帐户并允许选择新的 STP 根端口。使用 no 形式禁用此功能。

语法

[no] spanning-tree root-guard

缺省配置

禁用

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

◆具有较低网桥标识符（或相同标识符和较低 MAC 地址）的网桥可以随时作为根网桥接管。

◆ 当启用 Root Guard 并且交换机在此端口上接收到优质 BPDU 时，它将设置为 Discarding 状态，直到它在固定恢复期间接收到优先 BPDU。在丢弃状态中，没有流量通过端口转发。

◆ Root Guard 可用于确保根桥未形成在次优位置。应该在连接到低速网桥的指定端口上启用 Root Guard，这可能会通过接管根端口并形成新的生成树拓扑而过载较低的链路。它还可以用于在允许根桥的网络的一部分周围形成边界。

◆ 在交换机或接口上全局初始化生成树时，交换机将等待 20 秒，以确保在启用 Root Guard 之前，生成树已收敛。

范例

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#spanning-tree root-guard
Console(config-if)#
```

18.1.31 spanning-tree spanning-disabled

此命令禁用指定接口的生成树算法。使用 no 形式为指定接口重新启用生成树算法。

语法

[no] spanning-tree spanning-disabled

缺省配置

启用

命令模式

接口配置 (Ethernet, Port Channel)

范例

此示例禁用端口 5 的生成树算法。

```
Console(config)#interface ethernet 1/5

Console(config-if)#spanning-tree spanning-disabled

Console(config-if)#
```

18.1.32 spanning-tree loopback-detection release

此命令通过回环检测手动释放放置在丢弃状态中的端口。

语法

spanning-tree loopback-detection release *interface*

interface

ethernet *单元 / 端口*

unit -单位标识符。(范围：1)

port -端口号。(范围：1-28)

port-channel *channel-id* (范围: 1-12)

命令模式

特权模式

命令用法

如果通过 spanning-tree loopback-detection release-mode 命令将环回检测释放模式设置为“手动”，并且发生 BPDU 环回，则使用此命令从丢弃状态释放接口。

范例

```
Console#spanning-tree loopback-detection release ethernet 1/1

Console#
```

18.1.33 spanning-tree protocol-migration

此命令重新检查相应的 BPDU 格式以在所选接口上发送。

语法

spanning-tree protocol-migration *interface*

interface

ethernet *单元 / 端口*

unit - 单位标识符。 （范围：1）

port - 端口号。 （范围：1-28）

port-channel *channel-id* (范围: 1-12)

命令模式

特权模式

命令用法

如果交换机在任何时候检测到 STP BPDU，包括配置或拓扑更改通知 BPDU，它将自动将所选接口设置为强制 STP 兼容模式。但是，您也可以随时使用 **spanning-tree protocol-migration** 命令手动重新检查要在所选接口上发送的相应 BPDU 格式（即 RSTP 或 STP 兼容）。

范例

```
Console#spanning-tree protocol-migration eth 1/5
Console#
```

18.1.34 show spanning-tree

此命令显示公共生成树（CST）的配置，适用于多生成树（MST）中的所有实例或多生成树（MST）中的特定实例。

语法

show spanning-tree [*interface* | **mst** *instance-id* | **brief** |**stp-enabled-only**]

interface

ethernet *单元 / 端口*

unit - 单位标识符。 （范围：1）

port - 端口号。 （范围：1-28）

port-channel *channel-id* (范围: 1-12)

instance-id -多生成树的实例标识符。（范围：0-4094）

brief -显示全局和界面设置的主要内容。

stp-enabled-only -显示全局设置以及启用了 STP 的接口设置。

缺省配置

无

命令模式

特权模式

命令用法

◆使用 **show spanning-tree** 命令（不带参数 s）显示 CommonSpanning Tree（CST）交换机的生成树配置以及树中的每个接口。

◆ 使用 **show spanning-tree** *interface* 命令显示 CommonSpanning Tree（CST）中 接口的生成树配置。

◆使用 **show spanning-tree mst** 命令显示多生成树（MST）中所有实例的生成树配置，包括活动接口的全局设置和设置。

◆使用 **show spanning-tree mst** *instance-id* 命令用来显示这个生成树配置为多实例生成树（MST）内的情况下，包括全局设置和设置所有端口。

范例

```
Console#show spanning-tree

Spanning Tree Information

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

Spanning Tree Mode : MSTP

Spanning Tree Enabled/Disabled : Enabled

Instance : 0

VLANs Configured : 1-4093

Priority : 32768

Bridge Hello Time (sec.) : 2

Bridge Max. Age (sec.) : 20

Bridge Forward Delay (sec.) : 15

Root Hello Time (sec.) : 2

Root Max. Age (sec.) : 20
```

Root Forward Delay (sec.) : 15

Max. Hops : 20

Remaining Hops : 20

Designated Root : 32768.0.0001ECF8D8C6

Current Root Port : 21

Current Root Cost : 100000

Number of Topology Changes : 5

Last Topology Change Time (sec.): 11409

Transmission Limit : 3

Path Cost Method : Long

Flooding Behavior : To VLAN

Cisco Prestandard : Disabled

Eth 1/ 1 information

Admin Status : Enabled

Role : Disabled

State : Discarding

External Admin Path Cost : 0

Internal Admin Path Cost : 0

External Oper Path Cost : 100000

Internal Oper Path Cost : 100000

Priority : 128

Designated Cost : 100000

Designated Port : 128.1

Designated Root : 32768.0.0001ECF8D8C6

Designated Bridge : 32768.0.123412341234

Forward Transitions : 4

Admin Edge Port : Disabled

Oper Edge Port : Disabled

```
Admin Link Type : Auto

Oper Link Type : Point-to-point

Flooding Behavior : Enabled

Spanning-Tree Status : Enabled

Loopback Detection Status : Enabled

Loopback Detection Release Mode : Auto

Loopback Detection Trap : Disabled

Loopback Detection Action : Block

Root Guard Status : Disabled

BPDU Guard Status : Disabled

BPDU Guard Auto Recovery : Disabled

BPDU Guard Auto Recovery Interval : 300

BPDU Filter Status : Disabled

...
```

此示例显示了全局和接口设置的简短摘要生成树。

```
Console#show spanning-tree brief

Spanning Tree Mode : RSTP

Spanning Tree Enabled/Disabled : Enabled

Designated Root : 32768.0000E89382A0

Current Root Port : 0

Current Root Cost : 0

Interface Pri Designated Designated Oper STP Role State Oper

Bridge ID Port ID Cost Status Edge

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

Eth 1/ 1 128 32768.0000E89382A0 128.1 100000 EN DESG FWD No

Eth 1/ 2 128 32768.0000E89382A0 128.2 10000 EN DISB BLK No

Eth 1/ 3 128 32768.0000E89382A0 128.3 10000 EN DISB BLK No

Eth 1/ 4 128 32768.0000E89382A0 128.4 10000 EN DISB BLK No

Eth 1/ 5 128 32768.0000E89382A0 128.5 10000 EN DISB BLK No

...
```

18.1.35 show spanning-tree mst configuration

此命令显示多生成树的配置。

命令模式

特权模式

范例

```
Console#show spanning-tree mst configuration

Mstp Configuration Information

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

Configuration Name : R&D

Revision Level :0

Instance VLANs

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

0 1-4093

Console#
```

19 ERPS 命令

G.8032 建议（也称为以太网环保护切换（ERPS））可用于提高以太网环的可用性和稳健性。
本章介绍用于配置 ERPS 的命令。

ERPS 配置指南

1. 创建 ERPS 环：使用 erps domain 命令创建环。环名称用作 G.8032 数据库中的索引。

2. 配置东西接口：环上的每个节点通过两个环网口连接。使用 ring-port 命令用来在环向东（或 顺时针方向）连接到下一个节点配置一个端口 ； 然后再次使用 ring-port 命令配置环中面向西的另一个端口。

3. 配置 RPL 所有者：使用 rpl owner 命令将环中的一个节点配置为 RingProtection Link（RPL）所有者。当此交换机配置为 RPL 所有者时，西环端口设置为连接到 RPL。在正常操作（空闲状态）下，RPL 被阻塞以确保环中不能形成环路。如果信号故障导致环中的任何其他链路断开，则 RPL 将被解锁（保护状态）以确保所有环节点之间的正确连接，直到故障恢复。

4. 配置 ERPS 定时器：使用 guard-timer 命令设置防止环节点接收过时 R-APS 消息的时间，使用 holdoff-timer 命令过滤掉间歇性链路故障，使用 wtr-timer 命令验证在从信号故障中恢复之后，环在稳定之前已经稳定。

5. 配置 ERPS 控制 VLAN（CVLAN）：使用 control-vlan 命令创建用于传递 R-APS 环网维护命令的 VLAN。CVLAN 不得配置 IP 地址。此外只有环形端口可以添加到 CVLAN（之前将 VLAN 配置为 CVLAN）。 没有其他端口可以成为此 VLAN 的成员（一旦设置为 CVLAN）。 此外，CVLAN 的环端口必须加贴标签。不遵守这些限制可能导致网络中的 aloop。

6. 启用 ERPS：在按照下一步所述启用振铃之前，首先使用 erps 命令在交换机上全局启用 ERPS。如果尚未启用 ERPS 或已使用 no erps 命令禁用 ERPS，则不会有 ERPS 提醒。

7. 启用 ERPS 环：在 ERPS 环可以工作之前，必须使用 enable 命令启用它。配置完成并启用启用后，R-APS 消息将开始在控制 VLAN 中流动，正常流量将开始在数据 VLAN 中流动。 要停止响

铃，可以使用 no enable 命令在任何节点上禁用它 。

8. 显示 ERPS 状态信息：使用 show erps 命令显示特定环的一般 ERPS 状态信息或详细的 ERPS 状态信息。

19.1.1 erps

此命令在交换机上启用 ERPS。使用 no 形式禁用此功能。

语法

[no] erps

缺省配置

禁用

命令模式

全局配置

命令用法

必须先在交换机上全局启用 ERPS，然后才能使用 enable 命令在 ERPS 环上启用 ERPS 。

范例

```
Console(config)#erps
Console(config)#
```

19.1.2 erps domain

此命令创建 ERPS 环并进入指定域的 ERPS 配置模式。 使用 no 形式删除一个环。

语法

[no] erps domain *name*

name -特定 ERPS 环的名称。（范围：1-12 个字符）

缺省配置

无

命令模式

全局配置

命令用法

特定 ERPS 环的名称。（范围：1-12 个字符）

范例

```
Console(config)#erps domain r&d

Console(config-erps)#
```

19.1.3 control-vlan

此命令指定用于发送和接收 ERPS 协议消息的专用 VLAN。 使用 **no** 形式删除 Control VLAN。

语法

[**no**] **control-vlan** *vlan-id*

vlan-id - VLAN ID（范围：1-4093）

缺省配置

无

命令模式

ERPS 配置

命令用法

◆为每个 ERPS 环配置一个控制 VLAN。首先创建 VLAN，作为控制 VLAN，将东西接口的环网端口作为标记成员添加到该 VLAN，然后使用 control-vlan 命令将其添加到环中。

◆控制 VLAN 不能配置为第 3 层接口（具有 IP 地址），也不能配置为动态 VLAN（启用 GVRP）。此外，只有环网端口可以添加到控制 VLAN。没有其他端口可以成为此 VLAN 的成员。此外，必须标记 ControlVLAN 的环网端口。不遵守这些限制可能会导致网络中出现环路。

◆ 使用 enable 命令激活环后，无法修改控制 VLAN 的配置。 在对控制 VLAN 进行任何配置更改之前，请使用命令停止 ERPS 环。

范例

```
Console(config)#vlan database

Console(config-vlan)#vlan 2 name rdc media ethernet state active

Console(config-vlan)#exit

Console(config)#interface ethernet 1/12

Console(config-if)#switchport allowed vlan add 2 tagged

Console(config-if)#interface ethernet 1/11

Console(config-if)#switchport allowed vlan add 2 tagged
```

```
Console(config-if)#exit
Console(config)#erps domain rd1
Console(config-erps)#control-vlan 2
Console(config-erps)#
```

19.1.4 enable

此命令激活当前的 ERPS 环。使用 no 形式禁用当前环。

语法

[no] enable

缺省配置

禁用

命令模式

ERPS 配置

命令用法

◆在启用环之前，应使用 erps 命令启用全局 ERPS 功能，使用 ring-port 命令在每个节点上配置东西环端口，使用 rpl owner 命令指定 RPL 所有者，并使用配置的控制 VLAN 启用控制 vlan 命令。

◆ 一旦启用，RPL 所有者节点和非所有者节点状态机将启动，如果未检测到信号故障，则环将进入空闲状态。

范例

```
Console(config-erps)#enable
Console(config-erps)#
```

19.1.5 guard-timer

此命令设置保护定时器，以防止环节点接收过时的 R-APS 消息。 使用 no 形式恢复默认设置。

语法

guard-timer *milliseconds*

milliseconds -保护定时器用于防止环节点接收过时的 R-APS 消息。 在保护定时器的持续时间内，所有接收到的 R-APS 消息都被环保护控制过程忽略，从而为仍在环上循环的旧消息提供时

间到期。 （范围：10-2000 毫秒，步长 10 毫秒）

缺省配置

500 毫秒

命令模式

ERPS 配置

命令用法

保护定时器持续时间应大于 R-APS 消息绕过环路的最大预期转发延迟。A 面-保护定时器的效果是，它的持续时间期间，节点将是从其他节点发送的新的或现有的环的请求。

范例

```
Console(config-erps)#guard-timer 300

Console(config-erps)#
```

19.1.6 holdoff-timer

此命令设置定时器以过滤掉间歇性链路故障。使用 no 形式恢复默认设置。

语法

holdoff-timer *milliseconds*

milliseconds-延迟计时器用于过滤掉间歇性链路故障。如果此计时器到期，故障将仅报告给环保护机制。（范围：0-10000 毫秒，步长 100 毫秒）

缺省配置

0 毫秒

命令模式

ERPS 配置

命令用法

为了协调多层保护开关的定时，可能需要保持关闭定时器。其目的是允许，例如服务器层保护开关有机会在客户端层切换之前解决问题。当出现新的缺陷或更严重的缺陷（新的信号故障）时，此事件不会立即报告给保护切换机制，如果提供的延迟定时器值不为零。相反，将启动 thehold-off 计时器。 当计时器到期时，无论是否存在缺陷，都将检查计时器。 如果确实存在，则将该缺陷报告给保护切换机制。报告的缺陷与启动计时器的缺陷不同。

范例

```
Console(config-erps)#holdoff-timer 300

Console(config-erps)#
```

19.1.7 major-domain

此命令指定用于发送控制数据包的 ERPS 环。使用 no 形式删除当前设置。

语法

major-domain *name*

no major-domain

name -用于发送控制报文的 ERPS 环的名称（范围：1-32 个字符）

缺省配置

无

命令模式

ERPS 配置

命令用法

◆此开关最多可支持两个环。但是 ERPS 控制数据包只能在一个环上发送。此命令用于指示当前环是辅助环，并指定将用于发送 ERPS 控制数据包的主环。

◆Ring Protection Link（RPL）是西端口无法配置。因此辅助环上的物理端口必须是 westport。换句话说，如果域具有两个物理环端口，则该环可以是主环，而不是仅具有一个物理环端口的辅环（或子域）。因此，如果已配置东端口，则此命令将失败（请参阅 ring-port 命令）。

范例

```
Console(config-erps)#major-domain rd0

Console(config-erps)#
```

19.1.8 meg-level

此命令设置环的维护实体组级别。使用 no 形式恢复默认设置。

语法

meg-level *level*

level -维护实体组（MEG）级别，为环路自动保护切换（R-APS）信息提供通信信道。（范围：0-7）

缺省配置

1

命令模式

ERPS 配置

命令用法

◆此参数用于确保收到的 R-APS PDU 指向此环。如果有许多 R-APS PDU 通过此交换机，则应为每个本地环配置唯一级别 。

◆ 如果使用 CFM 连续性检查消息来监视 mep-monitor 命令指定的 ERPS 环节点的链路状态，则 **meg-level** 命令设置的 MCC 级别必须与指定 MEP 所属的 CFM 域的授权维护级别匹配。

范例

```
Console(config-erps)#meg-level 0

Console(config-erps)#
```

19.1.9 mep-monitor

此命令指定用于监视环节点上的链路的 CCM MEP。使用 **no** 形式恢复默认设置。

语法

mep-monitor {**east** | **west**} **mep** *mpid*

east -连接到东边的下一个环节点。

west -连接到西边的下一个环节点。

mpid -维护终点标识符。（范围：1-8191）

缺省配置

无

命令模式

ERPS 配置

命令用法

◆如果此命令用于监视具有 CFM 连续性检查消息的 ERPS 节点的链路状态，则 meg - level 命令设置的 MEG 级别 必须与指定 MEP 所属的 CFM 域的授权维护级别匹配 。

◆要确保完全监视环节点，请使用 **mep-monitor** 命令指定用于监视环节点的东部和西部端口的 CFM MEP。

◆如果CFM确定已　使用此命令配置了监控　端口　的MEP节点已关闭，则此信息将传递给ERPS，后者又将其作为环节点故障处理。

范例

```
Console(config-erps)#mep-monitor east mep 1

Console(config-erps)#
```

19.1.10 node-id

此命令设置环节点的 MAC 地址。使用 **no** 形式恢复默认设置。

语法

node-id *mac-address*

mac-address - 环节点唯一的 MAC 地址。必须以 xx-xx-xx-xx-xx-xx 或 xxxxxxxxxxx 格式指定 MAC 地址。

缺省配置

CPU MAC 地址

命令模式

ERPS 配置

命令用法

环节点标识符是信息性的，不影响环保护切换操作。它可以用于调试，例如在节点连接到多个环时区分消息。

范例

```
Console(config-erps)#node-id 00-12-CF-61-24-2D

Console(config-erps)#
```

19.1.11 non-erps-dev-protect

当所有者节点进入保护状态而没有通过 SF 消息检测到任何链路断开事件时，此命令发送非标准的健康检查数据包。使用 **no** 形式可以禁用此功能。

语法

[no] non-erps-dev-protect

缺省配置

禁用

命令模式

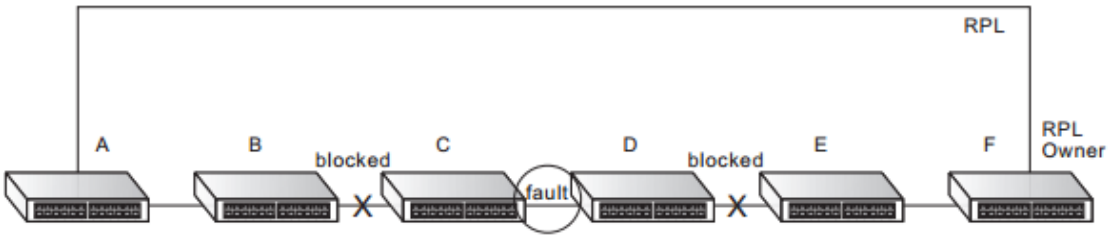
ERPS 配置

命令用法

◆当 RPL 所有者节点从与　故障链路　相邻的节点接收到 R-APS（SF 信号故障）消息时，它会检测到链路故障。然后，所有者通过解锁 RPL 进入保护状态。但是使用此标准恢复过程可能会导致非 EPRS 设备在与其相邻的 ERPS 设备检测到连续性检查消息（CCM）丢失事件并阻止之间的链接时变得孤立。

非 ERPS 设备和 ERPS 设备。

CCM 通过“CFM 命令”中描述的连通性故障管理(CFM)协议传播　。如果使用标准恢复过程，　如下图所示，并且节点 E 检测到 CCM　，则它将向 RPL 所有者发送 R-APS（SF）消息并阻止到节点 D 的链路，隔离该非 ERPS 设备。



当环上引入非 ERPS 设备保护时，当 CCM 丢失事件检测到信号丢失时，RPL 所有者节点和非所有者节点上的环端口将不会被阻塞　。

◆当在 RPL 所有者节点上启用非 ERPS 设备保护时，它将发送非标准的健康检查数据包，以便在进入保护状态时轮询环网健康状况。它不使用等待从恢复的链路附近的节点接收 R-APS（NR - 无请求）消息的正常过程。相反，它等待查看标准的健康检查数据包是否循环回来。如果他们这样做，表明故障已经解决，则 RPL 将被阻止。在阻止 RPL 之后，所有者节点仍将发送 R-APS（NR，RB - 环阻塞)消息。接收此消息的 ERPS 兼容节点刷新其转发数据库并取消阻止先前阻塞的端口。环现在返回到空闲状态。

范例

```
Console(config-erps)#non-erps-dev-protect

Console(config-erps)#
```

19.1.12 propagate-tc

此命令允许将辅助环的拓扑更改消息传播到主环。使用 no 形式禁用此功能。

语法

[no] propagate-tc

缺省配置

禁用

命令模式

ERPS 配置

命令用法

◆当辅助环检测到拓扑变化时，它可以将这个事件的消息传递给主环。当主环从次级环接收到这种消息时，它可以清除其环端口上的 MAC 地址，从而通过保护切换帮助第二级环更快地恢复其连接。

◆当 MAC 地址被清除时，数据流可能溢出到主环上。在 MAC 地址再次被学习之后，数据流将变得稳定。主环不会被破坏，但是由于这种泛洪行为，主环上的数据业务的带宽可能在短时间内受损。

范例

```
Console(config-erps)#propagate-tc

Console(config-erps)#
```

19.1.13 ring-port

此命令通过东/西接口配置节点与环的连接。使用 no 形式取消节点与环的关联。

语法

ring-port {**east** | **west**} **interface** *interface*

east -连接到东边的下一个环节点。

west - 连接到西边的下一个环节点。

interface

ethernet *unit/port*

unit -单位标识符。（范围：1）

port -端口号。（范围： 1-28）

缺省配置

没有关联

命令模式

ERPS 配置

命令用法

◆每个节点必须连接到环上的两个邻居。方便的是，连接的端口称为东和西港。或者，最靠近东部的邻居应该是环中顺时针方向的下一个节点，而最靠近西部的邻居应该是环中逆时针方向的下一个节点。

◆注意，环端口不能被配置为 SpungIt 树、动态中继线或静态中继线的成员。

范例

```
Console(config-erps)#ring-port east interface ethernet 1/12

Console(config-erps)#
```

19.1.14 rpl owner

此命令将环节点配置为环保护链路（RPL）所有者或非所有者。

语法

[no] rpl owner

缺省配置

非所有者

命令模式

ERPS 配置

命令用法

◆只能在一个环上配置一个 RPL 所有者。所有者在空闲状态期间阻止 RPL，并在 Protectionstate 期间（即，在环上检测到信号故障时）将其解除阻塞。

◆必须使用 ring-port 命令为所有环节指定环的东西连接。当此交换机配置为 RPL 所有者时，西环端口设置为连接到 RPL。

范例

```
Console(config-erps)#rpl owner

Console(config-erps)#
```

19.1.15 wtr-timer

此命令设置等待恢复计时器，用于在从信号故障恢复后阻止 RPL 之前验证环已稳定。使用 **no** 形式恢复默认设置。

语法

wtr-timer *minutes*

minutes-等待恢复计时器用于在从信号故障恢复后阻止 RPL 之前验证环已稳定。 （范围：5-12 分钟）

缺省配置

5 分钟

命令模式

ERPS 配置

命令用法

如果交换机由于信号故障而进入环保护状态，则在故障条件被清除后，RPL 所有者将启动等待恢复时间并等待它到期以确认环已经稳定，然后阻塞 RPL 并返回到空闲（正常运行）状态。

范例

```
Console(config-erps)#wtr-timer 10

Console(config-erps)#
```

19.1.16 show erps

此命令显示所有已配置环的状态信息，或指定环的状态信息。

语法

show erps [**domain** *ring-name*]

ring-name -特定 ERPS 环的名称。（范围：1-32 个字符）

命令模式

特权模式

范例

此示例显示在交换机上配置的所有 ERPS 环的摘要。

```
Console#show erps

ERPS Status : Enabled
```

```
Number of ERPS Domains : 1

Domain State MEL Enabled West East RPL Owner Ctrl VLAN

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

rd1 Idle 0 Yes Eth 1/12 Eth 1/10 Yes 100

rd2 Protection 0 Yes Eth 1/3 Eth 1/4 No 200

Console#
```

20 VLAN 命令

VLAN 是一组端口，可以位于网络中的任何位置，但是就像它们属于同一物理段一样进行通信。本节介绍用于创建 VLAN 组，添加端口成员，指定如何使用 VLAN 标记以及启用的命令所选接口的自动 VLAN 注册。

20.1 编辑 VLAN 组

20.1.1 vlan database

该命令进入 VLAN 数据库模式。此模式中的所有命令将立即生效。

缺省配置

无

命令模式

全局配置

命令用法

◆使用 VLAN 数据库命令模式添加，更改和删除 VLAN。完成配置更改后，您可以通过输入 show vlan 命令来显示 VLAN 设置 。

◆ 使用 interface vlan 命令模式定义端口成员资格模式，并添加从 VLAN 中删除端口。这些命令的结果将写入运行配置文件，您可以通过输入 show running-config 命令来显示此文件 。

范例

```
Console(config)#vlan database
Console(config-vlan)#
```

20.1.2 vlan

该命令用来配置 VLAN。使用 no 形式恢复默认设置或删除 VLAN。

语法

vlan *vlan-id* [**name** *vlan-name*] **media ethernet**[**state** {**active** | **suspend**}] [**rspan**]

no vlan *vlan-id* [**name** | **state**]

vlan-id - VLAN ID，指定为单个数字，由连字符分隔的连续数字范围或由逗号分隔的多个数字。 （范围：1-4093）

name -要为 VLAN 名称后跟的关键字。

vlan-name - 1 到 32 个字符的 ASCII 字符串。

media ethernet -以太网媒体类型。

state -要遵循 VLAN 状态的关键字。

active - VLAN 正常运行。

suspend - VLAN 已暂停。挂起的 VLAN 不会传递数据包。

rspan -创建用于镜像来自远程交换机的流量的 VLAN 的关键字。 用于 RSPAN 的 VLAN 不能包括 VLAN 1（交换机的默认 VLAN），也不能包括 VLAN 4093（用于交换机群集的 VLAN）。 有关通过 CLI 配置 RSPAN 的更多信息，请参阅“RSPAN Mirroring Commands” 。

缺省配置

默认情况下，仅存在 VLAN1 且处于活动状态。

命令模式

VLAN 数据库配置

命令用法

◆**no vlan** *vlan-id* 删除 VLAN。

◆**no vlan** *vlan-id* **name** 删除 VLAN 名称。

◆**no vlan** *vlan-id* **state** 将 VLAN 恢复为默认状态（即活动状态）。

◆交换机上最多可以配置 4093 个 VLAN。

注释：该开关允许 256 个用户可管理的 VLAN。

范例

以下示例使用 VLAN ID 105 和名称 RD5 添加 VLAN。默认情况下，VLAN 处于激活状态。

```
Console(config)#vlan database
```

```
Console(config-vlan)#vlan 105 name RD5 media ethernet

Console(config-vlan)#
```

20.2 配置 VLAN 接口

20.2.1 interface vlan

该命令进入 VLAN 的接口配置模式，用于配置物理接口的 VLAN 参数。

语法

[no] **interface vlan** *vlan-id*

vlan-id -配置的 VLAN 的 ID。(范围: 1-4093)

缺省配置

无

命令模式

全局配置

范例

以下示例显示如何将接口配置模式设置为 VLAN1，然后为 VLAN 分配 IP 地址：

```
Console(config)#interface vlan 1

Console(config-if)#ip address 192.168.1.254 255.255.255.0

Console(config-if)#
```

20.2.2 Switchport acceptable-frame-types

此命令配置端口的可接受帧类型。使用 no 形式恢复默认值。

语法

switchport acceptable-frame-types {**all** | **tagged**}

no switchport acceptable-frame-types

all -端口接受所有帧，标记或未标记。

tagged -端口只接收带标记的帧。

缺省配置

所有帧类型

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

设置为接收所有帧类型时，任何未标记的接收帧都将分配给默认 VLAN。

范例

以下示例显示如何将端口 1 上收到的流量限制为标记帧：

```
Console(config)#interface ethernet 1/1

Console(config-if)#switchport acceptable-frame-types tagged

Console(config-if)#
```

20.2.3 switchport allowed vlan

此命令用于配置所选接口上的 VLAN 组。使用 **no** 形式恢复默认值。

语法

switchport allowed vlan {**add** *vlan-list* [**tagged** | **untagged**] |**remove** *vlan-list*}

no switchport allowed vlan

add *vlan-list* -要添加的 VLAN 标识符列表。

remove *vlan-list* -要删除的 VLAN 标识符列表。

vlan-list-使用逗号分隔不连续的 VLAN 标识符，不包含空格； 使用连字符指定一系列 ID。(范围：1-4093)。

缺省配置

默认情况下，所有端口都设置为 VLAN 1。

默认帧类型未标记。

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

◆交换机端口模式设置为 **hybrid** 的端口或中继必须至少分配给一个 VLAN 为 untagged。

◆如果 trunk 的 switchport 模式设置为 **trunk**（即 802.1Q Trunk），则只能将 VLAN 组的接口分配为标记成员。

◆帧始终标记在交换机内。向接口添加 VLAN 时使用的标记/未标记参数告诉交换机是否要保留或删除出口帧中的标记。

◆如果连接的其他任何中间网络设备和主机都不支持 VLAN，则应将该接口添加到 VLAN 中作为未标记的成员。　否则只需要将最多一个 VLAN 添加为无标记，这应该对应于接口的 VLAN。

◆　如果在接口的禁止列表中手动添加了接口的禁用列表中的 VLAN，则会自动从该接口的禁用列表中删除该 VLAN　。

范例

以下示例显示如何将 VLAN 1,2,5 和 6 添加到允许列表中作为端口 1 的标记 VLAN：

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport allowed vlan add 1,2,5,6 tagged
Console(config-if)#
```

20.2.4 switchport ingress-filtering

此命令启用接口的入口筛选。使用 no 形式恢复默认值。

语法

[no] switchport ingress-filtering

缺省配置

禁用

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

◆入口过滤仅影响已标记的帧。

◆　如果禁用入口筛选且端口收到标记为不是其成员的 VLAN 的帧，则这些帧将被泛洪到其他所有端口（此端口上明确禁止的 VLAN 除外　）。

◆　如果启用了入口过滤并且端口接收标记为不是其成员的 VLAN 的帧，则将丢弃这些帧。

◆　入口过滤不会影响 VLAN 独立的 BPDU 帧，例如 GVRP 或 STA。但是它们会影响 VLAN 依赖的 BPDU 帧，例如 GMRP。

范例

以下示例显示如何将接口设置为端口 1 以及可进入的入口过滤：

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport ingress-filtering
Console(config-if)#
```

20.2.5 switchport mode

此命令配置端口的 VLAN 成员资格模式。使用 no 形式恢复默认值。

语法

switchport mode {**access** | **hybrid** | **trunk**}

no switchport mode

access -指定访问 VLAN 接口。端口仅在单个 VLAN 上传输和接收未标记的帧。

hybrid -指定混合 VLAN 接口。端口可以传输带标签或未标记的帧。

trunk -指定端口作为 VLAN 中继的端点。中继是两个交换机之间的直接链路，因此端口传输标识源 VLAN 的标记帧。请注意，属于端口默认 VLAN 的帧（即与 PVID 相关联）也作为标记帧传输。

缺省配置

所有端口都处于访问模式，PVID 设置为 VLAN 1。

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

访问模式与 VLAN 中继互斥（请参阅 vlan-trunking 命令）。 如果在接口上启用了 VLAN 中继，则无法将该接口设置为访问模式，反之亦然。

范例

以下显示如何将配置模式设置为端口 1，然后将 switchport 模式设置为 hybrid：

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport mode hybrid
Console(config-if)#
```

20.2.6 switchport native vlan

此命令配置端口的 PVID（即默认 VLAN ID）。使用 no 形式恢复默认值。

语法

switchport native vlan *vlan-id*

no switchport native vlan

vlan-id -端口的缺省 VLAN ID。 （范围：1-4093）

缺省配置

VLAN 1

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

◆使用访问模式，并将接口分配给新 VLAN 时，其 PVID 将自动设置为该 VLAN 的标识符。 使用混合模式时，接口的 PVID 可以设置为任何 VLAN，因为它是未标记的成员。

◆ 如果可接受的帧类型设置为 **all** 或者 switchport 模式设置为 **hybrid** ，则 PVID 将插入到进入 aningress 端口的所有未标记帧中。

范例

The following 范例 shows how to set the PVID for port 1 to VLAN 3:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport native vlan 3
Console(config-if)#
```

20.2.7 vlan-trunking

此命令允许未知的 VLAN 组通过指定的接口。使用 **no** 形式禁用此功能。

语法

[no] **vlan-trunking**

缺省配置

禁用

命令模式

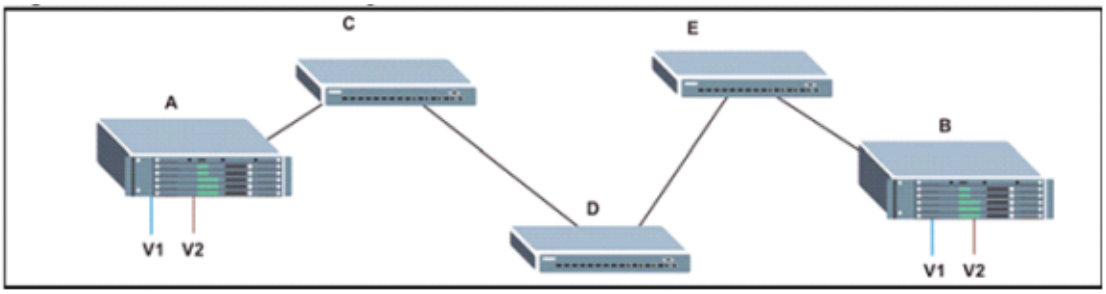
接口配置 (Ethernet, Port Channel)

命令用法

◆使用此命令配置跨越一个或多个中间交换机的隧道，这些交换机为不属于它们的 VLAN 组传递

流量。下图显示　了交换机 A 和 B 上　配置的 VLAN 1 和 2　，VLAN 中继用于为这些 VLAN 传输流量 VLAN 组跨越交换机 C，D 和 E。

20.3 配置 VLAN 中继



如果没有 VLAN 中继，则必须在所有中间交换机上配置 VLAN 1 和 2 - C，D 和 E;　否则这些交换机将丢弃具有未知 VLAN 组标签的任何帧。但是通过沿着连接 VLAN 1 和 2 的路径上的中间交换机端口启用 VLAN 中继，您只需要在交换机 A 和 B 中创建这些 VLAN 组。交换机 C，D 和 E 自动允许具有 VLAN 组标签 1 和 2 的帧（组是未知的 thoseswitches）通过他们的 VLAN 中继端口。

◆　VLAN 中继与“access”switchport 模式互斥(请参阅　switchport mode　命令)。　如果　在接口上启用 VLAN 中继，则该接口不能设置为访问模式，反之亦然。

◆　为防止在生成树中形成环路，所有未知 VLAN 将绑定到单个实例（STP / RSTP 或 MSTP 实例，取决于　所选的 STA 模式)。

◆　如果在接口上禁用 VLAN 中继和入口过滤，则仍允许具有未知 VLAN 标记的数据包进入此接口，并且将被泛洪到启用 VLAN 中继的所有其他端口。(换句话说，对于未知 VLAN，仍然可以有效地启用 VLAN 中继)。

范例

以下示例在端口 9 和 10 上启用 VLAN 中继，以便为未知 VLAN 组建立跨交换机的路径：

```
Console(config)#interface ethernet 1/9

Console(config-if)#vlan-trunking

Console(config-if)#interface ethernet 1/10

Console(config-if)#vlan-trunking

Console(config-if)#
```

20.4 显示 VLAN 信息

20.4.1 show vlan

This command shows VLAN information.

语法

show vlan [**id** *vlan-id* | **name** *vlan-name*]

id -要跟随 VLAN ID 的关键字。

vlan-id -配置的 VLAN 的 ID。 （范围：1-4093）

name -要为 VLAN 名称后跟的关键字。

vlan-name - 1 到 32 个字符的 ASCII 字符串。

缺省配置

显示所有 VLAN

命令模式

普通模式, 特权模式

范例

以下示例显示如何显示 VLAN 1 的信息：

```
Console#show vlan id 1

VLAN ID: 1

Type: Static

Name: DefaultVlan

Status: Active

Ports/Port Channels : Eth1/ 1(S) Eth1/ 2(S) Eth1/ 3(S) Eth1/ 4(S) Eth1/ 5(S)

Eth1/ 6(S) Eth1/ 7(S) Eth1/ 8(S) Eth1/ 9(S) Eth1/10(S)

Eth1/11(S) Eth1/12(S) Eth1/13(S) Eth1/14(S) Eth1/15(S)

Eth1/16(S) Eth1/17(S) Eth1/18(S) Eth1/19(S) Eth1/20(S)

Eth1/21(S) Eth1/22(S) Eth1/23(S) Eth1/24(S) Eth1/25(S)

Eth1/26(S) Eth1/27(S) Eth1/28(S)

Console#
```

20.5 配置基于协议的 VLAN

支持多种协议所需的网络设备不能轻易地分组到公共 VLAN 中。这可能需要非标准设备在不同 VLAN 之间传递流量，以包含参与特定协议的所有设备。这种配置剥夺了用户 VLAN 的基本优势，包括安全性和易接近性。

要避免这些问题，可以使用基于协议的 VLAN 配置此交换机，该物理网络将物理网络划分为每个所需协议的逻辑 VLAN 组。 当在端口处接收到帧时，可以基于入站分组使用的协议类型来确定其 VLAN 成员。

要配置基于协议的 VLAN，请按照下列步骤操作：

1. 首先为要使用的协议配置 VLAN 组。虽然不是强制性的，但我们建议为网络上运行的每个主要协议配置一个单独的 VLAN。此时不要添加端口成员。
2. 使用 protocol-vlan protocol-group 命令（全局配置模式）为要分配给 VLAN 的每个协议创建协议组 。
3. 然后使用 protocol-vlan protocol-group 命令（接口配置模式）将每个接口的协议映射到适当的 VLAN。

20.5.1 protocol-vlan protocol-group

此命令创建协议组，或将特定协议添加到一个组。使用 no 形式删除协议组。

语法

protocol-vlan protocol-group *group-id* [{**add** | **remove**}**frame-type** *frame* **protocol-type** *protocol*]

no protocol-vlan protocol-group *group-id*

group-id -该协议组的组标识符。（范围：1-2147483647）

frame-此协议使用的帧类型。 （选项：ethernet，rfc_1042，llc_other）

protocol -协议类型。 llc_other 帧类型的唯一选项是 ipx_raw。 所有其他帧类型的选项包括：arp，ip，ipv6，rarp。

缺省配置

没有配置协议组

命令模式

全局配置

范例

以下创建协议组 1，并指定具有 IP 和 ARP 协议类型的以太网帧：

```
Console(config)#protocol-vlan protocol-group 1 add frame-type ethernet
protocol-type ip
Console(config)#protocol-vlan protocol-group 1 add frame-type ethernet
protocol-type arp
Console(config)#
```

20.5.2 protocol-vlan protocol-group

此命令将协议组映射到当前接口的 VLAN。使用 no 形式删除此接口的协议映射。

语法

protocol-vlan protocol-group *group-id* **vlan** *vlan-id* **priority** *priority*

no protocol-vlan protocol-group *group-id* **vlan**

group-id -该协议组的组标识符。（范围：1-2147483647）

vlan-id -转发匹配协议流量的 VLAN。（范围：1-4093）

priority -分配给未标记的入口流量的优先级。（范围：0-7，其中 7 是最高优先级）

缺省配置

没有为任何接口映射协议组

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

◆创建基于协议的 VLAN 时，仅通过此命令分配接口。如果使用任何其他 VLAN 命令（例如 vlan 命令）分配接口，则这些接口将允许任何协议类型进入关联的 VLAN。

◆ 当同时支持基于 MAC，基于 IP 子网和基于协议的 VLAN 时，将按此顺序应用优先级，然后基于端口的 VLAN 持续使用。

◆ 当帧进入已分配给协议 VLAN 的端口时，将按以下方式处理：

- 如果框架已标记，则将根据应用于标记框架的标准规则对其进行处理。
- 如果帧未标记且协议类型匹配，则帧将转发到相应的 VLAN。
- 如果帧未标记但协议类型不匹配，则将帧转发到此接口的默认 VLAN。

范例

以下示例将进入端口 1 的流量映射到与协议组 1 中指定的协议类型匹配到 VLAN 2。

```
Console(config)#interface ethernet 1/1

Console(config-if)#protocol-vlan protocol-group 1 vlan 2

Console(config-if)#
```

20.5.3 show protocol-vlan protocol-group

此命令显示与协议组关联的帧和协议类型。

语法

show protocol-vlan protocol-group [*group-id*]

group-id - Group identifier for a protocol group.(范围: 1-2147483647)

缺省配置

显示所有协议组

命令模式

特权模式

范例

这显示了为以太网 IP 配置的协议组 1：

```
Console#show protocol-vlan protocol-group

Protocol Group ID Frame Type Protocol Type

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

1 ethernet 08 00

Console#
```

20.5.4 show interfaces protocol-vlan protocol-group

此命令显示从协议组到所选接口的 VLAN 的映射。

语法

show interfaces protocol-vlan protocol-group [*interface*]

interface

ethernet *单元 / 端口*

unit - 单位标识符。 （范围：1）

port - 端口号。 （范围：1-28）

port-channel *channel-id* (范围: 1-12)

缺省配置

显示所有接口的映射

命令模式

特权模式

范例

这表明进入端口 1 的与协议组 1 的规范匹配的流量将映射到 VLAN 2：

```
Console#show interfaces protocol-vlan protocol-group

Port ProtocolGroup ID VLAN ID

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

Eth 1/1 1 vlan2

Console#
```

20.6 配置 IP 子网 VLAN

使用基于 IEEE 802.1Q 端口的 VLAN 分类时，端口接收的所有未标记帧都归类为属于其 VSID（PVID）与该端口关联的 VLAN。

启用基于 IP 子网的 VLAN 分类时，将根据 IP 子网到 VLAN 映射表检查非标记入口帧的源地址。 如果找到该子网的条目，则这些帧区域指向条目中指示的 VLAN。 如果没有匹配 IP 子网，则将标记的帧分类为属于接收端口的 VLAN ID（PVID）。

20.6.1 subnet-vlan

此命令配置 IP 子网 VLAN 分配。使用 **no** 形式删除 IP 子网到 VLAN 的分配。

语法

subnet-vlan subnet *ip-address mask* **vlan** *vlan-id* [**priority** *priority*]

no subnet-vlan subnet {*ip-address mask* | **all**}

ip-address - 定义子网的 IP 地址。有效的 IP 地址由四个十进制数组成，0 到 255，由句点分隔。

mask - 此掩码标识 IP 子网的主机地址位。

vlan-id - 转发匹配 IP 子网流量的 VLAN。（范围：1-4093）

priority - 分配给未标记的入口流量的优先级。（范围：0-7，其中 7 是最高优先级）

缺省配置

Priority: 0

命令模式

全局配置

命令用法

◆每个 IP 子网只能映射到一个 VLAN ID。IP 子网包含 IP 地址和子网掩码。指定的 VLAN 不需要是现有 VLAN。

◆ 当端口收到未标记的帧时，源 IP 地址对 IP 子网到 VLAN 映射表进行了缺失 ，如果找到该条目，则将相应的 VLAN ID 分配给该帧。如果未找到映射，则将接收端口的 PVID 分配给帧。

◆ IP 子网不能是广播或多播 IP 地址。

◆ 当同时支持基于 MAC，基于 IP 子网和基于协议的 VLAN 时，将按此顺序应用优先级，然后继续使用基于端口的 VLAN。

范例

以下示例将子网 192.168.12.192（mask255.255.255.224）的流量分配给 VLAN 4。

```
Console(config)#subnet-vlan subnet 192.168.12.192 255.255.255.224 vlan 4
Console(config)#
```

20.6.2 show subnet-vlan

此命令显示 IP 子网 VLAN 分配。

命令模式

特权模式

命令用法

◆使用此命令显示子网到 VLAN 映射。

◆ 如果可以匹配多个条目，则使用最后匹配的条目。

范例

以下示例显示所有已配置的基于 IP 子网的 VLAN。

```
Console#show subnet-vlan

IP Address Mask VLAN ID Priority

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

192.168.12.0 255.255.255.128 1 0

192.168.12.128 255.255.255.192 3 0

192.168.12.192 255.255.255.224 4 0

192.168.12.224 255.255.255.240 5 0

192.168.12.240 255.255.255.248 6 0

192.168.12.248 255.255.255.252 7 0

192.168.12.252 255.255.255.254 8 0

192.168.12.254 255.255.255.255 9 0

192.168.12.255 255.255.255.255 10 0

Console#
```

20.7 配置基于 MAC 的 VLAN

使用基于 IEEE 802.1Q 端口的 VLAN 分类时，端口接收的所有未标记帧都归类为属于其 VSID（PVID）与该端口关联的 VLAN。

启用基于 MAC 的 VLAN 分类时，将根据 MAC 地址到 VLAN 映射表检查分区入口帧的源地址。 如果找到该地址的条目，则这些帧区域指向条目中指示的 VLAN。如果没有匹配的 MAC 地址，则未标记的帧被分类为属于接收端口的 VLAN ID(PVID)。

20.7.1 mac-vlan

该命令用来配置 MAC 地址到 VLAN 的映射关系。使用 no 形式删除作业。

语法

mac-vlan mac-address *mac-address* **vlan** *vlan-id* [**priority** *priority*]

no mac-vlan mac-address {*mac-address* | **all**}

mac-address - 要匹配的源 MAC 地址。ConfiguredMAC 地址只能是单播地址。MAC 地址必须以

xx-xx-xx-xx-xx-xx 或 xxxxxxxxxxxx 格式指定。

vlan-id - 匹配源 MAC 地址流量转发到的 VLAN。（范围：1-4093）

priority - 分配给未标记的入口流量的优先级。（范围：0-7，其中 7 是最高优先级）

缺省配置

无

命令模式

全局配置

命令用法

◆MAC-to-VLAN 映射适用于交换机上的所有端口。

◆源 MAC 地址只能映射到一个 VLAN ID。

◆配置的 MAC 地址不能是广播或 组播地址。

◆当同时支持基于 MAC，基于 IP 子网和基于协议的 VLAN 时，将按此顺序应用优先级，然后继续使用基于端口的 VLAN。

范例

以下示例将来自源 MAC 地址 00-00-00-11-22-33 的流量分配给 VLAN 10。

```
Console(config)#mac-vlan mac-address 00-00-00-11-22-33 vlan 10

Console(config)#
```

20.7.2 show mac-vlan

此命令显示 MAC 地址到 VLAN 的分配。

命令模式

特权模式

命令用法

使用此命令可以显示 MAC 地址到 VLAN 的映射。

范例

以下示例显示所有已配置的基于 MAC 地址的 VLAN。

```
Console#show mac-vlan

MAC Address VLAN ID Priority

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

00-00-00-11-22-33 10 0

Console#

20.8 配置语音 VLAN

交换机允许您为网络指定语音 VLAN，并为 VoIP 流量设置 aCoS 优先级。可以使用数据包的源 MAC 地址在交换机端口上检测 VoIP 流量，也可以使用 LLDP（IEEE802.1AB)来发现连接的 VoIP 设备。在配置的端口上检测到 VoIP 流量时，交换机会自动将端口分配给 VoiceVLAN。或者可以手动配置交换机端口。

20.8.1 voice vlan

此命令启用 VoIP 流量检测并定义语音 VLANID。使用 **no** 形式禁用 Voice VLAN。

语法

voice vlan *voice-vlan-id*

no voice vlan

voice-vlan-id -指定语音 VLAN ID。 （范围：1-4093）

缺省配置

禁用

命令模式

全局配置

命令用法

◆在企业网络中部署 IP 电话时 ，建议将 IP 语音（VoIP）网络流量与其他数据流量隔离开来。 流量隔离有助于防止过多的数据包延迟，数据包丢失和抖动，从而提高语音质量。 最好通过将所有 VoIP 流量分配到单个 VLAN 来实现。

◆ 可以使用数据包的源 MAC 地址在交换机端口上检测 VoIP 流量，也可以使用 LLDP（IEEE 802.1AB）来发现连接的 VoIP 设备。在配置端口上检测到 VoIP 流量时，交换机会自动将端口分配为 语音 VLAN 的成员。

◆ 只能支持一个 Voice VLAN,并且必须先在该开关上创建,然后才能将其指定为 Voice VLAN。

◆ 启用全局自动检测状态时，无法修改语音 VLAN ID（请参阅 switchp ort voice vlan 命令。

范例

以下示例启用 VoIP 流量检测，并将 VoiceVLAN ID 指定为 1234。

```
Console(config)#voice vlan 1234

Console(config)#
```

20.8.2 voice vlan aging

此命令用于设置 Voice VLAN ID 超时。使用 no 形式恢复默认值。

语法

voice vlan aging *minutes*

no voice vlan

minutes -指定端口 Voice VLAN 成员资格超时。（范围：5-43200 分钟）

缺省配置

1440 分钟

命令模式

全局配置

命令用法

Voice VLAN 老化时间是在端口上不再接收 VoIP 流量时从语音 VLAN 中删除端口的时间。

范例

以下示例将 Voice VLAN 老化时间配置为 3000 分钟。

```
Console(config)#voice vlan aging 3000

Console(config)#
```

20.8.3 voice vlan mac-address

此命令指定要添加到 OUI 列表的 MAC 地址范围。 使用 no 形式从列表中删除条目。

语法

voice vlan mac-address *mac-address* **mask** *mask-address*[**description** *description*]

no voice vlan mac-address *mac-address* **mask** *mask-address*

mac-address -定义标识网络中 VoIP 设备的 MAC 地址 OUI。 （例如，01-23-45-00-00-00）

mask-address -标识一系列 MAC 地址。 （范围：80-00-00-00-00-00 至 FF-FF-FF-FF-FF-FF）

description -标识 VoIP 设备的用户自定义文本。（范围：1-32 个字符）

缺省配置

无

命令模式

全局配置

命令用法

◆连接到交换机的 VoIP 设备可以通过制造商的组织唯一标识符（OUI）在收到的数据包的 sourceMAC 地址中进行标识。 OUI 号码被分配给制造商并形成设备 MAC 地址的前三个八位字节。 可以在交换机上配置 VoIP 设备的 MAC OUI 号码，以便来自这些设备的流量被识别为 VoIP。

◆ 选择 FF-FF-FF-00-00-00 的掩码可识别具有相同 OUI（前三个八位字节）的所有设备。 其他掩码限制 MAC 地址范围。选择 FF-FF-FF-FF-FF-FF 指定单个 MAC 地址。

范例

以下示例将 MAC OUI 添加到 OUI 电话列表。

```
Console(config)#voice vlan mac-address 00-12-34-56-78-90 mask ff-ff-ff-00-00-
00 description A new phone
Console(config)#
```

20.8.4 switchport voice vlan

此命令指定端口的语音 VLAN 模式。 在端口上 使用 no 形式禁用 Voice VLAN 功能。

语法

switchport voice vlan {**manual** | **auto**}

no switchport voice vlan

manual -端口上已启用 Voice VLAN 功能，但必须手动将端口添加到 Voice VLAN。

auto -当在端口上检测到 VoIP 流量时，该端口将作为标记成员添加到 VoiceVLAN。

缺省配置

禁用

命令模式

接口配置

命令用法

◆选择 auto 时，必须使用 switchport voicevlan rule 命令选择用于检测 Voip 流量的方法，OUI 或 802.1ab(LLDP)。当选择 OUI，务必使用语音 VLAN MAC 在电话 OUI 列表配置 theMAC 地址范围-address 命令。

◆ 默认情况下，所有端口都设置为 VLAN 混合模式。在为端口启用 VoIP 之前（通过将 VoIP 模式设置为 Auto 或 Manual，如下所述），确保使用 switchport mode 命令 未将 VLAN 成员资格设置为访问模式 。

范例

以下示例将端口 1 设置为语音 VLAN 自动模式。

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport voice vlan auto
Console(config-if)#
```

20.8.5 switchport voice vlan priority

此命令指定端口上 VoIP 流量的 CoS 优先级。使用 no 形式恢复端口的默认优先级。

语法

switchport voice vlan priority *priority-value*

no switchport voice vlan priority

priority-value - The CoS priority value. (范围: 0-6)

缺省配置

6

命令模式

接口配置

命令用法

指定应用于语音 VLAN 上的端口 VoIP 流量的 CoS 优先级。当端口的语音 VLAN 功能处于活动状态时，任何接收到的 VoIP 数据包的优先级都会被新优先级覆盖。

范例

以下示例将端口 1 上的 CoS 优先级设置为 5。

```
Console(config)#interface ethernet 1/1

Console(config-if)#switchport voice vlan priority 5

Console(config-if)#
```

20.8.6 switchport voice vlan rule

此命令选择用于检测端口上的 VoIP 流量的方法。使用 no 形式禁用端口上的检测方法。

语法

[no] **switchport voice vlan rule** {**oui** | **lldp**}

oui -来自 VoIP 设备的流量由源 MAC 地址的组织独特标识符（OUI）检测。

lldp -使用 LLDP 发现连接到端口的 VoIP 设备。

缺省配置

OUI: 启用

LLDP: 禁用

命令模式

接口配置

命令用法

◆选择 OUI 时，请务必在 Telephony OUI 列表中配置 MAC 地址范围（请参阅 voice vlan mac-address 命令。必须在 Telephony OUI 列表中配置 MAC 地址 OUI 号，以便交换机将流量识别为来自 VoIP 装置。

◆ LLDP 检查的“电话位”的系统能力 TLV isturned 上。见 “LLDP 指令” 更多 informationon LLDP。

范例

以下示例启用端口 1 上的 OUI 方法以检测 VoIP 流量。

```
Console(config)#interface ethernet 1/1

Console(config-if)#switchport voice vlan rule oui

Console(config-if)#
```

20.8.7 switchport voice vlan security

此命令启用端口上 VoIP 流量的安全筛选。使用 no 形式禁用端口上的过滤。

语法

[no] switchport voice vlan security

缺省配置

禁用

命令模式

接口配置

命令用法

◆安全过滤会丢弃在使用语音 VLAN ID 标记的端口上收到的所有非 VoIP 数据包。VoIP 流量由 Telephony OUI 列表中配置的源 MAC 地址识别，或通过发现连接到交换机的 VoIP 设备的 LLDP 识别。从非 VoIP 源接收的数据包将被丢弃。

◆启用后，请确保在 OUI 列表（ voice vlan mac-address ）中配置 VoIP 设备的 MAC 地址范围 。

范例

以下示例在端口 1 上启用安全筛选。

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport voice vlan security
Console(config-if)#
```

20.8.8 show voice vlan

此命令显示交换机上的语音 VLAN 设置和 OUI 电话列表。

语法

show voice vlan {oui | status}

oui -显示 OUI 电话列表。

status -显示全局和端口语音 VLAN 设置。

缺省配置

无

命令模式

特权模式

范例

```
Console#show voice vlan status

Global Voice VLAN Status

Voice VLAN Status : Enabled

Voice VLAN ID : 1234

Voice VLAN aging time : 1440 minutes

Voice VLAN Port Summary

Port Mode Security Rule Priority Remaining Age

(minutes)

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

Eth 1/ 1 Auto Enabled OUI 6 100

Eth 1/ 2 Disabled Disabled OUI 6 NA

Eth 1/ 3 Manual Enabled OUI 5 100

Eth 1/ 4 Auto Enabled OUI 6 100

Eth 1/ 5 Disabled Disabled OUI 6 NA

Eth 1/ 6 Disabled Disabled OUI 6 NA

Eth 1/ 7 Disabled Disabled OUI 6 NA

Eth 1/ 8 Disabled Disabled OUI 6 NA

Eth 1/ 9 Disabled Disabled OUI 6 NA

Eth 1/10 Disabled Disabled OUI 6 NA

Console#show voice vlan oui

OUI Address Mask Description

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

00-12-34-56-78-9A FF-FF-FF-00-00-00 old phones

00-11-22-33-44-55 FF-FF-FF-00-00-00 new phones

00-98-76-54-32-10 FF-FF-FF-FF-FF-FF Chris' phone

Console#
```

21 类服务指令

本节中描述的命令允许您指定在交换机 dueto 拥塞中缓冲流量时哪些数据包具有更高的优先级。此交换机支持 CoS，每个端口有 8 个优先级队列。端口高优先级队列中的数据包将在优先级较低的队列之前传输。 可以为每个接口设置默认优先级，也可以为队列服务模式设置默认优先级，并且可以配置帧优先级标记到交换机优先级队列的映射。

21.1 优先命令（第 2 层）

本节介绍用于在交换机上配置第 2 层流量优先级的命令。

21.1.1 queue mode

此命令设置用于处理每个服务类（CoS）优先级队列的调度模式。选项包括严格优先级，加权循环（WRR）或严格和加权排队的组合。使用 no 形式恢复默认值。

语法

queue mode {**strict** | **wrr** | **strict-wrr** [*queue-type-list*]}

no queue mode

strict -按顺序为出口队列提供服务，在服务较低优先级之前在较高优先级队列中传输所有流量。这可确保始终优先考虑优先级最高的数据包，优先于所有其他流量。

wrr -加权 Round-Robin 使用调度权重（基于队列权重命令）在出口端口共享带宽，并以循环方式为每个队列服务。

strict-wrr -严格优先级用于高优先级队列，WRR 用于其余队列。

queue-type-list -指示队列是普通类型还是严格类型。（选项：0 表示正常队列，1 表示严格队列）

缺省配置

WRR

命令模式

全局配置

命令用法

◆交换机可以设置为基于 严格 优先级，WRR 或 严格和加权 队列的组合来服务端口队列 。

◆ 严格优先级要求在为优先级较低的队列提供服务之前，处理优先级较高的队列中的所有流量。

◆Wei Ghted Round Robin（WRR）使用预定义的相对权重 foreach 队列，该队列确定 switch 在转移到下一个队列之前服务每个队列的服务时间百分比。这可以防止严格优先级排队时发生的行头阻塞。使用 queue weight 命令为 WRR 队列分配权重给优先级队列。

◆ 如果选择了 Strict 和 WRR 模式，则对高优先级队列和剩余队列的加权服务使用严格服务的组合。应使用严格模式字段参数指定分配给使用严格优先级的队列。

◆ 可以为每个加权队列分配（从而分配给相应的流量优先级）。此权重设置每个队列轮询服务的频率，并随后影响分配了特定优先级值的软件应用程序的响应时间。

◆通过定义 WRR 的调度权限或使用严格和加权排队组合的排队模式，在出口端口共享服务时间。通过计算每轮精确的每秒字节数来为每个队列分配服务时间 。

◆指定的队列模式适用于所有接口。

◆用于同步分布式交换机的协议使用 1588 字节的数据包来控制同步过程。 因此将此大小的数据包分配给最高优先级队列，以确保快速通过。

范例

以下示例将队列模式设置为严格优先级服务模式：

```
Console(config)#queue mode strict

Console(config)#
```

21.1.2 queue weight

当使用加权排队时，该命令将权重分配给八类服务（CoS）优先级，或者使用严格加权排队和加权排队组合的一种排队模式。使用 no 形式恢复默认权重。

语法

queue weight *weight0...weight7*

no queue weight

weight0...weight7 -队列 0 至 7 的权重比决定了 WRR 调度器所使用的权重。（范围：1-255）

缺省配置

Weights 1, 2, 4, 6, 8, 10, 12, 14 are assigned to queues 0 - 7 respectively.

命令模式

全局配置

命令用法

◆此命令通过定义加权循环的权重，或者使用严格加权排队和加权排队组合的排队模式，在出口端口具有带宽。

◆　通过计算每轮将要服务的精确每个字节数来为每个队列分配带宽　。

范例

以下示例显示如何将 1 - 4 的循环权重分配给 CoS 优先级队列 0 - 7。

```
Console(config)#queue weight 1 2 3 4 5 6 7 8

Console(config)#
```

21.1.3 switchport priority default

此命令为传入的未标记帧设置优先级。使用 no 形式恢复默认值。

语法

switchport priority 缺省配置 *default-priority-id*

no switchport priority 缺省配置

default-priority-id-未标记入口流量的优先级编号。优先级是 0 到 7 之间的数字.7 是最高优先级。

缺省配置

未设置优先级，并且接口上接收的未标记帧的默认值为零。

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

◆优先级映射的优先级是 IP DSCP，然后是缺省端口优先级。

◆默认优先级适用于在端口集上接收的未标记帧以接受所有帧类型（即接收未标记帧和标记帧）。　此优先级不适用于 IEEE 802.1Q VLAN 标记帧。如果传入帧是 IEEE 802.1Q VLAN 标记帧，则将使用 IEEE 802.1p 用户优先级位。

◆交换机为每个端口提供 8 个优先级队列。它可以配置为使用严格优先级排队，Weighted Round Robin（WRR），或使用 queue mode 命令组合严格和加权排队。没有 VLAN 标记的入站帧使用输入端口的默认入口用户优先级标记，然后放在输出端口的适当优先级队列中。　所有入端口的默

认优先级为零。因此任何没有优先级标记的入站帧都将放置在输出端口的队列 2 中。（请注意，如果输出端口是关联 VLAN 的未标记成员，则在传输之前会删除所有 VLAN 标记。）

范例

以下示例显示如何在端口 3 到 5 上设置默认优先级：

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport priority default 5
Console(config-if)#
```

21.1.4 show queue mode

此命令显示当前队列模式。

命令模式

特权模式

范例

```
Console#show queue mode
Queue Mode : Weighted Round Robin Mode
Console#
```

21.1.5 show queue weight

此命令显示用于加权队列的权重。

命令模式

特权模式

范例

```
Console#show queue weight
Queue ID Weight
-------- ------
0 1
1 2
2 4
3 6
```

```
4 8

5 10

6 12

7 14

Console#
```

21.2 优先命令（第 3 层和第 4 层）

本节介绍用于在交换机上配置第 3 层和第 4 个交通优先权映射的命令。

21.2.1 qos map cos-dscp

此命令将传入数据包中的 CoS / CFI 值映射到每个跃点行为，并删除优先级处理的优先级值。 使用 no 形式恢复默认设置。

语法

qos map cos-dscp *phb drop-precedence* **from** *cos0 cfi0...cos7 cfi7*

no qos map cos-dscp *cos0 cfi0...cos7 cfi7*

phb -每跳行为，或此路由器跃点使用的优先级。（范围：0-7）

drop-precedence -用于控制流量拥塞的丢弃优先级。（范围：0-绿色，3-黄色，1-红色）

cos -入口数据包中的 CoS 值。（范围：0-7）

cfi -规范格式指示器。将此参数设置为“0”表示帧中携带的 MAC 地址信息为标准化的格式。（范围：0-1）

缺省配置

缺省配置 Mapping of CoS/CFI to Internal PHB/Drop Precedence

CoS	CFI	0	1
0		(0,0)	(0,0)
1		(1,0)	(1,0)
2		(2,0)	(2,0)
3		(3,0)	(3,0)
4		(4,0)	(4,0)
5		(5,0)	(5,0)
6		(6,0)	(6,0)
7		(7,0)	(7,0)

命令模式

接口配置 (Port, Static Aggregation)

命令用法

◆CoS 到 PHB 值的默认映射基于 IEEE 802.1p 中用于将 CoS 值映射到输出队列的建议设置。

◆输入内部每跳行为和下降优先权的值对，后跟关键字“from”，然后输入最多八个 CoS / CFI 配对值，用空格分隔。

◆如果数据包到达时带有 802.1Q 报头但不是 IP 数据包,则使用 CoS/CFI 到 PHB/Drop Precedenc 映射表生成内部处理的优先级和丢弃优先级值。注意优先级标记在此命令不会修改原始数据包。

◆ 内部 DSCP 由用于每跳行为（PHB）的三个比特组成，用于确定 发送数据包的队列； 和两位 fordrop 优先级（即颜色），用于控制流量拥塞。

范例

```
Console(config)#interface ethernet 1/5

Console(config-if)#qos map cos-dscp 0 0 from 0 1

Console(config-if)#
```

21.2.2 qos map dscp-mutation

此命令将传入数据包中的 DSCP 值映射到优先级处理的每跳行为和丢弃优先级值。使用 no 形式恢复默认设置。

语法

qos map dscp-mutation *phb drop-precedence* **from** *dscp0 ... dscp7*

no qos map dscp-mutation *dscp0 ... dscp7*

phb-每跳行为，或此路由器跃点使用的优先级。（范围：0-7）

drop-precedence-用于控制流量拥塞的丢弃优先级。（范围：0-绿色， 3-黄色，1-红色）

dscp-入口数据包中的 DSCP 值。（范围：0-63）

缺省配置

缺省配置 Mapping of DSCP Values to Internal PHB/Drop Values

ingress-dscp1 ingress-dscp10	0	1	2	3	4	5	6	7	8	9
0	0,0	0,1	0,0	0,3	0,0	0,1	0,0	0,3	1,0	1,1
1	1,0	1,3	1,0	1,1	1,0	1,3	2,0	2,1	2,0	2,3
2	2,0	2,1	2,0	2,3	3,0	3,1	3,0	3,3	3.0	3,1
3	3,0	3,3	4,0	4,1	4,0	4,3	4,0	4,1	4.0	4,3
4	5,0	5,1	5,0	5,3	5,0	5,1	6,0	5,3	6,0	6,1
5	6,0	6,3	6,0	6,1	6,0	6,3	7,0	7,1	7.0	7,3
6	7,0	7,1	7,0	7,3						

命令模式

接口配置 (Port, Static Aggregation)

命令用法

◆输入内部每跳行为和下降优先权的值对，后跟关键字“from”，然后输入最多八个以空格分隔的 DSCP 值。

◆此映射仅在 qos map trust-mode 命令将 QoS 映射模式设置为“DSCP”时使用，并且入口数据包类型为 IPv4。

◆两个 QoS 域可以具有不同的 DSCP 定义，因此 DSCP-toPHB/Drop Precedence 变异映射可用于修改一组 DSCP 值以匹配另一个域的定义。应该在 QoS 管理域的边界处的接收端口 （入口突变）应用变异映射 。

◆指定的映射适用于所有接口。

范例

此示例更改进入端口 1 的所有数据包的优先级，其中 DSCP 值为 1，每跳行为为 3，下降优先权为 1.参考映射表，请注意这些数据包的 DSCP 值现在设置为 25（ $3x2^3+1$）并传递到出口接口。

```
Console(config)#interface ethernet 1/5
```

```
Console(config-if)#qos map dscp-mutation 3 1 from 1

Console(config-if)#
```

21.2.3 qos map phb-queue

此命令根据内部每跳行为值确定要使用的硬件输出队列。 使用 no 表单恢复默认设置。.

语法

qos map phb-queue *queue-id* **from** *phb0 ... phb7*

no map phb-queue *phb0 ... phb7*

phb -此命令根据内部每跳行为值确定要使用的硬件输出队列 使用 no 形式恢复默认设置。

缺省配置

Mapping Internal Per-hop Behavior to Hardware Queues

Per-hop Behavior	0	1	2	3	4	5	6	7
Hardware Queues	2	0	1	3	4	5	6	7

命令模式

接口配置 (Port, Static Aggregation)

命令用法

◆输入一个队列标识符，后跟关键字“from”，然后输入由空格分隔的内部每跳行为值。

◆ 根据此命令定义的映射，将出口数据包放入硬件队列。

范例

```
Console(config)#interface ethernet 1/5

Console(config-if)#qos map phb-queue 0 from 1 2 3

Console(config-if)#
```

21.2.4 qos map trust-mode

此命令将 QoS 映射设置为 DSCP 或 CoS。使用 no 形式恢复默认设置。

语法

qos map trust-mode {**dscp** | **cos**}

no qos map trust-mode

dscp -将 QoS 映射模式设置为 DSCP。

cos -将 QoS 映射模式设置为 CoS。

缺省配置

CoS

命令模式

接口配置（Port）

命令用法

◆如果使用此命令将 QoS 映射模式设置为 DSCP，并且应用程序包类型为 IPv4，则优先级处理将基于入口数据包中的 DSCP 值。

◆如果 QoS 映射模式设置为 DSCP，并且接收到非 IP 数据包，则在标记数据包时，将使用数据包的 CoS 和 CFI（规范格式指示符）值进行优先级处理。对于未带标记的数据包，默认端口优先级用于优先级处理。

◆如果使用此命令将 QoS 映射模式设置为 CoS，并且入口数据包类型为 IPv4，则优先级处理将基于入口数据包中的 CoS 和 CFI 值。对于未标记数据包，默认端口优先级用于优先级处理。

范例

此示例根据“命令用法”部分中描述的条件将 QoS 优先级映射模式设置为使用 DSCP。

```
Console(config)#interface ge1/1

Console(config-if)#qos map trust-mode dscp

Console(config-if)#
```

21.2.5 show qos map cos-dscp

此命令显示入口 CoS / CFI 到内部 DSCP 映射。

语法

show qos map cos-dscp interface *interface*

interface

ethernet *unit/port*

unit -单位标识符。（范围：1）

port -端口号。（范围：1-28）

port-channel *channel-id*（范围：1-12）

命令模式

特权模式

范例

```
Console#show qos map cos-dscp interface ethernet 1/5

CoS Information of Eth 1/5

CoS-DSCP map.(x,y),x: PHB,y: drop precedence:

CoS : CFI 0 1

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

0 (0,0) (0,0)

1 (1,0) (1,0)

2 (2,0) (2,0)

3 (3,0) (3,0)

4 (4,0) (4,0)

5 (5,0) (5,0)

6 (6,0) (6,0)

7 (7,0) (7,0)

Console#
```

21.2.6 show qos map dscp-mutation

此命令显示入口 DSCP 到内部 DSCP 映射。

语法

show qos map dscp-mutation interface *interface*

interface

ethernet *unit/port*

unit -单位标识符。（范围：1）

port -端口号。（范围：1-28）

port-channel *channel-id*（范围：1-12）

命令模式

特权模式

命令用法

此映射仅在 qos map trust-mode 命令将 QoS 映射模式设置为“DSCP”时使用，并且入口数据包类型为 IPv4。

范例

入口 DSCP 由“d1”（左列中的最高有效位）和“d2”（顶行中的最低有效位（换句话说，入口 DSCP=d1*10+d2））组成;以及相应的内部 DSCP 和滴点优先级显示在表格中的交叉单元格中。

```
Console#show qos map dscp-mutation interface ethernet 1/5

Information of Eth 1/5

DSCP mutation map.(x,y),x: PHB,y: drop precedence:

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

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

0 : (0,0) (0,1) (0,0) (0,3) (0,0) (0,1) (0,0) (0,3) (1,0) (1,1)

1 : (1,0) (1,3) (1,0) (1,1) (1,0) (1,3) (2,0) (2,1) (2,0) (2,3)

2 : (2,0) (2,1) (2,0) (2,3) (3,0) (3,1) (3,0) (3,3) (3,0) (3,1)

3 : (3,0) (3,3) (4,0) (4,1) (4,0) (4,3) (4,0) (4,1) (4,0) (4,3)

4 : (5,0) (5,1) (5,0) (5,3) (5,0) (5,1) (6,0) (5,3) (6,0) (6,1)

5 : (6,0) (6,3) (6,0) (6,1) (6,0) (6,3) (7,0) (7,1) (7,0) (7,3)

6 : (7,0) (7,1) (7,0) (7,3)

Console#
```

21.2.7 show qos map phb-queue

此命令显示硬件队列映射的内部每跳行为。

语法

show qos map phb-queue interface *interface*

interface

ethernet *unit/port*

unit -单位标识符。（范围：1）

port -端口号。（范围：1-28）

port-channel *channel-id*（范围：1-12）

命令模式

特权模式

范例

```
Console#show qos map phb-queue interface ethernet 1/5

Information of Eth 1/5

PHB-queue map:

PHB: 0 1 2 3 4 5 6 7

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

Queue: 2 0 1 3 4 5 6 7

Console#
```

21.2.8 show qos map trust-mode

此命令显示 QoS 映射模式。

语法

show qos map trust-mode interface *interface*

interface

ethernet *unit/port*

unit -单位标识符。（范围：1）

port -端口号。（范围：1-28）

命令模式

特权模式

范例

以下显示信任模式设置为 CoS：

```
Console#show qos map trust-mode interface ethernet 1/5

Information of Eth 1/5

CoS Map Mode: CoS mode

Console#
```

22 服务质量指令

本节中描述的命令用于配置差异化服务（DiffServ）分类标准和服务策略。您可以根据访问列表，IP 优先级或 DSCP 值或 VLAN 对流量进行分类。 使用访问列表允许您根据每个数据包中包含的第 2 层，第 3 层或第 4 层信息选择流量。

QoS 配置指南

要为特定类别的入口流量创建服务策略，请按以下步骤操作：

1. 使用 class-map 命令为特定流量类别指定类名，并进入类映射配置模式。

2. 使用 match 命令根据访问列表，IPv4 DSCP 值，IPv4 优先级值，IPv6 DSCP 值或 VLAN 选择特定类型的流量。

3. 使用 policy-map 命令为将在其中处理入口流量的特定方式指定策略名称，并进入 PolicyMap 配置模式。

4. 使用 class 命令标识类映射，并进入 Policy MapClass 配置模式。策略映射最多可包含 16 个类映射。

5. 使用 set phb、set cos 或 set ip dscp 命令修改每跳行为、VLAN 标记中的服务值类或匹配业务类的 IP 报头的优先级位（IP DSCP 值），并使用警务命令之一监视参数，例如话务流和突发速率，并且丢弃任何超过指定速率的通信量，或者仅仅减少用于超过指定速率的通信的 DSCP 服务级别。

6. 使用 service-policy 命令将策略映射分配给特定接口。

备注：创建策略映射之前创建一个类映射。

22.1.1 class-map

此命令创建用于将数据包匹配到指定类的类映射，并进入类映射配置模式。使用 no 形式删除类映射。

语法

[no] **class-map** *class-map-name* [**match-any**]

class-map-name -*类映射的名称*。（范围：1-32 个字符）

match-any -匹配类地图中的任何条件。

缺省配置

无

命令模式

全局配置

命令用法

◆首先输入此命令以指定类映射并进入 ClassMap 配置模式。 然后使用 match 命令指定将在此类映射下分类的入口流量的标准。

◆ 可以将一个或多个类映射分配给策略映射。然后策略映射由服务策略绑定到接口。服务策略定义了数据包分类，服务标记和带宽管制。将策略映射绑定到接口后，不会在策略映射中添加其他类映射，也没有使用 match 或 set 命令对指定的类映射进行任何更改 。

范例

此示例创建一个类映射调用“rd-class”，并将其设置为标记为 DSCP 服务值 3 的匹配包：

```
Console(config)#class-map rd-class match-any
Console(config-cmap)#match ip dscp 3
Console(config-cmap)#
```

22.1.2 description

此命令指定类映射或策略映射的描述。

语法

description *string*

string -类映射或策略映射的描述。（范围：1-64 个字符）

命令模式

类映射配置

策略映射配置

范例

```
Console(config)#class-map rd-class#1
```

```
Console(config-cmap)#description matches packets marked for DSCP servicevalue 3
Console(config-cmap)#
```

22.1.3 match

此命令定义用于对流量进行分类的标准。使用 no 形式删除匹配条件。

语法

[no] match {access-list *acl-name* | cos *cos* | ip dscp *dscp* |ip precedence *ip-precedence* | ipv6 dscp *dscp* |source-port *interface* | vlan *vlan*}

acl-name - 访问控制列表的名称。可以指定任何类型的 ACL，包括标准或扩展 IPv4 / IPv6 ACL 和 MACACL。（范围：1-16 个字符）

cos - 一类服务价值。（范围：0-7）

dscp - 差分服务代码点值。（范围：0-63）

ip-precedence - IP 优先级值。（Ra nge：0-7）

interface

unit/port

unit -单位标识符。（范围：1）

port -端口号。（范围：1-28）

vlan - A VLAN. (范围:1-4093)

缺省配置

无

命令模式

Class Map 配置

命令用法

◆首先输入 class-map 命令以指定类映射并进入 Class Map 配置模式。然后使用 match 命令来指定必须匹配的入口数据包中的字段以限定该类映射。

◆如果入口数据包与此命令指定的 ACL 匹配，则将忽略 ACL 中包含的任何规则 。

◆如果匹配条件包括 IP ACL 或 IP 优先级规则，则 VLAN 规则不会包含在同一个类映射中。

◆如果匹配条件包括 MAC ACL 或 VLAN 规则，则 IPACL 和 IP 优先级规则都不能包含在同一个类映

射中。

◆类地图中最多可包含 16 个匹配条目。

范例

此示例创建一个名为“rd-class＃1”的类映射，并将其设置为标记为 DSCP 服务值 3 的匹配包。

```
Console(config)#class-map rd-class#1 match-any

Console(config-cmap)#match ip dscp 3

Console(config-cmap)#
```

此示例创建一个类映射调用“rd-class＃2”,并将其设置为标记为 IP 优先级服务值 5 的匹配包。

```
Console(config)#class-map rd-class#2 match-any

Console(config-cmap)#match ip precedence 5

Console(config-cmap)#
```

此示例创建一个类映射调用“rd-class＃3”，并将其设置为标记为 VLAN 1 的匹配包。

```
Console(config)#class-map rd-class#3 match-any

Console(config-cmap)#match vlan 1

Console(config-cmap)#
```

22.1.4 rename

此命令重新定义类映射或策略映射的名称。

语法

rename *map-name*

map-name -类映射或策略映射的名称。（范围：1-32 个字符）

命令模式

Class Map 配置

Policy Map 配置

范例

```
Console(config)#class-map rd-class#1

Console(config-cmap)#rename rd-class#9

Console(config-cmap)#
```

22.1.5 policy-map

此命令创建可附加到多个接口的策略映射，并进入策略映射配置模式。使用 no 形式删除策略映射。

语法

[no] **policy-map** *policy-map-name*

policy-map-name -策略映射的名称。（范围：1-32 个字符）

缺省配置

无

命令模式

全局配置

命令用法

◆使用 **policy-map** 命令指定策略映射的名称，然后使用 class 命令配置与类映射中定义的条件匹配的流量策略 。

◆ 策略映射可以包含多个类语句，这些语句可以应用于 service-policy 命令的同一接口 。

◆ 在将类映射分配给策略映射之前创建它。

范例

此示例创建一个名为“rd-policy”的策略，使用 class 命令指定先前定义的“rd-class”，使用 **set** 命令对传入数据包将接收的服务进行分类，然后使用 policeflow 命令限制平均值带宽为 100,000 Kbps，突发速率为 4000 字节，并配置响应以丢弃任何违规数据包。

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set cos 0
Console(config-pmap-c)#police flow 10000 4000 conform-action transmit
violate-action drop
Console(config-pmap-c)#
```

22.1.6 class

此命令定义策略可以在其上执行的流量分类，并进入策略映射类配置模式。使用 **no** 形式删除类映射。

语法

[**no**] **class** *class-map-name*

class-map-name - Name of the class map. (Range: 1-32 characters)

缺省配置

无

命令模式

Policy Map 配置

命令用法

◆使用 policy-map 命令指定策略映射，并进入 PolicyMap 配置模式。然后使用 **class** 命令进入 PolicyMap 类配置模式。最后使用 **set** 命令和 **police** 命令之一来指定匹配条件，其中：

■set phb 命令用于设置匹配包中的每跳行为值。(这仅修改内部处理的数据包优先级。)

■set cos 命令用于设置 matchingpackets 中的服务类值。 (这会修改 VLAN 标记 中的数据包优先级 。)

■set ip dscp 命令用来设置匹配报文中的 IP DSCP 值（这会修改 IP 报头中的报文优先级。)

■police 命令定义参数，例如最大吞吐量，突发速率和对不符合流量的响应。

◆策略映射中最多可包含 16 个类 。

范例

此示例创建一个名为“rd-policy”的策略，使用 **class** 命令指定先前定义的“rd-class”，使用 set phb 命令对传入数据包将接收的服务进行分类法，然后使用 police flow 命令限制平均带宽为 100,000 Kbps，突发速率为 4,000 字节，并配置响应以丢弃任何违规数据包。

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set phb 3
Console(config-pmap-c)#police flow 10000 4000 conform-action transmit
violate-action drop
Console(config-pmap-c)#
```

22.1.7 police flow

此命令根据主题流速定义分类流量的实施者。使用 no 形式删除监察器。

语法

[no] **police flow** *committed-rate committed-burst***conform-action transmit** **violate-action** {**drop**| *new-dscp*}

committed-rate -承诺信息速率（CIR），以千比特为单位。（范围：0-1000000 kbps，粒度为 64 kbps 或最大端口速度，以较低者为准）

committed-burst -承诺突发尺寸（BC），以字节为单位。（范围：64-16000000，粒度为 4k 字节）

conform-action -当数据包在 CIR 和 BC 内时采取的行动。（有足够的令牌来处理数据包，数据包设置为绿色）。

violate-action -数据包超过 CIR 和 BC 时采取的行动。（没有足够的令牌来处理数据包，数据包设置为红色）。

transmit -无需采取任何行动即可进行传输。

drop -违反行为要求丢弃数据包。

new-dscp -差分服务代码点（DSCP）值。（范围：0-63）

缺省配置

无

命令模式

Policy Map Class 配置

命令用法

◆您最多可以为入口端口配置 16 个策略（即类映射）。

◆承诺速率不能超过所配置的接口速度，并且所述承诺突发不能超过 16 个字节。

◆策略基于令牌桶，其中桶深度（即桶溢出之前的最大突发）通过指定承诺突发字段，并且 通过 承诺速率 选项 指定添加到桶 的平均速率 到桶。请注意，令牌桶的功能类似于 RFC 2697 和 RFC2698 中描述的功能。

◆仪表的行为是根据一个令牌桶（C）， 令牌递增的速率（CIR - CommittedInformation Rate）以及令牌桶的最大大小（BC -Committed Burst Size）来指定的。

令牌桶 C 最初是满的，即令牌计数 Tc（0）= BC。

此后，令牌计数 Tc 每秒更新 CIR 次数，如下所示：

■如果 Tc 小于 BC，则 Tc 增加 1，否则

■Tc 未递增。

当大小为 B 字节的数据包在时间 t 到达时，会发生以下情况：

■如果 Tc（t） ≥ ，则数据包为绿色，Tc 减少 B 向下最小值 0

■否则数据包为红色且 Tc 未递减。

范例

此示例创建一个名为“rd-policy”的策略，使用 class 命令指定先前定义的“rd-class”，使用 set phb 命令对传入数据包将接收的服务进行分类法，然后使用 **police flow** 命令限制平均带宽为 100,000 Kbps，突发速率为 4000 字节，并配置响应以丢弃任何违规数据包。

```
Console(config)#policy-map rd-policy

Console(config-pmap)#class rd-class

Console(config-pmap-c)#set phb 3

Console(config-pmap-c)#police flow 100000 4000 conform-action transmit

violate-action drop

Console(config-pmap-c)#
```

22.1.8 police srtcm-color

此命令基于单一三色计（srTCM）定义分类流量的执行器。使用 no 形式删除监察器。

语法

[no] police {srtcm-color-blind | srtcm-color-aware} *committed-rate committed-burst excess-burst* conform-action transmit exceed-action {drop | *new-dscp*} violate action {drop | *new-dscp*}

srtcm-color-blind -单色三色仪，采用彩色盲模式。

srtcm-color-aware -单色三色仪，采用颜色识别模式。

committed-rate -承诺信息速率（CIR），以千比特为单位。（范围：0-10000000 kbps，粒度为 64 kbps 或最大端口速度，以较低者为准）

committed-burst -承诺突发尺寸（BC），以字节为单位。（范围：64-16000000，粒度为 4k 字节）

excess-burst -超出突发尺寸（BE），以字节为单位。（范围：64-1600000，粒度为 4k 字节）

conform-action -当费率在 CIR 和 BC 范围内时采取的行动。（存储桶 BC 中有足够的令牌来处理数据包，数据包设置为绿色）。

exceed-action -当速率超过 CIR 且 BC 但在 BE 内时采取的行动。（存储桶中有足够的令牌来处理数据包，数据包设置为黄色。）

violate-action -当费率超过 BE 时采取的行动。（存储桶 BE 中没有足够的令牌来处理数据包，包装设置为红色。）

transmit -无需采取任何行动即可进行传输。

drop -超出操作或违规操作所需的丢弃数据包。

new-dscp -差分服务代码点（DSCP）值。（范围：0-63）

缺省配置

无

命令模式

Policy Map Class 配置

命令用法

◆您最多可以为入口端口配置 16 个策略（即类映射）。
◆承诺速率不能超过所配置的接口速度，并且所述承诺突发和过量突发不能超过 16 个字节。
◆ RFC 2697 中定义的 srTCM 对流量 流进行计量，并根据三个流量参数-提交信息速率(CIR)，承诺突发大小（BC）和过度突发大小（BE）处理其数据包。
◆ PHB 标签由五个比特组成，每个跳行为有三个比特， 用于控制队列拥塞的 两个比特用于 控制队列拥塞。如果 Apacket 没有超过 CIR 和 BC，则标记为绿色;如果它超过 CIR 和 BC，则为黄色，但不是 BE，否则为红色。
◆ 仪表以两种模式之一运行。在色盲模式下，仪表假定数据包流未着色。在颜色识别模式中，仪表假定某些前面的实体已预先对输入的数据包流进行着色，以使每个数据包为绿色，黄色或红色。标记(重新)根据仪表的结果对 IP 包进行着色。颜色在数据包的 DS 字段[RFC 2474]中编码。
◆仪表的行为是根据其模式和双声道桶 C 和 E 来指定的，它们都共享公共速率 CIR。令牌桶 C 的最大大小是 BC，并且桶 E 的最大大小是 BE。
令牌桶 C 和 E 最初 是满的，即令牌 countTc（0）= BC 和令牌计数 Te（0）= BE。此后，令牌计数 Tc 和 Te 每秒更新 CIR 次数，如下所示：

■如果 Tc 小于 BC，则 Tc 增加 1，否则

■如果 Te 小于 BE，则 Te 增加 1，否则

■Tc 和 Te 都不增加。

当大小为 B 字节的数据包在时间 t 到达时，如果将 srTCM 配置为在色盲模式下运行，则会发生以下情况：

■如果 Tc（t） ≥ ，则数据包为绿色，Tc 递减 B 低于 0 的 最小值，否则

■如果 Te（t） ≥ ，数据包为黄色，Te 按 B 下行递减至最小值 0，

■否则数据包为红色，Tc 和 Te 都不会递减。

当大小为 B 字节的数据包在时间 t 到达时，如果将 srT CM 配置为在颜色感知模式下运行， 则会发生以下情况 ：

■如果数据包已预先显示为绿色且 Tc（t） ≥ ，则数据包为绿色，Tc 将减少 B，最小值为 0

■如果数据包已预先着色为黄色或绿色以及是否已预先着色

■ Te（t） ≥ ，数据包为黄色，Te 向下递减至最小值 0，否则数据包为红色，均未递减。

计量策略保证了确定性行为，其中绿色数据包的体积永远不会小于 CIR 和 BC 确定的数量，也就是说，给定颜色的令牌总是花在该颜色的数据包上。有关 srTCM 其他方面的更多信息，请参阅 RFC 2697。

范例

此示例创建一个名为“rd-policy”的策略，使用 class 命令去定义先前定义的“rd-class”，使用 set phb 命令归类传入数据包将接收的服务，然后使用 **policy srtcm-color-blind** 命令将平均带宽限制为 100,000 Kbps，承诺突发速率限制为 4000 字节，超出突发速率限制为 6000 字节，用于标记超过提交的突发大小的任何数据包，并丢弃超过超出突发大小的任何数据包。

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set phb 3
Console(config-pmap-c)#police srtcm-color-blind 100000 4000 6000 conform-action transmit exceed-action 0
violate-action drop
Console(config-pmap-c)#
```

22.1.9 police trtcm-color

此命令基于两个三速率三色计（trTCM）定义分类流量的执行器。使用 **no** 形式删除监察器。

语法

[no] **police** {**trtcm-color-blind** | **trtcm-color-aware**} *committed-rate committed-burst peak-rate peak-burst* **conform-action transmit exceed-action** {**drop** | *new-dscp*} **violate action** {**drop** | *new-dscp*}

trtcm-color-blind -双色三色计，采用彩色盲模式。

trtcm-color-aware -双色三色仪，采用颜色识别模式。

committed-rate -承诺信息速率（CIR），以千比特为单位。 （范围：0-1000000 kbps，粒度为 64 kbps 或最大端口速度，以较低者为准）

committed-burst -承诺突发尺寸（BC），以字节为单位。（范围：64-16000000，粒度为 4k 字节）

peak-rate -峰值信息速率（PIR），单位为千位/秒（范围：0-10000000 kbps，粒度为 64 kbps 或最大速度，以较低者为准）

peak-burst -峰值突发大小（BP），以字节为单位。（范围：64-16000000，粒度为 4k 字节）

conform-action -当 rate 在 CIR 和 BP 之内时 **采取的** 行动。 （数据包大小不超过 BP，并且有足够的令牌 inbucket BC 来为数据包提供服务，数据包设置为绿色。）

exceed-action -当费率超过 CIR 但在 PIR 中时 **采取的** 行动。 （数据包大小超过 BC 但在存储桶 BP 中存在 enoughtokens 来为数据包提供服务，数据包设置为黄色。）

violate-action -当费率超过 PIR 时 **采取的** 行动。 （存储桶 BP 中没有足够的令牌来为数据包提供服务，数据包设置为红色。）

drop -超出操作或违规操作所需的丢弃数据包。

transmit -传输它而不采取任何行动。

new-dscp -差分服务代码点（DSCP）值。（范围：0-63）

缺省配置

无

命令模式

Policy Map Class 配置

命令用法

◆您最多可以为入口端口配置 16 个策略（即类映射）。

◆承诺速率和峰值速率不能超过配置接口的速度，并且承诺突发和峰值突发不能超过 16 兆字节。

◆RFC 2698 中定义的 trTCM 计量流量流并根据两种速率处理其数据包 - 承诺 信息速率(CIR)和峰值信息速率（PIR）及其关联的突发 - 承诺突发大小（BC）和峰值突发大小（BP） ）。

◆ PHB 标签由五个比特组成，每个跳行为有三个比特，用于控制队列拥塞的颜色方案有两个比特 。如果 Apacket 超过 PIR，则标记为红色。否则，它标记为黄色或绿色，具体取决于它是否超过或不超过 CIR。 trTCM 对于服务的入口监管很有用，其中峰值速率需要与承诺速率分开执行。

◆ 仪表以两种模式之一运行。 在色盲模式下，仪表假定数据包流未着色。 在颜色识别模式中，仪表假定某些前面的实体已预先对输入的数据包流进行着色，以使每个数据包为 绿色，黄色或红色。 标记(重新)根据仪表的结果对 IP 包进行着色。 颜色在数据包的 DS 字段[RFC 2474]中编码。

◆ 仪表的行为根据其模式和双声道桶 P 和 C 来指定，它们分别基于 PIR 和 CIR 速率。 令牌桶 P 的最大大小是 BP，令牌桶 C 的最大大小是 BC。

◆ 令牌桶 P 和 C 最初(在时间 0)满，即令牌计数 Tp(0)=BP 并且令牌计数 T c(0)=BC。 此后，令牌计数 Tp 每秒递增一次 PIR 时间直到 BP，并且该计数计数 Tc 每秒递增一次 CIR，直到 BC。

当大小为 B 字节的数据包在时间 t 到达时，如果将-TCMM 配置为在色盲模式下运行，则会发生以下情况：

- 如果 Tp（t）-B <0，则数据包为红色，否则为
- 如果 Tc（t）-B <0，则数据包为黄色，Tp 减去 B，否则
- 数据包为绿色，Tp 和 Tc 均减少 B.

当大小为 B 字节的数据包在时间 t 到达时，如果将-TCMM 配置为在颜色感知模式下运行， 则会发生以下情况 ：

- 如果数据包已预先显示为红色或 Tp（t）-B <0，则数据包为红色，否则
- 如果数据包已预先显示为黄色或 Tc（t）-B <0，则数据包为黄色，Tp 减少 B，否则
- 数据包 为绿色，Tp 和 Tc 均减少 B.

◆ trTCM 可用于标记服务中的 IP 数据包流，不同的是，对绿色，黄色或红色的数据包给予降低的保证级别（绝对或相对）。 有关 trTCM 其他方面的更多信息， 请参阅 RF C 2698。

范例

这个例子创建了一个名为“rd-policy”的策略，使用 class 命令来指定先前定义的“rd-class”，使用 set phb 命归类传入数据包将接收的服务，然后使用 **policy trtcm-color-blind** 命令将平均带宽限制 100,000 Kbps，承诺突发速率为 4000 字节，峰值信息速率为 1,000,000 kbps，峰值突发大小为 6000，超过承诺突发大小的任意数据包，以及丢弃任何数据包超过峰值信息率。

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set phb 3
Console(config-pmap-c)#police  trtcm-color-blind  100000  4000  100000  6000conform-action  transmit
exceed-action 0 violate-action drop
Console(config-pmap-c)#
```

22.1.10 set cos

此命令修改数据包的 VLAN 标记中匹配数据包（由 match 命令指定）的服务类（CoS）值 。 使用 no 形式删除他的设置。

语法

[no] set cos *cos-value*

cos-value -服务等级值。 （范围：0-7）

缺省配置

无

命令模式

Policy Map Class 配置

命令用法

◆set cos 命令被用于设置在 VLAN 标签的 CoS 值匹配 的数据包。

◆set cos 和 set phb 命令函数在同一水平优先权。因此设置这些命令中的任何一个都将覆盖另一个命令已经配置的任何操作。

范例

此示例创建一个名为“rd-policy”的策略，使用 class 命令指定先前定义的“rd-class”，使用 set cos 命令归类传入数据包将接收的服务，然后使用 police flow 命令限制平均带宽为 100,000 Kbps，突发速率为 4000 字节，并配置响应以丢弃任何违规数据包。

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set cos 3
```

```
Console(config-pmap-c)#police flow 10000 4000 conform-action transmitviolate-action drop
Console(config-pmap-c)#
```

22.1.11 set ip dscp

此命令修改匹配数据包中的 IP DSCP 值（由 match 命令指定）。使用 no 形式删除此业务分类。

语法

[no] **set ip dscp** *new-dscp*

new-dscp -新的差分服务代码点（DSCP）值。（范围：0-63）

缺省配置

无

命令模式

Policy Map Class 配置

命令用法

这个 **set ip dscp** 命令被用于设置在数据包的 ToS 字段优先级值用于匹配的数据包。

范例

此示例创建一个名为“rd-policy”的策略，使用 class 命令指定先前定义的“rd-class”，使用 **set ip dscp** 命令归类传入数据包将接收的服务，然后使用 police flow 命令限制平均带宽为 100,000 Kbps，突发速率为 4000 字节，并配置响应以丢弃任何违规数据包。

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set ip dscp 3
Console(config-pmap-c)#police flow 10000 4000 conform-action transmitviolate-action drop
Console(config-pmap-c)#
```

22.1.12 set phb

此命令通过为内部处理设置匹配数据包（由 match 命令指定）的每跳行为值来为 IP 流量提供服务。使用 no 形式删除此设置。

语法

[no] **set phb** *phb-value*

phb-value -每跳行为值。（范围：0-7）

缺省配置

无

命令模式

Policy Map Class 配置

命令用法

◆**set PHB** 命令被用于设置在硬件匹配分组的内部 QoS 值（见 "Default Mapping of DSCP Valuesto Internal PHB/Drop Values"）。 QoS 标签由五个比特组成，每个跳行为有三个比特，两个比特用于通过 police srtcm-color 命令和 police trtcm-color 命令控制队列拥塞的颜色方案 。

◆ set COS 和 **set PHB** 命令函数在同一水平优先权。因此设置这些命令中的任何一个都将覆盖另一个命令已经配置的任何操作。

范例

此示例创建一个名为“rd-policy”的策略，使用 class 命令指定先前定义的“rd-class”，使用 **set phb** 命令对传入数据包将接收的服务进行分类法，然后使用 police flow 命令限制平均带宽为 100,000 Kbps，突发速率为 4000 字节，并配置响应以丢弃任何违规数据包。

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set phb 3
Console(config-pmap-c)#police flow 10000 4000 conform-action transmitviolate-action drop
Console(config-pmap-c)#
```

22.1.13 service-policy

此命令将 **policy-map** 命令定义的策略映射应用于特定接口的入口或出口侧。使用 **no** 形式删除此映射。

语法

[**no**] **service-policy** {**input** | **output**} *policy-map-name*

input -应用于输入流量。

output -应用于输出流量。

policy-map-name -该接口的策略映射名称（范围：1-32 个字符 ）

缺省配置

没有策略映射附加到接口

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

◆只能为接口分配一个策略映射。

◆ 首先定义类映射，然后定义策略映射，最后使用 **service-policy** 命令将策略映射绑定到需求面。

范例

此示例将服务策略应用于入口接口。

```
Console(config)#interface ethernet 1/1

Console(config-if)#service-policy input rd-policy

Console(config-if)#
```

22.1.14 show class-map

此命令显示 QoS 类映射，这些映射定义用于对流量进行分类的匹配条件。

语法

show class-map [*class-map-name*]

class-map-name -*类映射的名称*。（范围：1-32 个字符）

缺省配置

显示所有类映射

命令模式

特权模式

范例

```
Console#show class-map

Class Map match-any rd-class#1

Description:

Match ip dscp 10
```

```
Match access-list rd-access

Match ip dscp 0

Class Map match-any rd-class#2

Match ip precedence 5

Class Map match-any rd-class#3

Match vlan 1

Console#
```

22.1.15 show policy-map

此命令显示 QoS 策略映射，该策略映射定义传入业务的分类标准，并且可以包括用于带宽限制的策略。

语法

show policy-map [*policy-map-name* [**class** *class-map-name*]]

policy-map-name -*策略映射的名称* 。（范围：1-32 个字符）

class-map-name -*类映射的名称* 。 （范围：1-32 个字符）

缺省配置

显示所有策略映射和所有类。

命令模式

特权模式

范例

```
Console#show policy-map

Policy Map rd-policy

Description:

class rd-class

set PHB 3

Console#show policy-map rd-policy class rd-class

Policy Map rd-policy

class rd-class
```

```
set PHB 3

Console#
```

22.1.16 show policy-mapinterface

此命令显示分配给指定接口的服务策略。

语法

show policy-map interface *interface* **input**

interface

unit/port

unit -单位标识符。（范围：1）

port -端口号。（范围：1-28）

port-channel *channel-id* (范围: 1-12)

命令模式

特权模式

范例

```
Console#show policy-map interface 1/5 input

Service-policy rd-policy

Console#
```

23 组播过滤命令

此交换机使用 IGMP（Internet 组管理协议）来检查想要接收特定多播服务的可用连接主机。 它标识包含请求服务的主机的端口，并仅将数据发送到这些端口。 然后，它将服务请求传播到任何相邻的多播交换机/路由器，以确保它将继续接收多播服务。

23.1 IGMP SNOOPING

本节介绍用于在交换机上配置 IGMP Snooping 的命令。

23.1.1 ip igmp snooping

该命令用来在交换机或选择的 VLAN 接口上全局使能 IGMP Snooping。使用 **no** 形式禁用它。

语法

[**no**] **ip igmp snooping** [**vlan** *vlan-id*]

vlan-id - VLAN ID (范围: 1-4093)

缺省配置

启用

命令模式

全局配置

命令用法

◆全局启用 IGMP 侦听时，IGMP 侦听的每 VLAN 接口设置优先。

◆全局禁用 IGMP 侦听时，仍然可以按照 VLAN 接口配置侦听，但在全局重新启用侦听之前，接口设置不会生效。

范例

以下示例全局启用 IGMP 侦听。

```
Console(config)#ip igmp snooping

Console(config)#
```

23.1.2 ip igmp snooping priority

此命令为所有多播流量分配优先级。 使用 no 形式恢复默认设置。

语法

ip igmp snooping priority *priority*

no ip igmp snooping priority

priority -分配给所有多播流量的 CoS 优先级。（范围：0-6，其中 6 是最高优先级）

缺省配置

2

命令模式

全局配置

命令用法

此命令可用于为低延迟多播流量（如视频会议）设置高优先级，或为对延迟不敏感的正常多播流量设置低优先级。

范例

```
Console(config)#ip igmp snooping priority 6

Console(config)#
```

23.1.3 ip igmp snooping proxy-reporting

此命令启用 IGMP Snooping 和代理报告。使用 no 形式恢复默认设置。

语法

[no] **ip igmp snooping proxy-reportingip igmp snooping vlan** *vlan-id* **proxy-reporting**

{**enable** | **disable**}

no ip igmp snooping vlan *vlan-id* **proxy-reporting**

vlan-id - VLAN ID (范围: 1-4093)

enable -在指定的 VLAN 上启用。

disable -在指定的 VLAN 上禁用。

缺省配置

全局：启用

VLAN：基于全局设置

命令模式

全局配置

命令用法

◆使用此命令启用代理报告时，交换机将执行“IGMP Snooping with Proxy Reporting”（如 DSLForum TR-101，2006 年 4 月中所定义），包括上次休假和查询抑制。当最后一个成员离开多播组时，上一个离开发出代理查询，而查询抑制意味着特定查询不会从上游多播路由器转发到此设备的下游主机。

◆ 如果在 VLAN 上配置了 IGMP 代理报告，则此设置优先于全局配置。

范例

```
Console(config)#ip igmp snooping proxy-reporting

Console(config)#
```

23.1.4 ip igmp snooping querier

该命令用来将交换机作为 IGMP 查询器。使用 no 形式禁用它。

语法

[no] **ip igmp snooping querier**

缺省配置

启用

命令模式

全局配置

命令用法

◆IGMPv3 snooping 不支持 IGMP Snooping 查询器（请参阅 ipigmp snooping 版本 ）。

◆如果启用，则交换机将在选举时充当查询器。查询者负责询问主机是否希望接收多播流量。

范例

```
Console(config)#ip igmp snooping querier
Console(config)#
```

23.1.5 ip igmp snooping router-alert-option-check

此命令会丢弃任何不包含路由器警报选项的 IGMPv2 / v3 数据包。接收 IGMP 消息时， 使用 no 形式忽略路由器警告选项。

语法

[no] ip igmp snooping router-alert-option-check

缺省配置

禁用

命令模式

全局配置

命令用法

如 IGMP 版本 3 的 RFC 3376 第 9.1 节所述，RouterAlert 选项可用于防止 DOS 攻击。 一个常见的攻击方法是由一个接管角色的入侵者发起的，并通过发送大量特定于组和源的查询开始重载多播主机，每个查询都有一个大的源列表，并且最大响应时间设置为一个大值。

为了防止这种攻击，(1)路由器不应该转发查询。如果查询携带路由器报警，则更容易实现。 (2)此外，当交换机作为多播主机的角色（例如使用代理路由时）时，它应该忽略不包含路由器警报选项的版本 2 或 3 查询。

范例

```
Console(config)#ip igmp snooping router-alert-option-check
Console(config)#
```

ip igmp snoopingrouter-port-expire-time

此命令配置查询器超时。使用 no 形式恢复默认值。

语法

ip igmp snooping router-port-expire-time *seconds*

no ip igmp snooping router-port-expire-time

seconds-交换机在上一个查询器在其认为已过期之前停止之后等待的时间。 （范围：1-65535；推荐范围：300-500）

缺省配置

300 秒

命令模式

全局配置

范例

以下显示如何将超时配置为 400 秒：

```
Console(config)#ip igmp snooping router-port-expire-time 400
Console(config)#
```

23.1.6 ip igmp snooping tcn-flood

如果发生跨越树梢拓扑变化通知（TCN），则此命令可启用多播流量的泛滥。使用 no 形式禁用泛洪。

语法

[no] ip igmp snooping tcn-flood

缺省配置

禁用

命令模式

全局配置

命令用法

◆发生生成树拓扑更改时，交换机学习到的组播成员信息可能已过期。 例如，在拓扑改变（TC）之前链接到一个端口的主机可以在改变之后移动到另一个端口。为了确保将多播数据传送到所有接收者，默认情况下，接收到具有 TC 位（由根桥）设置的桥协议数据单元（BPDU）的 VLAN 中的交换机（启用 IGMP 侦听）将进入“多播洪泛模式”在拓扑稳定并且学习所有多播接收器的新位置之前的一段时间。

◆如果接收到拓扑更改通知（TCN），并且随后删除了所有上行链路端口，则使用超时机制来删除所有当前学习的多播信道。

◆当新的上行链路端口启动时，交换机会通过新的上行链路端口向所有当前学习的信道发送未经

请求的报告。

◆默认情况下，当发生生成树拓扑更改时，交换机立即进入“multicast flooding mode”。 在此模式下，组播流量将被泛洪到所有 VLAN 端口。如果许多端口已订阅到不同的多播组，则泛洪可能会导致交换机与终端主机之间的链路过载。可能会禁用泛洪以避免这种情况，从而导致组播流量仅传递到已学习多播组成员的端口。

◆当生成树拓扑发生更改时，根网桥会发送代理查询，以快速重新学习主机成员关系/端口关系。 根网桥还发送未经请求的 Multicast Router Discover（MRD）请求，以快速定位此 VLAN 中的多播路由器。

当交换机接收到这样的数据包时,代理查询和未经请求的 MRD 请求将被泛洪到除接收端口之外的所有 VLAN 端口。

范例

The following 范例 enables TCN flooding.

```
Console(config)#ip igmp snooping tcn-flood

Console(config)#
```

23.1.7 ip igmp snoopingtcn-query-solicit

此命令指示交换机在发生生成树拓扑更改通知（TCN）时发出 IGMP 常规查询。使用 no 形式禁用此功能。

语法

[no] ip igmp snooping tcn-query-solicit

缺省配置

禁用

命令模式

全局配置

命令用法

◆当生成树中的根网桥接收到启用了 IGMP 侦听的 VLAN 的拓扑更改 通知时 ，它会发出全局 IGM P 离开消息（查询请求）。 当交换机收到此请求时，它会将其泛洪到发生在生成树更改的 VLAN 中的所有端口。当上游多播路由器收到此请求时，它也会立即发出 IGMP 通用查询。

◆该 ip igmp snooping tcn query-solicit 命令发送每当它注意到一个拓扑变化，甚至如果交

换机不在生成树的根桥查询征集中。

范例

以下示例指示交换机在收到生成树拓扑更改通知时发出 IGMP 常规查询。

```
Console(config)#ip igmp snooping tcn query-solicit

Console(config)#
```

23.1.8 ip igmp snoopingunregistered-data-flood

此命令将未注册的多播流量泛洪到连接的 VLAN 中。使用 no 形式删除未注册的多播流量。

语法

[no] ip igmp snooping unregistered-data-flood

缺省配置

禁用

命令模式

全局配置

命令用法

一旦填充了用于存储 IGMP 侦听和多播路由的多播条目的表，就不会学习新条目。如果在连接的 VLAN 中未配置路由器端口，并且禁用了 unregistered-flooding，则表中未找到的任何后续多播流量将被丢弃，否则将在整个 VLAN 中泛洪 。

范例

```
Console(config)#ip igmp snooping unregistered-data-flood

Console(config)#
```

23.1.9 ip igmp snooping unsolicited-report-interval

此命令指定启用代理报告时上游接口应传输未经授权的 IGMP 报告的频率。 使用 no 形式恢复默认值。

语法

ip igmp snooping unsolicited-report-interval *seconds*

no ip igmp snooping version-exclusive

seconds -发出未经请求的报告的时间间隔。（范围：1-65535 秒）

缺省配置

400 秒

命令模式

全局配置

命令用法

◆当新的上游接口（即上行链路端口）启动时，交换机会通过新的上游接口向所有当前学习的多播信道发送未经请求的报告。

◆此命令仅在启用代理报告时适用。

范例

```
Console(config)#ip igmp snooping unsolicited-report-interval 5

Console(config)#
```

23.1.10 ip igmp snooping version

该命令用来配置 IGMP Snooping 版本。使用 no 形式恢复默认值。

语法

ip igmp snooping [**vlan** *vlan-id*] **version** {**1** | **2** | **3**}

no ip igmp snooping version

vlan-id - VLAN ID (Range: 1-4093)

1 - IGMP Version 1

2 - IGMP Version 2

3 - IGMP Version 3

缺省配置

全局: IGMP Version 2

VLAN: 全局无配置

命令模式

全局配置

命令用法

◆该命令用于配置 IGMPsnooping 使用的 IGMP 报告/查询版本。版本 1- 3 全部受支持，版本 2

和版本 3 向后兼容，因此无论采用何种窥探版本，交换机都可以与其他设备一起运行。

◆ 如果在 VLAN 上配置了 IGMP Snooping 版本，则此设置优先于全局配置。

范例

以下配置 IGMP Snooping 的全局设置为版本 1。

```
Console(config)#ip igmp snooping version 1

Console(config)#
```

23.1.11 ip igmp snooping version-exclusive

此命令会丢弃使用与 ip igmp snooping version 命令当前配置的版本不同的任何收到的 IGMP 消息（组播协议数据包除外）。使用 no 形式禁用此功能。

语法

ip igmp snooping [**vlan** *vlan-id*] **version-exclusive**

no ip igmp snooping version-exclusive

vlan-id - VLAN ID (范围: 1-4093)

缺省配置

Global: 禁用

VLAN: 禁用

命令模式

全局配置

命令用法

◆如果在 VLAN 上禁用版本独占，则此设置基于全局设置。如果在 VLAN 上启用，则此设置优先于全局设置。

◆禁用此功能时，当前选择的版本向后兼容（请参阅 ip igmp snoop ing version 命令 ）。

范例

```
Console(config)#ip igmp snooping version-exclusive

Console(config)#
```

23.1.12 ip igmp snooping vlan general-query-suppression

除了连接下行流组播主机的端口外，此命令禁止一般查询。除组播路由器端口外，使用 no 形式将常规查询泛洪到所有端口。

语法

[no] **ip igmp snooping vlan** *vlan-id* **general-query-suppression**

vlan-id - VLAN ID (范围: 1-4093)

缺省配置

禁用

命令模式

全局配置

命令用法

◆默认情况下，一般查询消息将泛洪到所有端口，但接收它们的多播路由器除外。

◆如果启用了常规查询抑制，则这些消息仅转发到已加入多播服务的下游端口 。

范例

```
Console(config)#ip igmp snooping vlan 1 general-query-suppression
Console(config)#
```

23.1.13 ip igmp snooping vlan immediate-leave

如果在该端口接收到离开数据包并且对父 VLAN 启用了立即离开，则此命令会立即删除多播服务的成员端口。使用 no 形式恢复默认值。

语法

[no] **ip igmp snooping vlan** *vlan-id* **immediate-leave**

vlan-id - VLAN ID (范围: 1-4093)

缺省配置

禁用

命令模式

全局配置

命令用法

◆如果未使用 immediate-leave，则在收到 IGMPv2/v3 组离开信息时，组播路由器（或查询器）将发送特定于组的查询消息。仅当没有主机在超时期限内回复查询时，路由器/查询器才会停止转发该组的流量。（此版本的超时当前由 Last MemberQuery Interval 定义（固定为 1 秒）* Robustness Variable（固定为 2））如 RFC 2236 中所定义。

◆如果启用 immediate-leave，则交换机假定只有一个主机连接到该接口。因此如果仅连接到一个启用 IGMP 的设备（服务主机或运行 IGMP 监听的邻居），则应仅在接口上启用立即休假。

◆ 该命令仅在启用 IGMP Snooping 且使用 GUMPv2 或 IGMPv3 监听时有效。

范例

以下显示了如何启用立即离开。

```
Console(config)#ip igmp snooping vlan 1 immediate-leave
Console(config)#
```

23.1.14 ip igmp snooping vlan last-memb-query-count

此命令配置在系统假定不再有本地成员之前发出的特定于 IGMP 代理组或特定于组和源的查询消息的数量。使用 no 形式恢复默认值。

语法

ip igmp snooping vlan *vlan-id* **last-memb-query-count** *count*

no ip igmp snooping vlan *vlan-id* **last-memb-query-count**

vlan-id - VLAN ID (范围: 1-4093)

count -代理和特定组群和源的数量-特定的查询信息假设有曲子组成员之前发出。(范围：1-255)

缺省配置

2

命令模式

全局配置

命令用法

只有启用 IGMP 侦听代理报告或 IGMP 查询时，此命令才会生效。

范例

```
Console(config)#ip igmp snooping vlan 1 last-memb-query-count 7

Console(config)#
```

23.1.15 ip igmp snooping vlan last-memb-query-intvl

此命令配置最后一个成员查询间隔。使用 no 形式恢复默认值。

语法

ip igmp snooping vlan *vlan-id* **last-memb-query-intvl** *interval*

no ip igmp snooping vlan *vlan-id* **last-memb-query-intvl**

vlan-id - VLAN ID (范围: 1-4093)

interval -等待对特定于组的 OR 群组和源特定查询消息的响应的间隔。(第 1 秒至 11744 秒)

缺省配置

10 (1 秒)

命令模式

全局配置

命令用法

◆当组播主机离开组时，它发送一个 IGMP 离开消息。当交换机接收到该离开消息时，它通过发送一个 IGMP 组特定或组与源特定查询消息来检查该主机是否是最后一个离开组的主机，并启动 atimer。如果在定时器到期之前没有收到报告，则删除组记录，并向上游多播路由器发送报告。

◆ 减少的值将导致检测组或源的最后成员的丢失的时间减少，但是可能产生更多的突发业务。

◆ 只有在启用 IGMP 监听代理报告时，此命令才会生效。

范例

```
Console(config)#ip igmp snooping vlan 1 last-memb-query-intvl 700

Console(config)#
```

23.1.16 ip igmp snooping vlan mrd

此命令可以发送多播路由器请求消息。使用 no 形式禁用这些消息。

语法

[no] **ip igmp snooping vlan** *vlan-id* **mrd**

vlan-id - VLAN ID (范围: 1-4093)

缺省配置

启用

命令模式

全局配置

命令用法

◆组播路由器发现（MRD）使用组播路由器通告，组播路由器请求和组播路由器终止消息来发现组播路由器。 设备发送请求消息以便从 m ulticast 路由器 请求广告消息。这些消息用于在直接连接的链路上发现多播路由器。每当初始化或重新初始化多播转发接口时，也会发送请求消息。当在具有 IP 多播转发和 MRDenabled 的接口上接收到 asolicitation 时，路由器将响应广告。

◆ 路由器发送广告以通告已启用 IP 多播转发。这些消息会在所有启用了多播转发的路由器接口上定期发送。它们在周期性定时器到期时发送，作为路由器启动过程的一部分，在重新启动多播转发接口期间，以及在接收到请求消息时发送。当提供给 VLAN 的多播服务相对稳定时， 不需要使用请求消息，可以使用 **no ip igmpsnooping vlan mrd** 命令禁用 。

◆ 当上游路由器不支持 MRD 时，此命令也可用于禁用组播路由器请求消息，以减少繁忙的上游路由器上的负载，或者在 VLAN 中禁用 IGMP 侦听时。

范例

此示例禁用在 VLAN 1 上发送多播路由器请求消息。

```
Console(config)#no ip igmp snooping vlan 1 mrd
Console(config)#
```

23.1.17 ip igmp snooping vlan proxy-address

此命令为本地生成的查询配置静态源地址，并报告 IGMP 代理报告使用的报告消息。使用 no 形式恢复默认源地址。

语法

[no] **ip igmp snooping vlan** *vlan-id* **proxy-address** *source-address*

vlan-id - VLAN ID (范围: 1-4093)

source-address -用于代理 IGMP 查询和报告的源地址，并保留消息。(任何有效的 IP 单播地址)

缺省配置

0.0.0.0

命令模式

全局配置

命令用法

IGMP 侦听使用空 IP 地址 0.0.0.0 作为 IGMP 查询消息的来源，这些消息代理到下游主机以指示它不是选定的查询器，而是仅代理 RFC 4541 中定义的这些消息。交换机也使用空地址在 IGMP 报告中发送了 toupstream 端口。

许多主机不实现 RFC 4541，因此不理解源地址为 0.0.0.0 的查询消息。因此这些主机不会回复查询，导致多播路由器停止向它们发送流量。

要解决此问题，可以使用此命令将代理的 IGMP 查询和报告消息中的源地址替换为任何有效的单播地址（除路由器自己的地址之外）。

用于代理报告的规则

禁用 IGMP 代理报告时，除非 已设置代理查询地址，否则交换机将使用空 IP 地址作为 IGMP 查询和报告消息的来源 。

启用 IGMP 代理报告时，源地址基于以下标准：

◆ 如果配置了代理查询地址，交换机将使用该地址作为一般的源 IP 地址和发送给下游主机的特定于组的查询消息，以及从多播路由器端口发送的报告和离开消息。

◆ 如果未配置代理查询地址，交换机将使用 theVLAN 的 IP 地址作为在一般和组的 IP 源地址-向下游发送特定的查询信息，并使用从下游主机在报告中接收的最后一个 IGMP 消息的源地址，并将消息往上游组播路由器端口发送。

范例

以下示例将代理的 IGMP 查询信息的源地址设置为 10.0.1.8。

```
Console(config)#ip igmp snooping vlan 1 proxy-address 10.0.1.8

Console(config)#
```

23.1.18 ip igmp snooping vlan query-interval

此命令配置发送 IGMP 通用查询之间的时间间隔。使用 no 形式恢复默认值。

语法

ip igmp snooping vlan *vlan-id* **query-interval** *interval*

no ip igmp snooping vlan *vlan-id* **query-interval**

vlan-id - VLAN ID (范围: 1-4093)

interval -发送 IGMP 常规查询之间的间隔。（范围：10-31740 秒）

缺省配置

100 (10 秒)

命令模式

全局配置

命令用法

◆交换机以此命令指定的间隔发送 IGMP 通用查询消息。当下游主机收到此消息时，所有接收者都会为他们已加入的多播组构建 IGMP 报告。

◆ 当交换机用作查询器时,此命令适用当启用 IGMP 侦听代理报告时,此命令适用于代理主机。

范例

```
Console(config)#ip igmp snooping vlan 1 query-interval 150

Console(config)#
```

23.1.19 ip igmp snooping vlan query-resp-intvl

此命令配置系统等待一般查询的最长时间。使用 no 形式恢复默认值。

语法

ip igmp snooping vlan *vlan-id* **query-resp-intvl** *interval*

no ip igmp snooping vlan *vlan-id* **query-resp-intvl**

vlan-id - VLAN ID (范围: 1-4093)

interval -系统等待对一般查询的响应的最长时间。（范围：10-31744）

缺省配置

100 (10 秒)

命令模式

全局配置

命令用法

当交换机作为查询器时，或者当启用 IGMP 侦听代理报告时，此命令适用于代理主机。

范例

```
Console(config)#ip igmp snooping vlan 1 query-resp-intvl 20

Console(config)#
```

23.1.20 ip igmp snooping vlan static

此命令将端口添加到多播组。使用 no 形式删除端口。

语法

[no] **ip igmp snooping vlan** *vlan-id* **static** *ip-address interface*

vlan-id - VLAN ID (范围: 1-4093)

ip-address -组播组的 IP 地址

interface

ethernet *单元 / 端口*

unit - 单位标识符。 （范围：1）

port - 端口号。 （范围：1-28）

port-channel *channel-id* (范围: 1-12)

缺省配置

无

命令模式

全局配置

命令用法

◆静态组播条目永远不会老化。

◆ 将组播条目分配给特定 VLAN 中的接口时，相应的流量只能转发到该 VLAN 内的端口。

范例

以下显示如何在端口上静态配置多任务组。

```
Console(config)#ip igmp snooping vlan 1 static 224.0.0.12 ethernet 1/5

Console(config)#
```

23.1.21 show ip igmp snooping

此命令显示 IGMP 侦听，代理和查询配置设置。

语法

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

vlan-id - VLAN ID (1-4093)

命令模式

特权模式

命令用法

此命令显示全局和 VLAN 特定的 IGMP 配置设置。 有关显示项目的说明，请参阅 “配置 IGMP Snooping 和查询参数” 。

范例

以下显示了当前的 IGMP Snooping 配置：

```
Console#show ip igmp snooping

IGMP Snooping : Enabled

Router Port Expire Time : 300 s

Router Alert Check : Disabled

TCN Flood : Disabled

TCN Query Solicit : Disabled

Unregistered Data Flood : Disabled

802.1p Forwarding Priority : Disabled

Unsolicited Report Interval : 400 s

Version Exclusive : Disabled

Version : 2

Proxy Reporting : Disabled

Querier : Disabled

VLAN 1:

--------

IGMP Snooping : Enabled

IGMP Snooping Running Status : Inactive

Version : Using global Version (2)

Version Exclusive : Using global status (Disabled)

Immediate Leave : Disabled

Last Member Query Interval : 10 (unit: 1/10s)
```

```
Last Member Query Count : 2

General Query Suppression : Disabled

Query Interval : 125

Query Response Interval : 100 (unit: 1/10s)

Proxy Query Address : 0.0.0.0

Proxy Reporting : Using global status (Disabled)

Multicast Router Discovery : Disabled

VLAN Static Group Port

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

1 224.1.1.1 Eth 1/ 1

...
```

23.1.22 show ip igmp snooping group

此命令显示指定 VLAN 接口的已知组播组，源和主机端口映射，如果未指定，则显示所有接口。

语法

show ip igmp snooping group [**host-ip-addr** *ip-address interface* |**igmpsnp** | **sort-by-port** | **user** | **vlan** *vlan-id* [**user** | **igmpsnp**]]

ip-address -组播组的 IP 地址

interface

ethernet *单元 / 端口*

unit - 单位标识符。 （范围：1）

port - 端口号。 （范围：1-28）

port-channel *channel-id* (范围: 1-12)

igmpsnp -仅显示通过 IGMP 监听获知的条目。

sort-by-port -显示按端口排序的条目。

user -仅显示用户配置的组播表项。

vlan-id - VLAN ID (1-4093)

缺省配置

无

命令模式

特权模式

命令用法

显示的成员类型包括 IGMP 或用户，具体取决于所选选项。

范例

以下是通过 IGMP Snooping 为 VLAN 1 学习到的组播表项。

```
Console#show ip igmp snooping group vlan 1

Bridge Multicast Forwarding Entry Count:1

Flag: R - Router port, M - Group member port

H - Host counts (number of hosts join the group on this port).

P - Port counts (number of ports join the group).

Up time: Group elapsed time (d:h:m:s).

Expire : Group remaining time (m:s).

VLAN Group Port Up time Expire Count

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

1 224.1.1.1 00:00:00:37 2(P)

Eth 1/ 1(R)

Eth 1/ 2(M) 0(H)

Console#
```

23.1.23 show ip igmp snooping statistics

此命令显示指定接口的 IGMP 侦听协议统计信息。

语法

show ip igmp snooping statistics{**input** [**interface** *interface*] |**output** [**interface** *interface*] |**query** [**vlan** *vlan-id*]}

interface

ethernet *单元 / 端口*

unit - 单位标识符。 （范围：1）

port - 端口号。 （范围：1-28）

port-channel *channel-id* (范围: 1-12)

vlan *vlan-id* - VLAN ID (范围: 1-4093)

query -显示与 IGMP Snooping 相关的统计信息。

缺省配置

无

命令模式

特权模式

范例

以下显示了 IGMP 协议统计信息输入：

```
Console#show ip igmp snooping statistics input interface ethernet 1/1

Interface Report Leave G Query G(-S)-S Query Drop Join Succ Group

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

Eth 1/ 1 23 11 4 10 5 14 5

Console#
```

23.2 静态组播路由

本节介绍用于在交换机上配置静态组播路由的命令。

23.2.1 ip igmp snooping vlan mrouter

该命令静态配置指定 VLAN 上的（二层）组播路由器端口。使用 **no** 形式删除配置。

语法

[**no**] **ip igmp snooping vlan** *vlan-id* **mrouter** *interface*

vlan-id - VLAN ID (范围: 1-4093)

interface

ethernet *unit/port*

unit -单位标识符。(范围：1)

port -端口号。(范围：1-28)

port-channel *channel-id* (范围: 1-12)

缺省配置

未配置静态组播路由器端口。

命令模式

全局配置

命令用法

◆根据您的网络连接，IGMP 侦听可能无法找到 IGMP 查询器。因此如果 IGMP 查询器是通过网络连接到该交换机上的接口（端口或中继）的已知多播路由器或交换机，则可以手动配置该接口以加入所有当前多播组。

◆必须在交换机上全局启用 IGMP Snooping（使用 ip igmp snooping 命令）才能使组播路由器端口生效。

范例

以下显示如何将端口 10 配置为 VLAN 1 中的多播路由器端口。

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet 1/10
Console(config)#
```

23.2.2 show ip igmp snooping mrouter

此命令显示有关静态配置和动态学习的多播路由器端口的信息。

语法

show ip igmp snooping mrouter [**vlan** *vlan-id*]

vlan-id - VLAN ID (范围: 1-4093)

缺省配置

显示所有已配置 VLAN 的组播路由器端口。

命令模式

特权模式

命令用法

显示的多播路由器端口类型包括静态或动态。

范例

以下显示 VLAN 1 中连接到多路径的端口。

```
Console#show ip igmp snooping mrouter vlan 1

VLAN M'cast Router Port Type

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

1 Eth 1/10 Static

Console#
```

23.3 IGMP 过滤和限制

在某些交换机应用程序中，管理员可能希望控制最终用户可用的多个服务。例如基于特定订阅计划的 IP / TV 服务。IGMP 过滤功能通过限制对交换机端口的指定多播服务的访问来满足此要求，IGMP 限制限制端口可以加入的同时多播组的数量。

23.3.1 ip igmp filter (Global Configuration)

此命令全局启用交换机上的 IGMP 过滤和限制。使用 no 形式禁用该功能。

语法

[no] ip igmp filter

缺省配置

禁用

命令模式

全局配置

命令用法

◆IGMP 过滤使您可以将配置文件分配给交换机端口，以指定端口上允许或拒绝的多播组。 IGMP 过滤器配置文件可以包含一个或多个或一系列多播地址； 但只能为端口分配一个配置文件。启用后，IGMP 加入端口收到的报告是针对 thefilter 轮廓检查。如果允许请求的多播组，则正常转发 IGMP 加入报告。如果请求的多播组被拒绝，IGMP 联接报告已删除。

◆ IGMP 过滤和限制仅适用于动态学习的多组，它不适用于静态配置的组。

◆ 当 MVR 用于转发多播流量时，IGMP 过滤功能的运行方式相同。

范例

```
Console(config)#ip igmp filter

Console(config)#
```

23.3.2 ip igmp profile

此命令创建 IGMP 过滤器配置文件编号并进入 IGMP 配置模式。 使用 no 形式删除配置文件编号。

语法

[no] **ip igmp profile** *profile-number*

profile-number - IGMP 过滤器配置文件号。(范围: 1-4294967295)

缺省配置

禁用

命令模式

全局配置

命令用法

配置文件定义允许订户加入的多播组。相同的配置文件可以应用于许多接口，但只能将一个配置文件分配给一个接口。每个配置文件只有一个访问模式：允许或否认。

范例

```
Console(config)#ip igmp profile 19

Console(config-igmp-profile)#
```

23.3.3 permit, deny

此命令设置 IGMP 过滤器配置文件的访问模式。使用 no 形式删除配置文件编号。

语法

{**permit** | **deny**}

缺省配置

拒绝

命令模式

IGMP 配置文件配置

命令用法

◆每个配置文件只有一种访问模式：允许或否认。

◆当访问模式设置为允许时，当组播组在控制范围内时，处理 IGMP 加入报告。当访问模式设置为拒绝时，仅当组播组不在受控范围内时，才会报告 IGMP 加入报告 。

范例

```
Console(config)#ip igmp profile 19
Console(config-igmp-profile)#permit
Console(config-igmp-profile)#
```

23.3.4 range

此命令指定配置文件的多播组地址。使用 no 形式从配置文件中删除地址。

语法

[no] **range** *low-ip-address* [*high-ip-address*]

low-ip-address -多播组的有效 IP 地址或组范围的开始。

high-ip-address -多播组范围结束时的有效 IP 地址。

缺省配置

无

命令模式

IGMP 配置文件配置

命令用法

多次输入此命令以指定配置文件的多个多播地址或地址范围。

范例

```
Console(config)#ip igmp profile 19
Console(config-igmp-profile)#range 239.1.1.1
Console(config-igmp-profile)#range 239.2.3.1 239.2.3.100
Console(config-igmp-profile)#
```

23.3.5 ip igmp filter(Interface Configuration)

此命令将 IGMP 过滤配置文件分配给交换机上的接口。使用 no 形式从界面中删除配置文件 。

语法

[no] **ip igmp filter** *profile-number*

profile-number - IGMP 过滤器配置文件号。（范围：1-4294967295）

缺省配置

无

命令模式

接口配置

命令用法

◆必须首先使用 ip igmp profile 命令创建 IGMP 过滤配置文件，然后才能将其分配给接口。

◆只能为界面分配一个配置文件。

◆还可以将配置文件分配给中继接口。当端口配置为中继成员时，中继使用过滤配置文件分配给中继中的第一个端口成员。

范例

```
Console(config)#interface ethernet 1/1

Console(config-if)#ip igmp filter 19

Console(config-if)#
```

23.3.6 ip igmp max-groups

此命令设置交换机上接口的 IGMP 限制编号。使用 no 形式恢复默认设置。

语法

ip igmp max-groups *number*

no ip igmp max-groups

number -接口可以同时加入的最大组播组数。（范围：1-255）

缺省配置

255

命令模式

接口配置 (Ethernet)

命令用法

◆IGMP 限制设置端口可以同时加入的最大组播组数。当端口上达到最大组数时，交换机可以执行以下两个操作之一：“拒绝”或“代替”。如果操作设置为拒绝，则将删除任何新的 IGMP 加入报告。如果操作设置为代替，则交换机会随机删除现有组并将其替换为新组播组。

◆ 也可以在 Trunk 接口上设置 IGMP 限制。当端口配置了中继成员时，中继使用中继中第一个端口成员的限制设置。

范例

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp max-groups 10
Console(config-if)#
```

23.3.7 ip igmp max-groupsaction

此命令为交换机上的接口设置 IGMP 限制操作。

语法

ip igmp max-groups action {**deny** | **replace**}

deny -删除新的多播组加入报告。

replace -新的多播组替换现有组。

缺省配置

拒绝

命令模式

接口配置 (Ethernet)

命令用法

当端口上达到最大组数时，交换机会捕获两个操作中的一个:“拒绝”或“代替”。如果操作设置为拒绝，则将删除任何新的 IGMP 连接报告。如果操作设置为“替换”，则交换机将随机删除现有组并将其替换为新的多播组。

范例

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp max-groups action replace
Console(config-if)#
```

23.3.8 ip igmp query-drop

此命令将丢弃所有收到的 IGMP 查询数据包。使用 no 形式恢复默认设置。

语法

[no] ip igmp query-drop

缺省配置

禁用

命令模式

接口配置 (Ethernet)

命令用法

此命令可用于删除在指定接口上接收的任何查询数据包。如果此交换机充当查询器，则可以防止它受到从另一个查询器收到的消息的影响。

范例

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp query-drop
Console(config-if)#
```

23.3.9 show ip igmp filter

此命令显示 IGMP 筛选的全局和接口设置。

语法

show ip igmp filter [**interface** *interface*]

interface

ethernet *unit/port*

unit -单位标识符。（范围：1）

port -端口号。（范围：1-28）

port-channel *channel-id* (范围: 1-12)

缺省配置

无

命令模式

特权模式

范例

```
Console#show ip igmp filter
IGMP filter Enabled
```

```
Console#show ip igmp filter interface ethernet 1/1

Ethernet 1/1 information

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

IGMP Profile 19

Deny

Range 239.1.1.1 239.1.1.1

Range 239.2.3.1 239.2.3.100

Console#
```

23.3.10 show ip igmp profile

此命令显示在交换机上创建的 IGMP 过滤配置文件。

语法

show ip igmp profile [*profile-number*]

profile-number -现有的 IGMP 过滤器配置文件号。（范围：1-4294967295）

缺省配置

无

命令模式

特权模式

范例

```
Console#show ip igmp profile

IGMP Profile 19

IGMP Profile 50

Console#show ip igmp profile 19

IGMP Profile 19

Deny

Range 239.1.1.1 239.1.1.1

Range 239.2.3.1 239.2.3.100

Console#
```

23.3.11 show ip igmp query-drop

此命令显示指定的接口是否配置为丢弃 IGMP 查询数据包。

语法

show ip igmp throttle interface [*interface*]

interface

ethernet *unit/port*

unit -堆叠单位。(范围：1)

port -端口号。(范围：1-28)

port-channel *channel-id* (范围：1-12)

缺省配置

无

命令模式

特权模式

命令用法

使用此命令而不指定接口将显示所有接口。

范例

```
Console#show ip igmp query-drop interface ethernet 1/1

Ethernet 1/1: Enabled

Console#
```

23.3.12 show ip igmp throttle interface

此命令显示 IGMP 限制的接口设置。

语法

show ip igmp throttle interface [*interface*]

interface

ethernet *unit/port*

unit -单位标识符。(范围：1)

port -端口号。(范围：1-28)

port-channel *channel-id* (范围：1-12)

缺省配置

无

命令模式

特权模式

命令用法

使用此命令而不指定接口会显示所有接口的信息。

范例

```
Console#show ip igmp throttle interface ethernet 1/1

Eth 1/1 Information

Status : TRUE

Action : Deny

Max Multicast Groups : 32

Current Multicast Groups : 0

Console#
```

23.4 MVR FOR IPV4

本节介绍用于配置 IPv4（MVR）的多播 VLAN 注册的命令。可以使用单个网络范围的 VLAN 在服务提供商的网络中传输多播流量（例如电视频道）。进入 MVR VLAN 的任何多播流量都将发送给所有订户。这可以显着降低为动态监视和建立正常组播 VLAN 的分发树所需的处理开销。另请注意，MVR 通过仅将多播流量传递到订户所属的其他 VLAN 来维护 VLAN 隔离提供的用户隔离和数据安全性。

23.4.1 mvr

此命令在交换机上全局启用多播 VLAN 注册（MVR）。使用此命令的 no 形式全局禁用 MVR。

语法

[no] mvr

缺省配置

禁用

命令模式

全局配置

命令用法

只有 IGMP 版本 2 或 3 主机才能发出组播加入或离开消息。如果必须为 IGMP 版本 1 主机配置 MVR，则必须使用 mvr vlan group 命令静态分配组播组。

范例

以下示例全局启用 MVR。

```
Console(config)#mvr
Console(config)#
```

23.4.2 mvr associated-profile

此命令将配置文件中指定的 MVR 组地址绑定到 MVR 域。使用此命令的 no 形式删除绑定。

语法

[no] **mvr domain** *domain-id* **associated-profile** *profile-name*

domain-id -独立的组播域。（范围：1-5）

profile-name -包含一个或多个 MVR 组地址的配置文件的名称。（范围：1-21 个字符）

缺省配置

禁用

命令模式

全局配置

范例

以下是域 1 的 MVR 组地址配置文件：

```
Console(config)#mvr domain 1 associated-profile rd
Console(config)#
```

23.4.3 mvr domain

此命令为特定域启用多播 VLAN 注册（MVR）。使用此命令的 no 形式禁用域的 MVR。

语法

[no] **mvr domain** *domain-id*

domain-id -独立的组播域。（范围：1-5）

缺省配置

禁用

命令模式

全局配置

命令用法

只有 IGMP 版本 2 或 3 主机才能发出组播加入或离开消息。如果必须为 IGMP 版本 1 主机配置 MVR，则必须使用 mvr vlan group 命令静态分配组播组。

范例

以下示例为域 1 启用 MVR：

```
Console(config)#mvr domain 1
Console(config)#
```

23.4.4 mvr profile

此命令将一系列 MVR 组地址映射到配置文件。使用此命令的 no 形式删除配置文件。

语法

mvr profile *profile-name start-ip-address end-ip-address*

profile-name -包含一个或多个 MVR 组地址的配置文件的名称。（范围：1-21 个字符）

start-ip-address -启动 MVR 组播组的 IPv4 地址。 （范围：224.0.1.0 - 239.255.255.255）

end-ip-address -结束 MVR 组播组的 IPv4 地址。（范围：224.0.1.0 - 239.255.255.255）

缺省配置

没有定义配置文件

命令模式

全局配置

命令用法

◆使用此命令静态配置将加入 MVR VLAN 的所有组播组地址。 与 MVR 组相关联的任何多播数据从所有源端口发送到已注册以从该多播组接收数据的所有接收器端口 。

◆IP 地址范围从 224.0.0.0 到 239.255.255.255 用于单播流。MVR 组地址不能超出 224.0.0.x 的 reservedIP 组播地址范围。

◆IGMP 侦听和 MVR 共享最多 1024 个组。任何超过此限制的多个流都将被流向相关域中的所有端口。

范例

以下示例将一系列 MVR 组地址映射到配置文件：

```
Console(config)#mvr profile rd 228.1.23.1 228.1.23.10
Console(config)#
```

23.4.5 mvr proxy-query-interval

以下示例将一系列 MVR 组地址映射到配置文件：

语法

mvr proxy-query-interval *interval*

no mvr proxy-query-interval

interval -接收端口发送通用查询的时间间隔。（范围：2-31744 秒）

缺省配置

125 秒

命令模式

全局配置

命令用法

此命令设置主动查询端口发送一般查询的一般查询间隔。当 MVR 代理切换命令启用代理切换时，此间隔仅有效。

范例

此示例设置 MVR 代理切换的代理查询间隔。

```
Console(config)#mvr proxy-query-interval 250
Console(config)#
```

23.4.6 mvr priority

此命令为 MVR VLAN 中的所有多播流量分配优先级。使用 no 命令恢复默认设置。

语法

mvr priority *priority*

no mvr priority

priority -分配给转发到 MVR VLAN 的所有多播流量的 CoS 优先级。（范围：0-6，其中 6 是最高优先级）

缺省配置

禁用

命令模式

全局配置

命令用法

此命令可用于为低延迟多播流量（如视频会议）设置高优先级，或为对延迟不敏感的正常多播流量设置低优先级。

范例

```
Console(config)#mvr priority 6
Console(config)#
```

23.4.7 mvr proxy-switching

此命令启用 MVR 代理切换，其中源端口充当主机，接收器端口充当具有查询器服务启用的 MVR 路由器。使用 no 形式禁用此功能。

语法

[no] **mvr proxy-switching**

缺省配置

启用

命令模式

全局配置

命令用法

◆启用 MVR 代理切换时，MVR 源端口用作上游或主机接口。源端口通过发送汇总的成员资格报告仅执行 MVR 的主机部分，并且自动禁用 MVR 路由器功能。

◆ 接收者端口称为下游或路由器接口。这些接口通过在下游接口上维护所有 MVR 订阅的数据库来执行标准 MVR 路由器功能。必须在需 MVR 代理服务的所有下游接口上配置接收端口 。

◆当源端口收到报告并保留消息时，它只会将它们转发到其他源端口。

◆当接收方端口收到任何查询消息时，它们将被丢弃。

◆当接收器端口通过报告和离开消息学习下游 MVR 组中发生的更改时，将创建 MVR 状态更改报告并将其发送到上游源端口，该端口将此信息转发到上游。

◆禁用 MVR 代理切换时：

- 从接收器/源端口接收的任何成员身份报告都将转发到所有源端口。
- 当源端口收到查询消息时，它将被转发到所有下游接收器端口。
- 当接收方端口收到查询消息时，它将被删除。

范例

以下示例启用 MVR 代理切换。

```
Console(config)#mvr proxy-switching
Console(config)#
```

23.4.8 mvr robustness-value

此命令配置预期的数据包丢失，从而配置生成报告和特定于组的查询的次数。使用 no 形式恢复默认设置。

语法

mvr robustness-value *value*

no mvr robustness-value

value -用于所有接口的健壮性。（范围：1-255）

缺省配置

2

命令模式

全局配置

命令用法

◆此命令用于设置在获知有关下游组的更改时上行报告消息的次数，以及将特定于组的查询发送到下游接收器端口的次数。

◆此命令仅在启用 MVR 代理切换时才会生效 。

范例

```
Console(config)#mvr robustness-value 5

Console(config)#
```

23.4.9 mvr source-port-mode dynamic

此命令将交换机配置为仅转发源端口已动态连接的多播流。使用 no 形式恢复默认设置。

语法

[no] mvr source-port-mode dynamic

缺省配置

转发已在配置文件中指定并绑定到域的所有多播流。

命令模式

全局配置

命令用法

◆默认情况下，交换机会在配置文件设置的地址范围内转发所有组播流，并绑定到域。多播流被发送到交换机上的所有源端口以及已选择接收该多播地址上的数据的所有接收器端口。

◆使用 mvr source-port-mode dynamic 命令时，交换机只转发源端口动态加入的组播流。 换句话说，在将组播流转发到任何连接的客户端之前，接收器端口和源端口都必须订阅组播组。请注意，请求的流仍然限制在已绑定到域的配置文件中指定的地址范围。

范例

```
Console(config)#mvr source-port-mode dynamic

Console(config)#
```

23.4.10 mvr upstream-source-ip

此命令配置分配给在所有域或指定域上游发送的所有 MVR 控制包的源 IP 地址。使用 no 形式恢复默认设置。

语法

mvr [domain *domain-id*] upstream-source-ip *source-ip-address*

no mvr [domain *domain-id*] upstream-source-ip

domain-id -独立的组播域。（范围：1-5）

source-ip-address - 分配给上游发送的所有 MVR 控制数据包的源 IPv4 地址。

缺省配置

上游发送的所有 MVR 报告都使用空源 IP 地址。

命令模式

全局配置

范例

```
Console(config)#mvr domain 1 upstream-source-ip 192.168.0.3

Console(config)#
```

23.4.11 mvr vlan

此命令指定接收 MVR 多播数据的 VLAN。使用此命令的 no 形式恢复默认 MVR VLAN。

语法

mvr domain *domain-id* **vlan** *vlan-id*

no mvr domain *domain-id* **vlan**

domain-id -独立的组播域。（范围：1-5）

vlan-id-指定接收 MVR 组播数据的 VLAN。这也是必须分配所有源端口的 VLAN。（范围：1-4093）

缺省配置

VLAN 1

命令模式

全局配置

命令用法

◆此命令指定接收 MVR 多播数据的 VLAN。这是必须为所有源端口分配的 VLAN。

◆ 此命令指定的 VLAN 必须是使用 vlan 命令配置的现有 VLAN。

◆ MVR 源端口可以使用 switchport allowed vlan 命令和 switchport native vlan 命令配置为 MVR VLAN 的成员，但 MVR 接收器端口不应静态配置为此 VLAN 的成员。

范例

以下示例将 MVR VLAN 设置为 VLAN 2：

```
Console(config)#mvr

Console(config)#mvr domain 1 vlan 2

Console(config)#
```

23.4.12 mvr immediate-leave

此命令使交换机在收到该组的离开消息后立即从多播流中删除接口。使用 no 形式恢复默认设置。

语法

[no] mvr [domain *domain-id*] immediate-leave

domain-id -独立的组播域。（范围：1-5）

缺省配置

禁用

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

◆立即执行仅适用于接收器端口。启用后，将立即从离开消息中标识的多播组中删除该接收器端口。当禁用立即离开时，开关遵循标准规则，通过向接收器端口发送特定于组的查询并等待响应以确定在删除之前是否存在该组播组的任何剩余订户组列表中的端口。

◆使用立即离开可以加快离开延迟，但只能在仅连接到一个多播用户的端口上进行，以避免中断连接到同一接口的其他组成员的服务。

◆立即离开不适用于已使用 mvr vlan group 命令暂时分配给端口的组播组。

范例

以下内容允许在接收器端口上立即离开。

```
Console(config)#interface ethernet 1/5
Console(config-if)#mvr domain 1 immediate-leave
Console(config-if)#
```

23.4.13 mvr type

此命令将接口配置为 MVR 接收器或源端口。使用 no 形式恢复默认设置。

语法

[no] mvr [domain *domain-id*] type {receiver | source}

domain-id -独立的组播域。（范围：1-5）

receiver -将接口配置为可以接收组播数据的用户端口。

source -将接口配置为上行端口，可以为配置的组播组发送和接收组播数据。

缺省配置

端口类型未定义。

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

◆未配置为 MVR 接收器或源端口的端口可以使用 IGMP 侦听来使用标准规则加入或离开组播组以进行组播过滤。

◆接收者端口可以属于不同的 VLAN，但通常不应配置为 MVR VLAN 的成员。IGMP 侦听还可用于允许接收器端口动态加入或离开未通过 MVR VLAN 获取的多播组。另请注意 MVR 接收器端口的 VLAN 成员不能设置为访问模式（请参见 switchport mode 命令）。

◆可以将一个或多个接口配置为 MVR 源端口。 一个源端口既可以接收和发送通过 MVR 协议加入的组播组的数据，也可以通过 mvr vlan group 命令分配。

◆只有 IGMP 版本 2 或 3 主机才能发出多播加入或离开消息。如果必须为 IGMP 版本 1 主机配置 MVR，则必须使用 mvr vlan group 命令静态分配多个组。

范例

以下配置一个源端口和几个接收端口开关。

```
Console(config)#interface ethernet 1/5

Console(config-if)#mvr domain 1 type source

Console(config-if)#exit

Console(config)#interface ethernet 1/6

Console(config-if)#mvr domain 1 type receiver

Console(config-if)#exit

Console(config)#interface ethernet 1/7

Console(config-if)#mvr domain 1 type receiver

Console(config-if)#
```

23.4.14 mvr vlan group

此命令将组播组静态绑定到端口，该端口将接收与稳定主机集关联的长期组播流。使用 no 形式恢复默认设置。

语法

[no] **mvr** [**domain** *domain-id*] **vlan** *vlan-id* **group** *ip-address*

domain-id -独立的组播域。（范围：1-5）

vlan-id -指定组播流量被刷新的接收者 VLAN。（范围：1-4093）

group -定义发送到所选端口的多播服务。

ip-address -静态配置接口，以便从为 MVR 组播组指定的 IPv4 地址接收组播通信。（范围：224.0.1.0 - 239.255.255.255）

缺省配置

没有接收器端口是任何已配置的多播组的成员。

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

◆可以使用此命令将多播组静态分配给接收方端口。

◆IP 地址范围从 224.0.0.0 到 239.255.255.255 用于单播流。 MVR 组地址不能超出 224.0 的 reservedIP 组播地址范围。

◆只有 IGMP 版本 2 或 3 主机可以发出多播加入或离开消息。如果必须为 IGMP 版本 1 主机配置 MVR，则必须使用 **mvr vlan group** 命令静态分配多个组。

◆MVR VLAN 不能指定为静态绑定的接收者 VLAN。

范例

以下静态分配组播组到接收端口：

```
Console(config)#interface ethernet 1/7
Console(config-if)#mvr domain 1 type receiver
Console(config-if)#mvr domain 1 vlan 3 group 225.0.0.5
Console(config-if)#
```

23.4.15 show mvr

此命令显示有关 MVR 域设置的信息，包括 MVR 操作状态，组播 VLAN，当前组地址数和上游源 IP 地址。

语法

show mvr [**domain** *domain-id*]

domain-id -独立的组播域。（范围：1-5）

缺省配置

显示所有 MVR 域的配置设置。

命令模式

特权模式

范例

以下显示了 MVR 设置：

```
Console#show mvr

MVR 802.1p Forwarding Priority : Disabled

MVR 802.1p Forwarding Priority : Disabled

MVR Proxy Switching : Enabled

MVR Robustness Value : 1

MVR Proxy Query Interval : 125(sec.)

MVR Source Port Mode : Always Forward

MVR Domain : 1

MVR Config Status : Enabled

MVR Running Status : Active

MVR Multicast VLAN : 1

MVR Current Learned Groups : 10

MVR Upstream Source IP : 192.168.0.3

...
```

23.4.16 show mvr associated-profile

此命令显示绑定指定域的概要文件。

语法

show mvr [**domain** *domain-id*] **associated-profile**

domain-id -独立的组播域。（范围：1-5）

缺省配置

显示绑定到所有 MVR 域的配置文件。

命令模式

特权模式

范例

以下显示绑定到域 1 的配置文件：

```
Console#show mvr domain 1 associated-profile

Domain ID : 1

MVR Profile Name Start IP Addr. End IP Addr.

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

rd 228.1.23.1 228.1.23.10

testing 228.2.23.1 228.2.23.10

Console#
```

23.4.17 show mvr interface

此命令显示连接到 MVR VLAN 的接口的 MVR 配置设置。

语法

show mvr [**domain** *domain-id*] **interface**

domain-id -独立的组播域。（范围：1-5）

缺省配置

显示所有连接接口的配置设置。

命令模式

特权模式

范例

以下显示有关连接到域 1 中的 MVR VLAN 的接口的信息：

```
Console#show mvr domain 1 interface

MVR Domain : 1

Port Type Status Immediate Static Group Address

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

Eth 1/ 1 Source Active/Forwarding

Eth 1/ 2 Receiver Inactive/Discarding Disabled 234.5.6.8(VLAN2)

Eth1/ 3 Source Inactive/Discarding

Eth1/ 1 Receiver Active/Forwarding Disabled 225.0.0.1(VLAN1)
```

225.0.0.9(VLAN3)

Eth1/ 4 Receiver Active/Discarding Disabled

Console#

23.4.18 show mvr members

此命令显示有关转发数据库中当前条目数的信息，有关特定多播地址的详细信息，订阅所有活动多播组的主机的 IP 地址或与每个端口关联的多播组。

语法

show mvr [**domain** *domain-id*] **members** [*ip-address* /**host-ip-address** [*interface*] / **sort-by-port** [*interface*]]]

domain-id -独立的组播域。（范围：1-5）

ip-address - MVR 组播组的 IPv4 地址。（范围：224.0.1.0 - 239.255.255.255）

members -分配给 MVR VLAN 的多播组。

host-ip-address -用户 IP 地址。

sort-by-port -与接口关联的组播组。

interface

ethernet *unit/port*

unit -单位标识符。（范围：1）

port -端口号。（范围：1-28）

port-channel *channel-id* (范围: 1-12)

缺省配置

显示所有域和所有转发条目的配置设置。

命令模式

特权模式

范例

以下显示有关域 1 中当前活动的多播转发数量的信息：

Console#show mvr domain 1 members

MVR Domain : 1

```
MVR Forwarding Entry Count :1

Flag: S - Source port, R - Receiver port.

H - Host counts (number of hosts joined to group on this port).

P - Port counts (number of ports joined to group).

Up time: Group elapsed time (d:h:m:s).

Expire : Group remaining time (m:s).

Group Address VLAN Port Up time Expire Count

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

234.5.6.7 1 00:00:09:17 2(P)

1 Eth 1/ 1(S)

2 Eth 1/ 2(R)

Console#
```

以下示例显示有关特定多播地址的详细信息：

```
Console#show mvr domain 1 members 234.5.6.7

MVR Domain : 1

MVR Forwarding Entry Count :1

Flag: S - Source port, R - Receiver port.

H - Host counts (number of hosts joined to group on this port).

P - Port counts (number of ports joined to group).

Up time: Group elapsed time (d:h:m:s).

Expire : Group remaining time (m:s).

Group Address VLAN Port Up time Expire Count

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

234.5.6.7 1 2(P)

1 Eth 1/ 1(S)

2 Eth 1/ 2(R)

Console#
```

23.4.19 show mvr profile

此命令显示所有已配置的 MVR 配置文件。

命令模式

特权模式

范例

以下显示了所有已配置的 MVR 配置文件：

```
Console#show mvr profile

MVR Profile Name Start IP Addr. End IP Addr.

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

rd 228.1.23.1 228.1.23.10

testing 228.2.23.1 228.2.23.10

Console#
```

23.4.20 show mvr statistics

此命令显示指定接口的 MVR 协议相关统计信息。

语法

show mvr statistics {**input** | **output**} [**interface** *interface*]

show mvr domain *domain-id* **statistics**{**input** [**interface** *interface*] | **output** [**interface** *interface*] |**query**}

domain-id -独立的组播域。（范围：1-5）

interface

ethernet *unit/port*

unit -单位标识符。（范围：1）

port -端口号。（范围：1-28）

port-channel *channel-id* (范围: 1-12)

vlan *vlan-id* - VLAN ID (范围: 1-4093)

query -显示与 MVR 查询相关的统计信息。

缺省配置

显示所有域的统计信息。

命令模式

特权模式

范例

以下显示收到的与 MVR 协议相关的统计信息：

```
Console#show mvr domain 1 statistics input

MVR Domain : 1

Input Statistics:

Interface Report Leave G Query G(-S)-S Query Drop Join Succ Group

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

Eth 1/ 1 23 11 4 10 5 20 9

Eth 1/ 2 12 15 8 3 5 19 4

VLAN 1 2 0 0 2 2 20 9

Console#
```

23.5 MVR FOR IPV6

本节介绍用于配置 IPv6 的组播 VLAN 注册（MVR6）的命令。可以使用单个网络范围的 VLAN 在服务提供商的网络中传输多播流量（例如电视频道）。进入 MVR VLAN 的任何多播流量都将发送给所有订户。 这可以显着降低为动态监视和建立正常组播 VLAN 的分发树所需的处理开销。另请注意，MVR 通过仅将多播流量传递到订户所属的其他 VLAN 来维护 VLAN 隔离提供的用户隔离和数据安全性。

23.5.1 mvr6 associated-profile

此命令将配置文件中指定的 MVR 组地址绑定到 MVR 域。 使用此命令的 no 形式删除绑定。

语法

[no] **mvr6 domain** *domain-id* **associated-profile** *profile-name*

domain-id -独立的组播域。（范围：1-5）

profile-name -包含一个或多个 MVRgroup 地址的配置文件的名称。（范围：1-21 个字符）

缺省配置

禁用

命令模式

全局配置

命令用法

MRV6 域可以与多个 MVR6 配置文件相关联。 但是，由于 MVR6 域不能共享组范围，因此 MRV6 配置文件通常与一个 MVR6 域相关联。

范例

以下是域 1 的 MVR 组地址配置文件：

```
Console(config)#mvr6 domain 1 associated-profile rd

Console(config)#
```

23.5.2 mvr6 domain

此命令为特定域启用多播 VLAN 注册（MVR）。使用此命令的 no 形式禁用域的 MVR。

语法

[no] **mvr6 domain** *domain-id*

domain-id -独立的组播域。（范围：1-5）

缺省配置

禁用

命令模式

全局配置

命令用法

当在域上启用 MVR6 时，与 mVR6 组关联的任何多播数据将从所有指定的源端口发送到已注册以从该多播组接收数据的所有接收器端口。

范例

以下示例为域 1 启用 MVR：

```
Console(config)#mvr6 domain 1

Console(config)#
```

23.5.3 mvr6 profile

此命令将一系列 MVR 组地址映射到配置文件。使用此命令的 no 形式删除配置文件。

语法

mvr6 profile *profile-name start-ip-address end-ip-address*

profile-name -包含一个或多个 MVR 组地址的配置文件的名称。（范围：1-21 个字符）

start-ip-address-启动 MVR 组播组的 IPv6 地址。此参数必须是完整的 IPv6 地址，包括网络前缀和主机地址位。

end-ip-address-结束 MVR 组播组的 IPv6 地址。此参数必须是完整的 IPv6 地址，包括网络前缀和主机地址位。

缺省配置

没有定义配置文件

命令模式

全局配置

命令用法

◆使用此命令静态配置将加入 MVR VLAN 的所有组播组地址。与 MVR 组相关联的任何多播数据都从所有源端口发送到所有已注册以从该多播组接收数据的接收器端口。

◆所有 IPv6 地址必须符合 RFC 2373“IPv6 Addressing Architecture”，使用 8 个冒号分隔的 16 位十六进制值。可以在地址中使用一个双冒号来指示填充未定义字段所需的零的数量。（注意 IP 地址 ff02 :: X 是保留的。）

◆分配给配置文件的 MVR6 组地址范围不能与任何其他配置文件的组地址范围重叠。

范例

以下示例将一系列 MVR 组地址映射到配置文件：

```
Console(config)#mvr6 profile rd ff00::1 ff00::9

Console(config)#
```

23.5.4 mvr6 proxy-query-interval

此命令配置接收方端口发送外部查询的时间间隔。使用 no 形式恢复默认设置。

语法

mvr proxy-query-interval *interval*

no mvr proxy-query-interval

interval -接收端口发送通用查询的时间间隔。（范围：2-31744 秒）

缺省配置

125 秒

命令模式

全局配置

命令用法

此命令设置活动接收器端口发送常规查询的常规查询间隔。此间隔仅在使用 mvr6 proxy-switching 命令启用代理交换机时有效。

范例

此示例设置 MVR 代理切换的代理查询间隔。

```
Console(config)#mvr profile rd 228.1.23.1 228.1.23.10
Console(config)#
```

23.5.5 mvr6 proxy-switching

此命令启用 MVR 代理切换，其中源端口充当主机，接收器端口充当具有服务启用功能的 MVR 路由器。使用 no 形式禁用此功能。

语法

[no] **mvr6 proxy-switching**

缺省配置

启用

命令模式

全局配置

命令用法

◆启用 MVR 代理切换时，MVR 源端口用作上游或主机　接口，MVR 接收端口用作伪装。　源端口通过发送汇总的成员资格报告仅执行 MVR 的主机部分，并自动禁用 MVR 路由器功能。

◆接收器端口称为下游或路由器接口。这些接口通过维护下游接口上所有 MVR 订阅的数据库来执行标准 MVR 路由器功能。因此，必须在需要 MVR 代理服务的所有下游接口上配置接收端口。

◆当源端口收到报告并保留消息时，它只会将它们转发到其他源端口。

◆当接收方端口收到任何查询消息时，它们将被丢弃。

◆当接收器端口通过报告和离开消息学习下游 MVR 组中发生的更改时，将创建 MVR 状态更改报告并将其发送到上游源端口，该端口将此信息转发到上游。

◆禁用 MVR 代理切换时：

- 从接收器/源端口接收的任何成员身份报告都将发送到所有源端口。
- 当源端口收到查询消息时，它将被转发到所有下游接收器端口。
- 当接收方端口收到查询消息时，它将被删除。

范例

以下示例启用 MVR 代理切换。

```
Console(config)#mvr proxy-switching

Console(config)#
```

23.5.6 mvr6 robustness-value

此命令配置预期的数据包丢失，从而配置生成报告和特定于组的查询的次数。使用 no 形式恢复默认设置。

语法

mvr6 robustness-value *value*

no mvr6 robustness-value

value -用于所有接口的健壮性。（范围：1-10）

缺省配置

2

命令模式

全局配置

命令用法

◆此命令用于设置在获知有关下游组的更改时上行报告消息的次数，以及将特定于组的查询发送到下游接收器端口的次数。

◆此命令仅在启用 MVR　6 代理切换时生效　。

范例

```
Console(config)#mvr6 robustness-value 5

Console(config)#
```

23.5.7 mvr6 source-port-mode dynamic

此命令将交换机配置为仅源端口动态连接的转发多播流。使用“no”形式来恢复缺省配置。

语法

[no] mvr6 source-port-mode dynamic

缺省配置

转发已在配置文件中指定并绑定到域的所有多播流。

命令模式

全局配置

命令用法

◆默认情况下，交换机会在配置文件设置的地址范围内转发所有组播流，并绑定到域。 多播流被发送到交换机上的所有源端口以及已选择接收该多播地址上的数据的所有接收器端口。

◆使用 mvr6 source-port-mode dynamic 命令时，该交换机只转发源端口动态加入的组播流。换句话说，在将组播流转发到任何连接的客户端之前，接收器端口和源端口都必须订阅组播组。请注意，请求的流仍然限制在已绑定到域的配置文件中指定的地址范围。

范例

```
Console(config)#mvr6 source-port-mode dynamic
Console(config)#
```

23.5.8 mvr6 upstream-source-ip

此命令配置分配给指定域上游发送的所有 MVR 控制数据包的源 IPv6 地址。使用 no 形式恢复默认设置。

语法

mvr6 domain *domain-id* **upstream-source-ip** *source-ip-address*

no mvr6 domain *domain-id* **upstream-source-ip**

domain-id -独立的组播域。（范围：1-5）

source-ip-address - 分配给上游发送的所有 MVRcontrol 数据包的源 IPv6 地址。此参数必须是完整的 IPv6 地址，包括网络前缀和主机地址位。

缺省配置

上游发送的所有 MVR 报告都使用空源 IP 地址

命令模式

全局配置

命令用法

所有 IPv6 地址必须符合 RFC 2373“IPv6 Addressing Architecture”，使用 8 个冒号分隔的 16 位十六进制值。可以在地址中使用一个双冒号来指示填充未定义字段所需的零的适当数量。（注意 IP 地址 ff02 :: X 是保留的。）

范例

```
Console(config)#mvr6 domain 1 upstream-source-ip 2001:DB8:2222:7223::72
Console(config)#
```

23.5.9 mvr6 vlan

此命令指定接收 MVR 多播数据的 VLAN。使用此命令的 no 形式恢复默认 MVR VLAN。

语法

mvr6 domain *domain-id* **vlan** *vlan-id*

no mvr6 domain *domain-id* **vlan**

domain-id -独立的组播域。（范围：1-5）

vlan-id-指定接收 MVR 组播数据的 VLAN。这也是必须分配所有源端口的 VLAN。（范围：1-4093）

缺省配置

VLAN 1

命令模式

全局配置

命令用法

可以使用 switchport allowed vlan 命令和 switchport native vlan 命令将 MVR 源端口配置为 MVR VLAN 的成员，但不应将 MVR 接收器端口静态配置为此 VLAN 的成员。

范例

以下示例将 MVR VLAN 设置为 VLAN 1：

```
Console(config)#mvr6 domain 1 vlan 1
Console(config)#
```

23.5.10 mvr6 immediate-leave

此命令使交换机在收到该组的离开消息后立即从多播流中删除接口。使用 no 形式恢复默认设置。

语法

[no] **mvr6 domain** *domain-id* **immediate-leave**

domain-id -独立的组播域。（范围：1-5）

缺省配置

禁用

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

◆立即请假仅适用于接收端口。启用后，将立即从离开消息中标识的多播组中删除该接收器端口。当禁用立即离开时，开关遵循标准规则，通过向接收器端口发送特定于组的查询并等待响应以确定在删除之前是否有该组播组的剩余订户组列表中的端口。

◆使用立即离开可以加快保留时间，但只应在仅连接到一个多播用户的端口上进行，以避免中断对连接到同一接口的其他组成员的服务。

◆立即离开不适用于已使用 mvr6 vlan group 命令暂时分配给端口的多播组 。

范例

以下内容允许在接收器端口上立即离开。

```
Console(config)#interface ethernet 1/5
Console(config-if)#mvr6 domain 1 immediate-leave
Console(config-if)#
```

23.5.11 mvr6 type

此命令将接口配置为 MVR 接收器或源端口。使用 no 形式恢复默认设置。

语法

[no] **mvr6 domain** *domain-id* **type** {**receiver** | **source**}

domain-id -独立的组播域。（范围：1-5）

receiver -将接口配置为可以的用户端口接收组播数据。

source -将接口配置为上行端口，可以为配置的组播组发送和接收组播数据。请注意，必须使用

switchport allowed vlan 命令手动将源端口配置为 MVR6 VLAN 的成员 。

缺省配置

端口类型未定义。

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

◆配置为 MVR6 接收器或源端口的端口可以加入或离开在 MVR6 下配置的多播组。

◆接收端口可以属于不同的 VLAN，但不应将其配置为 MVR VLAN 的成员。 另请注意，MVR 收发器端口的 VLAN 成员身份无法设置为访问模式（请参见 switchport mode 命令）。

◆可以将一个或多个接口配置为 MVR 源端口。源端口能够接收和发送通过 MVR6 协议加入的组播组的数据，或者通过 mvr6 vlan group 命令分配的组播组。所有源端口必须属于 MVR6 VLAN.订阅户不应直接连接到源端口。

◆同一端口不能配置为一个 MVR 域中的源端口，也不能配置为另一个域中的接收端口。

范例

以下配置在交换机上配置一个源端口和多个接收端口。

```
Console(config)#interface ethernet 1/5

Console(config-if)#mvr6 domain 1 type source

Console(config-if)#exit

Console(config)#interface ethernet 1/6

Console(config-if)#mvr6 domain 1 type receiver

Console(config-if)#exit

Console(config)#interface ethernet 1/7

Console(config-if)#mvr6 domain 1 type receiver

Console(config-if)#
```

23.5.12 mvr6 vlan group

此命令将组播组静态绑定到端口，该端口将接收与稳定主机集关联的长期组播流。 使用 no 形式恢复默认设置。

语法

[no] **mvr6 domain** *domain-id* **vlan** *vlan-id* **group** *ip-address*

domain-id -独立的组播域。（范围：1-5）

vlan-id -指定组播流量被刷新的接收者 VLAN。（范围：1-4093）

group -定义发送到所选端口的多播服务。

ip-address -静态配置接口以接收来自为 MVR 多播组指定的 IPv6 地址的 多播流量。此参数必须是完整的 IPv6 地址，包括网络前缀和主机地址位。

缺省配置

没有接收器端口是任何已配置的多播组的成员。

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

◆可以使用此命令将多播组静态分配给接收方端口。分配的地址必须在 mvr6 associated-profile 命令设置的范围内 。

◆所有 IPv6 地址必须符合 RFC 2373“IPv6 Addressing Architecture”，即 8 个冒号分隔的 16 位十六进制值。可以在地址中使用一个双冒号来指示填充未定义字段所需的零的适当数量。（注意 IP 地址 ff02 :: X 是保留的。）

◆ MVR VLAN 不能指定为静态绑定的接收者 VLAN。

范例

以下静态分配组播组到接收端口：

```
Console(config)#interface ethernet 1/2
Console(config-if)#mvr6 domain 1 type receiver
Console(config-if)#mvr6 domain 1 vlan 2 group ff00::1
Console(config-if)#
```

23.5.13 show mvr6

此命令显示有关 MVR 域设置的信息，包括 MVR 操作状态，组播 VLAN，当前组地址数和上游源 IP 地址。

语法

show mvr6 [**domain** *domain-id*]

domain-id -独立的组播域。（范围：1-5）

缺省配置

显示所有 MVR 域的配置设置。

命令模式

特权模式

范例

以下显示了 MVR 设置：

```
Console#show mvr6

MVR6 Proxy Switching : Enabled

MVR6 Robustness Value : 1

MVR6 Domain : 1

MVR6 Config Status : Enabled

MVR6 Running Status : Active

MVR6 Multicast VLAN : 1

MVR6 Upstream Source IP : FF05::25

Console#
```

23.5.14 show mvr6 associated-profile

此命令显示绑定指定域的概要文件。

语法

show mvr6 [**domain** *domain-id*] **associated-profile**

domain-id -独立的组播域。（范围：1-5）

缺省配置

显示绑定到所有 MVR 域的配置文件。

命令模式

特权模式

范例

以下显示绑定到域 1 的配置文件：

```
Console#show mvr6 domain 1 associated-profile
```

```
Domain ID : 1

MVR Profile Name Start IPv6 Addr. End IPv6 Addr.

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

rd FF00::1 FF00::9

Console#
```

23.5.15 show mvr6 interface

此命令显示连接到 MVR VLAN 的接口的 MVR 配置设置。

语法

show mvr6 [**domain** *domain-id*] **interface**

domain-id -独立的组播域。（范围：1-5）

缺省配置

显示所有连接接口的配置设置。

命令模式

特权模式

范例

以下显示有关连接到域 1 中的 MVR VLAN 的接口的信息：

```
Console#show mvr6 domain 1 interface

MVR6 Domain : 1

Port Type Status Immediate Static Group Address

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

Eth1/ 1 Source Active/Up

Eth1/ 2 Receiver Active/Up 禁用 FF00::1(VLAN2)

Console#
```

23.5.16 show mvr6 members

此命令显示有关转发数据库中当前条目数的信息，或有关特定多播地址的详细信息。

语法

show mvr6 [**domain** *domain-id*] **members** [*ip-address*]

domain-id -独立的组播域。（范围：1-5）

ip-address - MVR 组播组的 IPv6 地址。

缺省配置

显示所有域和所有转发条目的配置设置。

命令模式

特权模式

范例

以下显示有关域 1 中当前活动的多播转发数量的信息：

```
Console#show mvr6 domain 1 members

MVR6 Domain : 1

MVR6 Forwarding Entry Count :1

Flag: S - Source port, R - Receiver port.

H - Host counts (number of hosts join the group on this port).

P - Port counts (number of ports join the group).

Up time: Group elapsed time (d:h:m:s).

Expire : Group remaining time (m:s).

Group Address VLAN Port Up time Expire Count

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

FF00::1 1 2(P)

1 Eth1/ 1(S)

2 Eth1/ 2(S)

Console#
```

以下示例显示有关特定多播地址的详细信息：

```
Console#show mvr6 domain 1 members ff00::1

MVR6 Domain : 1

MVR6 Forwarding Entry Count :1

Flag: S - Source port, R - Receiver port.

H - Host counts (number of hosts join the group on this port).

P - Port counts (number of ports join the group).

Up time: Group elapsed time (d:h:m:s).
```

```
Expire : Group remaining time (m:s).

Group Address VLAN Port Up time Expire Count

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

FF00::1 1 2(P)

1 Eth1/ 1(S)

2 Eth1/ 2(S)

Console#
```

23.5.17 show mvr6 profile

此命令显示所有已配置的 MVR 配置文件。

命令模式

特权模式

范例

以下显示了所有已配置的 MVR 配置文件：

```
Console#show mvr6 profile

MVR Profile Name Start IPv6 Addr. End IPv6 Addr.

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

rd FF00::1 FF00::9

Console#
```

23.5.18 show mvr6 statistics

此命令显示指定接口的 MVR 协议相关统计信息。

语法

show mvr6 statistics {**input** | **output**} [**interface** *interface*]

show mvr6 domain *domain-id* **statistics**{**input** [**interface** *interface*] | **output** [**interface** *interface*] |**query**}

domain-id -独立的组播域。（范围：1-5）

interface

ethernet *unit/port*

unit -单位标识符。（范围：1）

port -端口号。（范围：1-28）

port-channel *channel-id*（范围：1-12）

vlan *vlan-id* - VLAN ID（范围：1-4093）

query -显示与 MVR 查询相关的统计信息。

缺省配置

显示所有域的统计信息。

命令模式

特权模式

范例

以下显示收到的与 MVR 协议相关的统计信息：

```
Console#show mvr6 domain 1 statistics input

MVR Domain : 1

Input Statistics:

Interface Report Leave G Query G(-S)-S Query Drop Join Succ Group

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

Eth 1/ 1 23 11 4 10 5 20 9

Eth 1/ 2 12 15 8 3 5 19 4

VLAN 1 2 0 0 2 2 20 9

Console#
```

以下显示了与 MVR 协议相关的统计信息：

```
Console#show mvr6 domain 1 statistics output

MVR Domain : 1

Output Statistics:

Interface Report Leave G Query G(-S)-S Query

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

Eth 1/ 1 12 0 1 0

Eth 1/ 2 5 1 4 1

VLAN 1 7 2 3 0

Console#
```

以下显示了与 MVR 查询相关的统计信息：

```
Console#show mvr6 domain 1 statistics query

Querier IPv6 Address : FE80::2E0:CFF:FE00:FB/64

Querier Expire Time : 00(h):00(m):30(s)

General Query Received : 10

General Query Sent : 0

Specific Query Received : 2

Specific Query Sent : 0

Number of Reports Sent : 2

Number of Leaves Sent : 0

Console#
```

24 LLDP 命令

链路层发现协议（LLDP）用于发现本地广播域上相邻设备的基本信息。LLDP 是第 2 层协议，它使用周期广播来通告有关这些设备的信息。通告信息根据 IEEE 802.1ab 标准以类型长度值（TLV）格式表示，并且可以包括诸如设备标识、端口配置之类的细节。LLDP 还定义如何存储和维护关于它发现的相邻网络节点的信息。链路层发现协议 - 媒体端点发现（LLDP-MED）是 LLDP 的扩展，用于管理端点设备，如 Voice over IP 电话和网络交换机。 LLDP-MED TLV 通告信息，例如网络策略、电源、设备位置等详细信息。 SNMP 应用程序可以使用 LLDP 和 LLDP-MED 信息来进行简单故障排除，增强网络管理，并维护准确的物理网络拓扑。

24.1.1 lldp

此命令在交换机上全局启用 LLDP。使用 no 形式禁用 LLDP。

语法

[no] lldp

缺省配置

启用

命令模式

全局配置

范例

```
Console(config)#lldp

Console(config)#
```

24.1.2 lldp holdtime-multiplier

此命令配置 LLDP 公示中发送的生存时间（TTL）值。使用 no 形式恢复默认设置。

语法

lldp holdtime-multiplier *value*

no lldp holdtime-multiplier

value -根据以下规则以秒为单位计算 TTL：最小值（(传输间隔*保持时间乘数）或 65536）(范围：2 - 10)

缺省配置

保持时间乘数：4

TTL：4*30 = 120 秒

命令模式

全局配置

命令用法

生存时间告诉接收 LLDP 代理如果没有及时发送更新，保留与发送 LLDP 代理有关的所有信息需要多长时间。

范例

```
Console(config)#lldp holdtime-multiplier 10
Console(config)#
```

24.1.3 lldp med-fast-start-count

此命令指定在 LLDP-MED 快速启动机制的激活过程中要传输的 MED 快速启动 LLDPDU 的数量。

语法

lldp med-fast-start-count *packets*

seconds -数据包的数量。(范围：1-10 包;默认值：4 包)

缺省配置

4 包

命令模式

全局配置

命令用法

此参数是计时器的一部分，用于确保 LLDP-MED FastStart 机制对端口有效。LLDP-MED 快速启动对于 LLDP 的及时启动至关重要，因此对于紧急呼叫服务的快速可用性是不可或缺的。

范例

```
Console(config)#lldp med-fast-start-count 6

Console(config)#
```

24.1.4 lldp notification-interval

此命令配置发送有关 LLDP MIB 更改的 SNMP 通知的允许时间间隔。使用 no 形式恢复默认设置。

语法

lldp notification-interval *seconds*

no lldp notification-interval

seconds -指定发送 SNMP 通知的时间间隔。（范围：5 - 3600 秒）

缺省配置

5 秒

命令模式

全局配置

命令用法

◆此参数仅适用于使用 LLDP MIB 中存储的数据进行网络监视或管理的 SNMP 应用程序。

◆在 SNMP 通知之间发生的关于 LLDP 邻居的改变的信息不被发送。只有在通知时存在的状态变化包含在传输中。SNMP 代理应该定期检查 lldp Stats Rem Table 变更时间的值，以检测由于节流或传输丢失而遗漏的任何 lldp Rem Tables 变更通知事件。

范例

```
Console(config)#lldp notification-interval 30

Console(config)#
```

24.1.5 lldp refresh-interval

此命令配置 LLDP 推送的周期性传输间隔。使用 no 形式恢复默认设置。

语法

lldp refresh-interval *seconds*

no lldp refresh-delay

seconds -指定发送 LLDP 推送的周期性间隔。 （范围：5 - 32768 秒）

缺省配置

30 秒

命令模式

全局配置

范例

```
Console(config)#lldp refresh-interval 60
Console(config)#
```

24.1.6 lldp reinit-delay

此命令在禁用 LLDP 端口、链路断开后，尝试重新初始化之前的延迟。使用 no 形式恢复默认设置。

语法

lldp reinit-delay *seconds*

no lldp reinit-delay

seconds -指定尝试重新初始化 LLDP 之前的延迟。（范围：1 - 10 秒）

缺省配置

2 秒

命令模式

全局配置

命令用法

在端口上重新初始化 LLDP 时，将删除与此端口关联的远程系统 LLDP MIB 中的所有信息。

范例

```
Console(config)#lldp reinit-delay 10
Console(config)#
```

24.1.7 lldp tx-delay

本地 LLDP MIB 变量的更改，会启动连续的报文传输，本命令配置这些连续的报文之间的延迟。

使用 no 形式恢复默认设置。

语法

lldp tx-delay *seconds*

no lldp tx-delay

seconds -指定传输数据。（范围：1 - 8192 秒）

缺省配置

2 秒

命令模式

全局配置

命令用法

◆传输延迟用于在本地 LLDP MIB 对象的短时间快速变化期间防止一系列连续的 LLDP 传输，并增加在每次传输中报告多个而不是单个变化的概率。

◆ 此属性必须符合以下规则：（4 * tx-delay） ≤ 刷新间隔

范例

```
Console(config)#lldp tx-delay 10

Console(config)#
```

24.1.8 lldp admin-status

此命令在指定端口上启用 LLDP 发送、接收模式。使用 no 形式禁用此功能。

语法

lldp admin-status {**rx-only** | **tx-only** | **tx-rx**}

no lldp admin-status

rx-only -仅接收 LLDP PDU。

tx-only - 仅发送 LLDP PDU。

tx-rx - 发送和接收 LLDP 协议数据单元（PDU）。

缺省配置

tx-rx

命令模式

接口配置 (Ethernet, Port Channel)

范例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp admin-status rx-only
Console(config-if)#
```

24.1.9 lldp basic-tlv management-ip-address

此命令配置启用 LLDP 的端口以通告此设备的管理地址。使用 no 形式禁用此功能。

语法

[no] lldp basic-tlv management-ip-address

缺省配置

启用

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

◆管理地址协议包包括交换机的 IPv4 地址。如果没有可用的管理地址，则该地址应该是 CPU 的 MAC 地址或发送此广告的端口。

◆管理地址 TLV 还可以包括关于与该地址相关联的特定接口的信息，以及指示与该地址相关联的硬件组件或协议实体的类型的对象标识符。包括接口号和 OID 以帮助 SNMP 应用程序通过指示搜索的企业特定或其他起始点（例如接口或实体 MIB）来执行网络发现 。

◆由于通常存在与第 3 层设备相关联的多个不同地址，因此单个 LLDP PDU 可以包含多个管理地址 TLV。

◆通过特定端口报告端口和协议 VLAN 上可访问的地址的每个管理地址 TLV 应附有端口和协议 VLAN TLV，该 TLV 指示与此 TLV 报告的管理地址关联的 VLAN 标识符（VID）。

范例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv management-ip-address
Console(config-if)#
```

24.1.10 lldp basic-tlv port-description

此命令配置启用 LLDP 的端口以通告其端口描述。使用 no 形式禁用此功能。

语法

[no] lldp basic-tlv port-description

缺省配置

启用

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

端口描述取自 RFC 2863 中的 ifDescr 对象，其中包括有关制造商，产品名称和接口硬件/软件版本的信息。

范例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv port-description
Console(config-if)#
```

24.1.11 lldp basic-tlv system-capabilities

此命令配置启用 LLDP 的端口以通告其系统功能。使用 no 形式禁用此功能。

语法

[no] lldp basic-tlv system-capabilities

缺省配置

启用

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

系统功能识别系统的主要功能以及是否启用这些主要功能。该 TLV 所转发的信息在 IEEE 802.1AB 中描述。

范例

```
Console(config)#interface ethernet 1/1
```

```
Console(config-if)#lldp basic-tlv system-capabilities

Console(config-if)#
```

24.1.12 lldp basic-tlv system-description

此命令配置启用 LLDP 的端口以通告系统描述。使用 no 形式禁用此功能。

语法

[no] lldp basic-tlv system-description

缺省配置

启用

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

系统描述取自 RFC 3418 中的 sysDescr 对象，其中包括系统硬件类型，软件操作系统和网络软件的全名和版本标识。

范例

```
Console(config)#interface ethernet 1/1

Console(config-if)#lldp basic-tlv system-description

Console(config-if)#
```

24.1.13 lldp basic-tlv system-name

此命令配置启用 LLDP 的端口以通告系统名称。使用 no 形式禁用此功能。

语法

[no] lldp basic-tlv system-name

缺省配置

启用

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

系统名称取自 RFC 3418 中的 sysName 对象，该对象包含系统的管理分配名称，并依次基于

hostname 命令。

范例

```
Console(config)#interface ethernet 1/1

Console(config-if)#lldp basic-tlv system-name

Console(config-if)#
```

24.1.14 lldp dot1-tlv proto-ident

此命令配置启用 LLDP 的端口以通告支持的协议。使用 no 形式禁用此功能。

语法

[no] lldp dot1-tlv proto-ident

缺省配置

启用

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

此选项公布可通过此接口访问的协议。

范例

```
Console(config)#interface ethernet 1/1

Console(config-if)#no lldp dot1-tlv proto-ident

Console(config-if)#
```

24.1.15 lldp dot1-tlv proto-vid

该命令用来配置 LLDP 功能端口发布基于端口的协议 VLAN 信息。使用 no 形式禁用此功能。

语法

[no] lldp dot1-tlv proto-vid

缺省配置

启用

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

此选项通告在此接口上配置的基于端口的协议 VLAN（请参阅“配置基于协议的 VLAN”）。

范例

```
Console(config)#interface ethernet 1/1

Console(config-if)#no lldp dot1-tlv proto-vid

Console(config-if)#
```

24.1.16 lldp dot1-tlv pvid

此命令配置启用 LLDP 的端口以通告其缺省 VLAN ID。 使用 no 形式禁用此功能。

语法

[no] lldp dot1-tlv pvid

缺省配置

启用

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

端口的默 VLAN 标识符（PVID）表示与标记的帧或优先级标记的帧关联的 VLAN（请参阅 switchportnative vlan 命令）。

范例

```
Console(config)#interface ethernet 1/1

Console(config-if)#no lldp dot1-tlv pvid

Console(config-if)#
```

24.1.17 lldp dot1-tlv vlan-name

此命令配置启用 LLDP 的端口以通告其 VLAN 名称。使用 no 形式禁用此功能。

语法

[no] lldp dot1-tlv vlan-name

缺省配置

启用

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

此选项通告已为此接口分配的所有 VLAN 的名称。请参阅“switchport allowed vlan”和“protocolvlan protocol-group（配置接口）” 。

范例

```
Console(config)#interface ethernet 1/1

Console(config-if)#no lldp dot1-tlv vlan-name

Console(config-if)#
```

24.1.18 lldp dot3-tlv link-agg

此命令配置启用 LLDP 的端口以通告链路聚合功能。使用 no 形式禁用此功能。

语法

[no] lldp dot3-tlv link-agg

缺省配置

启用

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

如果此接口当前是链路聚合成员，则此选项通告链路聚合功能，链路的聚合状态以及 802.3 聚合端口标识符。

范例

```
Console(config)#interface ethernet 1/1

Console(config-if)#no lldp dot3-tlv link-agg

Console(config-if)#
```

24.1.19 lldp dot3-tlv mac-phy

此命令配置启用 LLDP 的端口以通告其 MAC 和物理层功能。使用 no 形式禁用此功能。

语法

[no] lldp dot3-tlv mac-phy

缺省配置

启用

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

此选项通告 MAC / PHY 配置/状态这包括信息关于自动协商支持/能力，operational Multi - 站接入单元（MAU）类型。

范例

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot3-tlv mac-phy
Console(config-if)#
```

24.1.20 lldp dot3-tlv max-frame

此命令配置启用 LLDP 的端口以通告其最大帧大小。使用 no 形式禁用此功能。

语法

[no] lldp dot3-tlv max-frame

缺省配置

启用

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

有关配置此开关的最大帧大小的信息，请参阅“帧大小”。

范例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp dot3-tlv max-frame
Console(config-if)#
```

24.1.21 lldp med-location civic-addr

此命令用于配置 LLDP-MED 端口，所通告的位置标识详细信息。使用 no 形式恢复默认设置。

语法

lldp med-location civic-addr [[**country** *country-code*] |[**what** *device-type*] | [*ca-type ca-value*]]

no lldp med-location civic-addr [[**country**] | [**what**] | [*ca-type*]]

country-code - 使用大写 ASCII 字母的双字母 ISO 3166 国家代码。（例如：DK，DE 或 US）

device-type - 位置适用的设备类型。

0 - DHCP 服务器的位置。

1 - 最靠近客户端的网络元素的位置。

2 - 客户的位置。

ca-type - 数据城市地址值的一个八位字节描述符。（范围： 0-255）

ca-value - 位置描述。（范围：1-32 个字符）

缺省配置

无

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

◆使用此命令不带任何关键字来宣传位置详细信息。

◆使用 *ca-type* 宣传设备的物理位置，即城市，街道号，建筑物和房间信息。地址位置被指定为类型和值对，其中城市地址（CA）类型在 RFC 4776 中定义。下表描述了一些 CA 类型编号并提供了示例。可以为 civic 地址位置指定任意数量的 CA 类型和值对，只要总数不超过 250 个字符即可。

◆对于为设备类型定义的位置选项，通常选项 **2** 用于指定客户端设备的位置。在客户端设备位置未知的情况下，可以使用 **0** 和 **1**，前提是客户端设备在物理上靠近 DHCP 服务器或网络元件。

范例

以下示例启用位置标识详细信息。

```
Console(config)#interface ethernet 1/1

Console(config-if)#lldp med-location civic-addr

Console(config-if)#lldp med-location civic-addr 1 California

Console(config-if)#lldp med-location civic-addr 2 Orange

Console(config-if)#lldp med-location civic-addr 3 Irvine

Console(config-if)#lldp med-location civic-addr 4 West Irvine

Console(config-if)#lldp med-location civic-addr 6 Exchange

Console(config-if)#lldp med-location civic-addr 18 Avenue

Console(config-if)#lldp med-location civic-addr 19 320
```

```
Console(config-if)#lldp med-location civic-addr 27 5

Console(config-if)#lldp med-location civic-addr 28 509B

Console(config-if)#lldp med-location civic-addr country US

Console(config-if)#lldp med-location civic-addr what 2

Console(config-if)#
```

24.1.22 lldp med-notification

此命令开启端口传输 LTDP-MED 更改的 SNMP 通知。使用 no 形式禁用 LLDP-MED 通知。

语法

[no] lldp med-notification

缺省配置

禁用

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

◆此选项以 lldp notification-interval 命令指定的时间间隔向指定的目标站发送 SNMP 通知。通知包括有关 LLDP MIB（IEEE 802.1AB），LLDP-MED MIB（ANSI / TIA 1057）或组织特定 LLDP-EXT-DOT1 和 LLDP-EXT-DOT3 MIB 中的状态更改的信息。

◆使用 snmp-server host 命令定义 SNMP 主机。

◆不传输有关 SNMP 通知之间发生的 LLDP 邻居的其他更改的信息。在传输中仅包含状态更改。因此 SNMP 代理应定期检查 lldpStatsRemTableLast 更改时间的值，以检测由于限制或传输丢失而丢失的任何 lldpRemTables 更改通知事件。

范例

```
Console(config)#interface ethernet 1/1

Console(config-if)#lldp med-notification

Console(config-if)#
```

24.1.23 lldp med-tlv inventory

此命令配置启用 LLDP-MED 的端口以通告其库存标识详细信息。使用 no 形式禁用此功能。

语法

[no] lldp med-tlv inventory

缺省配置

启用

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

此选项公布对库存管理有用的设备详细信息，例如制造商、型号、软件版本和其他相关信息。

范例

```
Console(config)#interface ethernet 1/1

Console(config-if)#no lldp med-tlv inventory

Console(config-if)#
```

24.1.24 lldp med-tlv location

此命令用于配置 LLDP-MED 端口，以通告其位置标识详细信息。使用 no 形式禁用此功能。

语法

[no] lldp med-tlv location

缺省配置

启用

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

此选项公布位置标识详细信息。

范例

```
Console(config)#interface ethernet 1/1

Console(config-if)#lldp med-tlv location

Console(config-if)#
```

24.1.25 lldp med-tlv med-cap

此命令配置启用 LLDP-MED 的端口以通告其媒体端点设备功能。使用 no 形式禁用此功能。

语法

[no] lldp med-tlv med-cap

缺省配置

启用

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

此选项通告 LLDP-MED TLV 功能，允许媒体端点连接设备有效地发现交换机支持哪些 LLDP-MED 相关的 TLV。

范例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp med-tlv med-cap
Console(config-if)#
```

24.1.26 lldp med-tlv network-policy

此命令用于配置 LLDP-MED 端口，以通告其网络策略配置。使用 no 形式禁用此功能。

语法

[no] lldp med-tlv network-policy

缺省配置

启用

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

此选项通告网络策略配置信息，帮助发现和诊断端口上的 VLAN 配置不匹配。不正确的网络策略配置经常导致语音质量下降或完全服务中断。

范例

```
Console(config)#interface ethernet 1/1
```

```
Console(config-if)#lldp med-tlv network-policy

Console(config-if)#
```

24.1.27 lldp notification

此命令可以传输有关 LTDP 更改的 SNMP trap 通知。使用 no 形式禁用 LLDP 通知。

语法

[no] lldp notification

缺省配置

禁用

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

◆此选项以 lldp notification-interval 命令指定的时间间隔向指定的目标站发送 SNMP trap 通知。trap 通知包括有关 LLDP MIB(IEEE 802.1AB)或组织特定 LLDP-EXT-DOT1 和 LLDP-EXT-DOT3 MIB 中的状态更改的信息。

◆使用 snmp-server host 命令定义 SNMP trap 目标。

◆不传输有关 SNMP 通知之间发生的 LLDP 邻居的其他更改的信息。在传输中仅包括 trap 通知时的状态变化。因此 SNMP 代理应定期检查 lldpStatsRemTable 最后更改时间的值，以检测由于限制或传输丢失而丢失的任何 lldpRemTables 更改通知事件。

范例

```
Console(config)#interface ethernet 1/1

Console(config-if)#lldp notification

Console(config-if)#
```

24.1.28 show lldp config

此命令显示所有端口的 LLDP 配置设置。

语法

show lldp config [**detail** *interface*]

detail - Shows configuration summary.

interface

ethernet *unit/port*

unit -单位标识符。（范围：1）

port -端口号。（范围：1-28）

port-channel *channel-id* (范围: 1-12)

命令模式

特权模式

范例

```
Console#show lldp config

LLDP Global Configuation

LLDP Enabled : Yes

LLDP Transmit Interval : 30 sec.

LLDP Hold Time Multiplier : 4

LLDP Delay Interval : 2 sec.

LLDP Re-initialization Delay : 2 sec.

LLDP Notification Interval : 5 sec.

LLDP MED Fast Start Count : 4

LLDP Port Configuration

Port Admin Status Notification Enabled

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

Eth 1/1 Tx-Rx True

Eth 1/2 Tx-Rx True

Eth 1/3 Tx-Rx True

Eth 1/4 Tx-Rx True

Eth 1/5 Tx-Rx True

...
```

24.1.29 show lldp info local-device

此命令显示此设备的 LLDP 全局和接口特定的配置设置。

语法

show lldp info local-device [**detail** *interface*]

detail - Shows configuration summary.

interface

ethernet *unit/port*

unit -单位标识符。(范围：1)

port -端口号。(范围：1-28)

port-channel *channel-id* (范围: 1-12)

命令模式

特权模式

范例

```
Console#show lldp info local-device

LLDP Local System Information

Chassis Type : MAC Address

Chassis ID : 00-01-02-03-04-05

System Name :

System Description : ECS4510-28T

System Capabilities Support : Bridge

System Capabilities Enable : Bridge

Management Address : 192.168.0.101 (IPv4)

LLDP Port Information

Port PortID Type PortID Port Description

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

Eth 1/1 MAC Address 00-12-CF-DA-FC-E9 Ethernet Port on unit 0, port 1

Eth 1/2 MAC Address 00-12-CF-DA-FC-EA Ethernet Port on unit 0, port 2

Eth 1/3 MAC Address 00-12-CF-DA-FC-EB Ethernet Port on unit 0, port 3

Eth 1/4 MAC Address 00-12-CF-DA-FC-EC Ethernet Port on unit 0, port 4
```

```
...

Console#show lldp info local-device detail ethernet 1/1

LLDP Port Information Details

Port : Eth 1/1

Port Type : MAC Address

Port ID : 00-12-CF-DA-FC-E9

Port Description : Ethernet Port on unit 0, port 1

MED Capability : LLDP-MED Capabilities

Network Policy

Location Identification

Inventory

Console#
```

24.1.30 show lldp inforemote-device

此命令显示远程设备的 LLDP 全局和接口设置。

语法

show lldp info remote-device [**detail** *interface*]

detail - Shows configuration summary.

interface

ethernet *unit/port*

unit -单位标识符。（范围：1）

port -端口号。（范围：1-28）

port-channel *channel-id* (范围: 1-12)

命令模式

特权模式

范例

请注意，必须将用于通告 LLDPMED 功能的 IP 电话或其他终端节点设备连接到交换机，以便在“设备类”和其他相关字段中显示信息。

```
Console#show lldp info remote-device
```

LLDP Remote Devices Information

Interface Chassis ID Port ID System Name

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

Eth 1/1 00-E0-0C-00-00-FD 00-E0-0C-00-01-02

Console#show lldp info remote-device detail ethernet 1/1

Local Port Name : Eth 1/2

Chassis Type : MAC Address

Chassis ID : 70-72-CF-18-B7-E0

Port ID Type : MAC Address

Port ID : 70-72-CF-18-B7-E1

System Name :

System Description : ECS4510-28T

Port Description : Ethernet Port on unit 0, port 1

SystemCapSupported : Bridge

SystemCap 启用 : Bridge

Remote Management Address :

192.168.0.5 (IPv4)

Remote Port VID : 1

Remote Port-Protocol VLAN :

VLAN-3 : supported, Enabled

Remote VLAN Name :

VLAN-1 : default Vlan

Remote Protocol Identity (Hex) :

88-CC

Remote MAC/PHY Configuration Status :

Remote port auto-neg supported : Yes

Remote port auto-neg Enabled : Yes

Remote port auto-neg advertised cap (Hex) : 0000

Remote port MAU type : 6

```
Remote Power via MDI :

Remote power class : PSE

Remote power MDI supported : Yes

Remote power MDI Enabled : Yes

Remote power pair controllable : No

Remote power pairs : Spare

Remote power classification : Class1

Remote Link Aggregation :

Remote link aggregation capable : Yes

Remote link aggregation enable : No

Remote link aggregation port ID : 0

Remote Max Frame Size : 1518

LLDP-MED Capability :

Device Class : Type Not Defined

Console#
```

24.1.31 show lldp info statistics

此命令显示接口接收的 LLDP 流量的统计信息。

语法

show lldp info statistics [**detail** *interface*]

detail - Shows configuration summary.

interface

ethernet *unit/port*

unit -单位标识符。(范围：1)

port -端口号。(范围：1-28)

port-channel *channel-id* (范围: 1-12)

命令模式

特权模式

范例

```
Console#show lldp info statistics

LLDP Device Statistics

Neighbor Entries List Last Updated : 2450279 seconds

New Neighbor Entries Count : 1

Neighbor Entries Deleted Count : 0

Neighbor Entries Dropped Count : 0

Neighbor Entries Ageout Count : 0

Port NumFramesRecvd NumFramesSent NumFramesDiscarded

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

Eth 1/1 0 83 0

Eth 1/2 11 12 0

Eth 1/3 0 0 0

Eth 1/4 0 0 0

Eth 1/5 0 0 0

...

Console#show lldp info statistics detail ethernet 1/1

LLDP Port Statistics Detail

PortName : Eth 1/1

Frames Discarded : 0

Frames Invalid : 0

Frames Received : 12

Frames Sent : 13

TLVs Unrecognized : 0

TLVs Discarded : 0

Neighbor Ageouts : 0

Console#
```

25 CFM 命令

连接故障管理（CFM）是一种 OAM 协议，包括使用连续性检查消息进行主动连接监控，通过环回消息进行故障验证，以及通过提供商边缘设备之间或客户边缘设备之间的端到端连接进行故障隔离。

CFM 被实现为基于服务实例的服务级别协议，该服务实例仅包含支持特定客户的城域网的那部分。CFM 还可以提供对维护域层次结构（例如客户，服务提供商和设备运营商）的受控管理访问。

以下命令列表支持定义 CFM 结构的功能，包括域，维护关联和维护访问点。它还通过所有已知维护点的连续性检查消息提供故障检测命令，并为位于其他设备上的静态配置维护点提供交叉检查消息。通过回送消息支持故障验证，通过链路跟踪消息进行故障隔离。故障通知还由 SNMP 警报提供，当在本地维护域中检测到连接故障或配置错误时，这些警报由维护点自动生成。

CFM 的基本配置步骤

1. 使用 ethernet cfm domain 命令配置维护域 。
2. 使用 ma index name 命令配置维护关联 。
3. 使用 ethernet cfm mep 命令配置本地维护端点（MEP），该端点将作为指定维护关联的域服务访问点 。
4. 使用 mep crosscheck mpid 命令输入分配给同一维护关联中其他设备的 MEP 的静态列表。这允许 CFM 通过交叉检查此设备上配置的静态列表与通过连续性获知的信息来自动验证这些远程端点的功能。检查消息。
5. 使用 ethernet cfm enable 命令在交换机上全局启用 CFM。
6. 使用 ethernet cfm port-enable 命令在本地 MEP 上启用 CFM。
7. 使用 ethernet cfm cc enable 命令启用连续性检查操作。
8. 使用 ethernet cfm mep crosscheck 命令启用交叉检查操作。

25.1 定义 CFM 结构

25.1.1 ethernet cfm aislevel

此命令用于配置在指定 MA 内发送 Alarm Indication Signal（AIS）信息的维护级别。使用 **no** 形式恢复默认设置。

语法

ethernet cfm ais level *level-id* **md** *domain-name* **ma** *ma-name*

no ethernet cfm ais level md *domain-name* **ma** *ma-name*

level-id - 发送 AIS 信息的维护级别。（范围：0-7）

domain-name -域名。（范围：1-43 个字母数字字符）

ma-name - 维护关联名称。（范围：1-43 个字母数字字符）

缺省配置

Level 0

命令模式

全局配置

命令用法

配置的 AIS 级别必须高于包含指定 MA 的域的维护级别。

范例

此示例设置在指定的 MA 上发送 AIS 消息的维护级别。

```
Console(config)#ethernet cfm ais level 4 md voip ma rd
Console(config)#
```

25.1.2 ethernet cfm ais ma

该命令使指定 MA 内的 MEP 能够在检测到缺陷条件后发送带有 AIS 信息的帧。使用 **no** 形式禁用此功能。

语法

[**no**] **ethernet cfm ais md** *domain-name* **ma** *ma-name*

domain-name -域名。（范围：1-43 个字母数字字符）

ma-name – 维护关联名称。（范围：1-43 个字母数字字符）

缺省配置

禁用

命令模式

全局配置

命令用法

◆ 每个 MA 名称在 CFM 域中必须是唯一的。

◆在检测到缺陷条件时，MEP 可以在客户的维护级别发布具有 AIS 信息的框架。例如，缺陷条件可能包括：

- 如果启用了连续性检查，则表示信号故障。
- 如果禁用连续性检查，则为 AIS 条件或 LCK 条件。

◆MEP 继续发送带有 AIS 信息的周期帧，直到删除缺陷条件。

范例

此示例使指定 MA 内的 MEP 能够发送带有 AIS 信息的帧。

```
Console(config)#ethernet cfm ais md voip ma rd

Console(config)#
```

25.1.3 ethernet cfm aisperiod

此命令用于配置发送 AIS 信息的时间间隔。使用 no 形式恢复默认设置。

语法

ethernet cfm ais period *period* **md** *domain-name* **ma** *ma-name*

no ethernet cfm ais period md *domain-name* **ma** *ma-name*

period – 发送 AIS 信息的时间间隔（选项：1 秒，60 秒）

domain-name –域名。（范围：1-43 个字母数字字符）

ma-name – 维护关联名称。（范围：1-43 个字母数字字符）

缺省配置

1 秒

命令模式

全局配置

范例

此示例设置发送带有 AIS 信息的帧的间隔为 60 秒。

```
Console(config)#ethernet cfm ais period 60 md voip ma rd

Console(config)#
```

25.1.4 ethernet cfm ais suppress alarm

该命令禁止在检测到故障条件之后发送包含 AIS 信息的帧。使用 no 形式恢复默认设置。

语法

[no] **ethernet cfm ais suppress alarm md** *domain-name*

ma *ma-name*

domain-name -域名。(范围：1-43 个字母数字字符)

ma-name -维护关联名称。(范围：1-43 个字母数字字符)

缺省配置

抑制被禁用

命令模式

全局配置

命令用法

◆对于多点连接,MEP 无法确定在接收到具有 AIS 信息的帧时遇到故障条件的特定维护级别实体。更重要的是它无法确定其对等 MEP 的相关子集，因为它应该抑制警报，因为收到的 AIS 信息不包含该信息。因此在接收到具有 AIS 信息的帧时，MEP 将抑制所有对等 MEP 的警报，此时它们仍然是连接的。

◆但是对于点对点连接，MEP 只有一个同等的 MEP，当它接收到带有 AIS 信息的帧时，可以抑制警报。

◆如果通过此命令启用抑制，则在收到带有 AIS 信息的帧时，MEP 会检测到 AIS 条件并抑制与其所有对等MEP关联的连续性警报丢失。在没有AIS消息的情况下检测到连续性故障条件的丢失时，MEP 恢复丢失连续性警报。

范例

此示例禁止发送带有 AIS 信息的帧。

```
Console(config)#ethernet cfm ais suppress alarm md voip ma rd
Console(config)#
```

25.1.5 ethernet cfm domain

此命令定义 CFM 维护域，设置授权维护级别，并进入 CFM 配置模式。使用 **no** 形式删除 CFM 维护域。

语法

ethernet cfm domain index *index* **name** *domain-name* **level** *level-id*[**mip-creation** *type*]

no ethernet cfm domain index *index*

index - 域索引。 （范围：1-65535）

domain-name - 域名。 （范围：1-43 个字母数字字符）

level-id - 此域的授权维护级别。（范围：0-7）

type - 指定 CFM 协议在此域中维护中间点（MIP）的创建方法：

default - 可以为 MA 的 VID 可以通过的任何网桥端口上的此域中配置的任何维护关联（MA）创建 MIP。

显式 - 只有在 MA 的 VID 可以通过的桥接端口上，才能为此域中配置的任何 MA 创建 MIP ，并且只有在某个较低的 MA 级别创建维护端点（MEP）时才能创建 MIP。

none - 无法为此域中配置的任何 MA 创建 MIP。

缺省配置

没有配置维护域。

没有为指定域中的任何 MA 创建 MIP。

命令模式

全局配置

命令用法

◆域只能配置一个名称。

◆在嵌套域的情况下，上层分层域必须具有比其包含的更高的维护级别。较低级域类型的较高级通常包括诸如客户，服务提供商和运营商之类的实体。

◆可以在同一维护级别配置多个域，但只能为一个域配置一个维护级别。

◆如果使用 ethernet cfm mep 命令或 ma index name 命令为域配置了 MEP 或 MA ，则必须先

删除它们，然后才能删除域。

◆维护域旨在提供透明的方法来验证和解决端到端连接的连接问题。 默认情况下，这些连接在为域定义的每个 MA 内的域服务访问点（DSAP）之间 运行，并使用 ethernet cfm mep 命令手动配置。相反，MIP 是构成 DSAP 内所有可能路径的互连点。当此命令中的 *mip-creation* 选项设置为“default”或“explicit”时，由 CFM 协议自动生成 MIP，并调用 MIP 创建状态机（如 IEEE 802.1ag 中所定义）。 无论维护层次结构中的域级别如何，都要为 MA 内的所有互连点创建默认的可选 MIP（例如，客户，提供商或运营商）。 虽然显式选项仅在 MA 中生成 MIP，如果其关联域不在维护层次结构的底部。 此选项用于隐藏最低域级别的网络结构.CFM 提供的诊断功能可用于检测 MA 中任何一对 MEP 之间的连接故障。使用 MIP 可以将这些故障隔离到网络的较小部分。生成 MIP 的 CFM 使更多网络结构暴露给更高域级别的用户，但可以加速故障检测和恢复过程。 在设计 CFM 维护结构时应该考虑这种权衡。还要注意，虽然 MEP 是可以发起一致性检查消息（CCM）的活动代理，但是传输环回或链接跟踪消息，并维护本地 CCM 数据库。 另一方面，MIP 是被动代理，只能验证收到的 CFM 消息，并响应循环返回和链接跟踪消息 index index 命令定义的 MIP 创建方法优先于此命令定义的方法。

范例

此示例创建一个维护域设置为维护级别 3，并进入该域的 CFM 配置模式。

```
Console(config)#ethernet cfm domain index 1 name voip level 3 mip-creation
explicit
Console(config-ether-cfm)#
```

25.1.6 ethernet cfm enable

此命令在交换机上启用 CFM 处理。使用 no 形式全局禁用 CFM 处理。

语法

[no] ethernet cfm enable

缺省配置

禁用

命令模式

全局配置

命令用法

◆为了避免生成过多的 traps，应该在使用此命令全局启用 CFM 处理之前配置完整的 CFM 维护结构和进程参数。具体而言，应在每个参与的网桥上配置维护域，维护关联和 MAC。

◆启用 CFM 后，将为 CFM 处理分配硬件资源。

范例

此示例在交换机上全局启用 CFM。

```
Console(config)#ethernet cfm enable

Console(config)#
```

25.1.7 ma index name

此命令在当前维护域中创建维护关联（MA），将其映射到客户服务实例（S-VLAN），并设置为此服务实例创建 MIP 的方式。使用带有 **vlan** 关键字的 **no** 形式从指定的 MA 中删除 S-VLAN。 或者使用仅带有 **index** 关键字的 **no** 形式从当前域中删除 MA。

语法

ma index *index* **name** *ma-name* [**vlan** *vlan-id* [**mip-creation** *type*]]

no ma index *index* [**vlan** *vlan-id*]

index - MA 标识符。（范围：1-2147483647）

ma-name - MA 名字。（范围：1-43 个字母数字字符）

vlan-id - 服务 VLAN ID。（范围：1-4093）

type - 指定此 MA 中 CFM 协议的维护中间点（MIP）的创建方法：

default - 可以在 MA 的 VID 可以通过的任何网桥端口上为此 MA 创建 MIP。

显式 - MIP 只能在 MA 的 VID 可以通过的桥接端口上创建此 MA，并且只有在某个较低的 MA 级别创建维护点（MEP）时才能创建。

none - 无法为此 MA 创建 MIP。

缺省配置

10 秒

命令模式

CFM 域配置

命令用法

◆用于输入 CFM 域配置模式的维护域，此命令指定的 MA 名称和 VLAN 标识符，以及使用 mep

crosscheck mpid 命令配置的 DSAP 为每个客户创建唯一的服务实例。

◆如果仅为此命令输入 MA 索引名字，则 MA 将记录在域数据库中，但不起作用。在 MA 与服务 VLAN 关联之前，不能创建 MEP。

◆请注意同一维护级别的多个域（请参阅 ethern et cfm domain 命令）不能在同一 VLAN 上具有 MA。此外每个 MA 名称在 CFM 管理的网络中必须是唯一的。

◆在删除 MA 之前，首先删除为其配置的所有 MEP（参见 mep crosscheck mpid 命令）。

◆如果此命令未定义 MIP 创建方法，则 ethernet cfm domain 命令定义的创建方法将应用于此 MA。有关 MIP 类型的详细说明，请参阅 ethernet cfm domain 命令下的“命令用法”部分。

范例

此示例创建维护关联，将其绑定到 VLAN 1，并允许使用默认方法在此 MA 中创建 MIP。

```
Console(config)#ethernet cfm domain index 1 name voip level 3
Console(config-ether-cfm)#ma index 1 name rd vlan 1 mip-creation Default
Console(config-ether-cfm)#
```

25.1.8 ma index name-format

此命令指定基于 IEEE 802.1ag 字符的维护关联的名称格式，或 ITU-T SG13 / SG15 Y.1731 定义的基于 ICC 的格式。使用 no 形式恢复默认设置。

语法

ma index *index* **name-format** {**character-string** | **icc-based**}

no ma index *index* **name-format**

index -MA 标识符。 （范围：1-2147483647）

character-string -IEEE802.1ag 定义的字符串格式。这是 IETF RFC 2579 显示字符。

icc-based -ITU-T SG13 / SG15 Y.1731 定义了基于 ICC 的格式。

缺省配置

字符串

命令模式

CFM 域配置

范例

此示例将名称格式指定为字符串。

```
Console(config)#ethernet cfm domain index 1 name voip level 3
Console(config-ether-cfm)#ma index 1 name-format character-string
Console(config-ether-cfm)#
```

25.1.9 ethernet cfm mep

该命令将接口设置为域边界，将其定义为维护端点（MEP），并设置 MEP 关于接收和接收 CFM 消息的方向。使用 no 形式删除 MEP。

语法

ethernet cfm mep mpid *mpid* **md** *domain-name* **ma** *ma-name* [**up**]

no ethernet cfm mep mpid *mpid* **ma** *ma-name*

mpid - 维护终点标识符。（范围：1-8191）

domain-name - 域名。（范围：1-43 个字母数字字符）

ma-name - 维护关联名称。（范围：1-43 个字母数字字符）

up - 表示 MEP 朝向交换机交叉连接矩阵向内，并向内部网桥中继机制的方向发送 CFM 消息并从中接收。如果此命令中不包含 **up** 关键字，则 MEP 正在离开交换机，并向其发送 CFM 消息，并从物理介质的方向接收它们。

缺省配置

没有配置 MEP

MEP 面向外（向下）

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

◆必须按以下顺序配置 CFM 元素：(1) 与要配置的 MEP 处于同一级别的维护域（使用 ethernet cfm domain 命令），(2) 域内的维护关联（使用 ma index name 命令），以及 (3) 使用此命令最终使用 MEP。

◆接口可能属于多个域。此命令可用于将接口配置为不同域中不同 MA 的 MEP。

◆要更改 MEP 的 MA 或其面向的方向，请先删除 MEP，然后再创建一个新的。

范例

此示例将端口 1 设置为指定维护关联的 DSAP。

```
Console(config)#interface ethernet 1/1
Console(config-if)#ethernet cfm mep mpid 1 md voip ma rd
Console(config-if)#
```

25.1.10 ethernet cfm port-enable

此命令在接口上启用 CFM 处理。在接口上使用 no 形式禁用 CFM 处理。

语法

[no] ethernet cfm port-enable

缺省配置

启用

命令模式

接口配置 (Ethernet, Port Channel)

命令用法

◆必须先启用接口，然后才能使用 ethernet cfm mep 命令创建 MEP 。

◆ 如果在使用 ethernet cfm mep 命令的接口上配置了 MEP 则必须首先将其删除，然后才能在该接口上禁用 CFM。

◆当 CFM 被启用时，先前用于该接口上的 CFM 处理的硬件资源被释放，并且进入该接口的所有 CFM 帧将作为正常数据流量转发。

范例

此示例在端口 1 上启用 CFM。

```
Console(config)#interface ethernet 1/1
Console(config-if)#ethernet cfm port-enable
Console(config-if)#
```

25.1.11 clear ethernet cfm ais mpid

该命令清除指定 MEP 的 AIS 缺陷信息。

语法

clear ethernet cfm ais mpid *mpid* **md** *domain-name* **ma** *ma-name*

mpid - 维护终点标识符。（范围：1-8191）

domain-name - 域名。(范围：1-43 个字母数字字符)

ma-name - 维护关联名称。(范围：1-43 个字母数字字符)

缺省配置

无

命令模式

特权模式

命令用法

如果在解决所有错误时 MEP 确实记录了 AIS 状态，则此命令可用于清除 AIS 缺陷条目。

范例

此示例清除端口 1 上的 AIS 缺陷条目。

```
Console#clear ethernet cfm ais mpid 1 md voip ma rd

Console(config)#
```

25.1.12 show ethernet cfm configuration

此命令显示 CFM 配置设置，包括全局设置，SNMP 陷阱和接口设置。

语法

show ethernet cfm configuration {**global** | **traps** |**interface** *interface*}

global - 显示全局设置，包括 CFM 全局状态，交叉检查启动延迟和链接跟踪参数。

traps - 显示所有连续性检查和交叉检查陷阱的状态。

interface - 显示指定接口的 CFM 状态。

ethernet *unit/port*

unit -单位标识符。 (范围：1)

port -端口号。 (范围：1-28)

port-channel *channel-id* (范围：1-12)

缺省配置

无

命令模式

特权模式

范例

此示例显示 CFM 的全局设置。

```
Console#show ethernet cfm configuration global

CFM Global Status : Enabled

Crosscheck Start Delay : 10 seconds

Linktrace Cache Status : Enabled

Linktrace Cache Hold Time : 100 minutes

Linktrace Cache Size : 100 entries

Console#
```

25.1.13 show ethernet cfm md

此命令显示已配置的维护域。

语法

show ethernet cfm md [**level** *level*]

level - Maintenance level. (Range: 0-7)

缺省配置

无

命令模式

特权模式

范例

此示例显示所有已配置的维护域。

```
Console#show ethernet cfm md

MD Index MD Name Level MIP Creation Archive Hold Time (m.)

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

1 rd 0 default 100

Console#
```

25.1.14 show ethernet cfm ma

此命令显示已配置的维护关联。

语法

show ethernet cfm ma [**level** *level*]

level -维护级别。(范围：0-7)

缺省配置

无

命令模式

特权模式

命令用法

有关 CC Interval 字段中显示的值的说明，请参阅 ethernet cfm cc ma interval 命令。

范例

此示例显示所有已配置的维护关联。

```
Console#show ethernet cfm ma

MD Name MA Index MA Name Primary VID CC Interval MIP Creation

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

steve 1 voip 1 4 default

Console#
```

25.1.15 show ethernet cfm maintenance-pointslocal

此命令显示在此设备上配置的维护点。

语法

show ethernet cfm maintenance-points local{**mep** [**domain** *domain-name* | **interface** *interface* |**level** *level-id*] | **mip** [**domain** *domain-name* | **level** *level-id*]}

mep - 仅显示本地维护端点。

mip - 仅显示本地维护中间点。

domain-name - 域名。(范围：1-43 个字母数字字符)

interface - 显示指定接口的 CFM 状态。

ethernet *unit/port*

unit -单位标识符。(范围：1)

port -端口号。(范围：1- 28)

port-channel *channel-id*（范围：1-12）

level-id - 此域的维护级别。（范围：0-7）

缺省配置

无

命令模式

特权模式

命令用法

◆使用带有此命令的**mep**关键字通过ethernet cfm mep命令将此设备上配置的**MEP**显示为DSAP。

◆当mip-creationmethod通过ethernet cfmdomain命令或ma index name命令设置为“default”或“explicit”时，使用带有此命令的**mip**关键字显示CFM协议在此设备上生成的MIP。

范例

此示例显示在此设备上为主域rd配置的所有MEP。

```
Console#show ethernet cfm maintenance-points local mep

MPID MD Name Level Direct VLAN Port CC Status MAC Address

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

1 rd 0 UP 1 Eth 1/ 1 Enabled 00-12-CF-3A-A8-C0

Console#
```

25.1.16 show ethernet cfm maintenance-pointslocal detail mep

此命令显示有关连续性检查数据库中本地MEP的详细CFM信息。

语法

show ethernet cfm maintenance-points local detail mep[**domain** *domain-name* | **interface** *interface* | **level** *level-id*]

domain-name - 域名。（范围：1-43个字母数字字符）

interface - 显示指定接口的CFM状态。

ethernet *unit/port*

unit -单位标识符。（范围：1）

port -端口号。（范围：1-28）

port-channel *channel-id*（范围：1-12）

level-id －此域的维护级别。（范围：0-7）

缺省配置

无

命令模式

特权模式

范例

此示例显示有关端口 1 上的本地 MEP 的详细信息。

```
Console#show ethernet cfm maintenance-points local detail mep interface

ethernet 1/1

MEP Settings:

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

MPID : 1

MD Name : vopu

MA Name : r&d

MA Name Format : Character String

Level : 0

Direction : Up

Interface : Eth 1/ 1

CC Status : Enabled

MAC Address : 00-E0-0C-00-00-FD

Defect Condition : No Defect

Received RDI : False

AIS Status : Enabled

AIS Period : 1 seconds

AIS Transmit Level : default

Suppress Alarm : Disabled

Suppressing Alarms : Disabled

Console#
```

25.1.17 show ethernet cfm maintenance-pointsremote detail

此命令显示有关连续性检查数据库中远程 MEP 的详细 CFM 信息。

语法

show ethernet cfm maintenance-points remote detail {**mac** *mac-address* | **mpid** *mpid*} [**domain** *domain-name* | **level** *level-id* | **ma** *ma-name*]

mac-address - 远程维护点的 MAC 地址。此地址可以采用以下任一格式输入：xxxx-xx-xx-xx-xx-xx 或 xxxxxxxxxxxx

mpid - 维护终点标识符。（范围：1-8191）

domain-name - 域名。（范围：1-43 个字母数字字符）

level-id - 此域的授权维护级别。（范围：0-7）

ma-name - 维护关联名称。（范围：1-43 字母数字字符）

缺省配置

无

命令模式

特权模式

命令用法

将 **mpid** 关键字与此命令一起使用可显示有关特定维护点的信息，或使用 **mac** 关键字显示有关具有指定 MAC 地址的所有维护点的信息。

范例

此示例显示有关 MPID 2 指定的远程 MEP 的详细信息 。

```
Console#show ethernet cfm maintenance-points remote detail mpid 2

MAC Address : 00-0D-54-FC-A2-73

Domain/Level : voip / 3

MA Name : rd

Primary VLAN : 1

MPID : 2

Incoming Port : Eth 1/ 2

CC Lifetime : 645 seconds

Age of Last CC Message : 2 seconds

Frame Loss : 137

CC Packet Statistics : 647/1
```

```
Port State : Up

Interface State : Up

Crosscheck Status : Enabled

Console#
```

25.2 连续性检查操作

25.2.1 ethernet cfm cc mainterval

此命令设置连续性检查消息（CCM）之间的传输延迟。使用 no 形式恢复默认设置。

语法

ethernet cfm cc md *domain-name* **ma** *ma-name***interval** *interval-level*

no ethernet cfm cc ma *ma-name* **interval**

domain-name - 域名。（范围：1-43 个字母数字字符）

ma-name - 维护关联名称。（范围：1-43 个字母数字字符）

interval-level - 连接检查消息之间的传输延迟。此参数的设置表示为 4 到 7 级，后者又映射到特定的时间间隔。（CCM 寿命字段选项：4 - 100 ms，5 - 1 秒，6 - 10 秒，7 - 60 秒 ）。

缺省配置

4 (100 ms)

命令模式

全局配置

命令用法

◆CCM 提供了发现其他 MEP 并检测 MA 中的连接故障的方法。如果任何 MEP 未能从其 MA 中的任何其他 MEP 接收到三个连续的 CCM，则会注册连接故障。发布 CCM 的时间间隔应根据 MA 的性质和规模进行配置，以便及时发现连接问题。

◆MIP 维护 MIP CCM 数据库对于承载大量服务实例的网桥来说存在困难，并且因为哪些 MEP 以高频率发布 CCM。因此，可能必须使用较慢的 CCM 传输速率。

范例

此示例设置连续性检查消息 7（60 秒）的传输延迟。

```
Console(config)#ethernet cfm cc md voip ma rd interval 7
Console(config)#
```

25.2.2 ethernet cfm cc enable

此命令用于在指定的维护关联中传输连续性检查消息（CCM）。使用 no 形式可以传输这些消息。

语法

[no] **ethernet cfm cc enable md** *domain-name* **ma** *ma-name*

domain-name - 域名。（范围：1-43 个字母数字字符）

ma-name - 维护关联名称。（范围：1-43 个字母数字字符）

缺省配置

禁用

命令模式

全局配置

命令用法

◆CCM 定期通过 MEP 进行组播，以发现同一 MA 中的其他 MEP，并确保连接 MA 中的所有其他 MEP / MIP。

◆检查收到的每个 CCM 以验证在消息中发送的 MEP 标识符字段与其自己的 MEPID 不匹配 ，这表示 重复的 MEP 或网络循环。如果未找到这些错误类型，则 CCM 将存储在 MEP 的本地数据库中，直到老化。

◆如果维护点无法从同一 M A 中的任何其他 MEP 接收三个连续 CCM ，则会注册连接故障。

◆如果维护点收到的 CCM 具有无效的 MEPID 或 MAlevel 或 MA 级别低于其自身，则会注册失败，表示配置错误或交叉连接错误（即重叠 MA）。

范例

此示例为指定的维护关联启用连续性检查消息。

```
Console(config)#ethernet cfm cc enable md voip ma rd
Console(config)#
```

25.2.3 snmp-server enable traps ethernet cfm cc

此命令为 CFM 连续性检查事件启用 SNMP 陷阱。使用 no 形式禁用这些陷阱。

语法

[no] snmp-server enable traps ethernet cfm cc [config | loop |mep-down | mep-up]

config -如果此设备收到的 CCM 具有与其自身相同但具有不同源 MAC 地址的 CCM,则发送陷阱，指示存在 CFM 配置错误。

loop - 如果此设备接收到具有相同源 MAC 地址和 MPID 的 CCM，则发送陷阱，表示存在转发循环。

mep-down - 如果此设备与 ismote MEP 失去连接，或者连接已恢复到已从错误状态恢复的远程 MEP，则发送陷阱。

mep-up - 如果发现远程 MEP 并将其添加到本地数据库，先前发现的远程 MEP 的端口状态发生更改，或者从远程 MEP 接收 CCM（作为存档数据库中的过期条目），则发送陷阱。

缺省配置

所有连续性检查均已启用。

命令模式

全局配置

命令用法

当启用 MEP 的交叉检查时，所有 mep-up 陷阱都被抑制，因为交叉检查陷阱包括更详细的状态信息。

范例

此示例为 mep-up 事件启用 SNMP 陷阱。

```
Console(config)#snmp-server enable traps ethernet cfm cc mep-up

Console(config)#
```

25.2.4 mep archive-hold-time

此命令设置在清除之前，来自缺失 MEP 的数据在连续性检查消息（CCM）数据库中保留的时间。使用 no 形式恢复默认设置。

语法

mep archive-hold-time *hold-time*

hold-time -保留缺少的 MEP 数据的时间。（范围：1-65535 分钟）

缺省配置

100 分钟

命令模式

CFM 域配置

命令用法

保留时间的更改仅适用于输入此命令后存储在数据库中的条目。

范例

此示例将 CCM 数据库中缺少的 MEP 的老化时间设置为 30 分钟。

```
Console(config)#ethernet cfm domain index 1 name voip level 3
Console(config-ether-cfm)#mep archive-hold-time 30
Console(config-ether-cfm)#
```

25.2.5 clear ethernet cfm maintenance-points remote

此命令清除连续性检查数据库的内容。

语法

clear ethernet cfm maintenance-points remote[**domain** *domain-name* | **level** *level-id*]

domain-name - 域名。（范围：1-43 个字母数字字符）

level-id - 维护级别。（范围：0-7）

缺省配置

无

命令模式

特权模式

命令用法

使用此命令不带任何关键字清除 CCM 数据库中的所有条目。使用 **domain** 关键字清除特定域的 CCM 数据库，或使用 **level** 关键字清除特定维护级别的 CCM 数据库 。

范例

```
Console#clear ethernet cfm maintenance-points remote domain voip

Console#
```

25.2.6 clear ethernet cfm errors

此命令清除为指定的维护域或维护级别记录的连续性检查错误。

语法

clear ethernet cfm errors [**domain** *domain-name* | **level** *level-id*]

domain-name - 域名。(范围：1-43 个字母数字字符)

level-id - 维护级别。(范围：0-7)

缺省配置

无

命令模式

特权模式

命令用法

使用不带任何关键字的此命令可清除错误数据库中的所有条目。使用 **domain** 关键字清除特定域的错误数据库，或使用 **level** 关键字清除特定维护级别的错误数据库 。

范例

```
Console#clear ethernet cfm errors domain voip

Console#
```

25.2.7 show ethernet cfm errors

此命令显示此设备上记录的 CFM 连续性检查错误。

语法

show ethernet cfm errors [**domain** *domain-name* | **level** *level-id*]

domain-name - 域名。(范围：1-43 个字母数字字符)

level-id - 此域的授权维护级别。(范围：0-7)

缺省配置

无

命令模式

特权模式

范例

```
Console#show ethernet cfm errors

Level VLAN MPID Interface Remote MAC Reason MA Name

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

5 2 40 Eth 1/1 ab.2f.9c.00.05.01 LEAK provider_1_2

Console#
```

25.3 交叉检查操作

25.3.1 ethernet cfm mepcrosscheck start-delay

此命令设置设备在开始交叉检查操作之前等待远程 MEPs 出现的最大延迟。使用 no 形式恢复默认设置。

语法

ethernet cfm mep crosscheck start-delay *delay*

delay - 设备在开始交叉检查之前等待远程 MEP 出现的时间。（范围：1-65535 秒）

缺省配置

30 秒

命令模式

全局配置

命令用法

◆此命令设置设备等待远程 MEP 带来的延迟，并开始交叉检查本地维护域中静态配置远程 MEP 列表与通过 CCM 学习的 MEP。

◆交叉检查状态延迟应配置为大于或等于连续性检查消息间隔的值，以避免不必要的陷阱。

范例

此示例设置启动交叉检查进程之前的最大延迟。

```
Console(config)#ethernet cfm mep crosscheck start-delay 60
Console(config)#
```

25.3.2 snmp-server enable traps ethernet cfm crosscheck

此命令为 CFM 连续性检查事件启用 SNMP 陷阱，与静态配置的 MEP 之间的交叉检查操作以及通过连续性检查消息（CCM）学习的交叉检查操作相关。使用 no 形式禁用这些陷阱。

语法

[no] snmp-server enable traps ethernet cfm crosscheck [ma-up | mep-missing | mep-unknown]

ma-up - 当 MA 中的所有远程 MEP 出现时发送陷阱。

mep-missing - 如果交叉检查计时器到期并且未从静态列表中配置的远程 MEP 接收到 CCM，则发送陷阱。

mep-unknown - 如果出现未配置的 MEP，则发送陷阱。

缺省配置

所有连续性检查均已启用。

命令模式

全局配置

命令用法

◆要使此陷阱类型起作用，必须使用 ethernet cfm mepcrosscheck 命令在所需的维护关联上启用交叉检查 。

◆如果启用了交叉检查（使用 ethernet cfm mep cro sscheck 命令），则会发送 mep-missing 陷阱，并且没有收到静态列表中配置的远程 MEP 的 CCM（使用 mep crosscheck mpid 命令）。

◆如果启用了交叉检查，则会发 mep-unknown 陷阱，并且从未在状态列表中配置的远程 MEP 接收 CCM 。

◆如果启用了交叉检查，则会发送 ma-up 陷阱，并且会从静态列表中为此维护关联配置的所有远程 MEP 接收 CCM。

范例

此示例为检测到的 mep-unknown 事件启用 SNMP 陷阱交叉检查操作。

```
Console(config)#snmp-server enable traps ethernet cfm crosscheck mep-unknown
Console(config)#
```

25.3.3 mep crosscheck mpid

此命令在维护关联中静态定义远程 MEP。使用 **no** 形式删除远程 MEP。

语法

[no] **mep crosscheck mpid** *mpid* **ma** *ma-name*

mpid -维护端点的标识符,该端点存在于同一 MA 内的另一个支持 CFM 的设备上。(范围:1-8191)

ma-name -维护关联名称。(范围: 1-43 个字母数字字符)

缺省配置

没有配置远程 MEP。

命令模式

CFM 域配置

命令用法

◆使用此命令静态配置维护关联中存在的远程MEP。这些远程MEP用于交叉检查操作,以验证 指定 MA 中的所有端点是否可操作。

◆如果已使用 ethernet cfm mep 命令在相同的维护级别和相同的 MA 中创建了域服务访问点(DSAP),则只能使用此命令配置远程 MEP。DSAP 是 存在于域边缘的 MEP,并且作为端到端交叉检查,环回和链路跟踪功能的主要服务访问点。

范例

此示例为指定的维护关联定义静态 MEP。

```
Console(config)#ethernet cfm domain index 1 name voip level 3
Console(config-ether-cfm)#ma index 1 name rd vlan 1
Console(config-ether-cfm)#mep crosscheck mpid 2 ma rd
Console(config-ether-cfm)#
```

25.3.4 ethernet cfm mep crosscheck

此命令可以在分配给同一维护关联中的其他设备的 MEP 的静态列表与通过连续性检查消息(CCM)学习的 MEP 之间进行交叉检查。使用 **disable** 关键字可以停止交叉检查过程。

语法

ethernet cfm mep crosscheck {**enable** | **disable**}**md** *domain-name* **ma** *ma-name*

enable - 启动交叉检查过程。

disable - 停止交叉检查过程。

domain-name - 域名。（范围：1-43 个字母数字字符）

ma-name - MA 名字。（范围：1-43 个字母数字字符）

缺省配置

禁用

命令模式

特权模式

命令用法

◆在使用此命令启动交叉检查过程之前，首先使用 mep crosscheck mpid 命令配置维护关联内其他设备上存在的远程 MEP。这些远程 MEP 用于交叉操作以验证所有端点。指定的 MA 是可操作的。

◆默认情况下禁用交叉检查过程，必须使用此命令并使用 **enable** 关键字手动启动。

范例

此示例允许在规定的维护关联中进行交叉检查。

```
Console#ethernet cfm mep crosscheck enable md voip ma rd

Console#
```

25.3.5 show ethernet cfm maintenance-points remote crosscheck

此命令显示有关在交叉检查列表中静态配置的远程 MEP 的信息。

语法

show ethernet cfm maintenance-points remote crosscheck[**domain** *domain-name* | **mpid** *mpid*]

domain-name - 域名。（范围：1-43 个字母数字字符）

mpid - 维护终点标识符。（范围：1-8191）

缺省配置

无

命令模式

特权模式

范例

此示例显示在此设备上静态配置的所有远程 MEP。

```
Console#show ethernet cfm maintenance-points remote crosscheck
```

```
MPID MA Name Level VLAN MEP Up Remote MAC
---- -------------------- ----- ---- ------ -----------------
2 downtown 4 2 Yes 00-0D-54-FC-A2-73
Console#
```

25.4 链接跟踪操作

25.4.1 ethernet cfm linktrace cache

此命令可以缓存通过链接跟踪消息学习的 CFM 数据。使用 no 形式禁用缓存。

语法

[no] ethernet cfm linktrace cache

缺省配置

启用

命令模式

全局配置

命令用法

◆链路跟踪消息是由 MEP 发起的组播 CFM 帧，并且从 MIP 转发到 MIP，每个 MIP 生成链路跟踪应答，直到链路跟踪消息到达其目的地的点不能再被转发。

◆使用此命令启用链接跟踪高速缓存以存储在此设备上启动的链接跟踪操作的结果。使用 ethernet cfmlinktrace 命令传输链接跟踪消息。

◆链路跟踪响应从每个 MIP 沿路径和目标 MEP 返回。存储在缓存中的信息包括维护域名，MA 名称，MEPID，序列号和 TTL 值。

范例

此示例启用链接跟踪缓存。

```
Console(config)#ethernet cfm linktrace cache
Console(config)#
```

25.4.2 ethernet cfm linktrace cache hold-time

此命令设置 CFM 链接跟踪高速缓存条目的保持时间。使用 no 形式恢复默认设置。

语法

ethernet cfm linktrace cache hold-time *minutes*

minutes -存储在链接跟踪缓存中的条目的老化时间。（范围：1-65535 分钟）

缺省配置

100 分钟

命令模式

全局配置

命令用法

在设置缓存条目的老化时间之前，必须首先使用 ethernet cfm linktrace cache 命令启用缓存 。

范例

此示例将链接跟踪高速缓存中的条目的老化时间设置为 60 分钟。

```
Console(config)#ethernet cfm linktrace cache hold-time 60
Console(config)#
```

25.4.3 ethernet cfm linktrace cache size

此命令设置链接跟踪高速缓存的最大大小。使用 no 形式恢复默认设置。

语法

ethernet cfm linktrace cache size *entries*

entries -链接跟踪缓存中存储的链接跟踪响应数。（范围：1-4095 条目）

缺省配置

100 条目

命令模式

全局配置

命令用法

◆在设置高速缓存大小之前，必须首先使用 ethernet cfm linktrace cache 命令启用高速缓存 。

◆如果高速缓存达到指定条目的最大数量，或者将大小设置为小于当前存储条目数的值，则不添

加任何条目。要添加其他条目，必须首先使用此命令增加高速缓存大小，或使用 clear Ethernet cfm linktrace-cache 命令清除高速缓存大小 。

范例

此示例将链接跟踪高速缓存的最大大小限制为 500 个条目。

```
Console(config)#ethernet cfm linktrace cache size 500
Console(config)#
```

25.4.4 ethernet cfm linktrace

此命令将 CFM 链路跟踪消息发送到远端 MEP 的 MAC 地址。

语法

ethernet cfm linktrace {**dest-mep** *destination-mpid* | **src-mep***source-mpid* {**dest-mep** *destination-mpid* | *mac-address*} |*mac-address*} **md** *domain-name* **ma** *ma-name* [**ttl** *number*]

destination - *mpid* - 作为链接跟踪消息 *目标* 的远程 MEP 的标识符。(范围:1-8191)

source - *mpid* - 将发送 linktrace 消息的源 MEP 的标识符。(范围：1-8191)

mac-address - 作为链路跟踪消息目标的远程 MEP 的 MAC 地址。可以使用以下任一格式输入此地址：xx-xx-xx-xx-xx-xx 或 xxxxxxxxxxxx

domain-name - 域名。(范围：1-43 个字母数字字符)

ma-name - 维护关联名称。(范围：1-43 个字母数字字符)

number - linktrace 消息的生存时间。(范围：1-255hops)

缺省配置

无

命令模式

特权模式

命令用法

◆链接跟踪消息可以针对 MEP，而不是 MIPS。在发送链接跟踪消息之前，请确保已为指定的 MA 配置目标 MEP。

◆如果目标 MEP 的 MAC 地址没有被任何本地 MEP 学习,则链路跟踪可能失败。使用 show ethernet cfmmaintenance-points remote crosscheck 命令远程交叉检查命令来验证目标 MEP 的 MAC 地址已被学习。

◆链路跟踪消息(LTM)作为组播 CFM 帧发送，并且从 MIP 转发到 MIP，每个 MIP 生成链路跟踪应答，直到 LTM 到达其目的地或者不再能够被转发。

◆链接跟踪消息用于隔离故障。然而，这个任务在以太网环境中是困难的，因为每个节点通过多点链路连接。故障隔离更具挑战性，因为目标节点的 MAC 地址可能在几分钟内老化。这可能导致跟踪路径随时间变化，或者如果故障导致目标 MEP 与 MA 中的其他 MEP 隔离，则连接性丢失。

◆当使用命令行或 Web 接口时，CFM 协议选择发送链接跟踪消息的源 MEP usedby，但是当使用 SNMP 时，用户可以指定源 MEP。

范例

此示例将链接跟踪消息发送到指定的 MEP，其最大跳数为 25。

```
Console#linktrace ethernet dest-mep 2 md voip ma rd ttl 25

Console#
```

25.4.5 clear ethernet cfm linktrace-cache

此命令清除此设备上记录的链接跟踪消息。

命令模式

特权模式

范例

```
Console#clear ethernet cfm linktrace-cache

Console#
```

25.4.6 show ethernet cfm linktrace-cache

此命令显示链接跟踪缓存的内容。

命令模式

特权模式

范例

```
Console#show ethernet cfm linktrace-cache

Hops MA IP / Alias Ingress MAC Ing. Action Relay

Forwarded Egress MAC Egr. Action

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

2 rd 192.168.0.6 00-12-CF-12-12-2D ingOk Hit

Not Forwarded

Console#

25.5 环回操作

25.5.1 ethernet cfm loopback

此命令将 CFM 环回消息发送到 MEPor MIP 的 MAC 地址。

语法

ethernet cfm loopback{**dest-mep** *destination-mpid* | **src-mep***source-mpid* {**dest-mep** *destination-mpid* | *mac-address*} |*mac-address*} **md** *domain-name* **ma** *ma-name*[**count** *transmit-count*] [**size** *packet-size*]

destination - mpid - 作为回放消息的目标的 MEP 的标识符。 （范围：1-8191）

source - mpid - 将发送回传消息的源 MEP 的标识符。 （范围：1-8191）

mac-address - 作为环回消息目标的远程维护点的 MAC 地址。 可以使用以下任一格式输入此地址：xx-xx-xx-xx-xx-xx 或 xxxxxxxxxxxx

domain-name - 域名。（范围：1-43 个字母数字字符）

ma-name - 维护关联名称。（范围：1-43 个字母数字字符）

transmit-count - 回送消息所在的次数。（范围：1-1024）

packet-size - 环回消息的大小。（范围：64-1518bytes）

缺省配置

环回计数：发送一个环回消息。

环回大小：64 字节

命令模式

特权模式

命令用法

◆使用此命令测试维护点之间的连接。如果连续性检查数据库没有指定维护点的条目，则将显示错误消息。

◆传输环回消息的点（即 DSAP）和该命令中指定的目标维护点必须在同一 MA 内。

◆自动检测故障或接收其他一些错误报告后，回送消息可用于故障验证和隔离。环回消息还可用于确认成功恢复或启动连接。接收维护点应该通过环回应答来响应环回消息。

◆使用命令行或 Web 接口时，CFM 协议选择用于发送环回消息的源 MEP。但是使用 SNMP 时，用户

可以指定源 MEP。

范例

此示例将 loopback 消息发送到指定的远程 MEP。

```
Console#ethernet cfm loopback dest-mep 1 md voip ma rd

Console#
```

25.6 故障发生器操作

25.6.1 mep fault-notifyalarm-time

此命令设置在发出故障警报之前缺陷必须存在的时间。使用 no 形式恢复默认设置。

语法

mep fault-notify alarm-time *alarm-time*

no fault-notify alarm-time

alarm-time -在产生故障警报之前必须存在一个或多个缺陷的时间。（范围：3-10 秒）

缺省配置

3 秒

命令模式

CFM 域配置

命令用法

当 MEP 故障通知生成器状态机检测到该命令配置的时间段已超出指示的一个或多个缺陷，并且启用故障报警或高于 mep fault-notify 最低优先级命令设置的优先级时，将发出故障报警 。

范例

此示例设置生成故障警报之前的延迟时间。

```
Console(config)#ethernet cfm domain index 1 name voip level 3

Console(config-ether-cfm)#mep fault-notify alarm-time 10

Console(config-ether-cfm)#
```

25.6.2 mep fault-notify lowest-priority

此命令设置允许生成远程警报的最低优先级缺陷。使用 no 形式恢复默认设置。

语法

mep fault-notify lowest-priority *priority*

no fault-notify lowest-priority

priority -允许生成故障警报的最低优先级缺省值。（范围：1-6）

缺省配置

优先级 2

命令模式

CFM 域配置

命令用法

◆故障警报可以生成 SNMP 通知。当 MIC 故障通知生成器状态机检测到配置的时间段（参见 mep fault-notify alarm-time 命令）已经过了指示的一个或多个缺陷，并且在此命令设置的优先级下启用故障报警时发出。在通过配置的时间段重置状态机之前，状态机不再发送故障报警（请参阅 mep fault-notify reset-time 命令）

没有缺陷指示。接收到警报后的正常程序是使用适当的SNMP软件工具检查报告的MEP管理对象，诊断故障，纠正故障，重新检查 MEP 的管理对象，以查看 MEP 故障通知生成器状态机是否已重置，并重复直到故障解决为止。

◆在故障报警中仅报告当前检测到的最高优先级缺陷 。

范例

此示例设置将生成故障报警的最低优先级缺陷。

```
Console(config)#ethernet cfm domain index 1 name voip level 3
Console(config-ether-cfm)#mep fault-notify lowest-priority 1
Console(config-ether-cfm)#
```

25.6.3 mep fault-notify reset-time

该命令用于配置发出故障报警后的时间，并且在发出另一个故障报警之前不存在缺陷。使用 no 形式恢复默认设置。

语法

mep fault-notify reset-time *reset-time*

no fault-notify reset-time

reset-time -在生成另一个故障报警之前必须经过的时间，没有任何进一步的缺陷。(范围：3-10秒)

缺省配置

10 秒

命令模式

CFM 域配置

范例

此示例设置重置时间，之后可以生成另一个故障警报。

```
Console(config)#ethernet cfm domain index 1 name voip level 3
Console(config-ether-cfm)#mep fault-notify reset-time 7
Console(config-ether-cfm)#
```

25.6.4 show ethernet cfm fault-notify-generator

此命令显示故障通知生成器的配置设置。

语法

show ethernet cfm fault-notify-generator mep *mpid*

mpid -维护终点标识符。(范围：1-8191)

缺省配置

无

命令模式

特权模式

范例

此示例显示为一个 MEP 配置的故障通知设置。

```
Console#show ethernet cfm fault-notify-generator mep 1
MD Name MA Name Highest Defect Lowest Alarm Alarm Time Reset Time
---------- ---------- ---------- ---------- ---------- ----------
```

voip rd 无 macRemErrXcon 3sec. 10sec.

Console#

25.7 延迟测量操作

25.7.1 ethernet cfm delay-measure two-way

此命令将定期延迟测量请求发送到维护关联中的指定 MEP。

语法

ethernet cfm delay-measure two-way [**src-mep** *source-mpid*]{**dest-mep** *destination-mpid* | *mac-address*} **md** *domain-name***ma** *ma-name* [**count** *transmit-count*] [**interval** *interval*][**size** *packet-size*] [**timeout** *timeout*]

source - mpid - 将发送延迟测量消息的源 MEP 的标识符。 （范围：1-8191）

destination - mpid - 作为延迟测量消息的 *目标* 的远程 MEP 的标识符。 （范围：1-8191）

mac-address - 作为延迟测量消息的目标的远程 MEP 的 MAC 地址。 可以使用以下格式输入此地址：xx-xx-xx-xx-xx-xx 或 xxxxxxxxxxxx

domain-name - 域名。（范围：1-43 个字母数字字符）

ma-name - 维护关联名称。（范围：1-43 个字母数字字符）

count - 如果在指定的超时之前收到 noresponse，则重试发送消息的次数。（范围：1-5）

interval - 延迟测量消息之间的传输延迟。（范围：1-5 秒）

packet-size - 延迟测量消息的大小。（范围：64-1518 字节）

timeout - 等待响应的超时。（范围：1-5 秒）

缺省配置

数：5

间隔：1 秒

大小：64 字节

超时：5 秒

命令模式

特权模式

命令用法

◆延迟测量可用于测量 MEP 之间的帧延迟和帧延迟变化。

◆必须先为同一 MA 配置本地 MEP，然后才能使用此命令。

◆如果启用 MEP 以生成具有延迟测量（DM）信息的帧，则它会周期性地将 DM 帧发送到同一 MA 中的对等 MEP，并期望从其接收 DM 帧。

◆帧延迟测量只能用于双向测量，其中 MEP 使用 TxTimeStampf（ 发送具有 DM 请求信息的帧时的时间戳）发送具有 DM 请求信息的帧，并且接收 MEP 响应具有 DM 回复信息的帧。从 DM 请求信息复制 TxTimeStampf，RxTimeStampf（时间戳时间）

接收具有 DM 请求信息的帧）和 TxTimeStampb（在发送具有 DM 应答信息的帧时的时间戳）：

帧延迟=（RxTimeStampb-TxTimeStampf） - （TxTimeStampbRxTimeStampf）

◆MEP 还可以根据其计算两个后续双向帧延迟测量之间差异的能力进行双向帧延迟变化测量。

范例

此示例将定期延迟测量请求发送到远程 MEP。

```
Console#ethernet cfm delay-measure two-way dest-mep 1 md voip ma rd

Type ESC to abort.

Sending 5 Ethernet CFM delay measurement message, timeout is 5 sec.

Sequence Delay Time (ms.) Delay Variation (ms.)

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

1 < 10 0

2 < 10 0

3 < 10 0

4 40 40

5 < 10 40

Success rate is 100% (5/5), delay time min/avg/max=0/8/40 ms.

Average frame delay variation is 16 ms.

Console#
```

26 OAM 命令

交换机提供 OAM 远程管理工具，监控和维护 CPEs（客户端设备）的链路。本节介绍的功能包括为选定端口启用 OAM，环回测试以及显示设备信息。

26.1.1 efm oam

此命令在指定端口上启用 OAM 功能。使用 no 形式禁用此功能。

语法

[no] efm oam

缺省配置

禁用

命令模式

接口配置

命令用法

◆如果远程设备也支持 OAM，则交换 InformationOAMPDU 以建立 OAM 链路。

◆并非所有 CPE 都支持 OAM 功能，因此默认情况下禁用 OAM。如果连接到端口的 CPE 支持 OAM，则必须首先通过 efm oam 命令启用此功能，以获取对其他远程配置功能的访问权限。

范例

```
Console(config)#interface ethernet 1/1
Console(config-if)#efm oam
Console(config-if)#
```

26.1.2 efm oam critical-link-event

此命令可以报告 critical-event 事件或 dying-gasp 事件。使用 no 形式禁用此功能。

语法

[no] efm oam critical-link-event {critical-event | dying-gasp}

critical-event -如果发生严重事件,本地 OAM 实体(thisswitch)通过在要发送的下一个 OAMPDU 中设置适当的标志并将此信息存储在其 OAMevent 日志中，向其对等体指示此情况。

dying-gasp -如果发生不可恢复的情况，本地 OAMentity 会立即发送 trap 消息来指示此情况。

缺省配置

启用

命令模式

接口配置

命令用法

◆critical-event 是特定于供应商的，可能包括各种故障，例如异常电压波动，检测到超出范围的温度，风扇故障，闪存中的 CRC 错误，内存不足或其他硬件故障。

◆dying-gasp 是由不可恢复的故障引起的，例如电源故障或设备复位。

注释: 当系统电源故障时，交换机将总是在断电之前发送一个陷阱消息。

范例

```
Console(config)#interface ethernet 1/1

Console(config-if)#efm oam critical-link-event dying-gasp

Console(config-if)#
```

26.1.3 efm oam link-monitor frame

此命令可以报告错误的帧链接事件。使用 no 形式禁用此功能。

语法

[no] efm oam link-monitor frame

缺省配置

启用

命令模式

接口配置

命令用法

◆错误帧是一个错误导致一个或多个位的帧。

◆如果启用此功能并发生错误帧链接事件，则本地 OAM 实体（此设备）将发送事件通知 OAMPDU。

范例

```
Console(config)#interface ethernet 1/1

Console(config-if)#efm oam link-monitor frame

Console(config-if)#
```

26.1.4 efm oam link-monitor framethreshold

此命令设置错误帧链接事件的阈值。使用 no 形式恢复默认设置。

语法

[no] **efm oam link-monitor frame threshold** *count*

count -错误帧链接事件的阈值。（范围：1-65535）

缺省配置

1

命令模式

接口配置

命令用法

如果启用此功能，则在 efmoam link-monitor frame window 命令指定的时间内达到或超过阈值时，将发送事件通知消息。错误帧事件 TLV 包括在指定时段内检测到的错误帧数。

范例

```
Console(config)#interface ethernet 1/1

Console(config-if)#efm oam link-monitor frame threshold 5

Console(config-if)#
```

26.1.5 efm oam link-monitor framewindow

此命令设置错误帧链接事件的监视周期。使用 no 形式恢复默认设置。

语法

[no] **efm oam link-monitor frame window** *size*

size -检查错误帧链接事件的报告阈值的时间段。（范围：10-65535 单位 10 毫秒）

缺省配置

10（100 毫秒的单位）= 1 秒

命令模式

接口配置

命令用法

如果启用此功能，如果在此 命令指定的时间内达到或超过 efm oam link-monitor frame threshold 命令指定的阈值，则会发送事件通知消息。错误帧事件 TLV 包括在指定时间段内检测到的错误帧数。

范例

此示例将窗口大小设置为 5 秒。

```
Console(config)#interface ethernet 1/1

Console(config-if)#efm oam link-monitor frame window 50

Console(config-if)#
```

26.1.6 efm oam mode

此命令设置指定端口上的 OAM 模式。使用 no 形式恢复默认设置。

语法

efm oam mode {**active** | **passive**}

no efm oam mode

active -启用所有 OAM 功能。

passive -除 OAM 发现和发送环回控制 OAMPDU 外，所有 OAM 功能均已启用。

缺省配置

Active

命令模式

接口配置

命令用法

设置为活动模式时，所选接口将启动 OAM 发现过程。在被动模式下，它只能响应发现消息。

范例

```
Console(config)#interface ethernet 1/1

Console(config-if)#efm oam mode active

Console(config-if)#
```

26.1.7 clear efm oam counters

此命令清除各种 OAM PDU 消息类型的统计计数器。

语法

clear efm oam counters [*interface-list*]

interface-list - *unit/port*

unit -单位标识符。(范围：1)

port -端口号或端口列表。 要输入列表，请使用逗号分隔非连续端口标识符，不要使用空格；使用连字符指定一系列端口。(范围：1-28)

命令模式

特权模式

范例

```
Console#clear efm oam counters

Console#
```

26.1.8 efm oam remote-loopback

此命令启动或停止 OAM 环回测试模式到固定 CPE。

语法

efm oam remote-loopback {**start** | **stop**} *interface*

start -启动远程环回测试模式。

stop -停止远程环回测试模式。

interface - *unit/port*

unit -单位标识符。(范围：1)

port -端口号。(范围：1-28)

缺省配置

无

命令模式

特权模式

命令用法

◆OAM 远程环回可用于故障定位和链路性能测试。在回环测试期间，可以随时查询和比较本地和远程 DTE 的统计信息。

◆使用 **efm oam remote-loopback start** 命令在指定端口上启动 OAM 远程环回测试模式。然后使用 efm oam remote-loopback test 命令开始发送测试数据包。然后使用 **efm oam remote loopback stop** 命令终止测试（如果仍在发送测试数据包）并终止环回测试模式。

◆您指定运行此测试的端口必须连接到能够进入 OAM 远程环回模式的各自 OAM 设备。在远程环回测试期间，远程 OAM 实体将循环返回除 OAMPDU 和暂停帧之外的所有帧。

◆在环回测试期间，交换机和远程设备都被允许将 OAM PDU 发送到对端设备并处理从对端设备接收的任何 OAM PDU。

范例

```
Console#efm oam remote-loopback start 1/1

Loopback operation is processing, please wait.

Enter loopback mode succeeded.

Console#
```

26.1.9 efm oam remote-loopback test

此命令执行远端环回测试，发送指定数量的数据包。

语法

efm oam remote-loopback test *interface* [*number-of-packets*[*packet-size*]]

interface - *unit*/*port*

unit -单位标识符。（范围：1）

port -端口号。（范围：1-28）

number-of-packets -要发送 *的包*数。（范围：1-99999999）

packet-size -要发送的数据*包的大小*。（范围：64-1518 字节）

缺省配置

包数：10,000

数据包大小：64 字节

命令模式

特权模式

命令用法

◆您可以使用此命令在指定端口上执行 OAM 远程环回测试。您指定运行此测试的端口必须连接到能够进入 OAM remoteloopback 模式的对等 OAM 设备。在远程环回测试期间，远程 OAM 实体将覆盖除 OAM PDU 和 pause 帧之外的每个帧。

◆OAM 远程环回可用于故障定位和链路性能测试。在 loopback 测试期间，可以随时查询和比较本地和远程 DTE 的统计信息 。

◆ 完成后显示测试结果。

范例

```
Console#efm oam remote-loopback test 1/1

Loopback test is processing, press ESC to suspend.

....

Port OAM loopback Tx OAM loopback Rx Loss Rate

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

1/2 1990 1016 48.94 %

Console#
```

26.1.10 show efm oam counters interface

此命令显示各种 OAM PDU 消息类型的计数器。

语法

show efm oam counters interface [*interface-list*]

interface-list - *unit*/*port*

unit -单位标识符。（范围：1）

port -端口号或端口列表。使用字符指定一系列端口（范围：1-28）。若是非连续端口，请使用逗号分隔。

命令模式

普通模式，特权模式

范例

```
Console#show efm oam counters interface 1/1

Port OAMPDU Type TX RX

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

1/1 Information 1121 1444

1/1 Event Notification 0 0

1/1 Loopback Control 1 0

1/1 Organization Specific 76 0

Console#
```

26.1.11 show efm oam event-log interface

此命令显示指定端口或所有含有日志的端口的 OAM 事件日志。

show efm oam event-log interface [*interface-list*]

interface-list - *unit/port*

unit -单位标识符。(范围：1)

port -端口号或端口列表。要输入列表，请使用逗号分隔端口标识符，不要使用空格;使用连字符指定一系列端口。(范围：1-28)

命令模式

普通模式, 特权模式

命令用法

◆发生链接事件时，无论位置是本地还是远程，都会在 OAM 事件日志中输入该信息。

◆当日志系统已满时，将自动删除旧事件为新条目腾出空间。

范例

```
Console#show efm oam event-log interface 1/1

OAM event log of Eth 1/1:

00:24:07 2001/01/01

"Unit 1, Port 1: Dying Gasp at Remote"

Console#
```

26.1.12 show efm oam remote-loopbackinterface

此命令显示 OAM 远程环回测试的结果。

语法

show efm oam remote-loopback interface [*interface-list*]

interface-list - *unit/port*

unit -单位标识符。(范围：1)

port -端口号或端口列表。要输入列表，请使用逗号分隔非连续端口标识符，不要使用空格;使用连字符指定一系列端口。(范围：1-28)

命令模式

普通模式, 特权模式

范例

```
Console#show efm oam remote-loopback interface 1/1

Port OAM loopback Tx OAM loopback Rx

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

1/1 2300 2250

Console#
```

26.1.13 show efm oam status interface

此命令显示 OAM 配置设置和事件计数器。

语法

show efm oam status interface [*interface-list*] [**brief**]

interface - *unit/port*

unit -单位标识符。(范围：1)

port -端口号或端口列表。要输入列表，请使用逗号分隔非连续端口标识符，不要使用空格;使用连字符指定一系列端口。(范围：1-28)

brief -显示 OAM 配置状态的简短列表。

命令模式

普通模式, 特权模式

范例

```
Console#show efm oam status interface 1/1

OAM information of Eth 1/1:

Basic Information:

Admin State : Enabled

Operation State : Operational

Mode : Active

Dying Gasp : Enabled

Critical Event : Enabled

Link Monitor (Errored Frame) : Enabled

Link Monitor:

Errored Frame Window (100msec) : 10

Errored Frame Threshold : 1

Console#show efm oam status interface 1/1 brief

$ = local OAM in loopback

* = remote OAM in loopback

Port Admin Mode Remote Dying Critical Errored

State Loopback Gasp Event Frame

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

1/1 Enabled Active Disabled Enabled Enabled Enabled

Console#
```

26.1.14 show efm oam status remoteinterface

此命令显示有关已连接的已启用 OAM 的设备的信息。

语法

show efm oam status remote interface [*interface-list*]

interface-list - *unit/port*

unit -单位标识符。(范围：1)

port -端口号或端口列表。要输入列表，请使用逗号分隔非连续端口标识符，不要使用空格;使

用连字符指定一系列端口。（范围：1-28）

命令模式

普通模式，特权模式

范例

```
Console#show efm oam status remote interface 1/1

Port MAC Address OUI Remote Unidirectional Link MIB Variable

Loopback Monitor Retrieval

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

1/1 00-12-CF-6A-07-F6 000084 Enabled Disabled Enabled Disabled

Console#
```

27 域名服务命令

这些命令用于配置域命名系统（DNS）服务。可以手工配置 DNS 域名和 IP 的对应关系、默认域名配置、1 个或多个用于 IP 地址解析的域名服务器。注意：只有同时使用 dns name-server 命令配置了域名服务器和 dns domain-lookup 命令使能域名查找功能后，域名服务才能生效。

27.1.1 dns domain-list

此命令定义可以附加到不完整主机名的域名列表(即主机名是从不是用点分格式表示的客户端传递过来的)。使用 no 形式从此列表中删除名称。

语法

[no] dns domain-list *name*

name -主机的名称。不要包含从域名中分离主机名的初始点。（范围：1-127 个字符）

缺省配置

无

命令模式

全局配置

命令用法

◆域名一次添加到列表末尾。

◆当此服务上的 DNS 服务收到不完整的主机名时，它将通过域列表工作，将列表中的每个域名附加到主机名，并检查指定名称服务器是否匹配。

◆如果没有域列表，则使用 dns domain-name 命令指定的域名。如果存在域列表，则不使用缺省域名名称。

范例

此示例将两个域名添加到当前列表，然后显示列表。

```
Console(config)#dns domain-list sample.com.jp

Console(config)#dns domain-list sample.com.uk

Console(config)#end

Console#show dns

Domain Lookup Status:

DNS Disabled

default Domain Name:

sample.com

Domain Name List:

sample.com.jp

sample.com.uk

Name Server List:

Console#
```

27.1.2 dns domain-lookup

此命令启用 DNS 主机名到地址转换。使用 no 形式禁用 DNS。

语法

[no] dns domain-lookup

缺省配置

禁用

命令模式

全局配置

命令用法

◆在启用 DNS 之前，必须至少指定一个名称服务器。

◆如果删除了所有名称服务器，将自动禁用 DNS。

范例

此示例启用 DNS，然后显示配置。

```
Console(config)#dns domain-lookup

Console(config)#end

Console#show dns

Domain Lookup Status:
```

```
DNS Enabled

default Domain Name:

sample.com

Domain Name List:

sample.com.jp

sample.com.uk

Name Server List:

192.168.1.55

10.1.0.55

Console#
```

27.1.3 dns domain-name

此命令定义默认域名附加到 incomplete host 名称（即主机名是从不是用点分格式表示的客户端传递过来的）。使用 no 形式删除当前域名。

语法

dns domain-name *name*

no dns domain-name

name -主机的名称。不要包含从域名中分离主机名的初始点。（范围：1-127 个字符）

缺省配置

无

命令模式

全局配置

范例

```
Console(config)#dns domain-name sample.com

Console(config)#end

Console#show dns

Domain Lookup Status:

DNS Disabled

default Domain Name:
```

```
sample.com

Domain Name List:
```

27.1.4 dns host

此命令在 DNS 表中创建一个静态条目，用于将主机名映射到 IP 地址。 使用 no 形式删除条目。

语法

[no] dns host *name address*

name - DNS 主机的名称。（范围：1-100 个字符）

address -对应的 IP 地址。

缺省配置

没有静态条目

命令模式

全局配置

命令用法

使用 no dns host 命令清除静态条目，使用 clear host 命令清除动态条目。

范例

此示例将 IP 地址映射到主机名。

```
Console(config)#dns host rd5 192.168.1.55

Console(config)#end

Console#show hosts

No. Flag Type IP Address TTL Domain

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

0 2 Address 192.168.1.55 rd5

Console#
```

27.1.5 dns name-server

此命令指定域名服务器的地址。使用 no 形式从此列表中删除域名服务器。

语法

[no] dns name-server *server-address1* [*server-address2* …*server-address6*]

server-address1 -域名服务器的 IP 地址。

server-address2 … *server-address6* - 域名服务器的 IP 地址。

缺省配置

无

命令模式

全局配置

命令用法

列出的域名服务器按指定的顺序查询，直到收到响应，或者到达列表的末尾而没有响应。

范例

此示例将两个域名服务器添加到列表中，然后显示列表。

```
Console(config)#dns name-server 192.168.1.55 10.1.0.55

Console(config)#end

Console#show dns

Domain Lookup Status:

DNS Disabled

Default Domain Name:

sample.com

Domain Name List:

sample.com.jp

sample.com.uk

Name Server List:

192.168.1.55

10.1.0.55

Console#
```

27.1.6 clear dns cache

此命令清除 DNS 缓存中的所有条目。

命令模式

特权模式

范例

```
Console#clear dns cache

Console#show dns cache

No. Flag Type DNS Address TTL Domain

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

Console#
```

27.1.7 clear host

此命令从 DNS 表中删除动态条目。

语法

clear host {*name* / *}

name -主机的名称。 （范围：1-100 个字符）

* - 删除所有条目。

缺省配置

无

命令模式

特权模式

命令用法

使用 **clear host** 命令清除动态条目，或 no dns host 命令清除静态条目。

范例

此示例清除 DNS 表中的所有动态条目。

```
Console(config)#clear host *

Console(config)#
```

27.1.8 show dns

此命令显示 DNS 服务的配置。

命令模式

特权模式

范例

```
Console#show dns

Domain Lookup Status:

DNS Enabled

Default Domain Name:

sample.com

Domain Name List:

sample.com.jp

sample.com.uk

Name Server List:

192.168.1.55

10.1.0.55

Console#
```

27.1.9 show dns cache

此命令显示 DNS 缓存中的条目。

命令模式

特权模式

范例

```
Console#show dns cache

No. Flag Type IP Address TTL Host

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

3 4 Host 209.131.36.158 115 www-real.wa1.b.yahoo.com

4 4 CNAME POINTER TO:3 115 www.yahoo.com

5 4 CNAME POINTER TO:3 115 www.wa1.b.yahoo.com

Console#
```

27.1.10 show hosts

此命令显示静态主机名到地址映射表。

命令模式

特权模式

范例

请注意，如果主机名作为先前配置的条目映射到同一地址，则它将显示为别名。

```
Console#show hosts

No. Flag Type IP Address TTL Domain

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

0 2 Address 192.168.1.55 rd5

1 2 Address 2001:DB8:1::12 rd6

3 4 Address 209.131.36.158 65 www-real.wa1.b.yahoo.com

4 4 CNAME POINTER TO:3 65 www.yahoo.com

5 4 CNAME POINTER TO:3 65 www.wa1.b.yahoo.com

Console#
```

28 DHCP 命令

这些命令用于配置动态主机配置协议（DHCP）客户端和中继功能。任何 VLAN 接口都可以配置为通过 DHCP 自动获取 IP 地址。此交换机可配置为将 DHCP 客户端配置请求中继到另一网络上的 DHCP 服务器。

28.1 DHCP 客户端

使用本节中的命令允许交换机的 VLAN 接口以动态方式获取 IP 地址信息。

28.1.1 ip dhcp clientclass-id

此命令指定当前接口的 DCHP 客户端供应商类标识符。使用 **no** 形式从 DHCP 数据包中删除类标识符选项。

语法

ip dhcp client class-id [**text** *text* | **hex** *hex*]

no ip dhcp client class-id

text -文本字符串。（范围：1-32 个字符）

hex -十六进制值。（范围：1-64 个字符）

缺省配置

启用了类标识符选项

命令模式

接口配置 (VLAN)

命令用法

◆使用不带任何关键字的命令恢复默认设置。

◆此命令用于标识 DHCP 服务器交换机的供应商类和配置，然后使用此信息确定如何为客户端提供服务或返回要返回的信息类型 。

◆此 DHCP 选项的一般框架在 RFC 2132（选项 60）中列出。此信息用于传达配置设置或有关客户端的其他标识信息，但应由服务提供商或网络管理员提供要使用的特定字符串。

◆服务器应回复 Option 43 信息，其中包含选项 66 属性，包括 TFTP 服务器名称和引导文件名。

范例

```
Console(config)#interface vlan 2

Console(config-if)#ip dhcp client class-id hex 0000e8666572

Console(config-if)#
```

28.1.2 ip dhcp restart client

此命令提交 BOOTP 或 DHCP 客户端请求。

缺省配置

无

命令模式

特权模式

命令用法

◆此命令通过 ipaddress 命令发出 BOOTP 或 DHCP 客户端请求或任何已设置为 BOOTP 或 DHCP 模式的 IP 接口。

◆DHCP 要求服务器重新分配客户端的最后一个地址（如果可用）。

◆如果 BOOTP 或 DHCP 服务器已移至其他域，则提供给客户端的地址的网络部分将基于此新域。

范例

在以下示例中，将为设备重新分配相同的地址。

```
Console(config)#interface vlan 1

Console(config-if)#ip address dhcp

Console(config-if)#exit

Console#ip dhcp restart client
```

```
Console#show ip interface

VLAN 1 is Administrative Up - Link Up

Address is 00-E0-00-00-00-01

Index: 1001, MTU: 1500

Address Mode is DHCP

IP Address: 192.168.0.2 Mask: 255.255.255.0

Console#
```

28.1.3 ipv6 dhcp client rapid-commit vlan

此命令为从指定接口提交的所有 DHCPv6 客户端请求指定 DHCPv6 消息交换的“快速提交”选项。使用 no 形式禁用此选项。

语法

[no] **ipv6 dhcp client rapid-commit vlan** *vlan-id*

vlan-id - VLAN ID，指定为单个数字，由连字符分隔的连续数字范围或由逗号分隔的多个数字。（范围：1-4093）

缺省配置

禁用

命令模式

全局配置

命令用法

◆DHCPv6 客户端可以通过正常的四消息交换（征求，通告，请求，回复）或通过快速双消息交换（征求，回复）从服务器获取配置参数。 必须在客户端和服务器上启用 The rapid-commit 选项才能使用两个消息交换。

◆此命令允许用于前缀委托的双消息交换方法。启用后，从指定接口提交的 DCHPv6 客户端请求将在所有请求消息中包含快速提交选项。

范例

```
Console(config)#ipv6 dhcp client rapid-commit vlan 2

Console(config)#
```

28.1.4 ipv6 dhcp restart client vlan

此命令提交 DHCPv6 客户端请求。

语法

ipv6 dhcp restart client vlan *vlan-id*

vlan-id - VLAN ID，指定为单个数字，由连字符分隔的连续数字范围或由逗号分隔的多个数字。（范围：1-4093）

缺省配置

无

命令模式

特权模式

命令用法

◆如果 DHCPv6 客户端进程尚未运行，则通过指定的接口提交配置信息请求，从而启动 DHCPv6 客户端进程。重启 DHCPv6 后，交换机可能会尝试通过有状态地址自动配置获取 IP 地址前缀。如果路由器通告设置了“其他有状态配置”标志，则交换机也可以尝试获取其他重启 DHCPv6 时的非地址配置信息（如默认网关或 DNS 服务器）。在向 DHCPv6 服务器提交客户端请求之前，应使用 ipv6 addressautoconfig 命令配置交换机本地地址。在路由器广告消息中接收的管理地址配置标志（M 标志）和其他状态配置标志（O 标志）的状态将确定该设备应该尝试从 DHCPv6 服务器获取的信息，如下所述。

■ M 和 O 标志都设置为 1：

DHCPv6 用于地址和其他配置设置。这种组合称为 DHCPv6 有状态，其中 DHCPv6 服务器为 IPv6 主机分配有状态地址。

■ M 标志设置为 0，O 标志设置为 1：

DHCPv6 仅用于其他配置设置。邻居路由器配置为广告非链路 - 本地地址前缀，IPv6 主机从该前缀获取无状态地址。这种组合称为 DHCPv6 无状态，其中 DHCPv6 服务器不为 IPv6 主机分配有状态地址，但是分配无状态配置设置。

◆DHCPv6 客户端通过发送请求消息和收集通告的消息回复来构建服务器列表。然后，这些服务器根据其广告的偏好值进行排名。如果客户端需要从服务器获取前缀，则仅考虑具有广告前缀的服务器。

◆如果使用 ipv6 dhcp client rapid-commit vlan 命令在交换机上启用了快速提交选项，并且

在 DHCPv6 服务器上，则可以将消息交换从正常的四个步骤减少到只需要请求和回复的两步交换消息。

范例

以下命令在 VLAN 1 上提交客户端请求。

```
Console#ipv6 dhcp restart client vlan 1

Console#
```

28.1.5 show ipv6 dhcp duid

此命令显示此交换机的 DHCP 唯一标识符。

命令模式

特权模式

命令用法

◆DHCPv6 客户端和服务器由客户端标识符和服务器标识符选项中包含的 DHCP 唯一标识符(DUID)标识。静态或动态地址前缀可由 DHCPv6 服务器根据客户端的 DUID 分配。

◆ 要显示分配给此设备的 DUID，请先输入 ipv6 addressautoconfig 命令。

范例

```
Console#show ipv6 dhcp duid

DHCPv6 Unique Identifier (DUID): 0001-0001-4A8158B4-00E00C0000FD

Console#
```

28.1.6 show ipv6 dhcp vlan

此命令显示指定接口的 DHCPv6 信息。

语法

show ipv6 dhcp vlan *vlan-id*

vlan-id - VLAN ID，指定为单个数字，由连字符分隔的连续数字范围或由逗号分隔的多个数字。（范围：1-4093）

命令模式

特权模式

范例

```
Console#show ipv6 dhcp vlan 1
```

```
VLAN 1 is in DHCP client mode, Rapid-Commit

List of known servers:

Server address : FE80::250:FCFF:FEF9:A494

DUID : 0001-0001-48CFB0D5-F48F2A006801

Server address : FE80::250:FCFF:FEF9:A405

DUID : 0001-0001-38CF5AB0-F48F2A003917

Console#
```

28.2 DHCP 中继选项 82

本节介绍用于配置交换机从本地主机到远程 DHCP 服务器的中继 DHCP 请求的命令。

28.2.1 ip dhcp relay server

此命令启用 DHCP 中继服务，并指定要使用的服务器的地址。使用 no 形式清除所有地址。

语法

ip dhcp relay server *address1* [*address2* [*address3* ...]]

no ip dhcp relay server

address - IP address of DHCP server. (范围: 1-5 addresses)

缺省配置

无

命令模式

全局配置

命令用法

◆DHCP 中继服务适用于在任何配置的 VLAN（管理 VLAN 和非管理 VLAN）上接收的 DHCP 客户端请求。

◆ 此命令用于为连接到交换机的主机设备配置 DHCP 中继。如果启用了 DHCP 中继服务（通过 指定至少一个 DHCP 服务器的地址），并且此交换机看到 DHCPrequest 广播，它会将自己的 IP 地址插入到请求中，以便 DHCP 服务器知道客户端所在的子网。然后交换机将数据包转发到另一个网络上的 DHCP 服务器。当服务器收到 DHCP 请求时，它会从 DHCP 客户端子网的已定义范围

中为 DHCP 客户端分配一个空闲 IP 地址，并将 DHCP 响应发送回 DHCP 中继代理（即此交换机）。然后此交换机　传递 DHCP 响应从服务器接收到客户端。

◆　必须为至少一个 DHCP 服务器指定 IP 地址。否则，交换机的 DHCP 中继代理不会将客户端请求转发到 DHCP 服务器。最多可以指定五个 DHCP 服务器　。

◆　要终止 DHCP 中继服务，必须使用 no 命令清除所有已配置的服务器地址　。

范例

```
Console(config)#ip dhcp relay server 192.168.10.19

Console(config)#
```

28.2.2 ip dhcp relay information option

此命令启 DHCP Option 82 信息中继，并指定当交换机生成 Option 82 信息时用于 remote-id 的帧格式。使用此命令的 no 形式禁用此功能。

语法

ip dhcp relay information option[**encode no-subtype**][**remote-id** {**ip-address** [**encode** {**ascii** | **hex**}] |**mac-address** [**encode** {**ascii** | **hex**}] | **string** *string*}]

no ip dhcp rely information option [**encode no-subtype**][**remote-id** [**ip-address encode**] | [**mac-address encode**]]

encode no-subtype -禁用在 Option 82 信息中使用 circuit-ID（CID）和 remote-ID（RID）中的子类型和子长度字段。

mac-address -包含中继代理的 MAC 地址字段（即交换机 CPU 的 MAC 地址）。

ip-address -包括中继代理的 IP 地址字段（即管理接口的 IP 地址）。

encode -表示 ASCII 或十六进制的编码。

string -插入远程标识符字段的任意字符串。（范围：1-32 个字符）

缺省配置

Option 82: 禁用

CID/RID sub-type: 启用

Remote ID: MAC 地址

命令模式

全局配置

命令用法

使用不带任何关键字的命令启用 DHCP Option 82 信息中继。

◆　DHCP 提供中继代理信息选项，用于将　其 DHCP 客户端或中继代理本身的　信息发送　到 DHCP 服务器。也称为 DHCP 选项 82，它允许兼容的 DHCP 服务器在分配 IP 地址时使用此信息，或为客户端设置其他服务或策略。

◆　启用　Option 82 后，可以在交换机转发的 DHCP 请求报文中识别请求客户端（或使用信息字段描述自身的中间代理），并回复 DHCP 服务器发回的报文。　根据通过此命令为 remote-id 设置的所选帧格式，此信息可以指定请求设备的 MAC 地址，IP 地址或任意字符串（即，此上下文中的中继代理）。

◆ 默认情况下，中继代理还会填写 Option 82 circuit-id 字段，表示交换机收到 DHCP 客户端请求的本地接口，包括 VLAN ID，堆叠单元和端口。这样可以实现 DHCP 客户端-服务器交换要在服务器和客户端之间转发的消息，而不必将它们泛洪到整个 VLAN。

◆ 交换机收到的 DHCP 请求报文处理如下：

■ 如果在交换机上设置了 DHCP 中继服务器，当交换机从管理 VLAN 或非管理 VLAN 接收到 没有 选项 82 信息 的 DHCP 请求包 时，它将向 DHCP 请求包添加 选项 82 中继信息和中继代理的地址。然后将其单播到 DHCP 服务器。

■ 如果交换机上设置 了 DHCP 中继服务器，当交换机接收到来自管理 VLAN 或非管理 VLAN 的 带有选项 82 信息的 DHCP 请求报文时，它将根据配置的中继进行处理信息选择政策：

■ 如果策略是“replace”，则 DHCP 请求数据包的选项 82 内容（RID 和 CID 子选项）将替换为交换机提供的信息。中继代理地址插入 DHCP 请求数据包，然后交换机将此数据包单播到 DHCP 服务器。

■ 如果策略为“keep”，则将保留 DHCP 请求数据包的选项 82 内容。中继代理地址被插入到 DHCP 请求数据包中，然后交换机将此数据包单播到 DHCP 服务器 。

■ 如果策略为“drop”，则原始 DHCP 请求数据包将被刷新到接收数据包但未重新接收的 VLAN。

◆ 中继代理收到的 DHCP 应答报文处理如下：

当中继代理通过管理 VLAN 接收带有选项 82 信息的 DHCP 回复数据包时，它首先确保数据包的目的地为它。

■ 如果 DHCP 回复数据包中的 RID 与交换机上配置的 RID 不同，则保留选项 82 信息，并将数据包泛洪到接收它的 VLAN。

■ 如果 DHCP 回复数据包中的 RID 与交换机上配置的 RID 相匹配，则会从数据包中删除 Option 82 信息，并按如下方式发送：

■ 如果 DHCP 数据包的广播标志为开，则交换机 使用选项 82 信息字段中包含的电路 ID 信息来识别连接到请求客户端的 VLAN，然后将 DHCP 应答数据包广播到此 VLAN。

■ 如果 DHCP 数据包的广播标志为关闭，则交换机使用选项 82 字段中的 ccc uit-id 信息来标识连接到请求客户端的接口，并将回复数据包单播到客户端。

◆ 如果在交换机上启用了 DHCPrelay 服务，则 DHCP 数据包将泛洪到接收它们的 VLAN 上，并且应用以下任何一种情况：

■ 当交换机接收 DHCP 数据包时，交换机上没有设置 DHCP 中继服务器。

■ 当交换机接收到具有非零中继代理地址字段的 DHCP 请求数据包 （不是此交换机的地址） 时，交换机上已设置 DHCP 中继服务器 。

■ 当交换机接收到来自管理 VLAN 的没有选项 82 信息的 DHCP 回复数据包时，交换机上已设置 DHCP 中继服务器。

■ 回复数据包包含有效的中继代理地址字段（不在此交换机的地址），或通过管理 VLAN 接收带有零中继代理地址的应答数据包。

■ 交换机上已设置 DHCP 中继服务器，交换机在非管理 VLAN 上接收应答报文。

◆ 使用 ip dhcp relay information policy 命令指定如何处理已包含 Option 82 信息的 DHCP 客户端请求数据包。

◆ DHCP Snooping Information Option 82 和 DHCP RelayInformation Option 82 不能同时启用。

范例

此示例启用选项 82，并为选项设置 remoteID 的帧格式以使用交换机 CPU 的 MAC 地址。

```
Console(config)#ip dhcp relay information option remote-id mac-address
Console(config)#
```

28.2.3 ip dhcp relay information policy

此命令指定如何处理已包含 DHCP Option 82 信息的客户端请求。

语法

ip dhcp relay information policy {**drop** | **keep** | **replace**}

drop -将原始请求数据包泛洪到接收它的 VLAN 而不是中继它。

keep -保留客户端请求中的 Option82 信息，插入中继代理的地址，并将数据包单播到 DHCP 服务器。

replace -用客户端请求中提供的信息替换客户端请求中的 Option 82 信息 circuit-id 和 remoteid 字段，插入中继代理的地址，并将该数据包单播到 DHCP 服务器。

缺省配置

丢弃

命令模式

全局配置

命令用法

◆有关交换机何时处理 Option 82 信息的信息，请参阅 ip dhcp relay information option 命令下的使用指南 。

◆当 Option 82 策略设置为“保留”请求数据包中的原始信息时，将忽略 ip dhcp relay information 选项命令指定的帧类型。

范例

此示例设置 Option 82 策略，以将客户端信息保留在中继代理接收的请求数据包中，并将此数据包转发到 DHCP 服务器上。

```
Console(config)#ip dhcp relay information policy keep
Console(config)#
```

28.2.4 show ip dhcp relay

此命令显示 DHCP 中继服务的配置设置。

命令模式

特权模式

范例

```
Console#show ip dhcp relay

Status of DHCP relay information:

Insertion of relay information: enabled.

DHCP option policy: drop.

DHCP relay-server address: 192.168.0.4

0.0.0.0

0.0.0.0

0.0.0.0

0.0.0.0

DHCP sub-option format: extra subtype included

DHCP remote id sub-option: mac address (hex encoded)

Console#
```

29 IP 接口命令

IP 版本 4 和版本 6 地址可用于通过网络对交换机进行管理访问。 可以同时使用 IPv4 或 IPv6 地址来访问交换机。 您可以手动配置特定的 IPv4 或 IPv6 地址，或指示交换机在上电时从 BOOTP 或 DHCP 服务器获取 IPv4 地址。 可以手动配置或动态生成 IPv6 地址。

默认情况下，VLAN 1 配置静态 IPv4 地址。您可能还需要在该设备和另一个网络段上存在的管理站之间建立 IPv4 或 IPv6 默认网关。

29.1 IPV4 接口

默认情况下，此开关没有分配 IP 地址。您必须手动配置新地址以管理网络上的交换机，以将交换机连接到现有 IP 子网。 您可能还需要在此设备和管理站之间或其他网段上存在的其他设备之间建立默认网关。

本节包括配置 IP 接口的命令，Address Resolution Protocol（ARP）和 Proxy ARP。

29.1.1 ip address

此命令设置当前所选 VLAN 接口的 IPv4 地址。使用 **no** 形式删除 IP 地址。

语法

ip address {*ip-address netmask* [**secondary**][**default-gateway** *ip-address*] | **bootp** | **dhcp**}

no ip address [*ip-address netmask* [**secondary**] | **dhcp**]

ip-address - IP 地址

netmask -关联 IP 子网的网络掩码。此掩码标识用于路由到特定子网的主机地址位。

secondary -指定辅助 IP 地址。

default-gateway -默认网关。（请参阅 ip default gateway 命令，它提供相同的功能 ）

bootp -从 BOOTP 获取 IP 地址。

dhcp -从 DHCP 获取 IP 地址。

缺省配置

DHCP

命令模式

接口配置 (VLAN)

命令用法

◆必须为此设备分配 IP 地址才能通过网络获取管理访问权限或将交换机连接到现有 IP 子网。可以手动配置特定 IP 地址，或者交换机可以通过 BIOTP 或 DHCP 获取地址服务器。有效的 IP 地址由四个数字组成，0 到 255，以句点分隔。配置程序不接受除此格式之外的任何内容。

◆一个接口只能有一个主 IP 地址，但可以有多个二级 IP 地址。换句话说如果可以通过此接口访问多个 IP 子网，则需要指定辅助地址。请注意，在设置主 IP 地址之前无法配置辅助地址，如果辅助地址仍然存在，则无法删除主地址。此外如果网段中的任何路由器/交换机使用辅助地址，则该网段中的所有其他路由器/交换机也必须使用来自同一网络或子网地址空间的辅助地址。

◆ 如果选择了 **bootp** 或 **dhcp** 选项，系统将立即启动所有配置为通过 BOOTP 或 DHCP 获取地址分配的 VLAN 的广播服务请求。 IP 已启用但在收到 BOOTP 或 DHCP 回复之前将无法运行。路由器周期性地广播请求以了解其 IP 地址。(BOOTP 和 DHCP 值可以包括 IP 地址，默认网关和子网掩码)。 如果 DHCP / BOOTP 服务器响应缓慢，您可能需要使用 ip dhcp restart client 命令重新启动广播服务请求，或重新启动交换机。

范例

在以下示例中，将为设备分配 VLAN 1 中的地址。

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.5 255.255.255.0
Console(config-if)#
```

29.1.2 ip default-gateway

此命令指定在本地路由表中找不到的目标的默认网关。使用 **no** 形式删除默认网关。

语法

ip default-gateway *gateway*

no ip default-gateway

gateway -默认网关的 IP 地址

缺省配置

没有网关

命令模式

全局配置

命令用法

◆只有在交换机上配置了直接连接网关的网络接口时，才能成功设置默认网关。

◆如果管理站位于不同的 IP 段，则必须定义网关。

范例

以下示例为此设备定义默认网关：

```
Console(config)#ip default-gateway 10.1.1.254
Console(config)#
```

29.1.3 show ip default-gateway

此命令显示为此设备配置的 IPv4 默认网关。

缺省配置

无

命令模式

特权模式

范例

```
Console#show ip default-gateway
IP default gateway 10.1.0.254
Console#
```

29.1.4 show ip interface

此命令显示 IPv4 接口的设置。

命令模式

特权模式

范例

```
Console#show ip interface

VLAN 1 is Administrative Up - Link Up

Address is 00-E0-00-00-00-01

Index: 1001, MTU: 1500

Address Mode is DHCP

IP Address: 192.168.0.2 Mask: 255.255.255.0

Console#
```

29.1.5 show ip traffic

此命令显示 IP，ICMP，UDP，TCP 和 ARP 协议的统计信息。

命令模式

特权模式

范例

```
Console#show ip traffic

IP Statistics:

IP received

7845 total received

header errors

unknown protocols

address errors

discards

7845 delivers

reassembly request datagrams

reassembly succeeded

reassembly failed

IP sent

forwards datagrams

9903 requests
```

discards

no routes

generated fragments

fragment succeeded

fragment failed

ICMP Statistics:

ICMP received

input

errors

destination unreachable messages

time exceeded messages

parameter problem message

echo request messages

echo reply messages

redirect messages

timestamp request messages

timestamp reply messages

source quench messages

address mask request messages

address mask reply messages

ICMP sent

output

errors

destination unreachable messages

time exceeded messages

parameter problem message

echo request messages

echo reply messages

redirect messages

timestamp request messages

```
timestamp reply messages

source quench messages

address mask request messages

address mask reply messages

UDP Statistics:

input

no port errors

other errors

output

TCP Statistics:

7841 input

input errors

9897 output

Console#
```

29.1.6 traceroute

此命令显示路由数据包到达指定目标。

语法

traceroute *host*

host -主机的 IP 地址或别名。

缺省配置

无

命令模式

特权模式

命令用法

◆使用 **traceroute** 命令确定到达指定目标所用的路径。

◆当目标响应，超出最大超时（TTL）或超过最大跳数时跟踪终止。

◆traceroute 命令首先发送探测数据报，TTL 值设置为 1。这会导致第一个路由器丢弃 datagramand 返回错误消息。跟踪功能然后在每个后续 TTL 级别发送多个探测消息，并显示每条

消息的往返时间。并非所有设备都通过返回“ICMP 端口不可达”消息正确响应探测。如果在返回响应之前计时器关闭，则跟踪功能会打印一系列的磁盘和“请求超时”消息。只有在达到最大超时时才终止的长序列消息可能表明目标设备存在此问题。

◆ 如果目标设备没有响应或检测到其他错误，则交换机将通过以下消息之一指示：

- * -无响应
- H-主机无法访问
- N-网络无法访问
- P-协议无法访问
- O-其他

范例

```
Console#traceroute 192.168.0.1

Press "ESC" to abort.

Traceroute to 192.168.0.99, 30 hops max, timeout is 3 seconds

Hop Packet 1 Packet 2 Packet 3 IP Address

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

1 20 ms <10 ms <10 ms 192.168.0.99

Trace completed.

Console#
```

29.1.7 ping

此命令将（IPv4）ICMP 回应请求数据包发送到网络上的另一个节点。

语法

ping *host* [**count** *count*] [**size** *size*]

host -*主机的* IP 地址或别名。

count -要发送的数据包数。（范围：1-16）

size -数据包中的字节数。（范围：32-512）实际数据包大小将比指定的大小大 8 个字节，因为路由器添加了标头信息。

缺省配置

计数：5

大小: 32 bytes

命令模式

普通模式, 特权模式

命令用法

◆使用 ping 命令查看是否可以访问网络上的其他站点。

◆以下是 **ping** 命令的一些结果 ：

- *正常响应*-正常响应发生在一到三秒内，具体取决于网络流量。
- *目标未响应*-如果主机未响应，则会在十秒钟内显示“超时”。
- *目标无法访问*-此目标的网关表示目标无法访问。
- *网络或主机无法访问*-网关在路由表中未找到任何对应关系。

◆ 在 ping 主机名时，请确保已定义 DNS 服务器并启用主机名到地址转换。如有必要，还可以在 DNS 静态主机表中指定本地设备 。

范例

```
Console#ping 10.1.0.9

Type ESC to abort.

PING to 10.1.0.9, by 5 32-byte payload ICMP packets, timeout is 5 seconds

response time: 10 ms

response time: 10 ms

response time: 10 ms

response time: 10 ms

response time: 0 ms

Ping statistics for 10.1.0.9:

5 packets transmitted, 5 packets received (100%), 0 packets lost (0%)

Approximate round trip times:

Minimum = 0 ms, Maximum = 10 ms, Average = 8 ms

Console#
```

29.1.8 arp timeout

此命令设置 Address Resolution Protocol（ARP）缓存中动态条目的老化时间。使用 no 形式恢复缺省超时时间。

语法

arp timeout *seconds*

no arp timeout

seconds -动态条目保留在 ARP 缓存中的时间。（范围：300-86400；86400 秒为一天）

缺省配置

1200 秒(20 分钟)

命令模式

全局配置

命令用法

◆当 ARP 条目到期时，将从缓存中删除，并发送 ARPrequest 数据包以重新建立 MAC 地址。

◆ 老化时间决定动态条目在缓存中保留的时间。如果超时太短交换机可能会占用资源，从而对最近从表中刷新的地址的 ARP 请求进行处理。

范例

此示例将 ARP 缓存超时设置为 15 分钟（即 900 秒）。

```
Console(config)#arp timeout 900

Console(config)#
```

29.1.9 clear arp-cache

此命令从地址解析协议（ARP）缓存中删除所有动态条目。

命令模式

特权模式

范例

此示例清除 ARP 缓存中的所有动态条目。

```
Console#clear arp-cache

This operation will delete all the dynamic entries in ARP Cache.
```

```
Are you sure to continue this operation (y/n)?y

Console#
```

29.1.10 show arp

此命令显示地址解析协议（ARP）缓存中的条目。

命令模式

普通模式，特权模式

命令用法

此命令显示有关 ARP 缓存的信息。第一行显示缓存超时。它还显示每个缓存条目，包括 IP 地址，MAC 地址，类型（动态，其他）和 VLAN 接口。请注意条目类型“other”表示此路由器的本地地址。

范例

此示例显示 ARP 缓存中的所有条目。

```
Console#show arp

ARP Cache Timeout: 1200 (seconds)

IP Address MAC Address Type Interface

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

10.1.0.0 FF-FF-FF-FF-FF-FF other VLAN1

10.1.0.254 00-00-AB-CD-00-00 other VLAN1

10.1.0.255 FF-FF-FF-FF-FF-FF other VLAN1

145.30.20.23 09-50-40-30-20-10 dynamic VLAN3

Total entry : 4

Console#
```

29.2 IPV6 接口

29.2.1 ipv6 default-gateway

此命令设置当目标位于不同网段时使用的IPv6默认网关。使用no形式删除以前配置的默认网关。

语法

ipv6 default-gateway *ipv6-address*

no ipv6 address

ipv6-address -当目的地位于不同的网段时，默认下一跳路由器的 IPv6 地址。

缺省配置

无

命令模式

全局配置

命令用法

◆所有 IPv6 地址必须符合 RFC 2373“IPv6 寻址体系结构”，使用 8 个冒号分隔的 16 位十六进制值。可以在地址中使用双冒号来指示填充未定义字段所需的零的适当数量。

◆不同区域（RFC4007）中的不同接口/节点可以使用相同的链路本地地址。因此在指定链路本地地址时，请在%分隔符后包含指示 VLAN 标识符的 zone-id 信息。例如，FE80 :: 7272%1 将 VLAN 1 识别为接口。

◆如果目标已分配 IPv6 地址且位于不同的 IP 段，则必须定义 IPv6 默认网关。

◆只有在交换机上配置了直接连接到网关的网络接口时，才能成功设置 IPv6 默认网关 。

范例

以下示例为此设备定义默认网关：

```
Console(config)#ipv6 default-gateway FE80::269:3EF9:FE19:6780%1
Console(config)#
```

29.2.2 ipv6 address

此命令配置 IPv6 全球单播地址，并在接口上启用 IPv6。使用 no 带任何参数的 no 形式从接口中删除所有 IPv6 地址，或使用带有特定 IPv6 地址的 no 形式从接口中删除该地址。

语法

[no] **ipv6 address** *ipv6-address*[/*prefix-length*]

ipv6-address -一个完整的 IPv6 地址，包括网络前缀和主机地址位。

prefix-length -一个十进制值，表示地址的多少个连续位（左起）包含前缀（即地址的网络部分）。

缺省配置

无

命令模式

接口配置 (VLAN)

命令用法

◆所有 IPv6 地址必须符合 RFC 2373“IPv6 Addressing Architecture”，使用 8 个冒号分隔的 16 位十六进制值。可以在地址中使用双冒号来指示填充未定义字段所需的零的适当数量。

◆ 要连接到具有多个子网的大型网络，必须配置全局单播地址。可以使用此命令手动配置此地址，也可以使用 ip ipv6 address autoconfig 命令自动配置该地址 。

◆ 如果尚未为此接口分配链路位置地址，则此命令将分配指定的静态全球单播地址，并为接口动态生成链路本地单播地址。(链路本地地址使用地址前缀 FE80 和基于交换机 MAC 地址的主机部分，采用修改后的 EUI-64 格式。)

◆ 如果检测到重复的地址，则会向控制台发送警告消息。

范例

此示例指定完整的 IPv6 地址和前缀长度。

```
Console(config)#interface vlan 1

Console(config-if)#ipv6 address 2001:DB8:2222:7272::72/96

Console(config-if)#end

Console#show ipv6 interface

VLAN 1 is up

IPv6 is enabled

Link-local address:

FE80::2E0:CFF:FE00:FD/64

Global unicast address(es):

2001:DB8:2222:7272::72/96, subnet is 2001:DB8:2222:7272::/96
```

```
Joined group address(es):

FF02::1:FF00:72

FF02::1:FF00:FD

FF02::1

IPv6 link MTU is 1500 bytes

ND DAD is enabled, number of DAD attempts: 3.

ND retransmit interval is 1000 milliseconds

ND advertised retransmit interval is 0 milliseconds

ND reachable time is 30000 milliseconds

ND advertised reachable time is 0 milliseconds

Console#
```

29.2.3 ipv6 address autoconfig

此命令在接口上启用 IPv6 地址的无状态自动配置，并在接口上启用 IPv6。地址的网络部分基于 IPv6 路由器广告消息中接收的前缀;主机部分基于修改的 EUI-64 形式的接口标识符（即交换机的 MAC 地址）。使用 no 形式删除此命令生成的地址。

语法

[no] ipv6 address autoconfig

缺省配置

无

命令模式

接口配置 (VLAN)

命令用法

◆如果尚未为此接口分配链接本地地址，则此命令将动态生成全局单播地址（如果接收的路由器通告中包含全局前缀）和接口的链接本地地址。（链路本地地址使用地址前缀 FE80 和主机部分基于交换机的 MAC 地址以修改后的 EUI-64 格式。）

◆ 如果检测到重复的地址，则会向控制台发送警告消息 。

◆ 重启 DHCPv6 后，交换机可能会尝试通过有状态地址自动配置获取 IP 地址前缀。如果路由广告设置了“其他有状态配置”标志，则当重新启动 DHCPv6 时，该开关还可以尝试获取她的非

地址配置信息（例如默认网关）。

范例

此示例分配动态全球单播地址

2001：DB8：2222：7272：2E0：CFF：FE00：FD 到交换机。

```
Console(config-if)#ipv6 address autoconfig

Console(config-if)#ipv6 enable

Console(config-if)#end

Console#show ipv6 interface

VLAN 1 is up

IPv6 is enabled

Link-local address:

FE80::2E0:CFF:FE00:FD/64

Global unicast address(es):

2001:DB8:2222:7272:2E0:CFF:FE00:FD/64, subnet is 2001:DB8:2222:7272::/

64[AUTOCONFIG]

valid lifetime 2591628 preferred lifetime 604428

Joined group address(es):

FF02::1:FF00:FD

FF02::1

IPv6 link MTU is 1280 bytes

ND DAD is enabled, number of DAD attempts: 3.

ND retransmit interval is 1000 milliseconds

ND advertised retransmit interval is 0 milliseconds

ND reachable time is 30000 milliseconds

ND advertised reachable time is 0 milliseconds

Console#
```

29.2.4 ipv6 address eui-64

此命令使用低位 64 位的 EUI-64 接口 ID 为接口配置 IPv6 地址，并在接口上启用 IPv6。使用 no 带任何参数的 no 形式从接口中删除所有手动配置的 IP 地址。使用带有特定地址的 no 形式将其从界面中删除。

语法

ipv6 address *ipv6-prefix/prefix-length* **eui-64**

no ipv6 address [*ipv6-prefix/prefix-length* **eui-64**]

ipv6-prefix -分配给接口的地址的 IPv6 网络部分。

prefix-length -一个十进制值，表示地址的多少个连续位（左起）包含前缀（即地址的网络部分）。

缺省配置

无

命令模式

接口配置 (VLAN)

命令用法

◆必须使用 8 个冒号分隔的 16 位十六进制值根据 RFC 2373“IPv6 Addressing Architecture”格式化前缀。可以在地址中使用双冒号来指示填充未定义字段所需的零的适当数量。

◆ 如果尚未为此接口分配链接本地地址，则此命令将为此接口动态生成全局单播地址和本地链接地址。（链路本地地址使用地址前缀 FE80 和主机部分基于交换机的 MAC 地址以修改后的 EUI-64 格式。）

◆请注意如果指定的前缀长度小于 64 位，则 ipv6-prefix 中指定的值可能包含一些高阶主机位。如果指定的前缀长度超过 64 位，则地址的网络部分将优先于接口标识符。

◆如果检测到重复的地址，则会向控制台发送警告消息。

◆IPv6 地址长度为 16 个字节，其中底部 8 个字节通常根据设备的 MAC 地址形成唯一的主机标识符。EUI-64 规范适用于使用前 8 字节 MAC 地址的设备。对于仍使用 6 字节 MAC 地址（也称为 EUI-48 格式）的设备，必须通过反转地址中的通用/本地位并插入，将其转换为 EUI-64 格式 MAC 地址的上下三字节之间的十六进制数 FFFE。

◆例如如果设备的 EUI-48 地址为 28-9F-18-1C-82-35，则必须首先反转全局/本地位以满足 EUI-64 要求（即全局定义的地址和 0 表示本地定义的地址），将 28 更改为 2A。然后在 OUI（即公司 ID）和地址的其余部分之间插入两个字节 FFFE，得到修改的 EUI-64 接口标识符 2A-9F-18-FF-FE-1C-82-35。

◆此主机寻址方法允许在单个设备的多个 IP 接口上使用相同的接口标识符，只要这些接口连接到不同的子网即可。

范例

此示例使用网络前缀 2001：0DB8：0：1 :: / 64，并指定 EUI-64 接口标识符用于地址的低 64 位。

```
Console(config)#interface vlan 1
```

```
Console(config-if)#ipv6 address 2001:0DB8:0:1::/64 eui-64

Console(config-if)#end

Console#show ipv6 interface

VLAN 1 is up

IPv6 is enabled

Link-local address:

FE80::2E0:CFF:FE00:FD/64

Global unicast address(es):

2001:DB8::1:2E0:CFF:FE00:FD/64, subnet is 2001:DB8::1:0:0:0:0/64[EUI]

2001:DB8:2222:7272::72/96, subnet is 2001:DB8:2222:7272::/96[EUI]

Joined group address(es):

FF02::1:FF00:72

FF02::1:FF00:FD

FF02::1

IPv6 link MTU is 1500 bytes

ND DAD is enabled, number of DAD attempts: 3.

ND retransmit interval is 1000 milliseconds

ND advertised retransmit interval is 0 milliseconds

ND reachable time is 30000 milliseconds

ND advertised reachable time is 0 milliseconds

Console#
```

29.2.5 ipv6 address link-local

此命令用于配置接口上可扩展 IPv6 的接口的 IPv6 链路本地地址。使用 no 带任何参数的 no 形式从界面中删除所有手动配置的 IPv6 地址。使用带有特定地址的 no 形式将其从界面中删除。

语法

ipv6 address *ipv6-address* **link-local**

no ipv6 address [*ipv6-address* **link-local**]

ipv6-address -分配给接口的 IPv6 地址。

缺省配置

无

命令模式

接口配置 (VLAN)

命令用法

◆必须使用 8 个冒号分隔的 16 位十六进制值根据 RFC 2373“IPv6 Addressing Architecture”格式化指定的地址。可以在地址中使用一个双冒号来指示填充未定义字段所需的零的适当数量。地址前缀必须在 FE80~FEBF 的范围内。

◆使用此命令指定的地址将替换为接口自动生成的链接本地地址。

◆您可以为每个接口配置多个 IPv6 全局单播地址，但每个接口只能配置一个链路本地地址。

◆ 如果检测到重复的地址，则会向控制台发送警告消息。

范例

此示例将链路本地地址 FE80 :: 269：3EF9：FE19：6779 分配给 VLAN 1.请注意，链路本地地址和主机地址中的第一个 16 位组需要 FE80~FEBF 范围内的前缀以 0269 的形式填充零。

```
Console(config)#interface vlan 1

Console(config-if)#ipv6 address FE80::269:3EF9:FE19:6779 link-local

Console(config-if)#end

Console#show ipv6 interface

VLAN 1 is up

IPv6 is enabled

Link-local address:

FE80::269:3EF9:FE19:6779/64

Global unicast address(es):

2001:DB8::1:2E0:CFF:FE00:FD/64, subnet is 2001:DB8::1:0:0:0:0/64[EUI]

2001:DB8:2222:7272::72/96, subnet is 2001:DB8:2222:7272::/96[EUI]

Joined group address(es):

FF02::1:FF19:6779

FF02::1:FF00:72

FF02::1:FF00:FD
```

```
FF02::1

IPv6 link MTU is 1500 bytes

ND DAD is enabled, number of DAD attempts: 3.

ND retransmit interval is 1000 milliseconds

ND advertised retransmit interval is 0 milliseconds

ND reachable time is 30000 milliseconds

ND advertised reachable time is 0 milliseconds

Console#
```

29.2.6 ipv6 enable

此命令在未配置显式 IPv6 地址的接口上启用 IPv6。使用 no 形式在尚未使用显式 IPv6 地址配置的接口上禁用 IPv6 。

语法

[no] ipv6 enable

缺省配置

禁用

命令模式

接口配置 (VLAN)

命令用法

◆此命令在当前 VLAN 接口上启用 IPv6，并自动生成链路本地单播地址。地址前缀 FE80，地址的主机部分是通过将交换机的 MAC 地址转换为修改后的 EUI-64 格式生成的。此地址类型使交换机可通过 IPv6 访问对于连接到同一本地子网的所有设备。

◆如果在本地段上检测到重复的地址，将禁用此接口并在控制台上显示警告消息。

◆已显式配置了 IPv6 地址的接口，是不能用这个 no ipv6 enable 命令禁用的。

范例

在此示例中，在 VLAN 1 上启用 IPv6，并且交换机自动生成链路本地地址 FE80 :: 2E0:CFF:FE00:FD / 64。

```
Console(config)#interface vlan 1

Console(config-if)#ipv6 enable
```

```
Console(config-if)#end

Console#show ipv6 interface

VLAN 1 is up

IPv6 is enabled

Link-local address:

FE80::2E0:CFF:FE00:FD/64

Global unicast address(es):

2001:DB8:2222:7273::72/96, subnet is 2001:DB8:2222:7273::/96

Joined group address(es):

FF02::1:FF00:72

FF02::1:FF00:FD

FF02::1

IPv6 link MTU is 1280 bytes

ND DAD is enabled, number of DAD attempts: 3.

ND retransmit interval is 1000 milliseconds

ND advertised retransmit interval is 0 milliseconds

ND reachable time is 30000 milliseconds

ND advertised reachable time is 0 milliseconds

Console#
```

29.2.7 ipv6 mtu

此命令设置接口上发送的 IPv6 数据包的最大传输单元（MTU）的大小。使用 **no** 形式恢复默认设置。

语法

ipv6 mtu *size*

no ipv6 mtu

size -指定 MTU 大小。（范围：1280-65535 字节）

缺省配置

1500 字节

命令模式

接口配置 (VLAN)

命令用法

◆此命令设置的最大值不能超过物理接口的 MTU，当前固定为 1500 字节。

◆ IPv6 路由器不会分割从其他路由器转发的 IPv6 数据包。但是源自连接到 IPv6 路由器的终端站的流量可能会碎片化。

◆ 同一物理介质上的所有设备必须使用相同的 MTU 才能正常运行。

◆必须先在接口上启用 IPv6，然后才能设置 MTU。

范例

以下示例将 VLAN 1 的 MTU 设置为 1280 字节：

```
Console(config)#interface vlan 1

Console(config-if)#ipv6 mtu 1280

Console(config-if)#
```

29.2.8 show ipv6 default-gateway

此命令显示当前的 IPv6 默认网关。

命令模式

普通模式，特权模式

范例

以下显示为此设备配置的默认网关：

```
Console#show ipv6 default-gateway

IPv6 default gateway 2001:DB8:2222:7272::254

Console#
```

29.2.9 show ipv6 interface

此命令显示 IPv6 接口的可用性和已配置设置。

语法

show ipv6 interface [**brief** [**vlan** *vlan-id* [*ipv6-prefix/prefix-length*]]]

brief -显示 IPv6 操作状态的简要摘要以及为每个接口配置的地址。

vlan-id - VLAN ID (范围: 1-4093)

ipv6-prefix -分配给接口的地址的 IPv6 网络部分。必须使用 8 个冒号分隔的 16 位十六进制值根据 RFC 2373“IPv6 寻址体系结构”格式化前缀。在 addressto 中可以使用一个双冒号表示填充未定义字段所需的适当零数。

prefix-length -一个十进制值表示地址的多少个连续位(左起)包含前缀(即地址的网络部分)。

命令模式

普通模式, 特权模式

范例

此示例显示为交换机配置的所有 IPv6 地址。

```
Console#show ipv6 interface

VLAN 1 is up

IPv6 is enabled

Link-local address:

FE80::2E0:CFF:FE00:FD/64

Global unicast address(es):

2001:DB8:2222:7273::72/96, subnet is 2001:DB8:2222:7273::/96

Joined group address(es):

FF02::1:FF00:72

FF02::1:FF00:FD

FF02::1

IPv6 link MTU is 1280 bytes

ND DAD is enabled, number of DAD attempts: 3.

ND retransmit interval is 1000 milliseconds

ND advertised retransmit interval is 0 milliseconds

ND reachable time is 30000 milliseconds

ND advertised reachable time is 0 milliseconds

Console#
```

29.2.10 show ipv6 mtu

此命令显示已返回 ICMP 数据包太大消息的目标的最大传输单元（MTU）高速缓存以及可接受的 MTU 到此交换机。

命令模式

普通模式，特权模式

范例

以下示例显示了此设备的 MTU 缓存：

```
Console#show ipv6 mtu

MTU Since Destination Address

1400 00:04:21 5000:1::3

1280 00:04:50 FE80::203:A0FF:FED6:141D

Console#
```

29.2.11 show ipv6 traffic

此命令显示有关通过此交换机的 IPv6 流量的统计信息。

命令模式

普通模式，特权模式

范例

以下示例显示了所有 IPv6 单播和多播流量的统计信息，以及 ICMP，UDP 和 TCP 统计信息：

```
Console#show ipv6 traffic

IPv6 Statistics:

IPv6 received

total received

header errors

too big errors

no routes

address errors

unknown protocols

truncated packets
```

discards

delivers

reassembly request datagrams

reassembly succeeded

reassembly failed

IPv6 sent

forwards datagrams

requests

discards

no routes

generated fragments

fragment succeeded

fragment failed

ICMPv6 Statistics:

ICMPv6 received

input

errors

destination unreachable messages

packet too big messages

time exceeded messages

parameter problem message

echo request messages

echo reply messages

router solicit messages

router advertisement messages

neighbor solicit messages

neighbor advertisement messages

redirect messages

group membership query messages

group membership response messages

```
group membership reduction messages

multicast listener discovery version 2 reports

ICMPv6 sent

output

destination unreachable messages

packet too big messages

time exceeded messages

parameter problem message

echo request messages

echo reply messages

router solicit messages

router advertisement messages

neighbor solicit messages

neighbor advertisement messages

redirect messages

group membership query messages

group membership response messages

group membership reduction messages

multicast listener discovery version 2 reports

UDP Statistics:

input

no port errors

other errors

output

Console#
```

29.2.12 clear ipv6 traffic

此命令重置 IPv6 流量计数器。

命令模式

特权模式

命令用法

此命令重置 show ipv6 traffic 命令显示的所有计数器。

范例

```
Console#clear ipv6 traffic

Console#
```

29.2.13 ping6

此命令将（IPv6）ICMP 回送请求数据包发送到网络上的另一个节点。

语法

ping6 {*ipv6-address* | *host-name*} [**count** *count*] [**size** *size*]

ipv6-address -邻居设备的 IPv6 地址。您可以使用 8colon 分隔的 16 位十六进制值来指定根据 RFC 2373“IPv6 寻址体系结构”格式化的链接本地或全球单播地址。可以在地址中使用一个双冒号来指示填充未定义字段所需的零的适当数量。

host-name -主机名字符串，可通过域名服务器解析为 IPv6 地址。

count -要发送的数据包数。（范围：1-16）

size-数据包中的字节数。(范围：48-18024 字节)实际数据包大小将比指定的大小大 8 个字节，因为路由器添加了标头信息。

缺省配置

计数：5

大小：100 字节

命令模式

特权模式

命令用法

◆使用 **ping6** 命令查看是否可以访问网络上的其他站点或者评估路径上的延迟。

◆不同区域（RFC 4007）中的不同接口/节点可以使用相同的链路本地地址。因此在指定链路本地地址时，请在%分隔符后包含指示 VLAN 标识符的 zone-id 信息。例如 FE80::7272%1 将 VLAN 1 识别为发送 ping 的接口。

◆在 ping 主机名时请确保已启用 DNS 服务器。如有必要还可以在 DNS 静态主机表中指定本地设

备。

◆将 ping6 与主机名一起使用时，交换机首先尝试将别名解析为 IPv6 地址，然后再尝试将其解析为 IP 地址。

范例

```
Console#ping6 FE80::2E0:CFF:FE00:FC%1/64

Type ESC to abort.

PING to FE80::2E0:CFF:FE00:FC%1/64, by 5 32-byte payload ICMP packets,

timeout is 3 seconds

response time: 20 ms [FE80::2E0:CFF:FE00:FC] seq_no: 1

response time: 0 ms [FE80::2E0:CFF:FE00:FC] seq_no: 2

response time: 0 ms [FE80::2E0:CFF:FE00:FC] seq_no: 3

response time: 0 ms [FE80::2E0:CFF:FE00:FC] seq_no: 4

response time: 0 ms [FE80::2E0:CFF:FE00:FC] seq_no: 5

Ping statistics for FE80::2E0:CFF:FE00:FC%1/64:

5 packets transmitted, 5 packets received (100%), 0 packets lost (0%)

Approximate round trip times:

Minimum = 0 ms, Maximum = 20 ms, Average = 4 ms

Console#
```

29.2.14 traceroute6

此命令显示路由数据包到达指定目标。

语法

traceroute {*ipv6-address* | *host-name*}

ipv6-address -邻居设备的 IPv6 地址。您可以使用 8 个冒号分隔的 16 位十六进制值来指定根据 RFC 2373“IPv6 寻址体系结构”格式化的链接本地或全球单播地址。可以在地址中使用一个双冒号来指示填充未定义字段所需的零个数量。

host-name -主机名字符串，可通过域名服务器解析为 IPv6 地址。

缺省配置

无

命令模式

特权模式

命令用法

◆使用 **traceroute6** 命令确定到达指定目标所用的路径。

◆不同区域（RFC 4007）中的不同接口/节点可以使用相同的链路本地地址。因此在指定本地地址链接时，请在％分隔符后包含指示 VLAN i 标识符的 zone-id 信息。例如 FE80 :: 7272％1 将 VLAN 1 识别为发送 ping 的接口。

◆当目标响应，超出最大超时（TTL）或超过最大跳数时跟踪终止。

◆traceroute 命令首先发送探测数据报，TTL 值设置为 1。这会导致第一个路由器丢弃数据语法返回错误的消息。跟踪功能然后在每个后续 TTL 级别发送多个探测消息，并显示每条消息的往返时间。并非所有设备都通过返回“ICMP 端口不可达”消息正确响应探测。如果在返回响应之前计时器关闭，则跟踪功能会打印一系列的磁盘和“请求超时”消息。这些消息的长序列仅在达到最大超时时终止，可能表明目标设备存在此问题。

范例

```
Console#traceroute6 FE80::2E0:CFF:FE9C:CA10%1/64

Press "ESC" to abort.

Traceroute to FE80::2E0:CFF:FE9C:CA10%1/64, 30 hops max, timeout is 3

seconds, 5 max failure(s) before termination.

Hop Packet 1 Packet 2 Packet 3 IPv6 Address

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

1 <10 ms <10 ms <10 ms FE80::2E0:CFF:FE9C:CA10%1/64

Trace completed.

Console#
```

29.2.15 ipv6 nd dad attempts

此命令用于配置重复地址检测过程中接口上发送的连续邻居请求消息的数量。使用 **no** 形式恢复默认设置。

语法

ipv6 nd dad attempts *count*

no ipv6 nd dad attempts

count -发送的邻居请求消息的数量，用于确定此接口上是否存在重复地址。（范围：0-600）

缺省配置

3

命令模式

接口配置 (VLAN)

命令用法

◆配置值 0 禁用重复地址检测。

◆重复地址检测确定在将新的单播 IPv6 地址分配给接口之前是否已存在新的单播 IPv6 地址。

◆在已暂停的任何接口上停止重复地址检测（请参阅 vlan 命令）。当接口挂起时，分配给该接口的所有单播 IPv6 地址都处于“挂起”状态。在管理上重新激活接口时，将自动重新启动重复地址检测。

◆重新激活的接口重新启动接口上的重复地址检测单播 IPv6 地址。虽然在接口的链路本地地址上执行重复地址检测，但其他 IP 地址仍处于“暂定”状态。 如果未找到重复的本地地址链接，则会为剩余的 IPv6 地址启动重复地址检测。

◆如果检测到重复地址，则将其设置为“重复”状态，并将警告消息发送到控制台。如果检测到重复的链路地址，则在该接口上禁用 IPv6 进程。如果检测到复制全局单播地址，则不使用它。 当地址处于“重复”状态时，与重复地址关联的所有配置命令仍保持配置状态。

◆如果更改了接口的链路本地地址，则会对新的链路本地地址执行重复的地址检测，但不会对已与该接口关联的任何 IPv6 全球单播地址执行重复的地址检测。

范例

以下配置在 VLAN 1 上配置的地址的五个邻居请求尝试 show ipv6 interface 命令指示重复地址检测过程仍在进行中。

```
Console(config)#interface vlan 1

Console(config-if)#ipv6 nd dad attempts 5

Console(config-if)#end

Console#show ipv6 interface

VLAN 1 is up

IPv6 is enabled

Link-local address:

FE80::200:E8FF:FE90:0/64

Global unicast address(es):

2009:DB9:2229::79, subnet is 2009:DB9:2229:0::/64
```

```
Joined group address(es):

FF01::1/16

FF02::1/16

FF02::1:FF00:79/104

FF02::1:FF90:0/104

IPv6 link MTU is 1500 bytes.

ND DAD is enabled, number of DAD attempts: 5.

ND retransmit interval is 1000 milliseconds

ND advertised retransmit interval is 0 milliseconds

ND reachable time is 30000 milliseconds

ND advertised reachable time is 0 milliseconds

Console#
```

29.2.16 ipv6 nd ns-interval

此命令用于配置接口上发送 IPv6 邻居选择消息的时间间隔。使用 no 形式恢复默认值。

语法

ipv6 nd ns-interval *milliseconds*

no ipv6 nd ns-interval

milliseconds -传输 IPv6 邻居选择消息之间的间隔。（范围：1000-3600000）

缺省配置

1000 毫秒用于邻居发现操作

命令模式

接口配置 (VLAN)

命令用法

◆ 此命令指定解析地址时或在探测邻居可达性时发送邻居消息的间隔。因此请避免在正常的 IPv6 操作中使用非常短的间隔。

范例

以下是将邻居请求消息发送到 30000 毫秒之间的时间间隔：

```
Console(config)#interface vlan 1
```

```
Console(config)#pv6 nd ns-interval 30000

Console(config)#end

Console#show ipv6 interface

VLAN 1 is up

IPv6 is enabled

Link-local address:

FE80::200:E8FF:FE90:0/64

Global unicast address(es):

2009:DB9:2229::79, subnet is 2009:DB9:2229:0::/64

Joined group address(es):

FF01::1/16

FF02::1/16

FF02::1:FF00:79/104

FF02::1:FF90:0/104

IPv6 link MTU is 1500 bytes.

ND DAD is enabled, number of DAD attempts: 5.

ND retransmit interval is 1000 milliseconds

ND advertised retransmit interval is 0 milliseconds

ND reachable time is 30000 milliseconds

ND advertised reachable time is 0 milliseconds

Console#
```

29.2.17 ipv6 nd raguard

此命令阻止传入的路由器通告和路由器重定向包。使用 no 形式禁用此功能。

语法

[no] ipv6 nd raguard

缺省配置

禁用

命令模式

接口配置（Ethernet, Port Channel）

命令用法

◆IPv6 路由器通告（RA）传达信息，使节点能够在网络上自动配置。该信息可以包括从 RA 消息的观察源地址获取的默认路由器地址，以及链接前缀信息。然而，无意识的配置，或者可能对网络的恶意攻击，可能导致发送虚假的 RA，这反过来又会给网络上的主机造成操作问题。

◆ 此命令可用于阻止指定接口上的 RA 和路由器重定向（RR）消息。确定哪些接口连接到已知路由器，并在所有其他不可信接口上启用 RA Guard。

范例

```
Console(config)#interface ethernet 1/1
Console(config-if)#pv6 nd raguard
Console(config-if)#
```

29.2.18 ipv6 nd reachable-time

此命令配置在发生某些可达性确认事件后，可以认为远程 IPv6 节点可以访问的时间量。

语法

ipv6 nd reachable-time *milliseconds*

no ipv6 nd reachable-time

milliseconds -接收到可达性确认后，可以认为节点可达的时间。（范围：0-3600000）

缺省配置

30000 毫秒用于邻居发现操作

命令模式

接口配置（VLAN）

命令用法

◆由这个命令配置的时限允许交换机检测可用邻居。

范例

以下设置远程节点的可达时间为 1000 毫秒：

```
Console(config)#interface vlan 1
```

```
Console(config)#pv6 nd reachable-time 1000

Console(config)#
```

29.2.19 clear ipv6 neighbors

此命令删除 IPv6 邻居 discoverycache 中的所有动态条目。

命令模式

特权模式

范例

以下内容删除 IPv6 邻居缓存中的所有动态条目：

```
Console#clear ipv6 neighbors

Console#
```

29.2.20 show ipv6 ndraguard

此命令显示 RA Guard 的配置设置。

语法

show ipv6 nd raguard [*interface*]

interface

ethernet *单元 / 端口*

unit - 单位标识符。 （范围：1）

port - 端口号。 （范围：1-28）

port-channel *channel-id* (范围: 1-12)

命令模式

特权模式

范例

```
Console#show ipv6 nd raguard interface ethernet 1/1

Interface RA Guard

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

Eth 1/ 1 Yes

Console#
```

29.2.21 show ipv6 neighbors

此命令显示 IPv6 邻居发现缓存中的信息。

语法

show ipv6 neighbors [**vlan** *vlan-id* | *ipv6-address*]

vlan-id - VLAN ID (范围: 1-4093)

ipv6-address -邻居设备的 IPv6 地址。您可以使用 8 个冒号分隔的 16 位十六进制值来指定根据 RFC 2373 “IPv6 寻址体系结构”格式化的链接本地或全球单播地址。 可以在地址中使用一个双冒号来指示填充未定义字段所需的适当数量的零。

缺省配置

将显示所有 IPv6 邻居发现缓存条目。

命令模式

特权模式

范例

以下显示了此交换机的所有已知 IPv6 邻居：

```
Console#show ipv6 neighbors

State: I1 - Incomplete, I2 - Invalid, R - Reachable, S - Stale, D - Delay,

P1 - Probe, P2 - Permanent, U - Unknown

IPv6 Address Age Link-layer Addr State VLAN

FE80::2E0:CFF:FE9C:CA10 4 00-E0-0C-9C-CA-10 R 1

Console#
```

30 RIP 命令

30.1.1 router rip

此命令为进入 RIP 配置，同时使能 rip。使用“no”形式禁用它。

语法

[no] router rip

命令模式

全局配置

缺省配置

禁用

命令用法

◆RIP 用于指定路由器如何交换路由表信息。

◆此命令还用于输入路由器配置模式。

范例

Console(config)#router rip

Console(config-router)#

30.1.2 default-information originate

此命令在本地 RIP 自治系统中生成默认外部路由。使用“no”形式禁用此功能。

语法

[no] default -information originate

缺省配置

禁用

命令模式

路由配置

命令用法

此命令为每个启用 RIP 的第 3 层接口设置默认路由。外部查询的响应包将每个活动的 RIP 接口标记为 IP 地址为 0.0.0.0 的默认路由器。

范例

```
Console(config-router)#default-information originate
Console(config-router)#
```

30.1.3 default-metric

此命令设置分配给从其他协议导入的外部路由的默认度量值。使用“no”形式还原默认值。

语法

default-metric *metric-value*

no default-metric

metric-value - 分配给外部路由的度量。（范围：1-15）

缺省配置

1

命令模式

路由配置

命令用法

◆此命令不重写由重新分配命令设置的度量值。当重新分发命令没有配置度量值时，默认 default-metric 命令设置要用于所有导入的外部路由的度量值。

◆必须使用默认度量来解决用不兼容度量重新分配外部路由的问题。

◆建议在重新分配路由时使用低度量。协议到 RIP。使用高度量限制外部路由的有用性重新分配到 RIP。例如，如果为重新分配定义了 10 的度量路线，这些路线只能宣传到路由器多达 5 跳，

在该度量超过 15 的最大跳数。通过定义一个 1 的低度量，交通可以遵循进口路线的最大数量在 RIP 域内允许跳变。然而，请注意，使用低度量 CAN 增加路由循环的可能性，例如，这可能发生，如果有多个重新分配点和路由器学习相同的外部网络具有更好的度量从除此之外的重新分配点源于原始来源。

范例

此示例将默认度量设置为 5。

```
Console(config-router)#default-metric 5

Console(config-router)#
```

30.1.4 distance

此命令定义了从其他路由协议中学习到的路由的管理距离。使用“no”形式还原默认设置。

语法

[no] distance *distance network-address netmask*

distance – 外部路由的管理距离。外部路由是从 RIP 自治系统外学习的路由。距离为 255 的路线不学习在路由表中。（范围：1-255）

network-address –路由条目的 IP 地址。

netmask –路由的网络掩码。此掩码标识网络。用于相关路由条目的地址位。

缺省配置

无

命令模式

路由配置

命令用法

◆路由器使用管理距离来选择首选路径。当到同一目的地有不同路由协议学习到的路由，较小的管理距离的路由协议学习到的路由，将被优先采用进行转发。

◆管理距离应用于指定的所有路由网络。

范例

```
Console(config-router)#distance 2 192.168.3.0 255.255.255.0

Console(config-router)#
```

30.1.5 maximum-prefix

此命令设置系统允许的最大 RIP 路由数。使用“no”形式恢复默认设置。

语法

maximum-prefix *maximum-routes*

no maximum-prefix

maximum-routes -最大可能的 RIP 路由数安装在路由表中。（范围：1-11766）

缺省配置

11766

命令模式

路由配置

命令用法

所有学习的RIP路由可能不被复制到ASIC的硬件表中由于硬件资源的限制而进行数据转发。

范例

```
Console(config-router)#maximum-prefix 1024

Console(config-router)#
```

30.1.6 neighbor

此命令定义了路由器的邻居。使用“no”形式删除条目。

语法

[no] **neighbor** *ip-address*

ip-address -相邻路由器的 IP 地址。

缺省配置

没有邻居定义。

命令模式

路由配置

命令用法

◆此命令可用于配置静态邻居（特别是针对点到点链接），路由器将与其交换路由信息，而不是依靠 RIP 协议生成的广播或多播消息。

◆与被动接口命令一起使用此命令控制发送给特定邻居的路由更新。

范例

```
Console(config-router)#neighbor 10.2.0.254

Console(config-router)#
```

30.1.7 network

此命令指定将包含在 RIP 中的网络接口。使用“no”形式删除条目。

语法

[no] **network** {*ip-address netmask* | **vlan** *vlan-id*}

ip-address - 直接连接到该路由器的网络的 IP 地址。

netmask -路由的网络掩码。

vlan-id - VLAN ID. (范围: 1-4094)

缺省配置

没有指定网络。

命令模式

路由配置

命令用法

◆RIP 只发送和接收由该命令指定的接口上的更新。如果未指定网络，则该网络中的接口将不会在任何 RIP 更新中被公告。

◆子网地址被解释为类 A、B 或 C，基于指定地址。换句话说，如果输入了子网地址 nnn.xx.xx.xxx，第一个字段（NNN）决定类：

0 - 127 是 A 类，只使用网络地址中的第一个字段。

128 - 191 是 B 类，并且使用网络地址中的前两个字段。

192 - 223 是 C 类，并且使用网络地址中的前三个字段。

范例

此示例包括 RIP 路由过程中的网络接口（1.1.0.0）。

```
Console(config-router)#network 10.1.0.0
Console(config-router)#
```

30.1.8 passive-interface

此命令阻止 RIP 在指定接口上发送路由更新。使用“no”形式禁用此功能。

语法

[no] **passive-interface vlan** *vlan-id*

vlan-id - VLAN ID. (Range: 1-4094)

缺省配置

禁用

命令模式

路由配置

命令用法

◆如果此命令用于停止在接口上发送路由更新，则附属子网仍将继续被广告到其他接口，以及将继续接收来自该接口上其他路由器的更新和处理。

◆与邻居命令一起使用此命令来控制路由更新发送到特定的邻居。

范例

```
Console(config-router)#passive-interface vlan1
Console(config-router)#
```

30.1.9 redistribute

此命令将外部路由信息从其他路由域（即，直接连接的路由、协议或静态路由）导入 RIP。使用“no”形式禁用此功能。

语法

[no] **redistribute** {**bgp** | **connected** | **ospf** | **static**} [**metric** *metric-value*]

bgp -将从边界网关协议导入外部路由（BGP）进入这个路由域。

connected -自动导入的路由在接口上启用 IP。

ospf -外部路由将从开放最短路径导入（OSPF）协议进入这个路由域。

static -静态路由将被导入到这个路由域中。

metric-value -赋值给指定的所有外部路由的度量值协议。（范围：1-16）

缺省配置

再分配- 无

度量值-由默认度量命令设置

命令模式

路由配置

命令用法

◆当重新分发命令没有配置度量值时，默认度量命令设置要用于所有导入的外部路由的度量值。

◆必须使用路由度量来解决不兼容度量重新分配外部路由的问题。

◆建议在从另一协议重新分配路由到 RIP 时使用低度量。使用高度量限制重新路由到 RIP 的外部路由的有用性。例如，如果为重新分配的路由定义了 10 度量，则这些路由只能通告到最多 5 跳远的路由器，此时该度量超过最大跳数 15。通过定义 1 的低度量，流量可以遵循导入的路由，RIP 域内允许的最大跳数。然而，使用低度量可以增加路由循环的可能性。例如，如果存在多个重新分配点，并且路由器从除了从原始源导出的度量之外的重新分配点学习具有更好度量的相同外部网络，则可能出现这种情况。

范例

此示例重新分发从 OSPF 学习的路由，并将从 OSPF 导入的所有外部路由的度量设置为 3。

```
Console(config-router)#redistribute ospf metric 3

Console(config-router)#
```

此示例重新分配静态路由并将所有这些路由的度量设置为 3 的值。

```
Console(config-router)#redistribute static metric 3

Console(config-router)#
```

30.1.10 timers basic

该命令用来配置 RIP 更新定时器，超时定时器和垃圾收集定时器。使用 no 形式恢复默认值。

语法

timers basic *update timeout garbage*

no timers basic

update - 将更新计时器设置为指定值。（范围：5-2147483647 秒）

timeout - 将超时计时器设置为指定值。 （范围：90-360 秒）

garbage - 将丢弃收集计时器设置为指定的值。

缺省配置

Update: 30 秒

Timeout: 180 秒

Garbage collection: 120 秒

命令模式

路由配置

命令用法

◆*更新* 计时器设置在其更新的发送速率。这是用于控制所有基本 RIP 进程的基本计时器。

◆超时定时器是在没有更新消息的情况下路由被宣告死亡的时间。该路径被标记为不可访问（即，度量设置为无穷大），并被广告为不可达。然而，分组仍在这条路线上转发。

◆在超时时间间隔过期之后，路由器在从路由表中删除该条目之前等待丢弃收集计时器指定的时间间隔。该定时器允许邻居在该设备被清除之前知道一条无效路由。

◆将更新计时器设置为短时间间隔会导致路由器花费过多的时间处理更新。

◆对于网络中的所有路由器，这些计时器必须设置为相同的值。

范例

此示例将更新计时器设置为 40 秒。　超时计时器是随后设置为 240 秒，丢弃收集计时器为 160 秒。

```
Console(config-router)#timers basic 15

Console(config-router)#
```

30.1.11 version

该命令指定路由器全局使用的 RIP 版本。使用 no 形式恢复默认值。

语法

version {1 | 2}

no version

1 - RIP Version 1

2 - RIP Version 2

缺省配置

Receive: 接受 RIPv1 或 RIPv2 数据包

Send: 路由信息通过 RIPv2 广播到其他路由器。

命令模式

路由配置

命令用法

◆使用此命令指定全局 RIP 版本时，任何 VLAN 接口以前没有通过 ip rip receive-version 或 ip rip send version 命令设置将使用全局 RIP 版本设置。

◆当使用此命令 的 no 形式恢复默认值时，任何以前没有通过 ip rip receive version 或 ip rip send version 设置的 VLAN 接口版本命令将设置为默认的发送或接收版本。

◆任何已配置的接口设置优先于全局设置。

范例

此示例设置 RIP 的全局版本以发送和接收版本 2 数据包。

```
Console(config-router)#version 2

Console(config-router)#
```

30.1.12 ip rip authentication mode

此命令指定可用于 RIPv2 的身份验证类型数据包。使用 no 形式恢复默认值。

语法

ip rip authentication mode {md5 | text}

no ip rip authentication mode

md5 -消息摘要 5（MD5）身份验证

text -表示将使用简单密码。

缺省配置

Text 身份验证

命令模式

接口配置 (VLAN)

命令用法

◆用于身份验证的密码在 ip rip authentication string 命令。

◆这个命令需要接口来交换路由信息。其他基于授权口令的路由器。(注意仅此命令）适用于 RIPv2。

◆对于认证功能正常，发送和接收必须使用相同的密码或身份验证密钥配置接口。

◆MD5 是一种单向哈希算法,它采用认证密钥和产生一个 128 位的消息摘要或“指纹”。这就是它在计算上不可行地产生具有相同消息的两个消息摘要，或产生具有给定预先指定的目标消息的任何消息消化。

范例

此示例将身份验证模式设置为纯文本。

```
Console(config)#interface vlan 1
```

```
Console(config-if)#ip rip authentication mode text

Console(config-if)#
```

30.1.13 ip rip authentication string

此命令指定 RIPv2 数据包的身份验证密钥。使用 no 形式删除身份验证密钥。

语法

ip rip authentication string *key-string*

no ip rip authentication string

key-string -用于身份验证的密码。（范围：1-16 个字符，区分大小写）

缺省配置

没有验证密钥

命令模式

接口配置 (VLAN)

命令用法

◆此命令可用于限制可以交换 RIPv2 的接口路由信息。 （请注意，此命令不适用于 RIPv1。）

◆对于认证功能正常，发送和接收必须使用相同的密码和身份验证配置接口通过 ip rip authentication mode 命令启用。

范例

此示例将身份验证密码设置为“small”以验证传入路由消息和标记传出路由消息。

```
Console(config)#interface vlan 1

Console(config-if)#ip rip authentication string small

Console(config-if)#
```

30.1.14 ip rip receive version

此命令指定要在接口上接收的 RIP 版本。使用 no 形式恢复默认值。

语法

ip rip receive version {1 | 2}

no ip rip receive version

1 -仅接受 RIPv1 数据包。

2 -仅接受 RIPv2 数据包。

缺省配置

RIPv1 和 RIPv2 报文

命令模式

接口配置 (VLAN)

命令用法

◆使用此命令覆盖由 RIP 版本指定的全局设置命令。

◆您可以根据以下选项指定接收版本：

■请将网络中的路由器配置相同版版本。

■如果本地网络中的某些路由器使用版本 1 或 2，则使用 RIPv2，但仍有一些使用 RIPv1 的老式路由器。

范例

此示例设置 VLAN 1 的接口版本以接收 RIPv1 数据包。

```
Console(config)#interface vlan 1

Console(config-if)#ip rip receive version 1

Console(config-if)#
```

30.1.15 ip rip receive-packet

该命令用来配置接口接收 RIP 报文。 使用 no 形式禁用此功能。

语法

[no] ip rip receive-packet

缺省配置

启用

命令模式

接口配置 (VLAN)

缺省配置

启用

命令用法

如果不需要添加任何动态条目，请使用此命令的 no 形式接口的路由表。例如当某个接口只有静态路由时。

范例

```
Console(config)#interface vlan 1
Console(config-if)#ip rip receive-packet
Console(config-if)#
```

相关命令

ip rip send version

此命令指定要在接口上发送的 RIP 版本。使用 no 形式恢复默认值。

语法

ip rip send version {1 | 2 | 1-compatible}

no ip rip send version

1 -仅发送 RIPv1 数据包。

2 -仅发送 RIPv2 数据包。

1-compatible - 已广播形式发送 RIPv2 报文。

缺省配置

1-compatible (路由信息通过 RIPv2 广播到其他路由器)

命令模式

接口配置 (VLAN)

命令用法

◆使用此命令覆盖 RIP 版本指定的全局设置命令。

◆您可以根据以下选项指定发送版本：

■如果本地网络中的所有路由器使用版本相同，请使用对应的版本 RIPv1 或 RIPv2。

■使用“1-compatible”通过广播报文发送 RIPv2，而不是组播。（使用此模式允许较旧的 RIPv2 路由器只接收 RIP 广播消息，以接收 RIPv2 报文提供的信息，包括子网掩码，下一跳和认证信息。）

范例

此示例设置 VLAN 1 的接口版本以发送 RIPv1 数据包。

```
Console(config)#interface vlan 1

Console(config-if)#ip rip send version 1

Console(config-if)#
```

30.1.16 ip rip send-packet

该命令用来配置发送 RIP 报文的接口。使用 no 形式禁用此功能。

[no] ip rip send-packet

缺省配置

启用

命令模式

接口配置 (VLAN)

缺省配置

启用

命令用法

此命令的 no 形式允许路由器被动地监视路由连接到网络的其他路由器通告的信息，没有传输任何 RIP 更新。

范例

```
Console(config)#interface vlan 1

Console(config-if)#ip rip send-packet

Console(config-if)#
```

30.1.17 ip rip split-horizon

此命令在接口上启用带毒性的水平分割或反转。使用 no 形式禁用此功能。

语法

ip rip split-horizon [poisoned]

no rip ip split-horizon

poisoned -带毒性逆转的水平分割方式。

命令模式

接口配置 (VLAN)

缺省配置

带毒性的水平分裂

命令用法

◆水平分割从不将路由转发到接收该路由的接口。

◆带毒性逆转的水平分割，会将收到的路由从接收到该路由的接口转发回去，但将距离矢量指标设置为无穷大。（这个提供更快的收敛。）

◆如果使用 no rip ip split-horizon 命令禁用水平分割，并且发生环路时，在路线被认为无法到达之前，路径的跳数可以逐渐增加到无穷大（即 16）。

范例

```
Console(config)#interface vlan 1

Console(config-if)#ip split-horizon poison-reverse

Console(config-if)#
```

30.1.18 clear ip rip route

该命令用于清除 RIP 路由表中的指定数据。

语法

clear ip rip route {*ip-address netmask* | **all** | **connected** | **ospf** | **rip** | **static**}

ip-address -路由条目的 IP 地址。

netmask -路由的网络掩码。 此掩码标识网络用于相关路由条目的地址位。

all -删除路由表中的所有条目。

connected -删除所有当前连接的条目。

ospf -删除通过 Open Shortest Path First 学习的所有条目路由协议。

rip -删除通过路由信息协议学习的所有条目。

static -删除所有静态条目。

缺省配置

无

命令模式

特权模式

命令用法

将此命令与“all”参数一起使用可清除所有路由的 RIP 表。至避免删除整个 RIP 网络，使用 redistribute connected 命令为 RIP 网络引入直连路由。 删除从中学习到的 RIP 路由邻居并保持 RIP 网络完好无损，使用“rip”参数命令（ **clear ip rip route rip** ）。

范例

此示例清除一个特定路由。

```
Console#clear ip rip route 192.168.1.0 255.255.255.0
Console#
```

show ip protocols rip

此命令显示 RIP 进程参数。

命令模式

特权模式

范例

```
Console#show ip protocols rip
```

```
Routing Protocol is "rip"

Sending updates every 30 seconds with +/-5 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:

Default version control: send version by interface set,receive version by

interface set

Interface Send Recv

VLAN1 1-compatible 1 2

Routing for Networks:

10.0.0.0/24

Routing Information Sources:

Gateway Distance Last Update Bad Packets Bad Routes

10.0.0.2 120 00:00:13 0 0

The maximum number of RIP routes allowed: 11766

Distance: Default is 120

Console#
```

30.1.19 show ip rip

此命令显示有关 RIP 路由和配置设置的信息。 使用不带任何关键字的命令显示所有 RIP 路由。

语法

show ip rip [**interface** [**vlan** *vlan-id*]]

interface -显示所有接口或 RIP 配置设置指定的接口。

vlan-id - VLAN ID. (Range: 1-4094)

命令模式

特权模式

范例

```
Console#show ip rip

Codes: R - RIP, Rc - RIP connected, Rs - RIP static,

C - Connected, S - Static, O - OSPF

Network Next Hop Metric From Interface Time

Rc 192.168.0.0/24 1 VLAN1 01:57

Console#show ip rip interface vlan 1

Interface: vlan1

Routing Protocol: RIP

Receive RIPv1 and RIPv2 packets

Send RIPv1 Compatible

Passive interface: Disabled

Authentication mode: (None)

Authentication string: (None)

Split horizon: Enabled with Poisoned Reverse

IP interface address: 192.168.0.2/24

Console#
```

31 OSPFv2

31.1.1 router ospf

此命令为所有 IP 启用开放最短路径优先（OSPFv2）路由路由器上的接口并进入路由器配置模式。 使用 no 形式为所有进程或指定进程禁用 OSPF。

语法

[no] router ospf [*process-id*]

process-id -配置多个路由时必须输入进程 ID 实例。（范围：1-65535;默认值：1）

命令模式

全局配置

缺省配置

没有定义路由进程。

命令用法

◆ OSPF 用于指定路由器如何交换路由表信息。

◆此命令还用于进入路由器配置模式。

◆如果未定义进程 ID，则默认为实例 1。

范例

```
Console(config)#router ospf
```

```
Console(config-router)#
```

31.1.2 compatible rfc1583

此命令使用 RFC 1583（早期 OSPFv2）计算汇总路由成本。使用 RFC 2328（OSPFv2）计算成本 的 no 形式。

语法

[no] compatible rfc1583

命令模式

路由配置

缺省配置

RFC1583 兼容

命令用法

◆启用 RFC 1583 兼容性，用于计算到达同一目的地的多个外部路由之间的 cost。 什么时候禁用，首选项基于路径类型（类型 1 外部路径为优于 2 型外部 path）。

◆OSPF 路由域中的所有路由器都应使用相同的 RFC 进行计算摘要路线。

◆如果区域中有任何 OSPF 路由器交换摘要信息（如，ABR）尚未升级到 OSPFv2，此命令应该在新升级的 OSPFv2 路由器上使用，以确保兼容仍然运行较旧的 OSPFv2 代码的路由器。一旦所有系统都存在升级到较新的 OSPFv2 代码，使用此命令的 no 形式进行恢复兼容 RFC 2328 的所有系统。

范例

```
Console(config-router)#compatible rfc1583

Console(config-router)#
```

31.1.3 default-informationoriginate

此命令生成进入自治系统的默认外部路由。使用 no 形式禁用此功能。

语法

缺省配置-information originate [always] [metric *interface-metric*]

[metric-type *metric-type*]

no 缺省配置-information originate [always | metric | metric-type]

always -始终将自己宣传为本地 AS 的默认外部路由，无论路由器是否具有默认路由。

interface-metric -分配给默认路由的度量标准。（范围：0-16777214）

metric-type -用于通告默认路由的外部链路类型。（选项：类型 1，类型 2）

命令模式

路由配置

缺省配置

禁用

Metric: 20

Metric 类型: 2

命令用法

◆ 如果 未选择 **always** 参数，则路由器只能发布默认值如果已配置为导入外部路由，则进入 AS 的外部路由通过其他路由 协议或静态路由，这样的路由是已知的。（请参阅 redistribute 命令。）

◆默认外部路由的度量标准用于计算路径成本通过 ASBR 从 AS 内的其他路由器传出的流量。

◆使用此命令将路由重新分配到路由域时（即一个自治系统，这个路由器自动成为一个自治系统系统边界路由器（ASBR）。但是默认情况下，ASBR 不会生成到路由域的默认路由。

■如果使用 **always** 关键字，路由器将自行通告为默认值进入 AS 的外部路由，即使实际上没有默认的外部路由存在。要定义默认路由，请使用 ip route 命令。

■如果不使用 **always** 关键字，则 路由器只能通告如果使用 redistribute 命令，则默认外部路由进入 AS 通过 RIP 或静态路由导入外部路由，这种路由是已知的。

◆类型 1 路由通告将内部成本添加到外部路由 meric。类型 2 路由不添加内部成本度量标准。比较类型 2 时如果有多条 2 型路线，内部成本仅用作决胜局有相同的成本。

◆ 此命令不应用于生成存根或的默认路由 NSSA。 要为这些区域类型生成默认路由，请使用 area stub 或 area nssa 命令。

范例

此示例将度量标准 20 分配给广告到的默认外部路由自治系统，将其作为 Type 2 外部指标发送。

```
Console(config-router)# default-information originate metric 20 metric-type 2

Console(config-router)#
```

31.1.4 router-id

此命令在自治系统中为此设备分配唯一的路由器 ID 系统用于当前的 OSPF 进程。 使用 no 形式使用默认的路由识别方法（即最高接口地址）。

语法

router-id *ip-address*

no router-id

ip-address -格式化为 IPv4 地址的路由器 ID。

命令模式

路由配置

缺省配置

最高的接口地址

命令用法

◆这个指令设置在路由器中指定的 OSPF 处理的路由器 ID ospf 命令。

◆对于自治系统中的每个路由器，路由器 ID 必须是唯一的。运用基于最高接口地址的默认设置可确保每个地址路由器 ID 是唯一的。（请注意路由器 ID 不能设置为 255.255.255.255。）

◆如果此路由器已经注册了邻居，路由器重新启动时将使用新的路由器 ID，或进入无 OSPF 的路由器使用 OSPF 命令手动重新启动。

◆如果路由器的优先级值是指定的路由器或一个区域的备份指定路由器是相同的，具有最高 ID 的路由器是当选。

范例

```
Console(config-router)#router-id 10.1.1.1
```

```
Console(config-router)#
```

31.1.5 timers spf

此命令在接收拓扑更改和启动后配置延迟最短路径优先（SPF）计算，以及两个之间的保持时间连续的 SPF 计算。 使用 no 形式恢复默认值。

语法

timers spf *spf-delay spf-holdtime*

no timers spf

spf-delay -接收拓扑更改通知后的延迟和开始 SPF 计算。（范围：0-2147483647 秒）

spf-holdtime -两次连续 SPF 计算之间的最短时间。（范围：0-2147483647 秒）

命令模式

路由配置

缺省配置

SPF 延迟：5 秒

SPF 保持时间：10 秒

命令用法

◆将 SPF 保持时间设置为 0 表示两者之间没有延迟连续计算。

◆使用较低的值可以 使路由器更快地切换到新路径，但会使用更多的 CPU 处理时间

范例

```
Console(config-router)#timers spf 20
Console(config-router)#
```

31.1.6 clear ip ospf process

此命令清除并重新启动 OSPF 路由进程。指定进程 ID 清除特定的 OSPF 进程。如果未指定进程 ID，则此命令清除所有正在运行的 OSPF 进程。

语法

clear ip ospf [*process-id*] **process**

process-id -指定路由进程 ID。（范围：1-65535）

缺省配置

清除所有路由进程

命令模式

特权模式

范例

```
Console#clear ip ospf process

Console#
```

31.1.7 area default-cost

此命令指定 ABR 发布到 stub 或 NSSA 区域的汇聚路由的 cost 值。使用 **no** 形式删除。

语法

area *area-id* **default-cost** *cost*

no area *area-id* **default-cost**

area-id -标识存根或 NSSA。（区域 ID 可以是一个 IPv4 地址或作为四个八位字节的无符号整数 0-4294967295）。

cost -发送到存根或 NSSA 的默认汇总路由的开销。（范围：0-16777215）

命令模式

路由配置

缺省配置

缺省配置开销：1

命令用法

◆如果默认开销设置为“0”，则路由器不会将默认路由通告给附属的 stub 或 NSSA。

范例

```
Console(config-router)#area 10.3.9.0 default-cost 10

Console(config-router)#
```

31.1.8 area range

该命令将 ABR 发布的路由进行汇聚。使用 no 形式禁用此功能。

语法

[no] area *area-id* range *ip-address* netmask [advertise | not-advertise]

area-id -标识路由汇总的区域。 区域 ID 可以是 IPv4 地址的形式，也可以是四个八位字节的无符号整数范围从 0-4294967295。

ip-address -要汇总的路由的基址。

netmask -摘要路由的网络掩码。

advertise -摘要路由的网络掩码。

not-advertise -不发送摘要，路由保持隐藏状态来自网络的其他部分。

命令模式

路由配置

缺省配置

禁用

命令用法

◆此命令可用于汇总区域内路由，并通过区域边界路由器（ABR）向其他区域传播。

◆ 如果区域内的网络地址是以连续方式分配的，ABR 可以通告一条汇聚路由，覆盖所有这些地址。

◆ 如果设置此功能，则路由器将发出类型 3 LSA。

◆ 此路由器支持 64 个区域范围汇总路由。

范例

此示例为 10.2.xx 范围内的所有区域路由创建汇总地址

```
Console(config-router)#area 10.2.0.0 range 10.2.0.0 255.255.0.0 advertise

Console(config-router)#
```

31.1.9 auto-costreference-bandwidth

使用此命令可基于计算接口的默认度量标准带宽。 使用 no 形式根据接口类型自动分配成本。

语法

auto-cost reference-bandwidth *reference-value*

no auto-cost reference-bandwidth

reference-value -接口带宽。 （范围：1-4294967 Mbps）

命令模式

路由配置

缺省配置

1 Mbps

命令用法

◆系统通过计算 cost 来区分接口。 默认情况下，所有端口类型的 cost 都是 1 Mbps（包括 100 Mbps、千兆端口、万兆端口）。

◆可以使用更高的参考带宽来指示聚合链路 cost 更低。

◆该 ip ospf cost 命令覆盖由自动计算成本的成本 reference-bandwidth 命令。

范例

此示例将参考值设置为 10000，这样 100 Mbps 端口的 cost 为 100，1 Gbps 端口的 cost 为 10，10 Gbps 端口的 cost 为 100。

```
Console(config-router)#auto-cost reference-bandwidth 10000

Console(config-router)#
```

31.1.10 default-metric

此命令设置从其他路由导入的外部路由的默认度量标准协议。使用 no 形式删除支持的协议的默认度量标准类型。

语法

缺省配置-metric *metric-value*

no 缺省配置-metric

metric-value - 分配给从其他路由导入的所有外部路由的度量标准协议。（范围：0-16777214）

命令模式

路由配置

缺省配置

20

命令用法

◆必须使用默认度量标准来解决重新分发问题来自使用不兼容指标的其他协议的外部路由。

◆ 此命令不重写由重新分配命令设置的度量值。当重新分发命令没有配置度量值时，默认度量命令设置要用于所有导入的外部路由的度量值。

范例

```
Console(config-router)#default-metric 100

Console(config-router)#
```

31.1.11 redistribute

此命令将其他协议的路由重发布到 OSPF 自治系统。使用 no 形式禁用此功能或恢复默认设置。

语法

redistribute {**bgp** | **connected** | **rip** | **static**} [**metric** *metric-value*] [**metric-type** *type-value*] [**tag** *tag-value*]

no redistribute {**bgp** | **connected** | **static**} [**metric**] [**metric-type**] [**tag**]

connected -导入所有当前连接的条目。

rip -导入 RIP 学习到的路由。

static -静态路由将导入此自治系统。

metric-value-分配给指定的所有外部路由的度量标准协议。（范围：0-16777214：默认值：10）

cost 计算类型：

1 -类型 1 外部路由

2 -类型 2 外部路由（默认）-cost 不包含到 ASBR 的区域内部开销。

tag-value -放置在 AS 外部 LSA 中的标记，用于标识特定的外部路由域，或在路由器之间传递附加信息。（范围：0-4294967295）

命令模式

路由配置

缺省配置

redistribution - 无

metric-value - 10

type-metric - 2

命令用法

◆该命令用于导入从其他路由协议学到的路由进入 OSPF 域，并生成 AS-external-LSA。

◆将外部路由重新分配到 OSPF 自治系统（AS）时，路由器自动成为自治系统边界路由器 （ASBR）。如果 **redistribute** 命令与 defaultinformation originate 命令 一起使用 ，则生成一个“默认”外部路由 AS，此命令中指定的度量标准值将取代指定的度量标准在 default-information originate 命令中。

◆度量标准类型指定向 AS 外部目标通告路由的方式

通过外部 LSA。 当路由器收到 Type 1 LSA 时，它会添加外部路由度量的内部成本。 换句话说，路线的成本来自 AS 内的 任何路径 都等于与达到该路径相关的成本广告 ASBR，加上外部路线的费用。 当 Type 2 LSA 是由路由器接收，它仅使用外部路由度量来确定路由成本。

◆标签可用于区分从不同协议学到的路由。例如，如果有的区域中有两个 ASBR：A 和 B. ASBR A 从 RIP 域 1 引入的外部路由（标记 1 标识）。ASBR B 从 RIP 域 2 学到的路由（由标记 2 标识）。

范例

此示例将从 RIP 获取的路由重新分配为 Type 1 外部路由。

```
Console(config-router)#redistribute rip metric-type 1
Console(config-router)#
```

31.1.12 summary-address

此命令聚合从其他协议获知的路由。使用 no 形式删除摘要地址。

语法

[no] summary-address *summary-address netmask*

summary-address -涵盖一系列地址*的* 摘要地址。

netmask -摘要路由的网络掩码。

命令模式

路由配置

缺省配置

禁用

命令用法

将其他协议的路由重分配到 OSPF 通常需要路由器在外部 LSA 中单独通告每条路由。自治系统边界路由器（ASBR）可以将学习到的外部路由进行聚合，再将聚合后的路由通告所有附近的自治系统。 这有助于减少外部 LSA 的数量和 OSPF 链路状态数据库大小。

范例

此示例为 192.168.xx 中包含的所有路由创建汇总地址。

```
Console(config-router)#summary-address 192.168.0.0 255.255.0.0

Console(config-router)#
```

31.1.13 Area Configuration

此命令用于启用 OSPF 区域的认证。使用 no 形式删除区域认证。

语法

[no] area *area-id* authentication [message-digest]

area-id -标识要配置身份验证的区域。

区域 ID 可以是 IPv4 地址的形式，也可以是无符号的四个八位字节

整数范围为 0-4294967295。

message-digest -指定消息摘要（MD5）身份验证。

命令模式

路由配置

缺省配置

没有认证

命令用法

◆使用身份验证来防止路由器无意中加入未授权区域。在同一区域中配置路由器使用相同的密码。同一网络上的所有相邻路由器使用相同的密码，才能交换路由数据。

◆配置区域认证前，先在三层接口下使用 ip ospf authentication-key 配置密码。这个密码将写入该接口发送的 OSPF 报文头部。可以给每个区域的不同接口配置不同的密码。

◆使用简单密码验证时，密码包含在报文中。收到该报文的路由器，若发现密码与自己接口的不匹配，则丢弃该报文。

◆使用 Message-Digest 5（MD5）身份验证时，路由器会使用特定的算法计算出密码。

◆在为区域指定 MD5 身份验证之前，请使用 ip ospf message-digest-key 接口命令配置 messagedigest key-id 和 key 。

◆纯文本认证键或 *键 MD5-id* 和密钥 ，必须在整个自治系统统一配置。

范例

此示例为指定区域启用消息摘要式身份验证。

```
Console(config-router)#area 10.3.0.0 authentication

Console(config-router)#
```

31.1.14 area nssa

此命令定义了一个 not-so-stubby 的区域（NSSA）。 要删除 NSSA，请使用 no 形式，并不带任何可选关键字。 要删除可选属性，请使用 no 加上对应关键字。

语法

[no] area *area-id* nssa

[translator-role [candidate | never | always]] |

[no-redistribution] | [no-summary] | [default-information-originate

[metric *metric-value* | metric-type *type-value*]]

area-id -标识 NSSA。区域 ID 可以是 IPv4 的形式地址或四字节无符号整数，范围为 0-4294967295。

translator-role -表示 Type 5 外部的 NSSA-ABR 转换器角色的 LSA。

candidate -如果是，则将 NSSA LSA 转换为 Type-5 外部 LSA。

never -路由器永远不会将 NSSA LSA 转换为 Type-5 外部 LSA。

always -路由器始终将 NSSA LSA 转换为 Type-5 外部 LSA。

no-redistribution - 该命令禁止 NSSA 区域的边界路由器（ABR）引入外部路由到本 NSSA。

no-summary -允许区域保留标准 NSSA 功能，但不引入区域间路由到该区域。

default-information-originate -当路由器是 NSSA 区域边界路由器（ABR）或 NSSA 自治系统边界路由器（ASBR），这个参数使其在 NSSA 中生成 Type-7 默认 LSA。 这个缺省为 NSSA ABR 提供到 AS 内其他区域或 AS 外的路由。

metric-value -分配给 Type-7 默认 LSA 的 **度量标准**。（范围：1-16777214：默认值：1）

类型值

1 -类型 1 外部路由

2 -类型 2 外部路由（默认）-路由器不添加区域内部路由度量。

命令模式

路由配置

缺省配置

无

命令用法

◆NSSA 中的所有路由器必须配置相同的区域 ID。

◆ NSSA 类似存根区域，ABR 可以使用 **default information-originate** 命令，引入一条默认路由到 NSSA 区域，目的为 AS 中其他区域的数据都走该默认路由。但是 NSSA 与存根不同，因为当路由器是 ASBR 时，它可以使用 **default-information-originate** 引入默认的外部 AS 路由（用于 NSSA 区域与 AS 系统外的路由）。

◆发布到到 NSSA 的外部路由可以包括直连路由、默认路由、静态路由、其他动态路由协议学习到的路由。

◆NSSA 外部 LSA（类型 7）由与 NSSA 相邻的任何 ABR 转换为外部 LSA（Type-5），并传

播到 AS 内的其他区域。

◆另请注意，与存根区域不同，始终导入所有 Type-3 类 LSA 进入 NSSA，以确保优先选择内部路由，而不是 Type-7 NSSA 外部路线。

◆此路由器最多可支持 16 个区域（正常传输区域，存根或 NSSA 区域）。

范例

此示例创建一个 NSSA 区域 10.3.0.0，并为所有接口分配 B 类地址为 NSS 的 10.3.xx。 它还指示路由器生成外部 LSA 当它是 NSSA ABR 或 NSSA ASBR 时进入 NSSA。

```
Console(config-router)#area 10.3.0.0 nssa default-information-originate

Console(config-router)#network 10.3.0.0 255.255.0.0 area 10.2.0.0

Console(config-router)#
```

31.1.15 area stub

此命令定义存根区域。要删除存根，请使用不带参数的 no 形式。要删除其他属性，请使用带有关键字的 no 形式命令。

语法

[no] area *area-id* stub [no-summary]

area-id -标识存根区域。区域 ID 可以是 IPv4 的形式地址或四字节无符号整数，范围为 0-4294967295。

no-summary -停止区域边界路由器（ABR）发送摘要将聚合路由发布到存根区域。

命令模式

路由配置

缺省配置

无

聚合路由将发送到存根。

命令用法

◆存根中的所有路由器必须配置相同的区域 ID。

◆存根区域阻止 Type-4 LSA 和 Type 5 发布到本区域。

◆配置 no-summary 参数，其他区域的 3 类汇总 LSA 也不发布到本存根区域。

◆使用 area default-cost 命令指定 ABR 发送到存根区域的路由的开销。

范例

此示例创建一个存根区域 10.2.0.0，并为所有接口分配 B 类 地址为 10.2.xx 到存根。

```
Console(config-router)#area 10.2.0.0 stub

Console(config-router)#network 10.2.0.0 0.255.255.255 area 10.2.0.0

Console(config-router)#
```

31.1.16 area virtual-link

此命令定义虚拟链接。要删除虚拟链接，请使用 no 形式不带可选关键字。要恢复属性的默认值，请使用 no 形式带上对应的关键字。

语法

area *area-id* **virtual-link** *router-id*

[**authentication**] [**dead-interval** *seconds*] [**hello-interval** *seconds*]

[**retransmit-interval** *seconds*] [**transmit-delay** *seconds*]

no area area-id virtual-link *router-id*

[**authentication** | **dead-interval** | **hello-interval** | **retransmit-interval** | **transmit-delay**]

area *area-id* **virtual-link** *router-id*

authentication [**message-digest** | **null**]

[**authentication-key** *key* | **message-digest-key** *key-id* **md5** *key*]

no area *area-id* **virtual-link** *router-id*

authentication [**authentication-key** | **message-digest-key** *key-id*]

area *area-id* **virtual-link** *router-id*

[**authentication-key** *key* | **message-digest-key** *key-id* **md5** *key*]

no area *area-id* **virtual-link** *router-id*

[**authentication-key** | **message-digest-key** *key-id*]

area-id -标识虚拟链路的传输区域。区域 ID 可以是 IPv4 地址的形式或四个八位字节无符号整数范围 从 0-4294967295。

router-id -虚连接邻居的路由器 ID。

dead-interval *seconds* - 等待 dead 时间未收到邻居路由器的 hello 数据包，则删除虚连接。该值各路由器必须配置相等。(范围:1-65535 秒； 默认值:4 x hello interval，或 40 秒)

hello-interval *seconds* -发送 hello 包的间隔时间。 将 hello 包间隔设置为较小的值可以减少拓扑变化的延迟检测，但会增加路由流量。对于连接到自治的所有路由器，此值必须相同。（范围：1-65535 秒;默认值：10 秒）

retransmit-interval *seconds* -ABR 通过虚拟链路重传链路状态通告（LSA）的时间间隔。（范围：1-3600 秒;默认值：5 秒）

transmit-delay *seconds* -发送虚连接链路变化的 LSA 更新报文的延迟时间。所有路由器，此值必须相同。（范围：1-65535 秒;默认值：1 秒）

authentication -指定身份验证模式。如果后面未接可选参数，则使用纯文本身份验证方式,以及 authentication-key 指定的密码。如果指定了 messagedigest 身份验证，则使用 message-digest-key 和 md5 参数。如果指定了 null 选项，则不对对任何 OSPF 路由协议消息执行身份验证。

message-digest -指定（MD5）身份验证。

null -表示不使用身份验证。

authentication-key *key* -设置纯文本密码（最多 8 个字符）。

message-digest-key *key-id* **md5** *key* -设置密钥标识符和密码。用于 MD5 认证。 *key-id* 是从 0 到 255 的整数，*key 是*最多 16 个字符的字母数字字符串。

命令模式

路由配置

缺省配置

area-id: 无

router-id: 无

hello-interval: 10 秒

retransmit-interval: 5 秒

transmit-delay: 1 秒

dead-interval: 40 秒

authentication-key: 无

message-digest-key: 无

命令用法

◆所有区域必须连接到骨干区域（0.0.0.0）以保持路由整个自治系统的连通性。 如果不可能将区域连接到主干，可以使用虚拟链接。虚拟链接可以为孤立区域的骨干提供逻辑路径。

◆可以在任何两个拥有的骨干路由器之间配置虚拟链路。 这两台路由器加入了一个虚拟链接被视为由未编号的点对点网络连接。

范例

此示例使用所有可选参数的默认值创建虚拟链接。

```
Console(config-router)#network 10.4.0.0 0.255.255.0.0 area 10.4.0.0

Console(config-router)#area 10.4.0.0 virtual-link 10.4.3.254

Console(config-router)#
```

此示例使用 MD5 身份验证创建虚拟链接。

```
Console(config-router)#network 10.4.0.0 0.255.255.0.0 area 10.4.0.0

Console(config-router)#area 10.4.0.0 virtual-link 10.4.3.254 message-digestkey 5 md5 ld83jdpq

Console(config-router)#
```

31.1.17 network area

此命令定义 OSPF 区域以及在此区域内运行的接口区。 使用 **no** 形式禁用指定接口的 OSPF。

语法

[no] **network** *ip-address netmask* **area** *area-id*

ip-address - 要添加到区域的接口的地址。

netmask - 要添加到区域的地址范围的网络掩码。

area-id - 指定地址或范围的区域。 一个 OSPF 区域标识一组共享公共路由信息的路由器。区域 ID 可以是 IPv4 地址的形式，也可以是无符号的四个八位字节整数范围为

0-4294967295。

命令模式

路由配置

缺省配置

禁用

命令用法

◆区域 ID 在 OSPF 广播区域中值唯一。区域 ID 0.0.0.0 表示 自治系统 的 OSPF 骨干网 。 每个路由器必须通过直接连接或虚拟链路连接到主干网。

◆不同路由器上，相连的同网段，需要设置为相同的区域 ID。

范例

此示例创建主干 0.0.0.0，涵盖 B 类地址 10.1.x.x 和 C 类地址 10.2.9.x.

```
Console(config-router)#network 10.1.0.0 255.255.0.0 area 0.0.0.0
Console(config-router)#network 10.2.9.0 255.255.255.0 area 10.1.0.0
Console(config-router)#
```

31.1.18 ip ospf authentication

此命令指定用于接口的身份验证类型。输入这个命令没有任何可选参数，则使用纯文本（或简单密码）身份验证。 使用 no 形式恢复默认值。

语法

ip-address - 接口的 IP 地址。

message-digest - 指定（MD5）身份验证。

null - 表示不使用身份验证。

命令模式

接口配置 (VLAN)

缺省配置

无

命令用法

◆使用身份验证来防止路由器无意中加入未授权区域。 在同一区域中配置路由器使用相同的密码。同一网络上的所有相邻路由器使用相同的密码，才能交换路由数据。

◆密码插入 OSPF 包头。

◆使用简单密码验证时，密码包含在包里。如果它与接收路由器上配置的密码不匹配，数据包被丢弃。

◆使用 Message-Digest 5（MD5）身份验证时。

◆在为接口指定明文密码验证之前，请进行配置使用 ip ospf authentication-key 配置密码。在指定之前接口的 MD5 身份验证，配置钥 ID 使 ip ospf message-digest-key 命令键入。

◆纯文本认证或 *MD5-id* 和 *密钥* ，必须在整个自治系统配置相同。

范例

此示例启用指定接口的身份验证。

```
Console(config)#interface vlan 1

Console(config-if)#ip ospf authentication message-digest

Console(config-if)#
```

31.1.19 ip ospf authentication-key

此命令配置验证密码。使用 no 形式删除密码。

语法

ip ospf [*ip-address*] **authentication-key** *key*

no ip ospf [*ip-address*] **authentication-key**

ip-address - 此参数可用于指示特定的 IP 地址连接到当前界面。如果未指定，则应用该命令到连接到当前接口的所有网络。

key - 设置纯文本密码。 （范围：1-8 个字符）

命令模式

接口配置 (VLAN)

缺省配置

无

命令用法

◆在为接口指定明文密码验证之前 ip ospf authentication 命令，使用该命令配置密码。

◆此命令创建插入 OSPF 包头的密码。

◆可以为每个网络接口分配不同的密码，但是相邻路由器必须使用相同的密码。

范例

此示例为指定的接口设置密码。

```
Console(config)#interface vlan 1

Console(config-if)#ip ospf authentication-key badboy

Console(config-if)#
```

31.1.20 ip ospf cost

该命令显式设置接口上发送协议报文的开销，其中值越高表示端口开销越大优先级越低。 使用 no 形式恢复默认值。

语法

ip ospf [*ip-address*] **cost** *cost*

no ip ospf [*ip-address*] **cost**

ip-address - 若配置此参数，则表示配置的 *cost* 是针对 IP 为该值的对端设备。

cost - 此接口的开销。使用较高的值表示优先级较低的端口。（范围：1-65535）

命令模式

接口配置 (VLAN)

缺省配置

1

命令用法

◆配置开销后，不再采用默认的开销值。

范例

```
Console(config)#interface vlan 1
```

```
Console(config-if)#ip ospf cost 10

Console(config-if)#
```

31.1.21 ip ospf dead-interval

此命令设置 dead 时间。 使用 **no** 形式恢复默认值。

语法

ip ospf [*ip-address*] **dead-interval** *seconds*

no ip ospf [*ip-address*] **dead-interval**

ip-address - 配置此参数则表示是针对该 IP 的邻居路由器。

seconds - 等待该时间未收到邻居路由器的 hello 报文，则将该邻居删除。相邻路由器必须配置相同。（范围：1-65535）

命令模式

接口配置 (VLAN)

缺省配置

40，或者是 ip ospf hello-interval 命令指定的间隔的四倍。

命令用法

dead-interval 包含在路由器的 hello 数据包中。 它必须是 hello-interval 的倍数。

范例

```
Console(config)#interface vlan 1

Console(config-if)#ip ospf dead-interval 50

Console(config-if)#
```

31.1.22 ip ospf hello-interval

该命令用来指定发送 Hello 报文的时间间隔。 使用 **no** 形式恢复默认值。

语法

ip ospf [ip-address] **hello-interval** *seconds*

no ip ospf [*ip-address*] **hello-interval**

ip-address -配置此参数则表示是针对该 IP 的邻居路由器。

seconds-从接口发送 hello 数据包的时间间隔。网络上的所有路由器将 interval 设置为相同的值。（范围：1-65535）

命令模式

接口配置 (VLAN)

缺省配置

10 秒

命令用法

Hello 数据包用于通知其他路由器发送路由器仍处于活动状态。将 hello interval 设置为较小的值可以减少检测拓扑变化的的延迟，但会增加路由流量。

范例

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf hello-interval 5
Console(config-if)#
```

31.1.23 ip ospf message-digest-key

此命令启用指定（MD5）身份验证。 使用 no 形式可以删除现有密钥。

语法

ip ospf [*ip-address*] **message-digest-key** *key-id* **md5** *key*

no ip ospf [*ip-address*] **message-digest-key** *key-id*

ip-address -配置此参数则表示是针对该 IP 的邻居路由器。

key-id - MD5 密钥的索引号。 （范围：0-255）

key - 用于生成 128 位消息摘要的字母数字密码。（范围：1-16 个字符）

命令模式

接口配置 (VLAN)

缺省配置

MD5 认证禁用

命令用法

◆在为 ip ospf authentication 命令指定接口的 MD5 身份验证之前，使用此命令配置消息摘要密钥 ID 和密钥。

◆通常，每个接口只使用一个密钥。相邻路由器必须使用相同的密钥标识符和密钥值。

◆更改为新密钥时，路由器将发送多个信息，一个使用旧密钥，另一个使用新密钥 。当所有相邻路由器开始使用新密钥，路由器将停止使用旧密钥。

范例

此示例设置消息摘要密钥标识符和密码。

```
Console(config)#interface vlan 1

Console(config-if)#ip ospf message-digest-key 1 md5 aiebel

Console(config-if)#
```

31.1.24 ip ospf priority

此命令设置优先级，该优先级用于 DR、BDR 选举。使用 no 形式恢复默认值。

语法

ip ospf [*ip-address*] **priority** *priority*

no ip ospf [*ip-address*] **priority**

ip-address - 此参数表示该命令针对特定 IP 的邻居路由器。

priority - 设置此路由器的接口优先级。（范围：0-255）

命令模式

接口配置 (VLAN)

缺省配置

1

命令用法

◆DR 失效，则 BDR 将接管此角色。

◆ 将优先级设置为零，路由器将不参与 DR 和 BDR 选举。 如果设置为零以外的任何值，具有最高优先级的路由器将成为 DR，具有次高优先级的路由器成为 BDR。如果两个或多个路由器具有相同的优先级，则路由器 router-id 大的优先选为 DR。

◆当新接口 up 时，如果网段已存在 DR，则新路由器将接受当前 DR，而不管其自身的优先级。DR 在下次选举过程开始之前不改变。

范例

```
Console(config)#interface vlan 1

Console(config-if)#ip ospf priority 5

Console(config-if)#
```

31.1.25 ip ospf retransmit-interval

此命令指定重新发送链接状态通告（LSA）的时间间隔。 使用 no 形式恢复默认值。

语法

ip ospf [*ip-address*] **retransmit-interval** *seconds*

no ip ospf [*ip-address*] **retransmit-interval**

ip-address -此参数指该配置针对特定 **ip 的路由器**。

seconds -设置从中重传 LSA 的时间间隔。（范围：1-65535）

命令模式

接口配置 (VLAN)

缺省配置

5 秒

命令用法

◆ 如果没有收到确认报文，路由器会根据重传间隔时间重新发送 LSA。

范例

```
Console(config)#interface vlan 1

Console(config-if)#ip ospf retransmit-interval 7

Console(config-if)#
```

31.1.26 ip ospf transmit-delay

此命令设置通过网络发送链路状态更新数据包的估计时间接口。 使用 no 形式恢复默认值。

语法

ip ospf [*ip-address*] **transmit-delay** *seconds*

no ip ospf [*ip-address*] **transmit-delay**

ip-address - 此参数可用于指示特定的 IP 地址连接到当前界面。如果未指定，则应用该命令到连接到当前接口的所有网络。

seconds - 设置发送链路状态更新所需的估计时间。（范围：1-65535）

命令模式

接口配置 (VLAN)

缺省配置

1 秒

命令用法

◆ LSA 在传输之前将其年龄增加了这个值 。什么时候估计传输延迟，考虑传输和传播接口延迟。使用根据链路速度设置传输延迟较低速度链接的较大值。

◆如果未添加此延迟，则通过链路传输 LSA 所需的时间为路由过程没有考虑到。在慢速链接上，路由器可以比设备接收数据包更快地发送数据包。为了避免这种情况问题，使用传输延迟强制路由器等待指定的时间间隔传输之间。

范例

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf transmit-delay 6
Console(config-if)#
```

31.1.27 passive-interface

此命令禁止指定接口上的 OSPF 路由流量。使用 no 形式允许在指定接口上发送和接收路由流量。

语法

[no] **passive-interface vlan** *vlan-id* [*ip-address*]

vlan-id - VLAN ID。 （范围：1-4094）

ip-address - 在此接口上配置的 IPv4 地址。

命令模式

路由配置

缺省配置

无

命令用法

您可以将 OSPF 接口配置为被动，以防止 OSPF 路由流量退出或进入该界面。 如果其中一个，则不能形成 OSPF 邻接涉及的接口设置为被动模式。指定的界面将显示为 OSPF 域中的 stub。此外如果将 OSPF 接口配置为被动式邻接已经存在，邻接将几乎立即下降。

范例

```
Console(config-router)#passive-interface vlan 1

Console(config-router)#
```

31.1.28 show ip ospf

此命令显示有关路由配置的基本信息。

语法

show ip ospf [*process-id*]

process-id -信息所在的路由器进程的 ID 显示。（范围：1-65535）

命令模式

特权模式

范例

```
Console#show ip ospf

Routing Process "ospf 1" with ID 192.168.1.3

Process uptime is 20 minutes

Conforms to RFC2328, and RFC1583Compatibility flag is disabled
```

```
Supports only single TOS(TOS0) routes

SPF schedule delay 5 secs, Hold time between two SPFs 10 secs

Refresh timer 10 secs

Number of incoming current DD exchange neighbors 0/5

Number of outgoing current DD exchange neighbors 0/5

Number of external LSA 0. Checksum 0x000000

Number of opaque AS LSA 0. Checksum 0x000000

LSDB database overflow limit is 20480

Number of LSA originated 1

Number of LSA received 0

Number of areas attached to this router: 1

Area 192.168.1.3

Number of interfaces in this area is 1(1)

Number of fully adjacent neighbors in this area is 0

Area has no authentication

SPF algorithm last executed 00:00:08.739 ago

SPF algorithm executed 1 times

Number of LSA 1. Checksum 0x007f09

Console#
```

31.1.29 show ip ospf border-routers

此命令显示路由表中通向区域边界路由器的条目(ABR)或自治系统边界路由器(ASBR)。

语法

show ip ospf [*process-id*] **border-routers**

process-id -信息所在的路由器进程的 ID　显示。（范围：1-65535）

命令模式

特权模式

范例

```
Console#show ip ospf border-routers

OSPF process 1 internal Routing Table

Codes: i - Intra-area route, I - Inter-area route

i 192.168.0.3 [1] via 192.168.0.3, vlan1, ABR, ASBR, Area 0.0.0.0

Console#
```

31.1.30 show ip ospf database

此命令显示有关不同 OSPF 链路状态通告的信息（LSA）存储在此路由器的数据库中。

语法

show ip ospf [*process-id*] **database**

[**asbr-summary** | **external** | **network** | **nssa-external** | **router** | **summary**]

[**adv-router** *ip-address* | *link-state-id* | **self-originate**]

process-id -信息所在的路由器进程的 ID 显示。（范围：1-65535）

adv-router -广告路由器的 IP 地址。如果没有输入，显示有关所有广告路由器的信息。

ip-address -指定路由器的 IP 地址。如果没有输入地址，在形成对本地路由器显示。

link-state-id - LSA 描述的网络部分。 *链路状态-ID*

输入应该是：

- 类型 3 摘要和外部 LSA 的 IP 网络号。
- 路由器，网络和类型 4 AS Summary LSA 的 路由器 ID 另请注意，当 Type 5 ASBR External LSA 描述默认值时 route，其 *link-state-id* 设置为默认目标（0.0.0.0）。

self-originate -显示由此路由器发起的 LSA。

asbr-summary -显示有关自治系统边界的信息路由器汇总 LSA。

external -显示有关外部 LSA 的信息。

network -显示有关网络 LSA 的信息。

nssa-external -显示有关 NSSA 外部 LSA 的信息。

router -显示有关路由器 LSA 的信息。

summary -显示有关汇总 LSA 的信息。

命令模式

特权模式

范例

以下显示了 **show ip ospf database** 命令的输出。

```
Console#show ip ospf database

OSPF Router with ID (192.168.0.2) (Process ID 1)

Router Link States (Area 0.0.0.0)

Link ID ADV Router Age Seq# CkSum Link count

192.168.0.2 192.168.0.2 225 0x80000004 0xdac5 1

192.168.0.3 192.168.0.3 220 0x80000004 0xd8c4 1

Net Link States (Area 0.0.0.0)

Link ID ADV Router Age Seq# CkSum

192.168.0.2 192.168.0.2 225 0x80000001 0x9c0f

AS External Link States

Link ID ADV Router Age Seq# CkSum Route Tag

0.0.0.0 192.168.0.2 487 0x80000001 0xd491 E2 0.0.0.0/0 0

0.0.0.0 192.168.0.3 222 0x80000001 0xce96 E2 0.0.0.0/0 0

Console#
```

以下显示使用 **asbr-summary** 关键字时的输出 。

```
Console#show ip ospf database asbr-summary

OSPF Router with ID (0.0.0.0) (Process ID 1)

ASBR-Summary Link States (Area 0.0.0.1)

LS Age: 0

Options: 0x2 (*|-|-|-|-|-|E|-)

LS Type: ASBR-summary-LSA

Link State ID: 2.1.0.0 (AS Boundary Router address)

Advertising Router: 192.168.2.1

LS Seq Number: 80000001

Checksum: 0x7b67

Length: 28

Network Mask: /0
```

```
TOS: 0 Metric: 10

Console#
```

以下显示使用 **external** 关键字时的输出 。

```
Console#show ip ospf database external

OSPF Router process 100 with ID (10.10.11.50)

AS External Link States LS age: 298

Options: 0x2 (*|-|-|-|-|-|E|-)

LS Type: AS-external-LSA

Link State ID: 10.10.100.0 (External Network Number)

Advertising Router: 10.10.11.50

LS Seq Number: 80000001

Checksum: 0x7033

Length: 36

Network Mask: /24

Metric Type: 2 (Larger than any link state path)

TOS: 0

Metric: 20

Forward Address: 10.10.11.50

External Route Tag: 0

OSPF Router with ID (0.0.0.0) (Process ID 1)

AS External Link States

LS Age: 0

Options: 0x2 (*|-|-|-|-|-|E|-)

LS Type: AS-external-LSA

Link State ID: 0.0.0.0 (External Network Number)

Advertising Router: 192.168.0.2

LS Seq Number: 80000005

Checksum: 0xcc95

Length: 36

Network Mask: /0
```

```
Metric Type: 2 (Larger than any link state path)

TOS: 0

Metric: 1

Forward Address: 0.0.0.0

External Route Tag: 0

Console#
```

以下显示使用 **network** 关键字时的输出 。

```
Console#show ip ospf database network

OSPF Router with ID (0.0.0.0) (Process ID 1)

Net Link States (Area 0.0.0.0)

LS Age: 0

Options: 0x2 (*|-|-|-|-|-|E|-)

LS Type: network-LSA

Link State ID: 192.168.0.2 (address of Designated Router)

Advertising Router: 192.168.0.2

LS Seq Number: 80000005

Checksum: 0x9413

Length: 32

Network Mask: /24

Attached Router: 192.168.0.2

Attached Router: 192.168.0.3
```

以下显示使用 **router** 关键字时的输出 。

```
Console#show ip ospf database router

OSPF Router with ID (0.0.0.0) (Process ID 1)

Router Link States (Area 0.0.0.0)

LS Age: 0

Options: 0x2 (*|-|-|-|-|-|E|-)

Flags: 0x2 : ASBR

LS Type: router-LSA

Link State ID: 192.168.0.2
```

```
Advertising Router: 192.168.0.2

LS Seq Number: 80000008

Checksum: 0xd2c9

Length: 36

Link connected to: a Transit Network

(Link ID) Designated Router address: 192.168.0.2

(Link Data) Router Interface address: 192.168.0.2

Number of TOS metrics: 0

TOS 0 Metric: 1

...
```

以下显示使用 **summary** 关键字时的输出 。

```
Console#show ip ospf database summary

OSPF Router with ID (0.0.0.0) (Process ID 1)

Summary Link States (Area 0.0.0.0)

LS Age: 1

Options: 0x0 (*|-|-|-|-|-|-)

LS Type: summary-LSA

Link State ID: 192.168.10.0 (summary Network Number)

Advertising Router: 2.1.0.0

LS Seq Number: 80000005

Checksum: 0x479d

Length: 28

Network Mask: /24

TOS: 0 Metric: 0

...
```

31.1.31 show ip ospf interface

此命令显示 OSPF 接口的摘要信息。

语法

show ip ospf interface [**vlan** *vlan-id*]

vlan-id - VLAN ID (范围: 1-4094)

命令模式

特权模式

范例

```
Console#show ip ospf interface vlan 1

VLAN1 is up, line protocol is up

Internet Address 192.168.0.2/24, Area 0.0.0.0, MTU 1500

Process ID 1, Router ID 192.168.0.2, Network Type BROADCAST, Cost: 1

Transmit Delay is 1 sec, State DR, Priority 1

Designated Router (ID) 192.168.0.2, Interface Address 192.168.0.2

Backup Designated Router (ID) 192.168.0.3, Interface Address 192.168.0.3

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

Hello due in 00:00:10

Neighbor Count is 1, Adjacent neighbor count is 1

Hello received 920 sent 975, DD received 5 sent 4

LS-Req received 1 sent 1, LS-Upd received 14 sent 18

LS-Ack received 17 sent 13, Discarded 0

Console#
```

31.1.32 show ip ospf neighbor

此命令显示每个接口上相邻路由器的信息在 OSPF 区域内。

语法

show ip ospf [*process-id*] **neighbor**

process-id -信息所在的路由器进程的 ID 显示。（范围：1-65535）

命令模式

特权模式

范例

```
Console#show ip ospf neighbor

ID Pri State Address Interface

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

192.168.0.3 1 FULL/BDR 192.168.0.3 VLAN1

Console#
```

31.1.33 show ip ospf route

此命令显示 OSPF 路由表。

语法

show ip ospf [*process-id*] **route**

process-id -信息所在的路由器进程的 ID 显示。（范围：1-65535）

命令模式

特权模式

范例

```
Console#show ip ospf route

OSPF process 1:

Codes: C - connected, D - Discard, 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

O 10.10.0.0/24 [10] is directly connected, fe1/1, Area 0.0.0.0

O 10.10.11.0/24 [10] is directly connected, fe1/2, Area 0.0.0.0

O 10.10.11.100/32 [10] is directly connected, lo, Area 0.0.0.0

E2 10.15.0.0/24 [10/50] via 10.10.0.1, VLAN1

IA 172.16.10.0/24 [30] via 10.10.11.50, VLAN2, Area 0.0.0.0
```

```
E2 192.168.0.0/16 [10/20] via 10.10.11.50, VLAN2

Console#
```

31.1.34 show ip ospf virtual-links

此命令显示有关虚拟链接的详细信息。

语法

show ip ospf virtual-links

命令模式

特权模式

范例

```
Console#show ip ospf virtual-links

Virtual Link VLINK1 to router 192.168.0.2 is up

Transit area 0.0.0.1 via interface VLAN1

Local address 192.168.0.3

Remote address 192.168.0.2

Transmit Delay is 1 sec, State Point-To-Point,

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

Hello due in 00:00:08

Adjacency state Down

Console#
```

31.1.35 show ip protocols ospf

此命令显示 OSPF 进程参数。

语法

show ip protocols ospf

命令模式

特权模式

范例

```
Console#show ip protocols ospf

Routing Protocol is "ospf 200"

Redistributing: rip

Routing for Networks:

192.30.30.0/24

192.40.40.0/24

Routing for Summary Address:

192.168.1.0/24

192.168.3.0/24

Distance: (default is 110)

Console#
```

32 VRRP

32.1.1 Vrrp 认证

此命令指定用于验证从中接收的 VRRP 数据包的密钥其他路由器。 使用 no 形式来阻止身份验证。

语法

vrrp *group* **authentication** *key*

no vrrp *group* **authentication**

group -标识虚拟路由器组。（范围：1-255）

key -验证字符串。（范围：1-8 个字母数字字符）

缺省配置

无

命令模式

接口 (VLAN)

命令用法

◆同一 VRRP 备份组中的所有路由器必须配置相同的路由器验证密钥。

◆当从组中的另一个路由器收到 VRRP 数据包时，它将身份验证密钥与此路由器上配置的字符串进行比较。如果密钥匹配，消息被接受。否则，丢弃该分组。

◆纯文本身份验证不提供任何真正的安全性。它仅受支持防止错误配置的路由器参与 VRRP。

范例

```
Console(config-if)#vrrp 1 authentication bluebird
Console(config-if)#
```

32.1.2 vrrp ip

此命令启用虚拟路由器冗余协议（VRRP）接口，指定虚拟路由器的 IP 地址。 使用 no 形式在接口上禁用 VRRP，并从虚拟路由器中删除 IP 地址。

语法

[no] **vrrp** *group* **ip** *ip-address*

group -标识虚拟路由器组。（范围：1-255）

ip-address - 虚拟路由器的 IP 地址。这是 IP 地址终端主机设置为其默认网关。

缺省配置

无

命令模式

接口 (VLAN)

命令用法

◆参与虚拟路由器组的所有路由器的接口必须是在同一 IP 子网内。

◆如果使用此命令分配给虚拟路由器的 IP 地址已经配置为此接口上的主地址，则此路由器被视为所有者，并将承担组中的主虚拟路由器的角色。

◆该接口用于两个目的——发送/接收广告消息以及作为主 VRRP 路由器操作时代表虚拟路由器转发。

◆输入此命令，将立即启用 VRRP。如果需要为 VRRP 定制任何其他参数，如身份验证、优先级或广告间隔，那么首先在启用 VRRP 之前配置这些参数。

范例

此示例使用 VLAN 1 的主接口作为 VRRP 组所有者创建 VRRP 组 1。

```
Console(config)#interface vlan 1
```

```
Console(config-if)#vrrp 1 ip 192.168.1.6

Console(config-if)#
```

32.1.3 vrrp preempt

如果路由器具有比当前代理主路由器更高的优先级，则此命令将路由器配置为接管 VRRP 组的主虚拟路由器。使用 no 形式禁用优先购买权。

语法

vrrp *group* **preempt** [**delay** *seconds*]

no vrrp *group* **preempt**

group -标识 VRRP 组。（范围：1-255）

seconds -在发出声明成为主人之前等待的时间。（范围：0-120 秒）

缺省配置

Preempt：启用

Delay：0 秒

命令模式

接口 (VLAN)

命令用法

◆如果抢占是启用的，并且该备份路由器的优先级高于当前代理主机，则它将接管作为新主机。但是，请注意，如果原始主机（即，VRRP IP 地址的所有者）重新联机，它总是会恢复作为主机的控制。

◆延迟可以给予额外的时间来接收来自当前主控器的广告消息，然后再进行控制。如果试图成为主路由器的路由器刚刚上线，则该延迟还给它时间收集路由表的信息，然后实际抢占当前活动的路由器。

范例

```
Console(config-if)#vrrp 1 preempt delay 10

Console(config-if)#
```

32.1.4 vrrp priority

该命令用来设置 VRRP 备份组中该路由器的优先级。 使用 no 形式恢复默认设置。

语法

vrrp *group* **priority** *level*

no vrrp *group* **priority**

group -标识 VRRP 组。（范围：1-255）

level -该路由器在 VRRP 组中的优先级。（范围：1-254）

缺省配置

Master：255

Backup：100

命令模式

接口(VLAN)

命令用法

◆具有与虚拟路由器使用的 IP 地址相同的物理接口的路由器（即，VRRP IP 地址的所有者）将成为主虚拟路由器。如果当前主机失败，具有最高优先级的备用路由器将成为主路由器。当原始主路由器恢复时，它将再次作为主动主路由器接管。

◆如果两个或多个路由器被配置为具有相同的 VRRP 优先级，则如果当前主路由器失败，则具有最高 IP 地址的路由器被选择为新的主路由器。

◆如果备份抢占功能是通过 vrrp 抢占命令启用的，并且具有比当前代理主机更高的优先级的备份路由器上线，则该备份路由器将接管作为新的代理主机。但是，请注意，如果原始主机（即，VRRP IP 地址的所有者）重新联机，它总是会恢复作为主机的控制。

◆如果 VRRP 组的虚拟 IP 地址，配置的设备一样，优先将自动被设置为 255，使用此命令之前。

范例

```
Console(config-if)#vrrp 1 priority 1

Console(config-if)#
```

32.1.5 vrrp timers advertise

此命令设置主虚拟路由器发送广告的状态，该状态将其状态作为主机发送。使用 no 形式来恢复间隔时间间隔。

语法

vrrp *group* **timers advertise** *interval*

no vrrp *group* **timers advertise**

group -标识 VRRP 组。（范围：1-255）

interval -主虚拟路由器的广告间隔。(范围：1-255 秒)

缺省配置

1 秒

命令模式

接口(VLAN)

命令用法

◆来自当前主虚拟路由器的 VRRP 广告包括关于其优先级和当前状态的信息作为主。

◆VRRP 广告被发送到多播地址 224.0.0.18。使用多播地址可以减少非指定 VRRP 组的网络设备必须处理的通信量。

◆如果主路由器停止发送广告，备份路由器将成为基于优先级的主路由器。在试图接通主机之前的死区是 Hello 间隔加上半秒的三倍。

范例

```
Console(config-if)#vrrp 1 timers advertise 5

Console(config-if)#
```

32.1.6 show vrrp

该命令显示 VRRP 的状态信息。

语法

show vrrp [**brief** | *group*]

brief - Displays summary information for all VRRP groups on this router.

group -标识 VRRP 组。　（范围：1-255）

缺省配置

无

命令模式

特权模式

命令用法

◆使用此命令不带任何关键字来显示完整的状态列表该路由器上配置的所有 VRRP 备份组的信息。

◆使用这个命令用简短关键字来显示在这个路由器上配置的所有 VRRP 组的状态信息摘要。

◆指定用于显示特定组的状态信息的组编号。

范例

此示例显示所有组的状态信息的完整列表。

```
Console#show vrrp

VLAN 1 - Group 1,

State Master

Virtual IP Address 192.168.1.6

Virtual MAC Address 00-00-5E-00-01-01

Advertisement Interval 5 sec

Preemption enabled

Min Delay 10 sec

Priority 255

Authentication SimpleText

Authentication Key bluebird

Master Router 192.168.1.6

Master Priority 255

Master Advertisement Interval 5 sec

Master Down Interval 15

Console#
```

此示例显示所有组的状态信息的简要列表。

```
Console#show vrrp brief

Interface Grp State Virtual Addr Interval Preempt Priority

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

VLAN 1 1 Master 192.168.0.3 1 E 255

Console#
```

32.1.7 show vrrp interface

该命令显示指定 VRRP 接口的状态信息。

语法

show vrrp interface vlan *vlan-id* [**brief**]

vlan-id -配置的 VLAN 接口的标识符。（范围：1-4094）

brief -显示此路由器上所有 VRRP 组的摘要信息。

缺省配置

无

命令模式

特权模式

范例

此示例显示 VLAN 1 的完整状态信息列表。

```
Console#show vrrp interface vlan 1

Vlan 1 - Group 1,

State Master

Virtual IP Address 192.168.1.6

Virtual MAC Address 00-00-5E-00-01-01

Advertisement Interval 5 sec

Preemption enabled

Min Delay 10 sec

Priority 1
```

```
Authentication SimpleText

Authentication Key bluebird

Master Router 192.168.1.6

Master Priority 1

Master Advertisement Interval 5 sec

Master Down Interval 15

Console#
```

32.1.8 show vrrp interface counters

此命令显示 VRRP 协议事件和错误的计数器发生在指定的组和接口上。

show vrrp *group* **interface vlan** *interface* **counters**

group -标识 VRRP 组。（范围：1-255）

interface -已配置 VLAN 接口的标识符。（范围：1-4094）

缺省配置

无

命令模式

特权模式

范例

```
Console#show vrrp 1 interface vlan 1 counters

Total Number of Times Transitioned to MASTER : 6

Total Number of Received Advertisements Packets : 0

Total Number of Received Error Advertisement Interval Packets : 0

Total Number of Received Authentication Failures Packets : 0

Total Number of Received Error IP TTL VRRP Packets : 0

Total Number of Received Priority 0 VRRP Packets : 0

Total Number of Sent Priority 0 VRRP Packets : 5

Total Number of Received Invalid Type VRRP Packets : 0

Total Number of Received Error Address List VRRP Packets : 0
```

```
Total Number of Received Invalid Authentication Type VRRP Packets : 0

Total Number of Received Mismatch Authentication Type VRRP Packets : 0

Total Number of Received Error Packet Length VRRP Packets : 0

Console#
```

32.1.9 show vrrp router counters

此命令显示 VRRP 协议数据包中发现的错误的计数器。

命令模式

特权模式

范例

注意，未知错误指示以未知或不支持的版本号接收的 VRRP 包。

```
Console#show vrrp router counters

Total Number of VRRP Packets with Invalid Checksum : 0

Total Number of VRRP Packets with Unknown Error : 0

Total Number of VRRP Packets with Invalid VRID : 0

Console#
```