



配置手册

NBS 5528XG & NBS 5552XG 交换机
RGOS 10.4(3)

文档版本号:V1.0

版权声明

福建星网锐捷网络有限公司©2014

锐捷网络有限公司版权所有，并保留对本手册及本声明的一切权利。

未得到锐捷网络有限公司的书面许可，任何人不得以任何方式或形式对本手册内的任何部分进行复制、摘录、备份、修改、传播、翻译成其他语言、将其全部或部分用于商业用途。

、、、、
RGOS®、**RGNOS®**、、
Red-Giant®、**Red-Giant 锐捷®**、**锐捷®** 都是福建星网锐捷网络有限公司的注册商标，不得仿冒。

免责声明

本手册依据现有信息制作，其内容如有更改，恕不另行通知，请关注锐捷网络有限公司网站提供的最新信息。锐捷网络有限公司在编写本手册时已尽力保证其内容准确可靠，但对于本手册中的遗漏、不准确或错误，以及由此导致的损失和损害，锐捷网络有限公司不承担责任。

技术支持

- 锐捷网络官方网站: <http://www.ruijie.com.cn/>

您可以在官网中获得最新的产品技术资料、产品故障原因及问题分析、产品的应用解决方案、软件升级资料等等。

- 锐捷网络在线客服: <http://webchat.ruijie.com.cn。>

您可以在工作日早 8:30 至晚 6 点, 通过“在线客服”获得信息咨询、远程调试故障、软件维护等技术支持。无需下载客户端, 可以即时截图、发附件, 方便快捷。

- 锐捷网络远程技术支持中心: <http://www.ruijie.com.cn/service.aspx>

锐捷网络远程技术支持中心可以为所有的客户提供所需要的技术帮助和解决方案。对于客户遇到的产品的安装、软件的配置以及其它的网络性能的问题, 客户服务中心都将提供迅速的技术支持。

- 7×24 小时技术服务热线: 4008-111-000

- 锐捷网络技术论坛: <http://support.ruijie.com.cn>

- 锐捷网络技术支持与反馈信箱: service@ruijie.com.cn

手册名称	说明
产品 安装手册	本手册介绍了产品在功能和物理上的一些特性, 提供了设备安装步骤、硬件故障排除、模块技术规格, 以及电缆和连接器的规格和使用准则等。
产品 命令手册	本手册对产品支持的配置命令做了详细的描述。包括命令模式、参数说明和使用指南等, 并配有具体的实例。
产品 WEB 管理手册	本手册对产品支持的各功能的 WEB 界面进行描述, 并配有详细的配置实例。

前言

版本说明

本手册对应的软件版本为:RGOS[®]10.4(3)版。

读者对象

本书适合下列人员阅读

- 网络工程师
- 技术推广人员
- 网络管理员

本书约定

1. 命令行格式约定

命令行字体采用用 Arial，具体相关格式意义如下：

粗体：命令行关键字（命令中保持不变必须照输的部分）采用加粗字体表示。

斜体：命令行参数（命令中必须由实际值进行替代的部分）采用斜体表示

{ }：表示用{ }括起来的部分，在命令配置时是可选的。

[x|y|...]：表示从两个或多个选项中选取一个。

{x|y|...}：表示从两个或多个选项中选取一个，多个或者不选。

//：由双斜杠开始的行表示为注释行。

2. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

⚡：注意、警告、提醒操作中应注意的事项。

📖：说明、提示、窍门、对操作内容的描述进行必要的补充。

3. 说明

- 本手册举例说明部分的端口类型同实际可能不符，实际操作中需要按照各产品所支持的端口类型进行配置。
- 本手册部分举例的显示信息中可能含有其它产品系列的内容（如产品型号、描述等），具体显示信息请以实际使用的设备信息为准。
- 手册中涉及的路由器及路由器产品图标，代表了一般意义下的路由器，以及运行了路由协议的三层交换机。

4. 用户权限

Web 账户	默认管理员账户：admin，密码：admin，可以在 WEB 上对交换机进行管理配置。如果用户创建一个管理员权限账号，该默认账户 admin/admin 将自动失效；如果用户删除所有创建的账号，该默认账户 admin/admin 将自动生效。
CLI 账户	管理员账户：默认用户名密码为 ruijie/ruijie，可以使用交换机所有管理功能。



配置指南-系统配置

本分册介绍系统配置配置指南相关内容，包括以下章节：

1. 基础管理
2. LINE 模式
3. 系统升级
4. 文件系统
5. 配置文件管理
6. 系统管理
7. 系统日志
8. POWER
9. 调试命令

1 基础管理

1.1 基础管理概述

通过命令的授权控制用户访问

控制网络上的终端访问网络设备的一个简单办法，就是使用口令保护和划分特权级别。口令可以控制对网络设备的访问，特权级别可以在用户登录成功后，控制其可以使用的命令。

从安全角度来看，口令是保存在配置文件中的，在网络上传输这些文件时（比如使用 TFTP），我们希望保证口令的安全。因此口令在保存入参数文件之前将被加密处理，明文形式的口令变成密文形式的口令。命令 `enable user_account encryption` 使用了私有的加密算法。

登录认证控制

前面我们描述了如何通过本地保存的口令来控制对网络设备的访问。除了线路口令保护和本地认证外，如果启用了 AAA 模式，则在用户登录网络设备进行管理时，在登录时我们还可以通过一些服务器来根据用户名和密码进行用户的管理权限的认证，目前我们还支持利用 RADIUS 服务器根据用户登录时的用户名和密码控制用户对网络设备的管理权限。

利用 RADIUS 服务器对用户登录时的用户名和密码进行控制，这样网络设备不再用本地保存的密码信息进行认证，而是将加密后的用户信息发送到 RADIUS 服务器上验证，服务器统一配置用户的用户名、用户密码、共享密码和访问策略等信息，便于管理和控制用户访问，提高用户信息的安全性。

系统时间配置

每台网络设备中均有自己的系统时钟，该时钟提供具体日期（年、月、日）和时间（时、分、秒）以及星期等信息。对于一台网络设备，当第一次使用时需要首先手工配置网络设备系统时钟为当前的日期和时间。当然，根据需要，也可以随时修正系统时钟。网络设备的系统时钟主要用于系统日志等需要记录事件发生时间的地方。

系统名称和命令提示符

为了管理的方便，可以为一台网络设备配置系统名称(System Name)来标识它。同时如果还没有为 CLI 配置命令提示符，则系统名称（如果系统名称超过 32 个字符，则截取其前 32 个字符）将作为默认的命令提示符，提示符将随着系统名称的变化而变化。默认情况下，系统名为“Ruijie”。

标题配置

当用户登录网络设备时，需要告诉用户一些必要的信息。可以通过设置标题来达到这个目的。可以创建两种类型的标题（banner）：每日通知和登录标题。每日通知针对所有连接到网络设备的用户，当用户登录网络设备时，通知消息将首先显示在终端上。利用每日通知，可以发送一些较为紧迫的消息（比如系统即将关闭等）给网络用户。登录标题显示在每日通知之后，它的主要作用是提供一些常规的登录提示信息。缺省情况下，每日通知和登录标题均未设置。

查看系统信息

可以通过命令行中的显示命令查看一些系统的信息，主要包括系统的版本信息，系统中的设备信息等。

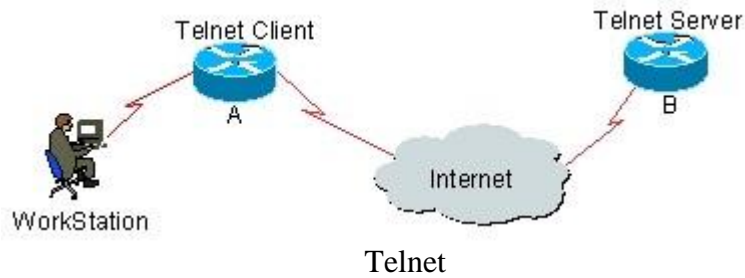
控制台速率配置

网络设备有一个控制台接口（Console），通过这个控制台接口，可以对网络设备进行管理。当网络设备第一次使用的时候，必须采用通过控制台方式对其进行配置。可以根据需要改变网络设备串口的速率。需要注意的是，用来管理网络设备的终端的速率设置必须和网络设备的控制台的速率一致。

在网络设备上使用 telnet

Telnet 在 TCP/IP 协议族中属于应用层协议，它给出了通过网络提供远程登录和虚拟终端通讯功能的规范。Telnet Client 服务为已登录到本网络上的本地用户或远程用户提供使用本网络设备的 Telnet Client 程序访问网上其他远程系统资源的服务。如下图所示用户在微机上通过终端仿真程序或 Telnet 程序建立与网络设备 A 的连接后，可通过输入 telnet 命令再登录设备 B，并对其进行配置管理。

锐捷网络的 Telnet 程序支持使用 IPV4 地址进行通讯。目前仅只能作为 Telnet Server，接受 IPV4 的 Telnet 连接请求，不支持 Telnet client。



连接超时设置

可以通过配置设备的连接超时时间，控制该设备已经建立的连接（包括已接受连接，以及该设备到远程终端的会话），当空闲时间超过设置值，没有任何输入输出信息时，中断此连接。

1.2 帮助

用户可以在命令提示符下输入 help 命令获得帮助系统的简要描述信息。

命令	作用
help	该命令用于显示帮助系统的简单描述。任何命令模式下都可以使用 help 命令。

显示帮助系统的简单描述：

```
Ruijie#help

The switch CLI provides advanced help feature.
1. Help is available when you are ready to enter a command argument (e.g. 'show ?') and want to know each possible available options.
2. Help is provided when an abbreviated argument is entered and you want to know what arguments match the input(e.g. 'show ve?').If nothing matches, the help list will be empty and you must backup until entering a '?' shows the available options.
3. For completing a partial command name could enter the abbreviated command name immediately followed by a <Tab> key.

Note:
Since the character '#' is used for help purpose, to enter the character '?' in a string argument, press ctrl+v immediately followed by the character '?'.

Ruijie#
```

使用 Word 的帮助来显示所有开头字母为“re”的特权 EXEC 模式命令。在问号（？）之前输入的字母会重新打印到下一个命令行，用户可以在后面继续输入命令：

```
Ruijie#re?
reboot          rename          renew          reset

Ruijie#re
```

使用命令语法 help 显示部分完成的 IP 访问列表标准命令的下一个参数。在问号（？）之前输入的字符会重新打印到下一个命令行，用户可以在后面继续输入命令。

```
Ruijie(config)#ip access-list standard ?
<1-1999>        Standard IP access-list number
<cr>

Ruijie(config)#ip access-list standard
```


1.3 启用

此命令用于进入特权 EXEC 模式。如果当前的等级低于运行命令所需的等级，则执行此命令。如果特权等级需要密码，请在提供的字段中输入。只能尝试三次。

命令	作用
enable [PRIVILEGE-LEVEL]	此命令用于进入特权 EXEC 模式。

进入特权 EXEC 模式：

```
Ruijie# enable 15
password:***
Ruijie#
```

1.4 禁用

使用 disable [PRIVILEGE-LEVEL]命令在用户 EXEC 模式或特权 EXEC 模式下将用户级别降至低于特权级别的用户级别。如果当前级别高于特权级别，则使用此命令进入特权级。使用此命令进入特权级别时，如果已经配置了密码，则不需要输入密码。

命令	作用
disable [PRIVILEGE-LEVEL]	此命令用于将用户级别降至低于特权级别的用户级别。

如何登出：

```
Ruijie# disable
Ruijie> logout
```

1.5 配置终端

在 CLI 命令提示符下使用 configure terminal 命令进入全局配置模式。

命令	作用
configure terminal	此命令用于进入全局配置模式。

进入全局配置模式：

```
Ruijie# configure terminal
Ruijie(config)#
```

1.6 登录 (EXEC)

使用此命令更改登录帐户。登录交换机的界面的尝试为三次。当使用 Telnet 时，如果所有尝试都失败，将返回到命令提示符。如果在 60 秒内没有信息输入，会话将返回至未登录状态。

命令	作用
login	此命令用于配置一个登录用户名。

通过用户名“user1”登录：

```
Ruijie# login
Username: user1
Password: xxxxx
```

```
Ruijie#
```

1.7 登录 (Line)

在 CLI 命令提示符下使用 `login [local]` 命令设置登录方式。使用 `no` 命令禁止登录。

命令	作用
<code>login [local]</code>	此命令用于设置命令行登录方式。
<code>no login</code>	此命令将禁止登录。

进入线路配置模式，并为在线用户创建密码。这个密码只生效一次，相应的命令行设置为登录：

```
Ruijie# configure terminal
Ruijie(config)# line console 0
Ruijie(config-line)# password loginpassword
Ruijie(config-line)#
```

将命令行控制台登录方式配置为“登录”：

```
Ruijie# configure terminal
Ruijie(config)# line console 0
Ruijie(config-line)# login
Ruijie(config-line)#
```

输入 `login` 命令。设备将通过 `password create` 命令检查用户的合法性。如果正确，则用户可以以特定的级别进行访问：

```
Ruijie#login
Password:*****
Ruijie#
```

创建一个用户名“useraccount”，密码为“pass123”，以及权限为 12 的账户：

```
Ruijie# configure terminal
Ruijie(config)# username useraccount privilege 12 password 0 pass123
Ruijie(config)#
```

将登录方式配置为“login local”：

```
Ruijie# configure terminal
Ruijie(config)# line console 0
Ruijie(config-line)# login local
Ruijie(config-line)#
```

1.8 注销

在用户 EXEC 模式或者特权 EXEC 模式下使用 `logout` 命令执行注销操作。

命令	作用
<code>logout</code>	此命令可通过登出交换机来关闭一个活跃的终端会话。

如何注销：

```
Ruijie# disable
Ruijie# logout
```

1.9 结束

在 EXEC 模式或任何配置模式下使用此命令结束当前的配置模式。

命令	作用
----	----

end	此命令用于结束当前的配置模式，并返回到命令行模式中的最高层次结构模式，即用户 EXEC 模式或特权 EXEC 模式。
-----	--

结束接口配置模式并返回到特权 EXEC 模式：

```
Ruijie# configure terminal
Ruijie(config)# interface gi0/1
Ruijie(config-if)#end
Ruijie#
```

1.10 退出

使用 exit 命令退出当前模式。如果当前模式为用户 EXEC 模式或特权 EXEC 模式，执行 exit 命令会注销当前会话。

命令	作用
exit	此命令是用来结束配置模式并返回到上一个操作模式。

退出接口配置模式并返回到全局配置模式：

```
Ruijie# configure terminal
Ruijie(config) interface gi0/1
Ruijie(config-if)#exit
Ruijie(config)#
```

1.11 显示

使用下列命令在 EXEC 模式或任何配置模式下执行操作。通过按 Ctrl + P 或向上箭头键，可以将记录下的命令召回以前的命令队列中。历史缓冲区的大小是固定的 20 个命令。

命令	作用
show history	此命令用于列出在当前 EXEC 模式会话中输入的命令。
show environment [fan power temperature]	此命令用于显示风扇、温度、电源的可用性和状态信息。
show cpu	此命令用于显示系统在 5 秒、1 分钟和 5 分钟的间隔内 CPU 的利用率信息。
show version	此命令用于显示交换机的软件版本信息。

显示命令缓冲历史：

```
Ruijie# show history

help history

Ruijie#
```

显示风扇、温度、电源的可用性和状态信息：

```
Ruijie#show environment

Detail Temperature Status:
Unit   Temperature Descr/ID   Current/Threshold Range
-----
1      Central Temperature/1 27C/11~79C
Status code:* temperature is out of threshold range

Detail Fan Status:
-----
Right Fan 1 (OK)      Right Fan 2 (OK)

Detail Power Status:
Unit   Power Module   Power Status
-----
1      Power 1       in-operation

Ruijie#
```

显示 CPU 利用率信息:

```
Ruijie#show cpu

=====
          CPU Using Rate Information
CPU utilization in five seconds:  8 %
CPU utilization in one minute  :  8 %
CPU utilization in five minutes:  8 %
NO      5Sec      1Min      5Min      Process
 0      59 %      63 %      61 %      Idle
 1       1 %       1 %       1 %      GBIC_Pooling
 2       1 %       1 %       1 %      bcmCNTR.0
 3       0 %       1 %       1 %      bcmL2X.0
 4       0 %       0 %       0 %      HISR1
 5       0 %       0 %       0 %      socdmadesc.0
 6       0 %       0 %       0 %      bcmLINK.0
 7       0 %       0 %       0 %      MAUMIB_TASK
 8       0 %       0 %       0 %      cpuprotect
 9       0 %       0 %       0 %      CNT_TASK
10       0 %       0 %       0 %      CLI
11       0 %       0 %       0 %      bcmRX
12       0 %       0 %       0 %      DLKtimer
13       0 %       0 %       0 %      IP6-Tic
14       0 %       0 %       0 %      IP-Tic
15       0 %       0 %       0 %      OS_TIMER

Ruijie#
```

显示交换机的版本信息:

```
Ruijie#show version

System description      : Ruijie Full Gigabit Security & Intelligence Access Switch
(RG-NBS5552XG) By Ruijie Networks
System start time       : 2023-03-28 06:47:36
System uptime           : 0:1:55:22
System hardware version : 1.00
System software version : RGOS 10.4(3) Release(00008)
System BOOT version     : 1.00.02
Device information:
  Device-1
    Hardware version : 1.00
    Software version  : RGOS 10.4(3) Release(00008)
    BOOT version      : 1.00.02

Ruijie#
```

1.12 环境

此命令用于配置环境温度阈值。低阈值必须小于高阈值。配置的范围必须在可操作范围内，可操作范围对应的是为传感器定义的最小和最大许可温度。如果超出所配置的阈值，则会发送一个通知。使用 no 命令采用默认设置。

命令	作用
environment temperature threshold thermal THREMAL-ID [high VALUE] [low VALUE]	此命令用于配置环境温度阈值，该阈值对应的是为传感器定义的正常温度范围。
no environment temperature threshold thermal THREMAL-ID [high] [low]	此命令用于恢复默认设置。

为高温传感器配置环境温度阈值:

```
Ruijie# configure terminal
Ruijie(config)# environment temperature threshold thermal 1 high 100 low 20
Ruijie(config)#
```

1.13 access class

以下命令用于指定访问列表。一行最多可应用两个访问列表。如果已应用了两个访问列表，那么尝试应用新的访问列表将被拒绝，直至通过 no 命令删除了已应用的列表才可应用新的列表。

命令	作用
access-class IP-ACL	此命令用于指定一个访问列表，以限制通过命令行来访问。
no access-class IP-ACL	此命令用于删除已应用的列表。
ip http access-class IP-ACL	此命令用于指定一个访问列表，以限制访问 HTTP 服务器。
no ip http access-class IP-ACL	此命令用于取消选中的访问列表。

创建标准 IP 访问列表，以及如何将其指定为通过 Telnet 限制访问的访问列表。只有主机 226.1.1.1 被允许访问服务器。

```
Ruijie# configure terminal
Ruijie(config)# ip access-list standard vty-filter
Ruijie(config-ip-acl)# permit 226.1.1.1 0.0.0.0
Ruijie(config-ip-acl)# exit
Ruijie(config)# line telnet
Ruijie(config-line)# access-class vty-filter
Ruijie(config-line)#
```

创建标准 IP 访问列表，以及如何将其指定为访问 HTTP 服务器的访问列表。只有主机 226.1.1.1 被允许访问服务器。

```
Ruijie# configure terminal
Ruijie(config)# ip access-list http-filter
Ruijie(config-ip-acl)# permit 226.1.1.1 255.255.255.255
Ruijie(config-ip-acl)# exit
Ruijie(config)# ip http access-class http-filter
Ruijie(config)#
```

1.14 密码

以下命令用于启用或禁用密码服务。需要特定等级的确切密码，用以输入权限等级。各等级只具有一个密码，以输入等级。

命令	作用
enable password [level PRIVILEGE-LEVEL] [0 7] PASSWORD	此命令用于设置启用密码，以输入不同的权限等级。
no enable password [level PRIVILEGE-LEVEL]	此命令可使密码返回为空字符串。
service password-encryption	此命令用于为之前存储于配置文件中的密码启用加密。
no service password-encryption	此命令可禁用加密。
password [0 7] PASSWORD	此命令用于创建新一个新密码。
no password	此命令可清除密码。

在 MyEnablePassword 的权限等级为 15 的情况下创建一个 enable 密码：

```
Ruijie# configure terminal
Ruijie(config)# enable password MyEnablePassword
Ruijie# disable
Ruijie# enable Password:*****
Ruijie# show privilege Current privilege level is 15
Ruijie#
```

为之前存储于配置文件中的密码启用加密：

```
Ruijie# configure terminal
Ruijie(config)# service password encryption
Ruijie(config)#
```

为 console 行创建密码:

```
Ruijie# configure terminal
Ruijie(config)# line console 0
Ruijie(config-line)# password 123
Ruijie(config-line)#
```

1.15 http

使用下列命令执行 HTTP 服务的相关功能。

命令	作用
ip http server	此命令用于启用 HTTP 服务器。
no ip http server	此命令用于禁用 HTTP 服务器功能。
ip http secure-server [ssl-service-policy POLICY-NAME]	此命令用于启用 HTTPS 服务器。
no ip http secure-server	此命令用于禁用 HTTPS 服务器功能。
ip http service-port TCP-PORT	此命令用于为 HTTP 服务器指定 TCP 端口号。
no ip http service-port	此命令可将服务端口还原为 80。
ip http timeout-policy idle INT	此命令用于设置 HTTP 服务器连接的闲置超时值，单位以秒计。
no ip http timeout-policy idle	此命令用于设置闲置超时为默认值。
show ip http server	此命令用于获取 HTTP 服务器状态相关的信息。
show ip http secure-server	此命令用于获取 SSL 状态相关的信息。

启用 HTTP 服务器:

```
Ruijie# configure terminal
Ruijie(config)# ip http server
Ruijie(config)#
```

启用 HTTPS 服务器功能，以及如何使用名为“sp1”的 HTTPS 服务策略:

```
Ruijie# configure terminal
Ruijie(config)# ip http secure-server ssl-service-policy sp1
Ruijie(config)#
```

配置 HTTP TCP 端口号为 8080:

```
Ruijie# configure terminal
Ruijie(config)# ip http service-port 8080
Ruijie(config)#
```

配置闲置超时的值为 100 秒:

```
Ruijie#configure terminal
Ruijie(config)#ip http timeout-policy idle 100
Ruijie(config)#
```

显示 HTTP 服务器状态相关的信息:

```
Ruijie#show ip http server
ip http server state :      enable
Ruijie#
```

显示 SSL 状态相关的信息:

```
Ruijie#show ip http secure-server
ip http secure-server state :disable
Ruijie#
```

1.16 启用和禁用 telnet

通过执行以下命令打开网络设备的 Telnet Server 服务。

命令	作用
enable service telnet-server	此命令用于启用一个 Telnet 服务器。
no enable service telnet-server	此命令用于禁用 Telnet 服务器功能。

启用 Telnet 服务器:

```
Ruijie# configure terminal
Ruijie(config)# enable service telnet-server
Ruijie(config)#
```

1.17 终端

使用以下命令设置终端的相关功能。

命令	作用
show terminal	此命令用于获取用于当前终端行的终端配置参数设置相关信息。
terminal length NUMBER	此命令用于配置屏幕上显示的行的数量。
no terminal length	此命令用于恢复默认设置。
terminal length default NUMBER	此命令用于设置默认值。
no terminal length default	此命令用于恢复默认值。
terminal speed BPS	此命令用于设置终端速度。
no terminal speed	此命令用于恢复默认设置。
terminal width NUMBER	此命令用于为当前会话行设置终端屏幕上字符列的数量。
no terminal width	此命令用于恢复默认设置。
terminal width default NUMBER	此命令用于设置默认值。
no terminal width default	此命令用于恢复默认值。

显示用于当前终端行的终端配置参数设置相关信息:

```
Ruijie# show terminal
Terminal Settings:Length:24 lines
Width:80 columns Default Length:24 lines
Default Width:80 columns Baud rate:9600 bps

Ruijie#
```

将屏幕显示的行数更改为 60:

```
Ruijie# terminal length 60
Ruijie#
```

配置串行端口波特率为 9600bps:

```
Ruijie# configure terminal
Ruijie(config)# terminal speed 9600
Ruijie(config)#
```

将当前会话终端的宽度调整为 120 个字符:

```
Ruijie# show terminal

Length:24 lines
Width:80 columns Default Length:24 lines
Default Width:80 columns Baud rate:9600

Ruijie# terminal width 120 Ruijie# show terminal

Length:24 lines
Width:120 columns Default Length:24 lines Default Width:80 columns Baud rate:9600

Switch #
```

1.18 显示用户

在 EXEC 模式或任何配置模式下使用 show users 命令查看登录用户。

命令	作用
show users	该命令用于显示交换机上活跃用户的相关信息。

显示会话信息:

```
Ruijie# show users

Type      User-Name      Privilege Login-Time  IP address
-----
* console Anonymous  15      2M57S

Total Entries:1

Ruijie#
```

1.19 会话超时

在命令行配置模式下使用此命令设置会话超时。

命令	作用
session-timeout MINUTES	此命令用于配置行会话超时的值。
no session-timeout	此命令用于恢复默认设置。

将 console 会话配置成“从不超时”:

```
Ruijie# configure terminal
Ruijie(config)# line console 0
Ruijie(config-line)# session-timeout 0
Ruijie(config-line)#
```

1.20 用户名

在全局配置模式下使用以下命令创建或删除用户账户。当用户通过等级 1 登录时，用户将处于用户 EXEC 模式。用户需要进一步使用“enable”命令，以进入特权 EXEC 模式。

当用于以高于或等于 2 的等级登录时，用户将直接进入特权 EXEC 模式。因此，特权 EXEC 模式可用于等级 2-15。

用户可指定加密形式或纯文本形式的密码。如果是纯文本形式，但又启用了服务密码加密项，那么密码将被转换成加密形式。如果在未指定用户名的情况下使用了“no username”命令，¹将删除所有的用户。

默认情况下，用户账户为空。当用户账户为空时，用户将直接以等级 1 进入用户 EXEC 模式。用户可使用“enable”命令进一

步进入特权 EXEC 模式。

命令	作用
username NAME [privilege LEVEL] [nopassword password [0 7] PASSWORD]	此命令用于创建一个用户账户。
no username [NAME]	此命令用于删除用户账户。

创建名为“admin”的管理用户，以及一个名为“mypassword”的密码：

```
Ruijie# configure terminal
Ruijie(config)# username admin privilege 15 password 0 mypassword
Ruijie(config)#
```

通过用户 admin 删除用户账户：

```
Ruijie# configure terminal
Ruijie(config)# no username admin
Ruijie(config)#
```

2 LINE 模式

2.1 Line

在全局配置模式下执行此命令设置 SSH 终端行的类型和配置模式。

命令	作用
<code>line {console telnet ssh}</code>	此命令用于识别配置的行类型和输入行配置模式。

输入 SSH 终端行的行配置模式，并将其访问类型配置为 vty-filter:

```
Ruijie# configure terminal
Ruijie(config)# line ssh
Ruijie(config-line)# access-class vty-filter
Ruijie(config-line)#
```

3 系统升级

3.1 系统中的映像概述

本文中所提到的“映像”指的是，以文件或者数据块形式存储在设备各个存储介质中的各种功能的软件程序。所有的锐捷网络设备销售时都已经预装了特定版本的映像。用户可以通过更新这些映像，将设备升级到最新版本。通过 `show switch` 命令，可以了解当前设备上各种映像的版本，以及运行的主程序名称。

RGOS 软件主要有如下几种类型的映像：

- 主程序：有时也称为 FIRMWARE。它是一个完整的设备映像软件包。它可能包含设备的引导程序映像等。当设备启动的时候，它将被装载，并且执行设备上的各种业务。用户一般使用操作的都是主程序映像。
- PROM：最基本的设备初始化和引导程序。这个映像在上电是最早被运行。它一般不会被升级，用于保证系统能够始终被正确的初始化，以及引导和升级主程序。

在以上的程序映像中，主程序可以使用文件系统命令查看并且可以通过文件系统命令对该文件进行更新和修改。PROM 则通常是保存在并行 flash 中，用户无法直接管理。

映像集的更新

用户一般期望通过升级得到更加稳定的软件版本和更多的软件特性。在绝大部分情况下，这些特性都是针对主程序而言的。因此这里所说的升级文件一般是指主程序的更新，同时设备中可以存在多份功能各不相同的主程序映像，并且这些主程序映像之间可以相互切换（通过 `config firmware image` 命令配置下一次启动时所引导的主程序）

工作原理

设备在升级的时候，首先用户需要通过文件系统操作，将新版本的主程序映像（FIRMWARE）拷贝到设备上。之后用户可以将该主程序映像配置为下一次启动时所引导的主程序。系统将自动保障升级后整机的兼容性，而不需要用户做更多的识别。

3.2 启动

使用下列命令指定启动时加载的文件。默认的启动配置文件名为 `config.cfg`。如果没有有效的配置文件，设备将被配置为默认状态。

命令	作用
<code>boot config URL</code>	此命令用于指定下次启动时加载的配置文件。
<code>boot image [check] URL</code>	此命令用于指定下次启动时加载的映像文件。
<code>show boot</code>	此命令用于显示启动配置文件和启动映像设置。

将文件“`switch-config.cfg`”配置为启动配置文件：

```
Ruijie# configure terminal
Ruijie(config)# boot config c:/switch-config.cfg
Ruijie(config)#
```

指定交换机应该使用名为“`switch-image1.had`”的映像文件作为下次启动时的引导映像文件：

```
Ruijie# configure terminal
Ruijie(config)# boot image c:/switch-image1.had
Ruijie(config)#
```

检查一个指定的名为“C:/runtime.switch.had”映像文件。映像文件的校验和已被验证为正常，并显示映像文件的信息：

```
Ruijie# configure terminal
Ruijie(config)# boot image check c:/runtime.switch.had

-----
Image information
-----
Version:1.00.009
Description:RG-NBS5552XG Gigabit Ethernet Web-Smart Switch

Ruijie(config)#
```

检查一个指定的名为“runtime.wrongswitch.had”映像文件。映像文件的校验和已被验证为错误，并显示一条错误消息：

```
Ruijie# configure terminal
Ruijie(config)#boot image check runtime.wrongswitch.had
ERROR: Invalid firmware image.

Ruijie(config)#
```

显示系统启动信息：

```
Ruijie# show boot

Boot image: c:/bootimage.had
Boot config: c:/def_usr.cfg

Ruijie#
```

3.3 复位系统

使用此命令将系统恢复为默认设置。使用此命令之前，请使用 copy 命令保存配置的备份，或将配置文件上传到 TFTP 服务器。此命令会将交换机恢复到出厂默认设置。对交换机所做的所有配置都将丢失。如要保留最近的配置，强烈建议在恢复出厂设置之前备份配置文件。

命令	作用
reset system	此命令用于复位系统，清除系统的配置，然后保存并重新启动交换机。

将交换机恢复到出厂默认设置：

```
Ruijie# reset system

This command will clear the system's configuration to the factory default settings,
including the IP address.
Clear running configuration?(y/n) [n]      n
```

3.4 复制

使用下列命令执行复制操作。为了表示文件位于远程 TFTP 服务器上，URL 必须带有前缀“TFTP://”。

命令	作用
copy SOURCE-URL DESTINATION-URL	此命令用于在文件系统中将一个文件复制到另一个文件。
copy SOURCE-URL tftp://LOCATION/DESTINATION-URL	此命令用于复制源 URL。
copy tftp://LOCATION/SOURCE-URL DESTINATION-URL	此命令用于复制目的 URL。

从地址为 10.1.1.254 的 TFTP 服务器上下载名为 “switch-config.cfg” 的配置，并利用增量方式配置交换机的运行配置：

```
Ruijie# copy tftp://10.1.1.254/switch-config.cfg running-config

Address of remote host [ ]?10.1.1.254
Source filename [ ]? switch-config.cfg
Destination filename running-config?[y/n]: y

Accessing tftp://10.1.1.254/switch-config.cfg...
Transmission start...
Transmission finished, file length 45421 bytes.
Executing script file switch-config.cfg .....
Executing done

Ruijie#
```

将运行配置上传到 TFTP 服务器进行存储：

```
Ruijie# copy running-config tftp://10.1.1.254/switch-config.cfg

Address of remote host [ ]?10.1.1.254
Destination filename [ ]? switch-config.cfg
Accessing tftp://10.1.1.254/switch-config.cfg...
Transmission start...
Transmission finished, file length 45421 bytes.

Ruijie#
```

将系统的运行配置保存到 FLASH 内存，并设定为下次启动时的配置：

```
Ruijie# copy running-config startup-config

Destination filename startup-config?[y/n]: y

Saving all configurations to NV-RAM.....Done.

Ruijie#
```

通过增量方式来立即运行 NVRAM 中的 “switch-config.cfg” 文件：

```
Ruijie# copy flash: switch-config.cfg running-config

Source filename [switch-config.cfg]?
Destination filename running-config?[y/n]: y

Executing script file switch-config.cfg .....
Executing done

Ruijie#
```

将映像文件从 TFTP 服务器上下载到堆栈中的所有单元：

```
Ruijie# copy tftp://10.1.1.254/image.had flash: image.had

Address of remote host [10.1.1.254]?
Source filename [image.had]?
Destination filename [image.had]?
Accessing tftp://10.1.1.254/image.had...
Transmission start...
Transmission finished, file length 8315060 bytes.
Transmission to slave start..... Done.
Transmission to slave finished, file length 8315060 bytes.
Please wait, programming flash.....Done.
Wait slave programming flash complete...Done.

Ruijie#
```

4 文件系统

4.1 文件系统概述

本章介绍 RGOS 软件上的文件系统管理。RGOS 文件管理提供跨平台的统一的文件管理功能。不论设备的型号和存储介质的类型以及进行文件传输的协议类型，都将采用相同的文件管理接口。

RGOS 本地有多种存储介质，比如 USB(Universal Serial BUS)和 flash，而存储介质还可能分布在不同的板卡上，比如主设备和从设备上。RGOS 还能够支持和远程设备实现文件交换，比如通过 xmodem 和 tftp 协议和远程设备实现文件交换。这些功能都将使用相同的文件管理命令来实现。

不是所有设备类型和文件系统类型都支持本章描述的所有文件系统命令。因为不同型号的设备 and 软件版本支持不同类型的文件操作。在使用的时候，可以通过帮助命令来了解当前文件操作命令所支持的存储介质类型和协议。

RGOS 设备上的文件系统管理为设备上的各种文件相关的操作提供统一的命令接口。它能够提供如下主要的特性：

- 使用 URL 来定位文件
- 显示文件系统信息
- 管理本地设备上的文件
- 通过通信协议传递文件

4.2 Cd

使用此命令更改一个当前目录。如果未指定 URL，则不会更改当前目录。

命令	作用
cd [DIRECTORY-URL]	此命令用于更改一个当前目录。

将当前目录更改至文件系统“c:/”盘上的目录“日志”：

```
Ruijie# dir
Directory of /c:
 1 d   0 Dec 29 2013 17:49:36   images
 2 d   0 Jan 02 2013 18:42:53   configurations
 3 d   0 Jan 02 2013 18:42:53   log
 4 -   639 Jan 03 2013 12:09:32  new_config.cfg

20578304 bytes total (3104544 bytes free)

Ruijie#cd c:/log
Ruijie#dir
Directory of /c:/log      No files in directory
20578304 bytes total (3104544 bytes free)

Ruijie#
显示当前目录:
Ruijie# cd
Current directory is /c:/log

Ruijie#:
```

该例演示了如何显示当前目录：

```
Ruijie# cd
Current directory is /c:/log

Ruijie#
```

4.3 删除

使用此命令删除一个文件。不能删除指定作为启动文件的固件镜像或配置文件。

命令	作用
delete FILE-URL	此命令用于删除一个文件。

删除本地 flash 上文件系统中名为“test.txt”的文件：

```
Ruijie# delete c:/test.txt
Delete test.txt?(y/n) [n] y
File is deleted
Ruijie#
```

4.4 Dir

使用此命令显示文件信息或指定路径名称中的文件列表。如果未指定 URL，则使用当前目录。默认情况下，当前目录位于本地 flash 中文件系统的根目录中。存储媒体安装在文件系统中，对于用户来说，即为根目录下的子目录。

用户通过根目录的 dir 命令可显示支持的文件系统。通过 show storage media 命令可显示映射到文件系统的存储媒体。

命令	作用
dir [URL]	此命令用于显示文件信息或指定路径名称中的文件列表。

显示独立交换机中的根目录：

```
Ruijie# dir /
Directory of /
1 d-- 0 Jun 31 2013 17:49:36      c:
0 bytes total (0 bytes free)
Ruijie#
```

4.5 Mkdir

使用 mkdir DIRECTORY-NAME 命令在特权 EXEC 模式下创建一个目录。

命令	作用
mkdir DIRECTORY-NAME	此命令用于在当前目录下创建一个目录。

在当前目录下创建一个名为“newdir”的目录：

```
Ruijie# mkdir newdir
Ruijie#:
```

4.6 More

该命令通常用于显示文本文件。如果文件内容包含了非标准的可打印字符，显示出来的内容将为无法读取的字符，甚至是空格。

命令	作用
more FILE-URL	该命令用于显示文件系统中的文件内容。

显示文件名为“usr_def.conf”的内容：

```
Ruijie# more /c:/configuration/usr_def.conf

!SBG-3000 Series
!Firmware Version:1.00.009
!Slot Model
!-----
!1 SBG-3000-244P
!2 -
!3 SBG-3000-244P
!4 SBG-3000-244P
!
ip igmp snooping vlan 1
!.
end

Ruijie#
```

4.7 重命名

使用该命令可以将一个文件重命名为位于相同目录或其他目录下的文件。

命令	作用
rename FILE-URL1 FILE-URL2	此命令用于重新命名一个文件。

将一个文件名为“doc.1”的文件重新命名为“test.txt”：

```
Ruijie# rename /c:/doc.1 /c:/test.txt

Rename file doc.1 to text.txt?(y/n) [n] y

Ruijie#
```

4.8 Rmdir

在特权 EXEC 模式下，使用此命令删除当前目录下的一个目录。

命令	作用
rmdir DIRECTORY-NAME	此命令用于在工作目录下移除一个目录。

使用参数“recursive”删除一条目录，在当前目录下移除一个名为“newdir”的目录：

```
Ruijie# rmdir newdir

Remove directory newdir?(y/n) [n] y
The directory is removed

Ruijie#
```

4.9 显示存储媒体信息

在 EXEC 模式或任何配置模式下使用 show storage media-info 命令显示存储媒体信息。

命令	作用
show storage media-info	此命令用于显示存储媒体信息。

显示所有部件的存储媒体信息:

```
Ruijie# show storage media-info  


| Drive | Media Type | Size  | FS-Type | Label |
|-------|------------|-------|---------|-------|
| c:    | Flash      | 24 MB | FFS     |       |

  
Ruijie#
```

5 配置文件管理

5.1 配置文件概述

随着网络的快速发展，网络环境越来越复杂，配置信息越来越多，对网管的要求也越来越高。配置信息的变化可能对整个网络产生不可预知的影响，因此，对配置文件的管理显得尤为重要。通过拷贝当前运行配置文件和启动配置文件、逐行比较两个文件中命令差异的方式可以确定配置是否发生变化，同时配置文件管理可以在配置发生变化并保存后，记录日志提醒管理人员。

配置文件管理基本特性

配置文件管理包括显示，设置，备份，更新，保存设备的配置。

5.2 启动配置

使用此命令启用加载的配置文件。默认的启动配置文件名为 config.cfg。如果没有有效的配置文件，设备将被配置为默认状态。

命令	作用
boot config URL	此命令用于指定下次启动时加载的配置文件。

将文件“switch-config.cfg”配置为启动配置文件：

```
Ruijie# configure terminal
Ruijie(config)# boot config c:/switch-config.cfg
Ruijie(config)#
```

5.3 运行配置

使用以下命令显示或清除留在 DRAM 的系统配置。

命令	作用
clear running-config	此命令用于清除留在 DRAM 的系统配置。
show running-config	此命令用于显示运行配置文件中的命令。

清除系统正在运行的配置：

```
Ruijie# clear running-config

This command will clear the system's configuration to the factory default settings,
including the IP address.
Clear running configuration?(y/n) [n] y

Ruijie#
```

显示正在运行的配置文件的内容:

```
Ruijie#show running-config
Building configuration...

Current configuration : 4795 bytes

#-----
#           RG-NBS5552XG Full Gigabit Security & Intelligence Access Switch
#                               Configuration
#
#           Firmware: Build 10.4(1) Release(00003)
#           Copyright(C) 2014 Ruijie Networks. All rights reserved.
#-----
class-map cos
class-map police
match access-group name
class-map class-dscp-red
#
username admin password 0 admin

username admin privilege 15
#
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

5.4 配置替换

此命令将使用指定配置文件的内容替换当前运行的配置。因此，指定的配置文件被假定为一个完整的配置，而不是部分配置。使用 `configure replace` 命令之前，请使用 `copy` 命令保存配置的备份，或将配置文件上传到 TFTP 服务器。

命令	作用
<code>configure replace</code> <code>{(tftp://location/filename</code> <code>flash:FILENAME) [force]</code>	此命令用于以指定的配置文件替换当前运行的配置。

从 TFTP 服务器上下载 “config.cfg” 文件，并用它替换当前运行的配置:

```
Ruijie# configure replace tftp://10.0.0.66/config.cfg

This will apply all necessary additions and deletions to replace the current running
configuration with the contents of the specified configuration file, which is assumed
to be a complete configuration, not a partial configuration.[y/n]:      y

Accessing tftp://10.0.0.66/config.cfg...
Transmission start...
Transmission finished, file length 45422 bytes.
Executing script file config.cfg .....
Executing done

Ruijie#
```

使用存储在设备的 NVRAM 中特定的配置文件 “config.cfg” 来替换当前运行的配置。立即执行命令，无需确认:

```
Ruijie# configure replace flash: config.cfg force

Executing script file config.cfg .....
Executing done

Ruijie#
```

5.5 显示启动配置

使用 `show startup-config` 命令显示启用配置文件的内容。

命令	作用
----	----

show startup-config

此命令用于显示启动配置文件的内容。

显示启动配置文件的内容:

```
Ruijie#show startup-config
#-----
#           RG-NBS5552XG Full Gigabit Security & Intelligence Access Switch
#                   Configuration
#
#           Firmware: Build 10.4(1) Release(00003)
#           Copyright(C) 2014 Ruijie Networks. All rights reserved.
configure terminal

#
#
#
username admin password 0 admin
username admin privilege 15
#
#
#
line cty 0 17
 login local
 exit
#
#
#
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

6 系统管理

6.1 监控会话

使用以下命令执行监控会话相关操作。

命令	作用
<code>monitor session SESSION-NUMBER destination interface INTERFACE-ID</code>	此命令用于为端口监控会话配置目的端口，使得通过源端口的报文在目的端口上得到监测。
<code>no monitor session SESSION-NUMBER destination interface INTERFACE-ID</code>	此命令用于删除端口监控会话的目的端口。
<code>monitor session SESSION-NUMBER source interface {INTERFACE-ID [, -] [both rx tx] cpu rx}</code>	此命令用于配置端口监控会话的源端口。
<code>no monitor session SESSION-NUMBER source interface {INTERFACE-ID [, -] cpu rx }</code>	此命令用于从端口监控会话中删除源端口。
<code>no monitor session SESSION-NUMBER</code>	此命令用于删除端口监控会话。
<code>monitor session SESSION-NUMBER source acl ACCESS-LIST-NAME</code>	该命令用于配置访问列表到基监控会话，实现基于流的监控。
<code>no monitor session SESSION-NUMBER source acl ACCESS-LIST-NAME</code>	此命令用于从基于流的监控会话中删除访问列表。
<code>show monitor session [SESSION-NUMBER]</code>	此命令用于显示所有或特定端口监控会话。

使用会话编号 1 创建端口监控会话。它指定一个物理端口 0/1 为目的端口和三个物理源端口（端口 0/2，0/3 和 0/4）作为监控会话的源端口：

```
Ruijie# configure terminal
Ruijie(config)# monitor session 1 destination interface gi0/1
Ruijie(config)# monitor session 1 source interface gi0/2-4
Ruijie(config)#
```

使用会话编号 1 创建端口监控会话。

它指定分配一个物理端口 0/1 为目的端口和三个物理端口（0/2，0/3 和 0/4）作为监控会话的源端口：

```
Ruijie# configure terminal
Ruijie(config)# monitor session 1 destination interface gi0/1
Ruijie(config)# monitor session 1 source interface gi0/2-4
Ruijie(config)#
```

使用会话编号 2 创建监控会话。指定 MAC 地址列表 MAC-Monitored-flow 作为监控源：

```
Ruijie# configure terminal
Ruijie(config)# monitor session 2 destination interface gi0/1
Ruijie(config)# monitor session 2 source acl MAC-Monitored-flow
Ruijie(config)#
```

显示编号为 1 的端口监控会话：

```
Ruijie# show monitor session 1

Session 1
  Session Type: local session
  Destination Port: GigabitEthernet0/1
  Source Ports:
    Both:
      GigabitEthernet0/2
      GigabitEthernet0/3
      GigabitEthernet0/4
    RX:
      GigabitEthernet0/5
    TX:
      GigabitEthernet0/7
```

Total Entries: 1
Ruijie#

7 系统日志

7.1 系统日志概述

设备在运行过程中，会发生各种状态变化如链路状态 UP、DOWN 等，也会遇到一些事件如收到异常报文、处理异常等。锐捷产品日志提供一种机制，在状态变化或发生事件时，就自动生成固定格式的消息（日志报文），这些消息可以被显示在相关窗口（控制台等）上或被记录在相关媒介（内存缓冲区、文件系统）上或发送到网络上的一组日志服务器上，供管理人员分析网络情况和定位问题。

7.2 启用命令记录

在全局配置模式下执行此命令，该操作不会影响交换机配置或操作的命令将不会被记录，比如 show 命令。保存或查看系统日志的信息将在系统日志功能规格中进行描述。使用 no 命令禁止命令记录功能。

注意:交换机在 BAT 进程下时，（比如正在启动，执行下载配置文件，等等），将不会记录所有的配置命令。

命令	作用
command logging enable	此命令用于记录已通过命令行，在交换机上成功配置的命令。
no command logging enable	此命令将禁用命令记录功能。

启用命令记录功能:

```
Ruijie# configure terminal
Ruijie(config)# command logging enable
Ruijie(config)#
```

7.3 删除日志

在特权 EXEC 模式下使用 clear logging 命令清除日志信息。

命令	作用
clear logging	此命令用于删除系统日志缓冲区中的日志信息。

删除日志缓冲区中的所有日志信息:

```
Ruijie# enable
Ruijie# clear logging
Clear logging?(y/n) [n] y
Ruijie#
```

7.4 日志缓冲

在全局配置模式下设置系统消息记录方式。使用默认的 logging buffered 命令可返回默认设置。

命令	作用
logging buffered [SIZE] [SEVERITY-LEVEL SEVERITY-NAME]	此命令可以将系统消息记录到本地消息缓冲区。
no logging buffered	此命令用于禁用将消息记录到本地消息缓冲区。
default logging buffered	此命令用于恢复默认设置。

将消息记录到日志缓冲区，并限制记录的日志的安全级别为错误或更高：

```
Ruijie> enable
Ruijie# configure terminal
Ruijie(config)# logging buffered errors
```

7.5 日志控制台

在全局配置模式下将系统消息记录到本地控制台，使用 no 命令禁用记录并恢复到默认设置。

命令	作用
logging console [severity {SEVERITY-LEVEL SEVERITY-NAME}] [discriminator NAME]	此命令可以将系统消息记录到本地控制台。
no logging console	禁用将消息记录到本地控制台并恢复到默认设置。

将消息记录到本地控制台，并限制记录的日志的安全级别为错误或更高：

```
Ruijie> enable
Ruijie# configure terminal
Ruijie(config)# logging console severity errors
```

7.6 日志鉴别器

在全局配置模式下创建并设置日志鉴别器。使用使用 no 命令恢复到默认设置。

命令	作用
logging discriminator NAME [facility {drops STRING includes STRING}] [severity {drops SEVERITY-LIST includes SEVERITY-LIST }]	此命令用于创建一个鉴别器，并且可以进一步用于过滤发送到不同目的地的系统日志信息。
no discriminator NAME	此命令将恢复到默认设置。

创建一个名为“buffer-filter”的鉴别器，此鉴别器指定了两个子过滤，一个基于严重级别，另一个则基于设备：

```
Ruijie> enable
Ruijie# configure terminal
Ruijie(config)#logging discriminator buffer-filter facility includes STP severity
includes 1-4,6
Ruijie(config)#
```

输入命令 show running-config，验证设置。

7.7 日志服务器

在全局配置模式下使用以下命令设置日志服务器。

命令	作用
logging server { IP-ADDRESS } [severity {SEVERITY-LEVEL SEVERITY-NAME}] [facility { FACILITY-NUM FACILITY-NAME}] [discriminator NAME] [port UDP-PORT]	此命令用于创建一个 SYSLOG 服务器主机，以记录系统消息或调试输出。
no logging server {IP-ADDRESS IPV6-ADDRESS}	此命令用于删除系统日志服务器主机。。

将严重级别超过警告的系统消息记录到远程主机 20.3.3.3：

```
Ruijie> enable
Ruijie# configure terminal
Ruijie(config)# logging server 20.3.3.3 severity warnings
```



```
Ruijie(config)#
```

7.8 显示日志

在 EXEC 模式或任何配置模式使用 show logging 命令显示内存缓冲区中的日志信息。

命令	作用
show logging	此命令用于显示记录在本地信息缓冲区中的系统信息。

显示在本地消息缓冲区中的消息：

```
Ruijie#show logging
Syslog logging: enabled
  Console logging: level debugging
  Monitor logging: disabled
  Buffer logging: level debugging
  File logging: level informational
  File name: /c:/1.txt, size 131072 bytes
  Timestamp debug messages: uptime
  Timestamp log messages: uptime
  Sequence-number log messages: enabled
  Sysname log messages: enabled
  Trap logging: disabled

Log Buffer (4096 bytes):
%SYS-5-WARMSTART: System warm start.
%SYS-5-START: System started up.
%PORT-6-UPDOWN: Interface GigabitEthernet0/16,  changed state to up.
%CLI-6-LOGIN_SUCCESS: User(Anonymous) login from console OK.
Ruijie(config)#
```

7.9 攻击日志

在 EXEC 模式或任何配置模式下执行以下命令，显示或删除攻击日志消息。

命令	作用
show attack-logging unit UNIT-ID [index INDEX]	此命令用于显示攻击日志消息。
clear attack-logging {unit UNIT-ID all}	此命令用于删除攻击日志消息。

显示第一个攻击日志：

```
Ruijie# show attack-logging index 1
Attack log messages (total number:1)
1 2012-10-17 15:00:14 CRIT(2) Land attack is blocked from (IP: 10.72.24.1 Port: 7)
Ruijie#
```

删除所有攻击日志消息：

```
Ruijie# clear attack-logging all
Ruijie#
```

8 POWER

8.1 节能

使用下列命令执行节能配置的相关功能。

命令	作用
power-saving link-detection	此命令用于启用节能链路探测功能。
no power-saving link-detection	此命令用于禁用该功能。
power-saving eee	此命令用于在指定端口启用节能以太网（EEE）功能。
no power-saving eee	此命令用于禁用 EEE 功能。
show power-saving [link-detection] [eee]	此命令用于显示节能配置信息。

启用节能链路探测功能:

```
Ruijie# configure terminal
Ruijie(config)# power-saving link-detection
Ruijie(config)#
```

启用 EEE 节能功能:

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# power-saving eee
Ruijie(config-if)#
```

显示节能配置信息:

```
Ruijie#show power-saving

Link Detection Power Saving
  State:Disabled

EEE_Enabled Ports
gigabitEthernet 0/1

Ruijie#
```

9 调试命令

9.1 调试信息输出

使用下列命令设置调试信息输出。

命令	作用
debug enable	此命令用于启用调试信息输出。
no debug enable	此命令禁用调试信息输出。
debug output {module <MODULE-LIST> all} {buffer console}	此命令用于指定单个模块的调试信息输出。
no debug output { module <MODULE-LIST> all}	此命令用于指定无单个模块的调试信息输出。

启用调试信息输出：

```
Ruijie(config)#debug enable
Ruijie(config)#
```

禁用调试信息输出：

```
Ruijie(config)#no debug enable
Ruijie(config)#
```

配置指定模块(DHCPv6_CLIENT and DHCPv6_RELAY)调试信息输出至调试控制台：

```
Ruijie# debug output module "DHCPv6_CLIENT DHCPv6_RELAY" console
Ruijie#debug show output

Debug Global State : Disabled

Module name      Output      Enabled
-----
DHCPv6_CLIENT   console     No
DHCPv6_RELAY    console     No
.....
Ruijie#
```

9.2 重启操作

使用下列命令在致命错误出现时启用或禁用交换机重启操作。

命令	作用
debug reboot on-error	该命令用于当出现致命错误时，执行交换机重启操作。
no debug reboot on-error	该命令用于当致命错误出现时，不会执行交换机重启操作。

显示当致命错误出现时，如何启用交换机重启操作：

```
Ruijie(config)# debug reboot on-error
Ruijie(config)#
```

9.3 复制

使用以下命令设置是否复制调试信息到目的文件名。

命令	作用
----	----

debug copy SOURCE-URL DESTINATION-URL	该命令用于复制调试信息到目的文件名。
debug copy SOURCE-URL {tftp://LOCATION/DESTINATION-URL}	该命令用于不复制调试信息到目的文件名。

显示如何复制缓冲信息到 TFTP 服务器。(10.90.90.99):

```
Ruijie# debug copy buffer tftp://10.90.90.99/abc.txt
Address of remote host [10.90.90.99]?Destination filename [abc.txt]?
Accessing tftp://10.90.90.99/abc.txt...Transmission starts...
Finished network upload(65739) bytes.
Ruijie#
```

9.4 清除

使用以下命令清除相关信息。

命令	作用
debug clear buffer	该命令用于清除调试缓冲信息。
debug clear error-log	该命令用于清除错误日志信息。

显示如何清除调试缓冲信息):

```
Ruijie# debug clear buffer
Ruijie#
```

显示如何清除错误日志信息:

```
Ruijie# debug clear error-log
Ruijie#
```

9.5 显示

使用以下命令显示相关信息。

命令	作用
debug show error-log	该命令用于显示错误日志信息。
debug show buffer [utilization]	此命令用于显示调试缓冲区内容或调试缓冲区的使用信息。
debug show output	此命令用于显示调试状态或模块的输出信息。
show tech support	显示技术支持人员要求的信息。

显示错误日志信息:

```
Ruijie# debug show error log

# debug log:1
# level: fatal
# clock:10000ms
# time :2013/09/11 13:00:00
===== SOFTWARE FATAL ERROR =====
Invalid mutex handle :806D6480

Current TASK : bcmARL.0
----- TASK STACKTRACE -----
->802ACE98
->8018C814
->8028FF44
->8028352C
->801D703C
->8013B8A4
```

```

->802AE754
->802A5E0C
->802A5D6C

*****
# debug log:2
# level: fatal
# clock:1000ms
# time :2013/09/11 15:00:00
===== SOFTWARE FATAL ERROR =====
CLI_UTL_AllocateMemory Fail!

Current TASK :CLI
----- TASK STACKTRACE -----
->802ACE98
->802B4498
->802B4B00
->802BD140
->802BCB08

Total Log :2
<Output truncated>

```

显示如何清除错误日志信息:

```

Ruijie# debug clear error-log
Ruijie#

```

显示调试缓冲区信息:

```

Ruijie#debug show buffer
Debug buffer is empty
Ruijie#

```

显示调试缓冲区的使用情况:

```

Ruijie# debug show buffer utilization
Debug buffer is allocated from system memory
Total size is 2M
Utilization is 30%

Ruijie#

```

显示模块调试信息的输出信息:

```

Ruijie#debug show output
Debug Global State: Enabled
Module name   Output   Enabled
-----
Sys           console  No
os            buffer   Yes
bgp           buffer   Yes, but no specific output enabled
mstp         buffer   Yes, event brief on all interfaces, bpdu detail on all
interfaces
Ruijie #

```

显示所有模块的技术支持信息:

```

Ruijie# show tech support

#-----
#                               DXS-3600 TenGigabit Ethernet Switch
#                               Technical Support Information
#
#                               Firmware: Build 1.03.B055
#                               Copyright(C) 2011 D-Link Corporation. All rights reserved.
#-----

***** Basic System Information *****

[SYS 2009-9-8 08:59:20]

```

Boot Time : 8 Sep 2009 08:54:00
RTC Time : 2009/09/08 08:59:20
Boot PROM Version : Build 1.10.-B09
Firmware Version : Build 1.03.B055
Hardware Version :
MAC Address : 00-01-02-03-04-05
MAC Address Number : 0A2G

***** System Log *****

[SYS_LOG 2009-9-8 08:59:20]

Index	Date	Time	Level	Log Text
4	2009-09-08	08:54:58	INFO(6)	Successful login through Console (Username: Anonymous)
3	2009-09-08	08:54:32	INFO(6)	Port 4 link up, 100Mbps FULL duplex
2	2009-09-08	08:54:27	CRIT(2)	System started up
1	2009-09-08	08:54:27	INFO(6)	MSTP(8):Spanning Tree MST configuration ID name and revision level change (name:00:01:02:03:04:05 revision level:0)

***** Layer One Information *****

[PORT 2009-9-8 09:18:22]

[MIRROR 2009-9-8 09:18:22]

***** Mirror *****

Mirror SW table:
State: Disable

***** Layer Two Information *****

[VLAN 2009-9-8 09:18:22]

[LBD 2009-9-8 10:56:47]

LBD is disable

[TRAFFIC_SEG 2009-9-8 10:56:47]

.....
Ruijie#



配置指南-以太网交换

本分册介绍系统配置配置指南相关内容，包括以下章节：

1. 接口
2. MAC 地址
3. 链路聚合控制协议 (LACP)
4. VLAN
5. MSTP
6. LLDP

1 接口

1.1 线缆诊断

使用以下命令启动线缆诊断，显示或清除诊断测试结果。

命令	作用
<code>test cable-diagnostics interface INTERFACE-ID [, -]</code>	此命令用于启动线缆诊断，测试线缆状态和长度。
<code>show cable-diagnostics [interface INTERFACE-ID [, -]]</code>	此命令用于显示线缆诊断的测试结果。
<code>clear cable-diagnostics {all interface INTERFACE-ID [, -]}</code>	此命令用于清除线缆诊断的测试结果。

启动线缆诊断，测试铜线缆的状态和长度：

```
Ruijie# test cable-diagnostics interface gigabitEthernet 0/1
Ruijie#
```

显示线缆诊断的测试结果：

```
Ruijie# show cable-diagnostics gigabitEthernet0/1-8

Port    Type    Link Status    Test Result    Cable Length (M)
-----
-----
Gi0/1   1000BASE-T    Link Up OK     65
Gi0/2   1000BASE-T    Link Up OK     -
Gi0/3   1000BASE-T    Link Down     Shutdown      25
Gi0/4   1000BASE-T    Link Down     Shutdown      -
Gi0/5   1000BASE-T    Link Down     Unknown       -
Gi0/6   1000BASE-T    Link Down     Pair 1 Crosstalk at 30M -
Pair 2 Crosstalk at 30M Pair 3 OK at 110M
Pair 4 OK at 110M
Gi0/7   1000BASE-T    Link Down     NO Cable
Gi0/8   1000BASE-T    Link Down     Pair 1 Open at 16M -
Pair 2 Open at 16M
Pair 3 OK at 50M
Pair 4 OK at 50M

Ruijie#
```

清除线缆诊断的测试结果：

```
Ruijie# clear cable-diagnostics interface gigabitEthernet 0/1
Ruijie#
```

1.2 显示接口收发器

在 EXEC 模式或任何配置模式下使用此命令显示接口收发器参数。

命令	作用
<code>show interfaces [INTERFACE-ID [, -]] transceiver [diagnosis]</code>	此命令用于显示指定端口当前的 SFP 模块参数以及 SFP 模块运行收发器监控参数值。

显示收发器端口的当前运行参数:

```
Ruijie#show interfaces transceiver

=====Interface TenGigabitEthernet 0/49=====
Transceiver Type      : 1000BASE-LX
Connector Type       : SFP LC
Wavelength(nm)      : 1310
Transfer Distance    :
  SMF Fiber
  -- 10km:
  50/125 um OM2 fiber
  -- 550m:
  62.5/125 um OM1 fiber
  -- 550m:
Digital Diagnostic Monitoring : NO
Vendor Serial Number   : D001135000093

=====Interface TenGigabitEthernet 0/50=====
Interface TenGigabitEthernet 0/50 : the transceiver is absent!

=====Interface TenGigabitEthernet 0/51=====
Interface TenGigabitEthernet 0/51 : the transceiver is absent!

=====Interface TenGigabitEthernet 0/52=====
Interface TenGigabitEthernet 0/52 : the transceiver is absent!
Ruijie#
```

显示用于收发器监控的所有端口的监控详细信息:

```
Ruijie# show interfaces transceiver diagnosis

++ : high alarm, +   : high warning, -   : low warning, -- : low alarm
mA: milliamperes, mW: milliwatts
A:The threshold is administratively configured.

gi0/25
Transceiver Monitoring is enabled
Transceiver Monitoring shutdown action: Alarm

Current High-Alarm      High-Warning      Low-Warning      Low-Alarm      Temperature(C) 30.090
75.000(A)      70.000 0.000 -5.000
Voltage (v)      3.353 3.630 3.465 3.135 2.970
Bias Current(mA)      16.794(++), 10.500 9.000 2.500 2.000
TX Power (mW)      0.258 1.413 0.708 0.186 0.074
RX Power (mW)      0.000(--), 1.585 0.794 0.102 0.041

Ruijie#
```

1.3 transceiver-monitoring action shutdown

使用该命令禁用一个接口。这种配置对物理端口有效。该命令也可以配置聚合端口成员端口。使用该命令将导致端口进入禁用状态。在禁用状态下，端口将无法接收或发送任何数据包。使用“no”命令，移除一个条目。关闭一个端口也将同时关闭链接状态。

命令	作用
transceiver-monitoring action shutdown {alarm warning}	出现警告信息或异常状态时，此命令可用于关闭一个端口。
no transceiver-monitoring action shutdown	此命令用于禁用关闭操作。

显示当检测到告警事件时，如何关闭接口 tenGigabitEthernet 0/28:

```
Ruijie# configure terminal
```

```
Ruijie(config)# interface tenGigabitEthernet 0/28
Ruijie(config-if)# transceiver-monitoring action shutdown alarm
Ruijie(config-if)#
```

1.4 transceiver-monitoring bias-current

使用此命令在指定的端口上配置偏置电流的阈值。该配置仅适合带收发器监控的光模块 SFP/SFP+接口。该值将保存在系统和 SFP/SFP+收发器中，并转为 16 位格式，再写入 SFP 模块中。

如果正在配置的 SFP 模块不支持阈值更改，则用户配置的阈值将保存在系统中，显示的数值为用户配置的阈值。如果用户配置的阈值不存在，显示的值则为供应商定义的出厂预设值。

命令	作用
transceiver-monitoring bias-current INTERFACE-ID {high low} {alarm warning} VALUE	此命令用于在指定的端口上配置偏置电流的阈值。
no transceiver-monitoring bias-current INTERFACE-ID {high low} {alarm warning}	此命令用于清除系统中已配置的阈值。

在接口 tenGigabitEthernet 0/28 上配置偏置电流告警高阈值 10.237:

```
Ruijie# configure terminal
Ruijie(config)# transceiver-monitoring bias-current tenGigabitEthernet 0/28 high
warning 10.237

WARNING:A closest value 10.236 is chosen according to the transceiver-monitoring
precision definition.

Ruijie(config)#
```

1.5 启用收发器监控

用户可通过该命令启用或禁用 SFP 端口的光纤收发器监控功能。启用监控功能后，如果正在监控的参数高于告警高阈值或低于告警低阈值，则发出告警信息。如果正在监控的参数高于警报高阈值或低于警报低阈值，则发出警报信息。

命令	作用
transceiver-monitoring enable	此命令用于启用 SFP 端口的光纤收发器监控功能。
no transceiver-monitoring enable	此命令用于禁用光纤收发器监控。

在接口 tenGigabitEthernet 0/28 上启用收发器监控:

```
Ruijie# configure terminal
Ruijie(config)# interface tenGigabitEthernet 0/28
Ruijie(config-if)# transceiver-monitoring enable
Ruijie(config-if)#
```

1.6 transceiver-monitoring rx-power

此命令用于指定或清除输入功率阈值。该配置只对带有收发器监控能力的光模块 SFP/SFP+接口有效。该值将保存在系统和 SFP/SFP+收发器中，并转为 16 位格式，再写入 SFP 模块中。

如果正在配置的 SFP 模块不支持阈值更改，则用户配置的阈值将保存在系统中，显示的数值为用户配置的阈值。如果用户配置的阈值不存在，显示的值则为供应商定义的出厂预设值。

使用 no 命令清除系统中已配置的阈值。没有更改保存在 SFP/SFP+收发器中的阈值。可阻止对新插入的 SFP/SFP+收发器的阈值进行更改。

命令	作用
transceiver-monitoring rx-power INTERFACE-ID {high low} {alarm warning} {mwatt VALUE dbm VALUE}	此命令用于为指定的端口配置输入功率阈值。
no transceiver-monitoring rx-power INTERFACE-ID {high low} {alarm warning}	此命令用于清除系统中已配置的阈值。

在接口 tenGigabitEthernet 0/28 上配置 RX 功率告警低阈值 0.135 mW:

```
Ruijie# configure terminal
Ruijie(config)# transceiver-monitoring rx-power tenGigabitEthernet 0/28 low warning
mwatt 0.135
Ruijie(config)#
```

1.7 transceiver-monitoring temperature

此命令用于指定或清除温度阈值。该配置只对带有收发器监控能力的光模块 SFP/SFP+接口有效。

该值将保存在系统和 SFP/SFP+收发器中，并转为 16 位格式，再写入 SFP 模块中。

如果正在配置的 SFP 模块不支持阈值更改，则用户配置的阈值将保存在系统中，显示的数值为用户配置的阈值。如果用户配置的阈值不存在，显示的值则为供应商定义的出厂预设值。

使用 no 命令清除系统中已配置的阈值。没有更改保存在 SFP/SFP+收发器中的阈值。可阻止对新插入的 SFP/SFP+收发器的阈值进行更改。

命令	作用
transceiver-monitoring temperature INTERFACE-ID {high low} {alarm warning} VALUE	此命令用于配置指定端口的温度阈值。
no transceiver-monitoring temperature INTERFACE-ID {high low} {alarm warning}	此命令用于清除系统中已配置的阈值。

在接口 tenGigabitEthernet 0/28 上配置温度告警高阈值 127.994:

```
Ruijie# configure terminal
Ruijie(config)# transceiver-monitoring temperature tenGigabitEthernet 0/28 high alarm
127.994

WARNING:A closest value 127.992 is chosen according to the transceiver-monitoring
precision definition.
Ruijie(config)#
```

1.8 transceiver-monitoring tx-power

此命令用于指定或清除输出功率阈值。该配置只对带有收发器监控能力的光模块 SFP/SFP+接口有效。该值将保存在系统和 SFP/SFP+收发器中，并转为 16 位格式，再写入 SFP 模块中。

如果正在配置的 SFP 模块不支持阈值更改，则用户配置的阈值将保存在系统中，显示的数值为用户配置的阈值。如果用户配置的阈值不存在，显示的值则为供应商定义的出厂预设值。

使用 no 命令清除系统中已配置的阈值。没有更改保存在 SFP/SFP+收发器中的阈值。可阻止对新插入的 SFP/SFP+收发器的阈值进行更改。

命令	作用
----	----

transceiver-monitoring tx-power INTERFACE-ID {high low} {alarm warning} {mwatt VALUE dbm VALUE}	此命令用于配置指定端口的输出功率阈值。
no transceiver-monitoring tx-power INTERFACE-ID {high low} {alarm warning}	此命令用于清除系统中已配置的阈值。

在接口 tenGigabitEthernet 0/28 上配置 TX 功率告警低阈值 0.181 mW:

```
Ruijie# configure terminal
Ruijie(config)# transceiver-monitoring tx-power tenGigabitEthernet 0/28 low warning
mwatt 0.181
Ruijie(config)#
```

1.9 transceiver-monitoring voltage

此命令用于指定或清除端口的阈值电压。该配置只对带有收发器监控能力的光模块 SFP/SFP+接口有效。该值将保存在系统和 SFP/SFP+收发器中，并转为 16 位格式，再写入 SFP 模块中。

如果正在配置的 SFP 模块不支持阈值更改，则用户配置的阈值将保存在系统中，显示的数值为用户配置的阈值。如果用户配置的阈值不存在，显示的值则为供应商定义的出厂预设值。

使用 no 命令清除系统中已配置的阈值。没有更改保存在 SFP/SFP+收发器中的阈值。可阻止对新插入的 SFP/SFP+收发器的阈值进行更改。

命令	作用
transceiver-monitoring voltage INTERFACE-ID {high low} {alarm warning} VALUE	此命令用于配置指定端口的阈值电压。
no transceiver-monitoring voltage INTERFACE-ID {high low} {alarm warning}	此命令用于清除系统中已配置的阈值。

在接口 tenGigabitEthernet 0/28 上配置电压告警低阈值 0.005:

```
Ruijie# configure terminal
Ruijie(config)# transceiver-monitoring voltage tenGigabitEthernet 0/28 low alarm 0.005
Ruijie(config)
```

1.10 errdisable recovery

该命令用于启用，禁用或显示错误恢复。一个端口可由于事件原因处于错误禁用状态，比如端口安全违反，风暴控制等等。当一个端口处于错误禁用状态，尽管正在运行的配置处于“不关闭”状态，端口也会关闭。

有两种方法来恢复错误禁用的端口。管理员可使用 errdisable recovery cause 命令，启用由于各种原因而被禁用的错误端口的自动恢复。或者管理员可首先输入 shutdown 命令手动恢复端口，再对端口使用 no shutdown 命令。

命令	作用
errdisable recovery cause {all psecure-violation storm-control arp- rate dhcp-rate loopback-detection} [interval SECONDS]	此命令用于启用原因的错误恢复，并配置恢复间隔。
no errdisable recovery cause {all psecure-violation storm-control arp- rate dhcp-rate loopback-detection} [interval]	此命令用于禁用自动恢复，或将间隔恢复到默认设置。
show errdisable recovery	此命令用于显示错误禁用恢复定时器相关设置。

为端口安全违反的恢复定时器设置为 200 秒:

```
Ruijie# configure terminal
Ruijie(config)# errdisable recovery cause psecure-violation interval 200
Ruijie(config)#
```

为端口安全隔离启用自动恢复功能:

```
Ruijie# configure terminal
Ruijie(config)# errdisable recovery cause psecurity-violation
Ruijie(config)#
```

显示错误禁用恢复定时器的设置:

```
Ruijie# show errdisable recovery

ErrDisable Cause          State          Interval
-----
Port Security             enabled        200 seconds
Storm Control             disabled       300 seconds
BPDU Attack Protection    disabled       300 seconds
Dynamic ARP Inspection    disabled       300 seconds
DHCP Snooping             disabled       300 seconds
Loop Detection            enabled        300 seconds

Interfaces that will be recovered at the next timeout:

Interface  Errdisable Cause          Time left(sec)
-----
Gi0/3      Loop Detection            297
Gi0/5      Loop Detection            297#

Ruijie#
```

1.11 计数器

在特权 EXEC 模式下使用该命令清除物理接口的统计信息。

命令	作用
<code>clear counters {all interface INTERFACE-ID [, -]}</code>	此命令用于清除物理接口的统计信息。

清除接口 gi0/1 的计数器:

```
Ruijie# clear counters interface GigabitEthernet 0/1
Ruijie#
```

1.12 描述

在接口配置模式下使用此命令为接口添加描述信息。指定对应 RFC 2233 中定义的 MIB 对象“ifAlias”的描述。

命令	作用
<code>description STRING</code>	此命令用于为接口添加描述信息。
<code>no description</code>	此命令用于恢复默认设置。

将描述“Physical Port 10”添加至以太网端口 0/10:

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/10
Ruijie(config-if)# description Physical Port 10
Ruijie(config-if)#
```

1.13 接口

此命令是用于为单一接口输入接口配置模式。接口编号的格式基于接口类型。使用“no”命令，移除一个接口。

对于物理接口，如果交换机的端口不存在，用户则不能设置接口。物理接口不能通过“no”命令删除。

命令	作用
interface INTERFACE-ID	此命令是用于为单一接口输入接口配置模式。
no interface INTERFACE-ID	此命令用于移除一个接口。
interface range INTERFACE-ID [,-]	此命令用于为多个接口设置接口范围配置模式。
show interfaces [INTERFACE-ID [,-]]	此命令用于显示接口信息。
show interfaces [INTERFACE-ID [,-]] counters [errors] rate summary	此命令用于显示指定接口的统计信息。
show interfaces [INTERFACE-ID [,-]] status	此命令用于显示交换机端口的连接状态。
show interfaces [INTERFACE-ID [,-]] utilization	此命令用于显示交换机的端口利用率。
show interfaces [INTERFACE-ID [,-]] auto-negotiation	此命令用于显示物理端口的自动协商详细信息。

为以太网端口 0/5 设置接口配置模式：

```
Ruijie# configure terminal
Ruijie(config)# interface GigabitEthernet 0/5
```

进入 VLAN 1 的接口配置模式：

```
Ruijie# configure terminal
Ruijie(config)# interface vlan1
Ruijie(config-if)#
```

为聚合端口 3 输入接口配置模式：

```
Ruijie# configure terminal
Ruijie(config)# interface aggregatePort 3
Ruijie(config-if)#
```

为端口范围 1/0/1 至 1/0/3 输入接口配置模式：

```
Ruijie# configure terminal
Ruijie(config)# interface range GigabitEthernet0/1-3
Ruijie(config-if-range)#
```

显示接口 VLAN 1 的 VLAN 接口信息：

```
Ruijie#show interfaces vlan 1
Index(dec): 5120, (hex): 1400
VLAN 1 is UP, line protocol is UP
Hardware is VLAN,address is 00-15-52-00-02-06
Description:
Interface address is: 172.18.62.47/8
ARP type: ARPA, ARP Timeout 1200 seconds.

Ruijie#
```

显示 GigabitEthernet0/1 的接口信息：

```
Ruijie#show interfaces gigabitEthernet 0/1

Index(dec):1 (hex):1
GigabitEthernet 0/1 is : DOWN
Hardware is BCM50282 GigabitEthernet
Interface address is: no ip address
MTU 1536 bytes, BW 1000000 Kbit
Switchport attributes:
```

```

interface's description: ""
oper medium-type is Copper
lastchange time: 0 Day: 0 Hour: 0 Minute:0 Second
current status duration: 0 Day: 0 Hour: 33 Minute:56 Second
Priority is 0
admin duplex mode is AUTO, oper duplex is Unknown
admin speed is AUTO, oper speed is Unknown
admin mdix is AUTO, oper mdix is Unknown
flow control admin status is OFF, flow control oper status is Unknown
admin negotiation mode is ON, oper negotiation state is ON
Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF
Port-type: access
Vlan id: 1
5 minutes input rate 0 bits/sec, 0 packets/sec
5 minutes output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer, 0 dropped
Received 0 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
0 packets output, 0 bytes, 0 dropped
0 output errors, 0 collisions

Ruijie#

```

显示聚合端口 1 接口信息:

```

Ruijie# show interfaces AggregatePort 1

Index(dec):897 (hex):381
AggregatePort 1 is UP
Hardware is Aggregate Link AggregatePort
MTU 1536 bytes, BW 8000000 Kbit
Encapsulation protocol is Ethernet-II
Switchport attributes:
  interface's description:""
  medium-type is Copper
  duplex is Full
  speed is 1000M
Aggregate Port Informations:
  Aggregate Number: 1
  Name: "AggregatePort 1"
  Members: (count=8)
  GigabitEthernet 0/1          Link Status: Down
  GigabitEthernet 0/2          Link Status: Down
  GigabitEthernet 0/3          Link Status: Down
  GigabitEthernet 0/4          Link Status: Down
  GigabitEthernet 0/15         Link Status: Up
  GigabitEthernet 0/16         Link Status: Down
  GigabitEthernet 0/17         Link Status: Up
  GigabitEthernet 0/18         Link Status: Down

Ruijie#

```

如何显示交换机端口 gigabitEthernet 0/1 的所有统计信息:

```

Ruijie# show interfaces gigabitEthernet 0/1 counters

Gi0/1 counters
rxHCTotalPkts          : 18373473
txHCTotalPkts          : 18373478
rxHCUnicastPkts        : 0
txHCUnicastPkts        : 0
rxHCMulticastPkts      : 1722751
txHCMulticastPkts      : 1722750
rxHCBroadcastPkts     : 16650718
txHCBroadcastPkts     : 16650727
rxHCOctets             : 2430682032
txHCOctets             : 2430683286
rxHCPkt64Octets        : 1722751
rxHCPkt65to127Octets   : 13175097
rxHCPkt128to255Octets  : 3467721
rxHCPkt256to511Octets  : 7901

```

```

rxHCPkt512to1023Octets      : 0
rxHCPkt1024to1518Octets    : 0
rxHCPkt1519to15220Octets   : 0
rxHCPkt1519to20470Octets   : 0
rxHCPkt2048to40950Octets   : 0
rxHCPkt4096to92160Octets   : 0
txHCPkt640Octets           : 1722750
txHCPkt65to1270Octets      : 13175103
txHCPkt128to2550Octets     : 3467723
txHCPkt256to5110Octets    : 7901
txHCPkt512to1023Octets     : 0
txHCPkt1024to1518Octets    : 0
txHCPkt1519to15220Octets   : 0
txHCPkt1519to20470Octets   : 0
txHCPkt2048to40950Octets   : 0
txHCPkt4096to92160Octets   : 0

rxCRCAAlignErrors          : 0
rxUndersizedPkts          : 0
rxOversizedPkts           : 0
rxFragmentPkts            : 0
rxJabbers                  : 0
rxSymbolErrors             : 0
rxBufferFullDropPkts      : 0
rxACLDropPkts             : 0
rxMulticastDropPkts       : 0
rxVLANIngressCheckDropPkts : 0
rxIpv6DropPkts            : 0
rxSTPDropPkts             : 0
rxStormAndFDBDropPkts     : 0
rxMTUDropPkts             : 0

txCollisions               : 0
ifInErrors                 : 0
ifOutErrors                : 0
ifInDiscards               : 0
ifInUnknownProtos         : 0
ifOutDiscards              : 0
txDelayExceededDiscards   : 0
txCRC                      : 0
txSTPDropPkts             : 0
txHOLDropPkts             : 0

dot3StatsAlignmentErrors   : 0
dot3StatsFCSErrors         : 0
dot3StatsSingleColFrames   : 0
dot3StatsMultiColFrames    : 0
dot3StatsSQETestErrors     : 0
dot3StatsDeferredTransmissions : 0
dot3StatsLateCollisions    : 0
dot3StatsExcessiveCollisions : 0
dot3StatsInternalMacTransmitErrors : 0
dot3StatsCarrierSenseErrors : 0
dot3StatsFrameTooLongs     : 0
dot3StatsInternalMacReceiveErrors : 0

linkChange                 : 1

Ruijie#

```

如何显示交换机端口 gigabitEthernet 0/1-2 的错误计数器信息:

```

Ruijie# show interfaces gigabitEthernet 0/1-2 counters errors

```

Interface	Align-Err	Fcs-Err	Rcv-Err	Undersize	Xmit-Err	OutDiscard
Gi0/1	0	0	0	0	0	0
Gi0/2	0	0	0	0	0	0

Interface	Single-Col	Multi-Col	Late-Col	Excess-Col	Carri-Sen	Runts
Gi0/1	0	0	0	0	0	0


```

Gi0/2      0      0      0      0      0      0
Interface  Giants    Symbol-Err  SQETest-Err  DeferredTx  IntMacTx  IntMacRx
-----
Gi0/1      0      0      0      0      0      0
Gi0/2      0      0      0      0      0      0

Total Entries:2

Ruijie#

```

显示交换机的端口 gigabitEthernet 0/1-2 的速率统计:

```

Ruijie#show interfaces gigabitEthernet 0/1-2 counters rate

Interface      Sampling Time      Input Rate      Input Rate      Output
Rate           Output Rate
(bits/sec)     (packets/sec)    (bits/sec)     (packets/sec)
-----
Gi0/1          2 seconds         901586808      613753
901586528      613752
Gi0/2          2 seconds         901585688      613750
901586008      613748

Total Entries:2

Ruijie#

```

显示交换机的端口连接状态:

```

Ruijie# show interfaces gigabitEthernet 0/1-8 status

Interface      Status  VLAN  Duplex  Speed  Type
-----
GigabitEthernet 0/1  up      1     Full    100M   copper
GigabitEthernet 0/2  down    1     Unknown Unknown copper
GigabitEthernet 0/3  down    1     Unknown Unknown copper
GigabitEthernet 0/4  down    1     Unknown Unknown copper
GigabitEthernet 0/5  down    1     Unknown Unknown copper
GigabitEthernet 0/6  down    1     Unknown Unknown copper
GigabitEthernet 0/7  down    1     Unknown Unknown copper
GigabitEthernet 0/8  down    1     Unknown Unknown copper

Total Entries: 8

Ruijie#

```

显示交换机的端口 gigabitEthernet 0/1-2 的利用率:

```

Ruijie#show interfaces gigabitEthernet 0/1-2 utilization

Interface      TX bits/sec      RX bits/sec      Utilization
-----
Gi0/1          909614312        909614960        100
Gi0/2          909613752        909615064        100

Total Entries:2

Ruijie#

```

显示自动协商信息:

```

Ruijie# show interfaces gigabitEthernet 0/1-2 auto-negotiation

Gi0/1
Auto Negotiation: Enabled

Speed auto downgrade: Disabled
Remote Signaling: Not detected

```

```

Configure Status: Complete
Capability Bits: 10M_Half, 10M_Full, 100M_Half, 100M_Full, 1000M_Full
Capability Advertised Bits: 10M_Half, 10M_Full, 100M_Half, 100M_Full, 1000M_Full
1
Capability Received Bits: 10M_Half, 10M_Full, 100M_Half, 100M_Full
RemoteFaultAdvertised: Disabled
RemoteFaultReceived: NoError

Gi0/2
Auto Negotiation: Enabled

Speed auto downgrade: Disabled
Remote Signaling: Not detected
Configure Status: Configuring
Capability Bits: 10M_Half, 10M_Full, 100M_Half, 100M_Full, 1000M_Full
Capability Advertised Bits: 10M_Half, 10M_Full, 100M_Half, 100M_Full, 1000M_Full
1
Capability Received Bits: -
RemoteFaultAdvertised: Disabled
RemoteFaultReceived: NoError

Ruijie#

```

1.14 关闭

使用该命令禁用或移除一个接口。这种配置对物理端口有效。该命令也可以配置聚合端口成员端口。使用该命令将导致端口进入禁用状态。在禁用状态下，端口将无法接收或发送任何数据包。使用“no”命令，移除一个条目。关闭一个端口也将同时关闭链接状态。

命令	作用
shutdown	此命令用于禁用一个接口。
no shutdown	此命令用于移除一个条目。

对端口 1/0/1 使用关闭命令禁用端口状态：

```

Ruijie# configure terminal
Ruijie(config)# interface GigabitEthernet0/1
Ruijie(config-if)# shutdown

```

1.15 巨型帧

该命令用于物理端口的巨型帧配置。超大帧将被丢弃，并在入站端口进行检查。使用此命令通过交换机系统传送超大帧或巨型帧，优化服务器至服务器的性能。使用“no”命令恢复默认设置。

命令	作用
max-rcv-frame-size BYTES	此命令用于配置允许的最大以太网帧大小。
no max-rcv-frame-size	此命令用于恢复默认设置。

在端口 1/0/1 配置接收的最大以太网帧为 9216 字节：

```

Ruijie# configure terminal
Ruijie(config)# interface GigabitEthernet0/1
Ruijie(config-if)# max-rcv-frame-size 9216
Ruijie(config-if)#

```

1.16 Duplex

在接口配置模式下使用此命令配置物理接口上的双工设置。使用 no 命令恢复默认设置。

对于 1000BASE-T 模块，如果速度被设置为 1000，则双工模式不能被设置为半双工。如果双工模式被设置为半双工，则速度不能被设置为 1000。

命令	作用
duplex {full half auto}	此命令用于配置物理端口接口上的双工设置。
no duplex	此命令用于恢复默认设置。

将接口 GigabitEthernet0/1 配置为强制运行 100Mbps 的速率，并将双工模式设置为自动协商：

```
Ruijie# configure terminal
Ruijie(config)# interface GigabitEthernet0/1
Ruijie(config-if)# speed 100
Ruijie(config-if)# duplex auto
Ruijie(config-if)#
```

1.17 Flowcontrol

在接口配置模式下设置流量控制。如果速度设置为强制模式，最终流控制的设置将由已配置的流控制设置来确定。如果速度被设置为自动模式，最后流控制设置之间的协商结果将基于本地端设置和合作伙伴端设置。这里配置的流量控制设置是本地端的设置。

命令	作用
flowcontrol {on off}	此命令用于配置端口的流量控制能力。
no flowcontrol	此命令用于恢复默认设置。

在接口 GigabitEthernet0/1 和 gi0/1 上启用流控制：

```
Ruijie# configure terminal
Ruijie(config)# interface GigabitEthernet0/1
Ruijie(config-if)# flowcontrol on
Ruijie(config-if)#
```

1.18 Mdx

在接口配置模式下配置端口的 MDIX 状态。使用 no 命令恢复默认设置。当端口的介质是光纤时，不能在端口上应用此命令。

命令	作用
mdix {auto normal cross}	该命令用来配置端口的介质相关接口交叉（MDIX）状态。
no mdix	此命令用于恢复默认设置。

在接口 GigabitEthernet0/1 上将 MDIX 状态配置为 auto：

```
Ruijie# configure terminal
Ruijie(config)# interface GigabitEthernet0/1
Ruijie(config-if)# mdix auto
Ruijie(config-if)#
```

1.19 Speed

在接口配置模式下配置物理端口接口上的速率设置。使用 no 命令恢复默认设置。

如果硬件不支持指定的速率，则会发回错误信息。对于 1000BASE-T 连接，如果速率指定为 1000 Mbps，那么端口必须配置为主端口或从端口。

命令	作用
<code>speed {10 100 1000 [master slave] 10giga auto [SPEED-LIST]}</code>	此命令用于配置物理端口接口上的速率设置。
<code>no speed</code>	此命令用于恢复默认设置。

将 GigabitEthernet0/1 配置为仅自动协商、10 或 100 Mbps:

```
Ruijie# configure terminal
Ruijie(config)# interface GigabitEthernet0/1
Ruijie(config-if)# speed auto 10,100
Ruijie(config-if)#
```

1.20 speed auto-downgrade

此命令用于启用自动降速功能，以便在链接无法建立有效速率时，自动下降标定速率。使用 no 命令禁止该功能。

命令	作用
<code>speed auto-downgrade</code>	此命令用于配置物理端口接口上的速率设置。
<code>no speed auto-downgrade</code>	此命令用于禁止该功能。

启用自动降速功能:

```
Ruijie#configure terminal
Ruijie(config)#interface gigabitEthernet0/1
Ruijie(config-if)#speed auto-downgrade
Ruijie(config-if)#
```

2 MAC 地址

2.1 MAC 地址表

使用下列命令显示或删除特定接口上的 MAC 地址。

命令	作用
<code>clear mac-address-table dynamic {all address MAC-ADDR interface INTERFACE-ID vlan VLAN-ID}</code>	该命令用于删除一个特定动态 MAC 地址和所有动态 MAC 地址，特定接口上所有动态 MAC 地址，或 MAC 地址中所有动态 MAC 地址。
<code>show mac-address-table [dynamic static] [address MAC-ADDR interface [INTERFACE-ID vlan VLAN-ID]]</code>	该命令用于显示特定接口或 VLAN 的 MAC 地址条目或指定的 MAC 地址条目。

从动态 MAC 地址表中移除 MAC 地址 00:08:00:70:00:07:

```
Ruijie# clear mac-address-table dynamic address 00:08:00:70:00:07
Ruijie#
```

显示 MAC 地址 00-02-4b-28-c4-82 的所有 MAC 地址表条目:

```
Ruijie# show mac-address-table address 00:02:4B:28:C4:82

VLAN   MAC Address      Type      Ports
-----
1       00-02-4B-28-C4-82  Static   CPU

Total Entries:1

Ruijie#
```

显示所有静态 MAC 地址表条目:

```
Ruijie# show mac-address-table static
VLAN   MAC Address      Type      Ports
-----
1       00-02-4B-28-C4-82  Static   CPU
4       00-01-00-02-00-04  Static   GigabitEthernet
4       C2-F3-22-0A-12-F4  Static   Aggregateport
6       00-01-00-02-00-07  Static   GigabitEthernet
6       00-01-00-02-00-10  Static   Drop

Total Entries :5

Ruijie#
```

显示所有 VLAN1 的 MAC 地址表条目:

```
Ruijie# show mac-address-table vlan 1

VLAN   MAC Address      Type      Ports
-----
1       00-02-4B-28-C4-82  Static   CPU
1       00-03-40-11-22-33  Dynamic  GigabitEthernet0/2

Total Entries:2

Ruijie#
```

2.2 MAC 地址老化

使用下列命令配置 MAC 地址表老化时间相关功能。如果老化时间设置为 0，将禁用 MAC 地址表老化功能。

命令	作用
----	----

mac-address-table aging-time SECONDS	此命令用于配置 MAC 地址表的老化时间。
no mac-address-table aging-time	此命令用于恢复默认设置。
mac-address-table aging destination-hit	此命令用于启用目的 MAC 地址触发更新功能。
no mac-address-table aging destination-hit	此命令用于禁用目的 MAC 地址触发更新功能。
show mac-address-table aging-time	此命令用于显示 MAC 地址表的老化时间。

配置老化时间值为 200 秒：

```
Ruijie# configure terminal
Ruijie(config)# mac-address-table aging-time 200
Ruijie(config)#
```

启用目的 MAC 地址触发更新功能：

```
Ruijie# configure terminal
Ruijie(config)# mac-address-table aging destination-hit
Ruijie(config)#
```

显示 MAC 地址表的老化时间。

```
Ruijie# show mac-address-table aging-time
Aging Time is 300 seconds

Ruijie#
```

2.3 MAC 地址学习

使用下列命令配置 MAC 地址学习的相关功能。

命令	作用
mac-address-table learning interface INTERFACE-ID [, -]	此命令用于启用物理端口上的 MAC 地址学习。
no mac-address-table learning interface INTERFACE-ID [, -]	此命令用于禁用学习功能。
show mac-address-table learning [interface INTERFACE-ID [, -]]	此命令用于显示 MAC 地址学习状态。

启用 MAC 地址学习选项：

```
Ruijie# configure terminal
Ruijie(config)# mac-address-table learning interface GigabitEthernet 0/5
Ruijie(config)#
```

显示所有物理端口 1 至 10 的 MAC 地址学习状态：

```
Ruijie# show mac-address-table learning interface GigabitEthernet 0/1-10

Interface                               State
-----                               -
GigabitEthernet 0/1                     Enabled
GigabitEthernet 0/2                     Enabled
GigabitEthernet 0/3                     Enabled
GigabitEthernet 0/4                     Enabled
GigabitEthernet 0/5                     Enabled
GigabitEthernet 0/6                     Enabled
GigabitEthernet 0/7                     Enabled
GigabitEthernet 0/8                     Enabled
GigabitEthernet 0/9                     Enabled
GigabitEthernet 0/10                    Enabled

Ruijie#
```

2.4 静态 MAC 地址

此命令用于添加或删除一个静态地址到 MAC 地址表。对于单播 MAC 地址条目，只能指定一个接口。对于组播 MAC 地址条目，可指定多个接口。如想删除一个单播 MAC 地址条目，则无需指定接口 ID。如想删除一个组播 MAC 地址条目，如果接口 ID 已指定，只能移除该接口，否则移除整个组播 MAC 条目。选项 drop 只能为单播 MAC 地址条目指定。

命令	作用
<code>mac-address-table static MAC-ADDR vlan VLAN-ID {interface INTERFACE- ID [-] drop}</code>	此命令用于添加一个静态地址到 MAC 地址表。
<code>no mac-address-table static {all MAC- ADDR vlan VLAN-ID [interface INTERFACE-ID] [-]}</code>	此命令用于从表中删除一条静态 MAC 地址条目。

添加一个静态地址 C2:F3:22:0A:12:F4 到 MAC 地址列表：

```
Ruijie# configure terminal
Ruijie(config)# mac-address-table static C2:F3:22:0A:12:F4 vlan 4 interface
GigabitEthernet 0/1
Ruijie(config)#
```

添加一个静态地址 C2:F3:22:0A:22:33 到 MAC 地址列表：

```
Ruijie# configure terminal
Ruijie(config)# interface range GigabitEthernet 0/5-6
Ruijie(config-if-range)# port-group 2
Ruijie(config-if-range)# exit
Ruijie(config)# mac-address-table static C2:F3:22:0A:22:33 vlan 4 interface
aggregateport 2
Ruijie(config)#
```

2.5 组播过滤模式

使用以下命令配置 VLAN 组播数据包的处理方式。过滤模式仅适用于非保留地址组播数据包。使用“no”命令恢复默认设置。

命令	作用
<code>multicast filtering-mode {forward- unregistered filter-unregistered}</code>	该命令用于配置 VLAN 组播数据包的处理方式。
<code>no multicast filtering-mode</code>	该命令用于恢复默认设置。
<code>show multicast filtering-mode [interface VLAN-ID]</code>	该命令用于显示接口上接收到的处理组播数据包的过滤模式。

设置 VLAN 100 的组播过滤模式，以过滤未注册数据包：

```
Ruijie# configure terminal
Ruijie(config)# vlan 100
Ruijie(config-vlan)# multicast filtering-mode filter-unregistered
Ruijie(config-vlan)#
```

显示所有 VLAN 的组播过滤模式配置：

```
Ruijie#show multicast filtering-mode

Interface                               Layer 2 Multicast Filtering Mode
-----
Default                                 forward-unregistered

Total Entries:1

Ruijie#
```

3 链路聚合控制协议 (LACP)

3.1 聚合组

使用以下命令设置聚合组的相关功能。当一个物理端口首先加入一个聚合组时，系统会自动创建聚合端口。

如果命令不指定模式，则聚合组的类型为静态。如果命令中的指定模式为“active”或“passive”，聚合组的类型为LACP。

一个聚合组只能包含静态成员或LACP成员。当聚合组的类型已经确定后，其它类型的接口不能再加入聚合组。

如果在端口上启用安全功能，则该端口不能被指定为一个聚合组成员。

命令	作用
<code>port-group AGGREGATE-NO [mode {active passive}]</code>	使用该命令为信道组分配接口。此命令可用于物理端口配置。一个接口只能加入一个聚合组。
<code>no port-group</code>	使用“no”命令，从信道组移除接口。如果移除端口后信道组没有成员端口，聚合组会被自动删除。聚合端口也可以由“no interface AggregatePort”命令删除。
<code>show aggregateport {AGGREGATE-NO summary load-balance summary}</code>	如果未指定端口-信道编号，则显示所有端口-信道。如果没有使用 <code>show aggregateport</code> 命令指定信道，负载平衡关键字，将显示聚合组的简要信息。
<code>show lacp summary [AGGREGATE-NO]</code>	该命令用于显示LACP信道组信息。如果未指定LACP端口-信道编号，则显示所有LACP端口-信道。

如何分配以太网接口 1/0/4-1/0/5 到一个新的 LACP 聚合组，ID 为 3 并设置 LACP 模式为主动。：

```
Ruijie# configure terminal
Ruijie(config)# interface range eth1/0/4-1/0/5
Ruijie(config-if)# port-group 3 mode active
Ruijie(config-if)#
```

本例说明如何显示所有端口-信道的摘要信息。

```
Ruijie# show channel-group channel detail

AggregatePort MaxPorts  SwitchPort Mode  Ports
-----
Ag1            8           Access    0/1-0/7
Ag3            8           Access    0/8-0/12
Ag8            8           Access    0/17-0/21

Ruijie#
```

本例说明如何显示所有 LACP 端口-信道的摘要信息。

```
Ruijie# show lacp summary

System priority : 32768                System ID: 00-79-43-22-35-67

Flags : S - Port perform slow timeout  F - Port perform fast timeout
        A - Port is in active mode      P - Port is in passive mode

Aggregate port 1 :
Local information :

Port   Flags   State   LACP Port   Oper   Port   Port
-----
0/1    FA     down    32768       0x0    0x0    0x0
0/2    FA     down    32768       0x0    0x0    0x0
0/3    FA     down    32768       0x0    0x0    0x0
0/4    FA     down    32768       0x0    0x0    0x0
0/15   FA     bndl    32768       0x1    0xf    0x3f
0/16   FA     down    32768       0x0    0x0    0x0
0/17   FA     bndl    32768       0x1    0x11   0x3f
```



```

0/18   FA       down       32768       0x0        0x0        0x0

Partner information :
Port   Flags     LACP Port   Dev ID      Oper   Port   Port   System
-----|-----|-----|-----|-----|-----|-----|-----
0/1    SP       0           00-00-00-00-00-00 0x0    0x0    0x0    0
0/2    SP       0           00-00-00-00-00-00 0x0    0x0    0x0    0
0/3    SP       0           00-00-00-00-00-00 0x0    0x0    0x0    0
0/4    SP       0           00-00-00-00-00-00 0x0    0x0    0x0    0
0/15   FP       1           5C-D9-98-C9-BE-6D 0x1    0x3    0x3e   1
0/16   SP       0           00-00-00-00-00-00 0x0    0x0    0x0    0
0/17   FP       1           5C-D9-98-C9-BE-6D 0x1    0x1    0x3e   1
0/18   SP       0           00-00-00-00-00-00 0x0    0x0    0x0    0

Ruijie#

```

3.2 端口优先级

使用该命令配置端口优先级。LACP 端口优先级确定哪些端口可以加入一个聚合端口，哪些端口被置于独立模式。值越低，优先级越高。如果两个或多个端口具有相同的优先级，则通过端口号决定优先级。使用“no”命令恢复默认设置。

命令	作用
lacp port-priority PRIORITY	此命令用于配置端口优先级。
no lacp port-priority	此命令用于恢复默认设置。

配置接口 1/0/4-1/0/5 的优先级为 20000:

```

Ruijie# configure terminal
Ruijie(config)# interface range gi0/4-1/0/5
Ruijie(config-if)# lacp port-priority 20000
Ruijie(config-if)#

```

3.3 超时

在接口配置模式下设置配置 LACP 长或短定时器。使用“no”命令恢复默认设置。

命令	作用
lacp timeout {short long}	此命令用于配置 LACP 长或短定时器。此命令只能用于物理端口的接口配置。
no lacp timeout	此命令用于恢复默认设置。

将以太网接口 1/0/1 的端口 LACP 超时配置为长计时器:

```

Ruijie# configure terminal
Ruijie(config)# interface gi0/1
Ruijie(config-if)# lacp timeout long
Ruijie(config-if)#

```

3.4 系统优先级

使用该命令配置系统优先级。使用“no”命令，将系统优先级恢复为默认值。

值越低，优先级越高。如果两台交换机具有相同的系统优先级，由 LACP 的系统 ID (MAC) 确定优先级。LACP 协议优先级命令适用于交换机所有 LACP 端口信道。

命令	作用
lACP system-priority PRIORITY	此命令用于配置系统优先级。
no lACP system-priority	此命令用于将系统优先级恢复为默认值。

配置 LACP 系统优先级值为 30000:

```
Ruijie# configure terminal
Ruijie(config)# lACP system-priority 30000
Ruijie(config)#
```

3.5 负载均衡

在全局配置模式下使用该命令用于配置负载均衡算法。使用“no”命令恢复默认设置。

命令	作用
aggregateport load-balance {dst-ip dst-mac src-dst-ip src-dst-mac src-ip src-mac}	此命令用于配置负载均衡算法，交换机采用此算法分配相同信道中跨越不同端口的数据包。只能指定一种算法。
no aggregateport load-balance	此命令用于恢复为默认值。

此实例用于说明如何配置负载均衡算法为 **src-ip**。

```
Ruijie# configure terminal
Ruijie(config)# aggregateport load-balance src-ip
Ruijie(config)#
```

4 VLAN

4.1 可接受帧

在接口配置模式下使用 `acceptable-frame {tagged-only | untagged-only | admit-all}` 命令设置可接受的帧类型。使用 `no` 命令恢复默认设置。

命令	作用
<code>acceptable-frame {tagged-only untagged-only admit-all}</code>	此命令用于通过一个端口来设置可接受的帧类型。
<code>no acceptable-frame</code>	使用 <code>no</code> 命令恢复默认设置。

将端口 `gi0/1` 的可接受帧类型设置为 `tagged-only`:

```
Ruijie# configure terminal
Ruijie(config)# interface gi0/1
Ruijie(config-if)# acceptable-frame tagged-only
Ruijie(config-if)#
```

4.2 入栈检查

在接口配置模式下使用此命令启用入栈检查。如果已经启用了入栈检查，当接收端口不是接收到的数据包中的 VLAN 成员端口时，该数据包会被丢弃。使用 `no` 命令禁用入栈检查。

命令	作用
<code>ingress-checking</code>	此命令用于对一个端口上接收到到帧启用入栈检查。
<code>no ingress-checking</code>	此命令用于禁用入栈检查。

将端口 `gi0/1` 上的入栈检查设置为启用:

```
Ruijie# configure terminal
Ruijie(config)# interface gi0/1
Ruijie(config-if)# ingress-checking
Ruijie(config-if)#
```

4.3 VLAN

使用以下命令设置、添加或删除 VLAN。

命令	作用
<code>show vlan [VLAN-ID [, -] interface [INTERFACE-ID [, -]]</code>	此命令用于显示交换机的一个或全部已配置的 VLAN 的参数。
<code>vlan VLAN-ID [, -]</code>	此命令用于添加 VLAN 并进入 VLAN 配置模式。
<code>no vlan VLAN-ID [, -]</code>	此命令用于删除指定的 VLAN。
<code>name VLAN-NAME</code>	此命令用于指定 VLAN 的名称。
<code>no name</code>	此命令用于将 VLAN 名重置为默认的 VLAN 名。

显示当前所有 VLAN 条目:

```
Ruijie#show vlan

VLAN 1
Name : default
Tagged Member Ports :
Untagged Member Ports :1/0/1-1/0/28

Total Entries :1

Ruijie#
```

显示 PVID, 入栈检查, 以及端口 gi0/1-1/0/4 上的可接受帧类型信息:

```
Ruijie#show vlan interface gi0/1-1/0/4

gi0/1
VLAN mode      :Hybrid
Native VLAN    :1
Hybrid untagged VLAN :1
Hybrid tagged VLAN :
Ingress checking :Enabled
Acceptable frame type :Admit-All

gi0/2
VLAN mode      :Hybrid
Native VLAN    :1
Hybrid untagged VLAN :1
Hybrid tagged VLAN :
Ingress checking :Enabled
Acceptable frame type :Admit-All

gi0/3
VLAN mode      :Hybrid
Native VLAN    :1
Hybrid untagged VLAN :1
Hybrid tagged VLAN :
Ingress checking :Enabled
Acceptable frame type :Admit-All

gi0/4
VLAN mode      :Hybrid
Native VLAN    :1
Hybrid untagged VLAN :1
Hybrid tagged VLAN :
Ingress checking :Enabled
Acceptable frame type :Admit-All

Ruijie#
```

添加新的 VLAN, 并为新的 VLAN 分配 1000 至 1005 的 VLAN ID

```
Ruijie# configure terminal
Ruijie(config)# vlan 1000-1005
Ruijie(config-vlan)#
```

将 VLAN1000 的 VLAN 名配置为 “admin-vlan”

```
Ruijie# configure terminal
Ruijie(config)# vlan 1000
Ruijie(config-vlan)# name admin-vlan
Ruijie(config-vlan)#
```

4.4 访问 VLAN

此命令用于指定访问 VLAN。使用 no 命令恢复默认设置。当接口设置为访问模式时此命令生效。指定为访问模式的 VLAN 无需配

置命令。只能指定一个访问 VLAN。新的命令将覆盖先前的命令。

命令	作用
switchport access vlan VLAN-ID	此命令用于指定一个接口的访问 VLAN。
no switchport access vlan	此命令用于恢复默认设置。

将接口 1/0/1 配置为访问模式，访问 VLAN 为 VLAN 1000

```
Ruijie# configure terminal
Ruijie(config)# interface gi0/1
Ruijie(config-if)# switchport mode access
Ruijie(config-if)# switchport access vlan 1000
Ruijie(config-if)#
```

4.5 Hybrid 端口 VLAN

使用下列命令为 Hybrid 端口指定 VLAN 或 VLAN ID。使用 no 命令恢复默认设置。

以不同的 VLAN ID 多次运行 hybrid VLAN 命令，使端口可以成为一个 tagged 成员端口，或是多个 VLAN 的 untagged 成员端口。

命令	作用
switchport hybrid allowed vlan {[add] {tagged untagged} remove} VLAN-ID [,-]	此命令用于为 Hybrid 端口指定 tagged 或 untagged VLAN。
no switchport hybrid allowed vlan	此命令用于恢复默认设置。
switchport hybrid native vlan VLAN-ID	此命令用于设置 Hybrid 端口的本地 VLAN ID。
no switchport hybrid native vlan	此命令用于恢复默认设置。

将接口 gi0/1 配置成 VLAN1000 的 tagged 成员，以及 VLAN2000 和 VLAN3000 的 untagged 成员：

```
Ruijie# configure terminal
Ruijie(config)# interface gi0/1
Ruijie(config-if)# switchport mode hybrid
Ruijie(config-if)# switchport hybrid allowed vlan add tagged 1000
Ruijie(config-if)# switchport hybrid allowed vlan add untagged 2000,3000
Ruijie(config-if)#
```

将接口 gi0/1 配置成一个 Hybrid 接口，并且将 PVID 配置为 20：

```
Ruijie# configure terminal
Ruijie(config)# interface gi0/1
Ruijie(config-if)# switchport mode hybrid
Ruijie(config-if)# switchport hybrid allowed vlan add untagged 1000,20
Ruijie(config-if)# switchport hybrid native vlan 20
Ruijie(config-if)#
```

4.6 Trunk 端口 VLAN

在接口配置模式下使用下列命令配置 VLAN。使用 no 命令恢复默认设置。

接口设置为 Trunk 模式时，该命令才会生效。如果在 Trunk 端口上允许有 VLAN，那么该端口将成为该 VLAN 的 tagged 成员。

当允许 VLAN 项设置为 all 时，此端口将被自动添加到由系统创建的全部 VLAN 上。

命令	作用
<code>switchport trunk allowed vlan {all [add remove except] VLAN-ID [-]}</code>	此命令用于配置 VLAN，此 VLAN 可以在指定的接口上以 tagged 格式接收和发送流量。
<code>no switchport trunk allowed vlan</code>	此命令用于恢复默认设置。
<code>switchport trunk native vlan {VLAN-ID tag}</code>	此命令用于设置 Trunk 模式接口的本地 VLAN ID。
<code>no switchport trunk native vlan [tag]</code>	此命令用于恢复默认设置。

将接口 gi0/1 配置为 VLAN1000 的 tagged 成员：

```
Ruijie# configure terminal
Ruijie(config)# interface gi0/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# switchport trunk allowed vlan add 1000
Ruijie(config-if)#
```

将接口 gi0/1 配置为 Trunk 接口，并配置本地 VLAN 号 20：

```
Ruijie# configure terminal
Ruijie(config)# interface gi0/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# switchport trunk native vlan 20
Ruijie(config-if)#
```

4.7 VLAN 模式

在接口配置模式下使用此命令指定端口的 VLAN 模式。使用 **no** 命令恢复默认设置。

当一个端口设置为访问模式时，该端口将成为端口配置的访问 VLAN 的 untagged 成员。当一个端口设置为 Hybrid 模式时，该端口可以成为所有配置的 VLAN 的 Untagged 或 Tagged 成员。

当一个端口设置为 Trunk 模式时，该端口只能成为所在的本地 VLAN 的 Tagged 或 Untagged 成员端口中的一种，并且可以成为其他已配置 VLAN 的 tagged 成员。Trunk 端口的目的是支持交换机到交换机的连接。

当交换机端口模式被改变时，与以前的模式有关的 VLAN 相关设置都将丢失。

命令	作用
<code>switchport mode {access hybrid trunk}</code>	此命令用于指定端口的 VLAN 模式。
<code>no switchport mode</code>	此命令用于恢复默认设置。

将接口 gi0/1 设置为 Trunk 端口：

```
Ruijie# configure terminal
Ruijie(config)# interface gi0/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)#
```

5 MSTP

5.1 MSTP 概述

MSTP (Multiple Spanning Tree Protocol) 是一个多生成树协议。MSTP 的“多生成树”包括两层含义：一是在一个交换网络中可以基于 VLAN 划分出多个生成树实例 (STI)，二是在每个生成树实例中可以包括多个 VLAN。而不是像 Cisco 的 PVST、PVST+ 这样，虽然在整个交换网络中可以基于 VLAN 划分出多个生成树实例，但是每个生成树实例中仅包括一个 VLAN。所以相对 PVST、PVST+ 来说，MSTP 更适用于比较大的网络中，划分生成树实例也更灵活，可以根据实际应用需要来进行。

5.2 多生成树实例

MSTI (Multiple Spanning Tree Instance, 多生成树实例) 是指 MST 域内的生成树。一个 MST 域内可以通过 MSTP 生成多棵生成树，各棵生成树之间彼此独立。一个 MSTI 可以与一个或者多个 VLAN 对应，但一个 VLAN 只能与一个 MSTI 对应。

命令	作用
<code>instance INSTANCE-ID vlans VLANID [, -]</code>	此命令用于映射一个或一组 VLAN 到 MST 实例。
<code>no instance INSTANCE-ID [vlans VLANID [, -]]</code>	此命令用于将 VLAN 返回为默认实例 (CIST)。

映射一组 VLAN 到实例 2 上:

```
Ruijie# configure terminal
Ruijie(config)# spanning-tree mst configuration
Ruijie(config-mst)# instance 2 vlans 1-100
Ruijie(config-mst)#
```

5.3 名称和版本号

下列命令用于配置 MST 域的名称和版本号。如果域名称不同，具有相同 VLAN 映射和配置版本号的两个或两个以上的交换机应被视为不同的 MST 域。使用 no 命令，可恢复默认设置。

命令	作用
<code>name NAME</code>	此命令用于配置 MST 域的名称。
<code>no name NAME</code>	此命令用于恢复默认名称。
<code>revision VERSION</code>	此命令用于配置 MST 配置的版本号。
<code>no revision</code>	此命令用于恢复默认设置。

将 MSTP 配置名称设置成“MName”:

```
Ruijie# configure terminal
Ruijie(config)# spanning-tree mst configuration
Ruijie(config-mst)# name MName
Ruijie(config-mst)#
```

配置 MSTP 配置的修订级别为 2:

```
Ruijie# configure terminal
Ruijie(config)# spanning-tree mst configuration
Ruijie(config-mst)# revision 2
Ruijie(config-mst)#
```

5.4 显示 MSTP

使用下列命令显示 MSTP 配置信息。如果配置了 VLAN 并且备用 VLAN 未映射到相同的首选 VLAN，使用命令 `show spanning-tree mst configuration`，将显示一条指示该状态的消息。

命令	作用
<code>show spanning-tree mst [configuration [digest]]</code>	此命令用于显示 MSTP 配置和运行状态。
<code>show spanning-tree mst [instance INSTANCE-ID [, -]] [interface INTERFACE-ID [, -]] [detail]</code>	此命令用于显示指定实例详细的 MSTP 信息。

显示 MSTP 详细信息:

```
Ruijie#show spanning-tree mst detail

Spanning tree:Disabled,protocol:RSTP
Number of MST instances:1

>>>MST00      vlans mapped :1-4094
Bridge Address:00-01-02-03-04-00, Priority:32768 (32768 sysid 0)
Designated Root Address:00-00-00-00-00-00, Priority:0 (0 sysid 0)
Regional Root Bridge Address:00-00-00-00-00-00, Priority:0 (0 sysid 0)
Designated Bridge Address:00-00-00-00-00-00, Priority:0 (0 sysid 0)
Topology Changes Count:0

gi0/1
Port state: forwarding
Port role: nonStp
Port info : port ID 128.1, priority:128, cost:200000
Designated root address:00-00-00-00-00-00, priority:0
Regional Root address:00-00-00-00-00-00, priority:0
Designated bridge address:00-00-00-00-00-00, priority:0, port id:0.0

Ruijie#
```

如何显示用于接口 gi0/1 的 MSTP 详细信息:

```
Ruijie#show spanning-tree mst interface gi0/1 detail

gi0/1
Configured link type: auto, operation status: point-to-point
Configured fast-forwarding: auto, operation status: non-edge
Bpdu statistic counter: sent:0, received:0

>>>MST instance:00, vlans mapped :1-4094
Port state: forwarding
Port role: nonStp
Port info : port ID 128.1, priority:128, cost:200000
Designated root address:00-00-00-00-00-00, priority:0
Regional Root address:00-00-00-00-00-00, priority:0
Designated bridge address:00-00-00-00-00-00, priority:0, port id:0.0

Ruijie#
```

如何显示 MSTP 概要信息:

```
Ruijie#show spanning-tree mst

MST00 vlans mapped : 1-4094
  Root ID      Priority      0
    Address    00-00-00-00-00-00
    this bridge is root
    Hello Time 0 sec, Max Age 20 sec, Forward Delay 15 sec
```



```

Bridge ID Priority 32768
Address      00-00-11-11-00-00
Hello Time 2 sec, Max Age 20 sec, Forward Delay 15 sec

Interface      Role      Sts      Cost      Prio  OperEdge  Type
-----
Gi0/3          nonStp   forwarding 0          128    non-edge  p2p

```

Ruijie#

如何显示用于接口 gi0/1 的 MSTP 概要信息:

```
Ruijie# show spanning-tree mst interface gi0/3-4
```

```

gi0/3
Configured link type: auto, operation status: point-to-point
Configured fast-forwarding: auto, operation status: edge
Bpdu statistic counter: sent:4, received:0

```

Priority	Instance	Role	State	Cost	.Port#
MST00	designated	forwarding	20000	128.3	
MST01	backup	blocking	200000	128.3	

```

gi0/4
Configured link type: auto, operation status: point-to-point
Configured fast-forwarding: auto, operation status: edge
Bpdu statistic counter: sent:4, received:0

```

Priority	Instance	Role	State	Cost	.Port#
MST00	root	forwarding	20000	128.4	
MST01	backup	blocking	200000	128.4	

Ruijie#

如何显示用于 MST02 的接口 gi0/3 到 eth 1/0/4 的 MSTP 概要信息:

```
Ruijie# show spanning-tree mst instance 2 interface gi0/3-4
```

```

>>>>MST02 vlans mapped:      2-3
Bridge Address:00-12-d9-87-47-00 , Priority:32770 (32768 sysid 2)
Designated Root Address:00-12-d9-87-47-00 , Priority:32770
Designated Bridge Address:00-12-d9-87-47-00 , Priority:32770

```

Priority	Link	Interface	Role	State	Cost	.Port#	Type	Edge
		gi0/3	backup	blocking	200000	128.3	p2p	non-edge
		gi0/4	backup	blocking	200000	128.4	p2p	non-edge

Ruijie#

如何显示 MSTP 实例映射配置:

```
Ruijie# show spanning-tree mst configuration
```

```

Name      :[region1]
Revision  :2, Instances configured:3 Instance
          Vlans
-----
0         21-4094
1         1-10
2         11-20

```

Ruijie#

5.5 MSTP 路径开销

在接口配置模式下，使用 `spanning-tree mst` 命令，可配置路径开销和端口优先级参数；使用 `no` 命令可恢复默认设置：

命令	作用
<code>spanning-tree mst INSTANCE-ID {cost COST port-priority PRIORITY}</code>	此命令用于为任意 MST 实例配置路径开销和端口优先级参数（包括实例 ID 为 0 的 CIST）。
<code>no spanning-tree mst INSTANCE-ID {cost port-priority}</code>	此命令用于恢复默认设置

配置接口的路径开销：

```
Ruijie# configure terminal
Ruijie(config)# interface gi0/1
Ruijie(config-if)# spanning-tree mst 0 cost 17031970
Ruijie(config-if)#
```

5.6 进入配置模式

要进入 MST 配置模式，需在全局配置模式下使用 `spanning-tree mst configuration` 命令；使用 `no` 命令可恢复默认设置：

命令	作用
<code>spanning-tree mst configuration</code>	此命令用于进入 MST 配置模式。
<code>no spanning-tree mst configuration</code>	此命令用于恢复默认设置。

进入 MST 配置模式：

```
Ruijie# configure terminal
Ruijie(config)# spanning-tree mst configuration
Ruijie(config-mst)#
```

5.7 配置

在全局配置模式下，使用 `spanning-tree mst max-hops` 命令，配置 MSTP 的最大跳数的值；在接口配置模式下，使用 `spanning-tree mst hello-time` 命令，配置各端口用于 MSTP 版本的的 hello 时间；在全局配置模式下，使用 `spanning-tree mst priority` 命令，为所选 MSTP 实例配置网桥优先级值。使用相应的 `no` 命令，可恢复默认设置：

命令	作用
<code>spanning-tree mst max-hops HOP-COUNT</code>	此命令用于配置 MSTP 的最大跳数的值。
<code>no spanning-tree mst max-hops</code>	此命令用于恢复默认设置。
<code>spanning-tree mst hello-time SECONDS</code>	此命令用于配置各端口用于 MSTP 版本的的 hello 时间。
<code>no spanning-tree mst hello-time</code>	此命令用于恢复默认设置。
<code>spanning-tree mst INSTANCE-ID priority PRIORITY</code>	此命令用于为所选 MSTP 实例配置网桥优先级值。
<code>no spanning-tree mst INSTANCE-ID priority</code>	此命令用于恢复默认设置。

配置 MSTP 的最大跳数的值：

```
Ruijie# configure terminal
Ruijie(config)# spanning-tree mst max-hops 19
```

```
Ruijie(config)#
```

将以以太网接口 gi01 的端口 hello 时间配置成 1:

```
Ruijie# configure terminal
Ruijie(config)# interface gi0/1
Ruijie(config-if)# spanning-tree mst hello-time 1
Ruijie(config-if)#
```

为 MSTP 实例 2 配置网桥优先级:

```
Ruijie# configure terminal
Ruijie(config)# spanning-tree mst 2 priority 0
Ruijie(config)#
```

5.8 clear spanning-tree detected-protocols

在特权 EXEC 模式下, 使用 clear spanning-tree detected-protocols 命令, 重启协议迁移; 使用 no 命令可恢复默认设置:

命令	作用
clear spanning-tree detected-protocols {all interface INTERFACE-ID}	此命令用于重启协议迁移。

触发所有端口的协议迁移事件:

```
Ruijie# clear spanning-tree detected-protocols all

Clear spanning-tree detected-protocols?(y/n) [n] y

Ruijie#
```

5.9 显示 STP 信息

在 EXEC 模式或任何配置模式下, 使用 show spanning-tree 命令, 显示生成树协议运行的信息, 使用 show spanning-tree configuration interface 命令, 显示与配置相关的 STP 接口的信息:

命令	作用
show spanning-tree [interface [INTERFACE-ID [, -]]]	此命令用于显示生成树协议运行的信息。
show spanning-tree configuration interface [INTERFACE-ID [, -]]	此命令用于显示与配置相关的 STP 接口的信息。

当启用 STP 时显示生成树信息:

```
Ruijie# show spanning-tree

Spanning Tree: Enabled
Protocol Mode: RSTP
Tx-hold-count: 6
  Root ID      Priority      32768
             Address      00-00-11-11-00-00
             this bridge is root
             Hello Time 2 sec, Max Age 20 sec, Forward Delay 15 sec

  Bridge ID    Priority 32768
             Address      00-00-11-11-00-00
             Hello Time 2 sec, Max Age 20 sec, Forward Delay 15 sec
Topology Changes Count: 0

Interface      Role      State      Cost      Priority Link
-----      -
Gi0/3          designated forwarding 20000      128.3     p2p      non-edge
```

```
Ruijie#
```

显示接口 gi0/1 上的生成树配置信息:

```
Ruijie#show spanning-tree configuration interface ethe1/0/1

gi0/1
Spanning tree state :Enabled
Port path cost:0
Port priority:128
Port Identifier:      128.1
Link type: auto
Port fast: auto
Guard root:Disabled
TCN filter :Disabled
Bpdu forward:Disabled

Ruijie#
```

5.10 snmp-server enable traps stp

在全局配置模式下, 使用 `snmp-server enable traps stp` 命令, 启用生成树发送 SNMP 通知到 STP; 使用 `no` 命令可禁用发送通知:

命令	作用
<code>snmp-server enable traps stp [new-root] [topology-chg]</code>	此命令用于启用生成树发送 SNMP 通知到 STP。
<code>no snmp-server enable traps stp [new-root] [topology-chg]</code>	此命令用于禁用发送通知到 STP。

启用路由器发送所有的 STP trap 到具有定义为公共的团体字符串的主机 10.9.18.100:

```
Ruijie# configure terminal
Ruijie(config)# snmp-server enable traps
Ruijie(config)# snmp-server enable traps stp
Ruijie(config)# snmp-server host 10.9.18.100 version 2c public
Ruijie(config)#
```

5.11 全局生成树

在全局配置模式下, 使用 `spanning-tree global state` 命令, 启用全局配置中的全局生成树功能; 使用 `no` 命令可 STP 全局状态:

命令	作用
<code>spanning-tree global state {enable disable}</code>	此命令用于启用全局配置中的全局生成树功能。
<code>no spanning-tree global state</code>	此命令用于禁用 STP 全局状态。

启用生成树功能:

```
Ruijie# configure terminal
Ruijie(config)# spanning-tree global state enable
Ruijie(config)#
```

5.12 生成树计时器

在全局配置模式下，使用 `spanning-tree (timers)` 命令，配置生成树计时器的值；使用 `no` 命令可恢复默认设置：

命令	作用
<code>spanning-tree {hello-time SECONDS forward-time SECONDS max-age SECONDS}</code>	此命令用于配置生成树计时器的值。
<code>no spanning-tree {hello-time forward-time max-age}</code>	此命令用于恢复到默认设置。

显示如何配置 STP 计时器：

```
Ruijie# configure terminal
Ruijie(config)# spanning-tree hello-time 1
Ruijie(config)# spanning-tree forward-time 16
Ruijie(config)# spanning-tree max-age 21
Ruijie(config)#
```

5.13 STP 状态

在接口配置模式下，使用 `spanning-tree state` 命令，启用或禁用 STP 运行；使用 `no` 命令可恢复默认设置：

命令	作用
<code>spanning-tree state {enable disable}</code>	此命令用于启用或禁用 STP 运行。
<code>no spanning-tree state</code>	此命令用于恢复到默认设置。

在以太网接口 `gi0/1` 上启用生成树：

```
Ruijie# configure terminal
Ruijie(config)# interface gi0/1
Ruijie(config-if)# spanning-tree state enable
Ruijie(config-if)#
```

5.14 STP 路径开销

在接口配置模式下，使用 `spanning-tree cost` 命令，配置指定的端口上端口路径开销的值；使用 `no` 命令可恢复到自动计算路径开销：

命令	作用
<code>spanning-tree cost COST</code>	此命令用于配置指定的端口上端口路径开销的值。
<code>no spanning-tree cost</code>	此命令用于恢复到自动计算路径开销。

将以太网接口 `gi0/7` 的路径开销配置为 20000：

```
Ruijie# configure terminal
Ruijie(config)# interface gi0/7
Ruijie(config-if)# spanning-tree cost 20000
Ruijie(config-if)#
```

5.15 根保护

BPDU 保护将阻止端口成为一个根端口。此功能对服务供应商阻止外部网桥到达网络核心区域影响生成树活动拓扑是非常有用的，因为这些网桥并不完全在管理员的控制下。

在保护下，一个端口未成为根端口，那么此端口将仅作为指定端口。如果端口接收到具有较高优先级的配置 BPDU，在阻止状态下，此端口将成为替换端口。收到的较高因素将不参与 STP 计算。端口将侦听链路上的 BPDU。如果端口计算超过收到的较高 BPDU，它将祈祷指定端口的作用。由于根保护，当端口变为替换端口状态时，将生成一条系统信息。此配置将应用于所有生成树版本。

在接口配置模式下，使用 `spanning-tree guard root` 命令，启用根保护模式；使用 `no` 命令可恢复默认设置：

命令	作用
<code>spanning-tree guard root</code>	此命令用于启用根保护模式。
<code>no spanning-tree guard root</code>	此命令用于恢复到默认设置。

配置阻止以太网接口 `gi0/1` 成为根端口：

```
Ruijie# configure terminal
Ruijie(config)# interface gi0/1
Ruijie(config-if)# spanning-tree guard root
Ruijie(config-if)#
```

5.16 链路类型

全双工端口被认为具有点对点的连接；相反，半双工端口则被认为具有共享连接。通过设置链路类型为共享媒介，此端口不能转换为转发状态。因此，推荐 STP 模式使用的链路类型为 `auto-determined`。

在接口配置模式下，使用 `spanning-tree link-type` 命令，配置端口的链路类型；使用 `no` 命令可恢复默认设置：

命令	作用
<code>spanning-tree link-type {point-to-point shared}</code>	此命令用于配置端口的链路类型。
<code>no spanning-tree link-type</code>	此命令用于恢复到默认设置。

将端口 `gi0/7` 的链路类型配置为点对点连接

```
Ruijie# configure terminal
Ruijie(config)# interface gi0/7
Ruijie(config-if)# spanning-tree link-type point-to-point
Ruijie(config-if)#
```

5.17 STP 模式

如果该模式被配置为 STP 或 RSTP，所有当前正在运行 MSTP 实例将被自动取消。如果新配置的模式是由前一个模式更改而来的，生成树状态机将再次重新启动，因此，所有稳定的生成树端口状态将过渡到丢弃状态。

端口可以设为以下三个端口快速模式之一：

- 边缘模式 - 当一个无需等待转发时间延迟的连接生成时，端口会直接转换为生成树转发状态。如果稍后接口收到 BPDU 报文，那么端口会转换为非端口快速状态。
- 禁用模式 - 端口始终处于非端口快速状态下。端口会一直等待从转发时间延迟转换为转发状态。

- 网络模式 - 调制解调器端口将保持在非端口快速状态三秒。如果没有接收到 BPDU，该端口将切换到端口快速状态并转换为转发状态。如果端口稍后收到 BPDU 报文，那么端口会转换为非端口快速状态。

在全局配置模式下，使用 `spanning-tree mode` 命令，配置 STP 模式；在接口配置模式下，使用 `spanning-tree portfast` 命令，指定端口的快速模式；使用相应的 `no` 命令可恢复默认设置：

命令	作用
<code>spanning-tree mode {mstp rstp stp}</code>	此命令用于配置 STP 模式。
<code>no spanning-tree mode</code>	此命令用于恢复到默认设置。
<code>spanning-tree portfast {disable edge network}</code>	此命令用于指定端口的快速模式。
<code>no spanning-tree portfast</code>	此命令用于恢复到默认设置。

配置 RSTP STP 模块的运行版本：

```
Ruijie# configure terminal
Ruijie(config)# spanning-tree mode rstp
Ruijie(config)#
```

为端口 `gi0/7` 配置端口快速边缘模式：

```
Ruijie# configure terminal
Ruijie(config)# interface gi0/7
Ruijie(config-if)# spanning-tree portfast edge
Ruijie(config-if)#
```

5.18 优先级

端口优先级和端口号共同组成了端口标识符。这将用于端口角色的计算。此参数仅用于 RSTP 和 STP 兼容模式下。数字越小，表示优先级越高。

网桥优先级值是用来选择根网桥的两个参数之一。另一个参数是系统的 MAC 地址。网桥的优先级值必须能被 4096 整除，数字越小，优先值越高。该配置仅能在 STP 版本和 RSTP 模式下生效。

在接口配置模式下，使用 `spanning-tree port-priority` 命令，在指定的端口上配置 STP 端口优先级的值；在全局配置模式下，使用 `spanning-tree priority` 命令，配置网桥优先级；使用相应的 `no` 命令可恢复默认设置：

命令	作用
<code>spanning-tree port-priority PRIORITY</code>	此命令用于在指定的端口上配置 STP 端口优先级的值。
<code>no spanning-tree port-priority</code>	此命令用于重置默认优先级。
<code>spanning-tree priority PRIORITY</code>	该命令用于配置网桥优先级。
<code>no spanning-tree priority</code>	此命令用于恢复到默认设置。

将端口 `gi0/7` 的优先级配置为 0：

```
Ruijie# configure terminal
Ruijie(config)# interface gi0/7
Ruijie(config-if)# spanning-tree port-priority 0
Ruijie(config-if)#
```

配置 STP 网桥优先级值为 4096：

```
Ruijie# configure terminal
Ruijie(config)# spanning-tree priority 4096
Ruijie(config)#
```

5.19 TCN 过滤

对于一个 ISP 而言，在端口上启用 TC 过滤可以防止外部某些管理员无法完全控制的网桥接入网络核心区域而造成该区域的地址冲洗。当一个端口被设置为 TCN 过滤模式时，通过该端口收到 TC 事件将被忽略。此配置将应用于所有生成树模式。

在接口配置模式下，使用 `spanning-tree tcnfilter` 命令，在指定的接口上启用拓扑变化通知（TCN）过滤；使用 `no` 命令可恢复默认设置：

命令	作用
<code>spanning-tree tcnfilter</code>	此命令用于在指定的接口上启用拓扑变化通知（TCN）过滤。
<code>no spanning-tree tcnfilter</code>	此命令用于禁用 TCN 过滤。

在端口 `gi0/7` 上配置 TCN 过滤：

```
Ruijie# configure terminal
Ruijie(config)# interface gi0/7
Ruijie(config-if)# spanning-tree tcnfilter
Ruijie(config-if)#
```

5.20 保持计数

BPDU 端口的传输由计数器控制。计数器在每个 BPDU 传输时增加，然后每隔一秒减少。如果计数器达到发送保持计数，传输会被暂停一秒钟。使用 `no` 命令恢复默认设置。在全局配置模式下，使用 `spanning-tree tx-hold-count` 命令，限制在暂停 1 秒后可以发送的 BPDU 报文的最大数量；使用 `no` 命令可恢复默认设置：

命令	作用
<code>spanning-tree tx-hold-count VALUE</code>	此命令用于用来限制在暂停 1 秒后可以发送的 BPDU 报文的的最大数量。
<code>no spanning-tree tx- hold-count</code>	此命令用于恢复到默认设置。

将发送保持计数值配置为 5：

```
Ruijie# configure terminal
Ruijie(config)# spanning-tree tx-hold-count 5
Ruijie(config)#
```

5.21 BPDU 转发

如果启用生成树 BPDU 的转发，收到 STP 的 BPDU 将以未标记的形式转发到所有 VLAN 的成员端口。如果启用了 STP 协议的第 2 层协议隧道，那么该命令不会生效。在接口配置模式下，使用 `spanning-tree forward-bpdu` 命令，启用生成树 BPDU 的转发；使用 `no` 命令可禁用生成树 BPDU 的转发：

命令	作用
<code>spanning-tree forward-bpdu</code>	此命令用于启用生成树 BPDU 的转发。
<code>no spanning-tree forward-bpdu</code>	此命令用于禁止生成树 BPDU 的转发。

启用 STP 报文转发：

```
Ruijie# configure terminal
Ruijie(config)# interface gi0/1
```



```
Ruijie(config-if)# spanning-tree forward-bpdu  
Ruijie(config-if)#
```

6 LLDP

6.1 LLDP 概述

LLDP (Link Layer Discovery Protocol, 链路层发现协议) 是由 IEEE 802.1AB 定义的一种链路层发现协议。通过 LLDP 协议能够进行拓扑的发现及掌握拓扑的变化情况。LLDP 将设备本地的信息组织成 TLV 的格式 (Type/Lenth/Value, 类型/长度/值) 封装在 LLDPDU (LLDP data unit, 链路层发现协议数据单元) 中发送给邻居设备, 同时它将邻居设备发送的 LLDPDU 以 MIB (Management Information Base, 管理信息库) 的形式存储起来, 提供给网络管理系统访问。

通过 LLDP, 网络管理系统可以掌握拓扑的连接情况, 比如设备的哪些端口与其它设备相连接, 链路连接两端的端口的速率、双工是否匹配等, 管理员可以根据这些信息快速地定位及排查故障。

6.2 清除

使用该命令带 interface 关键字, 重置指定接口的 LLDP 统计信息。如果命令 clear lldp counters 使用 all 关键字发布, 则用于清除所有接口的全局 LLDP 统计和 LLDP 统计信息。当没有选择可选关键字, 只有 LLDP 全局计数器将被清除。

在特权 EXEC 模式下, 使用 clear lldp counters 命令, 删除 LLDP 统计信息, 使用 clear lldp table 命令, 删除从邻居设备学习到的 LLDP 信息。如果 clear lldp table 命令以不带 interface 的关键字, 将清除所有接口的所有邻居信息:

命令	作用
clear lldp counters [all interface INTERFACE-ID [, -]]	此命令用于清除 LLDP 统计信息。
clear lldp table {all interface INTERFACE-ID [, -]}	此命令清除从邻居设备学习到的 LLDP 信息。

显示所有 LLDP 统计信息:

```
Ruijie# clear lldp counters all
Ruijie#
```

此例说明如何清除所有接口的全部邻居信息:

```
Ruijie# clear lldp table all
Ruijie#
```

6.3 TLV

协议标识 TLV 可选数据类型指定了是否在端口通告相应本地系统协议身份的实例。协议标识 TLV 为设备提供了对网络运营十分重要的协议进行通告的方法。比如生成树协议、链路聚合控制协议、以及各类厂商协议的改版, 这些协议都负责维护网络的拓扑结构和连通性。当两组协议的功能是有效的, 而且端口启用了协议标识通告功能, 该协议识别 TLV 将被通告。

只有配置的 VLAN ID 与接口的 VLAN 协议配置相匹配时, 且 VLAN 存在时, 该 VLAN 的 PPVID TLV 将被发送。只有当接口是配置 VLAN ID 的成员端口时, 该 VLAN 才会在 VLAN Name TLV 通告。

命令	作用
lldp dot1-tlv-select {port-vlan protocol-vlan VLAN-ID [, -] vlan-name [VLAN-ID [, -]] protocol-identity [PROTOCOL-NAME]}	此命令用于指定哪一个 IEEE 802.1 机构特定 TLV 组的可选类型长度值 (TLV) 将被传输并封装在 LLDPDU, 然后发送给邻居设备。
no lldp dot1-tlv-select {port-vlan protocol-vlan [VLAN-ID [, -]] vlan-name [VLAN-ID [, -]] protocol-identity [PROTOCOL-NAME]}	此命令用于禁用 TLV 传输。

lldp dot3-tlv-select [mac-phy-cfg link-aggregation max-frame-size]	此命令用于指定哪一个 IEEE 802.3 机构特定 TLV 组的可选类型长度值 (TLV) 将被传输并封装在 LLDPDU, 然后发送给邻居设备。
no lldp dot3-tlv-select [mac-phy-cfg link-aggregation max-frame-size]	此命令用于禁用 TLV 传输。
lldp med-tlv-select [capabilities inventory-management]	此命令用于指定哪一个 LLDP-MED TLV 将被传输并封装在 LLDPDU 并发送给邻居设备。
no lldp med-tlv-select [capabilities inventory-management]	此命令用于禁用 TLV 传输。
lldp tlv-select [port-description system-capabilities system-description system-name]	此命令用于指定 802.1AB 基础管理集中的可选类型长度值 (TLV) 将被传输并封装在 LLDPDU, 然后发送给邻居设备。
no lldp tlv-select [port-description system-capabilities system-description system-name]	此命令用于禁用该功能。

启用通告端口 VLAN ID TLV:

```
Ruijie# configure terminal
Ruijie(config)# interface gi0/1
Ruijie(config-if)# lldp dot1-tlv-select port-vlan
Ruijie(config-if)#
```

启用通告端口和协议 VLAN ID TLV, 通告 VLAN 包括 1-3.:

```
Ruijie# configure terminal
Ruijie(config)# interface gi0/1
Ruijie(config-if)# lldp dot1-tlv-select protocol-vlan 1-3
Ruijie(config-if)#
```

启用 vlan1-vlan3 的 VLAN 名称和 TLV 通告:

```
Ruijie# configure terminal
Ruijie(config)# interface gi0/1
Ruijie(config-if)# lldp dot1-tlv-select vlan-name 1-3
Ruijie(config-if)#
```

启用 LACP 协议识别 TLV 通告:

```
Ruijie# configure terminal
Ruijie(config)# interface gi0/1
Ruijie(config-if)# lldp dot1-tlv-select protocol-identity lacp
Ruijie(config-if)#
```

启用通告 MAC / PHY 配置/状态 TLV:

```
Ruijie# configure terminal
Ruijie(config)# interface gi0/1
Ruijie(config-if)# lldp dot3-tlv-select mac-phy-cfg
Ruijie(config-if)#
```

启用传输 LLDP-MED TLV 和 MED Capabilities TLV:

```
Ruijie# configure terminal
Ruijie(config)# interface ethernet 1/0/1
Ruijie(config-if)# lldp med-tlv-select capabilities
Ruijie(config-if)#
```

启用所有支持的可选 802.1AB 基础管理 TLV:

```
Ruijie# configure terminal
Ruijie(config)# interface gi0/1
Ruijie(config-if)# lldp tlv-select
Ruijie(config-if)#
```

启用通告系统名称 TLV:

```
Ruijie# configure terminal
Ruijie(config)# interface gi0/1
Ruijie(config-if)# lldp tlv-select system-name
Ruijie(config-if)#
```

6.4 重复计数器

在全局配置模式下，使用 `lldp fast-count` 命令，配置快速启动重复计数器，指定在完整的快速启动间隔所传送的 LLDP 数量；当检测到 LLDP-MED Capabilities TLV，应用层将开启快速启动机制；使用 `no` 命令可恢复默认设置：

命令	作用
<code>lldp fast-count VALUE</code>	此命令用于配置快速启动重复计数器，指定在完整的快速启动间隔所传送的 LLDP 数量。
<code>no lldp fast-count</code>	此命令用于恢复默认设置。

配置 LLDP MED 快速启动重复计数：

```
Ruijie# configure terminal
Ruijie(config)# lldp fast-count 10
Ruijie(config)#
```

6.5 保持乘数

该参数用于计算 LLDPDU TTL 值的 LLDPDU 发送间隔的乘数。生存时间由保持乘数乘以 TX-间隔来确定。对于协同交换机，当给定通告的生存时间超时后，通告的数据会从邻居交换机的 MIB 中删除。在全局配置模式下，使用 `lldp hold-multiplier` 命令，配置交换机 LLDP 更新的保持乘数；使用 `no` 命令可恢复默认设置：

命令	作用
<code>lldp hold-multiplier VALUE</code>	此命令用于配置交换机 LLDP 更新的保持乘数。
<code>no hold-multiplier</code>	此命令用于恢复默认设置。

配置 LLDP 保持乘数值为 3：

```
Ruijie# configure terminal
Ruijie(config)# lldp hold-multiplier 3
Ruijie(config)#
```

6.6 管理地址

当没有使用 `lldp management-address` 指定可选地址，交换机将查找至少一个具有最小的 VLAN ID，IPv4 和 IPv6 地址的 VLAN。如果没有适用的 IPv4/IPv6 地址，则不会通告管理地址 TLV。一旦管理员配置了地址，默认的 IPv4 和 IPv6 管理地址将变为不活动且不被发送的地址。当所有的配置地址被移除，默认的 IPv4 或 IPv6 地址将被激活。多重 IPv4/IPv6 管理地址可以使用此命令多次进行配置。

使用不带管理地址的 `no lldp management-address` 命令可以关闭 LLDPDU 通告的管理地址。如果列表中没有有效的管理地址，将不会发送管理地址 TLV。

在接口配置模式下，使用 `lldp management-address` 命令，配置将物理接口上发布的管理地址，使用 `no` 命令可恢复默认设置；在 EXEC 模式或任何配置模式下，使用 `show lldp management-address` 命令，显示 LLDP 管理地址信息：

命令	作用
<code>lldp management-address IP-ADDRESS</code>	此命令用于配置将在物理接口上发布的管理地址。
<code>no lldp management-address IP-ADDRESS</code>	此命令用于删除该设置。

show lldp management-address IP-ADDRESS	此命令用于显示 LLDP 管理地址信息。
---	----------------------

启用 gi0/1 和 gi0/2 中管理地址条目 (IPv4) 的设置:

```
Ruijie# configure terminal
Ruijie(config)# interface range gi0/1-1/0/2
Ruijie(config-if-range)# lldp management-address 10.1.1.1
Ruijie(config-if-range)#
```

启用 gi0/3 和 gi0/4 中管理地址条目 (IPv6) 的设置:

```
Ruijie# configure terminal
Ruijie(config)# interface range gi0/3-1/0/4
Ruijie(config-if-range)# lldp management-address FE80::250:A2FF:FEBF:A056
Ruijie(config-if-range)#
```

从 gi0/1 和 gi0/2 删除管理地址 10.1.1.1:

```
Ruijie# configure terminal
Ruijie(config)# interface range gi0/1-1/0/2
Ruijie(config-if-range)# no lldp management-address 10.1.1.1
Ruijie(config-if-range)#
```

从 gi0/3 和 gi0/4 删除管理地址 FE80::250: A056: A2FF: FEBF:

```
Ruijie# configure terminal
Ruijie(config)# interface range gi0/3-1/0/4
Ruijie(config-if-range)# no lldp management-address FE80::250:A2FF:FEBF:A056
Ruijie(config-if-range)#
```

从 gi0/5 删除所有管理地址, 之后不会在 gi0/5 发送管理地址 TVL:

```
Ruijie# configure terminal
Ruijie(config)# interface gi0/5
Ruijie(config-if)# no lldp management-address
Ruijie(config-if)#
```

显示所有管理地址信息:

```
Ruijie#show lldp management-address

Address 1 : (default)
-----
Subtype           : IPv4
Address           : 10.90.90.90
IF Type          : IfIndex
OID               : 1.3.6.1.4.1.4881.1.1.10.1.206
Advertising Ports : -

Address 2 :
-----
Subtype           : IPv4
Address           : 10.90.90.90
IF Type          : IfIndex
OID               : 1.3.6.1.4.1.4881.1.1.10.1.206
Advertising Ports : -

Total Entries : 2
Ruijie#
```

6.7 LLDP 报文收发

如果没有运行 LLDP, 交换机不接收 LLDP 报文。当禁用 LLDP 全局状态, 且启用 LLD 转发状态时, 接收到的 LLDPDU 数据包将会被转发。如果没有运行 LLDP, 交换机不会传输 LLDP 报文。使用以下命令, 可启用或禁用 LLDP 报文的接收, 转发和发送:

命令	作用
lldp receive	此命令用于使能物理接口接收 LLDP 消息。

no lldp receive	此命令用于禁止接收 LLDP 报文。
lldp forward	此命令用于用于启用 LLDP 转发状态。
no lldp forward	此命令用于恢复默认设置。
lldp transmit	此命令用于启用物理接口的 LLDP 通告（传输）能力。
no lldp transmit	此命令用于禁止 LLDP 传输。

启用物理接口接收 LLDP 报文：

```
Ruijie# configure terminal
Ruijie(config)# interface gi0/1
Ruijie(config-if)# lldp receive
Ruijie(config-if)#
```

启用 LLDP 全局转发状态：

```
Ruijie# configure terminal
Ruijie(config)# terminal speed 3
Ruijie(config)#
```

启用 LLDP 传输：

```
Ruijie# configure terminal
Ruijie(config)# interface gi0/1
Ruijie(config-if)# lldp transmit
Ruijie(config-if)#
```

6.8 重新初始化

在全局配置模式下，使用 lldp reinit 命令，配置重新初始化交换机延迟间隔的最短时间；执行最后一条禁用命令之后，重新初始化之前，重新启用的 LDP 物理端口将等待重新初始化的延时；使用 no 命令可恢复默认设置：

命令	作用
lldp reinit SECONDS	此命令用于配置重新初始化交换机延迟间隔的最短时间。
no lldp reinit	此命令用于恢复默认设置。

将重新初始化延时间隔设置为 5 秒：

```
Ruijie# configure terminal
Ruijie(config)# lldp reinit 5
Ruijie(config)#
```

6.9 启用 lldp

LLDP 的发送和接收可分别通过 lldp transmit 命令和接口配置模式下的 lldp receive 命令控制。只有当 LLDP 全局并在物理接口启用时才会在物理接口发生作用。通过通告 LLDP 报文，交换机会通过物理接口向邻居发布信息。另一方面，交换机将学习向邻居发布的 LLDP 报文的连接和管理信息。

在全局配置模式下，使用 lldp run 命令，启用 LLDP 的全局状态；使用 no 命令可恢复默认设置：

命令	作用
lldp run	此命令用于全局启用 LLDP，之后交换机可以开始发送 LLDP 报文并接收和处理 LLDP 报文。
no lldp run	此命令用于恢复默认设置。

启用 LLDP：

```
Ruijie# configure terminal
```

```
Ruijie(config)# lldp run
Ruijie(config)#
```

6.10 传输延迟与间隔

延迟计时器定义了因 MIB 内容持续变更所导致的 LLDP 消息发送的最小时间间隔。LLDP 的发送间隔必须大于或等于传输延迟定时器的 4 倍。时间间隔控制了 LLDP 报文的发送速率。使用以下命令，可配置传输延迟计时器和 LLDPDU 传输间隔值：

命令	作用
lldp tx-delay SECONDS	此命令用于配置传输延迟计时器。
no lldp tx-delay	此命令用于恢复默认设置。
lldp tx-interval SECONDS	此命令用于配置交换机的 LLDPDU 传输间隔值。
no lldp tx-interval	此命令用于恢复默认设置。

配置 SSH 超时的值为 8 秒：

```
Ruijie# configure terminal
Ruijie(config)# lldp tx-delay 8
Ruijie(config)#
```

配置每隔 50 秒发送 LLDP 更新：

```
Ruijie# configure terminal
Ruijie(config)# lldp tx-interval 50
Ruijie(config)#
```

6.11 snmp-server enable traps lldp

在全局配置模式下，使用 `snmp-server enable traps lldp` 命令，启用 LLDP 和 LLDP-MED trap 状态，使用 `snmp-server enable traps lldp med` 命令启用发送 LLDP-MED 通告：

命令	作用
snmp-server enable traps lldp [med]	此命令用于启用 LLDP 和 LLDP-MED trap 状态。
no snmp-server enable traps lldp [med]	此命令用于恢复默认设置。

启用 LLDP MED trap：

```
Ruijie# configure terminal
Ruijie(config)# snmp-server enable traps lldp med
Ruijie(config)#
```

6.12 LLDP 通知

在接口配置模式下，使用 `lldp notification enable` 命令，启用发送接口的 LLDP 和 LLDP-MED 通知；使用 `no` 命令可禁止发送：

命令	作用
lldp [med] notification enable	此命令用于启用发送接口的 LLDP 和 LLDP-MED 通知。
no lldp [med] notification enable	此命令用于禁止发送。

发送 gi0/1 的 LLDP MED 通知：

```
Ruijie# configure terminal
Ruijie(config)# interface gi0/1
Ruijie(config-if)# lldp med notification enable
Ruijie(config-if)#
```

6.13 LLDP 子类型

端口 ID 子类型用于指示如何在端口 ID 字段引用端口。在接口配置模式下，使用 `lldp subtype` 命令，配置 LLDP TLV 子类型：

命令	作用
<code>lldp subtype port-id {mac-address local}</code>	此命令用于配置 LLDP TLV 子类型。

配置端口 ID TLV 至 MAC 地址的子网类型：

```
Ruijie# configure terminal
Ruijie(config)# interface gi0/1
Ruijie(config-if)# lldp subtype port-id mac-address
Ruijie(config-if)#
```

6.14 显示 LLDP

在 EXEC 模式或任何配置模式下，使用 `show lldp` 命令，显示交换机的普通 LLDP 配置状态：

命令	作用
<code>show lldp</code>	此命令用于显示交换机的普通 LLDP 配置状态。

显示 LLDP 系统全局配置状态：

```
Ruijie#show lldp

LLDP System Information
  Chassis ID Subtype      : MAC Address
  Chassis ID              : 00-01-02-03-04-00
  System Name             :
  System Description      : Full Gigabit Security & Intelligence Access Swit
ch
  System Capabilities Supported: Repeater, Bridge
  System Capabilities Enabled  : Repeater, Bridge
LLDP-MED System Information:
  Device Class            : Network Connectivity Device
  Hardware Revision       : 1.00
  Firmware Revision       : 1.00.02
  Software Revision       : 10.4(1) Release(00003)
  Manufacturer Name      : Ruijie Networks
  Model Name              : RG-NBS5552XG
  Asset ID                :

LLDP Configurations
  LLDP State              : Disabled
  LLDP Forward State      : Disabled
  Message TX Interval     : 30
  Message TX Hold Multiplier: 4
  ReInit Delay            : 2
  TX Delay                 : 2

LLDP-MED Configuration:
  Fast Start Repeat Count : 4

Ruijie#
```



```

Ruijie#
Ruijie#
Ruijie#show lldp

LLDP System Information
  Chassis ID Subtype      : MAC Address
  Chassis ID              : 00-01-02-03-04-00
  System Name             :
  System Description      : Full Gigabit Security & Intelligence Access Swit
ch
  System Capabilities Supported: Repeater, Bridge
  System Capabilities Enabled  : Repeater, Bridge
LLDP-MED System Information:
  Device Class            : Network Connectivity Device
  Hardware Revision       : 1.00
  Firmware Revision       : 1.00.02
  Software Revision       : 10.4(1) Release(00003)
  Manufacturer Name      : Ruijie Networks
  Model Name              : RG-NBS5552XG
  Asset ID                :

LLDP Configurations
  LLDP State              : Disabled
  LLDP Forward State     : Disabled
  Message TX Interval    : 30
  Message TX Hold Multiplier: 4
  ReInit Delay           : 2
  TX Delay                : 2

LLDP-MED Configuration:
  Fast Start Repeat Count : 4

Ruijie#

```

6.15 LLDP 接口

命令	作用
show lldp interface INTERFACE-ID [,-]	此命令用于显示物理接口的 LLDP 配置。
show lldp local interface INTERFACE-ID [,-] [brief detail]	此命令用于显示将在 LLDP TLV 中携带并发送给邻居设备的物理接口信息。
show lldp neighbors interface INTERFACE-ID [,-] [brief detail]	此命令用于显示当前从邻居学到的每个物理接口的信息。

显示指定物理接口的 LLDP 配置:

```

Ruijie#show lldp interface ethernet 1/0/1

Port ID: gi0/1
-----
Port ID:gi0/1
Admin Status   :TX and RX
Notification   :Disabled
Basic Management TLVs:
Port Description :Enabled
System Name     :Enabled
System Description :Enabled
System Capabilities :Enabled
Enabled Management Address:(None)
IEEE 802.1 Organizational Specific TLVs:

Port VLAN ID   :Enabled
Enabled Port_and_Protocol_VLAN_ID 1, 2, 3
Enabled VLAN Name 1-3
Enabled Protocol_Identity EAPOL, LACP, GVRP, STP

```

IEEE 802.3 Organizationally Specific TLVs:

MAC/PHY Configuration/Status :Enabled
Link Aggregation :Disabled
Maximum Frame Size :Disabled

LLDP-MED Organizationally Specific TLVs:

LLDP-MED Capabilities TLV :Enabled
LLDP-MED Network Policy TLV :Disabled
LLDP-MED Inventory TLV :Disabled

Ruijie#

显示详情模式下端口 1 的本地信息:

```
Ruijie#show lldp local interface gigabitEthernet 0/1 detail
```

```
Port ID: Gi0/1
-----
Port ID Subtype           : Local
Port ID                   : Gi0/1
Port Description          : Ruijie Networks Ruijie
                          10.4(1) Release(00003) Port
Port PVID                  : 1
Management Address Count  : 2

  Address 1 : (default)
    Subtype           : IPv4
    Address            : 172.18.55.200
    IF Type           : IfIndex
    OID                : 1.3.6.1.4.1.4881.1.1.10.1.206

  Address 2 :
    Subtype           : IPv4
    Address            : 172.18.55.200
    IF Type           : IfIndex
    OID                : 1.3.6.1.4.1.4881.1.1.10.1.206

PPVID Entries Count       : 0
( None )
```

显示常规模式下端口 1 的本地信息:

```
Ruijie#show lldp local interface gigabitEthernet 0/1
```

```
Port ID: Gi0/1
-----
Port ID Subtype           : Local
Port ID                   : Gi0/1
Port Description          : Ruijie Networks Ruijie
                          10.4(1) Release(00002) Port
                          on Unit 1
Port PVID                  : 1
Management Address Count  : 2
PPVID Entries Count       : 0
VLAN Name Entries Count   : 1
Protocol Identity Entries Count : 0
MAC/PHY Configuration/Status : (See Detail)
Link Aggregation          : (See Detail)
Maximum Frame Size        : 1536
LLDP-MED capabilities     : (See Detail)
```

显示简要模式下端口 1 的本地信息:

```
Ruijie#show lldp local interface gigabitEthernet 0/1 brief
```

```
Port ID: Gi0/1
-----
Port ID Subtype           : Local
Port ID                   : Gi0/1
Port Description          : Ruijie Networks Ruijie
```

显示详情模式下从 gi0/9 LLDP 学习到的邻居设备信息:

```
Ruijie# show lldp neighbor interface gi0/1-2 brief
```

```
Port ID: Gi0/1
```

```
-----  
Remote Entities Count :2
```

```
Entity 1
```

```
Chassis ID Subtype :MAC Address
```

```
Chassis ID :00-01-02-03-04-01
```

```
Port ID Subtype :Local
```

```
Port ID: gi0/1
```

```
Port Description :RMON Port 1 on Unit 3
```

```
Entity 2
```

```
Chassis ID Subtype :MAC Address
```

```
Chassis ID :00-01-02-03-04-02
```

```
Port ID Subtype :Local
```

```
Port ID: gi0/1
```

```
Port Description :RMON Port 1 on Unit 4
```

```
Port ID : Gi0/2
```

```
-----  
Remote Entities Count :3
```

```
Entity 1
```

```
Chassis ID Subtype :MAC Address
```

```
Chassis ID :00-01-02-03-04-03
```

```
Port ID Subtype :Local
```

```
Port ID: gi0/1
```

```
Port Description :RMON Port 2 on Unit 1
```

```
Entity 2
```

```
Chassis ID Subtype :MAC Address
```

```
Chassis ID :00-01-02-03-04-04
```

```
Port ID Subtype :Local
```

```
Port ID: gi0/2
```

```
Port Description :RMON Port 2 on Unit 2
```

```
Entity 3
```

```
Chassis ID Subtype :MAC Address
```

```
Chassis ID :00-01-02-03-04-05
```

```
Port ID Subtype :Local
```

```
Port ID: gi0/2
```

```
Port Description :RMON Port 2 on Unit 3
```

```
Total Entries:2
```

```
Ruijie#
```

显示常规模式下的远程 LLDP 信息:

```
Ruijie# show lldp neighbor interface gi0/1-2 brief
```

```
Port ID: Gi0/1
```

```
-----  
Remote Entities Count :2
```

```
Entity 1
```

```
Chassis ID Subtype :MAC Address
```

```
Chassis ID :00-01-02-03-04-01
```

```
Port ID Subtype :Local
```

```
Port ID: gi0/1
```

```
Port Description :RMON Port 1 on Unit 3
```

```
Entity 2
```

```
Chassis ID Subtype :MAC Address
```

```
Chassis ID :00-01-02-03-04-02
```

```
Port ID Subtype :Local
```

```
Port ID: gi0/1
```

```
Port Description :RMON Port 1 on Unit 4
```

```
Port ID : Gi0/2
```

```

-----
Remote Entities Count :3
Entity 1
Chassis ID Subtype   :MAC Address
Chassis ID           :00-01-02-03-04-03
Port ID Subtype      :Local
Port ID: gi0/1
Port Description     :RMON Port 2 on Unit 1
Entity 2
Chassis ID Subtype   :MAC Address
Chassis ID           :00-01-02-03-04-04
Port ID Subtype      :Local
Port ID: gi0/2
Port Description     :RMON Port 2 on Unit 2
Entity 3
Chassis ID Subtype   :MAC Address
Chassis ID           :00-01-02-03-04-05
Port ID Subtype      :Local
Port ID: gi0/2
Port Description     :RMON Port 2 on Unit 3

Total Entries:2

Ruijie#

```

显示简要模式下从 gi0/1 到 gi0/2 的邻居信息:

```

Ruijie# show lldp neighbor interface gi0/1-1/0/2 brief

Port ID: gi0/1
-----
Remote Entities Count :2 Entity 1
Chassis ID Subtype   :MAC Address
Chassis ID           :00-01-02-03-04-01
Port ID Subtype      :Local
Port ID: gi0/1
Port Description     :RMON Port 1 on Unit 3 Entity 2
Chassis ID Subtype   :MAC Address
Chassis ID           :00-01-02-03-04-02
Port ID Subtype      :Local
Port ID: gi0/1
Port Description     :RMON Port 1 on Unit 4

Port ID : gi0/2
-----
Remote Entities Count :3
Entity 1
Chassis ID Subtype   :MAC Address
Chassis ID           :00-01-02-03-04-03
Port ID Subtype      :Local
Port ID: gi0/1
Port Description     :RMON Port 2 on Unit 1
Entity 2
Chassis ID Subtype   :MAC Address
Chassis ID           :00-01-02-03-04-04
Port ID Subtype      :Local
Port ID: gi0/2
Port Description     :RMON Port 2 on Unit 2
Entity 3
Chassis ID Subtype   :MAC Address
Chassis ID           :00-01-02-03-04-05
Port ID Subtype      :Local
Port ID: gi0/2
Port Description     :RMON Port 2 on Unit 3

Total Entries:2

Ruijie#

```

6.16 LLDP 流量

在 EXEC 模式或任何配置模式下，使用 show lldp traffic 命令，显示系统全局 LLDP 流量信息，使用 show lldp traffic interface 命令，显示每一个物理接口的 LLDP 流量信息：

命令	作用
show lldp traffic	此命令用于显示系统全局 LLDP 流量信息。
show lldp traffic interface INTERFACE-ID [, -]	此命令用于显示每一个物理接口的 LLDP 流量信息。

显示全局 LLDP 流量信息：

```
Ruijie#show lldp traffic
Last Change Time      :7958183
Total Inserts  :7
Total Deletes  :0
Total Drops    :0
Total Ageouts  :0
Ruijie#
```

显示端口 1 的统计信息：

```
Ruijie#show lldp traffic interface gi0/1
Port ID : gi0/1
-----
Total Transmits      :0
Total Discards       :0
Total Errors         :0
Total Receives       :0
Total TLV Discards   :0
Total TLV Unknowns   :0
Total Ageouts        :0
Ruijie#
```



配置指南-IP 地址及应用

本分册介绍系统配置配置指南相关内容，包括以下章节：

1. IP 地址与服务
2. DHCP
3. DNS
4. 网络通信检测工具

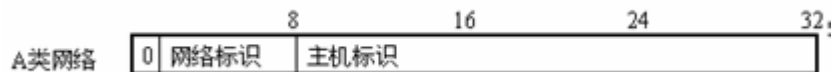
1 IP 地址与服务

1.1 IP 地址简介

IP 地址由 32 位二进制组成，为了书写和描述方便，一般用十进制表示。十进制表示时，分为四组，每组 8 位，范围从 0~255，组之间用“.”号隔开，比如“192.168.1.1”就是用十进制表示的 IP 地址。

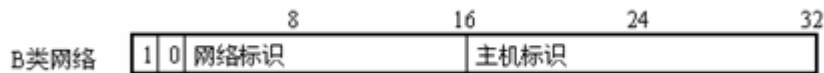
IP 地址顾名思义，自然是 IP 层协议的互连地址。32 位的 IP 地址由两个部分组成：1) 网络部分；2) 本地地址部分。根据网络部分的头几个比特位的值，目前使用中的 IP 地址可以划分成四大类。

A 类地址，最高比特位为“0”，有 7 个比特位表示网络号，24 个比特位表示本地地址。这样总共有 128 个 A 类网络。



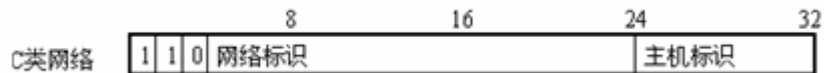
A 类地址

B 类地址，前两个最高比特位为“10”，有 14 个比特位表示网络号，16 个比特位表示本地地址。这样总共有 16,384 个 B 类网络。



B 类地址

C 类地址，前三个最高比特位为“110”，有 21 个比特位表示网络号，8 个比特位表示本地地址。这样总共有 2,097,152 个 C 类网络。



C 类地址

D 类地址，前四个最高比特位为“1110”，其余比特位为组播地址。



D 类地址

前四个最高比特位为“1111”的地址是不允许分配的，这些地址称为 E 类地址，属于保留地址。

在建设网络过程中，进行 IP 地址规划时，一定要根据建设网络的性质进行 IP 地址分配。如果建设的网络需要与互联网连接，则需要到相应的机构申请分配 IP 地址。中国地区可以向中国互联网信息中心（CNNIC）申请，负责 IP 地址分配的最终机构为国际互联网名字与编号分配公司（ICANN, Internet Corporation for Assigned Names and Numbers）。如果建设的网络为内部私有网络，就不需要申请 IP 地址，但是也不能随便分配，最好分配专门的私有网络地址。

下表为保留与可用的地址列表：

类别	地址空间	状态
A 类网络	0.0.0.0	保留
	1.0.0.0~126.0.0.0	可用
	127.0.0.0	保留
B 类网络	128.0.0.0~191.254.0.0	可用
	191.255.0.0	保留
C 类网络	192.0.0.0	保留
	192.0.1.0~223.255.254.0	可用
	223.255.255.0	保留
D 类网络	224.0.0.0~239.255.255.255	可用
E 类网络	240.0.0.0~255.255.255.254	保留
	255.255.255.255	组播

其中专门有三个地址块提供给私有网络，这些地址是不会在互联网中使用的，如果分配了这些地址的网络需要连接互联网，则需要将这些 IP 地址转换成有效的互联网地址。下表为私有网络地址空间，私有网络地址由 RFC 1918 文档定义：

类别	地址空间	状态
A 类网络	10.0.0.0~10.255.255.255	1 个 A 类网络
B 类网络	172.16.0.0~172.31.255.255	16 个 B 类网络
C 类网络	192.168.0.0~192.168.255.255	256 个 C 类网络

关于 IP 地址、TCP/UDP 端口及其它编码的分配情况，请参考 RFC 1166 文档。

1.2 添加 ARP 条目

ARP 表保持了网络层 IP 地址与本地数据链路 MAC 地址之间的联系。这样就不必重复解析该地址。使用此命令添加静态 ARP 条目。使用 no 命令清除 ARP 缓存中的一条静态条目。

在全局配置模式下，使用 arp IP-ADDRESS HARDWARE-ADDRESS 命令，在地址解析协议（ARP）缓存中添加一条静态条目，使用 no 命令可恢复默认设置：

命令	作用
arp IP-ADDRESS HARDWARE-ADDRESS	此命令用于在地址解析协议（ARP）缓存中添加一条静态条目。
no arp IP-ADDRESS HARDWARE-ADDRESS	此命令用于清除 ARP 缓存中的一条静态条目。

为一台以太网主机添加一条静态 ARP 条目

```
Ruijie# configure terminal
Ruijie(config)# arp 10.31.7.19 0800.0900.1834
Ruijie(config)#
```


1.3 ARP 老化时间

在接口配置模式下，使用 `arp timeout` 命令，为 ARP 表设置 ARP 老化时间；使用 `no` 命令可恢复默认设置：

命令	作用
<code>arp timeout MINUTES</code>	此命令用于为 ARP 表设置 ARP 老化时间。
<code>no arp timeout</code>	此命令用于恢复默认设置。
<code>show arp timeout [interface INTERFACE-ID]</code>	此命令用于显示已配置的 ARP 老化时间。

设置 ARP 超时时间为 60 分钟，允许条目比默认设置更快地执行超时时间：

```
Ruijie# configure terminal
Ruijie(config)# interface vlan1
Ruijie(config-if)# arp timeout 60
Ruijie(config-if)#
```

显示 ARP 老化时间：

```
Ruijie#show arp timeout

Interface      Timeout (minutes)
-----
vlan1 60
-----
Total Entries:1

Ruijie#
```

1.4 ARP 缓存

在特权 EXEC 模式下，使用 `clear arp-cache` 命令，清除表中的动态 ARP 条目；用户可选择删除所有动态条目，特定动态条目或所有与特定接口相关的动态条目；在 EXEC 模式或任何配置下，使用 `show arp` 命令，用于显示 ARP 缓存：

命令	作用
<code>clear arp-cache {all interface INTERFACE-ID IP-ADDRESS}</code>	此命令用于清除表中的动态 ARP 条目。
<code>show arp [ARP-TYPE] [IP-ADDRESS [MASK]] [INTERFACE-ID] [HARDWARE-ADDRESS]</code>	此命令用于显示 ARP 缓存。

清除 ARP 缓存中所有的动态条目：

```
Ruijie# clear arp-cache all
Ruijie#
```

显示 ARP 缓存：

```
Ruijie#show arp
S - Static Entry
IP address      hardware Addr      IP  Interface      Age<min>
-----
172.18.55.20    00-16-76-50-06-E7  vlan1              20
172.18.55.200   00-01-02-03-04-00  vlan1              forever
172.18.55.27    74-27-EA-F1-7B-F5  vlan1              20

Total Entries:3

Ruijie#
```

1.5 IPv4 地址

一个接口的 IPv4 地址可由用户手动分配，或由 DHCP 服务器动态分配。对于手动分配，用户可为一个 VLAN 分配多个网络，每个网络都有一个 IP 地址。首选地址将作为 SNMP trap 信息或接口发出的 SYSLOG 信息的源 IP 地址。在接口配置模式下，使用 ip address 命令，为一个接口设置首选 IPv4 地址；使用 no 命令清除 IP 地址的配置或禁用接口上的 DHCP：

命令	作用
ip address {IP-ADDRESS SUBNET-MASK dhcp}	此命令用于为一个接口设置首选 IPv4 地址，或从 DHCP 处获取一个接口的 IP 地址。
no ip address [IP-ADDRESS SUBNET-MASK dhcp]	此命令用于清除 IP 地址的配置或禁用接口上的 DHCP。

将 10.108.1.27 设置成 VLAN 100 的首选地址：

```
Ruijie# configure terminal
Ruijie(config)# interface vlan100
Ruijie(config-if)# ip address 10.108.1.27 255.255.255.0
Ruijie(config-if)#
```

1.6 显示接口信息

在 EXEC 模式或任何配置模式下，使用 show ip interface 命令，显示 IP 接口信息：

命令	作用
show ip interface [INTERFACE-ID] [brief]	此命令用于显示 IP 接口信息。

显示 IP 接口的主要信息：

```
Ruijie#show ip interface brief

Interface      IP Address      Link Status
-----
vlan1  10.90.90.90    up

Total Entries:1

Ruijie#
```

显示 VLAN 1 的 IP 接口信息：

```
Ruijie#show ip interface vlan1

Interface vlan1 is enabled, Link status is up IP address is 10.90.90.90/8 (Manual)
ARP timeout is 60 minutes.Proxy ARP is disabled
IP Local Proxy ARP is disabled
gratuitous-send is disabled, interval is 0 seconds

Total Entries:1

Ruijie#
```

1.7 免费 ARP 命令

免费 ARP 请求包是一个 ARP 请求包，其中源和目的 IP 地址都设置为发送设备的 IP 地址，目的 MAC 地址是广播地址。

一般来说，一个设备上使用的免费 ARP 请求报文来发现其他主机的 IP 地址是否被复制或预加载或重新配置，并连接到接口主机的 ARP 缓存项。

使用 `ip gratuitous-arps` 命令启用免费 ARP 请求传输。当 IP 接口变成 link-up，或者已配置或更改接口的 IP 地址时，该设备将发出数据包。

使用 `ip gratuitous-arps dad-reply` 命令启用免费 ARP 请求传输。当检测到相同的 IP 地址时，该设备将发出数据包。

如果交换机的接口被作为下行设备的网关使用，而伪造的网关发生在下行设备上，可以配置管理员定期发送该接口的免费 ARP 请求信息，通知此交换机才是真正的网关。

命令	作用
<code>ip arp gratuitous</code>	该命令可启用在 ARP 缓存表学习到的免费 ARP 报文。
<code>no ip arp gratuitous</code>	使用此命令禁用 ARP 控制。
<code>ip gratuitous-arps [dad-reply]</code>	该命令用于启用免费 ARP 请求数据包的传输。
<code>no ip gratuitous-arps [dad-reply]</code>	使用此命令禁止传输。
<code>arp gratuitous-send interval SECONDS</code>	使用该命令配置定期发送接口上免费 ARP 请求数据包的时间间隔。
<code>no arp gratuitous-send</code>	使用此命令禁用接口上的此功能。

禁用免费 ARP 请求数据包的学习：

```
Ruijie# configure terminal
Ruijie(config)# no ip arp gratuitous
switch(config)#
```

发送免费 ARP 信息：

```
#Ruijie# configure terminal
Ruijie(config)# ip gratuitous-arps dad-reply
switch(config)#
```

启用发送免费 ARP 信息：

```
Ruijie# configure terminal
Ruijie(config)# ip gratuitous-arps
Ruijie (config)# interface vlan1
Ruijie(config-if)# arp gratuitous-send interval 1
Ruijie(config-if)#
```

2 DHCP

2.1 DHCP 概述

DHCP(Dynamic Host Configuration Protocol, 动态主机配置协议)在 RFC 2131 中有详细的描述, DHCP 为互联网上主机提供配置参数。DHCP 是基于 Client/Server 工作模式, DHCP 服务器为需要动态配置的主机分配 IP 地址和提供主机配置参数。

DHCP 有三种机制分配 IP 地址:

- 1) 自动分配, DHCP 给客户端分配永久性的 IP 地址;
- 2) 动态分配, DHCP 给客户端分配过一段时间会过期的 IP 地址(或者客户端可以主动释放该地址);
- 3) 手工配置, 由网络管理员给客户端指定 IP 地址。管理员可以通过 DHCP 将指定的 IP 地址发给客户端。三种地址分配方式中, 只有动态分配可以重复使用客户端不再需要的地址。

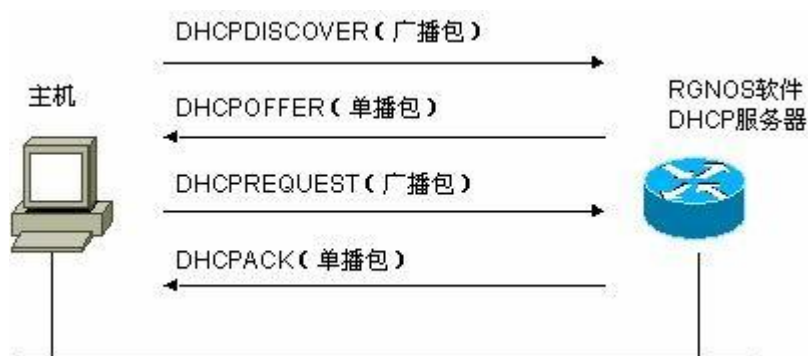
DHCP 消息的格式是基于 BOOTP(Bootstrap Protocol)消息格式的, 这就要求设备具有 BOOTP 中继代理的功能, 并能够与 BOOTP 客户端和 DHCP 服务器实现交互。BOOTP 中继代理的功能, 使得没有必要在每个物理网络都部署一个 DHCP 服务器。RFC 951 和 RFC 1542 对 DHCP 协议进行了详细描述。

DHCP 工作原理

DHCP 协议被广泛用来动态分配可重用的网络资源, 如 IP 地址。DHCP 客户端发出 DISCOVER 广播报文给 DHCP 服务器。DHCP 服务器收到 DISCOVER 报文后, 根据一定的策略来给客户端分配资源, 如 IP 地址, 发出 OFFER 报文。DHCP 客户端收到 OFFER 报文后, 验证资源是否可用。如果资源可用, 发送 REQUEST 报文; 如果资源不可用, 重新发送 DISCOVER 报文。服务器收到 REQUEST 报文, 验证 IP 地址资源(或其他有限资源)是否可以分配, 如果可以分配, 则发送 ACK 报文; 如果不可分配, 则发送 NAK 报文。DHCP 客户端收到 ACK 报文, 就开始使用服务器分配的资源; 如果收到 NAK 报文, 则可能重新发送 DISCOVER 报文。

DHCP 服务器

锐捷产品的 DHCP 服务器完全根据 RFC 2131 来实现的, 主要功能就是为主机分配和管理 IP 地址。DHCP 工作的基本流程如下图所示。




DHCP 基本工作流程

DHCP 请求 IP 地址的过程如下:

- 1) 主机发送 DHCPDISCOVER 广播包在网络上寻找 DHCP 服务器;
- 2) DHCP 服务器向主机发送 DHCPOFFER 单播数据包, 包含 IP 地址、MAC 地址、域名信息以及地址租期;
- 3) 主机发送 DHCPREQUEST 广播包, 正式向服务器请求分配已提供的 IP 地址;
- 4) DHCP 服务器向主机发送 DHCPACK 单播包, 确认主机的请求。

 DHCP 客户端可以接收到多个 DHCP 服务器的 DHCPOFFER 数据包, 然后可能接受任何一个 DHCPOFFER 数据包, 但客户端通常只接受收到的第一个 DHCPOFFER 数据包。

 DHCP 服务器 DHCP OFFER 中指定的地址不一定为最终分配的地址，通常情况下，DHCP 服务器会保留该地址直到客户端发出正式请求。

正式请求 DHCP 服务器分配地址 DHCP REQUEST 采用广播包，是为了让其它所有发送 DHCP OFFER 数据包的 DHCP 服务器也能够接收到该数据包，然后释放已经 OFFER（预分配）给客户端的 IP 地址。

如果发送给 DHCP 客户端的 DHCP OFFER 信息包中包含无效的配置参数，客户端会向服务器发送 DHCP DECLINE 信息包拒绝接受已经分配的配置信息。

在协商过程中，如果 DHCP 客户端没有及时响应 DHCP OFFER 信息包，DHCP 服务器会发送 DHCP NAK 消息给 DHCP 客户端，导致客户端重新发起地址请求过程。

在网络建设中，应用锐捷产品 DHCP 服务器，可以带来以下好处：

- 降低网络接入成本。一般采用静态地址分配的接入费用比较昂贵，应用动态地址分配的接入成本较低。
- 简化配置任务，降低网络建设成本。采用动态地址分配，大大简化了设备配置，对于在没有专业技术人员的地方部署更是降低了部署成本。
- 集中化管理。在对几个子网进行配置管理时，有任何配置参数的变动，只需要修改和更新 DHCP 服务器的配置即可。

DHCP 客户端

DHCP 客户端可以让设备自动地从 DHCP 服务器获得 IP 地址以及其它配置参数。DHCP 客户端可以带来如下好处：

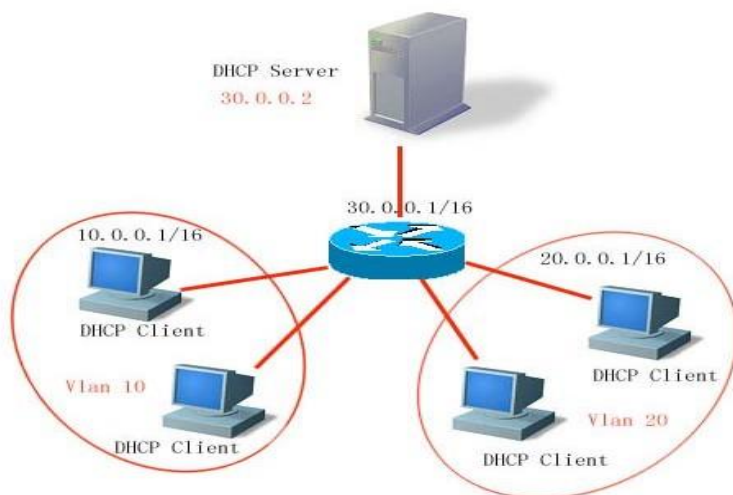
- 降低了配置和部署设备时间。
- 降低了发生配置错误的可能性。
- 可以集中化管理设备的 IP 地址分配。

DHCP 中继代理

DHCP 中继代理，就是在 DHCP 服务器和客户端之间转发 DHCP 数据包。当 DHCP 客户端与服务器不在同一个子网上，就必须有 DHCP 中继代理来转发 DHCP 请求和应答消息。DHCP 中继代理的数据转发，与通常路由转发是不同的，通常的路由转发相对来说是透明传输的，设备一般不会修改 IP 包内容。而 DHCP 中继代理接收到 DHCP 消息后，重新生成一个 DHCP 消息，然后转发出去。

在 DHCP 客户端看来，DHCP 中继代理就像 DHCP 服务器；在 DHCP 服务器看来，DHCP 中继代理就像 DHCP 客户端。

DHCP 中继将收到的 DHCP 请求报文以单播方式转发给 DHCP 服务器，同时将收到的 DHCP 响应报文转发给 DHCP 客户端。DHCP 中继相当于一个转发站，负责沟通位于不同网段的 DHCP 客户端和 DHCP 服务器。这样就实现了只要安装一个 DHCP 服务器，就可以实现对多个网段的动态 IP 管理，即 Client—Relay—Server 模式的 DHCP 动态 IP 管理。如下图所示：



VLAN 10 和 VLAN 20 分别对应 10.0.0.1/16 和 20.0.0.1/16 的网络，而 DHCP 服务器在 30.0.0.1/16 的网络上，30.0.0.2 的 DHCP 服务器要对 10.0.0.1/16 和 20.0.0.1/16 的网络进行动态 IP 管理，只要在作为网关的设备上打开 DHCP 中继功能，并配置 30.0.0.2 为 DHCP 服务器的 IP 地址。

理解 DHCP Relay Agent Information(option 82)

根据 RFC3046 的定义，中继设备进行 DHCP relay 时，可以通过添加 option 的方式来详细的标明 DHCP 客户端的一些网络信息，从而使服务器可以根据更精确的信息给用户分配不同权限的 IP，根据 RFC3046 的定义，所使用 option 选项的选项号为 82，故也被称作 option 82。

理解 DHCP relay Check Server-id 功能

在 DHCP 应用环境中，通常会为每一个网络配备多个 DHCP 服务器，从而进行备份，防止因为一台服务器的工作不正常影响网络的正常使用。在 DHCP 获取的四个交互过程中，当 DHCP 客户端在发送 DHCP REQUEST 时已经选定了服务器，此时会在请求的报文中携带一个 server-id 的 option 选项，在某些特定的应用环境中为了减轻网络服务器压力，需要我们 relay 能够使用此选项，只把请求报文发给此选项里的 DHCP 服务器，而不是发送给每一个配置的 DHCP 服务器，上述就是 DHCP relay check server-id 功能。

2.2 DHCP 客户端命令

DHCP 客户端可以让设备自动地从 DHCP 服务器获得 IP 地址以及其它配置参数。DHCP 客户端可以带来如下好处：

- 降低了配置和部署设备时间。
- 降低了发生配置错误的可能性。
- 可以集中化管理设备的 IP 地址分配。

命令	作用
ip dhcp client class-id {STRING hex HEXSTRING}	该命令用于指定 DHCP DISCOVER 报文中供应商类别标识符 (Option 60) 的值。
no ip dhcp client class-id	使用此命令，恢复到默认值。
ip dhcp client client-id INTERFACE-ID	该命令用于指定的 VLAN 接口的十六进制 MAC 地址将作为与 DHCP DISCOVER 报文同时发送的客户端 ID。
no ip dhcp client client-id	此命令用于恢复默认设置。
ip dhcp client hostname HOST-NAME	该命令用于指定与 DHCP DISCOVER 报文同时发送的主机名称字符串 (Option 12)。
no ip dhcp client hostname	使用此命令，恢复到默认值。
ip dhcp client lease DAYS [HOURS [MINUTES]]	该命令用于指定首选的租约时间，用于为从 DHCP 服务器处请求 IP 地址的时间。
no ip dhcp client lease	使用此命令禁用租约选项的发送。

启用 DHCP 客户端，启用供应商类别标识符的发送，并指定它的值作为 VLAN 100 的 VOIP 设备：

```
Ruijie# configure terminal
Ruijie(config)# interface vlan 100
Ruijie(config-if)# ip address dhcp
Ruijie(config-if)# ip dhcp client class-id VOIP-Device
Ruijie(config-if)#
```

将 VLAN 100 的 MAC 地址配置成与发现消息同时发送的客户端 ID：

```
Ruijie# configure terminal
Ruijie(config)# interface vlan 100
Ruijie(config-if)# ip dhcp client client-id vlan 100
Ruijie(config-if)#
```

将主机名称选项值设置为 Site-A-Switch：

```
Ruijie# configure terminal
Ruijie(config)# interface vlan 100
Ruijie(config-if)# ip dhcp client hostname Site-A-Switch
Ruijie(config-if)#
```

获得 IP 地址的 5 日租约时间:

```
Ruijie# configure terminal
Ruijie(config)# interface vlan 100
Ruijie(config-if)# ip address dhcp
Ruijie(config-if)# ip dhcp client lease 5
Ruijie(config-if)#
```

2.3 DHCP 自动配置

启用自动配置后，交换机重启时会自动成为 DHCP 客户端。自动配置进程可为以下几种：

- 如果 DHCP 服务器中有 TFTP 服务器 IP 地址和配置文件名称，并能在 DHCP 答复数据包的数据字段中写入这些信息，交换机即可获得“配置文件路径”名称和 DHCP 服务器分配的 TFTP 服务器 IP 地址。
- 正在运行的 TFTP 服务器收到交换机发出的请求时，会将请求配置文件存储在基本目录中，交换机再从 TFTP 服务器处下载配置文件。

如果交换机不能完成自动配置流程，那么之前保存在交换机存储器中的本地配置文件将被加载。

命令	作用
autoconfig enable	该命令用于启用自动配置功能。
no autoconfig enable	该命令用于禁止自动配置功能。
show autoconfig	该命令用于显示自动配置状态。

启用自动配置:

```
Ruijie# configure terminal
Ruijie(config)# autoconfig enable
Ruijie(config)#
```

显示自动配置的状态:

```
Ruijie# show autoconfig

Autoconfig State:Disabled

Ruijie#
```

3 域名系统 (DNS) 命令

3.1 DNS 概述

域名系统 (DNS) 用于贯穿整个因特网, 将名字映射为 IP 地址, 在内部网络内使用。提供域名服务的设备的地址通常由 DHCP 或 BOOTP 服务器提供, 或者在启动时人工输入该地址并配置到操作系统。

每个 IP 地址都可以有一个主机名, 主机名由一个或多个字符串组成, 字符串之间用小数点隔开。有了主机名, 就不要死记硬背每台 IP 设备的 IP 地址, 只要记住相对直观有意义的主机名就行了。这就是 DNS 协议所要完成的功能。

主机名到 IP 地址的映射有两种方式: 1) 静态映射, 每台设备上配置主机到 IP 地址的映射, 各设备独立维护自己的映射表, 而且只供本设备使用; 2) 动态映射, 建立一套域名解析系统 (DNS), 只在专门的 DNS 服务器上配置主机到 IP 地址的映射, 网络上需要使用主机名通信的设备, 首先需要到 DNS 服务器查询主机所对应的 IP 地址。

通过主机名, 最终得到该主机名对应的 IP 地址的过程叫做域名解析 (或主机名解析)。锐捷设备支持在本地进行主机名解析, 也支持通过 DNS 进行域名解析。在解析域名时, 可以首先采用静态域名解析的方法, 如果静态域名解析不成功, 再采用动态域名解析的方法。可以将一些常用的域名放入静态域名解析表中, 这样可以大大提高域名解析效率。

3.2 clear host {all | HOST-NAME}

在特权 EXEC 模式下, 使用 clear host 命令, 删除主机条目或所有通过 DNS 解析器或缓存服务器自动学习到的主机条目:

命令	作用
clear host {all HOST-NAME}	该命令用于删除主机条目或所有通过 DNS 解析器或缓存服务器自动学习到的主机条目。

删除主机表中的动态条目 “www.abc.com” :

```
Ruijie# clear host www.abc.com
Ruijie#
```

3.3 ip domain lookup

在全局配置模式下, 使用 ip domain lookup 命令, 启用 DNS, 执行域名解析; DNS 解析器发送请求到已配置好的名称服务器; 名称服务器发出的回应将被保存在缓存中, 用于回答后续请求; 使用 no 命令, 可禁用 DNS 域名解析功能:

命令	作用
ip domain lookup	该命令用于启用 DNS, 执行域名解析。
no ip domain lookup	该命令用于禁用 DNS 域名解析功能。

启用 DNS 域名解析功能:

```
Ruijie# configure terminal
Ruijie(config)# ip domain lookup
Ruijie(config)#
```


3.4 ip host

在全局配置模式下，使用 ip host 命令，配置主机名和主机表中的 IP 地址的静态映射条目；需要对该命令中指定的主机名称进行限定；使用 no 命令可清除静态主机条目：

命令	作用
ip host HOST-NAME {IP-ADDRESS }	该命令用于配置主机名和主机表中的 IP 地址的静态映射条目。
no ip host HOST-NAME {IP-ADDRESS}	使用此命令，清除静态主机条目。

配置主机名称“www.abc.com”的映射和 IP 地址 192.168.5.243：

```
Ruijie# configure terminal
Ruijie(config)# ip host www.abc.com 192.168.5.243
Ruijie(config)#
```

3.5 ip name-server

系统从 DNS 服务器处获得一个回应后，将尝试后续服务器，直到接收到一个响应。如果名称服务器已配置好，之后配置的服务器将添加到服务器列表中。用户可配置最多 2 台名称服务器。

命令	作用
ip name-server IP-ADDRESS	该命令用于配置域名服务器的 IP 地址。
no ip name-server [IP-ADDRESS]	该命令用于清除已配置好的或者所有的域名服务器。

配置域名服务器 192.168.5.134：

```
Ruijie# configure terminal
Ruijie(config)# ip name-server 192.168.5.134
Ruijie(config)#
```

3.6 ip name-server timeout

在全局配置模式下，使用 ip name-server timeout 命令，配置名称服务器的超时时间值；使用 no 命令可恢复默认设置：

命令	作用
ip name-server timeout SECONDS	此命令用于配置名称服务器的超时时间值。
no ip name-server timeout SECONDS	使用此命令恢复到默认值。

配置闲置超时的值为 5 秒：

```
Ruijie# configure terminal
Ruijie(config)# ip name-server timeout 5
Ruijie(config)#
```

3.7 show hosts

在 EXEC 模式或任何配置模式下，使用 show hosts 命令，显示 DNS 配置：

命令	作用
----	----

show hosts	该命令用于显示 DNS 配置。
------------	-----------------

显示 DNS 相关的配置信息：

```
Ruijie# show hosts

Number of Static Entries: 0
Number of Dynamic Entries:1

Host Name:      www.yes.com
IP Address:    10.0.0.88
Age:          1334

Ruijie#
```

3.8 show ip name server

在 EXEC 模式或任何配置模式下，使用 show ip name server 命令，显示 DNS 配置：

命令	作用
show ip name server	该命令用于显示 DNS 配置。

显示 DNS 相关的配置信息：

```
Ruijie# show ip name_server
Name servers are:1.1.1.1
Name servers are:2.2.2.2

Ruijie#
```

4 网络通信检测工具

4.1 ping

在 EXEC 模式下，使用 ping 命令，诊断基础网络连接；使用此命令验证可达性，可靠性和到目标主机的路径延迟；如果没有指定计数或超时值，停止 ping 的唯一途径是按下 CTRL+C 键：

命令	作用
ping {IP-ADDRESS HOST-NAME} [count TIMES] [timeout SECONDS] [source {IP-ADDRESS}]	此命令用于诊断基础网络连接。

ping IP 地址为 172.50.71.123 的主机：

```
Ruijie# ping 192.168.1.77

  Sending 5, 100-byte ICMP Echoes to 192.168.1.77, timeout is 1 second:
    < press Ctrl+C to break >
!!!!

  Success rate is 100 percent <5/5>, round-trip min/avg/max = 0/0/0 ms

Ruijie#
```

4.2 traceroute

在 EXEC 模式下，使用 traceroute 命令，通过 IP 地址显示从交换机到特定目标主机的逐跳路径：

命令	作用
traceroute { [ip] IP-ADDRESS HOST-NAME } [probe NUMBER] [timeout SECONDS] [max-ttl TTL] [port DEST-PORT]	此命令用于通过 IP 地址，显示从交换机到特定目标主机的逐跳路径。

对主机 172.50.71.123 进行路由跟踪：

```
Ruijie# traceroute 172.50.71.123
< press Ctrl+C to break >
Tracing the route to 172.50.71.123
 1  172.50.71.123  0 msec    0 msec    0 msec

Ruijie#
```

对主机 “172.50.71.123” 进行路由跟踪，但路由器未应答：

```
Ruijie# traceroute 172.50.71.123
< press Ctrl+C to break >
Tracing the route to 172.50.71.123
 1  *   *   *

Ruijie#
```

对主机 “172.50.71.123” 进行路由跟踪，但无法到达路由器所应答的目的地：

```
Ruijie# traceroute 172.50.71.123
 1  *   *   *

Ruijie#
```

配置指南-IP 路由

本分册介绍系统配置配置指南相关内容，包括以下章节：

1 协议无关

1 协议无关

1.1 IP 路由

支持浮动默认路由。这意味着，可存在两个具有相同目的网络地址和不同下一跳的路由。如果未指定首选或备用，静态路由将被自动确定为首选或备用路由。首选路由的优先级高于备用路由，并且在激活时始终用于转发。当首选路由出现故障，将使用备用路由。在全局配置模式下，使用 `ip route` 命令，创建一个默认路由条目：

命令	作用
<code>ip route NETWORK-PREFIX NETWORK-MASK IP-ADDRESS [primary backup]</code>	此命令用于创建一个默认路由条目。
<code>no ip route NETWORK-PREFIX NETWORK-MASK IP-ADDRESS</code>	此命令用于清除静态路由条目。
<code>show ip route [[IP-ADDRESS [MASK] connected static] hardware]</code>	此命令用于显示路由表中的条目。
<code>show ip route summary</code>	此命令用于显示工作路由条目的概要信息。

添加其下一跳为 10.1.1.254 的默认路由条目：

```
Ruijie# configure terminal
Ruijie(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.254
Ruijie(config)#
```

显示路由表：

```
Ruijie#show ip route
Code:C - connected, S - static
* - candidate default

Gateway of last resort is not set

C      10.0.0.0/8 is directly connected, vlan1

Total Entries:1

Ruijie#
```

显示 IP 路由条目：

```
Ruijie# show ip route summary

Route Source   Networks Connected    1
Static 0
Total 1

Ruijie#
```



配置指南-组播

本分册介绍系统配置配置指南相关内容，包括以下章节：

1. IGMP Snooping

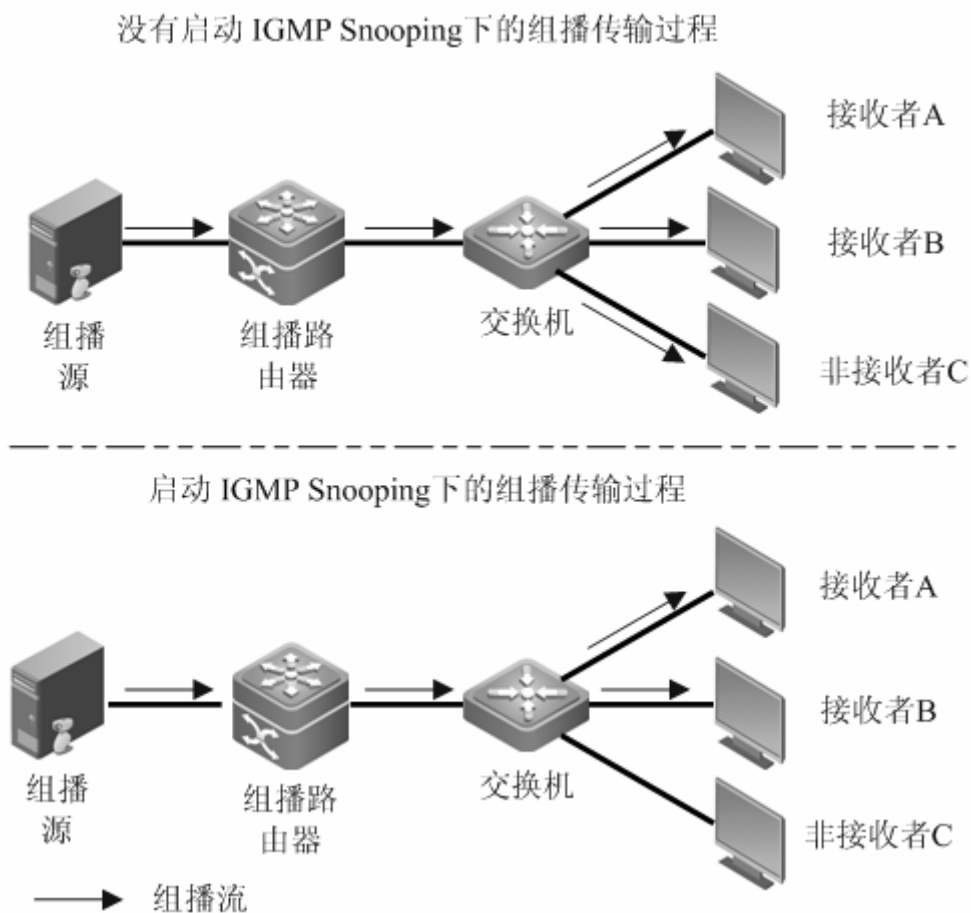
1 IGMP Snooping

1.1 概述

IGMP Snooping 的工作原理

IGMP Snooping 是 Internet Group Management Protocol (组播侦听者发现协议窥探) 的简称。它是运行在 VLAN 上的 IP 组播约束机制, 用于管理和控制 IP 组播流在 VLAN 内的转发, 属于二层组播功能。下面描述的 IGMP Snooping 功能, 都是在 VLAN 内进行的, 相关的端口也是指 VLAN 内部的成员口。

运行 IGMP Snooping 的设备通过对收到的 IGMP 报文进行分析, 为端口和组播地址建立起映射关系, 并根据这样的映射关系转发 IP 组播数据报文。如图 1 所示, 当交换机没有运行 IGMP Snooping 时, IP 组播数据报文在 VLAN 内被广播; 当交换机运行了 IGMP Snooping 后, 已知 IP 组播组的组播数据报文不会在 VLAN 内被广播, 而是发给指定的接收者。

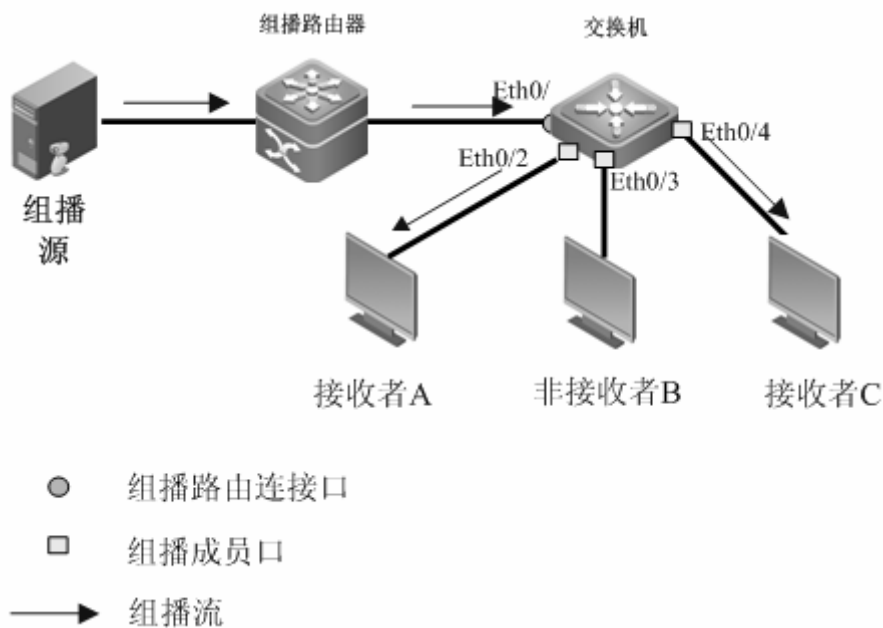


VLAN 上运行 IGMP Snooping 前后的对比

组播设备支持二层组播(IGMP Snooping)与三层组播(Multicast-routing)共同使用。即在一台设备上, 既支持三层组播的路由转发, 又支持在 VLAN 内的窥探, 以实现更为精确的报文转发功能。

IGMP Snooping 的两类端口

如图所示, Router 连接组播源, 在 Switch A 运行 IGMP Snooping, Host A 和 Host C 为接收者主机 (即 IP 组播组成员)。



IGMP Snooping 的两类端口。

- 路由连接口 (Multicast Router Port)：交换机上连接组播路由器（三层组播设备），如 Switch A 的 Eth0/1 端口。交换机将本设备上的所有路由连接口（包括动态和静态端口）都记录在路由连接口列表中。路由连接口缺省情况下是对应 VLAN 内组播数据的接收者，也会被添加到 IGMP Snooping 转发表中。
- 成员端口 (Member Port)：IP 组播组成员端口的简称，又称侦听器端口 (Listener Port)，表示交换机上连接 IP 组播组成员侧的端口，如 Switch A 的 Eth0/2 和 Eth0/4 端口。交换机将本设备上的所有成员端口（包括动态和静态端口）都记录在 IGMP Snooping 转发表中。

动态端口的老化定时器

类型	描述	触发定时器启动的事件	超时后交换机的动作
动态路由连接口的老化定时器	交换机为每个动态路由连接口都启动一个定时器，其超时时间就是动态路由连接口的老化时间	收到 IGMP 查询报文或组播路由协议报文	将该端口从路由连接口列表中删除
动态成员端口的老化定时器	交换机为该端口启动一个定时器，其超时时间就是动态成员端口老化时间	收到 IGMP 的加入报文	将该端口从 IGMP Snooping 组播组的转发表中删除

IGMP Snooping 的工作机制

I. 普遍组查询和特定组查询

IGMP 查询者定期向本地网段内的所有主机与路由器（地址为 224.0.0.1）发送普遍组查询报文，以查询该网段有哪些 IP 组播组的成员。在收到 IGMP 普遍组查询报文时，交换机将查询报文向本 VLAN 内的所有端口转发出去，并对该报文的接收端口做如下处理：

- 如果该端口已经在路由连接口列表中，则重置其老化定时器。
- 如果该端口不在路由连接口列表中，则将其添加到路由连接口列表中，并启动其老化定时器。

在收到 IGMP 的普遍组查询报文后，组播设备会对所有的成员端口启动各自的老化定时器，定时器时间为配置的对 IGMP 查询报文的 longest response time，当定时器超时，则认为该端口不再有成员接收组播流，组播设备就会把该端口从 IGMP Snooping 的转发表中删除。

在收到 IGMP 的特定组查询报文后，组播设备会对该特定组的所有成员端口启动老化定时器，定时器时间为最长响应时间，当定时器超时了还没有接收到主机的应答，则认为该端口不再有成员接收组播流，组播设备就会把该端口从 IGMP Snooping 的转发表中删除。收到 IGMP 的特定组源查询报文，组播设备则只会更新此特定组的源定时器。

II. 报告成员关系

以下情况，主机会向 IGMP 查询者发送 IGMP 成员关系报告报文：

- 当 IP 组播组的成员主机收到 IGMP 查询(普遍组查询或特定组查询)报文后，会应答 IGMP 成员关系报告报文。
- 如果主机要加入某个 IP 组播组，它会主动向 IGMP 查询者发送 IGMP 成员关系报告报文以声明加入该 IP 组播组。

在收到 IGMP 成员关系报告报文时，交换机将其通过 VLAN 内的所有路由连接口转发出去，从该报文中解析出主机要加入的 IP 组播组地址，并对该报文的接收端口做如下处理：

- 如果不存在该 IP 组播组所对应的转发表项，则创建转发表项，将该端口作为动态成员端口添加到出端口列表中，并启动其老化定时器；
- 如果已存在该 IP 组播组所对应的转发表项，但其出端口列表中不包含该端口，则将该端口作为动态成员端口添加到出端口列表中，并启动其老化定时器；
- 如果已存在该 IP 组播组所对应的转发表项，且其出端口列表中已包含该动态成员端口，则重置其老化定时器。

III. 离开组播组

当主机离开 IP 组播组时，会通过发送 IGMP 离开组报文，以通知组播路由器自己离开了某个 IP 组播组。两种离开方式：

- 自动离开：当交换机从某动态成员端口上收到 IGMP 离开组报文时，将直接向路由连接口转发。同时启动一个组成员超时定时器，定时器超时前还没有收到相应的应答报文，将相关成员口老化；
- 快速离开：当交换机从某动态成员端口上收到 IGMP 离开组报文时，将直接向路由连接口转发。同时直接删除相关的组成员接口。

IGMP Snooping 查询器

在运行了 IGMP 的组播网络中，会有一台三层组播设备充当 IGMP 查询者，负责发送 IGMP 查询报文，使三层组播设备能够在网络层建立并维护组播转发表项，从而在网络层正常转发组播数据。

但是，在一个没有三层组播设备的网络中，由于二层设备并不支持 IGMP，因此无法实现 IGMP 查询器的相关功能。为了解决这个问题，可以在二层设备上使能 IGMP Snooping 查询器，使二层设备能够在数据链路层建立并维护组播转发表项，从而在数据链路层正常转发组播数据。

1.2 启用或禁用 ip IGMP snooping

在全局配置模式下，使用 `ip igmp snooping` 命令，在交换机上启用 IGMP snooping 功能；使用 `no` 命令，可禁用 IGMP snooping 功能：

命令	作用
<code>ip igmp snooping</code>	该命令用于在交换机上启用 IGMP snooping 查询。
<code>no ip igmp snooping</code>	该命令用于禁用 IGMP snooping 功能。

禁用 IGMP snooping 全局状态：

```
Ruijie# configure terminal
Ruijie(config)# no ip igmp snooping
Ruijie(config)#
```

启用 IGMP snooping 全局状态：

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping
Ruijie(config)#
```

禁用 VLAN1 上的 IGMP snooping：

```
Ruijie# configure terminal
Ruijie(config)# vlan 1
Ruijie(config-vlan)# no ip igmp snooping
Ruijie(config-vlan)#
```

1.3 ip IGMP snooping 快速离开

IGMP snooping 快速离开功能允许端口收到 IGMP 离开消息但是没有收到特定组查询或者特定组-源查询时，立即将该端口从 IGMP 组成员中移除。

在接口配置模式下，使用 ip igmp snooping fast-leave 命令，配置 VLAN 接口上的 IGMP Snooping 快速离开功能；使用 no 命令，可禁用接口上的快速离开功能：

命令	作用
ip igmp snooping fast-leave	该命令用于配置接口上的 IGMP Snooping 快速离开功能。
no ip igmp snooping fast-leave	该命令用于禁用指定接口上的快速离开功能。

启用 VLAN 1 的 IGMP snooping 快速离开：

```
Ruijie# configure terminal
Ruijie(config)# vlan 1
Ruijie(config-vlan)# ip igmp snooping fast-leave
Ruijie(config-vlan)#
```

1.4 ip IGMP snooping 查询

命令	作用
ip igmp snooping last-member-query-interval SECONDS	该命令用于配置 IGMP snooping 查询者发送 IGMP 特定组查询或者特定组-源查询最长的间隔时间。
no ip igmp snooping last-member-query-interval	该命令用于恢复默认设置。
ip igmp snooping querier	该功能用于启用 IGMP 查询功能。
no ip igmp snooping querier	该命令用于禁用查询功能。
ip igmp snooping query-interval SECONDS	该命令用于配置 IGMP snooping 查询者周期性地发送 IGMP 通用查询报文的时间间隔。
no ip igmp snooping query-interval	该命令用于恢复默认设置。
ip igmp snooping query-max-response-time SECONDS	此命令用于配置组成员响应 IGMP snooping 查询报文的最大响应时间。
no ip igmp snooping query-max-response-time	该命令用于恢复默认设置。
ip igmp snooping query-version {1 2 3}	该命令用于配置 IGMP Snooping 查询者发送的通用查询报文的版本。
no ip igmp snooping query-version	该命令用于恢复默认设置。

配置特定查询消息的最长间隔时间为 3 秒：

```
Ruijie# configure terminal
Ruijie(config)# vlan 1000
Ruijie(config-vlan)# ip igmp snooping last-member-query-interval 3
Ruijie(config-vlan)#
```

启用 VLAN 1 上的 IGMP snooping 查询：

```
Ruijie# configure terminal
Ruijie(config)# vlan 1
Ruijie(config-vlan)# ip igmp snooping querier
Ruijie(config-vlan)#
```

在 VLAN 1000 上配置 IGMP snooping 查询时间间隔值为 300 秒:

```
Ruijie# configure terminal
Ruijie(config)# vlan 1000
Ruijie(config-vlan)# ip igmp snooping query-interval 300
Ruijie(config-vlan)#
```

在 VLAN 1000 上配置最大响应时间为 20 秒:

```
Ruijie# configure terminal
Ruijie(config)# vlan 1000
Ruijie(config-vlan)# ip igmp snooping query-max-response-time 20
Ruijie(config-vlan)#
```

在 VLAN 1000 上配置抑制时间为 2:

```
Ruijie# configure terminal
Ruijie(config)# vlan 1000
Ruijie(config-vlan)# ip igmp snooping query-version 2
Ruijie(config-vlan)#
```

1.5 ip IGMP snooping 组播路由

在接口配置模式下, 使用 `ip igmp snooping mrouter` 命令, 配置指定端口作为组播路由端口或者作为禁止组播路由端口; 使用 `no` 命令, 可将端口从组播路由端口或禁止组播路由端口移除:

命令	作用
<code>ip igmp snooping mrouter {interface INTERFACE-ID [, -] forbidden interface INTERFACE-ID [, -]}</code>	此命令用于配置指定端口作为组播路由端口或者作为禁止组播路由端口。
<code>no ip igmp snooping mrouter {interface INTERFACE-ID [, -] forbidden interface INTERFACE-ID [, -]}</code>	此命令用于将端口从组播路由端口或禁止组播路由端口移除。

为 VLAN 1 添加一个 IGMP snooping 静态组播路由端口:

```
Ruijie# configure terminal
Ruijie(config)# vlan 1
Ruijie(config-vlan)# ip igmp snooping mrouter interface gi0/1
Ruijie(config-vlan)#
```

1.6 ip IGMP snooping 代理

当已启用代理报告功能, 特定 (S, G) 上接收到的多个 IGMP 报告或离开信息将在被发送到路由器端口之前集成到报告报文中。代理报告源 IP 将作为该报告报文的来源 IP。当没有设置代理报告源 IP 时, IP 地址将使用 Zero IP 地址。

命令	作用
<code>ip igmp snooping proxy-reporting [source IP-ADDRESS]</code>	此命令用于启用代理报告功能。
<code>no ip igmp snooping proxy-reporting</code>	该命令用于禁用代理报告功能。

启用 VLAN 1 上的 IGMP snooping 代理报告, 并配置代理报告信息源 IP 为 1.2.2.2:

```
Ruijie# configure terminal
Ruijie(config)# vlan 1
Ruijie(config-if)# ip igmp snooping proxy-reporting source 1.2.2.2
Ruijie(config-if)#
```

1.7 ip IGMP snooping 报告抑制

报告抑制功能只对 IGMPv1 和 IGMPv2 的报文有效，该功能对 IGMP 的查询报文没有影响。当启用报告抑制时，交换机会抑制由主机发送的重复报文。抑制同一组报告或离开报文，直到抑制时间过期。对于同一个组中的报告或离开报文，只转发一个报告或离开报文。其余的报告和离开报文将会被抑制。

命令	作用
<code>ip igmp snooping report-suppression</code>	此命令用于启用报文抑制功能。
<code>no ip igmp snooping report-suppression</code>	使用此命令禁用报文抑制功能。

启用 VLAN 1 的报告压制：

```
Ruijie# configure terminal
Ruijie(config)# vlan 1
Ruijie(config-vlan)# ip igmp snooping report-suppression
Ruijie(config-vlan)#
```

1.8 ip IGMP snooping 健壮变量

健壮变量提供微调，以允许接口的预期丢包。健壮变量值用来计算以下 IGMP 报文间隔：

- Group member interval - 一个组播路由器决定网络上不再有组成员前必须等待的时间。
此时间间隔计算如下： $(\text{健壮变量} \times \text{查询间隔}) + (1 \times \text{查询响应间隔})$ 。
- Other querier present interval - 一个组播路由器决定没有其它组播路由器作为查询器前必须等待的时间。
此时间间隔计算如下： $(\text{健壮变量} \times \text{查询间隔}) + (0.5 \times \text{查询响应间隔})$ 。
- Last member query count - 路由器假设组里没有本地成员前要发送的指定组查询次数。默认数量为健壮变量的值。
如果子网结构可能改变，用户可以增加这个值。

命令	作用
<code>ip igmp snooping robustness-variable VALUE</code>	此命令用于设置 IGMP Snooping 功能使用的健壮系数。
<code>no ip igmp snooping robustness-variable</code>	此命令用于恢复至默认值。

在 VLAN 1000 上配置健壮系数为 3：

```
Ruijie# configure terminal
Ruijie(config)# vlan 1000
Ruijie(config-vlan)# ip igmp snooping robustness-variable 3
Ruijie(config-vlan)#
```

1.9 ip IGMP snooping 静态组

在 VLAN 接口配置模式下，使用 `ip igmp snooping static-group` 命令，可以在相连主机不支持 IGMP 协议的情况下，创建一个 IGMP Snooping 静态组播组；在 EXEC 模式或任何配置模式下，使用 `show ip igmp snooping static-group` 命令，可显示交换机 IGMP snooping 静态组播组信息：

命令	作用
<code>ip igmp snooping static-group GROUP-ADDRESS interface</code>	此命令用于配置 IGMP snooping 静态组播组。

INTERFACE-ID [, -]	
no ip igmp snooping static-group GROUP-ADDRESS [interface INTERFACE-ID [, -]]	使用此命令删除一个静态组播组。
show ip igmp snooping static-group [GROUP-ADDRESS vlan VLAN-ID]	该命令用于显示交换机 IGMP snooping 静态组播组信息。

为 IGMP snooping 添加静态组播组：

```
Ruijie# configure terminal
Ruijie(config)# interface vlan 1
Ruijie(config-vlan)# ip igmp snooping static-group 226.1.2.3 interface gi0/5
Ruijie(config-vlan)#
```

显示 IGMP snooping 静态组播组信息：

```
Ruijie# show ip igmp snooping static-group

VLAN ID Group address Interface
-----
2      226.1.2.2      1/0/3

Total Entries:1

Ruijie#
```

1.10 ip IGMP snooping 抑制时间

报告抑制功能将抑制重复的 IGMP 报告或离开报文在抑制时间间隔内不向路由端口转发。短暂的抑制时间会造成重复的 IGMP 报文被频繁地发送。

命令	作用
ip igmp snooping suppression-time SECONDS	此命令用于配置抑制重复 IGMP 报告或离开报文的间隔时间。
no ip igmp snooping suppression-time	此命令用于恢复默认设置。

在 VLAN 1000 上配置抑制时间为 125：

```
Ruijie# configure terminal
Ruijie(config)# interface vlan 1000
Ruijie(config-vlan)# ip igmp snooping suppression-time 125
Ruijie(config-vlan)#
```

1.11 ip IGMP snooping 版本

在 VLAN 接口配置模式下，使用 ip igmp snooping minimum-version 命令，配置 VLAN 接口所允许接收的 IGMP 报文的最低版本；使用 no 命令可从该接口移除限制：

命令	作用
ip igmp snooping minimum-version {2 3}	该命令用于配置 VLAN 接口所允许接收的 IGMP 报文的最低版本。
no ip igmp snooping minimum-version	该命令用于从该接口移除限制。

限制所有的 IGMPv1 主机加入 VLAN 1：

```
Ruijie# configure terminal
Ruijie(config)# interface vlan 1
Ruijie(config-vlan)# ip igmp snooping minimum-version 2
```

```
Ruijie(config-vlan)#
```

限制所有不被允许的 IGMPv1 和 IGMPv2 主机加入 VLAN1:

```
Ruijie# configure terminal
Ruijie(config)# interface vlan 1
Ruijie(config-vlan)# ip igmp snooping minimum-version 3
Ruijie(config-vlan)#
```

移除配置在 VLAN 1 上的限制:

```
Ruijie# configure terminal
Ruijie(config)# interface vlan 1
Ruijie(config-vlan)# no ip igmp snooping minimum-version
Ruijie(config-vlan)#
```

1.12 显示 ip IGMP snooping

在 EXEC 模式或任何配置模式下, 使用 show ip igmp snooping 命令, 显示所有启用 IGMP snooping 的 VLAN 的 IGMP snooping 信息:

命令	作用
show ip igmp snooping [vlan VLAN-ID]	本例用于显示所有启用 IGMP snooping 的 VLAN 的 IGMP snooping 信息。

显示 IGMP snooping 全局状态信息:

```
Ruijie#show ip igmp snooping

IGMP snooping global state:Enabled

Ruijie#
```

显示 VLAN 2 的 IGMP snooping 信息:

```
Ruijie#show ip igmp snooping vlan 2

VLAN #2 Configuration
IGMP snooping state   :Disabled
Minimum version       :v1
Fast leave            :Disabled (host-based)
Report suppression    :Disabled
Suppression time      :10 seconds
Querier state         :Disabled
Query version         :v3
Query interval        :125 seconds
Max response time     :10 seconds
Robustness value      :2
Last member query interval :1 seconds
Proxy reporting       :Disabled (Source 0.0.0.0)

Total Entries:1

Ruijie#
```

1.13 显示 ip IGMP snooping 组信息

在 EXEC 模式或任何配置模式下, 使用 show ip igmp snooping groups 命令, 显示从交换机上学习的 IGMP snooping 组播组相关信息:

命令	作用
----	----

show ip igmp snooping groups [vlan VLAN-ID IP-ADDRESS]	该命令用于显示从交换机上学习的 IGMP snooping 组播组相关信息。
--	--

显示 IGMP snooping 组播组信息：

```
Ruijie# show ip igmp snooping groups
IGMP Snooping Connected Group Membership:
VLAN ID Group address Source address FM Exp(sec) Interface
-----
239.255.255.250 * EX 382 0/7 ----- 1
Total Entries:1
Ruijie#
```

1.14 显示 ip IGMP snooping 路由器端口信息

在 EXEC 模式或任何配置模式下，使用 show ip igmp snooping mrouter 命令，显示在交换机上学习和配置的 IGMP snooping 路由器端口信息：

命令	作用
show ip igmp snooping mrouter [vlan VLAN-ID]	此命令用于显示在交换机上学习和配置的 IGMP snooping 路由器端口信息。

显示 IGMP snooping 路由器端口信息：

```
Ruijie# show ip igmp snooping mrouter
VLAN Ports
-----
1 1/0/3-1/0/4 (static)
1/0/6 (forbidden)
1/0/2 (dynamic)
2 1/0/4 (static)
1/0/3 (dynamic)
Total Entries:2
Ruijie#
```

1.15 显示或清除 IGMP snooping 统计

在 EXEC 模式或任何配置模式下，使用 show ip igmp snooping statistics 命令，显示交换机上的 IGMP snooping 统计信息；在特权 EXEC 模式下，使用 clear ip igmp snooping statistics 命令，清除 IGMP snooping 统计信息：

命令	作用
show ip igmp snooping statistics {interface [INTERFACE-ID] vlan [VLAN-ID]}	该命令用于显示交换机上的 IGMP snooping 统计信息。
clear ip igmp snooping statistics {all vlan VLAN-ID interface INTERFACE-ID}	该命令用于清除 IGMP snooping 相关统计信息。

显示 IGMP snooping 统计信息：

```
Ruijie# show ip igmp snooping statistics vlan 1
```

```
VLAN 1 Statistics:  
IGMPv1 Rx:Report 1, Query 0  
IGMPv2 Rx:Report 0, Query 0, Leave 0  
IGMPv3 Rx:Report 0, Query 0  
IGMPv1 Tx:Report 0, Query 0  
IGMPv2 Tx:Report 0, Query 0, Leave 0  
IGMPv3 Tx:Report 0, Query 0
```

```
Total Entries:1
```

```
Ruijie#
```

清除所有 IGMP snooping 统计信息:

```
Ruijie# clear ip igmp snooping statistics all  
Ruijie#
```


本分册介绍系统配置配置指南相关内容，包括以下章节：

1. SSH 终端服务
2. 基于端口的流控制
3. DoS 攻击阻止
4. DHCP Snooping
5. 动态 ARP 检测
6. IPSG

1 SSH 终端服务

1.1 SSH 简介

SSH 是英文 Secure Shell 的简写形式。SSH 连接所提供的功能类似于一个 Telnet 连接，与 Telnet 不同的是基于该连接所有的传输都是加密的。当用户通过一个不能保证安全的网络环境远程登录到设备时，SSH 特性可以提供安全的信息保障和强大的认证功能，以保护设备不受诸如 IP 地址欺诈、明文密码截取等攻击。

锐捷 SSH 服务同时支持 IPv4 和 IPv6 两种协议。

锐捷 SSH 支持算法

支持算法	SSH2
签名认证算法	RSA、DSA
密钥交换算法	KEX_DH_GEX_SHA1 KEX_DH_GRP1_SHA1
加密算法	DES、3DES、AES-128、AES-192、AES-256
用户认证算法	基于用户口令的认证方式
消息认证算法	MD5、SHA1、SHA1-96、MD5-96
压缩算法	NONE（无压缩）

1.2 SSH 密钥

在特权 EXEC 模式下，使用 `crypto key generate` 命令，生成 RSA 或 DSA 密钥对；在特权 EXEC 模式下，使用 `crypto key zeroize` 命令，删除 RSA 或 DSA 密钥对；在特权 EXEC 模式或任意配置模式下，使用 `show crypto key mypubkey` 命令，显示 RSA 或 DSA 密钥对：

命令	作用
<code>crypto key generate {rsa [modulus MODULUS-SIZE] dsa}</code>	此命令用于生成 RSA 或 DSA 密钥对。
<code>crypto key zeroize {rsa dsa}</code>	此命令用于删除 RSA 或 DSA 密钥对。
<code>show crypto key mypubkey {rsa dsa}</code>	此命令用于显示 RSA 或 DSA 密钥对。

创建 RSA 密钥：

```
Ruijie# crypto key generate rsa
The RSA key pairs already existed.
Do you really want to replace them?(y/n) [n]y
Choose the size of the key modulus in the range of 360 to 2048.The process may take a
few minutes.
Number of bits in the modulus [768]:768
Generating RSA key...Done
Ruijie#
```

删除 RSA 密钥：

```
Ruijie# crypto key zeroize rsa
```

```
Do you really want to remove the key?(y/n)[n]: y
Ruijie#
```

显示相关的 RSA 公钥信息：

```
Ruijie# show crypto key mypubkey rsa

% Key pair was generated at:09:48:40, 2013-11-29
Key Size:768 bits
Key Data:
AAAAB3Nz aC1yc2EA AAADAQAB AAAAQwCN 6IRFHCBf jsHvYjQG iCL0p2kz 2v38ULC8
kAKra/Ze mG7IW3eC 8STcrkr5 s719H/bh jG/oqkwj SlUJSGqR e/sj6Ws=

Ruijie#
```

1.3 SSH 配置

命令	作用
ip ssh {timeout SECONDS authentication-retries NUMBER}	此命令用于配置交换机的 SSH 控制参数。
no ip ssh {timeout authentication-retries}	此命令用于恢复到默认数值。
ssh user NAME authentication-method {password publickey URL hostbased URL host-name HOSTNAME [IP-ADDRESS IPV6-ADDRESS]}	此命令用于为用户帐户配置 SSH 验证办法。
no ssh user NAME authentication-method	此命令用于恢复默认验证方法。
show ip ssh	此命令用于显示用户 SSH 的配置设置。
show ssh	此命令用于显示 SSH 服务器连接状态。

配置 SSH 超时的值为 160 秒：

```
Ruijie# configure terminal
Ruijie(config)# ip ssh timeout 160
Ruijie(config)#
```

配置 SSH 验证重试的值为 2 次：

```
Ruijie# configure terminal
Ruijie(config)# ip ssh authentication-retries 2
Ruijie(config)#
```

为用户 user 1 配置验证方法为公钥：

```
Ruijie# configure terminal
Ruijie(config)# ssh user tom authentication-method publickey flash: c:/user1.pub
Ruijie(config)#
```

显示 SSH 的配置设置：

```
Ruijie# show ip ssh

IP SSH server :Enabled
IP SSH service port :22
SSH server mode :V2
Authentication timeout :120 secs
Authentication retries :3 times

Ruijie#
```

显示 SSH 连接的信息：

```
Ruijie# show ssh
```

```

SID Ver.Cipher Userid Client IP Address
-----
0      V2      3des-cbc/sha1-96      zhang3 192.168.0.100
1      V2      3des-cbc/hmac-sha1    lee4567890123456 2000::243
Total Entries:2
Ruijie#

```

1.4 SSH 服务

在全局配置模式下，使用 `ip ssh server` 命令，启用 SSH 服务器功能；在全局配置模式下，使用 `ip ssh service-port` 命令，指定 SSH 的服务端口：

命令	作用
<code>ip ssh server</code>	此命令用于启用 SSH 服务器功能。
<code>no ip ssh server</code>	此命令用于禁用 SSH 服务器功能。
<code>ip ssh service-port TCP-PORT</code>	此命令用于指定 SSH 的服务端口。
<code>no ip ssh service-port</code>	此命令用于将服务端口还原为 23。

启用 SSH 服务器功能：

```

Ruijie# configure terminal
Ruijie(config)# ip ssh server
Ruijie(config)#

```

将服务端口号更改为 3000：

```

Ruijie# configure terminal
Ruijie(config)# ip ssh service-port 3000
Ruijie(config)#

```

2 基于端口的流控制

2.1 显示或清除端口安全

在 EXEC 模式或任何配置模式下，使用 `show port-security` 命令，显示当前端口的安全设置；在特权 EXEC 模式下，使用 `clear port-security` 命令，清除自动学习到的动态或永久安全条目：

命令	作用
<code>show port-security [address] [[interface INTERFACE-ID [, -]]]</code>	此命令用于显示当前端口的安全设置。
<code>clear port-security {all {address MAC-ADDR interface INTERFACE-ID [, -]} [vlan VLAN-ID]}</code>	此命令用于清除自动学习到的动态或永久安全条目。

显示接口 `gigabitEthernet0/1` 的安全设置：

```
Ruijie# show port-security interface gigabitEthernet 0/1

Interface                : Gi0/1
Port Security            : Disabled
Port Status              : Down
Violation Mode          : Protect
Static Address Aging     : Disabled
Sticky Learning         : Disabled
Aging Time               : 0 mins
Aging Type               : Absolute
Maximum MAC Addresses    : 32
Total MAC Addresses      : 0
Configured MAC Addresses : 0

Ruijie#
```

从 MAC 地址表中移除特定的安全地址：

```
Ruijie# clear port-security address 0080.0070.0007
Ruijie#
```

2.2 配置端口安全

当使能端口安全后，如果使能端口的 `sticky` 状态，该端口上自动学习的地址类型将为 `sticky` 类型，这类地址具有跟手动配置的地址一样的特性，能够被存储在运行配置中。可以通过配置 `aging time` 进行老化。

当去使能 `sticky` 状态，`sticky` 类型的地址将被转化成动态的地址。

手动配置的安全地址将被保持在运行配置中，并且可通过 `copy` 命令保存到 NVRAM 中。用户配置的安全地址将被计入端口的最大地址数中。手动配置的地址和 `sticky` 类型的地址都不能移动到另外一个端口。

当配置端口学习的最大值时，学习到的地址将保持不变。如果配置的最大值小于现有的安全地址数目，该命令将被拒绝。

使能端口安全的端口具有如下限制。

- 端口安全不能与以下能够提供更高安全性能模块同时启用：802.1X，MAC（MAC 访问控制），JWAC，WAC 和 IMPB。
- 如果一个端口被指定为镜像功能的目标端口，则不能启用端口安全功能。

- 如果该端口属于链路聚合成员端口，也不能启用端口安全功能。

当端口上的安全地址的数量超过允许的最大用户数时，将作出以下动作之一：

- Protect - 带有未知源地址的数据包将被丢弃，直到某个安全条目被移除从而释放出空间。
- Restrict - 当发生安全违规时，访问该端口的新用户将受限。。
- Shutdown - 当发生安全违规后，该接口将被禁用。

命令	作用
switchport port-security [violation {protect restrict shutdown}] [{ mac-address <mac-address> [vlan <vlan-id>] mac-address sticky [<mac-address> [vlan <vlan-id>]] }] [maximum <value 1-6656 >]	此命令用于配置端口的安全设置，以限制被允许访问端口的用户的数量。
no switchport port-security [violation [{ mac-address <mac-address> [vlan <vlan-id>] mac-address sticky [<mac-address> [vlan <vlan-id>]] }]] [maximum]	此命令用于禁用端口安全或删除一个安全的 MAC 地址。
switchport port-security aging {static time MINUTES type {absolute inactivity}}	此命令用于配置接口上自动学习到的动态安全地址的老化时间。
no switchport port-security aging {static time type}	此命令用于恢复默认设置。

指定端口上最多允许 5 个安全的 MAC 地址：

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport port-security maximum 5
Ruijie(config-if)#
```

在 gigabitEthernet 0/1 接口手动添加 VID 为 5 的安全 MAC 地址 00-00-12-34-56-78：

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport port-security mac-address 0000.1234.5678 vlan 5
Ruijie(config-if)#
```

配置交换机的端口安全违规模式为限制模式：

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport port-security violation restrict
Ruijie(config-if)#
```

将老化时间应用于接口 gigabitEthernet 0/1 上自动学习到的安全 MAC 地址：

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport port-security aging time 1
Ruijie(config-if)#
```

配置接口 gigabitEthernet 0/1 的端口安全老化时间的类型：

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport port-security aging type inactivity
Ruijie(config-if)#
```

3 DoS 攻击阻止

3.1 DoS 攻击概述

DoS 是 Denial of Service 的简称，即拒绝服务，造成 DoS 的攻击行为被称为 DoS 攻击，其目的是使计算机或网络无法提供正常的服务。最常见的 DoS 攻击有计算机网络带宽攻击和连通性攻击。

3.2 配置阻止服务 (DoS) 攻击

该命令用于为特定 DoS 攻击类型或所有的支持类型启用和禁用 DoS 阻止机制。DoS 阻止机制（匹配和执行动作）为基于硬件的特性。

启用 DoS 阻止机制后，如果接收到任意攻击数据包，交换机将记录该事件。

使用 no 命令恢复默认设置。带有全部关键字的 no dos-prevention 命令用于禁用所有支持类型的 DoS 阻止机制。所有相关设置将恢复到特定攻击类型的默认值。

以下可被大多数交换机检测到的已知 DoS 类型：

- Blat: 这种类型的攻击会通过等同于目标设备之目标端口的 TCP/UDP 源端口来发送数据包。这可能会导致目标设备响应自己。
- Land: LAND 攻击涉及到 IP 数据包，其源和目的地址被设置为目标设备的地址。这可能会导致目标设备连续回复自己。
- TCP-NULl-scan: 通过包含序列号 0 且不含标志的特定数据包来进行端口扫描。
- TCP-SYN-fin: 通过包含标志 SYN 和 FIN 标志的特定数据包来进行端口扫描。
- TCP-SYN-SRCport-less-1024: 通过包含源端口 0-1023 和 SYN 标志的特定数据包来进行端口扫描。
- TCP-xmas-scan: 通过包含序列号 0 以及 Urgent (URG), Push (PSH), 和 FIN 标志的特定数据包来进行端口扫描。
- Ping-death: 死亡之 Ping 是一种计算机攻击类型，包括向计算机发送错误格式或其它恶意的 ping 包。通常，ping 的大小为 64 字节（许多计算机无法处理一个比最大 IP 数据包还大的 ping 包，最大的 IP 数据包为 65,535 字节）。发送此大小的 ping 包可导致目标计算机崩溃。传统上，这种 bug 相对比较容易利用。通常，根据网络协议，发送一个 65536 字节的 ping 包就算是非法的，但如果这样大小的数据包是零散的，也可以发送；当目标计算机重组数据包时，可能发生缓冲溢出，这往往会导致系统崩溃。
- TCP-tiny-frag: 这种极小的 TCP 数据段攻击者利用 IP 分片创建极小的数据段，并迫使 TCP 报头信息进入一个单独的包段，以通过路由器的检查，从而发出攻击。
- All: 上述所有的类型。

命令	作用
dos-prevention DOS-ATTACK-TYPE	该命令用于为特定 DoS 攻击类型或所有的支持类型启用和禁用 DoS 阻止机制。
no dos-prevention DOS-ATTACK-TYPE	该命令用于恢复默认设置。

为 land 攻击启用 DoS 阻止机制：

```
Ruijie# configure terminal
Ruijie(config)# dos-prevention land
Ruijie(config)#
```

在所有支持的类型上启用 DoS 阻止机制：

```
Ruijie# configure terminal
Ruijie(config)# dos-prevention all
Ruijie(config)#
```

为所有支持的类型启用 DoS 阻止机制:

```
Ruijie# configure terminal
Ruijie(config)# no dos-prevention all
Ruijie(config)#
```

3.3 显示 DoS 阻止信息

在 EXEC 模式或任何配置模式下, 使用 show dos-prevention 命令, 显示 DoS 阻止状态和相关 drop 计数器:

命令	作用
show dos-prevention [DOS-ATTACK-TYPE]	此命令用于 DoS 阻止状态和相关 drop 计数器。

显示 DoS 阻止的配置信息:

```
Ruijie# show dos-prevention

DoS Prevention Information
DoS Type                      State
-----                      -
Land Attack                    Enabled
Blat Attack                    Enabled
TCP Null                       Disabled
TCP Xmas                       Disabled
TCP SYN-FIN                   Disabled
TCP SYN SrcPort Less 1024     Disabled
Ping of Death Attack          Disabled
TCP Tiny Fragment Attack      Disabled
Ruijie#
```

显示 DoS 阻止的指定类型配置信息:

```
Ruijie# show dos-prevention land

DoS Type: Land Attack
State: Enabled

Ruijie#
```


4 DHCP snooping

4.1 启用 DHCP snooping

DHCP snooping 功能可嗅探到 VLAN（启用 DHCP snooping）上非信任接口的 DHCP 数据包。有了这项功能，来自非信任接口上的 DHCP 数据包将被合法化，一个专用于启用了 DHCP snooping 的 VLAN 的 DHCP 绑定数据库将被创建。该绑定数据库提供以后会在 IP 源保护和动态 ARP 检测进程中用到的 IP 和 MAC 绑定信息。

命令	作用
ip dhcp snooping	该命令用于全局启用 DHCP snooping。
no ip dhcp snooping	该命令用于禁用 DHCP snooping。
snmp-server enable traps dhcp-server-screen	该命令用于为 forge DHCP 服务器攻击启用发送 SNMP 通知。
show ip dhcp snooping	该命令用于显示 DHCP snooping 配置。

启用 DHCP snooping:

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping
Ruijie(config)#
```

显示 DHCP snooping 配置信息:

```
Ruijie# show ip dhcp snooping

DHCP Snooping is enabled
DHCP Snooping is enabled on VLANs:
10, 15-18
Verification of MAC address is disabled
Information option of allowed on un-trusted interface is disabled

Interface      TrustedRate Limit
-----
Gi0/1   no      10
Gi0/8   no      50
Gi0/9   yes     no_limit

Ruijie#
```

4.2 清除 DHCP snooping

在特权 EXEC 模式下，使用 `clear ip dhcp snooping database statistics` 命令，清除 DHCP 绑定的数据库统计信息；在特权 EXEC 模式下，使用 `clear ip dhcp snooping binding` 命令，清除 DHCP 绑定条目：

命令	作用
clear ip dhcp snooping database statistics	该命令用于清除 DHCP 绑定的数据库统计信息。
clear ip dhcp snooping binding [MAC-ADDRESS] [IP-ADDRESS] [vlan VLAN-ID] [interface INTERFACE-ID]	该命令用于清除 DHCP 绑定条目，包括手动配置的绑定条目。

清除 snooping 数据库统计信息:

```
Ruijie# clear ip dhcp snooping database statistics
```

```
Ruijie#
```

清除所有的 snooping 绑定条目:

```
Ruijie# clear ip dhcp snooping binding  
Ruijie#
```

4.3 DHCP snooping 绑定

命令	作用
ip dhcp snooping binding MAC-ADDRESS vlan VLAN-ID IP-ADDRESS interface INTERFACE-ID expiry SECONDS	该命令用于手动配置一个 DHCP snooping 项。
show ip dhcp snooping binding [IP-ADDRESS] [MAC-ADDRESS] [vlan VLAN-ID] [interface [INTERFACE-ID [.-]]]	该命令用于显示 DHCP snooping 绑定条目。
ip dhcp snooping limit entries NUMBER	该命令用于配置接口可学习的 DHCP snooping 绑定条目数量。
no ip dhcp snooping limit entries	使用此命令复位 DHCP 信息条目限制。
renew ip dhcp snooping database URL	该命令用于更新 DHCP 绑定的数据库。

配置 VLAN 2 中 IP 地址为 10.1.1.1, MAC 地址为 00-01-02-03-04-05 的 DHCP snooping 条目, 和终止时期为 100 秒的端口 gi0/10 :

```
Ruijie# ip dhcp snooping binding 00-01-02-03-04-05 vlan 2 10.1.1.1 interface gi0/10  
expiry 100  
Ruijie#
```

禁用 VLAN 2 中 IP 地址为 10.1.1.1, MAC 地址为 00-01-02-03-04-05 DHCP snooping 条目和端口 gi0/10:

```
Ruijie# ip dhcp snooping binding 00-01-02-03-04-05 vlan 2 10.1.1.1 interface gi0/10  
Ruijie#
```

显示 DHCP snooping 绑定条目:

```
Ruijie# show ip dhcp snooping binding  
  
MAC Address      IP Address      Lease(seconds)  Type           VLAN    Interface  
-----  
-  
00-01-02-03-04-05 10.1.1.10      1500            dhcp-snooping 100     Gi0/5  
00-01-02-00-00-05 10.1.1.11      1495            dhcp-snooping 100     Gi0/5  
  
Total Entries:2  
  
Ruijie#
```

显示 IP 10.1.1.1 的 DHCP snooping 绑定条目:

```
Ruijie# show ip dhcp snooping binding 10.1.1.1  
  
MAC Address      IP Address      Lease (seconds)  Type           VLAN    Interface  
-----  
00-01-02-03-04-05 10.1.1.1      1500            dhcp-snooping 100     Gi0/5  
  
Total Entries:1  
  
Ruijie#
```

显示 IP 10.1.1.1, MAC 00-01-02-00-00-05 的 DHCP snooping 绑定条目:

```
Ruijie# show ip dhcp snooping binding 10.1.1.11 00-01-02-00-00-05  
  
MAC Address      IP Address      Lease (seconds)  Type           VLAN    Interface  
-----  
00-01-02-00-00-05 10.1.1.11      1495            dhcp-snooping 100     Gi0/5
```

```
Total Entries:1
```

```
Ruijie#
```

显示 VLAN 100 上 IP 10.1.1.1, MAC 00-01-02-03-04-05 的 DHCP snooping 绑定条目:

```
Ruijie# show ip dhcp snooping binding 10.1.1.11 00-01-02-00-00-05 vlan 100
```

```
MAC Address      IP Address      Lease (seconds) Type      VLAN      Interface
-----
00-01-02-03-04-05 10.1.1.1      1500      dhcp-snooping 100      Gi0/5
```

```
Total Entries:1
```

```
Ruijie#
```

显示 VLAN 100 的 DHCP snooping 绑定条目:

```
Ruijie# show ip dhcp snooping binding vlan 100
```

```
MAC Address      IP Address      Lease (seconds) Type      VLAN      Interface
-----
00-01-02-03-04-05 10.1.1.10     1500      dhcp-snooping 100      Gi0/5
00-01-02-00-00-05 10.1.1.11     1495      dhcp-snooping 100      Gi0/5
```

```
Total Entries:2
```

```
Ruijie#
```

显示接口 gi0/5 的 DHCP snooping 绑定条目:

```
Ruijie# show ip dhcp snooping binding interface Gi0/5
```

```
MAC Address      IP Address      Lease (seconds) Type      VLAN      Interface
-----
00-01-02-03-04-05 10.1.1.10     1500      dhcp-snooping 100      Gi0/5
00-01-02-00-00-05 10.1.1.11     495       dhcp-snooping 100      Gi0/5
```

```
Total Entries:2
```

```
Ruijie#
```

在以太网端口 0/1 至 100 上配置绑定条目的限制:

```
Ruijie# configure terminal
Ruijie(config)# interface gi0/3
Ruijie(config-if)# ip dhcp snooping limit entries 100
Ruijie(config-if)#
```

更新 DHCP snooping 绑定的数据库:

```
Ruijie# renew ip dhcp snooping database tftp://10.0.0.2/store/dhcp-snp-bind
Ruijie#
```

4.4 DHCP snooping 配置

当 DHCP 数据包到达 VLAN (已启用 DHCP Snooping) 上的端口时, DHCP snooping 功能会确认该数据包。如果网关地址与 0 或现在的 Option 82 不相等, 确认进程默认将丢弃该数据包。

命令	作用
ip dhcp snooping information option allow-untrusted	该命令用于全局允许未信任接口上带有中继选项 82 信息的 DHCP 数据包。
no ip dhcp snooping information option allow-untrusted	该命令用于不允许带有中继 Option 82 的数据包。
ip dhcp snooping trust	该命令用于将一个端口配置成 DHCP snooping 的信任接口。
no ip dhcp snooping trust	该命令用于恢复默认设置。
ip dhcp snooping limit rate VALUE	该命令用于配置一个接口每秒可接收到的 DHCP 信息数量。
no ip dhcp snooping limit rate	该命令用于将 DHCP 信息的速率限制复位。

ip dhcp snooping station-move deny	该命令用于禁用 DHCP snooping station move 状态。
no ip dhcp snooping station-move deny	该命令用于启用 DHCP snooping 漫游状态。
ip dhcp snooping verify mac-address	该命令用于启用 DHCP 数据包中源 MAC 地址与客户端硬件地址进行匹配的验证。
no ip dhcp snooping verify mac-address	该命令用于禁用 MAC 地址的认证。
ip dhcp snooping vlan VLAN-ID [, -]	该命令用于启用一个 VLAN 或一个 VLAN 组上的 DHCP snooping。
no ip dhcp snooping vlan VLAN-ID [, -]	该命令用于禁用一个 VLAN 或一个 VLAN 组上的 DHCP snooping。

启用 Option 82 的 DHCP snooping，允许非信任端口：

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping information option allow-untrusted
Ruijie(config)#
```

启用端口 0/3 的 DHCP snooping 信任：

```
Ruijie# configure terminal
Ruijie(config)# interface gi0/3
Ruijie(config-if)# ip dhcp snooping trust
Ruijie(config-if)#
```

配置交换机每秒在端口 0/3 上可接收到的 DHCP 信息数量：

```
Ruijie# configure terminal
Ruijie(config)# interface gi0/3
Ruijie(config-if)# ip dhcp snooping limit rate 100
Ruijie(config-if)#
```

禁用漫游状态：

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping
Ruijie(config)# ip dhcp snooping vlan 10
Ruijie(config)# ip dhcp snooping station-move deny
Ruijie(config)#
```

启用 DHCP 数据包中源 MAC 地址与客户端硬件地址进行匹配的验证：

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping verify mac-address
Ruijie(config)#
```

启用 VLAN 10 上的 DHCP snooping：

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping vlan 10
Ruijie(config)#
```

启用一组 VLAN 的 DHCP snooping：

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping vlan 10,15-18
Ruijie(config)#
```

4.5 DHCP snooping 数据库

在全局配置模式下，使用 ip dhcp snooping database 命令，配置将 DHCP snooping 绑定项目存储到本地闪存或远程站点上，使用 no 命令可恢复默认设置；在 EXEC 模式或任何配置模式下，使用 show ip dhcp snooping database 命令，显示 DHCP snooping 数据库的统计信息：

命令	作用
ip dhcp snooping database {URL write-delay SECONDS}	该命令用于配置将 DHCP snooping 绑定项目存储到本地闪存或远程站点上。
no ip dhcp snooping database [write-delay]	该命令用于恢复默认设置。

```
show ip dhcp snooping database
```

该命令用于显示 DHCP snooping 数据库的统计信息。

将绑定条目存储到文件系统中的文件中:

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping database tftp://10.0.0.2/store/dhcp-snp-bind
Ruijie(config)#
```

显示 DHCP snooping 数据库统计信息:

```
Ruijie# show ip dhcp snooping database

URL: tftp://10.0.0.2/store/dhcp-snp-bind
Write Delay Time:300 seconds

Last ignored bindings counters :
Binding collisions : 0      Expiredlease : 0
Invalid interfaces : 0      Unsupported vlans : 0
Parse failures : 0      Checksum errors : 0

Ruijie#
```

5 动态 ARP 检测

5.1 arp access-list

该用于创建或修改一个 ARP 访问列表。该命令将进入 APP 访问列表配置模式。该名称在所有访问列表中必须是唯一的。该名称中所用的字符应区分大小写。访问列表末尾处有一则委婉的拒绝声明。使用 no 命令，可删除 ARP 访问列表。

命令	作用
arp access-list NAME	此命令用于创建或修改一个 ARP 访问列表。
no arp access-list NAME	该命令用于删除 ARP 访问列表。

配置带有两个允许条目的 ARP 访问列表：

```
Ruijie# configure terminal
Ruijie(config)# arp access-list static-arp-list
Ruijie(config-arp-nacl)# permit ip 10.20.0.0 0.0.255.255 mac any
Ruijie(config-arp-nacl)# permit ip 10.30.0.0 0.0.255.255 mac any
Ruijie(config-arp-nacl)#
```

5.2 clear ip arp inspection log

在特权 EXEC 模式下，使用 clear ip arp inspection log 命令，清除 ARP 检测日志缓冲：

命令	作用
clear ip arp inspection log	该命令用于清除 ARP 检测日志缓冲。

清除检测日志信息。

```
Ruijie# clear ip arp inspection log
Ruijie#
```

5.3 clear ip arp inspection statistics

在特权 EXEC 模式下，使用 clear ip arp inspection statistics 命令，清除动态 ARP 检测（DAI）统计信息：

命令	作用
clear ip arp inspection statistics {all vlan VLAN-ID [, -]}	该命令用于清除动态 ARP 检测（DAI）统计信息。

从 VLAN 1 处清除 DAI 统计信息。

```
Ruijie# clear ip arp inspection statistics vlan 1
Ruijie#
```

5.4 ip arp inspection filter vlan

该命令用于指定一个 ARP 访问列表，该列表用于 VLAN 的 ARP 检测。可为 VLAN 最多指定一个访问列表。使用 no 命令移除规格

动态 ARP 检测会在 VLAN 上检测到接收的 ARP 数据包，以便确认数据包绑定的源 IP 和源 MAC 地址为有效地址。验证过程将匹配地址绑定，并与 DHCP snooping 数据库条目相比较。

配置好命令后，验证过程将匹配地址绑定，并与 DHCP snooping 数据库和访问列表条目相比较。

ARP ACL 优先于 DHCPsnooping 绑定数据库中的条目。如果数据包通过访问控制列表明确被拒绝，该数据包被丢弃。如果数据包明确被拒绝，在没有指定关键字“static”情况下，将进一步匹配该数据包，并与 DHCP snooping 绑定条目相比较。如果指定关键字“static”，则丢弃明确拒绝的数据包。

命令	作用
<code>ip arp inspection filter ARP-ACL-NAME vlan VLAN-ID [, -] [static]</code>	该命令用于指定一个 ARP 访问列表，该列表用于 VLAN 的 ARP 检测。
<code>no ip arp inspection filter ARP-ACL-NAME vlan VLAN-ID [, -] [static]</code>	该命令用于移除规格。

为 DAI 应用 ARP ACL 静态 ARP 列表到 VLAN 10。

```
Ruijie# configure terminal
Ruijie(config)# ip arp inspection filter static-arp-list vlan 10
Ruijie(config)#
```

5.5 ip arp inspection limit

该命令用于限制接口上入站 ARP 请求和响应速率。该命令在信任和非信任接口上都生效。对于已配置的脉冲周期来说，当每秒 ARP 数据包速率超过限制，且该情况一直持续，该端口将处于错误禁用状态。使用 no 命令恢复默认设置。

命令	作用
<code>ip arp inspection limit {rate VALUE [burst interval SECONDS] none}</code>	该命令用于限制接口上入站 ARP 请求和响应速率。
<code>no ip arp inspection limit</code>	使用此命令恢复默认设置。

限制入站 ARP 请求为每秒 30 个数据包，并设置接口监控间隔为连续 5 秒。

```
Ruijie# configure terminal
Ruijie(config)# interface gi0/10
Ruijie(config-if)# ip arp inspection limit rate 30 burst interval 5
Ruijie(config-if)#
```

5.6 ip arp inspection log-buffer

该命令用于配置 ARP 检测日志缓冲参数。ARP 检测日志缓冲追踪 ARP 数据包信息。第一个检查的数据包将被发送到系统日志模块，并记录在检测日志缓冲中。属于同一个会话的后续数据包将不会发送到日志模块，除非它在日志缓冲区中的记录被清除。如果日志缓冲区已满，但是还是有更多的日至事件出现时，这些事件将不会被记录。如果用户指定的缓冲空间小于当前条目数量，则自动清除日志缓冲区。

命令	作用
<code>ip arp inspection log-buffer entries NUMBER</code>	该命令用于配置 ARP 检测日志缓冲参数。
<code>no ip arp inspection log-buffer entries</code>	使用此命令恢复默认设置。

将最大缓冲数量值更改为 64。

```
Ruijie# configure terminal
Ruijie(config)# ip arp inspection log-buffer entries 64
Ruijie(config)#
```

5.7 ip arp inspection trust

使用 `arp inspection trust` 命令，为动态 ARP 检测指定一个信任接口。如果接口处于信任状态，到达该接口的 ARP 数据包将不会被检测。如果接口处于非信任状态，到达该接口，属于此 VLAN 且支持检测特性的数据包将被检测。使用 `no` 命令可禁用信任状态。

命令	作用
<code>ip arp inspection trust</code>	该命令用于为动态 ARP 检测指定一个信任接口。
<code>no ip arp inspection trust</code>	使用此命令可禁用信任状态。

将端口 0/3 配置成为 DAI 的信任端口。

```
Ruijie# configure terminal
Ruijie(config)# interface gi0/3
Ruijie(config-if)# ip arp inspection trust
Ruijie(config-if)#
```

5.8 ip arp inspection validate

在 ARP 检测时期，该命令用于指定要执行的其它检测操作。将对到达此非信任接口，属于该 VLAN 且支持 IP ARP 检测的数据包执行指定的检测操作。如果未指定任何参数，所有选项处于启用或禁用状态。使用“no”命令，移除指定的其它检测。

命令	作用
<code>ip arp inspection validate [src-mac] [dst-mac] [ip]</code>	在 ARP 检测时期，该命令用于指定要执行的其它检测操作。
<code>no ip arp inspection validate [src-mac] [dst-mac] [ip]</code>	该命令用于移除指定的其它检测。

启用源 MAC 地址的认证。

```
Ruijie# configure terminal
Ruijie(config)# ip arp inspection validate src-mac
Ruijie(config)#
```

5.9 ip arp inspection vlan

如果 VLAN 的 ARP 检测已启用，则 ARP 数据包，包括属于该 VLAN，并到达此非信任接口的 ARP 请求和响应数据包都将被确认。如果在 ARP ACL 或 DHCP snooping 绑定库中不允许源 MAC 地址和源 IP 地址的 IP-to-MAC 地址绑定对，将丢弃 ARP 数据包。除了地址绑定检查，其它由 IP ARP 检测验证命令定义的检查都将被核实。

命令	作用
<code>ip arp inspection vlan VLAN-ID [, -]</code>	该命令用于为动态 ARP 检测启用特定的 VLAN。
<code>no ip arp inspection vlan VLAN-ID [, -]</code>	该命令用于禁用 VLAN 的动态 ARP 检测。

启用 VLAN 2 的 ARP 检测。

```
Ruijie# configure terminal
Ruijie(config)# ip arp inspection vlan 2
Ruijie(config)#
```


5.10 ip arp inspection vlan logging

使用 `ip arp inspection vlan logging` 命令，控制已登录的数据包类型。使用 `no` 命令，恢复到默认值。如果没有指定，拒绝 ARP 数据包后，所有正在登录的类型都将恢复到已登录状态。

命令	作用
<code>ip arp inspection vlan VLAN-ID [,-] logging {acl-match {permit all none} dhcp-bindings {permit all none}}</code>	该命令用于控制已登录的数据包类型。
<code>no ip arp inspection vlan VLAN-ID [,-] logging {acl-match dhcp-bindings}</code>	使用此命令，恢复到默认值。

配置 VLAN1 上的 ARP 检测，以添加数据包到与 ACL 相匹配的日志中：

```
Ruijie# configure terminal
Ruijie(config)# ip arp inspection vlan 1 logging acl-match all
Ruijie(config)#
```

5.11 permit | deny (arp access-list)

使用 `permit any` 选项将允许不与之前规则相匹配的数据包。使用 `deny` 命令定义 ARP 拒绝条目。在 ARP 访问列表配置模式下，使用 `permit | deny (arp access-list)` 命令，定义 ARP 允许条目；使用 `no` 命令，移除一个条目：

命令	作用
<code>{permit deny} ip {any host SENDER- IP SENDER-IP SENDER-IP-MASK} mac {any host SENDER-MAC SENDER- MAC SENDER-MAC- MASK}</code>	此命令用于定义 ARP 允许条目。
<code>no {permit deny} ip {any host SENDER-IP SENDER-IP SENDER- IP-MASK} mac {any host SENDER- MAC </code>	使用此命令，移除一个条目。

配置带有两个允许条目的 ARP 访问列表：

```
Ruijie# configure terminal
Ruijie(config)# arp access-list static-arp-list
Ruijie(config-arp-nacl)# permit ip 10.20.0.0 255.255.0.0 mac any
Ruijie(config-arp-nacl)# permit ip 10.30.0.0 255.255.0.0 mac any
Ruijie(config-arp-nacl)#
```

5.12 show ip arp inspection

要显示特定范围 VLAN 的 DAI 状态，在 EXEC 模式或任何配置模式中执行以下命令：

命令	作用
<code>show ip arp inspection [interfaces [INTERFACE-ID [,-]] statistics [vlan VLAN-ID [,-]]]</code>	此命令用于显示特定范围 VLAN 的 DAI 状态。

显示已通过 DAI 处理，VLAN10 中的数据包统计信息

```
Ruijie# show ip arp inspection statistics vlan 10
VLAN   Forwarded      Dropped      DHCP Drops    ACL Drops
-----
10     21546          145261       145261        0
VLAN   DHCP Permits  ACL Permits  Source MAC Failures
```

```

-----
10      21546      0      0
VLAN    Dest MAC Failures      IP Validation Failures
-----
10      0      0

Ruijie#

```

显示已通过 DAI 处理，所有活动 VLAN 中的数据包统计信息。

```

Ruijie# show ip arp inspection statistics

VLAN    Forwarded      DroppedDHCP Drops      ACL Drops
-----
1        0              0              0              0
2        0              0              0              0
10       21546         145261         145261         0
100      0              0              0              0
200      0              0              0              0
1024     0              0              0              0
VLAN    DHCP Permits   ACL Permits      Source MAC Failures
-----
1        0              0              0
2        0              0              0
10       21546         0              0
100      0              0              0
200      0              0              0
1024     0              0              0
VLAN    Dest MAC Failures      IP Validation Failures
-----
1        0              0
2        0              0
10       0              0
100      0              0
200      0              0
1024     0              0

Ruijie#

```

显示 DAI 的配置和操作模式。

```

Ruijie# show ip arp inspection

Source MAC Validation :Disabled
Destination MAC Validation:Disabled
IP Address Validation :Disabled
VLAN  State          ACL Match          Static ACL
-----
10    Enabled          -                  -
VLAN  ACL Logging DHCP Logging
-----
10    Deny             Deny

Ruijie#

```

显示接口 gi0/3 的信任状态。

```

Ruijie# show ip arp inspection interfaces gi0/3

Interface      Trust State      Rate(pps)      Burst Interval
-----
gi0/3 untrusted      30             5
Ruijie#

```

显示交换机接口的信任状态。

```

Ruijie# show ip arp inspection interfaces

Interface      Trust State      Rate(pps)      Burst Interval
-----
gi0/1 untrusted      30             1
gi0/2 untrusted      30             1
gi0/3 untrusted      30             5

```

```

gi0/5  trusted      None    1
gi0/6  untrusted     30     1
gi0/7  untrusted     30     1
gi0/8  untrusted     30     1
Total Entries:7
Ruijie#

```

5.13 show ip arp inspection log

要显示 ARP 检测日志缓冲区，在 EXEC 模式或任何配置模式下执行以下命令：

命令	作用
show ip arp inspection log	此命令用于显示 ARP 检测日志缓冲区。

显示检测日志缓冲区。

```

Ruijie# show ip arp inspection log

Total log buffer size:64

Interface      VLAN    Sender IP      Sender MAC      Occurrence
-----
gi0/1  100    10.20.1.1     00-20-30-40-50-60  1 (2013-12-28 23:08:66)
gi0/2  100    10.5.10.16    55-66-20-30-40-50  2 (2013-12-02 00:11:54)
gi0/3  100    10.58.2.30    10-22-33-44-50-60  1 (2013-12-30 12:01:38)

Total Entries:3

Ruijie#

```

5.14 show ip arp spoofing-prevention

要显示 ARP 攻击防御的配置，在 EXEC 模式或任何配置模式下执行以下命令：

命令	作用
show ip arp spoofing-prevention	此命令用于显示 ARP 攻击防御的配置。

命令 show ip arp spoofing-prevention 的示例输出。

```

Ruijie# show ip arp spoofing-prevention

IP              MAC              Interfaces
-----
10.254.254.251  00-00-00-11-11-11 eth2/0/10

Total Entries: 1
Ruijie#

```

6 IP Source Guard

6.1 理解 IP Source Guard

IP Source Guard 维护一个 IP 源地址绑定数据库，IP Source Guard 可以在对应的接口上对主机报文进行基于源 IP、源 IP 加源 MAC 的报文过滤，从而保证只有 IP 源地址绑定数据库中的主机才能正常使用网络；IP Source Guard 之所以在 DHCP 使用中能够有效的安全控制，这主要取决于 IP 源地址绑定数据库，IP Source Guard 会自动将 DHCP Snooping 绑定数据库中的合法用户绑定同步到 IP Source Guard 的 IP 源地址绑定数据库，这样 IP SourceGuard 就可以在打开 DHCP Snooping 的设备上对客户端的报文进行严格过滤。

默认情况下，打开 IP Source Guard 功能的端口会过滤所有非 DHCP 的 IP 报文；只有当客户端通过 DHCP 从服务器获取到合法的 IP 或者管理员为客户端配置了静态的 IP 源地址绑定后，端口才允许和这个客户端匹配的 IP 报文通过。

IP Source Guard 支持基于 IP+MAC 或者基于 IP 的过滤，如果打开基于 IP+MAC 的过滤，IP Source Guard 会对所有报文的 MAC+IP 进行检测，仅仅允许 IP 源地址绑定表格中存在的用户报文通过；而基于 IP 的过滤，仅仅会对报文的源 IP 地址进行检测。

在支持 ARP Check 功能的交换机系统上，开启 IP Source Guard 功能和 ARP Check 功能后，交换机能使用 IP Source Guard 对 IP 报文进行 IP+MAC 或仅源 IP 过滤，ARP Check 功能对 ARP 报文中的 Sender IP+Sender MAC 或仅对 Sender IP 检查过滤。

IP Source Guard 的相关过滤功能都是基于硬件实现的，接口上的 IP Source Guard 过滤规则可以理解为基于接口的可以动态改变的 ACL，各系列产品的过滤表容量存在差异，因此在规划 IP Source Guard 应用之前请参看相关产品规格说明。

6.2 ip verify source vlan dhcp-snooping

此命令用于启用端口的 IP Source Guard。此命令可用于物理端口和聚合端口配置。使用此命令启用已配置端口的 IP Source Guard。使用“no”命令禁用 IP 源保护。

当启用 IP 源保护端口，到达该端口的 IP 数据包将通过端口访问控制列表进行验证。端口访问控制列表是一种硬件机制，它的条目可以来自手动配置条目或 DHCP Snooping 绑定数据库。任何未能通过验证的数据包将被丢弃。

有两种类型的验证。

如果未指定选项 IP-MAC，则验证仅基于源 IP 地址和 VLAN 检测。

如果指定选项 IP-MAC，则验证基于源 MAC 地址，VLAN 和 IP 地址。

命令	作用
<code>ip verify source vlan dhcp-snooping [ip-mac]</code>	此命令用于启用端口的 IP Source Guard。此命令可用于物理端口和端口通道配置。使用此命令启用已配置端口的 IP Source Guard。
<code>no ip verify source vlan dhcp-snooping [ip-mac]</code>	使用此命令禁用 IP Source Guard。

启用 gi0/1 的 IP Source Guard:

```
Ruijie# configure terminal
Ruijie(config)# interface gi0/1
Ruijie(config-if)# ip verify source vlan dhcp-snooping
Ruijie(config-if)#
```

6.3 ip source guard binding

此命令用于为 IP 源保护创建静态条目。使用“no”命令，删除一条静态绑定条目。该命令指定的参数必须与要删除的配置参数完全匹配。

如果 MAC 地址和 VLAN 配置项已经存在，现有绑定条目将会更新。指定的接口可以是物理端口或端口信道接口。

命令	作用
<code>ip source binding MAC-ADDRESS vlan VLAN-ID IP-ADDRESS interface INTERFACE-ID [,-]</code>	此命令用于为 IP Source Guard 创建静态条目。
<code>no ip source binding MAC-ADDRESS vlan VLAN-ID IP-ADDRESS interface INTERFACE-ID [,-]</code>	使用此命令，删除一条静态绑定条目。此命令指定的参数必须与要删除的配置参数完全匹配。

在 VLAN 2，接口 0/10 中使用 IP 地址 10.1.1.1 和 MAC 地址 00-01-02-03-04-05 配置 IP Source Guard 条目：

```
Ruijie# configure terminal
Ruijie(config)# ip source binding 00-01-02-03-04-05 vlan 2 10.1.1.1 interface gi0/10
Ruijie(config)#
```

在 VLAN 2，gi0/10 中删除 IP 地址为 10.1.1.1 和 MAC 地址为 00-01-02-03-04-05 的 IP Source Guard 条目：

```
Ruijie# configure terminal
Ruijie(config)# no ip source binding 00-01-02-03-04-05 vlan 2 10.1.1.1 interface
gi0/10
Ruijie(config)#
```

6.4 show ip source binding

要显示 IP Source Guard 绑定条目，在 EXEC 模式或任何配置模式执行以下命令：

命令	作用
<code>show ip source binding [IP- ADDRESS] [MAC-ADDRESS] [dhcp- snoothing static] [vlan VLAN-ID] [interface INTERFACE-ID [,-]]</code>	此命令用于显示 IP Source Guard 绑定条目。IP Source Guard 绑定条目可以手动配置或通过 DHCP snooping 至保护 IP 流量学习获得。

在没有任何参数的情况下显示 IP Source Guard 绑定条目：

```
Ruijie# show ip source binding

MAC Address          IP Address          Lease(sec)  Type           VLAN  Interface
-----
00-01-01-01-01-01   10.1.1.10          infinite    static         100   gi0/3
00-01-01-01-01-10   10.1.1.11          3120       dhcp-snooping  100   gi0/3

Total Entries:2

Ruijie#
```

显示 IP 10.1.1.10 的 IP Source Guard 绑定条目：

```
Ruijie# show ip source binding 10.1.1.10

MAC Address  IP Address  Lease(sec)  Type  VLAN  Interface
-----
00-01-01-01-01-01 10.1.1.10  infinite    static  100   gi0/3

Total Entries:1

Ruijie#
```

由 DHCP snooping 学习到的，在 VLAN 100，gi0/3 中 IP 地址为 10.1.1.1 和 MAC 地址为 00-01-01-01-01-10 的 IP Source Guard 绑定条目：

```
Ruijie# show ip source binding 10.1.1.10 00-01-01-01-01-10 dhcp-snooping vlan 100
interface gi0/3

MAC Address  IP Address  Lease(sec)  Type           VLAN  Interface
-----
00-01-01-01-01-10 10.1.1.11   3564        dhcp-snooping  100   gi0/3

Total Entries:1

Ruijie#
```

6.5 show ip verify source

要显示特定端口的硬件端口 ACL 条目，在 EXEC 模式或任何配置模式下执行以下命令：

命令	作用
<code>show ip verify source [interface INTERFACE-ID [,]]</code>	此命令用于显示特定端口的硬件端口 ACL 条目。它表明了 IP Source Guard 验证后的硬件过滤行为。

当在 VLAN 100 - 110 启用 DHCP Snooping 功能，接口的 IP 源过滤模式为 IP，VLAN 100 现有 IP 地址绑定 10.1.1.1 时的相关信息：

```
Ruijie# show ip verify source interface gi0/3
Interface      Filter-type    Filter-mode IP address  MAC address  VLAN
-----
gi0/3 ip          active      10.1.1.1    100
gi0/3 ip          active      deny-all    101-120
Total Entries:2
Ruijie#
```

当接口的 IP 源过滤模式为 IP-MAC，VLAN 100 现有 IP-MAC 绑定 IP 地址 10.1.1.10 绑定 MAC 地址 00-01-01-01-01-01，VLAN 101 的 IP 地址 10.1.1.11 绑定 MAC 地址 00-01-01-01-01-10 时的相关信息：

```
Ruijie# show ip verify source interface gi0/3
Interface      Filter-type    Filter-mode IP address  MAC address  VLAN
-----
gi0/3 ip-mac    active      10.1.1.10  00-01-01-01-01-01 100
gi0/3 ip-mac    active      10.1.1.11  00-01-01-01-01-10 101
ip-mac active      deny-all   -            102-120
Total Entries:3
Ruijie#
```

7 风暴控制命令

7.1 风暴控制说明

该命令用于配置设备免受广播、组播和 DA 未知数据报风暴的攻击。使用 no 命令采用默认设置。输入 storm-control 命令，为接口上指定的流量类型启用风暴控制。有两种方法来恢复禁用的端口。

- 用户可以使用 errdisable recovery cause 命令，让被风暴控制禁用的端口自动恢复。
- 用户可以通过输入 shutdown 命令手动恢的端口，然后再对端口使用 no shutdown 命令。

在一个接口上只有一个计量模式（百分比、kbps 或 PPS）可以生效。在接口上，如果稍后指定的计量模式选择与之前的模式不同，之前配置的风暴将重置为默认状态（在此规范中禁用）。

由于硬件的限制，当计量模式为百分比或 kbps 时：

- 不能将动作指定为 shutdown 模式。
- drop 模式和 none 模式不记录系统 log。

7.2 storm-control

命令	作用
storm-control {{broadcast multicast unicast} level {pps PPS-RISE [PPS-LOW] kbps KBPS-RISE [KBPS-LOW] LEVEL-RISE [LEVEL-LOW]} action {shutdown drop none}}	此命令用于配置设备免受广播、组播和 DA 未知数据报风暴的攻击。。
no storm-control {broadcast multicast unicast action}	使用此命令，将恢复到默认设置。
storm-control polling {interval SECONDS retries {NUMBER infinite}}	此命令用于为收到的数据包计数配置轮询间隔。
no storm-control polling {interval retries}	使用此命令，将恢复到默认设置。
show storm-control interface INTERFACE-ID [, -] [broadcast multicast unicast]	此命令用于显示当前风暴控制设置。

在 gigabitEthernet 0/1 和 gigabitEthernet 0/2 上启用广播风暴控制。gigabitEthernet 0/1 的阈值设置为每秒 500 个数据报则关闭动作，接口端口 3.2 的阈值为达到 70%则采用丢弃动作：

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# storm-control broadcast level pps 500
Ruijie(config-if)# storm-control action shutdown
Ruijie(config)# interface gigabitEthernet 0/2
Ruijie(config-if)# storm-control broadcast level 70 60
Ruijie(config-if)# storm-control action drop
Ruijie(config-if)#
```

指定轮询时间间隔为 15 秒。

```
Ruijie# configure terminal
Ruijie(config)# storm-control polling interval 15
Ruijie(config)#
```

显示当前广播风暴控制设置。

```
Ruijie# show storm-control interface range gigabitEthernet 0/1-6 broadcast

Interface      Action Threshold      Current State
```

```

-----
Gi0/1 Drop 500/300 pps 200 pps Forwarding
Gi0/2 Drop 80/64 % 20 % Forwarding
Gi0/3 Drop 80/64 % 70 % Dropped
Gi0/4 Shutdown 60/50 % 20 % Forwarding
Gi0/5 None 60000/50000 kbps 2000 kbps Forwarding
Gi0/6 None - - Inactive

```

Total Entries:6

Ruijie#

显示端口 0/1 到端口 0/2 的所有接口设置。

```
Ruijie# show storm-control interface gigabitEthernet 0/1-2
```

```

Polling Interval:15 sec Shutdown Retries :Infinite
Interface Storm Action Threshold Current State
-----
eth1/0/1Broadcast Drop 80/64 % 50% Forwarding
eth1/0/1Multicast Drop 80/64 % 50% Forwarding
eth1/0/1Unicast Drop 80/64 % 50% Forwarding
eth1/0/2Broadcast Shutdown 500/300 pps - Error Disabled
eth1/0/2Multicast Shutdown 500/300 pps - Error Disabled
eth1/0/2Unicast Shutdown 500/300 pps - Error Disabled

```

Total Entries:6

Ruijie#

8 环路检测命令

8.1 环路检测说明

该命令用于全局启用环路检测功能。使用“no”命令，全局禁用该功能。

一般来说，当合作交换机不支持环路检测功能时，连接用户的端口使用基于端口的环路检测，聚合端口使用基于 VLAN 的检测。

在执行基于端口的检测时，启用环路检测功能的端口将发送未标记的基于端口的环路检测数据包，用于发现环路。如果路径上发生环路，那么该数据包将循环到同一端口或同一设备上的其他端口。当启用环路检测的端口检测到存在环路条件时，将禁止在该端口发送和接收数据包。

在执行基于 VLAN 的检测时，启用环路检测功能的 VLAN 成员端口将定期为每个端口发送基于 VLAN 的数据包。如果检测到的 VLAN 是已标记成员，将发送已标记的环路检测数据包。如果检测到的 VLAN 是未标记成员，将发送未标记的环路检测数据包。如果 VLAN 路径上产生环路，检测到有环路的 VLAN 端口将暂时停止发送或接收数据包。

当禁用环路检测的端口接收到环路检测数据包并检测到数据包由系统本身发送时，如果数据包基于端口的环路检测，则会阻止发送的端口，如果数据包基于 VLAN 的端口环路检测，则会阻止发送端口所在的 VLAN。

如果端口配置为基于 VLAN，且端口为多个 VLAN 的未标记成员，则该端口会向每一个 VLAN 发送一个未标记的端口环路检测数据包，带有数据包 VLAN 字段中指定的 VLAN 号。

有两种方法来恢复错误禁用的端口。用户可以使用 `errdisable recovery cause loopback-detect` 命令，开启由环路检测禁用的端口自动恢复功能。或者管理员可首先输入 `shutdown` 命令手动恢复端口，再对端口使用 `no shutdown` 命令。

如果配置 `errdisable recovery cause loopback-detect` 命令，封锁端口的 VLAN 可自动恢复。或者管理员可首先输入 `shutdown` 命令手动恢复端口，再对端口使用 `no shutdown` 命令。

8.2 loop-detection

命令	作用
<code>loop-detection [mode {port-based vlan-based}]</code>	此命令用于全局启用环路检测功能。
<code>no loop-detection [mode]</code>	使用此命令，全局禁用此功能。
<code>loop-detection</code>	此命令用于启用接口的环路检测功能。此命令可用于端口和端口信道接口配置。
<code>no loop-detection</code>	使用此命令，在接口禁用此功能。
<code>loop-detection interval SECONDS</code>	此命令用于配置发送环路检测数据包去探测环路的时间间隔。
<code>no loop-detection interval</code>	使用此命令恢复默认设置。
<code>loop-detection vlan VLAN-LIST</code>	此命令用于配置在 VLAN 中启用环路检测。
<code>no loop-detection vlan VLAN-LIST</code>	使用此命令恢复到默认设置。
<code>show loop-detection [interface INTERFACE-ID [,]-]</code>	此命令用于显示当前环路检测控制设置。

全局启用基于端口的环路检测功能，并设置检测模式为基于端口：

```
Ruijie# configure terminal
Ruijie(config)# loop-detection
Ruijie(config)# loop-detection mode port-based
Ruijie(config)#
```

在接口 gi0/1 和 gi0/1 上启用 Web 认证功能：

```
Ruijie# configure terminal
Ruijie(config)# interface gi0/1
Ruijie(config-if)# loop-detection
Ruijie(config-if)#
```

将时间间隔设置为 20 秒：

```
Ruijie# configure terminal
Ruijie(config)# loop-detection interval 20
Ruijie(config)#
```

启用 VLAN 100 至 200 的环路检测:

```
Ruijie# configure terminal
Ruijie(config)# loop-detection vlan 100-200
Ruijie(config)#
```

显示当前环路检测设置和状态:

```
Ruijie# show loop-detection

Loop Detection :Enabled Detection Mode : vlan-based LBD enabled VLAN : all VLANs Interval
:20 seconds

Interface      Result  Time Left(sec)
-----
gi0/1  Normal  -
gi0/8  Normal  - gi0/6 Loop on VLAN 2      120
Loop on VLAN 3  115
...
Po1     Loop    50
Po2     Normal  -

Ruijie#
```

显示端口 1/0/1 的环回检测状态:

```
Ruijie# show loop-detection interface gi0/1

Interface      Result  Time Left(sec)
-----
gi0/1  Normal  -

Ruijie#
```

显示聚合通道 2 的环回检测状态:

```
Ruijie# show loop-detection interface port-channel2

Interface      Result  Time Left(sec)
-----
Po2     Normal  -

Ruijie#
```

9 流量分割命令

9.1 traffic-segmentation

命令	作用
<code>show traffic-segmentation forward [interface INTERFACE-ID [,]-]</code>	此命令用于显示指定端口或所有端口上的流量分割。
<code>traffic-segmentation forward interface INTERFACE-ID [,]-]</code>	此命令用于限制已配置的端口接收有二层数据报转发域的数据报。
<code>no traffic-segmentation forward interface INTERFACE-ID [,]-]</code>	使用此命令删除转发域的规格。

显示 gi0/1 的流量分割配置:

```
Ruijie# show traffic-segmentation forward interface gi0/1

Interface      Forwarding Domain
-----
Total Entries:0

Ruijie#
```

配置流量分割, 它限制 gi0/1 到一组端口 (gi0/1 到 gi0/6) 的转发域:

```
Ruijie# configure terminal
Ruijie(config)# interface gi0/1
Ruijie(config-if)# traffic-segmentation forward interface range gi0/1-6
Ruijie(config-if)#
```



配置指南-ACL&QoS

本分册介绍系统配置配置指南相关内容，包括以下章节：

1. 访问控制列表
2. IP QoS

1 访问控制列表

1.1 概述

访问控制列表(Access Control Lists), 也称为接入列表 (Access Lists), 俗称为防火墙, 在有的文档中还称之为包过滤。ACLs 通过定义一些规则对网络设备接口上的数据报文进行控制: 允许通过或丢弃。按照其使用的范围, 可以分为安全 ACLs 和 QoS ACLs。

对数据流进行过滤可以限制网络中的通讯数据的类型, 限制网络的使用者或使用的设备。安全 ACLs 在数据流通过网络设备时对其进行分类过滤, 并对从指定接口输入或者输出的数据流进行检查, 根据匹配条件 (Conditions) 决定是允许其通过 (Permit) 还是丢弃 (Deny)。

总的来说, 安全 ACLs 用于控制哪些数据流允许从网络设备通过, QoS 策略对这些数据流进行优先级分类和处理。

ACLs 由一系列的表项组成, 我们称之为接入控制列表表项 (Access Control Entry: ACE)。每个接入控制列表表项都申明了满足此表项的匹配条件及行为。

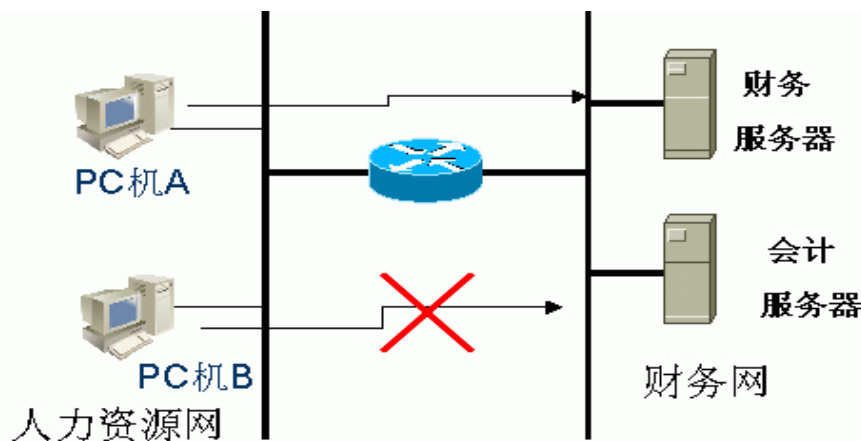
访问列表规则可以针对数据流的源地址、目标地址、上层协议, 时间区域等信息。

为什么要配置访问列表

配置访问列表的原因比较多, 主要有以下一些:

- 限制路由更新: 控制路由更新信息发往什么地方, 同时希望在什么地方收到路由更新信息。
- 限制网络访问: 为了确保网络安全, 通过定义规则, 可以限制用户访问一些服务 (如只需要访问 WWW 和电子邮件服务, 其他服务如 TELNET 则禁止), 或者仅允许在给定的时间段内访问, 或只允许一些主机访问网络等等。


下图是一个案例, 在此案例中, 只允许主机 A 访问财务网络, 而主机 B 禁止访问。如下图所示。



1.1.1.1.1.1.1 使用访问列表控制网络访问

什么时候配置访问列表

您可以根据需要选择基本访问列表或动态访问列表。一般情况下, 使用基本访问列表已经能够满足安全需要。但经验丰富的黑客可能会通过一些软件假冒源地址欺骗设备, 得以访问网络。而动态访问列表在用户访问网络以前, 要求通过身份认证, 使黑客难以攻入网络, 所以在一些敏感的区域可以使用动态访问列表保证网络安全。

 通过假冒源地址欺骗设备即电子欺骗是所有访问列表固有的问题, 使用动态列表也会遭遇电子欺骗问题: 黑客可能在用户通过身份认证的有效访问期间, 假冒用户的地址访问网络。解决这个问题的方法有两种, 一种是尽量将用户访问的

空闲时间设置小些，这样可以使黑客更难以攻入网络，另一种是使用 IPSEC 加密协议对网络数据进行加密，确保进入设备时，所有的数据都是加密的。

访问列表一般配置在以下位置的网络设备上：

- 内部网和外部网（如 INTERNET）之间的设备
- 网络两个部分交界的设备
- 接入控制端口的设备

访问控制列表语句的执行必须严格按照表中语句的顺序，从第一条语句开始比较，一旦一个数据包的报头跟表中的某个条件判断语句相匹配，那么后面的语句就将被忽略，不再进行检查。

1.2 ACL 硬件计数器

命令	作用
<code>acl-hardware-counter {access-group {ACCESS-LIST-NAME ACCESS-LIST-NUMBER} vlan-filter ACCESS-MAP-NAME}</code>	此命令用于启用指定访问列表名的 ACL 硬件计数器，用于访问 VLAN 过滤功能的组函数或映射。
<code>no acl-hardware-counter {access-group {ACCESS-LIST-NAME ACCESS-LIST-NUMBER} vlan-filter ACCESS-MAP-NAME}</code>	此命令禁止 ACL 硬件计数器功能。
<code>clear acl-hardware-counter {access-group [ACCESS-LIST-NAME ACCESS-LIST-NUMBER] vlan-filter [ACCESS-MAP-NAME]}</code>	此命令用于清除 ACL 硬件计数器。如果没有通过参数 <code>access-group</code> 指定访问列表的名称或编号，所有访问组的硬件计数器将被清除。如果没有通过参数 <code>vlan-filter</code> 指定访问映射的名称或编号，所有 VLAN 过滤器的硬件计数器将被清除。

启用 ACL 硬件计数器：

```
Ruijie# configure terminal
Ruijie(config)# acl-hardware-counter access-group abc
Ruijie(config)#
```

清除 ACL 硬件计数器：

```
Ruijie(config)# clear acl-hardware-counter access-group abc
Ruijie#
```

1.3 Action

此命令用于配置转发、丢弃，或在 VLAN 访问映射的子映射配置模式下重定向子映射的动作。使用 `no` 命令重置默认动作。

一个子映射只能有一个动作。新的动作配置会覆盖前一个动作。一个 VLAN 的访问映射可以包含多个子映射。匹配的子映射（由相关的访问列表允许的数据报）的数据报将采用子映射中指定的动作。没有进一步的检查，则完成了下一个子映射。如果数据报和子映射不匹配，那么下一个子映射将被检查。

命令	作用
<code>action {forward drop redirect INTERFACE-ID}</code>	此命令用于配置转发、丢弃，或在 VLAN 访问映射的子映射配置模式下重定向子映射的动作。
<code>no action</code>	此命令重置默认动作。

在子映射中配置动作：

```
Ruijie# show vlan access-map
VLAN access-map vlan-map 20
```

```

match mac address: ext_mac(ID:6856)
action: forward
Ruijie# configure terminal
Ruijie(config)# vlan access-map vlan-map 20
Ruijie(config-access-map)# action redirect gi0/5
Ruijie(config-access-map)# end
Ruijie# show vlan access-map
VLAN access-map vlan-map 20
match mac address: ext_mac(ID:6856)
action: redirect gi0/5
Ruijie#

```

1.4 备注

要添加或删除备注，在访问配置列表模式下执行以下命令：

命令	作用
list-remark TEXT	此命令用于为指定的 ACL 添加备注，可用于 MAC，IP，IPv6 和专家级访问列表配置模式。
no list-remark	此命令可删除备注。

为访问列表添加备注：

```

Ruijie# configure terminal
Ruijie(config)# ip extended access-list R&D
Ruijie(config-ip-ext-acl)# list-remark This access-list is used to match any IP
packets from the host 10.2.2.1.
Ruijie(config-ip-ext-acl)# end
Ruijie# show access-list ip

Extended IP access list R&D(ID:3999)
10 permit host 10.2.2.1 any
This access-list is used to match any IP packets from the host 10.2.2.1.

Ruijie#

```

1.5 允许或拒绝条目

此命令用于添加一个允许或拒绝条目。使用 no 命令，可清除条目。如果创建了一个无序列号的规则条目，将自动分配一个序列号。如果它是第一个条目，则分配的序列号为 10。随后的规则条目分配到的序列号将比该访问列表中的最大序列号大 10，并且将被置于列表末尾。

用户可使用该命令访问列表序列来更改指定访问列表的起始序列号和增量值。在应用该命令后，将为无指定序列号的新规则分配一个指定访问列表重基于序列的新序列设置。

当手动分配序列号时，最好为之后序列号更低的条目预留间隔。否则，需要花费额外时间插入序列号更低的条目。

该序列号必须为访问列表的域中唯一的号。如果您输入了一个已存在的序列号，将显示错误消息。

命令	作用
Extended Expert ACL: [SEQUENCE-NUMBER] {permit deny} PROTOCOL {SRC-IP-ADDR SRC-IP-WILDCARD host SRC-IP-ADDR any} {SRC-MAC-ADDR SRC-MAC-WILDCARD host SRC-MAC-ADDR any} {DST-IP-ADDR DST-IP-WILDCARD host DST- IP-ADDR	此命令用于添加一个允许或拒绝条目。如果创建了一个无序列号的规则条目，将自动分配一个序列号。如果它是第一个条目，则分配的序列号为 10。随后的规则条目分配到的序列号将比此访问列表中的最大序列号大 10，并且将被置于列表末尾。 用户可使用此命令访问列表序列来更改指定访问列表的起始序列号和增量值。在应用此命令后，将为无指定序列号的新规则分配一个指定访问列表重基于序列的新序列设置。 当手动分配序列号时，最好为之后序列号更低的条目预留间隔。否则，需要花

<pre>any} {DST-MAC-ADDR DST-MAC- WILDCARD host DST-MAC-ADDR any} [cos OUTER-COS] [vlan OUTER- VLAN] [[precedence PRECEDENCE] [tos TOS] dscp DSCP] [time-range PROFILE-NAME] [SEQUENCE-NUMBER] {permit deny} tcp {SRC-IP-ADDR SRC-IP- WILDCARD host SRC-IP-ADDR any} {SRC-MAC- ADDR SRC-MAC-WILDCARD host SRC-MAC-ADDR any} [{eq lt gt neq} PORT range MIN-PORT MAX- PORT] {DST-IP-ADDR DST-IP-WILDCARD host DST-IP-ADDR any} {DST-MAC- ADDR DST-MAC-WILDCARD host DST- MAC-ADDR any} [{eq lt gt neq} PORT range MIN-PORT MAX-PORT] [TCP-FLAG] [cos OUTER-COS] [vlan OUTER-VLAN] [[precedence PRECEDENCE] [tos TOS] dscp DSCP] [time-range PROFILE-NAME] [SEQUENCE-NUMBER] {permit deny} udp {SRC-IP-ADDR SRC-IP- WILDCARD host SRC-IP-ADDR any} {SRC-MAC- ADDR SRC-MAC-WILDCARD host SRC-MAC-ADDR any} [{eq lt gt neq} PORT range MIN-PORT MAX- PORT] {DST-IP-ADDR DST-IP-WILDCARD host DST-IP-ADDR any} {DST-MAC- ADDR DST-MAC-WILDCARD host DST- MAC-ADDR any} [{eq lt gt neq} PORT range MIN-PORT MAX-PORT] [cos OUTER-COS] [vlan OUTER- VLAN] [[precedence PRECEDENCE] [tos TOS] dscp DSCP] [time-range PROFILE-NAME] [SEQUENCE-NUMBER] {permit deny} icmp {SRC-IP-ADDR SRC-IP- WILDCARD host SRC-IP-ADDR any} {SRC- MAC-ADDR SRC-MAC- WILDCARD host SRC-MAC-ADDR any} {DST-IP-ADDR DST-IP- WILDCARD host DST-IP- ADDR any} {DST-MAC-ADDR DST-MAC- WILDCARD host DST-MAC-ADDR any} [ICMP-TYPE [ICMP-CODE] ICMP- MESSAGE] [cos OUTER-COS] [vlan OUTER-VLAN] [[precedence PRECEDENCE] [tos TOS] dscp DSCP] [time-range PROFILE-NAME]</pre>	<p>费额外时间插入序列号更低的条目。 此序列号必须为访问列表的域中唯一的号。如果您输入了一个已存在的序列号，将显示错误消息。</p>
<pre>no SEQUENCE-NUMBER</pre>	<p>此命令可清除条目。</p>
<pre>Extended Access List: [SEQUENCE-NUMBER] {permit deny} tcp {any host SRC-IP-ADDR SRC-IP-ADDR SRC-IP-WILDCARD} [{eq lt gt neq} PORT range MIN-PORT MAX- PORT] {any host DST-IP-ADDR DST-IP-ADDR DST-IP-WILDCARD} [{eq lt gt neq} PORT range MIN-PORT</pre>	<p>此命令用于添加一个允许或拒绝条目。如果创建了一个无序列号的规则条目，将自动分配一个序列号。如果它是第一个条目，则分配的序列号为 10。随后的规则条目分配到的序列号将比此访问列表中的最大序列号大 10，并且将被置于列表末尾。 用户可使用此命令访问列表序列来更改指定访问列表的起始序列号和增量值。在应用此命令后，将为无指定序列号的新规则分配一个指定访问列表重基于序列的新序列设置。 当手动分配序列号时，最好为之后序列号更低的条目预留间隔。否则，需要花</p>

<pre> MAX-PORT] [TCP-FLAG] [[precedence PRECEDENCE] [tos TOS] dscp DSCP] [time-range PROFILE-NAME] [SEQUENCE-NUMBER] {permit deny} udp {any host SRC-IP-ADDR SRC-IP-ADDR SRC-IP-WILDCARD} [{eq lt gt neq} PORT range MIN- PORT MAX-PORT] {any host DST- IP-ADDR DST-IP-ADDR DST-IP- WILDCARD} [{eq lt gt neq} PORT range MIN-PORT MAX-PORT] [[precedence PRECEDENCE] [tos TOS] dscp DSCP] [time-range PROFILE-NAME] [SEQUENCE-NUMBER] {permit deny} icmp {any host SRC-IP-ADDR SRC-IP-ADDR SRC-IP-WILDCARD} {any host DST-IP-ADDR DST-IP- ADDR DST-IP-WILDCARD} [ICMP- TYPE [ICMP-CODE] ICMP- MESSAGE] [[precedence PRECEDENCE] [tos TOS] dscp DSCP] [time-range PROFILE-NAME] [SEQUENCE-NUMBER] {permit deny} {gre esp eigrp igmp ipinip ospf pcp pim vrrp protocol-id PROTOCOL-ID} {any host SRC-IP- ADDR SRC-IP-ADDR SRC-IP- WILDCARD} {any host DST-IP-ADDR DST-IP- ADDR DST-IP-WILDCARD} [fragments] [[precedence PRECEDENCE] [tos TOS] dscp DSCP] [time-range PROFILE- NAME] [SEQUENCE-NUMBER] {permit deny} {any host SRC-IP-ADDR SRC-IP-ADDR SRC-IP-WILDCARD} [any host DST-IP-ADDR DST-IP- ADDR DST-IP-WILDCARD] [fragments] [[precedence PRECEDENCE] [tos TOS] dscp DSCP] [time-range PROFILE-NAME] Standard IP Access List: [SEQUENCE-NUMBER] {permit deny} {any host SRC-IP-ADDR SRC-IP-ADDR SRC-IP-WILDCARD} [any host DST-IP-ADDR DST-IP-ADDR DST- IP-WILDCARD] [time-range PROFILE- NAME] </pre>	<p>费额外时间插入序列号更低的条目。</p> <p>此序列号必须为访问列表的域中唯一的号。如果您输入了一个已存在的序列号，将显示错误消息。</p> <p>要为 IP 标准访问列表创建一个匹配规则，只需指定源 IP 地址或目的 IP 地址字段。</p>
<pre>no SEQUENCE-NUMBER</pre>	<p>此命令可移除一个条目。</p>
<pre> Extended IPv6 Access List: [SEQUENCE-NUMBER] {permit deny} tcp {any host SRC-IPV6-ADDR SRC-IPV6-ADDR/PREFIX-LENGTH} [{eq lt gt neq} PORT range MIN- PORT MAX-PORT] {any host DST- IPV6-ADDR DST-IPV6- ADDR/PREFIX-LENGTH} [{eq lt gt neq} PORT range MIN-PORT MAX-PORT] [TCP-FLAG] [dscp VALUE] [flow-label FLOW-LABEL] [time-range PROFILE-NAME] [SEQUENCE-NUMBER] {permit deny} udp {any host SRC-IPV6- </pre>	<p>此命令用于添加一个允许条目或拒绝条目到 IPv6 访问列表。如果创建了一个无序序列号的规则条目，将自动分配一个序列号。如果它是第一个条目，则分配的序列号为 10。随后的规则条目分配到的序列号将比此访问列表中的最大序列号大 10，并且将被置于列表末尾。</p> <p>用户可使用此命令访问列表序列来更改指定访问列表的起始序列号和增量值。在应用此命令后，将为无指定序列号的新规则分配一个指定访问列表重基于序列的新序列设置。</p> <p>当手动分配序列号时，最好为之后序列号更低的条目预留间隔。否则，需要花费额外时间插入序列号更低的条目。</p> <p>此序列号必须为访问列表的域中唯一的号。如果您输入了一个已存在的序列号，将显示错误消息。</p>

<pre> ADDR SRC-IPV6-ADDR/PREFIX-LENGTH} {{eq lt gt neq} PORT range MIN-PORT MAX-PORT} {any host DST-IPV6- ADDR DST-IPV6-ADDR/PREFIX- LENGTH} {{eq lt gt neq} PORT range MIN-PORT MAX-PORT} [dscp VALUE] [flow-label FLOW-LABEL] [time-range PROFILE- NAME] [SEQUENCE-NUMBER] {permit deny} icmp {any host SRC-IPV6- ADDR SRC-IPV6-ADDR/PREFIX- LENGTH} {any host DST-IPV6-ADDR DST-IPV6-ADDR/PREFIX-LENGTH} [ICMP-TYPE [ICMP-CODE] ICMP- MESSAGE] [dscp VALUE] [flow-label FLOW-LABEL] [time-range PROFILE-NAME] [SEQUENCE-NUMBER] {permit deny} {esp pcp sctp protocol-id PROTOCOL-ID} {any host SRC- IPV6-ADDR SRC-IPV6-ADDR/PREFIX-LENGTH} {any host DST-IPV6-ADDR DST- IPV6-ADDR/PREFIX-LENGTH} [fragments] [dscp VALUE] [flow-label FLOW- LABEL] [time-range PROFILE-NAME] [SEQUENCE-NUMBER] {permit deny} {any host SRC-IPV6-ADDR SRC-IPV6-ADDR/PREFIX-LENGTH} {any host DST-IPV6-ADDR DST- IPV6-ADDR/PREFIX-LENGTH} [fragments] [dscp VALUE] [flow-label FLOW-LABEL] [time-range PROFILE- NAME] Standard IPv6 Access List: [SEQUENCE-NUMBER] {permit deny} {any host SRC-IPV6-ADDR SRC-IPV6-ADDR/PREFIX-LENGTH} {any host DST-IPV6-ADDR DST-IPV6- ADDR/PREFIX-LENGTH} [time-range PROFILE-NAME] </pre>	
no SEQUENCE-NUMBER	此命令可从 IPv6 访问列表中清除一个条目。
<pre> [SEQUENCE-NUMBER] {permit deny} {any host SRC-MAC-ADDR SRC-MAC-ADDR SRC-MAC- WILDCARD} {any host DST-MAC- ADDR DST-MAC-ADDR DST-MAC- WILDCARD} [ethernet-type TYPE MASK [cos VALUE] [vlan VLAN- ID] [time-range PROFILE-NAME] </pre>	此命令用于为将被允许或拒绝的数据包定义规则。
no SEQUENCE-NUMBER	此命令移除条目“如果创建了一个无序列号的规则条目，将自动分配一个序列号”。

使用扩展专家级 ACL。其目的是通过源 IP 地址 192.168.4.12 和源 MAC 地址 00:13:00:49:82:72 来拒绝所有的 TCP 数据包创建一个 MAC 地址为 00-00-00-00-00-01，授权 VLAN 的名称为 default 的本地数据库：

```

Ruijie# configure terminal
Ruijie(config)# expert access-list extended exp_acl
Ruijie(config-exp-nacl)# deny tcp host 192.168.4.12 host 0013.0049.8272 any any

```

```
Ruijie(config-exp-nacl)# end
Ruijie# show access-lists
Extended Expert access list exp_acl(ID:9999)
10 deny tcp host 192.168.4.12 host 0013.0049.8272 any any
Ruijie#
```

为名为 **Strict-Control** 的 IP 扩展访问列表创建四个条目。这些条目分别为：允许 TCP 数据包发送到网络 10.20.0.0，允许 TCP 数据包发送到网络 10.100.1.2，允许所有数据包发送到目的 TCP 端口 80 和允许所有的 ICMP 数据包：

```
Ruijie# configure terminal
Ruijie(config)# ip extended access-list Strict-Control
Ruijie(config-ip-ext-acl)# permit tcp any 10.20.0.0 0.0.255.255
Ruijie(config-ip-ext-acl)# permit tcp any host 10.100.1.2
Ruijie(config-ip-ext-acl)# permit tcp any any eq 80
Ruijie(config-ip-ext-acl)# permit icmp any any
Ruijie(config-ip-ext-acl)#
```

为名为 **std-ip** 的 IP 标准访问列表创建两个条目。这两个条目分别为：允许 IP 数据包发送到网络 10.20.0.0，允许 IP 数据包发送到网络 10.100.1.2：

```
Ruijie# configure terminal
Ruijie(config)# ip access-list std-acl
Ruijie(config-ip-acl)# permit any 10.20.0.0 0.0.255.255
Ruijie(config-ip-acl)# permit any host 10.100.1.2
Ruijie(config-ip-acl)#
```

为名为 **ipv6-control** 的 IPv6 扩展访问列表创建四个条目。这些条目分别为：允许 TCP 数据包发送到网络 ff02::0:2/16，允许 TCP 数据包发送到网络 ff02::1:2，允许所有数据包发送到端口 80 和允许所有的 ICMP 数据包：

```
Ruijie# configure terminal
Ruijie(config)# ipv6 access-list extended ipv6-control
Ruijie(config-ipv6-ext-acl)# permit tcp any ff02::0:2/16
Ruijie(config-ipv6-ext-acl)# permit tcp any host ff02::1:2
Ruijie(config-ipv6-ext-acl)# permit tcp any any eq 80
Ruijie(config-ipv6-ext-acl)# permit icmp any any Ruijie(config-ipv6-ext-acl)#
```

为名为 **ipv6-std-control** 的 IPv6 标准访问列表创建两个条目。这两个条目分别为：允许 IP 数据包发送到网络 ff02::0:2/16，允许 IP 数据包发送到网络 ff02::1:2：

```
Ruijie# configure terminal
Ruijie(config)# ipv6 access-list ipv6-std-control
Ruijie(config-ipv6-acl)# permit any ff02::0:2/16
Ruijie(config-ipv6-acl)# permit any host ff02::1:2
Ruijie(config-ipv6-acl)#
```

在配置文件 **daily-profile** 中配置 MAC 访问条目，以允许两组源 MAC 地址：

```
Ruijie# configure terminal
Ruijie(config)# mac access-list extended daily-profile
Ruijie(config-mac-ext-acl)# permit 00:80:33:00:00:00 00:00:00:ff:ff:ff any
Ruijie(config-mac-ext-acl)# permit 00:f4:57:00:00:00 00:00:00:ff:ff:ff any
Ruijie(config-mac-ext-acl)#
```

1.6 VLAN

命令	作用
show vlan access-map [MAP-NAME]	此命令用于显示 VLAN 访问映射配置信息。如果指定了访问映射名称，将显示所有的 VLAN 访问映射信息。如果用户为访问映射启用了 ACL 硬件计数器，则将基于各子映射显示此计数器。
show vlan filter [access-map MAP-NAME vlan VLAN-ID]	此命令用于显示 VLAN 接口的 VLAN 过滤配置。命令“show vlan filter access-map”用于显示按访问映射过滤的 VLAN 过滤信息。命令“show vlan filter vlan”用于显示按 VLAN 过滤的 VLAN 过滤信息。
vlan access-map MAP-NAME [SEQUENCE-NUM]	此命令用于创建一个 VLAN 访问映射的子映射，并输入此子映射的配置模式。
no vlan access-map MAP-NAME [SEQUENCE-NUM]	此命令可删除访问映射或其子映射。

vlan filter MAP-NAME vlan-list VLAN-ID-LIST	此命令用于在 VLAN 中应用一个 VLAN 访问映射。一个 VLAN 只能关联一个 VLAN 访问映射。
no vlan filter MAP-NAME vlan-list VLAN-ID-LIST	此命令可从 VLAN 中清除 VLAN 访问映射。

显示 VLAN 访问映射:

```
Ruijie# show vlan access-map

VLAN access-map vlan-map 10
match ip access list: stp_ip1(ID:1888)
action: forward
VLAN access-map vlan-map 20
match mac access list:      ext_mac(ID:6995)
action: redirect          gi0/5

Ruijie#
```

在启用了硬件计数器的情况下如何显示 VLAN 访问映射的内容:

```
Ruijie# show vlan access-map

VLAN access-map vlan-map 10
match ip access list: stp_ip1(ID:1888)
action: forward
Counter enable on VLAN(s):1-2
match count:8541 packets
VLAN access-map vlan-map 20
match mac access list:      ext_mac(ID:6995)
action: redirect          gi0/5
Counter enable on VLAN(s):1-2
match count:5647 packets

Ruijie#
```

显示 VLAN 过滤信息:

```
Ruijie# show vlan filter

VLAN Map aa
Configured on VLANs:5-127,221-333
VLAN Map bb
Configured on VLANs:1111-1222

Ruijie#

Ruijie# show vlan filter vlan 5

VLAN ID 5
VLAN Access Map: aa

Ruijie#
```

创建 VLAN 访问映射:

```
Ruijie# configure terminal
Ruijie(config)# vlan access-map vlan-map 20
Ruijie(config-access-map)#
```

在 VLAN 5 中应用 VLAN 访问映射 vlan-map:

```
Ruijie# configure terminal
Ruijie(config)# vlan filter vlan-map vlan-list 5
Ruijie(config-access-map)# end
Ruijie# show vlan filter

VLAN Map vlan-map Configured on VLANs:5

Ruijie#
```

2 IP QoS

2.1 概述

随着 Internet 的飞速发展，人们对于在 Internet 上传输多媒体流的需求越来越大，一般说来，用户对不同的多媒体应用有着不同的服务质量要求，这就要求网络应根据用户的要求分配和调度资源，因此，传统所采用的“尽力而为”转发机制，已经不能满足用户的要求。QoS 应运而生。

QoS (Quality of Service, 服务质量) 是用来评估服务方满足客户需求的能力。在因特网中，为了提高网络服务质量，引入 QoS 机制，用 QoS 评估网络投递分组的能力。我们通常所说的 QoS，是对分组投递过程中为延迟、抖动、丢包等核心需求提供支持的服务能力的评估。

QoS 基础框架

不支持 QoS 功能的设备不具有提供传输品质服务的能力，它同等对待所有的交通数据流，并不保证某一特殊的数据流会受到特殊的转发待遇。当网络带宽充裕的时候，所有的数据流都得到了较好的处理，而当网络拥塞发生的时候，所有的数据流都有可能被丢弃。这种转发策略被称做提供最佳效果服务，因为这时设备是尽最大能力转发数据，设备本身的交换带宽得到了充分的利用。

本设备支持 QoS 功能，能够提供传输品质服务。针对某种类别的数据流，您可以为它赋予某个级别的传输优先级，来标识它的相对重要性，并使用设备所提供的各种优先级转发策略、拥塞避免等机制为这些数据流提供特殊的传输服务。配置了 QoS 的网络环境，增加了网络的性能可预知性，并能够有效地分配网络带宽，更加合理地利用网络资源。

本设备的 QoS 实符合 IEEE 802.1p 标准并能应用到 IETF (Internet Engineering Task Force) 的 DiffServ (Differentiated Service Mode)，差分服务模型体系中。在支持 QoS 的网络中传输的每一个报文将被划分成不同的 QoS 类别，在报文中包含了相应的分类信息。一般地，附带在报文中的分类信息有：

- 携带在 802.1Q 帧头的 Tag Control Information 中的前 3 个比特，它包含了 8 个类别的优先级信息，通常称为 802.1p Priority。
- 携带在 IPv4 报文头中的 TOS 或者 IPv6 报文头中的 Traffic Class 字段的前 3 个比特，称作 IPprecedence value；或者携带在 IPv4 报文头中的 TOS 或者 IPv6 报文头中的 Traffic Class 字段的前 6 个比特，称作 Differentiated Services Code Point (DSCP) value。

在遵循 DiffServ 体系的网络中，各设备对包含相同分类信息的报文采取相同的传输服务策略，对包含不同分类信息的报文采取不同的传输服务策略。报文的分类信息可以由网络上的主机、设备或其它网络设备赋予。可以基于不同的应用策略或者基于报文内容的不同为报文赋予类别信息。识别报文的内容以便为报文赋予类别信息的做法往往需要消耗网络设备的大量处理资源，为了减少骨干网络的处理开销，一般这种赋予类别信息的方式都使用在网络边界。设备根据报文所携带的类别信息，为各种交通流提供不同的传输优先级，或者为某种交通流预留带宽，或者适当地丢弃一些优先级较低的报文、或者采取其他一些操作等等。这些独立设备的这种行为在 DiffServ 体系中被称作每跳行为 (Per-hop Behavior)。

如果网络上的所有设备提供了一致的每跳行为，那么对于 DiffServ 体系来说，这个网络就可以构成 End-to-end QoS solution。


QoS 处理流程

Classifying


Classifying 即分类，其过程是根据信任策略或者根据分析每个报文的内容来确定将这些报文归类到以 CoS 值来表示的各个数据流中，因此分类动作的核心任务是确定输入报文的 CoS 值。分类发生在端口接收输入报文阶段。

对于一般非 IP 报文，设备将根据以下准则来归类报文：

- 如果报文本身不包含 QoS 信息，即报文的第二层报文头中不包含 802.1p Priority，那么可以根据报文输入端口的缺省 Priority 值来获得报文的 QoS 信息。端口的缺省 Priority 值和报文的 802.1p Priority 一样，取值范围为 0~7。
- 如果报文本身包含 QoS 信息，报文的第二层报文头中包含 802.1p Priority，那么可以直接从报文中获得 CoS 值。

 以上两种归类准则只有当端口的 DSCP 信任模式关闭，也就是端口工作在 CoS 信任模式下的时候才起作用。端口工作在 QoS 信任模式下意味着不通过分析报文的内容，而直接从报文中或报文的输入端口上获得报文 QoS 信息。

如果端口使用了 ACLs 归类，那么在此端口上，将通过提取报文相应字段匹配关联的 ACLs，以确定报文的 802.1p Priority 值。要注意的是，如果端口使用了 ACLs，但又没有为其设置相应的 802.1p Priority 值，则设备将按照缺省行为为符合这种归类的报文分配优先级：即根据报文第二层报文头中包含的优先级信息或端口的缺省优先级。

 上面三种归类准则可能会同时作用于一个端口上。在这种情况下，上面三种归类准则按 3、2、1 的优先级起作用。即先根据 ACLs 归类，在归类失败的情况下，才有可能选择归类准则 2、1。

对于 IP 报文，可以根据以下准则来归类报文：

- 如果端口信任模式为 Trust DSCP，则根据 IP 报文的 DSCP 字段（6 个比特）通过 DSCP to 802.1p Priority Mapping 映射到输出报文的 CoS 字段（3 个比特）。
- 如果端口信任模式为 Trust cos，则按照一般非 IP 报文归类准则 1 和 2 处理。
- 如果端口使用了 ACLs 归类，那么在此端口上，将通过提取报文的相应字段来匹配相关联的 ACLs，以确定报文的 DSCP 值。要注意的是，如果端口使用了 ACLs，但又没有为其设置相应的 DSCP 值，则设备将按照前面的规则 1、2 确定优先级。

和非 IP 报文归类准则一样，以上几种归类准则同样可以同时作用于一个端口上。在这种情况下，上面的归类准则按照 3、2、1 的优先级起作用。

Metering

Metering, 发生在数据流分类完成后, 用于约束被分类的数据流所占用的传输带宽。Metering 动作检查被归类的数据流中的每一个报文, 如果此报文超出了作用于此数据流所允许的限制带宽, 那么此报文将会被做特殊处理, 它或者要被丢弃, 或者要被赋予另外的 DSCP 值。

在 QoS 处理流程中, Metering 动作是可选的。

Marking

Marking 即标识, 经过 Classifying 和 Metering 动作处理之后, 为了确保被分类报文的 QoS 信息能够传递给网络上的下一跳设备, 需要通过 Marking 动作将为报文写入 QoS 信息, 此动作可以通过 ACLs 完成。

Queueing

Queueing 即队列, 负责将数据流中报文送往端口的某个输出队列中, 送往端口的不同输出队列的报文将获得不同等级和性质的传输服务策略。

每一个端口上都拥有 8 个输出队列, 通过设备上配置的 Priority-to-Queue 映射表来将报文的 802.1p Priority 值转化成输出队列号, 以便确定报文应此被送往的输出队列。

Scheduling

Scheduling 即调度, 为 QoS 流程的最后一个环节。当报文被送到端口的不同输出队列上之后, 设备将采用 WRR 或者严格优先级调度算法发送 8 个队列中的报文。

对于 WRR 调度算法, 可以通过设置权重值来配置各个输出队列在输出报文的时候所占用的每循环发送报文个数, 从而影响传输带宽。

严格优先级调度算法按照输出队列优先级从高到低 (7~0) 发送报文, 只有高优先级队列的报文全部发送完毕才会对下一队列中的报文进行发送。

2.2 class

命令	作用
class NAME	此命令用于指定将与流量策略相关联的类映射的名称, 然后进入策略映射类配置模式。如果指定的类映射名称不存在, 则不会有流量被归类到此类别。
no class NAME	此命令可移除指定类的策略定义。
class-map NAME	此命令用于创建或修改一个用以定义数据包匹配标准的类映射。类映射命令将进入类映射配置模式, 在此模式下, 输入匹配的命令将定义此类别的标准。
no class-map NAME	此命令从交换机移除现有的类映射。
show class-map [NAME]	此命令用于显示所有类型的映射以及与它们相匹配的标准。

定义策略映射 policy1, 它用于定义类 “class-dscp-red” 的策略。与 SRC IP 192.168.1.193 匹配的数据包将被标记为 DSCP10, 并由单速率策略器进行监督:

```
Ruijie# configure terminal
Ruijie(config)# ip access-list extended ip
Ruijie(config-ip-acl)# permit host 192.168.1.193 any
Ruijie(config-ip-acl)# exit
Ruijie(config)# class-map class-dscp-red
Ruijie(config-cmap)# match access-group ip
Ruijie(config-cmap)# exit
Ruijie(config)# policy-map policy1
Ruijie(config-pmap)# class class-dscp-red
Ruijie(config-pmap-c)# set ip dscp 10
Ruijie(config-pmap-c)# police 1000000 2000 exceed-action set-dscp-transmit 0
Ruijie(config-pmap-c)#
```

配置 class_home_user 为类映射的名称。在此类映射中, 匹配说明用于指定: 与访问控制列表 “acl_home_user” 匹配的流量将包含于类映射 “class_home_user” 中。

```
Ruijie# configure terminal
Ruijie(config)# class-map class_home_user
Ruijie(config-cmap)# match access-group acl_home_user
Ruijie(config-cmap)#
```

显示类映射：与访问列表“acl_home_user”相匹配的数据包属于“c3”类：

```
Ruijie# show class-map

Class Map c3
Match access-group acl_home_user

Ruijie#
```

2.3 mls qos

命令	作用
mls qos cos COS-VALUE	此命令用于配置端口服务类别（CoS）的值。
no mls qos cos	此命令可恢复到默认值。
mls qos map dscp-cos DSCP-LIST to COS-VALUE	此命令用于定义一个从 DSCP 到 CoS 的映射。从 DSCP 到 CoS 的映射用于 DSCP 信任端口，以将 DSCP 值映射到内部 CoS 值。之后，此 CoS 值将依次被映射到基于 CoS 的 CoS 队列，然后到通过命令 priority-queue cos-map 配置的队列映射。
no mls qos map dscp-cos DSCP-LIST	此命令恢复默认设置。
mls qos scheduler {sp rr wrr wdr}	此命令用于配置调度机制。
no mls qos scheduler	此命令可重置调度机制到默认设置。
mls qos trust {cos dscp}	此命令用于配置端口的信任状态，以信任后续 QoS 操作中到站数据包的 CoS 字段和 DSCP 字段。
no mls qos trust	此命令恢复默认设置。
show mls qos interface INTERFACE-ID [, -] {cos scheduler trust rate-limit map dscp-cos}	此命令用于显示端口级别的 QoS 配置。
show mls qos queuing [interface INTERFACE-ID [, -]]	此命令用于显示 QoS 队列信息和指定接口上的不同调度算法的权重配置。

将以太网端口 1/0/1 的默认 CoS 设置为 3：

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/1
switch(config-if)# mls qos cos 3
switch(config-if)#
```

配置 DSCP 到 CoS 的映射，从而将 DSCP12,16 和 18 映射到 gi0/6 的 CoS 1：

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/6
Ruijie(config-if)# mls qos map dscp-cos 12,16,18 to 1
Ruijie(config-if)#
```

将队列调度算法配置为严格优先级模式：

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# mls qos scheduler sp
Ruijie(config-if)#
```

配置端口 gi0/1，以信任 DSCP 模式：

```
Ruijie# configure terminal
Ruijie(config)# interface gi0/1
Ruijie(config-if)# mls qos trust dscp
Ruijie(config-if)#
```


显示从 gigabitEthernet 0/2 到 0/5 的默认 CoS:

```
Ruijie# show mls qos interface gigabitEthernet 0/2-5 cos

Interface      CoS
-----
gi0/2         3
gi0/3         4
gi0/4         4
gi0/5         3

Ruijie#
```

显示从 gigabitEthernet0/2 到 0/5 的端口信任状态:

```
Ruijie# show mls qos interface gigabitEthernet 0/2-5 trust

Interface      Trust State
-----
gi0/2         trust DSCP
gi0/3         trust CoS
gi0/4         trust DSCP
gi0/5         trust CoS

Ruijie#
```

显示 gigabitEthernet0/1 到 0/2 的调度配置:

```
Ruijie# show mls qos interface gigabitEthernet 0/1-2 scheduler

Interface      Scheduler Method
-----
gi0/1         sp
gi0/2         wr

Ruijie#
```

显示添加到 gigabitEthernet0/1 到 0/2 的 DSCP 突变映射:

```
Ruijie# show mls qos interface gigabitEthernet 0/1-2 dscp-mutation

Interface      DSCP Mutation Map
-----
gi0/1         Mutate Map 1
gi0/2         Mutate Map 2

Ruijie#
```

显示端口 gigabitEthernet0/1 到 0/4 的带宽分配:

```
Ruijie# show mls qos interface gigabitEthernet 0/1-4 rate-limit

Interface      Rx Rate          Tx Rate          Rx Burst         Tx Burst
-----
gi0/1         1000 kbps        No Limit         64 kbyte         No Limit
gi0/2         No Limit         2000 kbps        No Limit         2000 kbyte
gi0/3         No Limit         No Limit         64 kbyte         64 kbyte
gi0/4         No Limit         2000 kbps        64 kbyte         64 kbyte

Ruijie#
```

显示端口 gigabitEthernet0/1 上的 DSCP 转换为 CoS 映射:

```
Ruijie# show mls qos interface gigabitEthernet 0/1 map dscp-cos

gi0/1
0      1      2      3      4      5      6      7      8      9
-----
00     00     00     00     00     00     00     00     01     01
10     01     01     01     01     01     01     02     02     02
20     02     02     02     02     03     03     03     03     03
30     03     03     04     04     04     04     04     04     04
40     05     05     05     05     05     05     05     05     06
50     06     06     06     06     06     06     07     07     07
```

```
60    07    07    07    07
Ruijie#
```

显示 QoS 的队列信息:

```
Ruijie# show mls qos queueing
CoS-queue map:
CoS    QID
---    ---
0      2
1      0
2      1
3      3
4      4
5      5
6      6
7      7
Ruijie#
```

显示接口 gigabitEthernet0/3 的不同调度的权重配置:

```
Ruijie# show mls qos queueing interface gigabitEthernet 0/3
wrr bandwidth weights:
QID    Weights
---    -
1      2
2      3
3      4
4      5
5      6
6      7
7      8

wrrr bandwidth weights:
QID    Quantum
---    -
1      2
2      3
3      4
4      5
5      6
6      7
7      8
Ruijie#
```

2.4 police

此命令用于将流量监管模式配置成单速率监管模式。使用 no 命令，可取消流量监管。

使用 police 命令，丢弃数据包，或者基于数据包的符合性级别为数据包标记不同的 QoS 值。

组合此命令中使用的参数，可定义该命令对应的动作。

流量类别的 set 命令所配置的动作将应用至属于该类别的所有数据包。

可在策略映射类配置模式下执行以下命令:

命令	作用
police KBPS BURST-NORMAL exceed-action ACTION	此命令用于将流量监管模式配置成单速率监管模式。

no police	此命令可取消流量监管。
-----------	-------------

定义流量类别，以及如何将策略与策略映射中流量类别的匹配标准相关联。之后，使用命令 `service-policy`，以将此服务策略附加到接口。在此特定实例中，流量监管配置为：对于接口 `gigabitEthernet 0/1` 的所有进站数据包，平均速率为 64 千比特/秒，正常突发值大小为 4 千字节：

```
Ruijie# configure terminal
Ruijie(config)# class-map access-match
Ruijie(config-cmap)# match access-group acl_rd
Ruijie(config-cmap)# exit
Ruijie(config)# policy-map police-setting
Ruijie(config-pmap)# class access-match
Ruijie(config-pmap-c)# police 64 4 exceed-action drop
Ruijie(config-pmap-c)# exit
Ruijie(config-pmap)# exit
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# service-policy input police-setting
Ruijie(config-if)#
```

2.5 Policy

可将以下命令应用于接口上：

命令	作用
<code>policy-map NAME</code>	此命令用于输入策略映射的配置模式，以及用于创建或修改作为服务策略被附加到一个或多个接口的策略映射。
<code>no policy-map NAME</code>	此命令可删除策略映射。
<code>service-policy input NAME</code>	此命令用于在输入接口上添加一个策略映射。
<code>no service-policy input</code>	此命令可从输入接口清除服务策略。
<code>show policy-map [POLICY-NAME interface INTERFACE-ID]</code>	此命令用于显示策略映射配置。使用 <code>show policy-map</code> 命令显示任意或所有现有的服务策略映射的等级策略配置。

创建一个名为 `policy` 的策略映射，以及如何在此策略映射内配置类策略。名为 `class1` 的类策略是指用于与访问控制列表（ACL）`acl_rd` 匹配的流量的策略。：

```
Ruijie# configure terminal
Ruijie(config)# class-map class1
Ruijie(config-cmap)# match access-group acl_rd
Ruijie(config-cmap)# exit
Ruijie(config)# policy-map policy
Ruijie(config-pmap)# class class1
Ruijie(config-pmap-c)# set ip dscp 46
Ruijie(config-pmap-c)# exit
```

定义策略映射：(1) `cust1-classes` 和 (2) `cust2-classes`。

对 `cust1-classes` 而言，配置与 `access group rd` 相匹配的金色并由保证速率为 800 Kbps 的单个速率监视器进行监察。对 `cust2-classes` 而言，配置与 `access group rd2` 相匹配的银色并由保证速率为 1600 Kbps 的单个速率监视器进行监察。配置 `cust1-classes` 策略映射，然后添加至接口 `0/1` 和 `0/2` 的进站流量：

```
Ruijie# configure terminal
Ruijie(config)# class-map gold
Ruijie(config-cmap)# match access-group acl_rd
Ruijie(config-cmap)# exit
Ruijie(config)# class-map silver
Ruijie(config-cmap)# match access-group acl_rd2
Ruijie(config-cmap)# exit
Ruijie(config)# policy-map cust1-classes
Ruijie(config-pmap)# class gold
Ruijie(config-pmap-c)# police 800 2000 exceed-action set-dscp-transmit 0
Ruijie(config-pmap-c)# exit
Ruijie(config-pmap)# class silver
Ruijie(config-pmap-c)# police 1600 2000 exceed-action set-dscp-transmit 0
Ruijie(config-pmap-c)# exit
Ruijie(config-pmap)# exit
```

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# service-policy input cust1-classes
Ruijie(config-if)# exit
Ruijie(config)# interface gigabitEthernet 0/2
Ruijie(config-if)# service-policy input cust1-classes
Ruijie(config-if)#
```

显示上述创建的称为 **cust1-classes** 的策略映射:

```
Ruijie# show policy-map cust1-classes

Policy Map cust1-classes
Class gold
  police 800 2000 exceed-action set-dscp-transmit 0
Class silver
  police 1600 2000 exceed-action set-dscp-transmit 0
Ruijie#
```

在端口 1/0/1 上显示所有的策略映射:

```
Ruijie# show policy-map interface gigabitEthernet 0/1

Policy Map: cust1-classes: input
Class gold
  police 800 2000 exceed-action set-dscp-transmit 0
Class silver
  police 1600 2000 exceed-action set-dscp-transmit 0

Ruijie#
```

2.6 priority-queue cos-map

此命令用于定义服务类别 (CoS) 为队列映射。使用 **no** 命令恢复默认设置。

当收到数据包时, 该数据包将获得一个内部 CoS。该内部 CoS 用于基于 CoS 到队列的映射选择发送队列。数值较高的 CoS 队列将获得更高的优先级。可在全局配置模式下执行以下命令:

命令	作用
priority-queue cos-map QUEUE-ID COS1 [COS2 [COS3 [COS4 [COS5 [COS6 [COS7 [COS8]]]]]]]	此命令用于定义服务类别 (CoS) 为队列映射。当收到数据包时, 此数据包将获得一个内部 CoS。此内部 CoS 用于基于 CoS 到队列的映射选择发送队列。数值较高的 CoS 队列将获得更高的优先级。
no priority-queue cos-map	此命令恢复默认设置。

为队列 2 分配 CoS 优先级 3,5 和 6:

```
Ruijie# configure terminal
Ruijie(config)# priority-queue cos-map 2 3 5 6
Ruijie(config)#
```

2.7 rate-limit

此命令用于设置接口接收带宽的上限值。指定的限制不能超过指定接口的最大速度。入站带宽限制, 当接收的流量超过限制, 入站时将发送暂停帧或流量控制帧。要在接口上设置发送带宽上限值, 请在接口配置模式下使用 **rate-limit output** 命令。使用 **no** 命令, 可禁用带宽限制。可在接口配置模式下执行以下命令:

命令	作用
rate-limit {input output} {NUMBER-KBPS } BURST-SIZE	此命令用于设置接口接收带宽的上限值。指定的限制不能超过指定接口的最大速度。入站带宽限制, 当接收的流量超过限制, 入站时将发送暂停帧或流量控

	制帧。要在接口上设置发送带宽上限值，请在接口配置模式下使用 <code>rate-limit output</code> 命令。
<code>no rate-limit {input output}</code>	此命令可禁用带宽限制。

在 `gi0/5` 上配置最大带宽限制。入站带宽限制为 2000Kbps，突发流量带宽限制为 4096K 字节：

```
Ruijie# configure terminal
Ruijie(config)# interface gi0/5
Ruijie(config-if)# rate-limit input 2000 4096
Ruijie(config-if)#
```

2.8 Set

此命令用于配置出站数据包的新优先字段、DSCP 字段和 CoS 字段。

`set ip dscp` 命令不会影响 CoS 的队列选择。对同一类而言，用户可使用 `police` 命令和 `set` 命令。

可在策略映射类配置模式下执行以下命令：

命令	作用
<code>set {ip dscp DSCP cos COS}</code>	此命令用于配置出站数据包的 DSCP 字段和 CoS 字段。
<code>no set {ip dscp DSCP cos COS}</code>	此命令取消配置。

使用策略为 `class1` 类配置策略映射 `policy1`。包含在 `class1` 类的数据包将被设置为 10 的 DSCP 并由保证速率为 1Mbps 的监察器进行监察：

```
Ruijie# configure terminal
Ruijie(config)# policy-map policy1
Ruijie(config-pmap)# class class1
Ruijie(config-pmap-c)# set ip dscp 10
Ruijie(config-pmap-c)# police 1000 2000 exceed-action set-dscp-transmit 10
Ruijie(config-pmap-c)# exit
Ruijie(config-pmap)#
```

2.9 带宽

可在接口配置模式下执行以下命令：

命令	作用
<code>wrr-queue bandwidth QUANTUM1...QUANTUM127</code>	此命令用于设置 WDRR 调度模式中的队列数量。当调度模式在 WDRR 模式中时，此命令的此配置将起作用。使用 <code>mls qos scheduler wrr</code> 命令，更改调度模式为 WDRR 模式。
<code>no wrr-queue bandwidth</code>	此命令恢复到默认设置。
<code>wrr-queue WEIGHT1...WEIGHT127</code>	此命令用于设置 WRR 调度模式中的队列权重。
<code>no wrr-queue bandwidth</code>	此命令恢复到默认设置。

配置 WDRR 调度模式的队列数量，接口 `gi0/1` 上的 `queue 0`、`queue 1`、`queue 2`、`queue 3`、`queue 4`、`queue 5`、`queue 6`、`queue 7` 的队列数量分别为 1、2、3、4、5、6、7、8：

```
Ruijie# configure terminal
Ruijie(config)# interface gi0/1
Ruijie(config-if)# mls qos scheduler wrr
Ruijie(config-if)# wrr-queue bandwidth 1 2 3 4 5 6 7 8
Ruijie(config-if)#
```

配置 WRR 调度模式的队列权重，接口 `gi0/1` 上的 `queue 0`、`queue 1`、`queue 2`、`queue 3`、`queue 4`、`queue 5`

、 queue 6、 queue 7 的队列权重分别为 1、 2、 3、 4、 5、 6、 7、 8:

```
Ruijie# configure terminal
Ruijie(config)# interface gi0/1
Ruijie(config-if)# mls qos scheduler wrr
Ruijie(config-if)# wrr-queue bandwidth 1 2 3 4 5 6 7 8
Ruijie(config-if)#
```



配置指南-网管和监控

本分册介绍系统配置配置指南相关内容，包括以下章节：

1. SNMP
2. RMON
3. Sntp
4. 时间范围

1 SNMP

1.1 SNMP 相关知识

概述

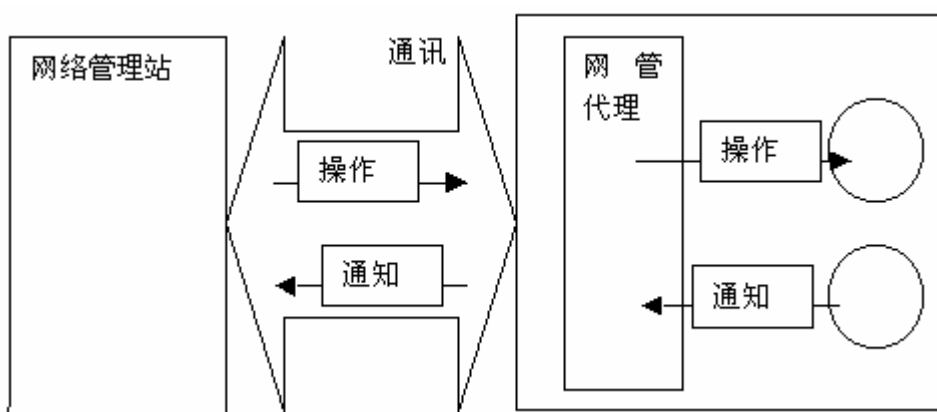
SNMP 是 Simple Network Management Protocol（简单网络管理协议）的缩写，在 1988 年 8 月就成为一个网络管理标准 RFC1157。到目前，因众多厂家对此协议的支持，SNMP 已成为事实上的网管标准，适合于在多厂家系统的互连环境中使用。利用 SNMP 协议，网络管理员可以对网络上的节点进行信息查询、网络配置、故障定位、容量规划，网络监控和管理是 SNMP 的基本功能。

SNMP 是一个应用层协议，为客户机/服务器模式，包括三个部分：

- SNMP 网络管理器
- SNMP 代理
- MIB 管理信息库
- SNMP 网络管理器，是采用 SNMP 来对网络进行控制和监控的系统，也称为 NMS（Network Management System）。
- SNMP 代理（SNMP Agent）是运行在被管理设备上的软件，负责接受、处理并且响应来自 NMS 的监控和控制报文，也可以主动发送一些消息报文给 NMS。

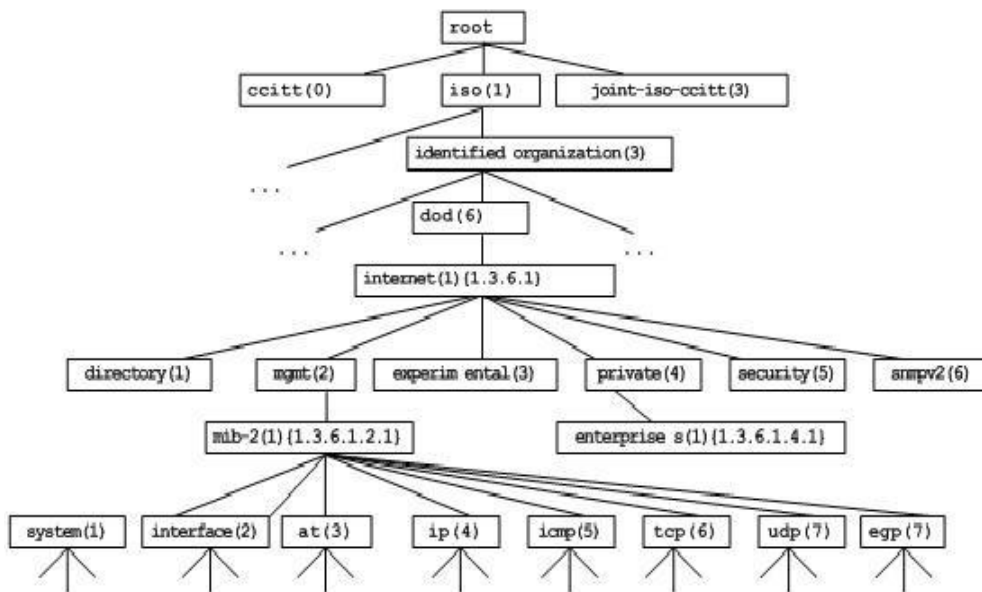
NMS 和 Agent 的关系可以用如下的图来表示：

网络管理站（NMS）与网管代理（Agent）的关系图



MIB（Management Information Base）是一个虚拟的网络管理信息库。被管理的网络设备中包含了大量的信息，为了能够在 SNMP 报文中唯一的标识某个特定的管理单元，MIB 采用树形层次结构来描述网络设备中的管理单元。树的节点表示某个特定的管理单元。如下图 MIB 对象命名树，为了唯一标识网络设备中的某个管理单元 System，可以采用一串的数字来表示，如{1.3.6.1.2.1.1}这一串数字即为管理单元的 Object Identifier（单元标识符），MIB 则是网络设备的单元标识符的集合。

MIB 树形层次结构



1.2 SNMP 协议版本

目前 SNMP 支持以下版本：

- SNMPv1：简单网络管理协议的第一个正式版本，在 RFC1157 中定义。
- SNMPv2C：基于共同体（Community-Based）的 SNMPv2 管理架构，在 RFC1901 中定义的一个实验性协议。
- SNMPv3：通过对数据进行鉴别和加密，提供了以下的安全特性：
 - 1) 确保数据在传输过程中不被篡改；
 - 2) 确保数据从合法的数据源发出；
 - 3) 加密报文，确保数据的机密性；

SNMPv1 和 SNMPv2C 都采用基于共同体（Community-based）的安全架构。通过定义主机地址以及认证名（Community String）来限定能够对代理的 MIB 进行操作的管理者。

SNMPv2C 增加了 Get-bulk 操作机制并且能够对管理工作站返回更加详细的错误信息类型。Get-bulk 操作能够一次性地获取表格中的所有信息或者获取大批量的

数据，从而减少请求-响应的次数。SNMPv2C 错误处理能力的提高包括扩充错误代码以区分不同类型的错误，而在 SNMPv1 中这些错误仅有一种错误代码。现在通过错误代码可以区分错误类型。由于网络上可能同时存在支持 SNMPv1 和 SNMPv2C 的管理工作站，因此 SNMP 代理必须能够识别 SNMPv1 和 SNMPv2C 报文，并且能返回相应版本的报文。

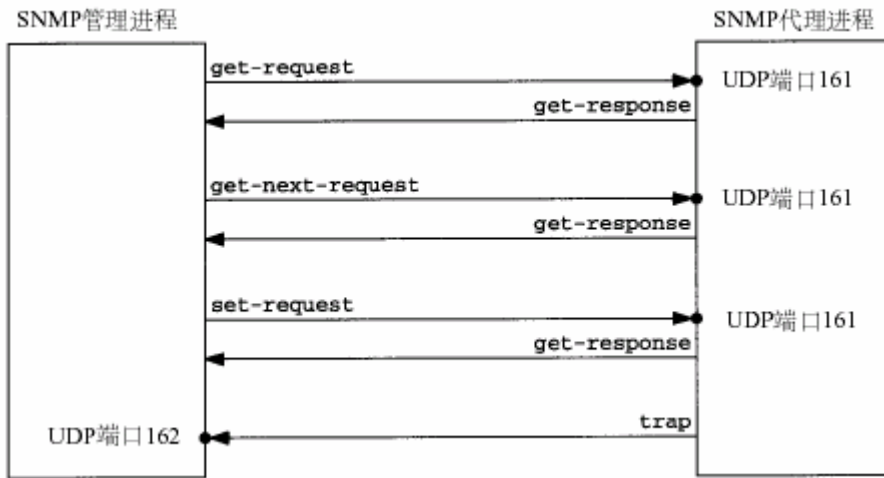
1.3 SNMP 管理操作

SNMP 协议中的 NMS 和 Agent 之间的交互信息，定义了 6 种操作类型：

- 1) Get-request 操作：NMS 从 Agent 提取一个或多个参数值。
- 2) Get-next-request 操作：NMS 从 Agent 提取一个或多个参数的下一个参数值。
- 3) Get-bulk 操作：NMS 从 Agent 提取批量的参数值；
- 4) Set-request 操作：NMS 设置 Agent 的一个或多个参数值。
- 5) Get-response 操作：Agent 返回的一个或多个参数值，是 Agent 对 NMS 前面 3 个操作的响应操作。
- 6) Trap 操作：Agent 主动发出的报文，通知 NMS 有某些事情发生。

前面的 4 个报文是由 NMS 向 Agent 发出的，后面两个是 Agent 发给 NMS 的（注意：SNMPv1 版本不支持 Get-bulk 操作）。下图描述了这几种操作。

SNMP 的报文类型



NMS 向 Agent 发出的前面 3 种操作和 Agent 的应答操作采用 UDP 的 161 端口。Agent 发出的 Trap 操作采用 UDP 的 162 端口。

1.4 SNMP 安全

SNMPv1 和 SNMPv2 版本使用认证名用来鉴别是否有权使用 MIB 对象。为了能够管理设备，网络管理系统（NMS）的认证名必须同设备中定义的某个认证名一致。

一个认证名可以有以下属性：

- 只读（Read-only）：为被授权的管理工作站提供对所有 MIB 变量的读权限。
- 读写（Read-write）：为被授权的管理工作站提供对所有 MIB 变量的读写权限。
- 在 SNMPv2 的基础上，SNMPv3 通过安全模型以及安全级别来确定对数据采用哪种安全机制进行处理；目前可用的安全模型有三种类别：SNMPv1、SNMPv2c、SNMPv3。
- 下表为目前可用的安全模型以及安全级别

安全模型	安全级别	鉴别	加密	说明
SNMPv1	noAuthNoPriv	认证名	无	通过认证名确认数据的合法性
SNMPv2c	noAuthNoPriv	认证名	无	通过认证名确认数据的合法性

SNMPv3	noAuthNoPriv	用户名	无	通过用户名确认数据的合法性
SNMPv3	authNoPriv	MD5 或者 SHA	无	提供基于 HMAC-MD5 或者 HMAC-SHA 的数据鉴别机制
SNMPv3	authPriv	MD5 或者 SHA	DES	提供基于 HMAC-MD5 或者 HMAC-SHA 的数据鉴别机制提供基于 CBC-DES 的数据加密机制

1.5 SNMP 引擎标识

引擎标识用于唯一标识一个 SNMP 引擎。由于每个 SNMP 实体仅包含一个 SNMP 引擎，它将在一个管理域中唯一标识一个 SNMP 实体。因此，作为一个实体的 SNMPv3 代理器必须拥有一个唯一的引擎标识，即 SntpEngineID。

引擎标识为一个 OCTET STRING，长度为 5~32 字节长。在 RFC3411 中定义了引擎标识的格式：

- 前 4 个字节标识厂商的私有企业号（由 IANA 分配），用 HEX 表示。
- 第 5 个字节表示剩下的字节如何标识：
 - 0：保留
 - 1：后面 4 个字节是一个 Ipv4 地址。
 - 2：后面 16 个字节是一个 Ipv6 地址。
 - 3：后面 6 个字节是一个 MAC 地址。
 - 4：文本，最长 27 个字节，由厂商自行定义。
 - 5：16 进制值，最长 27 个字节，由厂商自行定义。
 - 6-127：保留。
 - 128-255：由厂商特定的格式。

1.6 Trap

可将以下命令应用于接口上：

命令	作用
show snmp trap link-status [interface INTERFACE-ID [, -]]	此命令用于显示每个接口上的链路状态的 trap 状态。
snmp trap link-status	此命令用于启用发生在接口上的连接事件和断开连接事件的通知。
no snmp trap link-status	此命令禁用此通知。

显示端口 gi0/1 到 gi0/9 的接口连接/断开接口连接的 trap 状态：

```
Ruijie# show snmp trap link-status interface gi0/1-1/0/9

Interface      Trap state
-----
gi0/1          Enabled
gi0/2          Enabled
gi0/3          Disabled
```

```

gi0/4  Enabled
gi0/5  Enabled
gi0/6  Disabled
gi0/7  Enabled
gi0/8  Enabled
gi0/9  Enabled

Ruijie#

```

禁用 gi0/1 上连接和断开连接 trap 的生成:

```

Ruijie# configure terminal
Ruijie(config)# interface gi0/1
Ruijie(config-if)# no snmp trap link-status
Ruijie(config-if)#

```

1.7 SNMP 服务器

命令	作用
show snmp-server [traps]	此命令用于显示 SNMP 服务器的全局状态设置和与 trap 相关的设置。使用 show snmp-server 命令显示 SNMP 服务器的全局状态设置。使用 show snmp-server traps 命令显示与 trap 相关的设置。
show snmp-server trap-sending [interface INTERFACE-ID [, -]]	此命令用于显示每个端口的 SNMP trap 发送状态。
snmp-server	此命令用于启用 SNMP 代理。SNMP 管理器通过发送 SNMP 请求到代理并接收来自代理的 SNMP 响应和通知来管理 SNMP 代理。在管理代理前，代理上的 SNMP 服务器必须启用。
no snmp-server	此命令可禁用 SNMP 代理。
snmp-server contact TEXT	此命令用于为设备配置系统联系人信息。
no snmp-server contact	此命令可清除设置。
snmp-server enable traps	此命令用于启用 trap 数据包的全局发送。
no snmp-server enable traps	此命令禁用 trap 数据包的发送。
snmp-server enable traps snmp [authentication] [linkup] [linkdown] [coldstart] [warmstart]	此命令用于启用所有或指定的 SNMP 通知的发送。要启用通知 trap 的发送，全局设置也必须要启用。
no snmp-server enable traps snmp [authentication] [linkup] [linkdown] [coldstart] [warmstart]	此命令禁用所有或指定的 SNMP 通知的发送。
snmp-server location TEXT	此命令用于配置系统的本地信息。
no snmp-server location	此命令清除设置。
hostname NAME	此命令用于配置系统名称信息。
no hostname	此命令可清除设置。
snmp-server trap-sending disable	此命令用于禁用端口从已配置的端口发送 SNMP 通知 trap。如果发送被禁用，系统生成的 SNMP 通知 trap 将不被发送出端口。其它系统生成的 SNMP trap 和转发至端口的 SNMP trap 不受此限制。
no snmp-server trap-sending disable	此命令可禁用端口的 trap 发送状态。
snmp-server service-port PORT-NUMBER	此命令用于配置 SNMP UDP 端口号。代理将侦听服务 UDP 端口号上配置的 SNMP 请求数据包。
no snmp-server service-port	此命令复位 UDP 端口号到默认值。
snmp-server response broadcast-request	此命令用于启用服务器响应广播 SNMP GetRequest 数据包。NMS 工具将发送广播 SNMP GetRequest 数据包查找网络设备。要启用此功能，需启用响应广播 get request 数据包。
no snmp-server response broadcast-request	此命令禁用响应广播 SNMP GetRequest 数据包。
snmp-server community [0 7] COMMUNITY-STRING [view VIEW-NAME] [ro rw] [IP-ACL-NAME]	此命令用于配置团体字符串以便访问 SNMP。
no snmp-server community [0 7] COMMUNITY-STRING	此命令删除团体字符串。
snmp-server engineID local	此命令用于指定本地设备上的 SNMP 引擎 ID。

ENGINEID-STRING	运行配置中，SNMP 引擎 ID 不会显示和进行存储。SNMP 引擎 ID 是识别设备的唯一字符串。默认情况下，字符串是生成的。如果您配置的字符串少于 24 个字符，其后将添加 0，直至达到 24 个字符。
no snmp-server engineID local	此命令恢复 SNMP 引擎 ID 到默认值。
snmp-server group GROUP-NAME {v1 v2c v3 {auth noauth priv}} [read READ-VIEW] [write WRITE-VIEW] [notify NOTIFY-VIEW] [access IP-ACL-NAME]	此命令用于配置一个 SNMP 组。
no snmp-server group GROUP-NAME {v1 v2c v3 {auth noauth priv}}	此命令清除一个 SNMP 组，或使用特定的安全模式从中清除一个 SNMP 组。
snmp-server host {IP-ADDRESS IPV6-ADDRESS} [version {1 2c 3 {auth noauth priv}}] COMMUNITY-STRING [port PORT-NUMBER]	此命令用于指定 SNMP 通知的收件人。
no snmp-server host {IP-ADDRESS IPV6-ADDRESS}	此命令清除收件人。
snmp-server user USER-NAME GROUP-NAME {v1 v2c v3 [encrypted] [auth {md5 sha} AUTH-PASSWORD [priv des56 PRIV-PASSWORD]]} [access IP-ACL-NAME]	此命令用于创建 SNMP 用户。
no snmp-server user USER-NAME GROUP-NAME {v1 v2c v3}	此命令可清除 SNMP 用户。
snmp-server view VIEW-NAME OID-TREE {included excluded}	此命令用于创建 MIB 对象查看。
no snmp-server view VIEW-NAME	此命令删除一条指定的 SNMP 查看条目。

显示 SNMP 服务器的配置信息：

```
Ruijie#show snmp-server
SNMP Server : Enabled
Name       :
Location   :
Contact    :
SNMP UDP Port : 161
SNMP Response Broadcast Request : Disabled
0 SNMP packets input
  0 Bad SNMP version errors
  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 (Maximum packet size 1500)
  0 No such name errors
  0 Bad values errors
  0 General errors
  0 Get-response PDUs
  0 SNMP trap PDUs
SNMP global trap: disabled
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

显示与 trap 相关的设置：

```
Ruijie# show snmp-server traps
Global Trap State :Enabled
Individual Trap State:
Authentication :Enabled
linkup :Enabled
linkdown :Enabled
coldstart :Enabled
warmstart :Disabled
Ruijie#
```

端口 gi0/1 到 gi0/9 的 trap 发送状态:

```
Ruijie# show snmp-server trap-sending interface gi0/1-1/0/9

Port    Trap Sending
-----
gi0/1   Enabled
gi0/2   Enabled
gi0/3   Disabled
gi0/4   Enabled
gi0/5   Enabled
gi0/6   Disabled
gi0/7   Enabled
gi0/8   Enabled
gi0/9   Enabled

Ruijie#
```

启用 SNMP 服务器:

```
Ruijie# configure terminal
Ruijie(config)# snmp-server
Ruijie(config)#
```

配置具有字符串 MIS Department II 的系统联系人信息:

```
Ruijie# configure terminal
Ruijie(config)# snmp-server contact MIS Department II
Ruijie(config)#
```

启用 SNMP trap 的全局发送状态:

```
Ruijie# configure terminal
Ruijie(config)# snmp-server enable traps
Ruijie(config)#
```

启用交换机发送所有的 SNMP trap 到使用定义的公共的团体字符串的主机 10.9.18.100:

```
Ruijie# configure terminal
Ruijie(config)# snmp-server enable traps
Ruijie(config)# snmp-server enable traps snmp
Ruijie(config)# snmp-server host 10.9.18.100 version 2c public
Ruijie(config)#
```

启用 SNMP 验证 trap:

```
Ruijie# configure terminal
Ruijie(config)# snmp-server enable traps snmp authentication
Ruijie(config)#
```

配置具有字符串“HQ 15F”的系统本地信息:

```
Ruijie# configure terminal
Ruijie(config)# snmp-server location HQ 15F
Ruijie(config)#
```

将系统名称配置成“SiteA-switch”:

```
Ruijie#configure terminal
Ruijie(config)#hostname SiteA-switch
SiteA-switch(config)#
```

禁用通知 trap 发送出以太网接口 gi0/8:

```
Ruijie# configure terminal
Ruijie(config)# interface gi0/8
Ruijie(config-if)# snmp-server trap-sending disable
Ruijie(config-if)#
```

配置 SNMP UDP 端口号:

```
Ruijie# configure terminal
Ruijie(config)# snmp-server service-port 50000
Ruijie(config)#
```

演示了如何启用服务器响应广播 SNMP get request 数据包:

```
Ruijie# configure terminal
Ruijie(config)# snmp-server response broadcast-request
Ruijie(config)#
```

创建 MIB 查看 “interfacesMibView” 和可进行读写访问的 interfacesMibView 查看的团体字符串 “comaccess”。

```
Ruijie# configure terminal
Ruijie(config)# snmp-server view interfacesMibView 1.3.6.1.2.1.2 included
Ruijie(config)# snmp-server community comaccess view interfacesMibView rw
Ruijie(config)#
```

配置 SNMP 引擎 ID 为 33220000000000000000000000000000:

```
Ruijie# configure terminal
Ruijie(config)# snmp-server engineID local 332200000000000000000000
Ruijie(config)#
```

为 SNMPv3 访问和 SNMPv2c 创建 SNMP 服务器组 “guestgroup”:

```
Ruijie# configure terminal
Ruijie(config)# snmp-server view interfacesMibView 1.3.6.1.2.1.2 included
Ruijie(config)# snmp-server group guestgroup v3 auth read interfacesMibView
Ruijie(config)# snmp-server group guestgroup v2c read CommunityView write
CommunityView
Ruijie(config)#
```

配置具有团体字符串 “comaccess” 的版本 1 的 trap 收件人 163.10.50.126:

```
Ruijie# configure terminal
Ruijie(config)# snmp-server community comaccess rw
Ruijie(config)# snmp-server host 163.10.50.126 version 1 comaccess
Ruijie(config)#
```

配置具有版本 3 验证安全级别和用户名为 “username” 的 trap 收件人 163.10.50.126:

```
Ruijie# configure terminal
Ruijie(config)# snmp-server group groupaccess v3 auth read CommunityView write
CommunityView
Ruijie(config)# snmp-server user useraccess groupaccess v3 auth md5 12345678
Ruijie(config)# snmp-server host 163.10.50.126 version 3 auth useraccess
Ruijie(config)#
```

配置具有团体字符串 “comaccess” 的版本 1 的 trap 收件人 163.10.50.126。UDP 端口号配置为 50001:

```
Ruijie# configure terminal
Ruijie(config)# snmp-server community comaccess rw
Ruijie(config)# snmp-server host 163.10.50.126 version 1 comaccess port 50001
Ruijie(config)#
```

为公共 SNMPv3 组的用户 “user1” 配置纯文本格式的密码:

```
Ruijie# configure terminal
Ruijie(config)# snmp-server user user1 public v3 auth md5 authpassword priv des56
privpassword
Ruijie(config)#
```

使用 MD5 摘要字符串代替纯文本密码:

```
Ruijie# configure terminal
Ruijie(config)# snmp-server user user1 public v3 encrypted auth md5
00112233445566778899AABBCCDDEEFF
Ruijie(config)#
```

创建名为 “interfacesMibView” 的 MIB 查看并定义具有 “interfacesMibView” 的 SNMP 组 “guestgroup” 为读取查看:

```
Ruijie# configure terminal
Ruijie(config)# snmp-server view interfacesMibView 1.3.6.1.2.1.2 included
Ruijie(config)# snmp-server group guestgroup v3 auth read interfacesMibView
Ruijie(config)#
```

1.8 Show 命令

要显示 SNMP 设置和已配置的 SNMP 用户的信息，可执行以下命令：

命令	作用
show snmp {community host view group engineID}	此命令用于显示 SNMP 设置。显示 SNMP 团体字符时，不会显示创建的 SNMPv1 或 SNMPv2c 用户。
show snmp user [USER-NAME]	此命令用于显示已配置的 SNMP 用户的信息。如果未指定用户名参数，则显示所有已配置的用户。使用此命令，不会显示创建的字符串。

显示 SNMP 团体信息：

```
Ruijie# show snmp community

Community : ruijie
Access   : read-only
View     : default

Total Entries: 1
Ruijie#
```

显示 SNMP 服务器的主机设置：

```
Ruijie# show snmp host

Host IP Address : 10.90.90.90
SNMP Version   : V1
Community Name  : ruijie
UDP Port       : 162

Total Entries: 1
Ruijie#
```

显示 MIB 查看设置：

```
Ruijie# show snmp view

default(included) 1.3.6.1

Total Entries: 1
Ruijie#
```

显示 SNMP 组设置：

```
Ruijie# show snmp group

GroupName: public      SecurityModel: v1
ReadView   : CommunityView   WriteView   :
NotifyView : CommunityView
IP access control list:

GroupName: public      SecurityModel: v2c
ReadView   : CommunityView   WriteView   :
NotifyView : CommunityView
IP access control list:

GroupName: initial     SecurityModel: v3/noauth
ReadView   : restricted   WriteView   :
NotifyView : restricted
IP access control list:

GroupName: private     SecurityModel: v1
ReadView   : CommunityView   WriteView   : CommunityView
NotifyView : CommunityView
IP access control list:
```



```
GroupName: private      SecurityModel: v2c
ReadView      : CommunityView      WriteView      : CommunityView
NotifyView    : CommunityView
IP access control list:

Total Entries: 5

Ruijie#
```

显示 SNMP 引擎 ID:

```
Ruijie# show snmp engineID

Local SNMP engineID:0000000902000000C025808

Ruijie#
```

显示 SNMP 用户:

```
Ruijie# show snmp user authuser

User name: authuser
Security Model: v2c
Group Name:VacmGroupName
IP access control list:HB5

User name: authuser
Security Model: v3 priv
Group Name:VacmGroupName
Authentication Protocol:MD5
Privacy Protocol:DES
Engine ID:0000000902000000C025808
IP access control list:

Total Entries:2

Ruijie#
```

2 RMON

2.1 RMON 概述

RMON (Remote Monitoring, 远程监视) 是 IETF (Internet Engineering Task Force, Internet 工程专门小组) 标准的监控规范, 这个规范可以让各种网络监控器和控制台系统之间交换网络监控数据。RMON 在网络节点上放置探测器, 网络管理平台决定这些探测器汇报哪些信息, 如被监视的统计信息, 收集历史信息所使用的时间段等等。例如交换机和路由器等网络设备, 在网络上相当一个网络节点, 通过 RMON 功能, 可以监视当前所处节点位置的信息。

RMON 的发展经历了三个阶段, 第一阶段是以太网远程监视; 第二阶段增加了令牌环的功能, 称为令牌环远程监视模块; 第三阶段被称为 RMON2, 从而使 RMON 功能发展到协议监视的更高层次。

第一阶段的 RMON (下称 RMON1) 包含九个组, 所有的组都是可选择性 (而非强制性) 的, 但有些组的使用必须有其他组的支持。

交换机实现统计组、历史组、警告组、事件组的内容。

2.2 Collection

可将以下命令应用于接口上:

命令	作用
<code>rmon collection stats INDEX [owner NAME]</code>	此命令用于在配置的接口上启用 RMON 统计。
<code>no rmon collection stats INDEX</code>	此命令可禁用 RMON 统计。
<code>rmon collection history INDEX [owner NAME] [buckets NUM] [interval SECONDS]</code>	此命令用于启用配置端口上聚集的 RMON MIB 历史统计。
<code>no rmon collection history INDEX</code>	此命令可禁用接口聚集的历史统计。

配置以太网接口 gi0/2 上索引为 65 且所有者名称为 “guest” 的 RMON 统计条目:

```
Ruijie# configure terminal
Ruijie(config)# interface gi0/2
Ruijie(config-if)# rmon collection stats 65 owner guest
Ruijie(config-if)#
```

在以太网接口 1/0/8 上启用 RMON MIB 历史统计组:

```
Ruijie# configure terminal
Ruijie(config)# interface gi0/8
Ruijie(config-if)# rmon collection history 101 owner it@domain.com interval 2000
Ruijie(config-if)#
```

2.3 警告

警告组 (Alarm) 是 RMON 中的第 3 组, 以指定的时间间隔监控一个特定的 MIB (Management Information Base, 管理信息库) 对象, 当这个 MIB 对象的值超过一个设定的上限值或低于一个设定的下限值时, 会触发警报。警报被当作事件来处理, 处理事件的方式可以是记录日志或发送 SNMP Trap 的方式。可通过以下命令实现相应功能:

命令	作用
<code>rmon alarm INDEX VARIABLE INTERVAL {delta absolute} rising-threshold VALUE [RISING-EVENT-NUMBER] falling-threshold VALUE</code>	此命令用于配置告警条目以便监控接口。

[FALLING-EVENT-NUMBER] [owner STRING]	
no rmon alarm INDEX	此命令清除一个告警条目。
show rmon alarm	此命令用于显示告警配置。

配置告警条目以便监控接口：

```
Ruijie# configure terminal
Ruijie(config)# rmon alarm 783 1.3.6.1.2.1.2.2.1.12.6 30 delta rising-threshold 20 1
falling-
threshold 10 1 owner Name
Ruijie(config)#
```

显示 RMON 告警表：

```
Ruijie# show rmon alarm

Alarm index 23, owned by IT
Monitors OID:1.3.6.1.2.1.2.2.1.10.1
every 120 second(s)
Taking delta samples, last value was 2500
Rising threshold is 2000, assigned to event 12
Falling threshold is 1100, assigned to event 12
On startup enable rising or falling alarm

Ruijie#
```

2.4 事件

事件组 (Event) 是 RMON 中的第 9 组，决定由于警报而产生事件时，处理行为是产生一个日志记录表项还是一个 SNMP Trap。

可通过以下命令实现相应功能：

命令	作用
rmon event INDEX [log] [trap COMMUNITY] [owner NAME] [description TEXT]	此命令用于配置事件条目。
no rmon event INDEX	此命令清除事件条目。
show rmon events	此命令用于显示 RMON 事件表。

配置索引号为 13 的事件从而在事件发生时生成日志：

```
Ruijie# configure terminal
Ruijie(config)# rmon event 13 log owner it@domain.com description ifInNUcastPkts is
too much
Ruijie(config)#
```

演显示 RMON 事件表：

```
Ruijie# show rmon events

Event 1, owned by manager1
Description is Errors
Event trigger action: log & trap sent to community manager
Last triggered time:13:12:15, 2013-09-12

Event 2, owned by manager2
Description is Errors
Event trigger action: log & trap
Last triggered time:

Ruijie#
```

2.5 历史信息

历史组 (History) 是 RMON 中的第 2 组, 历史组定期地收集网络统计信息, 并记录下来以便日后处理。它包含两个小组:

- HistoryControl 组用来设置采样间隔时间、采样数据源等控制信息。
- EthernetHistory 组为管理员提供有关网段流量、错误包、广播包、利用率以及碰撞次数等其他统计信息的历史数据。

可在 EXEC 模式或任何配置模式下, 执行以下命令:

命令	作用
show rmon history	此命令用于显示 RMON 历史统计信息

显示 RMON 以太网历史统计:

```
Ruijie# show rmon history

Index 23, owned by Manager, Data source is gi0/2
Interval:30 seconds
Requested buckets:50, Granted buckets:50
Sample #1
Received octets:303595962, Received packets:357568
Broadcast packets:3289, Multicast packets:7287
Estimated utilization:19
Undersized packets:213, Oversized packets:24
Fragments:2, Jabbers:1
CRC alignment errors:0, Collisions:0
Drop events :0
Sample #2
Received octets:303596354, Received packets:357898
Broadcast packets:3329, Multicast packets:7337
Estimated utilization:19
Undersized packets:213, Oversized packets:24
Fragments:2, Jabbers:1
CRC alignment errors:0, Collisions:0
Drop events :0

Ruijie#
```

2.6 以太网统计信息

统计组是 RMON 中的第 1 组, 统计组统计被监控的每个子网的基本统计信息。目前只能对网络设备的以太网接口进行监控、统计。该组包含一个以太网统计表, 统计的内容包括丢弃的数据包、广播数据包、CRC 错误、大小块、冲突等。可在 EXEC 模式或任何配置模式下, 执行以下命令:

命令	作用
show rmon statistics	此命令用于显示 RMON 以太网统计信息。

显示 RMON 统计信息:

```
Ruijie# show rmon statistics

Index 32, owned by it@domain.com, Data Source is gi0/3 Received Octets :234000,
Received packets :9706
Broadcast packets:2266, Multicast packets:192
Undersized packets:213, Oversized packets:24
Fragments:2, Jabbers:1
CRC alignment errors:0, Collisions:0
Drop events :0
Packets in 64 octets:256, Packets in 65-127 octets :236
Packets in 128-255 octets :129, Packets in 256-511 octets :10
Packets in 512-1023 octets :38, Packets in 1024-1518 octets :2200
```

2.7 snmp-server enable traps rmon

可在全局模式下执行以下命令：

命令	作用
snmp-server enable traps rmon [rising-alarm falling-alarm]	此命令用于启用 RMON trap 状态。
no snmp-server enable traps rmon [rising-alarm falling-alarm]	此命令用于禁用 RMON trap 状态。

启用下降告警和上升告警发送 RMON trap 信息：

```
Ruijie# configure terminal
Ruijie(config)# snmp-server enable traps rmon
Ruijie(config)#
```

3 SNTP

3.1 概述

目前，因特网上普遍采用了通讯协议来实现网络时间同步，即 NTP (Network Time Protocol—网络时间协议)，还有一种协议是 NTP 协议的简化版，即 SNTP (Simple Network Time Protocol, 简单网络时间协议)。

NTP 协议可以跨越各种平台和操作系统，用非常精密的算法，因而几乎不受网络的延迟和抖动的影响，可以提供 1-50 ms 精度。NTP 同时提供认证机制，安全级别很高。但是 NTP 算法复杂，对系统要求较高。

SNTP (简单网络时间协议) 是 NTP 的简化版本，在实现时，计算时间用了简单的算法，性能较高。而精确度一般也能达到 1 秒左右，也能基本满足绝大多数场合的需要。

由于 SNTP 的报文和 NTP 的报文是完全一致的，所以本设备实现的 SNTP Client 能完全兼容 NTP Server。

3.2 时钟设置

命令	作用
<code>clock set HH:MM:SS DAY MONTH YEAR</code>	此命令用于手动设置系统时钟。
<code>clock summer-time recurring WEEK DAY MONTH HH:MM WEEK DAY MONTH HH:MM [OFFSET]</code>	此命令用于配置系统自动切换到夏令时间（夏时制）。此命令有两种形式。一种是循环形式，通过月份中的周和日期来指定时间。另一种形式是日期形式，即指定月份中的日期。
<code>clock summer-time date DATE MONTH YEAR HH:MM DATE MONTH YEAR HH:MM [OFFSET]</code>	命令中包含了日期形式和循环形式这两种，命令的第一部分指定夏令时的开始时间，命令的第二部分则指定夏令时的结束时间。
<code>no clock summer-time</code>	此命令禁止交换机自动切换到夏令时。
<code>clock timezone {+ -} HOURS-OFFSET [MINUTES-OFFSET]</code>	此命令可设置用于显示的时区。
<code>no clock timezone</code>	此命令将时间设置为协调世界时（UTC）。
<code>show clock</code>	此命令用于显示时间和日期信息。此命令还可以指示时钟源。时钟源可以设置为“无时钟源”或“SNTP”。

将软件时钟手动设置为 2013 年 7 月 4 日下午 6:00:

```
Ruijie# clock set 18:00:00 4 Jul 2013
Ruijie#
```

指定夏令时开始于四月的第一个星期天的凌晨 2 点，结束于十月的最后一个周日的凌晨 2 点:

```
Ruijie# configure terminal
Ruijie(config)# clock summer-time recurring 1 sun April 2:00 last sun October 2:00
Ruijie(config)#
```

将时区设置为太平洋标准时间（PST），这要比 UTC 早 8 小时:

```
Ruijie# configure terminal
Ruijie(config)# clock timezone - 8
Ruijie(config)#
```

显示当前时间:

```
Ruijie# show clock

Current Time Source   :SNTP
Current Time         :18:20:04, 2013-07-04
Time Zone            :UTC +02:30
Daylight Saving Time :Recurring
Offset in Minutes    :30
Recurring From       :Apr 2nd Tue 15:00
To                   :Oct 2nd Wed 15:30
```

```
Ruijie#
```

3.3 SNTP

SNTP 协议采用客户机/服务器工作方式，服务器通过接收 GPS 信号或自带的原子钟作为系统的时间基准，客户机通过定期访问服务器提供的时间服务获得准确的时间信息，并调整自己的系统时钟，达到网络时间同步的目的。可执行以下命令：

命令	作用
show sntp	此命令用于显示 SNTP 服务器的信息。
sntp enable	此命令用于启用 SNTP 功能。
no sntp enable	此命令禁用 SNTP 功能。
sntp interval SECONDS	此命令用于设置 SNTP 客户端与服务器同步时钟的时间间隔
no sntp interval	此命令禁用此功能。

显示 SNTP 信息：

```
Ruijie# show sntp

SNTP Status      :Enabled
SNTP Pool Interval  :720 seconds

SNTP Server Status:

SNTP Server      Stratum Version Last Receive
-----
----
10.0.0.11        8         4         00:02:02
10.0.0.12        7         4         00:01:02 Synced
10::2 -----
FE80::1111vlan1 -----
-----
--

Total Entries:4

Ruijie#
```

启用 SNTP 功能：

```
Ruijie# configure terminal
Ruijie(config)# sntp enable
Ruijie(config)#
```

将时间间隔设置为 100 秒：

```
Ruijie# configure terminal
Ruijie(config)# sntp interval 100
Ruijie(config)#
```

4 时间范围

4.1 时间范围

可在 EXEC 模式或任何配置模式下执行以下命令：

命令	作用
<code>periodic { daily HH:MM to HH:MM weekly WEEKLY-DAY HH:MM to [WEEKLY-DAY] HH:MM }</code>	用于为一个时间范围模板指定一个时间段，只能在时间范围配置模式下使用。
<code>no periodic { daily HH:MM to HH:MM weekly WEEKLY-DAY HH:MM to [WEEKLY-DAY] HH:MM }</code>	用于从一个时间范围模板删除一个时间段，只能在时间范围配置模式下使用。
<code>show time-range [NAME]</code>	用于显示时间范围模板。如果没有指定名称，则会显示所有配置的时间范围模板。
<code>time-range NAME</code>	用于在使用 <code>periodic</code> 命令指定一个时段之前，进入时间范围配置模式，以创建一个时间范围模板。如果在创建时间范围模板后没有设置任何时间间隔(时段)，这意味着此时间范围模板没有任何会生效的时段。
<code>no time-range NAME</code>	用于删除一个时间范围模板。

创建一个时间范围模板，包括每天 09:00 至 12:00，周六的 00:00 至周一的 00:00，以及删除每天 09:00 至 12:00 的时段：

```
Ruijie(config)#time-range rdtme
Ruijie(config-time-range)#periodic daily 9:00 to 12:00
Ruijie(config-time-range)#periodic weekly saturday 00:00 to monday 00:00
Ruijie(config-time-range)#no periodic daily 9:00 to 12:00
Ruijie(config-time-range)#exit
Ruijie(config)#
```

显示名为 `rdtme` 的时间范围模板的内容：

```
Ruijie#show time-range rdtme
Time Range Profile: rdtme
Daily 09:00 to 12:00
Weekly Saturday 00:00 to Monday 00:00
Ruijie#
```

显示所有已经配置的时间范围模板：

```
Ruijie#show time-range

Time Range Profile: rdtme
Daily 09:00 to 12:00
Weekly Saturday 00:00 to Monday 00:00

Time Range Profile: lunchtime
Daily 12:00 to 13:00

Total Entries:2

Ruijie#
```

创建名为 `rdtme` 的时间范围模板并进入时间范围配置模式。

```
Ruijie(config)# time-range rdtme
Ruijie(config-time-range)#
```

删除名为 `offtime` 的时间范围模板。

```
Ruijie(config)# no time-range offtime
Ruijie(config)#
```