配置手册

RG-S5750-S 系列交换机

RGOS 10.4(3b18)

文档版本号：V1.1

版权声明

锐捷网络©2017

锐捷网络版权所有，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®、

、

、

、锐捷®都是锐捷网络的注册商标，不得仿冒。

免责声明

本手册内容依据现有信息制作，由于产品版本升级或其他原因，其内容有可能变更。锐捷网络保留在没有任何通知或者提示的情况下对手册内容进行修改的权利。

本手册仅作为使用指导，锐捷网络在编写本手册时已尽力保证其内容准确可靠，但并不确保手册内容完全没有错误或遗漏，本手册中的所有信息也不构成任何明示或暗示的担保。

前　言

版本说明

本手册对应的软件版本为：RGOS 10.4 (3b18)

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

技术支持

- 锐捷网络官方网站：http://www.ruijie.com.cn/
- 锐捷网络在线客服：http://webchat.ruijie.com.cn
- 锐捷网络官方网站服务与支持版块：http://www.ruijie.com.cn/service.aspx
- 7×24 小时技术服务热线：4008-111-000
- 锐捷网络技术论坛：http://bbs.ruijie.com.cn/portal.php
- 常见问题搜索：http://www.ruijie.com.cn/service/know.aspx
- 锐捷网络技术支持与反馈信箱：4008111000@ruijie.com.cn

相关资料

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。

本书约定

1) 命令行格式约定

命令行格式意义如下：

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。

对于产品支持情况进行必要的补充。

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。
- 本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。

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. 命令行界面
2. 基础管理
3. LINE 模式
4. 系统升级
5. 文件系统
6. 配置文件管理
7. 系统管理
8. 系统内存状态查看
9. 系统日志
10. USB 使用
11. 集群管理
12. 设备冗余
13. SRM
14. 硬件表项容量

1 命令行界面

☑ 本章节说明使用命令行界面的方法，您可以通过使用命令行界面来管理网络设备。

1.1 命令模式概述

锐捷网络设备管理界面分成若干不同的模式，用户当前所处的命令模式决定了可以使用的命令。

在命令提示符下输入问号键（?）可以列出每个命令模式支持使用的命令。

当用户和网络设备管理界面建立一个新的会话连接时，用户首先处于用户模式（User EXEC 模式），可以使用用户模式的命令。在用户模式下，只可以使用少量命令，并且命令的功能也受到一些限制，例如像 show 命令等。用户模式的命令的操作结果不会被保存。

要使用所有的命令，首先必须进入特权模式（Privileged EXEC 模式）。通常，在进入特权模式时必须输入特权模式的口令。在特权模式下，用户可以使用所有的特权命令，并且能够由此进入全局配置模式。

使用配置模式（全局配置模式、接口配置模式等）的命令，会对当前运行的配置产生影响。如果用户保存了配置信息，这些命令将被保存下来，并在系统重新启动时再次执行。要进入各种配置模式，首先必须进入全局配置模式。从全局配置模式出发，可以进入接口配置模式等各种配置子模式。

下表列出了命令的模式、如何访问每个模式、模式的提示符、如何离开模式。这里假定网络设备的名字为缺省的“Ruijie”。命令模式概要：

命令模式	访问方法	提示符	离开或访问下一模式	关于该模式
User EXEC（用户模式）	访问网络设备时首先进入该模式。	Ruijie>	输入 **exit** 命令离开该模式。 要进入特权模式，输入 **enable** 命令。	使用该模式来进行基本测试、显示系统信息
Privileged EXEC（特权模式）	在用户模式下，使用 **enable** 命令进入该模式。	Ruijie#	要返回到用户模式，输入 **disable** 命令。 要进入全局配置模式，输入 **configure** 命令。	使用该模式来验证设置命令的结果。该模式是具有口令保护的。
Global configuration（全局配置模式）	在特权模式下，使用 **configure** 命令进入该模式。	Ruijie(config)#	要返回到特权模式，输入 **exit** 命令或 **end** 命令，或者键入 Ctrl+C 组合键。 要进入接口配置模式，输入 **interface** 命令。在 **interface** 命令中必须指明要进入哪一个接口配置子模式。 要进入 VLAN 配置模式，输入 **vlan** vlan_id 命令。	使用该模式的命令来配置影响整个网络设备的全局参数。
Interface configuration（接口配置模式）	在全局配置模式下，使用 **interface** 命令进入该模式。	Ruijie(config-if)#	要返回到特权模式，输入 **end** 命令，或键入 Ctrl+C 组合键。要返回到全局配置模式，输入 **exit** 命令。在 **interface** 命令中必须指明要进入哪一个接口配置子模式。	使用该模式配置网络设备的各种接口。

Config-vlan（VLAN 配置模式）	在全局配置模式下，使用 **vlan** *vlan_id* 命令进入该模式。	Ruijie(config-vlan)#	要返回到特权模式，输入 **end** 命令，或键入 Ctrl+C 组合键。 要返回到全局配置模式，输入 **exit** 命令。	使用该模式配置 VLAN 参数。

1.2 界面配置

1.2.1 获得帮助

用户可以在命令提示符下输入问号键（**?**）列出每个命令模式支持的命令。用户也可以列出相同开头的命令关键字或者每个命令的参数信息。见下表：

命令	作用
Help	在任何命令模式下获得帮助系统的摘要描述信息。
abbreviated-command-entry?	获得相同开头的命令关键字字符串。 例子： Ruijie# **di?** dir disable
abbreviated-command-entry<Tab>	使命令的关键字完整。 例子： Ruijie# **show conf<Tab>** Ruijie# **show configuration**
?	列出该命令的下一个关联的关键字。 例子： Ruijie# **show ?**
command keyword ?	列出该关键字关联的下一个变量。 例子： Ruijie(config)# **snmp-server community** ? WORD　SNMP community string

1.2.2 简写命令

如果想简写命令，只需要输入命令关键字的一部分字符，只要这部分字符足够识别唯一的命令关键字即可。

例如 **show configuration** 命令可以写成：

```
Ruijie# show conf
```

1.2.3 使用命令的no和default选项

几乎所有命令都有 no 选项。通常，使用 no 选项来禁止某个特性或功能，或者执行与命令本身相反的操作。例如接口配置命令 no shutdown 执行关闭接口命令 shutdown 的相反操作，即打开接口。使用不带 no 选项的关键字打开被关闭的特性或者打开缺省是关闭的特性。

配置命令大多有 default 选项，命令的 default 选项将命令的设置恢复为缺省值。大多数命令的缺省值是禁止该功能，因此在许多情况下 default 选项的作用和 no 选项是相同的。然而部分命令的缺省值是允许该功能，在这种情况下，default 选项和 no 选项的作用是相反的。这时 default 选项打开该命令的功能，并将变量设置为缺省的允许状态。

1.2.4 CLI的提示信息

下表列出了用户在使用 CLI 管理网络设备时可能遇到的错误提示信息。

常见的 CLI 错误信息：

错误信息	含义	如何获取帮助
% Ambiguous command: "show c"	用户没有输入足够的字符，网络设备无法识别唯一的命令。	重新输入命令，紧接着发生歧义的单词输入一个问号。可能输入的关键字将被显示出来。
% Incomplete command.	用户没有输入该命令的必需的关键字或者变量参数。	重新输入命令，输入空格再输入一个问号。可能输入的关键字或者变量参数将被显示出来。
% Invalid input detected at '^' marker.	用户输入命令错误，符号（^）指明了产生错误的单词的位置。	在所在地命令模式提示符下输入一个问号，该模式允许的命令的关键字将被显示出来。

1.2.5 使用历史命令

系统提供了用户输入的命令的记录。该特性在重新输入长而且复杂的命令时将十分有用。

从历史命令记录重新调用输入过的命令，执行下表中的操作：

操作	结果
Ctrl-P 或上方向键	在历史命令表中浏览前一条命令。从最近的一条记录开始，重复使用该操作可以查询更早的记录。
Ctrl-N 或下方向键	在使用了 Ctrl-P 或上方向键操作之后，使用该操作在历史命令表中回到更近的一条命令。重复使用该操作可以查询更近的记录。

1.2.6 使用编辑特性

本节描述在进行命令行编辑时可能使用到的编辑功能。

编辑快捷键

下表列出编辑快捷键：

功能	快捷键	说明

在编辑行内移动光标。	左方向键或 Ctrl-B	光标移到左边一个字符。
	右方向键或 Ctrl-F	光标移到右边一个字符。
	Ctrl-A	光标移到命令行的首部。
	Ctrl-E	光标移到命令行的尾部。
删除输入的字符。	Backspace 键	删除光标左边的一个字符。
	Delete 键	删除光标左边的一个字符。
输出时屏幕滚动一行或一页。	Return 键	在显示内容时用回车键将输出的内容向上滚动一行，显示下一行的内容，仅在输出内容未结束时使用。
	Space 键	在显示内容时用空格键将输出的内容向上滚动一页，显示下一页内容，仅在输出内容未结束时使用。

命令行滑动窗口

用户可以使用编辑功能中的滑动窗口特性，来编辑超过单行宽度的命令，使命令行的长度得以延伸。当编辑的光标接近右边框时，整个命令行会整体向左移动 20 个字符，但是仍然可以使光标回到前面的字符或者回到命令行的首部。

编辑命令行时光标移动操作如下表：

功能	快捷键
光标向左回退一个字符	左方向键或 Ctrl-B
光标回到行首	Ctrl-A
光标向右前进一个字符	右方向键或 Ctrl-F
光标移动到行尾	Ctrl-E

例如配置模式的命令 **access-list** 的输入可能超过一个屏幕的宽度。当光标第一次接近行尾时，整个命令行整体向左移动 20 个字符。命令行前部被隐藏的部分被符号（$）代替。每次接近右边界时都会向左移动 20 个字符长度。

```
access-list 199 permit ip host 192.168.180.220 host
$ost 192.168.180.220 host 202.101.99.12
$0.220 host 202.101.99.12 time-range tr
```

可以使用 Ctrl-A 快捷键回到命令行的首部。这时命令行尾部被隐藏的部分将被符号（$）代替：

```
access-list 199 permit ip host 192.168.180.220 host 202.101.99.$
```

默认的终端行宽是 80 个字符。

使用命令行滑动窗口结合历史命令的功能，可以重复调用复杂的命令。具体的快捷键的使用方法查看编辑快捷键。

1.2.7 CLI输出信息的过滤和查找

使用 Show 命令的查找和过滤

要在 **show** 命令输出的信息中查找指定的内容，可以在使用以下命令：

命令	作用

show *any-command*|**begin** *regular-expression*	在 **show** 命令的输出内容中查找指定的内容，将第一个包含该内容的行以及该行以后的全部信息输出。

支持在任意模式下执行 **Show** 命令。

查找的信息内容需要区分大小写，以下相同。

要在 **show** 命令的输出信息中过滤指定的内容，可以使用以下命令：

命令	作用
show *any-command*|**begin** *regular-expression*	在 **show** 命令的输出内容中进行过滤，除了包含指定内容的行以外，输出其他的信息内容。
show*any-command*|**include** *regular-expression*	在 **show** 命令的输出内容中进行过滤，仅输出包含指定内容的行，其他信息将被过滤。

要在 **show** 命令的输出内容中进行查找和过滤，需要输入管道符号（竖线，"|"）。在管道字符之后，可以选择查找和过滤的规则和查找和过滤的内容（字符或字符串）。并且查找和过滤的内容需要区分大小写。

1.2.8 使用命令别名

系统提供命令别名功能，可以指定任意单词作为命令的别名，例如：将单词"mygateway"定义为"ip route 0.0.0.0 0.0.0.0192.1.1.1"的别名，则输入这个单词就相当于输入后面的整个字符串。

通过配置命令别名，可以用一个单词来代替一条命令。例如，创建一个别名来代表一条命令的前一部分，然后可以继续输入后面的部分。

别名所代表的命令所处的命令模式是当前系统中存在的命令模式，在全局配置模式下，输入 alias ?可以列出当前可以配置别名的全部命令模式：

```
Ruijie(config)#alias ?
aaa-gs                  AAA server group mode
acl                      acl configure mode
bgp                      Configure bgp Protocol
config                  globle configure mode
......
```

命令别名支持帮助信息，在别名前面会显示一个星号（*），并且会用以下格式显示：

```
*command-alias=original-command
```

例如，在 EXEC 模式下，默认的命令别名"s"表示"show"关键字。则输入"s?"可以获取's'开头的关键字和别名的帮助信息：

```
Ruijie#s?
*s=show   show   start-chat   start-terminal-service
```

如果别名所代表的命令不止一个单词，则会使用引号将命令包括起来。例如，在 EXEC 模式下配置别名"sv"代替命令 **show version**，则：

```
Ruijie#s?
*s=show   *sv="show version" show   start-chat
```

```
start-terminal-service
```

别名必须从输入的命令行的第一个字符开始，前面不能有空格。如上面的例子，如果在命令之前输入了空格，就不能表示合法的别名：

```
Ruijie# s?
show  start-chat  start-terminal-service
```

命令别名也可以支持获取命令的参数的帮助信息，例如配置接口模式下的命令别名"ia"代表"ip address"，则在接口模式下：

```
Ruijie(config-if)#ia ?
  A.B.C.D  IP address
  dhcp     IP Address via DHCP
Ruijie(config-if)#ip address
```

这里列出了"**ip address**"命令后面的参数信息，并且将别名替换成实际的命令。

命令别名在使用时必须完整输入，否则不能被识别。

使用 **show aliases** 命令可以查看系统中的别名设置。

1.2.9 访问CLI

在使用 CLI 之前，用户需要使用一个终端或 PC 和网络设备连接。启动网络设备，在网络设备硬件和软件初始化后就可以使用 CLI。在网络设备的首次使用时只能使用串口（Console）方式连接网络设备，称为带外（Out band）管理方式。在进行了相关配置后，可以通过 Telnet 虚拟终端方式连接和管理网络设备。通过这两者都可以访问命令行界面。

2 基础管理

2.1 基础管理概述

2.1.1 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 secret** 使用了私有的加密算法。

2.1.2 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 服务器上进行验证，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。

2.1.3 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。

2.1.4 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”。

2.1.5 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。

2.1.6 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。

2.1.7 控制台速率配置

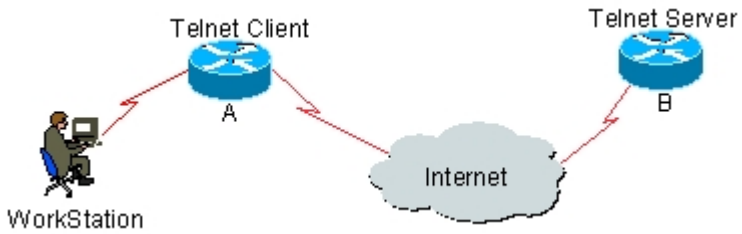
网络设备有一个控制台接口（Console），通过这个控制台接口，可以对网络设备进行管理。当网络设备第一次使用的时候，必须采用通过控制台口方式对其进行配置。可以根据需要改变网络设备串口的速率。需要注意的是，用来管理网络设备的终端的速率设置必须和网络设备的控制台的速率一致。

2.1.8 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设备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 程序同时支持使用 IPV4 和 IPV6 地址进行通讯。作为 Telnet Server，可以同时接受 IPV4 和 IPV6 的 Telnet 连接请求。作为 Telnet Client，可以向 IPV4 和 IPV6 地址的主机发起连接请求。

图 2-1



2.1.9 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。

2.2 基础管理配置

2.2.1 缺省的口令和特权级别配置

缺省没有设置任何级别的口令，缺省的级别是 15 级。

2.2.2 设置和改变各级别的口令

锐捷产品提供下面的命令用于设置和改变各级别的口令。

命令	作用
Ruijie(config)# **enable password** [**level** *level*] {*password* | *encryption-type encrypted-password*}	设置静态口令。目前只能设置 15 级用户的口令，并且只能在未设置安全口令的情况下有效。 如果设置非 15 级的口令，系统将会给出一个提示，并自动转为安全口令。 如果设置的 15 级静态口令和 15 级安全口令完全相同，系统将会给出一个警告信息。
Ruijie(config)# **enable secret** [**level** *level*] {*encryption-type encrypted-password*}	设置安全口令，功能与静态口令相同，但使用了更好的口令加密算法。为了安全起见，建议您使用安全口令。
Ruijie(config)#**service password-encryption**	设置是否对相关口令进行加密。
Ruijie# **enable** [*level*] 和 Ruijie# **disable** [*level*]	切换用户级别，从权限较低的级别切换到权限较高的级别需要输入相应级别的口令。

在设置口令中，如果您使用带 **level** 关键字时，则为指定特权级别定义口令。设置了特定级别的口令后，给定的口令只适用于那些需要访问该级别的用户。

2.2.3 配置多个特权级别

在缺省情况下，系统只有两个受口令保护的授权级别：普通用户级别（1 级）和特权用户级别（15 级）。但是用户可以为每个模式的命令划分 16 个授权级别。通过给不同的级别设置口令，就可以通过不同的授权级别使用不同的命令集合。

在特权用户级别口令没有设置的情况下，进入特权级别亦不需要口令校验。为了安全起见，我们提醒您最好为特权用户级别设置口令。

2.2.4 命令授权配置

如果想让更多的授权级别使用某一条命令，则可以将该命令的使用权授予较低的用户级别；而如果想让命令的使用范围小一些，则可以将该命令的使用权授予较高的用户级别。

你可以使用如下命令对命令进行授权：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式
Ruijie(config)# **privilege** *mode* [**all**] {**level** *level* | **reset**} *command-string*	设置命令的级别划分。 *mode*：要授权的命令所属的 CLI 命令模式，例如：config 表示全局配置模式；exec 表示特权命令模式，interface 表示接口配置模式等等。 all：将指定命令的所有子命令的权限，变为相同的权限级别。 **level** *level*：授权级别，范围从 0 到 15。 **reset**：将命令的执行权限恢复为默认级别。 *command-string*：要授权的命令。

要恢复一条已知的命令授权，可以在全局配置模式下使用 **no privilege** *mode* [**all**] **level** *level command* 命令。

2.2.5 命令授权配置实例

下面是将 **reload** 命令及其子命令授予级别 1 并且设置级别 1 为有效级别（通过设置口令为"**test**"）的配置过程：

```
Ruijie# configure terminal
Ruijie(config)# privilege exec all level 1 reload
Ruijie(config)# enable secret level 1 0 test
Ruijie(config)# end
```

进入 1 级，可以看见命令和子命令：

```
Ruijie# disable 1
Ruijie> reload ?
at                      reload at a specific time/date
cancel                  cancel pending reload scheme
in                      reload after a time interval
<cr>
```

下面是将 **reload** 命令及其子命令的权限恢复为默认值的配置过程：

```
Ruijie# configure terminal
Ruijie(config)# privilege exec all reset reload
Ruijie(config)# end
```

进入 1 级，命令权限已经被收回：

```
Ruijie# disable 1
Ruijie> reload ?
% Unrecognized command.
```

2.2.6 配置线路（line）口令保护

锐捷产品支持对远程登录（如 TELNET）进行口令验证，要配置 **line** 口令保护，请在 **line** 配置模式下执行以下命令：

命令	作用
Ruijie(config-line)# **password** [**0** | **7**] *line*	指定 line 线路口令 0：以明文方式配置口令； 7：以密文方式配置口令； *line*：配置的口令字符串；
Ruijie(config-line)# **secret** { [0] *password* | 5 *encrypted-secret* }	指定 line 线路的 MD5 不可逆加密口令： 0：（可选）指定明文口令文本，配置后将进行 MD5 不可逆加密； *password*：口令明文； ***5*** *encrypted-secret*：用于指定已经过 MD5 不可逆加密的口令文本，配置后将作为加密后的口令进行保存。

Ruijie(config-line)# **login**	启用 line 线路口令保护

如果没有配置登录认证，即使配置了 **line** 口令，登录时，也不会提示用户输入口令进行认证。登录认证在下一节介绍。

2.2.7 配置口令安全策略

锐捷产品支持对设备的本地口令设置口令安全策略。口令安全策略包括口令长度检查、强口令检查、重复口令检查和口令生存周期设置。口令安全配置只对全局口令（通过命令 **enable password**、**enable secret** 配置）和本地用户口令（通过 **username** 配置）生效，对于 line 下面的口令或远程认证的口令不生效。

2.2.7.1 配置口令长度检查

口令长度检查对本地口令的最小长度进行限制，不允许设置小于最小口令长度的口令。

命令	作用
Ruijie(config)# **password policy min-size** *length*	设置口令最小长度 *length*：口令最小长度
Ruijie(config)# **no password policy min-size**	取消口令最小长度检查

如果在配置口令最小长度之前，已经存在长度小于最小口令长度的口令，将在下一次用户使用该口令登录时，提示用户进行口令修改。如果用户不进行修改，将仍然能够继续使用当前命令。

如果在配置口令最小长度之后，配置长度小于最小口令长度的口令，将提示配置失败。

由于不可逆加密的口令通过密文无法解密出对应的明文，如果用户预先配置了不可逆加密的口令，之后再开启口令长度检查，此时无法对用户配置的不可逆加密的口令进行口令长度检查。

2.2.7.2 配置强口令检查

强口令检查对口令强度进行检查，限制使用弱强度的口令。弱口令是指：

- 与账号同名的口令；
- 只包含字符或数字的口令。

命令	作用
Ruijie(config)# **password policy strong**	设置强口令检查
Ruijie(config)# **no password policy strong**	取消强口令检查

如果在配置强口令检查之前，已经存在弱强度的口令，将在下一次用户使用该口令登录时，提示用户进行口令修改。如果用户不进行修改，将仍然能够继续使用当前命令。

如果在配置强口令检查之后，配置弱强度的口令，将提示配置失败。

由于不可逆加密的口令通过密文无法解密出对应的明文，如果用户预先配置了不可逆加密的口令，之后再开启口令强度检查，此时无法对用户配置的不可逆加密的口令进行口令强度检查。

2.2.7.3 配置重复口令检查

重复口令检查限制重复使用最近几次已配置过的口令。最近使用的次数通过命令 **password policy no-repeat-times** 配置。

命令	作用
Ruijie(config)# **password policy no-repeat-times** *times*	配置限制重复使用最近几次已配置过的口令 *times:* 最近几次已配置过的口令
Ruijie(config)# **no password policy no-repeat-times**	取消限制重复使用最近几次已配置过的口令

重复口令检查是基于特权级别或者用户分别记录最近使用过的口令，具体区别如下：

- 对于各个特权级别配置的口令，如使用 **enable password** 或者 **enable secret** 命令配置的口令 ，基于特权级别记录最近使用过的口令
- 对于本地用户配置的口令，如使用 **username** 配置的用户口令，是基于每个用户记录最近使用过的口令

如果用户配置最近几次已经使用过的命令，将提示配置失败。

2.2.7.4 配置口令生存周期

口令生存周期配置口令的有效生存时间。

命令	作用
Ruijie(config)# **password policy life-cycle** *days*	配置口令生存周期 *days:* 口令生存周期，单位：天
Ruijie(config)# **no password policy life-cycle**	取消口令生存周期

设备在用户使用口令进行登录时检查该口令是否已经超期。如果口令在用户登录后的使用过程中超期，将在用户下一次使用该口令登录时提示用户修改密码。如果用户不进行修改，将仍然能够继续使用当前命令。

如果要重新配置或修订口令生存周期，需要先将原来的配置取消。重新配置后，口令生存周期的超期时间点将进行重新计算。

口令生存周期检查是以配置口令生存周期命令时的系统时间点加上口令生存周期时间作为口令超期的时间点。例如：在系统日期为 2011-8-5 时配置了口令生存周期为 5 天，此时口令将在 2011-8-10 超期。所以，在配置口令生存周期之前，需要先保证系统日期是正确的。如果期间修改了设备系统日期，可能会导致口令生存周期出现偏差。例如：在系统日期为 2011-8-9 时，修正了系统日期为 2011-8-11，虽然此时口令只使用了 4 天，但已经超期了，在下次用户登录时，会提示口令超期需要修改密码。

2.2.8 支持会话锁定

锐捷产品支持通过 **lock** 命令将会话终端临时锁住，以防止访问。要使用锁住会话终端的功能，需要在 line 配置模式下打开支持终端锁定的功能，并在相应终端的 EXEC 模式下，通过使用 **lock** 命令锁住终端；终端被锁定后，在终端下输入任何字符，系统都会提示输入解锁口令，口令认证成功后，系统自动解锁。

命令	作用
Ruijie(config-line)# **lockable**	启用锁住 line 终端的功能
Ruijie# **lock**	锁住当前 line 终端

2.2.9 配置本地用户

锐捷产品支持基于本地数据库的身份认证系统，主要用于 AAA 模式下，通过方法列表中的本地认证；以及非 AAA 模式下，线路登录管理中的本地登录认证。

要建立用户名身份认证，请在全局配置模式下，根据具体需求执行以下命令：

命令	作用
Ruijie(config)# **username** *name* [**password** *password* | **password** *encryption-type encrypted password*]	使用加密口令建立用户名身份认证
Ruijie(config)# **username** *name* **secret** { [**0**] *password* | **5** *encrypted-secret* }	为本地用户配置 MD5 不可逆加密口令
Ruijie(config)# **username** *name* [**privilege** *level*]	为用户设置权限级别（可选）

2.2.10 配置用户文件操作权限

锐捷产品支持授予本地用户指定文件的操作权限。文件操作权限包括读（r）、写（w）、执行（x），为了兼容以前的用户操作，在未配置文件操作权限配置的情况下，用户对设备的文件具有所有的权限。

要设置本地用户的文件操作权限，请在全局配置模式下，根据具体需求执行以下命令：

命令	作用
Ruijie(config)#**username** *name* **permission** *oper-mode filename*	设置用户对指定文件操作权限
Ruijie(config)#**no username** *name* **permission** *oper-mode filename*	取消用户对指定文件操作权限的设置

命令中参数 *oper-mode* 代表操作权限，有效的操作权限值包括：null：无权限，r：读权限，w：写权限，x：执行权限。对于 rwx 权限可进行组合设置，如 rw 代表读、写权限，wx 代表写、执行权限。

参数 *filename* 代表文件名或者目录名，采用 linux/unix 的文件和目录表示方式。如“/config.text”表示根目录下的 config.text 文件。

使用 **username** *name* **permission** 可以为用户指定具体某个文件或者某个目录下的所有文件的操作权限，如使用以下命令指定用户具有根目录下所有文件的读写权限：

```
username test permission rx /
```

当用户操作的指定文件不存在相关的权限配置时，使用该文件的上一级目录的权限配置，若上一级目录也不存在权限配置，则继续往上一级目录查找，直到根目录；若根目录也没有存在权限配置，则认为该用户对于指定文件具有所有的操作权限。

2.2.11 配置线路登录认证

要建立线路登录身份认证，请在线路配置模式下，根据具体需求执行以下命令：

命令	作用
Ruijie(config-line)# **login local**	AAA 认证模式关闭时，设置线路登录进行本地认证
Ruijie(config-line)# **login authentication {default** | *list-name*}	AAA 认证模式打开时，设置线路登录进行 AAA 认证。认证时使用 AAA 方法列表中的认证方法，包括 Radius 认证、本地认证、无认证等。

设置 AAA 模式、Radius 服务器配置以及方法列表的配置，请参见 AAA 配置相关章节。

2.2.12 设置系统时间

你可以通过手工的方式来设置网络设备上的时间。当你设置了网络设备的时钟后，网络设备的时钟将以你设置的时间为准一直运行下去，即使网络设备下电，网络设备的时钟仍然继续运行。所以网络设备的时钟设置一次后，原则上不需要再进行设置，除非你需要修正网络设备上的时间。

但是对于没有提供硬件时钟的网络设备，手工设置网络设备上的时间实际上只是设置软件时钟，它仅对本次运行有效，当网络设备下电后，手工设置的时间将失效。

命令	作用
Ruijie# **clock set** *hh:mm:ss month day year*	设置系统的日期和时钟。

例如把系统时间改成 2003-6-20，10:10:12

```
Ruijie# clock set 10:10:12 6 20 2003        //设置系统时间和日期
Ruijie# show clock                           //确认修改系统时间生效
clock: 2003-6-20 10:10:54
```

2.2.13 查看系统时间

你可以在特权模式下使用 **show clock** 命令来显示系统时间信息，显示的格式如下：

```
Ruijie# show clock                                  //显示当前系统时间
clock: 2003-5-20 11:11:34
```

2.2.14 硬件时钟更新

一些平台使用硬件时钟（calendar）来补充软件时钟，硬件时钟是不间断持续运转的，因为硬件时钟是走电池的，即使设备关闭或重启状态下也在运转。

如果硬件时钟和软件时钟不同步，软件时钟是比较精确的，采用该命令将软件时钟的日期和时间复制给硬件时钟。

用软件时钟来更新硬件时钟，在特权模式下执行 **clock update-calendar** 这个命令，软件时钟就会覆盖硬件时钟的值。

命令	作用
Ruijie# **clock update-calendar**	用软件时钟来更新硬件时钟

使用如下命令可以将当前软件时钟的时间和日期复制到硬件时钟：

```
Ruijie# clock update-calendar
```

2.2.15 定时重启

本节描述如何使用 **reload** [*modifiers*]命令制定重启计划（scheme），以实现系统定时重启。定时重启功能，它在某些场合下(比如出于测试目的或其它需要)可以为用户提供操作上的便利。*modifers* 是 **reload** 提供的一组命令选项，可以使得该命令的使用更加灵活。可选的 *modifiers* 有 in、at、cancel。具体使用说明如下：

```
reload  in   mmm | hhh:mm  [string]
```

指定系统在经过一定时间间隔后重启。这里的时间间隔由 *mmm* 或 *hhh:mm* 决定，以分钟为单位，用户可以任选一种格式输入。参数 *string* 是一个帮助提示，用户可以在这里为这个计划起一个助记名，以便能直观地反映该重启的用途，比如如果出于测试目的，需要系统 10 分钟后重启，我们可以键入 **reload in** *10 test*。

```
reload  at  hh:mm month day year [string]
```

指定系统在将来的某个时间点重启。输入的时间值必须是将来的某个时间点。参数 *year* 是可选的,如果用户没有输入，则默认的年份是系统时钟的年份，由于我们限制了时间跨度不能超过 31 天，所以一般地，如果当前系统日期是在 1 月 1 日到 11 月 30 日之间，则用户就没有必要输入年份。但是，如果当前系统月份为 12 月份，这时用户指定的重启时间就有可能并且允许是明年 1 月的某个时间 ，在这种情况下，用户就需要输入年份来通知系统重启时间是明年 1 月份而不是今年 1 月份，如果没有输入，则默认的会被认为是今年 1 月份，从而导致设置失败。*string* 的用法同上。比如当前系统时间是 2005-01-10 14:31，我们想要系统在明天上班时重启，我们可以键入 **reload at** *08:30 11 1 newday*。或者假如当前系统时间是 2005-12-10 14:31，我们想要系统在 2006-01-01 12:00 重启，我们可以键入 **reload at** *12:00 1 1 2006 newyear*。

```
reload  cancel
```

该命令是删除用户已经指定的重启计划。比如前面我们指定了系统在明天 8 点 30 重启，键入 **reload cancel** 后，该设定将被删除。

如果用户要使用 **at** 选项，则要求当前系统必须支持时钟功能。建议使用之前先配置好系统的时钟，以便更切合您的用途。如果用户之前已经设置了重启计划，则后面再设置的计划将覆盖前面的设置。如果用户已经设置了重启计划，假如在该计划生效前用户重启了系统，则该计划将丢失。

重启计划中的时间与当前时间的跨度不能超过 31 天并且要大于当前系统时间。同时用户在设置了重启计划之后最好不要再修改系统时钟,否则有可能会导致设置失效，比如将系统时间调到重启时间之后。

指定系统在某个时间重启

在特权模式下，通过如下命令，可以指定系统在将来的某个时间重启：

命令	作用
Ruijie# **reload at** *hh:mm month day* [*year*] [*reload-reason*]	指定系统在 year 年 month 月 day 日 hh 时 mm 分 reload。relaod 的原因是 reload-reason (如果有输入的话)。

下面是一个指定系统在 2005 年 1 月 11 日中午 12:00 重启的例子(假定系统当前时钟是 2005 年 1 月 11 日 8:30)：

```
Ruijie# reload at 12:00 1 11 2005 midday//设置重启系统时间和日期
```

```
Ruijie# show reload                                    //确认修改重启时间生效
Reload scheduled in 16581 seconds.
At 2005-01-11 12:00
Reload reason: midday
```

指定系统一段时间后重启

在特权模式下，使用如下命令指定系统一段时间后重启：

命令	作用
Ruijie# **reload in** *mmm* [*reload-reason*]	指定系统 mmm 分钟后 reload，reload 的原因是 reload-reason(如果有输入的话)
Ruijie# **reload in** *hhh:mm* [*reload-reason*]	指定系统 hhh 小时 mm 分钟后 reload，reload 的原因是 reload-reason(如果有输入的话)

下面是一个指定系统 125 分钟后 **reload** 的例子(假定当前系统时间是 2005-01-10 12:00)：

```
Ruijie# reload in 125 test                             //设置重启系统时间
```

或者是：

```
Ruijie# reload in 2:5 test                             //设置重启系统时间
Ruijie# show reload                                   //确认修改重启时间生效
System will reload in 7485 seconds.
```

2.2.16 直接重启

不带重启计划参数的 **reload** 命令表示立即重启设备，用户可以在特权模式下直接键入 **reload** 命令来重启系统。

2.2.17 删除已设置的重启策略

在特权模式下，使用如下命令删除已设置的重启计划：

命令	作用
Ruijie# **reload cancel**	删除已设置的重启计划。

如果之前没有设置重启计划，则会提示之前没有配置重启动计划。

2.2.18 配置系统名称

锐捷产品提供全局配置模式下的命令来配置系统的名称：

命令	作用
Ruijie(Config)# **hostname** *name*	设置系统名称，名称必须由可打印字符组成，长度不能超过 63 个字节。

你可以在全局配置模式下使用 **no hostname** 来将系统名称恢复为缺省值。下面的例子将网络设备的名称改成 RGOS：

```
Ruijie# configure terminal                             //进入全局配置模式
```

```
Ruijie(config)# hostname RGOS       //设置网络设备名称为 RGOS
RGOS(config)#                                  //名称已经修改
```

2.2.19 配置命令提示符

如果你没有配置命令提示符，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）将作为缺省提示符，提示符将随着系统名称的变化而变化。可以在全局配置模式下使用 **prompt** 命令配置命令提示符，命令的提示符只对 EXEC 模式有效。

命令	作用
Ruijie# **prompt** *string*	设置命令提示符，名称必须由可打印字符组成，如果长度超过 32 个字符，则截取其前 32 个字符。

可以在全局配置模式下使用 **no prompt** 来将命令提示符恢复为缺省值。

2.2.20 配置每日通知

可以创建包含一行或多行信息的通知信息，当用户登录网络设备时，这些信息将会被显示。可以通过以下全局配置模式的命令来设置每日通知信息：

命令	作用
Ruijie(config)# **banner motd** *c message c*	设置每日通知(message of the day)的文本。c 表示分界符，这个分界符可以是任何字符(比如'&'等字符)。输入分界符后，然后按回车键，现在可以开始输入文本，需要在键入分界符并按回车键来结束文本的输入，需要注意的是，如果键入结束的分界符后仍然输入字符，则这些字符将被系统丢弃。需要注意的是，通知信息的文本中不应该出现作为分界符的字母，文本的长度不能超过 255 个字节。

可以在全局配置模式下使用 **no banner motd** 来删除已配置的每日通知信息。下面的例子说明了如何配置一个每日通知，我们使用(#)作为分界符，每日通知的文本信息为"Notice: system will shutdown on July 6th."，配置实例如下：

```
Ruijie(config)# banner motd #                          //开始分界符
Enter TEXT message.  End with the character '#'.
Notice: system will shutdown on July 6th.#        //结束分界符
Ruijie(config)#
```

2.2.21 配置登录标题

可以通过以下全局配置模式的命令来设置登录标题信息：

命令	作用
Ruijie(config)# **banner login** *c message c*	设置登录标题的文本。c 表示分界符，这个分界符可以是任何字符(比如'&'等字符)。输入分界符后，然后按回车键，现在可以开始输入文本，需要在键入分界符并按回车键来结束文本的输入，需要注意的是，如果键入结束的分界符后仍然输入字符，则这些字符将被系统丢弃。需要注意的是，登录标题的文本中不应该出现作为分界符的字母，文本的长度不能超过 255 个字节。

你可以在全局配置模式下使用 **no banner login** 来删除登录标题。

下面的例子说明了如何配置一个登录标题，我们使用(#)作为分界符，登录标题的文本为“Access for authorized users only. Please enter your password.”，配置实例如下：

```
Ruijie(config)# banner login #                    //开始分界符
Enter TEXT message.  End with the character '#'.
Access for authorized users only. Please enter your password.
#                                                 //结束分界符
Ruijie(config)#
```

2.2.22 显示标题

标题的信息将在你登录网络设备时显示，下面是一个标题显示的例子：

```
C:\>telnet 192.168.65.236
Notice:  system will shutdown on July 6th.
Access for authorized users only. Please enter your password.
 User Access Verification
Password:
```

其中“Notice：system will shutdown on July 6th.” 为每日通知，“Access for authorized users only. Please enter your password.”为登录标题。

2.2.23 显示当前模式配置

在具体的配置模式下，使用 **show this** 可以显示出当前模式的配置，如在 interface fastEthernet 0/1 接口模式下，使用 **show this** 命令可查看 interface fastEthernet 0/1 接口的配置：

```
Ruijie (config)#interface fastEthernet 0/1
Ruijie (config-if-FastEthernet 0/1)#show this
Building configuration...
 !
 spanning-tree link-type point-to-point
 spanning-tree mst 0 port-priority 0
 !
end
Ruijie (config-if-FastEthernet 0/1)#
```

2.2.24 查看系统、版本信息

系统信息主要包括系统描述，系统上电时间，系统的硬件版本，系统的软件版本，系统的 Ctrl 层软件版本，系统的 Boot 层软件版本。你可以通过这些信息来了解这个网络设备系统的概况。你可以在特权模式下使用下表所列的命令来显示这些系统信息：

命令	作用

show version	显示系统、版本信息

序列号在主程序界面上可以通过该命令显示；**show version** 中显示 SYSTEMUPTIME，显示格式为：DD:HH:MM:SS。

在用户执行升级动作时，可能产生运行的软件版本和文件系统中的版本不一致的情况。此时使用该命令显示的主程序版本是内存中运行的版本而显示的 Boot/Ctrl 软件的版本是当前 flash 中保持的版本。

2.2.25 显示硬件实体信息

硬件信息主要包括物理设备信息及设备上的插槽和模块信息。设备本身信息包括：设备的描述，设备拥有的插槽的数量；插槽信息：插槽在设备上的编号，插槽上的模块的描述（如果插槽没有插模块，则描述为空），插槽所插模块包括的物理端口数，插槽最多可能包含的端口的最大个数（所插模块包括的端口数）你可以在特权模式下使用下表所列的命令来显示设备和插槽的信息：

命令	作用
show version devices	显示网络设备当前的设备信息
show version slots	显示网络设备当前的插槽和模块信息

2.2.26 显示零配置和非零配置模式

可以在特权模式下使用下表所列的命令来显示设备当前模式是零配置模式还是非零配置模式：

命令	作用
show zcm mode	显示设备当前模式是零配置模式还是非零配置模式

2.2.27 设置控制台速率

在线路配置模式下，可以使用以下命令来设置控制台的速率：

命令	作用
Ruijie(config-line)# **speed** *speed*	设置控制台的传输速率，单位是 bps。对于串行接口，你只能将传输速率设置为 9600、19200、38400、57600、115200 中的一个，缺省的速率是 9600。

下面的例子表示如何将串口速率设置为 57600 bps：

```
Ruijie# configure terminal                          //进入全局配置模式
Ruijie(config)# line console 0                      //进入控制台线路配置模式
Ruijie(config-line)# speed 57600                    //设置控制台速率为 57600
Ruijie(config-line)# end                            //回到特权模式
Ruijie# show line console 0                         //查看控制台配置
CON      Type     speed    Overruns
* 0      CON      57600    0
Line 0, Location: "", Type: "vt100"
Length: 25 lines, Width: 80 columns
```

```
Special Chars: Escape  Disconnect  Activation
               ^^x     none        ^M
Timeouts:      Idle EXEC    Idle Session
               never        never
History is enabled, history size is 10.
Total input: 22 bytes
Total output:  115 bytes
Data overflow:  0 bytes
stop rx interrupt:  0 times
Modem: READY
```

2.2.28 使用Telnet Client

可以通过网络设备上的 telnet 命令登录到远程设备上去：

命令	作用
Ruijie# **telnet** *host* [*port*] [**/source** {**ip** *A.B.C.D* **| interface** *interface-name*}]	通过 telnet 登录到远程设备，可以是 IPV4 主机名或者 IPV6 主机名、IPV4 地址或者 IPV6 地址。 Telnet 命令支持可选的参数，详细用法参见基础配置管理命令中 **Telnet** 命令的相关章节描述。

下面的例子是如何建立与远程网络设备的 Telnet 会话。

远程网络设备的 IP 地址是 192.168.65.119：

```
Ruijie# telnet 192.168.65.119      //建立到远程设备的 telnet 会话
Trying 192.168.65.119 ... Open
User Access Verification            //进入远程设备的登录界面
Password:
```

使用 Telnet Server

可以通过执行以下命令，来打开网络设备的 Telnet Server 服务：

命令	作用
Ruijie(config)# **enable service telnet-server**	打开 Telnet Server 服务；该命令同时打开 IPV4 和 IPV6 服务；

2.2.29 连接超时

当前已接受的连接，在指定时间内，没有任何输入信息，服务器端将中断此连接。

锐捷产品提供 LINE 配置模式下的命令来配置连接超时时间：

命令	作用

Ruijie(config-line)# **exec-timeout** *minutes* [*seconds*]	配置 LINE 上，已接受连接的超时时间，当超过配置时间，没有任何输入时，将中断此连接。 minutes：指定的超时时间的分钟数； seconds：指定的超时时间的秒数；

可以在 LINE 配置模式下使用 **no exec-timeout** 命令，取消 LINE 下连接的超时设置。

```
Ruijie# configure terminal                    //进入全局配置模式
Ruijie# line vty 0                            //进入 LINE 配置模式
Ruijie(config-line)# exec-timeout 20      //设置超时时间为 20min
```

2.2.30 会话超时

当前 LINE 上已经建立的会话，在指定时间内，没有任何输入信息，将中断当前连接到远程终端的会话。并且恢复终端为空闲状态。

锐捷产品提供 LINE 配置模式下的命令来配置到远程终端的会话超时时间：

命令	作用
Ruijie(config-line)# **session-timeout** *minutes* [**output**]	配置 LINE 上，连接到远程终端的会话超时时间，在指定时间内，没有任何输入时，将中断此会话。 minutes：指定的超时时间的分钟数； output：是否将输出数据也作为输入，来判断是否超时；

可以在 LINE 配置模式下使用 **no session-timeout** 命令，取消 LINE 下到远程终端的会话超时时间设置。

```
Ruijie# configure terminal                      //进入全局配置模式
Ruijie(config)# line vty 0                      //进入 LINE 配置模式
Ruijie(config-line)# session-timeout 20     //设置超时时间为 20min
```

2.2.31 批处理执行文件中的命令

在系统管理中，有时候需要输入较多的配置命令来实现对某个功能的管理，完全通过 CLI 界面输入需要较长的时间，也很容易造成错误和遗漏。如果将这些功能的配置命令按配置步骤全部放在一个批处理文件中，在需要配置时，执行这个批处理文件，就可以将相关的配置全部配置完毕。

命令	作用
Ruijie# **execute** {[**flash:**] *filename*}	执行一个批处理文件。

例如：批处理文件 line_rcms_script.text 用于打开所有异步口上的反向 Telnet 功能，文件内容如下：

```
configure terminal
line tty 1 16
transport input all
no exec
end
```

执行的结果：

```
Ruijie# execute flash:line_rcms_script.text
executing script file line_rcms_script.text ......
executing done
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# line tty 1 16
Ruijie(config-line)# transport input all
Ruijie(config-line)# no exec
Ruijie(config-line)# end
```

批处理文件的文件名和文件中的内容可以自行指定，一般是在用户的 PC 上编辑完毕通过 TFTP 方式传输到设备的 Flash 中。批处理的内容完全是模仿用户的输入，因此，必须按照 CLI 命令的配置顺序来编辑批处理文件的内容。另外，对于一些交互式命令，则需要在批处理文件中预先写入相应的应答信息，保证命令能够正常执行。

批处理文件的大小不能超过 128K，否则将导致批处理文件执行失败。对于过大的批处理文件，可以通过将大文件分成多个较小的文件（小于 128K）来完成。

2.2.32 服务开关设置

在系统运行过程中，可以动态地调整系统所提供的服务，打开与关闭指定的服务（SNMP Server/SSH Server/Telnet Server/Web Server）。

命令	作用
Ruijie(config)# **enable service snmp-agent**	打开 SNMP Server
Ruijie(config)# **enable service ssh-server**	打开 SSH Server
Ruijie(config)# **enable service telnet-server**	打开 Telnet Server
Ruijie(config)# **enable service web-server**	同时打开 Http Server 和 https server

可以在配置模式下，使用 **no enable service** 命令，关闭对应的服务。

```
Ruijie# configure terminal                    //进入全局配置模式
Ruijie(config)# enable service ssh-server     //打开 SSH Server
```

如果只需打开 http 服务，使用如下命令：

```
Ruijie(config)# enable service web-server http
```

如果只需打开 https 服务，使用如下命令：

```
Ruijie(config)# enable service web-server https
```

enable service web-server 命令后面有 3 个可选关键字，如下：

enable service web-server [**http** | **https** | **all**]

如果执行该命令时后面不跟任何关键字，或跟 all 关键字，则表示同时打开 http 服务和 https 服务；如果跟 http 关键字，则表示只打开 http 服务；如果跟 https 关键字，则表示只打开 https 服务。

打开 https 服务后，还需要在设备文件系统根目录下存放服务器端的证书和私钥,https 服务器才能工作。将服务器端的证书文件命名为 httpd_cert.crt，密钥文件命名为 httpd_key.pem，通过 tftp 上传到设备根目录下即可。

2.2.33 HTTP服务参数设置

在使用设备内嵌的 Web 进行管理的时候，可以调整其 HTTP 的服务参数，指定服务的端口或登录服务的认证方法。

命令	作用
Ruijie(config)# **ip http port** *number*	指定 HTTP 服务端口，默认是 80
Ruijie(config)# **ip http authentication**{ **enable** | **local** }	设置 web 登录认证类型，默认为 enable。 **enable**：采用 **enable password** 或 **enable secret** 命令设置的口令进行认证，口令必须是 15 级的； **local**：采用本地 **username** 命令设置的用户名和口令进行认证，该用户必须绑定 15 级权限；

可以在配置模式下，使用以上命令的 **no** 参数，将设置恢复为默认值。以下例子在设备上打开 Http Server，设置服务端口为 8080，并采用本地用户名进行登录认证：

```
Ruijie# configure terminal                        //进入全局配置模式
Ruijie(config)# enable service web-server http //打开 http Server
Ruijie(config)# username name password pass  //设置本地用户
Ruijie(config)# username name privilege 15   //绑定用户权限
Ruijie(config)# ip http port 8080               //设置服务端口
Ruijie(config)# ip http authentication local //设置认证方式
```

使用如下命令配置 HTTPS 服务端口

命令	作用
Ruijie(config)# **ip http secure-port** *number*	指定 HTTPS 服务端口，默认是 443

可以在配置模式下，使用以上命令的 no 参数，恢复 https 服务端口为默认值。以下例子在设备上打开 Https Server，设置服务端口为 4443：

```
Ruijie# configure terminal                        //进入全局配置模式
Ruijie(config)# enable service web-server https //打开 https Server
Ruijie(Config)# ip http secure-port 4443
```

使用如下命令验证 web 服务器状态：

```
Ruijie# show web-server status
http server status : enabled
http server port : 8080
https server status:  enabled
https server port: 4443
```

应避免把 http 服务和 https 服务配置成同样的端口。如果在 http 服务已经打开的情况下，再打开 https 服务，并且不小心把端口配置成和 http 服务端口一样，则通过该端口只能访问 https 服务，http 服务被暂时屏蔽，直到 https 服务端口被改变或服务被关闭，http 服务才重新生效。

2.2.34 多重引导功能配置

在缺省情况下，设备在内置 Flash 中寻找主程序文件并引导运行。如果主程序文件因为意外而损坏（如：升级失败、Flash 被格式化等），那么设备将启动失败导致无法工作。

锐捷的部分产品提供了多重引导功能；这类设备支持配置多个主程序名，能够从本地 Flash、可移动存储设备（U 盘）或远程 TFTP 服务器中获取主程序文件引导设备运行。在设备启动时系统根据引导优先级从高到低的顺序依次尝试引导对应的主程序，如果一个主程序文件引导失败，系统会自动尝试引导下一个主程序文件，直到系统被成功引导或所有的主程序都引导失败为止。在一些对可靠性要求较高的环境中，配置多重引导功能是必要的。

以下将描述如何利用多重引导功能实现主程序冗余备份和利用可移动存储设备快速部署等功能。

添加启动主程序配置

锐捷产品提供如下命令配置设备的启动主程序文件名并指定引导优先级。在设备引导阶段系统将按照优先级从高到低的顺序（1 为最高，10 为最低）依次尝试引导对应的主程序。

命令	作用
Ruijie(config)# **boot system** [**switch all** | *switchid*] *priority* prefix:/[directory/]filename	设置设备的启动主程序文件名并指定引导优先级。引导优先级取值范围为 1～10；其中 1 为最高优先级。

支持使用 URL 前缀来定位文件（具体请参阅《文件系统配置指南》）。例如：usb0:/backup/rgos.bin 表示第一个 usb 设备上 backup 目录下的 rgos.bin 文件。flash:/rgos.bin 表示设备内置 flash 根目录下的 rgos.bin 文件。

VSU 模式下支持配置指定设备的引导路径。

不同的产品平台支持不同类型的 URL 前缀。要了解当前命令能够支持哪些类型，可以使用命令行中的帮助信息，如：

```
Ruijie(config)# boot system 2 ?
flash:   Boot from flash: file system
tftp:    Boot from tftp server
usb0:   Boot from usb0: file system
usb1:   Boot from usb1: file system
```

ISSU 操作期间不允许进行多重引导路径配置（参见“ISSU 升级”）。

默认设置的可引导主程序文件名为：“flash:/rgos.bin”；优先级为 5。

由于系统在引导阶段早期就必须使用该命令的配置，因此该配置存放于设备的 Boot ROM 内而并非保存于配置文件中。

■ 指定本地 Flash 上的文件

可以如下指定本地 Flash 上文件为主程序文件：

```
Ruijie(config)# boot system 5 flash:/rgos.bin
```

当使用 prefix 指定本地文件时，“: ”后的路径必须是绝对路径。

在进行 **boot system** 配置时，系统会对位于本地 Flash 上的主程序文件进行有效性检查。仅有对应文件满足如下要求时才能成功设置：

1) 文件必须存在；

2) 文件为合法的 RGOS 主程序；

3) 文件完整，能通过 CRC 校验。

只要有任一条件不能满足，系统都将提示错误并拒绝设置，如：

```
Ruijie(config)# boot system 5 flash:/foo.bin
Set boot system file error: [flash:/foo.bin] does not exist!
```

另外，不能为同一个引导优先级配置多个主程序文件。如果试图将多个主程序文件配置为相同的引导优先级，系统将提示错误并打印当前主程序文件列表以方便您选取可用的引导优先级。如：

```
Ruijie(config)# boot system 5 flash:/rgos.bin
Ruijie(config)# boot system 5 flash:/rgos_bak.bin
Set boot system file error: priority 5 was assigned to file [flash:/rgos.bin] already.
Boot system config:
=====================================================
Prio      Size               Modified  Name
---- --------- ------------------- ------------------
  1
  2
  3
  4
  5      3205120 2008-08-26 05:22:46 flash:/rgos.bin
  6
  7
  8
  9
 10
=====================================================
Ruijie(config)# boot system 6 flash:/rgos_bak.bin
```

■ 指定可移动存储设备上的文件

将主程序设置为存放与可移动存储设备上的文件的方法与设置为设备本地 Flash 内文件的方式几乎没有差别。唯一不同的是当配置为可移动存储设备上的文件时系统不会对文件的存在与合法性进行检查。

不对可移动存储设备上文件进行检查的目的是为了方便对设备进行远程配置——否则不得不到现场将包含合法主程序文件的 U 盘插入设备才能通过检查。但这也意味着必须自己保证输入的文件名的正确性。

可以如下配置设备从 U 盘引导：

```
Ruijie(config)# boot system 1 usb1:/rgos.bin
```

不支持从 U 盘引导 10.4（3b16）之前的 RGOS 安装包文件。

- VSU 模式下配置指定设备上的引导路径

VSU 模式下，可在主设备上配置指定设备上的引导路径。

可以如下配置设备 3 的优先级为 1 的引到路径：

```
Ruijie(config)# boot system switch 3 1 flash:/rgos.bin
```

修改主程序的引导优先级

使用 **boot system** 命令也可以修改主程序的引导优先级。假设当前系统中已配置的启动主程序列表如下：

```
Ruijie# show boot system
Boot system config:
=====================================================
Prio      Size               Modified  Name
---- --------- ------------------- ------------------
  1
  2
  3
  4
  5      3205120 2008-08-26 05:22:46 flash:/rgos.bin
  6
  7
  8      3205120 2008-08-26 05:25:09 flash:/rgos_bak.bin
  9
 10
=====================================================
```

若需要调整“flash:/rgos_bak.bin”的引导优先级为 1，可以如下操作：

```
Ruijie(config)# boot system 1 flash:/rgos_bak.bin
File [flash:/rgos_bak.bin] has been configured with priority 8,
Change the priority to [1]? [Yes/no] yes
```

调整后的结果如下：

```
Ruijie# show boot system
Boot system config:
=====================================================
Prio      Size               Modified  Name
---- --------- ------------------- ------------------
  1      3205120 2008-08-26 05:25:09 flash:/rgos_bak.bin
  2
  3
  4
  5      3205120 2008-08-26 05:22:46 flash:/rgos.bin
  6
```

```
 7
 8
 9
10
==================================================
```

删除启动主程序配置

使用如下命令删除启动主程序配置：

命令	作用
Ruijie(config)# **no boot system** [*priority*]	清除对应优先级的主程序名设置。引导优先级取值范围为 1～10；如果不指定 *priority* 参数则清空所有启动主程序文件名设置。

可以使用如下方法删除优先级为 8 的启动主程序配置，删除时系统会打印对应的主程序名并要求确认：

```
Ruijie(config)# no boot system 8
Delete boot system config: [Priority: 8; File Name: flash:/rgos_bak.bin]? [No/yes] yes
```

可以如下清空所有启动主程序文件名设置：

```
Ruijie(config)# no boot system
Clear ALL boot system config? [No/yes] yes
```

如果使用 **no boot system** 命令清空了所有启动主程序文件名设置后没有再配置可引导的主程序名，则在下次设备引导过程中系统将自动恢复为默认设置（主程序文件名为：“flash:/rgos.bin”；优先级为 5）。

查看多重引导功能相关配置

可以使用以下命令查看多重引导功能相关的配置：

命令	作用
show boot system [**switch all** | *switchid*]	显示设备的启动主程序文件名配置信息。
show boot ip	显示设备在启动过程中使用的本地 IP 配置信息。

可以如下显示设备在启动过程中使用的本地 IP 配置信息：

```
Ruijie# show boot ip
System boot ip: [192.168.7.11]
```

可以如下显示设备当前配置的主程序文件名和引导优先级：

```
Ruijie# show boot system
Boot system config:
==================================================
Prio      Size               Modified  Name
---- --------- ------------------- ------------------
  1          N/A                     N/A usb1:/rgos.bin
  2
```

```
  3
  4
  5      3205120 2008-08-26 05:22:46 flash:/rgos.bin
  6
  7
  8      3205120 2008-08-26 05:25:09 flash:/rgos_bak.bin
  9
 10
=====================================================
```

VSU 模式下在主设备上可以如下查看设备 3 当前配置的主程序文件名和引导优先级：

```
Ruijie# show boot system switch 3
Switch 3:
Boot system config:
=====================================================
Prio      Size               Modified  Name
---- --------- ------------------- ------------------
  1          N/A                     N/A usb1:/rgos.bin
  2
  3
  4
  5      3205120 2008-08-26 05:22:46 flash:/rgos.bin
  6
  7
  8      3205120 2008-08-26 05:25:09 flash:/rgos_bak.bin
  9
 10
=====================================================
```

位于远程 TFTP 服务器上的文件不会显示其长度和修改时间。这类文件的长度和修改时间均显示为“N/A”；

如果在执行 **show boot system** 命令时对应的主程序文件不存在，则该文件的长度和修改时间也会显示为“N/A”。

配置举例

以下举例如何将设备配置为：

若引导时在 USB 1 口有 U 盘插入，且 U 盘的根目录下包含一合法主程序文件，即从 U 盘引导；

若不满足上面条件，则正常从设备内置 Flash 根目录的 rgos.bin 主程序引导；

若 rgos.bin 主程序文件损坏或丢失导致无法引导，则尝试从备份主程序文件 rgos_bak.bin 引导；

若备份主程序文件也无法引导（可能因为设备内置 Flash 被格式化导致），则尝试从远程 TFTP 服务器下载主程序进行引导。

步骤 1：配置设备的默认主程序名

```
Ruijie(config)# boot system 5 flash:/rgos.bin
```

由于设备在初始状态就已经配置了主程序名为：“flash:/rgos.bin”，优先级为 5；因此这步通常可以省略。

建议将正常情况下使用的主程序配置为中等优先级，这样您日后可以很容易地根据需要再配置比其优先级更高或更低的主程序名。

步骤 2：配置设备的备份主程序名

备份主程序的优先级要比正常情况下使用的主程序的引导优先级稍低：

```
Ruijie(config)# boot system 8 flash:/rgos_bak.bin
```

步骤 3：配置设备的远程 TFTP 引导主程序名和设备的 Boot IP

一般将远程 TFTP 引导作为设备在内置 Flash 损坏情况下进行引导的最后手段。所以这里我们将 TFTP 的引导优先级配置得最低：

```
Ruijie(config)# boot ip 192.168.7.11
Ruijie(config)# boot system 10 tftp://192.168.7.24/rgos.bin
```

步骤 4：配置设备的 U 盘引导主程序名

U 盘引导可以用在某些需要快速部署临时版本短期试运行的场景中。

如果将设备配置为优先从 U 盘引导，那么在部署某些临时版本软件时仅需要将包含临时版本的 U 盘插入对应设备中并重启，则设备重启后就会自动使用 U 盘内的临时版本引导。如果需要撤除这个临时版本，仅需要简单地拔除 U 盘并重启即可，这样设备在重启后又会自动使用设备内置 Flash 中的主程序引导。配置 U 盘引导可以简化临时版本的部署工作，缩短设备的版本停机升级时间。

可以如下配置 U 盘引导主程序名，并指定最高的引导优先级：

```
Ruijie(config)# boot system 1 usb1:/rgos.bin
```

步骤 5：检查确认主程序名和优先级配置

最后可以使用 **show boot system** 命令检查以上配置：

```
Ruijie# show boot system
Boot system config:
==================================================
Prio      Size               Modified  Name
---- --------- ------------------- ------------------
  1           N/A                   N/A usb1:/rgos.bin
  2
  3
  4
  5     3205120 2008-08-26 05:22:46 flash:/rgos.bin
  6
  7
  8     3205120 2008-08-26 05:25:09 flash:/rgos_bak.bin
  9
 10           N/A                   N/A tftp://192.168.7.24/
```

```
                                        rgos.bin
==================================================
```

2.2.35 启动配置文件配置

锐捷的部分产品提供了指定启动配置文件的功能。这类设备的启动配置文件可以存放在本地 Flash、可移动存储设备（U 盘）或远程 TFTP 服务器中。

通过一定的设置，设备在启动后可以自动从指定的位置获取配置文件作为启动配置应用。

以下将描述如何配置和使用指定启动配置文件功能。

设置启动配置文件

锐捷产品提供如下命令设置设备的启动配置文件名：

命令	作用
Ruijie(config)# **boot config** *prefix:/[directory/]filename*	设置设备的启动配置文件名。
Ruijie(config)# **no boot config**	清除启动配置文件名设置。

可以使用命令行的帮助信息来查看当前软件版本支持的 URL 前缀，例如：

```
Ruijie(config)#boot config ?
  flash:   Startup-config filename
  usb0:    Startup-config filename
  usb1:    Startup-config filename
```

在设备启动时，系统根据如下原则加载配置文件：

配置文件的加载顺序为：boot config 配置的启动配置文件名、flash:/config.text、boot network 配置的网络启动配置文件名、默认出厂配置（空配置）。

在按顺序加载的过程中，只要有一个配置文件加载成功，系统即不会再加载其余的配置文件。

由于系统在引导阶段早期就必须使用该命令的配置，因此该配置存放于设备的 Boot ROM 内而并非保存于配置文件中。

在使用 **write** [*memory*]命令保存配置时，系统将按照如下规则保存启动配置文件：

如果没有使用 **boot config** 命令配置启动配置文件名，则系统默认将系统配置保存到设备内置 Flash 中的“flash:/config.text”文件中。

如果使用 **boot config** 命令配置了启动配置文件名，且该文件存在，则系统将系统配置保存到该文件中。

如果使用 **boot config** 命令配置了启动配置文件名，但该文件不存在，则：

- 如果该文件所处的设备存在，系统将自动创建指定文件并写入系统配置；
- 如果该文件所处的设备不存在（可能的情况为：启动配置文件被指定在如 U 盘可移动存储设备上，而在执行 **write** [**memory**]命令时该设备尚未被加载），则系统将询问是否要将当前配置保存于默认启动配置文件“/config”中，并根据用户的回答执行相应的操作。

以下举例说明如何将启动配置文件指定为 U 盘上的文件，并示范在移除 U 盘前后执行 **write** 命令的不同行为。

可以如下设置启动配置文件为 U 盘上文件：

```
Ruijie(config)# boot config usb1:/config.text
```

则在移除 U 盘之前执行 **write** 命令，当前配置将被保存于 **boot config** 命令所设定的文件中：

```
Ruijie# write
Building configuration...
Write to boot config file: [usb1:/config.text]
[OK]
```

移除 U 盘后再执行 **write** 命令。由于设备已被移除无法读写，系统将询问是否要将当前配置保存于默认启动配置文件“/config”中：

```
Ruijie# usb remove 1
0:1:1:38 Ruijie: USB-5-USB_DISK_REMOVED: USB Device <USB Mass Storage Device> Removed!
Ruijie# write
Building configuration...
Write to boot config file: [usb1:/config.text]
[Failed]
The device [usb1] does not exist, write to the default config file [flash:/config.text]? [No/yes] yes
Write to the default config file: [flash:/config.text]
[OK]
```

查看启动配置文件相关配置

可以使用以下命令查看多重引导功能相关的配置：

命令	作用
show boot config	显示设备的启动配置文件名配置信息。

可以如下显示设备当前配置的启动配置文件名：

```
Ruijie# show boot config
Boot config file: [flash:/config_main.text]
Service config: [Disabled]
```

可以如下显示设备当前配置的网络启动配置文件名：

```
Ruijie# show boot network
Network config file: [tftp://192.168.7.24/config.text]
Service config: [Enabled]
```

配置举例

以下举例如何将设备配置为：

优先从远程 TFTP 服务器获取配置文件；

如果从 TFTP 获取失败，使用设备内置 Flash 中的备份配置文件。

步骤 1：配置设备优先从网络服务器加载配置，并配置 Boot IP

```
Ruijie(config)# service config
Ruijie(config)# boot ip 192.168.7.11
```

步骤 2：配置设备的网络启动配置文件

```
Ruijie(config)# boot network tftp://192.168.7.24/router_1.text
```

步骤 3：配置设备的启动配置文件

```
Ruijie(config)# boot config flash:/router_1.text

步骤 4：检查确认配置
Ruijie# show boot network
Network config file: [tftp://192.168.7.24/router_1.text]
Service config: [Enabled]
Ruijie# show boot config
Boot config file: [flash:/router_1.text]
Service config: [Enabled]
```

2.2.36 设置零配置和非零配置模式

锐捷产品提供如下命令设置设备模式，可以切换为零配置模式和非零配置模式：

命令	作用
Ruijie# zcm enable	切换零配置模式
Ruijie# zcm disable	切换非零配置模式

产品配置文件中有定义配置宏 CONFIG_ZCM_ENABLE，则默认情况下，设备模式为零配置模式；否则为非零配置模式。

零配置模式是设备启机默认开启 DHCP CLIENT 功能，动态分配设备的管理地址和获取 ACS 服务器地址信息，若设备没有 config.text 文件，则从 ACS 服务器上下载配置文件，并通过执行命令 copy startup-config running-config 或者重启设备的方式生效下载配置的过程，若设备有 config.text 文件，则不从 ACS 服务器下载配置文件，直接使用设备保存的配置文件；非零配置模式是设备启机默认不开启 DHCP CLIENT 功能，无论设备是否存在配置文件，都不从 ACS 服务器上下载配置。

在进行零配置和非零配置模式切换时，命令的具体行为如下：

- 删除当前设备的配置文件。
- 保存设备当前模式到 flash:/ zcm_mode 文件中。
- 设备复位重启。

可以如下设置设备从非零配置模式切换到零配置模式：

```
Ruijie# zcm enable
% Warning: After switching mode the device will automatically restart!
```

```
% Do you want to switch to zero configuration mode? [yes/no]:y

*Apr 27 14:41:03: %ZCM-5-MODE_SWITCH: The device is reloading due to zero or non-zero configuration mode switch.
```

3 LINE 模式

3.1 LINE模式配置

3.1.1 进入LINE模式

通过进入到指定的 LINE 模式，可以在 LINE 模式下，对具体的 LINE 进行配置。要进入到指定的 LINE 模式，执行以下命令：

命令	作用
Ruijie(config)# **line** [**aux** | **console** | **tty** | **vty**] *first-line* [*last-line*]	进入指定的 LINE 模式

3.1.2 增加/减少LINE VTY数目

默认情况下，line vty 的数目为 5。可以通过命令增加或者减少 line vty 的数目。VTY 最大数目可以增加到 36。

命令	作用
Ruijie(config)# **line vty** *line-number*	将 LINE VTY 数目增加到某个值
Ruijie(config)# **no line vty** *line-number*	将 LINE VTY 数目减少到某个值

3.1.3 配置Line下的可通讯协议

如果需要限制 LINE 线路下可以通讯的协议类型，可以通过此命令进行设置。缺省情况下，VTY 类型可以允许所有协议进行通讯；而其它类型的 TTY，不允许任何协议进行通讯。

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **line vty** *first-line* [*last-line*]	进入 Line 配置模式
Ruijie(config-line)# **transport input** {**all | ssh | telnet | none**}	配置对应 Line 下可以通讯的协议
Ruijie(config-line)# **no transport input**	配置 LINE 下不允许任何协议通讯
Ruijie(config-line)# **default transport input**	恢复 LINE 下的通讯协议为默认配置

3.1.4 配置Line下的访问控制列表

如果需要配置 LINE 线路下的访问控制，可以通过此命令进行设置。缺省情况下，Line 下没有配置任何访问控制列表。接收所有连接，并允许所有外出的连接。

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **line vty** *first-line* [*last-line*]	进入 Line 配置模式

Ruijie(config-line)# **access-class** {*access-list-number* | *access-list-name*} {**in | out**}	配置对应 Line 下的访问控制列表
Ruijie(config-line)#**no access-class**{*access-list-number*| *access-list-name*} {**in|out**}	取消 Line 下配置的访问控制列表

4 系统升级

4.1 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 version 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 MAIN。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。
- **BOOT**：最基本的设备初始化和引导程序。这个映像在设备上电是最早被运行。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 CTRL。这个映像只存在于交换机设备中。
- **CTRL**：具备网络功能的引导程序。这个程序映像被 BOOT 所引导，它具备网络通信功能以及引导和升级主程序的功能。这个映像只存在于交换机中。交换机的程序引导过程为：BOOT 引导 CTRL；CTRL 引导主程序。
- **Bootloader**：具备设备初始化、网络通信功能以及引导升级主程序的功能。在设备上电的时候，它最先被装载，在完成设备初始化后，能够引导主程序运行。

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

4.1.1 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。由于设备中存在多份功能各不相同的程序映像（比如引导用的 BOOT/CTRL 等），而这些程序映像又需要互相配合工作。因此升级功能不仅仅是提供对于主程序的更新支持能力，同时还需要提供对于分布在设备上的各个程序映像进行同步自动更新，使设备整体上保持兼容工作的状态。

因此升级文件中，不仅仅包含了执行主要业务的主程序，还包含了和主程序配套的 BOOT/CTRL 等映像。当执行升级动作时，这些映像从升级文件中弹出，更新设备上对应的映像。

4.1.2 工作原理

针对锐捷设备发布的 RGOS 程序映像是一个自解压的可执行程序。在 RGOS 程序映像中，携带着设备上的主要程序映像。比如对于盒式设备，RGOS 程序映像中含有主程序和引导程序映像。

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 RGOS 程序映像拷贝到设备上。用户可以使用这个新的程序映像对设备进行安装。在安装过程中，系统会自动搜索需要升级的映像，将这些映像一一升级。系统将自动保障升级后整机各个映像的兼容性，而不需要用户做更多的识别。

用户在系统升级时，可以选择自动安装的安装方式：

自动安装：新版本文件拷贝到设备上→ 复位设备→ 等待设备安装完毕

自动安装功能的优点是操作简单，一旦开始升级用户就不需要介入直到升级完成。

4.2 升级步骤

设备的升级需要采用如下的步骤：

- 升级前的准备
- 将映像文件拷贝到设备上
- 设备安装和升级
- 确认设备安装情况

不要在设备出现异常繁忙（CPU 利用率>70%）的时候执行升级业务。此举可能导致升级动作失败。

4.2.1 升级前的准备

在进行设备升级之前需要做如下的准备工作：

- 备份配置文件
- 确认文件系统空间
- 确认文件下载方法

在设备繁忙或者遭受攻击的时候进行升级动作，可能会导致升级失败。可以通过 **show cpu** 命令查看系统的繁忙程度，建议在 CPU 利用率小于 20%时进行升级操作。

备份配置文件

升级前需要备份配置文件。因为不同版本的软件可能存在不同的缺省配置，新增的缺省配置可能和当前配置相冲突。为了确保升级不出现问题，升级前先备份原有配置文件。在升级成功后，确认是否存在配置冲突的情况。

确认文件系统空间

用户可以使用 **show file system** 或者 **dir** 命令来了解设备当前的文件系统空间和使用情况。

如果目标文件系统有足够的空间可以保存新旧两个程序映像，则升级过程中，原有的启动主程序将被更名为“原有文件名.bak”。当 CTRL 版本为 10.4 及以上的版本时，这个文件将作为新程序映像的备份启动文件。当新程序映像启动失败时，系统将使用这个备份文件启动。这种方式可以省去因为升级故障而要回滚版本的操作。

当系统几乎没有剩余空间时，用户需要对文件系统进行一些整理以确保升级能够成功。将不需要的文件通过 del 命令删除。

当文件系统空间不足以存放两个程序映像时，将不会产生原有程序映像的备份文件。

及时的清理文件系统有利于快速完成升级。文件系统上的文件数量和规模都比较大的时候，设备的启动速度将受到很大的影响。在升级前，尽量将不需要的文件删除。

确认文件下载方法

将 RGOS 程序映像下载到设备上有如下几种方案：

■ 通过 TFTP 服务器下载

这是最常用的方式。使用这种方式可以实现远程升级。

一种是从主机端下载文件到设备，另一种是从设备上传文件到主机端。

在 CLI 命令模式下，按如下步骤设置来完成文件的下载：

下载前，首先在本地主机端打开 TFTP Server 软件；然后选定要下载的文件所在的目录；而后登录到设备，在特权模式下使用以下命令下载文件，如果没有指明 Location 则需要单独输入 TFTP Server 的 IP 地址。

命令	作用
Ruijie# **copy tftp:** *//location / filename* **flash:** *filename* [**vrf** vrfname]	下载主机端的 URL 指定的文件 *filename* 到设备。

在 CLI 命令模式下，按如下步骤设置来完成文件的上传：

上传前，首先在本地主机端打开 TFTP Server 软件；然后在主机端选定要保存上传文件的目录，而后在特权模式下使用以下命令上传文件。

命令	作用
Ruijie# **copy flash:** *filename* **tftp:** *//location / filename* [**vrf** vrfname]	从设备端上传文件 *filename* 到主机端的 URL 指定的目录下，可重设文件名。

如果源文件的文件名中有空格，则需要给 tftp 链接加上引号，如下：

copy tftp:"//location/filename" **flash:***filename* [**vrf** *vrfname*]

同样的，如果目标的文件名中有空格，也需要将文件名加上引号，如下：

copy tftp://location/filename **flash:**"*filename*" [**vrf** *vrfname*]

■ 通过 TFTP IPv6 传输文件

一种是从主机端下载文件到设备，另一种是从设备上传文件到主机端。

在 CLI 命令模式下，按如下步骤设置来完成文件的下载：

下载前，首先打开 TFTP Server；而后登录到设备，在特权模式下使用以下命令下载文件。

命令	作用
Ruijie# **copy tftp:** //location/filename **flash:** filename	下载主机端的 tftp 服务器所指定的目录下的文件 *filename* 到设备。

在 CLI 命令模式下，按如下步骤设置来完成文件的上传：

上传前，首先在本地主机端打开 TFTP Server 软件；然后在主机端选定要保存上传文件的目录，而后在特权模式下使用以下命令上传文件。

命令	作用

Ruijie# **copy flash:** *filename* **tftp:** //location/filename	从设备端上传文件 *filename* 到主机端的 tftp 服务器所指定的目录下，可重设文件名。

如果 location 为链路本地地址则需要指定出口，请使用扩展命令进行指定。如下:

```
Ruijie# copy tftp: flash:
Address of remote host []?fe80::5efe:192.168.195.90
Output Interface: loopback 0
Source filename []?rgos.bin
Extended commands [n]:
Destination filename [rgos.bin]?
```

当用户通过 copy tftp 命令将文件从 tftp 服务器上下载到设备（主管理板），并且同时覆盖启动主程序文件的时候，系统会对下载的升级文件进行合法性检查（如发现下载了不适用的升级文件或者升级文件内容被破坏等）。而通过其他的途径（如 ftp、xmodem、其他文件系统命令等）更新启动主程序文件则不会进行合法性判断。另外，通过 copy tftp 命令单独覆盖从设备的启动文件也不会执行相应的检查。因此在选择文件下载方法的时候，一般推荐使用 copy tftp 覆盖设备启动文件（主管理板）的方法进行升级最为安全。

TFTP 仅能够支持 32M 以下的文件传输。如果超过 32M，需要使用 FTP 或者 U 盘进行文件下载。

■ 通过 xmodem 下载

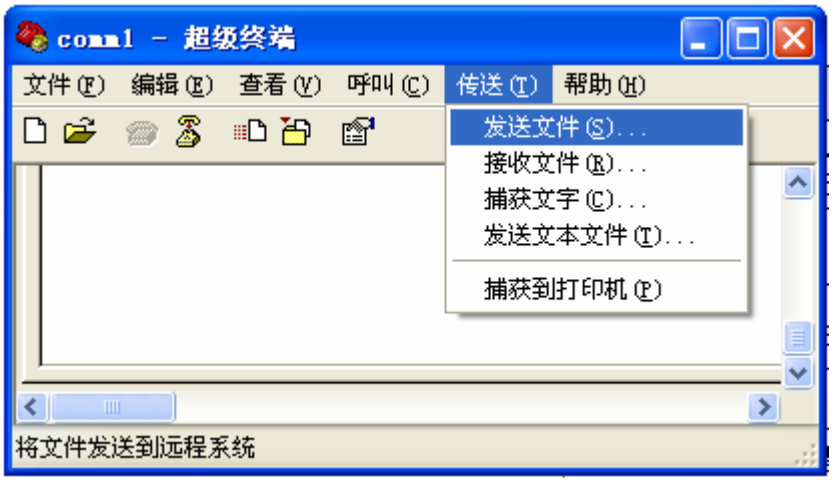
通过 xmodem 下载的方式适用于一些特殊情况，比如网络连接出现问题。使用 xmodem 下载之前必须确认当前和设备使用串口线连接了设备的控制台。一般为了取得较好的下载速度，可以提高连接的波特率。同时确认连接设备的终端软件支持 xmodem 传输。

一种是从主机端下载文件到设备，另一种是从设备上传文件到主机端。

在 CLI 命令模式下，按如下步骤设置来完成文件的下载：

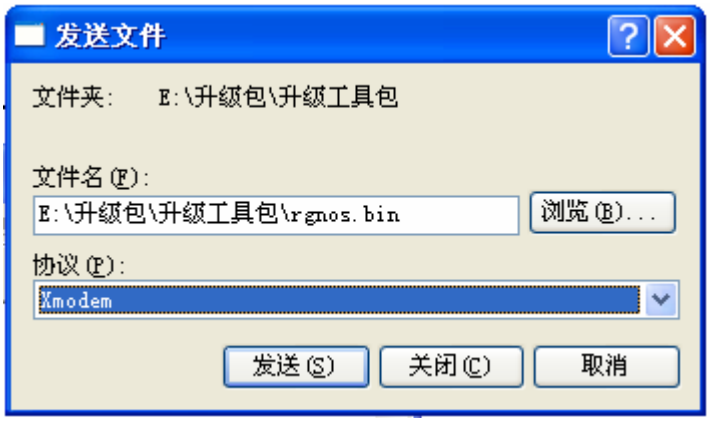
下载前，首先通过 Windows 超级终端登录到设备的带外管理界面；然后在特权模式下使用以下命令下载文件；而后在本地主机的 Windows 超级终端中，选择“传送”菜单中的“发送文件”功能，如图所示：

图 4-1



在弹出的对话框的文件名选择本地主机要下载的文件，协议选择“Xmodem”，点击“发送”，则 Windows 超级终端显示发送的进度以及数据包。如图所示：

图 4-2

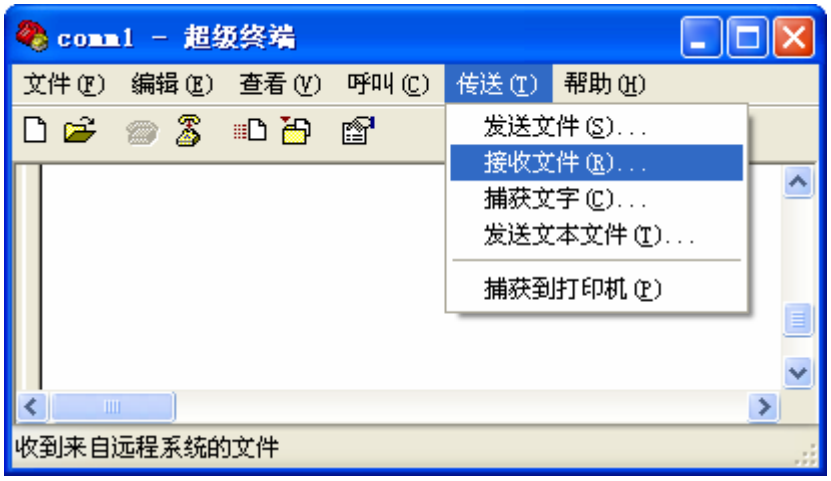


命令	作用
Ruijie# **copy xmodem flash**:*filename*	从主机端下载文件到设备端并命名为 *filename*。

在 CLI 命令模式下，按如下步骤设置来完成文件的上传：

上传前，首先通过 Windows 超级终端登录到设备的带外管理界面；然后在特权模式下使用以下命令上传文件；最后在本地主机的 Windows 超级终端中，选择“传送”菜单中的“接收文件”功能。如图所示：

图 4-3



在弹出的对话框选择上传文件的存储位置，接收协议选择“Xmodem”，点击“接收”，超级终端会进一步提示用户本地存储文件的名称，点击“确认”后开始接收文件。如图所示：

图 4-4

命令	作用
Ruijie# **copy flash**:*filename* **xmodem**	从设备端上传文件 *filename* 到主机端。

如果文件名中有空格，需要将文件名加上引号，如下：

```
copy xmodem flash:"filename"或者 copy flash:"filename" xmodem
```

该方法拷贝升级文件时不会进行合法性检查。

■ 通过 U 盘拷贝

将保存有 RGOS 程序映像的 U 盘插入到设备的 USB 插口上。确认设备已经找到该 USB 器件。

该方法拷贝升级文件时不会进行合法性检查。

■ 通过 FTP 下载

将设备设置为 FTP server，通过 FTP 客户端向设备下载升级软件。

该方法拷贝升级文件时不会进行合法性检查。

4.2.2 升级典型过程举例

盒式设备的升级

盒式设备的升级步骤为：

■ 将新版本软件拷贝到设备上

■ 复位设备

■ 等待设备安装

升级到更高版本

将新版本软件拷贝到设备上：

```
Ruijie#copy tftp://192.168.201.98/ rgos.bin flash:rgos.bin
Accessing tftp://192.168.201.98/ rgos.bin...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
.Checking file, please wait for a few minutes ....
Check file success.
Transmission finished, file length 7243040
THE PROGRAM VERSION: RGOS 10.4.*, Release(64047)
Upgrade Master CM main program OK.
```

```
CURRENT PRODUCT INFORMATION :
  PRODUCT ID: 0x20110010
  PRODUCT DESCRIPTION: Ruijie Gigabit Security & Intelligence Access Switch (S2628G) By Ruijie Network
SUCCESS: UPGRADING OK.
```

复位设备：

```
Ruijie# reload
```

设备重启后，等待设备的安装：

从旧版本升级到之后的版本在设备复位后，绝大部分情况设备不需要任何安装即可使用。只在很少数情况下会出现设备安装动作。此时系统会有如下升级 BOOT 或者 CTRL 映像的提示：

```
Upgrading CTRL...
DO NOT POWER OFF!
Erasing device...eeeeeeeeeeeeeeeeeeeeeeee [ok]
Writing flash #################### [OK - 1,215,488 bytes]
*Apr  1 07:32:44: %UPGRADE-5-LOCAL_FIN: New software image installed in flash.
```

当系统提示正在进行 flash 操作时，比如上文的 Erasing device 或者 Writing flash 这样的动作时，特别注意不要对设备下电。如果在操作 flash 期间下电可能导致设备无法启动，且不可恢复。

降级到 10.4(1)或更低版本

降级的步骤和升级完全一样，不同的是等待设备安装过程的界面不同。

将新版本软件拷贝到设备上：

```
Ruijie#copy tftp://192.168.201.98/ rgos bin flash:rgos.bin
Accessing tftp://192.168.201.98/ rgos.bin...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Transmission finished, file length 6128032 bytes.
Verify the system boot image .[ok]
CURRENT PRODUCT INFORMATION :
  PRODUCT ID: 0x20110010
  PRODUCT DESCRIPTION: Ruijie Gigabit Security & Intelligence Access Switch (S2628G) By Ruijie Networks
SUCCESS: UPGRADING OK.
```

复位设备：

```
Ruijie#reload
```

设备重启后，等待设备的安装：

设备启动后，会自动开始本地映像安装，例如：

```
Prepare installation data ...
```

```
Load install package file rgos.bin OK!
Installation is in process ...
ATTENTION: Do not restart your machine before finish !
Upgrading main ...
Size of main file rgos.bin is 10406464 Bytes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Checking file, please wait for a few minutes ....
Check file success.
Upgrade main succeed.
Installation process finished successfully ...
```

当设备自动安装完毕，系统将自动复位设备：

```
SYS-5-RESTART: The device is restarting. Reason: Upgrade product !.
```

复位完成后，设备即可进入就绪状态。

4.2.3 确认设备安装情况

当系统完成了安装，用户可以通过 **show version** 命令查看设备的升级情况，确认设备主程序版本是否和预先设定的版本相同。BOOT、CTRL、Bootloader 可能和升级的主程序包内的版本不同，属于正常的情况。

show version 中的主程序版本是指目前系统内存中正在运行的主程序版本号。因此在手工安装的情况下，**show version** 显示的主程序版本号不是新安装的软件的版本号，而是当前运行软件的版本号。

> 通过 **show version** 命令显示该映像的项目发布版本标示。发布版本标示即该版本的第几次发行，这个标示显示在版本号之后的括弧之中，如 10.4（2）中，“2”就是发布版本标示。

4.3 其它升级处理

当系统完成了上述升级安装过程后，部分产品、系统有时还需要一些额外的处理。如 VSU 堆叠环境中，为了保证系统起机配置的确定性，建议进行同步配置文件的处理。

4.3.1 同步配置文件

在部分产品系统，如 VSU 堆叠环境中，当用户使用 **rename** 或诸如 **copy tftp:**//172.18.2.65/config.text **startup-config** 形式的命令更新主设备上的起机配置文件时，该起机配置文件有时不会立即更新同步到从设备和候选设备（某些产品系统仅支持 **write** 命令触发的配置同步和定时同步），如果此时系统复位且复位后主设备变化了，就会使得系统起机配置非预期的情况。

为了避免上述问题的发生，可以在主设备配置文件更新后，通过 **synchronize** *filename* 命令将配置文件同步到各个非主设备上，如：

```
Ruijie#synchronize flash:rgos.bin
Synchornize file /rgos.bin to slave:/
Device(6): download
file!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!![OK - 10,414,752 bytes]
Synchornize file to slave devices successfully!
```

synchronize *filename* 可用于同步主设备上任意文件（不单是配置文件）到各个非主设备上，且同步为同路径下的同名文件。

因通信检测建立需要一定过程以及可能的拓扑环境的变化，请根据命令提示信息确认该文件是否已经如预期般同步到所有非主设备并同步成功，如果未能全部同步成功，可再次尝试该命令进行重试。

4.4 升级常见问题

4.4.1 主管理板主程序丢失

用户可能在意外的情况下将文件系统中的启动主程序删除，此时，系统将提示警告：

```
Warning: System boot file rgos.bin is missing.
```

4.4.2 文件系统空间不足

文件系统空间不足可能发生在下载或者拷贝文件的时候。相关的命令将提示：

```
Insufficient file system space。
```

此时需要清理文件系统上的无用的文件。对于文件系统空间较小的设备，在设备未下电的情况下，可以先删除当前的启动主程序，然后马上通过 copy tftp 将新的升级文件拷贝到设备上设置为启动主程序。

4.4.3 升级时未覆盖启动主程序

如果升级的时候没有更新系统的启动主程序，系统重新启动后，将不会运行新的程序。

对于从设备，升级前需要确认其启动主程序名。如果未更新其启动主程序，则系统启动的时候，可能出现主从设备版本不一致的情况。

4.4.4 启动主程序名称设置错误

用户可能使用 **boot system** 命令设置了不存在的启动主程序。

```
Warning: System boot file xxx is missing.
```

此时需要核对用户配置的文件名是否正确，尤其注意大小写敏感的问题。

4.4.5 升级时提示超时失败

在升级过程中，可能提示超时失败。

```
*Feb 10 15:47:12: %UPGRADE-4-PROTO_TIMEOUT: Server is busy and ack timeout.
```

此时可尝试如下处理：

- 确认待升级板卡是否被拔插或者复位；
- 确认待升级板卡是否系统繁忙（CPU 利用率高）；
- 确认待升级板卡是否使用较多文件系统空间，若如此可尝试删除一些无用文件，释放文件系统空间后再次尝试升级。

5 文件系统

5.1 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和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

5.1.1 使用URL来定位文件

RGOS 的文件系统使用 URL(Uniform Resource Locators)的表示方法来统一定位本地设备各种存储介质上的文件和目录或者定位远程文件。比如用户可以使用 **copy** *source-url destination-url* 命令将文件从一个位置拷贝到另外一个位置。这个位置可以是本地的也可以是远程服务器上的。

根据用户使用的不同的命令，URL 可以用不同的表示方法。如下章节进一步说明 URL 的使用方法：

- 指定服务器上的文件
- 指定本地文件
- URL 的前缀说明

指定服务器上的文件

要指定服务器上的文件，可以使用如下的形式：

```
tftp:[[//location]/directory]/filename
```

location 可以是 IP 地址或者是主机名。文件路径（目录和文件名）是指文件传输的相对位置。比如，tftp 服务器指定的文件传输目录为 c:\download，那么设备上指定的文件路径就是指向对于 c:\download 目录的文件位置。比如“tftp://192.168.0.1/binary/rgos.bin”的定位地址就是指 tftp 服务器（ip 地址为 192.168.0.1）上 c:\download\binary\rgos.bin 文件：

tftp 仅能够支持对 32M 以下的文件进行传输。如果要使用大于 32M 的文件传输，需要使用 ftp 协议。将设备作为 ftp 服务器，向设备上传或者下载文件。

指定本地文件

通过[*prefix*]:[*directory/*]*filename* 语法可以指定设备上的本地文件。使用这种方式可以指定 flash、usb 和从设备 flash 上的文件。

比如：

flash:/config.text 指明了在本地 flash 上的配置文件；

usb0:/backup/rgos.bin.bak 可以表示第一个 usb 设备上的文件。

slave:/rgos.bin 可以表示从设备上根目录上的文件

在指定本地文件时，如果不使用 prefix，则表示当前路径上的文件系统类型。比如当前路径在 usb0 的根目录下，则此时的文件系统操作如果不指定 prefix 就表示 usb0。

当使用 prefix 指定本地文件时，“：”后的路径必须是绝对路径。

URL 的前缀说明

URL 前缀用于指定特定的文件系统。不同的设备和文件操作命令能够操作不同的文件系统。通过 show file system 可以了解当前设备支持的文件系统。

当前支持的 URL 前缀如下：

前缀	说明
flash:	flash 存储介质。这个前缀在所有设备上都可以使用。出厂时设备的启动主程序都保存在 flash 上。
tftp:	TFTP 网络服务器
xmodem:	使用 xmodem 协议向网络设备收发文件
usb0:	第一个 usb 设备
usb1:	第二个 usb 设备

不同的文件系统命令以及不同的产品平台支持不同类型的文件系统，文件系统操作前缀组合支持情况也存在差异，使用时以实际情况为准。要了解当前命令能够支持哪些类型的文件系统服务，可以使用命令行中的帮助信息。如（示例仅供参考，各产品各版本可能存在差异）：

```
Ruijie#copy ?
  WORD            Copy from current file system
  flash:          Copy from flash file system
  ftp:            Copy from ftp: file system
  help            Help informatioin
  running-config  Copy from current system configuration
  startup-config  Copy from startup configuration
  tftp:           Copy from tftp: file system
  usb0:           Copy from usb0 file system
```

```
  usb1:           Copy from usb1 file system
  xmodem:         Copy from xmodem: file system

Ruijie#copy flash:/rgos.bin ?
  WORD     Copy to current file system
  flash:   Copy to flash file system
  ftp:     Copy to ftp: file system
  tftp:    Copy to tftp: file system
  usb0:    Copy to usb0 file system
  usb1:    Copy to usb1 file system
  xmodem:  Copy to xmodem: file system

Ruijie#copy tftp://172.18.2.18/rgos.bin ?
  WORD            Copy to current file system
  flash:          Copy to flash: file system
  running-config  Update (merge with) current system configuration
  startup-config  Copy to startup configuration
  usb0:           Copy to usb0 file system
  usb1:           Copy to usb1 file system
```

以上是单机模式下的示例，在 VSU 模式下，示例如下：

```
Ruijie#copy ?
  WORD            Copy from current file system
  flash:          Copy from flash file system
  ftp:            Copy from ftp: file system
  help            Help informatioin
  running-config  Copy from current system configuration
  startup-config  Copy from startup configuration
  sw1-disk0:      Copy from flash file system on switch 1
  sw1-usb0:       Copy from usb0 file system on switch 1
  sw1-usb1:       Copy from usb1 file system on switch 1
  sw2-disk0:      Copy from flash file system on switch 2
  sw2-usb0:       Copy from usb0 file system on switch 2
  sw2-usb1:       Copy from usb1 file system on switch 2
  sw3-disk0:      Copy from flash file system on switch 3
  sw3-usb0:       Copy from usb0 file system on switch 3
  sw3-usb1:       Copy from usb1 file system on switch 3
  sw4-disk0:      Copy from flash file system on switch 4
  sw4-usb0:       Copy from usb0 file system on switch 4
  sw4-usb1:       Copy from usb1 file system on switch 4
  sw5-disk0:      Copy from flash file system on switch 5
  sw5-usb0:       Copy from usb0 file system on switch 5
  sw5-usb1:       Copy from usb1 file system on switch 5
  sw6-disk0:      Copy from flash file system on switch 6
  sw6-usb0:       Copy from usb0 file system on switch 6
```

```
  sw6-usb1:       Copy from usb1 file system on switch 6
  sw7-disk0:      Copy from flash file system on switch 7
  sw7-usb0:       Copy from usb0 file system on switch 7
  sw7-usb1:       Copy from usb1 file system on switch 7
  sw8-disk0:      Copy from flash file system on switch 8
  sw8-usb0:       Copy from usb0 file system on switch 8
  sw8-usb1:       Copy from usb1 file system on switch 8
  tftp:           Copy from tftp: file system
  usb0:           Copy from usb0 file system
  usb1:           Copy from usb1 file system
  xmodem:         Copy from xmodem: file system

Ruijie#copy flash:/rgos.bin ?
  WORD        Copy to current file system
  flash:      Copy to flash file system
  ftp:        Copy to ftp: file system
  sw1-disk0:  Copy to flash file system on switch 1
  sw1-usb0:   Copy to usb0 file system on switch 1
  sw1-usb1:   Copy to usb1 file system on switch 1
  sw2-disk0:  Copy to flash file system on switch 2
  sw2-usb0:   Copy to usb0 file system on switch 2
  sw2-usb1:   Copy to usb1 file system on switch 2
  sw3-disk0:  Copy to flash file system on switch 3
  sw3-usb0:   Copy to usb0 file system on switch 3
  sw3-usb1:   Copy to usb1 file system on switch 3
  sw4-disk0:  Copy to flash file system on switch 4
  sw4-usb0:   Copy to usb0 file system on switch 4
  sw4-usb1:   Copy to usb1 file system on switch 4
  sw5-disk0:  Copy to flash file system on switch 5
  sw5-usb0:   Copy to usb0 file system on switch 5
  sw5-usb1:   Copy to usb1 file system on switch 5
  sw6-disk0:  Copy to flash file system on switch 6
  sw6-usb0:   Copy to usb0 file system on switch 6
  sw6-usb1:   Copy to usb1 file system on switch 6
  sw7-disk0:  Copy to flash file system on switch 7
  sw7-usb0:   Copy to usb0 file system on switch 7
  sw7-usb1:   Copy to usb1 file system on switch 7
  sw8-disk0:  Copy to flash file system on switch 8
  sw8-usb0:   Copy to usb0 file system on switch 8
  sw8-usb1:   Copy to usb1 file system on switch 8
  tftp:       Copy to tftp: file system
  usb0:       Copy to usb0 file system
  usb1:       Copy to usb1 file system
  xmodem:     Copy to xmodem: file system
```

```
Ruijie#copy tftp://172.18.2.18/rgos.bin ?
  WORD            Copy to current file system
  flash:          Copy to flash: file system
  running-config  Update (merge with) current system configuration
  startup-config  Copy to startup configuration
  usb0:           Copy to usb0 file system
  usb1:           Copy to usb1 file system
```

由于 xmodem 协议的限制，使用 xmodem 传输的文件尺寸会略大于实际文件尺寸。

5.1.2 显示文件系统信息

通过显示文件系统信息的命令，可以了解当前设备上所有支持的文件系统，以及这些文件系统上的可用空间情况。

在特权用户模式下，使用如下命令：

```
Ruijie#show file systems
File Systems:
         Size(b)         Free(b)         Type      Flags      Prefixes
    ------------    ------------    ---------    -------    ----------
*       33488896        16191488        flash         rw        flash:
               -               -        flash         rw         usb0:
               -               -        flash         rw         usb1:
               -               -        flash         rw        slave:
               -               -      network         rw         tftp:
               -               -      network         rw       xmodem:
------------------------------------------------------------------------
```

该命令显示信息中，“*”表示当前所在的文件系统。Size 表示该文件系统的空间大小；Free 表示空闲空间大小。

文件系统空闲空间尺寸表示系统的空闲状况，而不表示可以存储的文件大小。由于文件系统具有自身的管理开销，因此，系统最终能够保存的文件大小要略小于系统空闲空间尺寸。

5.1.3 管理本地设备上的文件

本地文件是指保存在设备上各种存储介质中的文件。例如 flash、usb 等等。设备的系统文件（如主程序、配置文件、日志文件、web 文件等）通常都保存在 flash 上。有的设备还可以提供 U 盘接口。U 盘上的文件管理也属于本地文件管理。

本地文件管理可执行如下的操作：

- 文件复制
- 文件移动
- 文件删除
- 目录创建

- 目录删除
- 目录内容显示
- 当前工作路径显示
- 工作路径更改

这些操作可以用于 slave、usb、flash 类型的文件系统。可以实现在这些文件系统之间互相拷贝文件。

在 flash、slave 上的文件系统中，文件大小写都是敏感的。例如 abc.txt 和 Abc.txt 是两个不同的文件。在指定文件时必须正确的书写大小写才能正确定位文件。而在 usb 这样的设备上，大小写不敏感。即认为 abc.txt 和 Abc.txt 是表示同一个文件。

文件数量和尺寸对于启动速度以及文件操作速度都有一定的影响。在 flash 上存放的文件尺寸和数量非常多的情况下，会使设备的启动速度明显的减慢，同时升级系统的速度也会大大被延迟。第一次设备启动使用 dir 命令的等待时间会比较长。一般的应用环境推荐使用 128M 以下的文件系统空间较为适宜。如果确实需要存放大量的文件，建议保存在 U 盘上。因此，建议在文件系统使用相当时间后，手动清理一些过时的无用文件。

文件系统支持的带路径的文件名长度不超过 4096 字节。所有的文件名以及路径信息均不支持通配符操作。

有些文件是系统正常运行所需的重要系统文件，如果删除了这些文件有可能造成系统无法工作或某些功能不能使用。目前重要的系统文件包括:

RCMS 的配置文件（/rcms_config.ini）

Web 管理文件包（/web_management_pack.upd）

设备的主程序文件（在支持多重引导功能的设备上主程序文件包括所有位于 boot system 配置中的文件）

系统会自动识别这些文件并在删除前给出警告。如果确认删除系统文件，系统将打印 WARN 级别日志。如:

```
Ruijie# delete rgos.bin
File [rgos.bin] is a system file. System may not work properly without it.
Are you sure you want to delete it? [no] yes
0:1:1:38 Ruijie: FS-4-SYSTEM_FILE_DELETED: System file [rgos.bin] deleted!
```

5.1.4 通过通信协议传递文件

- 通过 tftp 协议传递文件

支持从 tftp 服务器下载文件到设备，或者是从设备上传文件到 tftp 服务器上。在 CLI 特权模式下，使用如下命令可完成文件的下载：

```
Ruijie# copy tftp:[[//location]/directory]/filename destination-url
```

在 CLI 特权模式下，使用如下命令完成文件的上传：

```
Ruijie# copy source-url  tftp:[[//location]/directory]/filename
```

- 通过 xmodem 协议传递文件

在特权模式下使用以下命令下载文件到本地；

```
Ruijie# copy xmodem:  destination-url
```

在特权模式下使用以下命令上载文件到服务器；

```
Ruijie# copy source-url xmodem:
```

5.1.5 指定TFTP源地址与源接口号

TFTP 客户端在与 TFTP 服务器通信的时候，发送报文的源地址选取遵循以下规则：

1) 如果没有指定 TFTP 客户端的源地址，则采用路由决定的源地址进行通信。

2) 如果只用 **tftp-client source-addr** *source-ip* 或 **copy tftp** 命令指定了源地址或 **tftp-client source-intf** *source-interface* 指定了接口号，则采用该地址或该项接口的地址进行通信。

3) 如果执行 **tftp-client source-addr** *source-ip* 命令指定了源地址或 **tftp-client source-intf** *source-interface* 指定了源接口号后，又在 **copy tftp** 命令中指定了源地址，则采用 **copy tftp** 命令中指定的源地址进行通信。

4) **tftp-client source-addr** *source-ip* 命令指定的源地址和 **tftp-client source-intf** *source-interface* 指定源接口号对应的地址对所有的 tftp 传输有效，**copy tftp** 命令指定的源地址只对当前的 tftp 传输有效。

5) **tftp-client source-addr** *source-ip* 命令指定的源地址和 **tftp-client source-intf** *source-interface* 指定源接口号命令的配置是互斥的。

5.2 典型配置举例

5.2.1 从tftp服务器下载文件

以下例子说明用户如何将 a.dat 文件从 tftp 服务器的 c:\download\目录上下载到设备上：

1) 在主机端打开 TFTP Server 软件，选定要下载的文件所在的目录 c:\download。

2) 确定设备和 TFTP 服务器的网络连接。可以使用 ping 命令来测试。

3) 登录到设备，进入特权模式，执行以下命令：

```
Ruijie#copy tftp://192.168.201.54/a.dat flash: tftp-source-address 192.168.2.1.52
Destination filename [a.dat]?
Accessing tftp://192.168.201.54/a.dat
!!!!!!!!!!!!!!!!!!!!!!
Transmission finished, file length 343040
```

4) 使用 dir 命令查看设备上的文件

```
Ruijie#dir
Directory of flash:/
    Mode Link      Size               MTime Name
-------- ---- --------- ------------------- ------------------
            1    343040 2009-01-01 02:02:59 a.dat
```

```
            1  10838016 2009-01-01 00:08:38 rgos.bin
            1       399 2009-01-01 00:01:37 config.text
------------------------------------------------------------
3 Files (Total size 11181455 Bytes), 9 Directories.
Total 33030144 bytes (31MB) in this device, 20492288 bytes (19MB) available.
```

5.2.2 上传文件至tftp服务器

以下例子说明用户如何将 a.dat 文件从设备上传到 tftp 服务器的 C:\download 目录上：

1) 在主机端打开 TFTP Server 软件，选定要下载的文件所在的目录 C:\download。

2) 确定设备和 TFTP 服务器的网络连接。可以使用 ping 命令来测试。

3) 登录到设备，进入特权模式，执行以下命令：

```
Ruijie#copy flash:/a.dat tftp://192.168.201.54/a.dat tftp-source-address 192.168.2.1.52
Accessing flash:a.dat...
!!!!!!!!!!!!!!!!!!!!!
 Transmission finished, file length 343040
```

4) 确认 tftp 服务器上的 C:\download 目录下是否出现了 a.dat 文件

5.2.3 通过xmodem下载文件

以下例子说用户如何从 PC 上通过 xmodem 下载 config.text 文件到设备：

1) 首先用串口线将 PC 的串口和设备的串口连接起来。

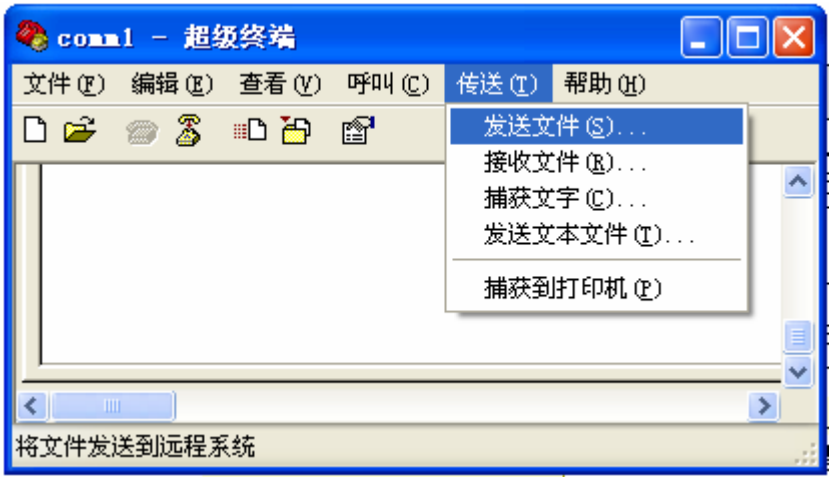
2) 打开 Windows 的超级终端，连接到设备控制台

3) 在特权模式下使用以下命令下载文件

```
Ruijie# copy xmodem: flash:/config.text
```

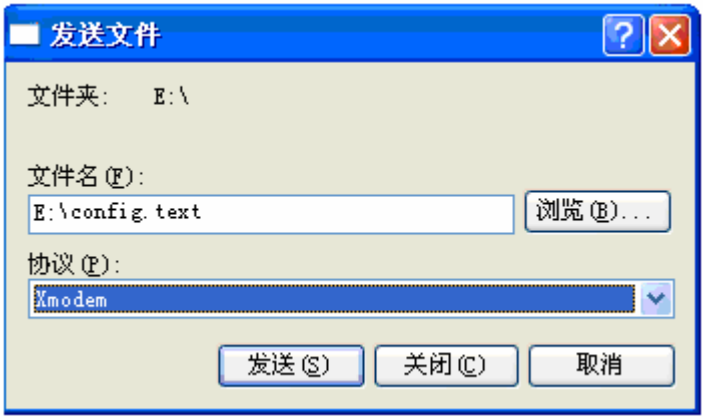
4) 在本地主机的 Windows 超级终端中，选择“传送”菜单中的“发送文件”功能，如下图所示：

图 5-1



5) 在弹出的对话框的文件名选择本地主机要下载的文件，协议选择“Xmodem”，点击“发送”，则 Windows 超级终端显示发送的进度以及数据包。

图 5-2



6) 使用 dir 命令查看设备上的文件

```
Directory of flash:/
    Mode Link      Size               MTime Name
-------- ---- --------- ------------------- ------------------
           1    343040 2009-01-01 02:02:59 a.dat
           1  10838016 2009-01-01 00:08:38 rgos.bin
           1       399 2009-01-01 00:01:37 config.text
-------------------------------------------------------------
3 Files (Total size 11181455 Bytes), 0 Directories.
Total 33030144 bytes (31MB) in this device, 20492288 bytes (19MB) available.
```

5.2.4 通过xmodem上传文件

以下例子说用户如何从设备上通过 xmodem 传 config.text 到 PC 上的 C:\Documents and Settings\ju：

1) 首先用串口线将 PC 的串口和设备的串口连接起来。

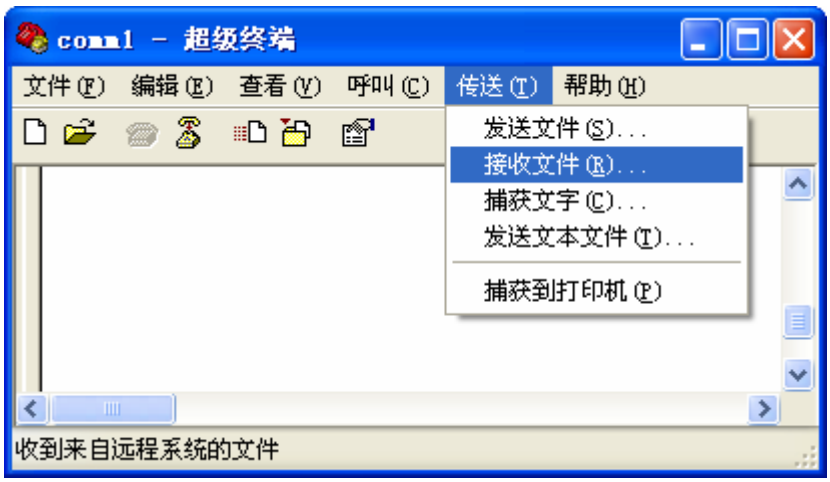
2) 打开 Windows 的超级终端，连接到设备控制台

3) 在特权模式下使用以下命令下载文件

```
Ruijie# copy flash:/config.text xmodem
```

4) 最后在本地主机的 Windows 超级终端中，选择“传送”菜单中的“接收文件”功能。如下图所示：

图 5-3



5) 在弹出的对话框选择上传文件的存储位置，接收协议选择“Xmodem”，点击“接收”，超级终端会进一步提示用户本地存储文件的名称，点击“确认”后开始接收文件。如图所示：

图 5-4

6) 确认 PC 上的 C:\Documents and Settings\ju 目录下是否出现了 config.text 文件

5.2.5 将flash中文件拷贝至usb设备

以下例子说明如何将设备上 flash 中的 config.txt 移动到 U 盘上（插在 usb0 上），并且将其保存在 U 盘上新建立的 backup 目录中。

1) 查看 flash 上的剩余空间

```
Directory of flash:/
    Mode Link      Size               MTime       Name
-------- ---- --------- ------------------- ------------------

           1    343040 2009-01-01 02:02:59     a.dat
```

```
            1  10838016 2009-01-01 00:08:38    rgos.bin
            1       399  2009-01-01 00:01:37     config.text
------------------------------------------------------------
3 Files (Total size 11181455 Bytes), 0 Directories.
Total 33030144 bytes (31MB) in this device, 20492288 bytes (19MB) available.
```

2) 转入 U 盘上根目录

```
Ruijie#cd usb0:/
```

3) 确认当前路径

```
Ruijie#pwd
usb0:/
```

4) 在 U 盘上创建 backup 目录

```
Ruijie#mkdir backup
```

5) 将文件拷贝到 U 盘

```
Ruijie#copy flash:/config.text config.text
```

6) 确认 U 盘上的文件确实已经拷贝完成

```
Ruijie#dir backup
Directory of usb0:/backup
    Mode Link      Size               MTime      Name
-------- ---- --------- ------------------- ------------------
            1       399    2009-01-01 00:01:37  config.text
------------------------------------------------------------
Total 33030144 bytes (31MB) in this device, 20488192 bytes (19MB) available.
```

5.2.6 删除目录

以下例子说明如何删除一个非空的 aaa 目录：

1) 查看当前目录状况

```
Ruijie#dir
Directory of flash:/
    Mode Link      Size                   MTime      Name
-------- ---- --------- ------------------- ------------------
            1       11014633 2006-01-01 08:00:46  rgos.bin
 <dir>     1       0         2006-01-01 08:00:00 aaa/
            1       399       2006-01-01 08:01:37 config.text
------------------------------------------------------------
2Files (Total size 11015032 Bytes), 1 Directories
Total 33030144 bytes (31MB) in this device, 9563693 bytes (9MB) available
```

2) 确认 aaa 目录中是否存在文件

```
Ruijie#dir aaa
Directory of flash:/aaa
    Mode Link      Size                   MTime      Name
-------- ---- --------- ------------------- ------------------
           1           149  2006-01-01 08:01:37 backup.txt
-----------------------------------------------------------------
1Files (Total size 149 Bytes), 0 Directories
Total 33030144 bytes (31MB) in this device, 9563693 bytes (9MB) available
```

3) 删除非空目录

```
Ruijie# delete recursive aaa
```

4) 删除空目录

```
Ruijie# rmdir aaa
```

5) 确认目录确实被删除

```
Ruijie#dir
Directory of flash:/
    Mode Link      Size                   MTime      Name
-------- ---- --------- ------------------- ------------------
           1      11014633 2006-01-01 08:00:46  rgos.bin
           1      399      2006-01-01 08:01:37 config.text
-----------------------------------------------------------------
2Files (Total size 11015032 Bytes), 0 Directories
Total 33030144 bytes (31MB)
in this device, 9563842 bytes (9MB) available
```

6 配置文件管理

6.1 配置文件管理概述

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，对配置变化的监控显得尤为重要。目前，只能通过拷贝当前运行配置文件（running-config）和启动配置文件（startup-config）、逐行比较两个文件中命令差异的方式来确定配置是否发生变化。这种方式虽然可以确认配置是否发生变化，但是仍然存在不少缺陷，比如：不能确定配置变化的先后顺序，不能及时通告网管人员，在配置发生变化导致网络出现问题时很难确认相关的责任人等。配置文件管理可以在配置发生变化时发出消息和日志提醒管理人员。

6.1.1 配置文件管理基本特性

配置文件管理包括配置变化时的消息和日志。

配置变化日志

配置变化日志功能（Configuration Change Logging）提供了一种新的确定配置是否发生变化的方式。这种方式可以跟踪到配置变化的时间、配置的内容、导致配置变化的用户，还可以实时通告网管人员。

6.1.2 工作原理

配置变化日志功能的原理是通过跟踪每一个被应用的配置命令，将对应的用户名、对应的时间、配置命令的内容、配置模式等信息记录下来，并通过通知机制实时发送给远端日志服务器。通过查找这些记录，就可以知道配置是否发生变化，发生了哪些变化，是哪个用户进行配置的。

6.2 配置配置变化日志

6.2.1 缺省配置

下表用来描述配置文件管理功能的缺省配置。

功能特性	缺省值
配置变化日志功能	缺省关闭
配置变化通知功能	缺省关闭
配置日志中保留的条目个数	100

6.2.2 打开变化日志功能

缺省情况下，变化日志功能处于关闭状态。进入特权模式，按以下步骤打开变化日志功能：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **archive**	进入存档配置模式。
Ruijie(config-archive)# **log config**	进入存档日志管理配置模式。
Ruijie(config-archive-log-config)# **logging enable**	打开配置变化日志功能。

如果要关闭配置变化日志功能，可以在 log config 配置模式下通过 **no logging enable** 命令进行设置。

配置举例：

打开配置变化日志功能

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# archive
Ruijie(config-archive)# log config
Ruijie(config-archive-log-config)# logging enable
```

6.2.3 指定配置日志中保留的条目最大个数

缺省情况下，配置日志中保留的条目最大个数是 100。进入特权模式，按以下步骤，可以指定配置日志中保留的条目最大个数：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **archive**	进入存档置模式。
Ruijie(config-archive)# **log config**	进入存档日志管理配置模式。
Ruijie(config-archive-log-config)#**logging size** *entries*	指定配置日志中保留的条目最大个数，范围 1-1000，缺省为 100。

如果要恢复为缺省配置，可以在 log config 配置模式下通过 **no logging size** 命令进行设置。

配置举例：

指定配置日志中保留的条目最大个数为 50。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# archive
Ruijie(config-archive)# log config
Ruijie(config-archive-log-config)# logging size 50
```

6.2.4 打开密码隐藏功能

缺省情况下，允许在配置日志中显示密码信息。进入特权模式，按以下步骤禁止在配置日志中显示密码信息：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。

Ruijie(config)# **archive**	进入存档配置模式。
Ruijie(config-archive)# **log config**	进入存档日志管理配置模式。
Ruijie(config-archive-log-config)# **hidekeys**	禁止在配置日志中显示密码信息。

如果要恢复为缺省配置，可以在 log config 配置模式下通过 **no hidekeys** 命令进行设置。

配置举例：

禁止在配置日志中显示密码信息。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# archive
Ruijie(config-archive)# log config
Ruijie(config-archive-log-config)# hidekeys
```

6.2.5 打开配置变化通知功能

缺省情况下，配置变化通知功能处于关闭状态。进入特权模式，按以下步骤可以打开配置变化通知功能：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **archive**	进入存档配置模式。
Ruijie(config-archive)# **log config**	进入存档日志管理配置模式。
Ruijie(config-archive-log-config)# **notify syslog**	打开配置变化通知功能。

如果要恢复为缺省配置，可以在 log config 配置模式下通过 **no notify syslog** 命令进行设置。

配置举例：

打开配置变化通知功能。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# archive
Ruijie(config-archive)# log config
Ruijie(config-archive-log-config)# notify syslog
```

6.2.6 查看配置日志信息

配置变化日志提供了如下命令，用于显示配置日志信息及内存使用情况。

命令	作用
Ruijie# **show archive log config** {{**all** | *start-num* [*end-num*]} [**provisioning | contenttype** [**plaintext**]] | **statistics**}	显示配置日志信息及内存使用情况。

6.3 配置文件管理典型配置举例

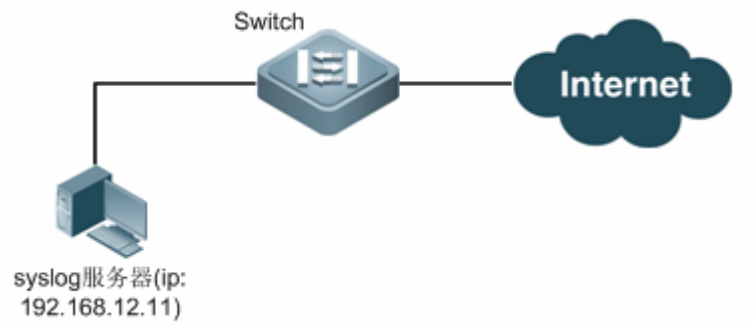
组网需求

为了及时跟踪配置变化情况，假设网管人员有如下要求：

- 打开配置变化日志功能；
- 设置配置日志中保留的最大条目个数为 1000；
- 禁止在配置日志中显示密码信息；
- 允许在配置发生变化时通告远端日志服务器(ip: 192.168.12.11)；

组网拓扑

图 6-1 配置变化日志组网图



配置步骤

1) 打开配置变化日志功能

打开配置变化日志功能，以便跟踪配置变化情况

```
Ruijie# configure terminal
Ruijie(config)# archive
Ruijie(config-archive)# log config
Ruijie(config-archive-log-config)# logging enable
```

2) 设置配置日志中保留的最大条目个数为 1000

设置配置日志中保留的最大条目个数

```
Ruijie(config-archive-log-config)# logging size 1000
```

3) 禁止在配置日志中显示密码信息

禁止在配置日志中显示密码信息

```
Ruijie(config-archive-log-config)# hidekeys
```

4) 允许配置发生变化时通告远端日志服务器(ip: 192.168.12.11)

打开允许配置发生变化时通告远端日志服务器的功能

```
Ruijie(config-archive-log-config)# notify syslog
```

配置远端日志服务器

```
Ruijie(config-archive-log-config)# exit
Ruijie(config-archive)# exit
Ruijie(config)# logging server 192.168.12.11
```

显示验证

查看配置日志信息

```
Ruijie(config)# show archive log config all
idx   sess      user@line      datetime              logged command
1     1    unknown@console  Mar 21 09:57:22   |  logging enable
2     1    unknown@console  Mar 21 09:59:42   |  logging size 1000
3     1    unknown@console  Mar 21 10:02:12   |  hidekeys
4     1    unknown@console  Mar 21 10:02:26   |  notify syslog
5     1    unknown@console  Mar 21 10:02:50   |  exit
6     1    unknown@console  Mar 21 10:03:01   |  exit
```

查看配置日志内存使用情况

```
Ruijie(config)# show archive log config statistic
Config Log Session Info:
Number of sessions being tracked: 1
Memory being held: 1270 bytes
Total memory allocated for session tracking: 1270 bytes
Total memory freed from session tracking: 0 bytes
Config Log log-queue Info:
Number of entries in the log-queue: 3
Memory being held in the log-queue: 671 bytes
Total memory allocated for log entries: 671 bytes
Total memory freed from log entries: 0 bytes
```

7 系统管理

7.1 配置系统管理

7.1.1 显示系统CPU利用率

使用 **show cpu** 命令将显示系统总的 CPU 利用率和每个任务 CPU 利用率的相关信息。

命令	作用
show cpu	查看系统 CPU 利用率信息

缺省情况下，设备的名称为 Ruijie。

下面举例显示 **show cpu** 运行的结果：

```
Ruijie# show cpu
=====================================
     CPU Using Rate Information
CPU utilization in five seconds: 25%
CPU utilization in one minute  : 20%
CPU utilization in five minutes: 10%
  NO    5Sec    1Min    5Min    Process
  0      0%      0%      0%     LISR INT
  1      7%      2%      1%     HISR INT
  2      0%      0%      0%     ktimer
  3      0%      0%      0%     atimer
  4      0%      0%      0%     printk_task
  5      0%      0%      0%     waitqueue_process
  6      0%      0%      0%     tasklet_task
  7      0%      0%      0%     kevents
  8      0%      0%      0%     snmpd
  9      0%      0%      0%     snmp_trapd
 10      0%      0%      0%     mtdblock
 11      0%      0%      0%     gc_task
 12      0%      0%      0%     Context
 13      0%      0%      0%     kswapd
 14      0%      0%      0%     bdflush
 15      0%      0%      0%     kupdate
 16      0%      3%      1%     ll_mt
 17      0%      0%      0%     ll main process
 18      0%      0%      0%     bridge_relay
 19      0%      0%      0%     d1x_task
```

20	0%	0%	0%	secu_policy_task
21	0%	0%	0%	dhcpa_task
22	0%	0%	0%	dhcpsnp_task
23	0%	0%	0%	igmp_snp
24	0%	0%	0%	mstp_event
25	0%	0%	0%	GVRP_EVENT
26	0%	0%	0%	rldp_task
27	0%	2%	1%	rerp_task
28	0%	0%	0%	reup_event_handler
29	0%	0%	0%	tpp_task
30	0%	0%	0%	ip6timer
31	0%	0%	0%	rtadvd
32	0%	0%	0%	tnet6
33	2%	0%	0%	tnet
34	0%	0%	0%	Tarptime
35	0%	0%	0%	gra_arp
36	0%	0%	0%	Ttcptimer
37	8%	1%	0%	ef_res
38	0%	0%	0%	ef_rcv_msg
39	0%	0%	0%	ef_inconsistent_daemon
40	0%	0%	0%	ip6_tunnel_rcv_pkt
41	0%	0%	0%	res6t
42	0%	0%	0%	tunrt6
43	0%	0%	0%	ef6_rcv_msg
44	0%	0%	0%	ef6_inconsistent_daemon
45	0%	0%	0%	imid
46	0%	0%	0%	nsmd
47	0%	0%	0%	ripd
48	0%	0%	0%	ripngd
49	0%	0%	0%	ospfd
50	0%	0%	0%	ospf6d
51	0%	0%	0%	bgpd
52	0%	0%	0%	pimd
53	0%	0%	0%	pim6d
54	0%	0%	0%	pdmd
55	0%	0%	0%	dvmrpd
56	0%	0%	0%	vty_connect
57	0%	0%	0%	aaa_task
58	0%	0%	0%	Tlogtrap
59	0%	0%	0%	dhcp6c
60	0%	0%	0%	sntp_recv_task
61	0%	0%	0%	ntp_task
62	0%	0%	0%	sla_deamon
63	0%	3%	1%	track_daemon
64	0%	0%	0%	pbr_guard

65	0%	0%	0%	vrrpd
66	0%	0%	0%	psnpd
67	0%	0%	0%	igsnpd
68	0%	0%	0%	coa_recv
69	0%	0%	0%	co_oper
70	0%	0%	0%	co_mac
71	0%	0%	0%	radius_task
72	0%	0%	0%	tac+_acct_task
73	0%	0%	0%	tac+_task
74	0%	0%	0%	dhcpd_task
75	0%	0%	0%	dhcps_task
76	0%	0%	0%	dhcpping_task
77	0%	0%	0%	dhcpc_task
78	0%	0%	0%	uart_debug_file_task
79	0%	0%	0%	ssp_init_task
80	0%	0%	0%	rl_listen
81	0%	0%	0%	ikl_msg_operate_thread
82	0%	0%	0%	bcmDPC
83	0%	0%	0%	bcmL2X.0
84	3%	3%	3%	bcmL2X.0
85	0%	0%	0%	bcmCNTR.0
86	0%	0%	0%	bcmTX
87	0%	0%	0%	bcmXGS3AsyncTX
88	0%	2%	1%	bcmLINK.0
89	0%	0%	0%	bcmRX
90	0%	0%	0%	mngpkt_rcv_thread
91	0%	0%	0%	mngpkt_recycle_thread
92	0%	0%	0%	stack_task
93	0%	0%	0%	stack_disc_task
94	0%	0%	0%	redun_sync_task
95	0%	0%	0%	conf_dispatch_task
96	0%	0%	0%	devprob_task
97	0%	0%	0%	rdp_snd_thread
98	0%	0%	0%	rdp_rcv_thread
99	0%	0%	0%	rdp_slot_change_thread
100	4%	2%	1%	datapkt_rcv_thread
101	0%	0%	0%	keepalive_link_notify
102	0%	0%	0%	rerp_msg_recv_thread
103	0%	0%	0%	ip_scan_guard_task
104	0%	0%	0%	ssp_ipmc_hit_task
105	0%	0%	0%	ssp_ipmc_trap_task
106	0%	0%	0%	hw_err_snd_task
107	0%	0%	0%	rerp_packet_send_task
108	0%	0%	0%	idle_vlan_proc_thread
109	0%	0%	0%	cmic_pause_detect

```
110      1%      1%      1%     stat_get_and_send
111      0%      1%      0%     rl_con
112     75%     80%     90%     idle
```

在上面的列表中，开头的 3 行分别表示系统在最近 5 秒钟、最近 1 分钟、最近 5 分钟内总的 CPU 利用率情况（包括 LISR、HISR 和任务）。下面则是具体的 CPU 利用率分布情况。其中，每一列的含义如下：

No：序号

5Sec：每一行表示的任务最近 5 秒钟内的 CPU 利用率

1Min：每一行表示的任务最近 1 分钟内的 CPU 利用率

5Min：每一行表示的任务最近 5 分钟内的 CPU 利用率

Process：任务名称

表格的前 2 行比较特殊，分别表示所有 LISR 的 CPU 利用率和所有 HISR 的 CPU 利用率，从第 3 行开始，就表示任务的 CPU 利用率了。最后一行是 idle 线程的 CPU 利用率，跟 Windows 下的“System Idle Process”一样，表示系统的空闲状态。在上面的例子中，idle 线程 5 秒内的 CPU 利用率为 75%，说明当前 CPU 有 75%是处于空闲状态。

7.1.2 配置CPU利用率日志信息触发门限

要手工配置 CPU 利用率日志信息触发门限,可以使用 **cpu-log**，使用该命令可以配置 CPU 利用率日志信息的触发门限。

命令	作用
Ruijie(config)# **cpu-log log-limit** *low_num high_num*	配置 CPU 利用率日志信息触发高门限和触发低门限

默认情况下该高门限为 100%，低门限为 90%。

下面的示例是将 CPU 利用率日志信息触发低门限配置为 70%，高门限配置为 80%。

```
Ruijie# configure terminal                    // 进入全局配置模式
Ruijie(config)# cpu-log log-limit 70 80     //设置 CPU 利用率日志信息触发门限
```

若 CPU 利用率高于 80%将显示如下信息：

```
Oct 20 15:47:01 %SYSCHECK-5-CPU_USING_RATE_LOG: CPU utilization rate in one minute: 95%. rl_con occupied most
CPU utilization rate: 94%.
```

若 CPU 利用率低于 70%将显示如下信息：

```
Oct 20 15:47:01 %SYSCHECK-5-CPU_USING_RATE_LOG: CPU utilization rate in one minute: 68%. rl_con occupied most
CPU utilization rate: 60%.
Oct 20 15:47:01 %SYSCHECK-5-CPU_USING_RATE_LOG: The CPU utilization ratio has been decreased
```

8 系统内存状态查看

8.1 基本系统管理

8.1.1 配置任务列表

显示系统内存使用情况。

8.1.2 查看系统内存使用情况

使用 **show memory** 命令将显示系统总的内存使用情况和内存状态的相关信息。

命令	作用
show memory	查看系统内存使用情况

缺省情况下，设备的名称为 Ruijie。

下面举例显示 **show memory** 运行的结果：

```
Ruijie#show memory
System Memory Statistic:
Free pages:174164
watermarks:min 2012,lower 4024,low 6036,high 9048
System Total Memory:1024MB,Current Free Memory:740580KB
Used Rate:29%
```

上面列表中的信息包含如下：

命令		说明
Free pages		所有区的空闲页总和
watermarks	min	内存极端不足，仅够维持基本的内核运行，到达此水线，所有上层应用模块将不可运行。
	lower	内存严重不足，到达此水线，将有一个上层路由协议自动退出，并释放内存。退出协议的控制参看 **memory-lack exit-policy** 命令。
	low	内存不足，到达此水线，上层路由协议将进入 OVERFLOW 状态，此状态下，路由设备将不再学习新的路由。内存不足时，系统控制台不允许命令执行。
	high	内存充裕，此水线以上，表示系统内存充裕，路由设备各路由协议将尝试从 OVERFLOW 状态恢复到正常状态。
System Total Memory		系统的物理内存总量
System Free Memory		系统总共剩余内存，包括空闲页空间和缓冲池的所有空闲空间
Used Rate		内存使用率

9 系统日志

9.1 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、VTY 等）上或被记录在相关媒介（内存缓冲区、FLASH）上或发送到网络上的一组日志服务器上，供管理员分析网络情况和定位问题。同时为了方便管理员对日志报文的读取和管理，这些日志报文可以被打上时间戳和序号，并按日志信息的优先级进行分级。

锐捷产品的日志报文格式如下：

```
<priority> seq no: timestamp sysname
%ModuleName-severity-MNEMONIC: description
```

其含义依次是：

命令	含义
<priority>	优先级，优先级值＝设备值×8＋严重性
seq no	系统序列号，6 位整型数，可以通过命令关闭该信息的输出
timestamp	时间戳，默认为本地时间。格式定义：Mmm dd hh:mm:ss，其中 Mmm 为月份的英文缩写，1-12 月分别为： Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec
sysname	系统名称，可以通过命令关闭系统名称的输出
ModuleName	功能模块名称缩写
severity	日志严重级别
MNEMONIC	信息简写
description	信息内容

例子：

```
<189> 226:Mar  5 02:09:10 S3250 %SYS-5-CONFIG_I: Configured from console by console
```

在用户窗口打印的日志报文是不带优先级字段的，优先级字段只出现在发送给 Syslog Server 的日志报文中。

9.2 日志配置

9.2.1 日志开关

日志开关默认情况下是打开的，如果关闭日志开关，设备将不会在用户窗口打印日志信息，不会将日志信息发送给 Syslog 服务器，也不会将日志信息记录在相关媒介（内存缓冲区、FLASH）上。

要打开或关闭日志开关，请在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)# **logging on**	打开日志开关
Ruijie(config)# **no logging on**	关闭日志开关

一般情况下，不要关闭日志开关，如果觉得打印的信息太多，则可以通过设置不同设备日志信息的显示级别来减少日志信息的打印。

9.2.2 设置日志信息显示设备

打开日志开关以后，日志信息不仅可以在控制台上显示，也可以发送给不同的显示设备。

要设置接收日志的不同显示设备，请在全局配置模式或特权用户层下执行以下命令：

命令	作用
Ruijie(config)# **buffered** [*buffer-size*] [*level*]	将日志记录到内存缓冲区
Ruijie# **terminal monitor**	允许日志信息显示在 VTY 窗口上
Ruijie(config)# **logging server** *host*	将日志信息发送给网络上的 Syslog Sever
Ruijie(config)# **logging file flash**:*filename* [*max-file-size*] [*level*]	将日志信息记录到扩展 FLASH 上，该命令将在 FLASH 上根据指定的文件名创建文件用于储存日志，文件大小会随日志增加而增加，但其上限以配置的 max-file-size 为准

logging buffered：将日志信息记录到内存缓冲区。日志内存缓冲区是循环使用的，即如果内存缓冲区满以后，最早的日志信息将被覆盖。要显示内存缓冲区中的日志信息，请在特权用户层执行命令 **show logging**。要清除内存缓冲区中的日志信息，请在特权用户层执行命令 **clear logging**。

terminal monitor：允许日志信息在当前 VTY(如 Telnet 窗口)上显示。

logging server *host*：指定接收日志信息的 Syslog Server 地址，锐捷产品允许配置最多 5 个 Syslog Server。日志信息将被同时分给配置的所有的 Syslog Server，也可以使用 logging host 配置达到相同效果。

要将日志信息发送给 Syslog Server，必须打开日志信息的时间戳开关或序号开关，否则日志信息将不会被发给 Syslog Server。

Logging File Flash：将日志信息保存到 FLASH 中，日志文件名不要带文件类型的后缀名。日志文件后缀为固定为 TXT，配置文件后缀名将被拒绝。

More Flash：Filename 命令可以查看 Flash 日志文件的内容。

部分设备支持扩展 FLASH，如果设备存在扩展 FLASH，日志信息将记录在扩展 FLASH 中。如果设备没有扩展 FLASH，日志信息将记录在串行 FLASH 中。

9.2.3 启用日志信息时间戳开关

要在日志信息上添加或取消时间戳，请在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)# **service timestamps** [*message-type* [**uptime** | **datetime** [**msec**] [**year**]]]	启用日志信息中的时间戳

Ruijie(config)# **no service timestamps** [*message-type*]	关闭日志信息中的时间戳

时间戳格式有两种：设备启动时间(**Uptime**)或者设备日期(**Datetime**)。请根据需要选择不同类型的时间戳。

消息类型：Log 或 Debug，Log 信息是指在严重性级别在 0－6 之间的日志信息，Debug 信息是严重性级别为 7 的日志信息。

> 如果当前设备不存在 RTC，缺省采用设备启动时间作为日志信息时间戳，此时配置设备时间无效，如果设备存在 RTC 则缺省采用设备时间作为日志信息时间戳。

9.2.4 启用日志信息系统名开关

默认情况下，日志信息不带系统名。要日志信息加上或取消系统名，请在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)# **no service sysname**	在日志报文中取消系统名。
Ruijie(config)# **service sysname**	在日志报文中添加系统名。

9.2.5 启用日志信息统计功能开关

默认情况下，日志信息统计功能关闭。要打开或者关闭日志信息统计功能，请在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)# **no logging count**	关闭日志信息统计功能，并清除日志信息统计数据。
Ruijie(config)# **logging count**	打开日志信息统计功能。

```
Ruijie# show logging count
Module Name    Message Name      Sev Occur   Last Time
============================================================
LINEPROTO      UPDOWN              5   2       Aug 20 01:41:19
------------------------------------------------------------
LINEPROTO TOTAL                          2
LINK           CHANGED             5   1       Aug 20 01:41:19
------------------------------------------------------------
LINK TOTAL                               1
SYS            CONFIG_I            5   1       Aug 20 01:40:55
------------------------------------------------------------
SYS TOTAL                                1
Ruijie #config
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie (config)#no logging count
Ruijie (config)#end
Ruijie #show logging count
Module Name    Message Name            Sev Occur   Last Time
============================================================
```

9.2.6 启用日志信息序列号开关

默认情况下，日志信息不带序列号。要日志信息加上或取消序列号，请在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)# **no service sequence-numbers**	在日志报文中取消序列号。
Ruijie(config)# **service sequence-numbers**	在日志报文中添加序列号。

日志序列号是一个长整型数值，每添加一条日志，序列号就递增，但是由于序列号只显示 5 位，故当序列号从 1 开始每增加到 100000 或序列号到达 2^32 时候就会发生一次翻转，即序列号又从 00000 开始显示。

9.2.7 设置用户输入与日志信息输出同步

默认情况下，用户输入与日志信息输出不同步，当用户正在输入字符时，如果有日志信息输出，用户输入将被打断，从而影响用户输入。如下所示，用户输入“vlan”后接口 0/12 发生状态改变，打印日志，造成用户忘记之前输入到哪个字符，影响到输入命令的连贯性。

```
Ruijie(config)#vlan Aug 20 16:46:49 %LINK-5-CHANGED: Interface FastEthernet 0/12, changed state to down
Aug 20 16:46:49 %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet 0/12, changed state to DOWN
% Incomplete command.
```

而配置输入同步功能后，即使在用户输入时打印日志，在打印结束后仍然会将用户之前的输入显示出来，从而保证输入的完整性和连贯性，如下所示，用户敲入“vlan”后接口 0/1 发生状态改变，打印日志，打印结束后日志模块会自动把用户已经输入的“vlan”打印出来，使得用户可以继续输入：

```
Ruijie(config)#vlan
*Aug 20 10:05:19: %LINK-5-CHANGED: Interface GigabitEthernet 0/1, changed state to up
*Aug 20 10:05:19: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet 0/1, changed state to up
Ruijie(config)#vlan
```

要设置用户输入与日志信息输出同步，请在线路配置模式下执行以下命令：

命令	作用
Ruijie(config-line)# **logging synchronous**	设置用户输入与日志信息输出同步；
Ruijie(config)# **no logging synchronous**	取消用户输入与日志信息输出同步；

9.2.8 设置日志信息速率控制

默认情况下，日志信息不进行速率控制。当出现大量日志的情况下，若不对日志信息进行速率控制，会对系统造成负担。要进行日志信息速率控制，请在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)# **logging rate-limit** *number*	设置对日志信息进行速率控制
Ruijie(config)# **no logging rate-limit**	取消对日志信息进行速率控制

9.2.9 设置日志信息显示级别

用户可以通过设置允许显示日志信息的严重性级别来实现只查看某个级别以上的日志。

要设置日志信息显示的级别，请在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)# **logging console** [*level*]	设置允许在控制台上显示的日志信息级别
Ruijie(config)# **logging monitor** [*level*]	设置允许在 VTY 窗口(如 telnet 窗口)上显示的日志信息级别
Ruijie(config)# **logging buffered** [*buffer-size*] [*level*]	设置允许记录在内存缓冲区的日志信息级别
Ruijie(config)# **logging file flash**:*filename* [*max-file-size*] [*level*]	设置允许记录在扩展 FLASH 上的日志信息级别
Ruijie(config)# **logging trap** [*level*]	设置允许发送给 Syslog Server 的日志信息级别

锐捷产品的日志信息分为以下 8 个级别：

关键字	等级	描述
Emergencies	0	紧急情况，系统不能正常运行
Alerts	1	需要立即采取措施改正的问题
Critical	2	重要情况
Errors	3	错误信息
warnings	4	警告信息
Notifications	5	普通类型，不过需要关注的重要信息
informational	6	说明性的信息
Debugging	7	调试信息

值越小，级别越高，即 0 级别的信息是最高级别的信息。

当指定设备设置允许显示的日志信息级别以后，所有等于或低于所设置值级别的日志信息将被允许显示。如配置命令 logging console *6* 以后，所有级别为 6 或小于 6 的日志信息将被显示在控制台上。

控制台默认允许显示的日志信息级别为 7。

VTY 窗口默认允许显示的日志信息级别为 7。

默认发送给 Syslog Server 日志信息级别为 6。

默认允许被记录在内存缓冲区的日志信息级别为 7。

默认允许被记录在扩展 FLASH 中日志信息级别为 6。

可以通过特权命令 show logging 来查看允许在不同设备上显示的日志信息级别。

9.2.10 设置日志信息的设备值

设备值是构成发送给 Syslog Server 报文优先级字段的一部分，指示产生信息的设备类型。

要设置日志信息的设备值，请在全局配置模式下执行以下命令：

命令	作用

Ruijie(config)# **logging facility** *facility-type*	设置日志信息的设备值
Ruijie(config)# **no logging facility**	恢复日志信息的设备值为默认值。

下面是各种设备值的含义：

Numerical Code	Facility
0	kernel messages
1	user-level messages
2	mail system
3	system daemons
4	security/authorization messages
5	messages generated internally by syslogd
6	line printer subsystem
7	network news subsystem
8	UUCP subsystem
9	clock daemon
10	security/authorization messages
11	FTP daemon
12	NTP subsystem
13	log audit
14	log alert
15	clock daemon
16	local use 0 (local0)
17	local use 1 (local1)
18	local use 2 (local2)
19	local use 3 (local3)
20	local use 4 (local4)
21	local use 5 (local5)
22	local use 6 (local6)
23	local use 7 (local7)

锐捷产品默认设备值为 23。

9.2.11 设置日志报文的源地址

默认情况下，发送给 Syslog Server 的日志报文源地址为发送报文接口的地址，可以通过命令来固定所有日志报文的源地址。

可以直接设定 Log 报文的源 IP 地址，也可以设定 Log 报文的源端口。

要设置日志报文的源地址，请在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)# **logging source interface** *interface-type interface-number*	设置日志信息的源端口
Ruijie(config)# **logging source** {**ip** *ip-address* | **ipv6** *ipv6-address*}	设置日志报文的源 ip 地址

如果配置了日志报文的源 ip 地址，而设备上所有接口都未配置该地址，那么日志报文的源 ip 地址为该不存在的 ip 地址。实际使用时，应该尽量避免这样的配置。

9.2.12 设置发送用户LOG信息

命令	作用
Ruijie(config)# **logging userinfo**	设置用户登录/退出的 LOG 信息；
Ruijie(config)# **logging userinfo command-log**	设置执行配置命令时，发送 LOG 信息

9.2.13 日志监控

为了监控日志信息，请在特权用户模式下执行以下命令：

命令	作用
Ruijie# **show logging**	查看内存缓冲区中的日志报文，以及日志相关统计信息
Ruijie# **show logging count**	查看系统中各模块日志信息统计情况
Ruijie# **clear logging**	清除内存缓冲区中的日志报文
Ruijie# **more flash**:*filename*	查看扩展 FLASH 中的日志文件

show logging count 命令输出信息中，显示的时间戳格式，是该日志信息最后一次输出时的时间戳格式。

9.3 日志配置举例

以下是配置一个启用日志功能的一个典型例子，设备和日志服务器连接，日志服务器 ip 地址为 192.168.200.2，若希望所有日志都带上时间戳，且所有级别的日志都发送到日志服务器，则可以如下配置：

```
Ruijie(config)# service timestamps debug datetime   //启用 debug 信息时间戳，日期格式
Ruijie(config)# service timestamps log datetime  //启用 log 信息时间戳，日期格式
Ruijie(config)# logging 192.168.200.2    //指定 syslog server 地址
Ruijie(config)# logging trap debugging  //所有级别的日志信息将发给 syslog server
Ruijie(config)# end
```

10 USB 使用

10.1 概述

☑ 10.4（2）及以上的版本才支持使用 URL 访问 U 盘。在此之前的软件版本请使用文件系统挂载路径进行定位和访问，如/mnt/usb0 访问 0 口的 USB 设备。挂载路径在设备插入时提示，或者使用 **show usb** 命令可见。

☑ 在 VSU 模式下时，主机没有 USB 功能而从机有 USB 功能的情况下，主机无法对从机的 USB 设备进行操作，本文介绍的 USB 功能均无法使用。

这里主要介绍 USB 存储设备（主要就是 U 盘）的使用。系统仅识别 FAT 分区的 U 盘，对于其它的文件系统，则无法识别。

在插入 U 盘后，系统会提示发现 U 盘。后续对于此 U 盘的上的文件可以使用 URL 进行定位和访问。如 usb0:/abc/1.txt。

10.2 设备使用的配置

USB 设备的插入无需操作，直接将设备插入 USB 插槽即可。系统找到设备并加载驱动的话，会打印出如下的提示信息。

```
*Jan  1 00:09:42: %USB-5-USB_DISK_FOUND: USB Disk <Mass Storage> has been inserted to USB port 0!
*Jan  1 00:09:42: %USB-5-USB_DISK_PARTITION_MOUNT: Mount usb0 (type:FAT32),size : 1050673152B(1002MB)
```

USB Mass Storage Device 是找到的设备的名称，“usb0：”是指第 1 个 USB 设备。Size 是分区的大小，如上，该 u 盘有 1002MB 的空间。

10.2.1 设备的使用

U 盘的分区加载到系统后，可以直接使用文件系统的命令（dir，copy，del 等）对 U 盘进行操作。如下操作则是将 u 盘的文件复制到 flash。

进入 u 盘分区

```
Ruijie# cd usb0:/
```

将 U 盘上的文件 a.txt 复制到设备上的根目录下。

```
Ruijie# copy usb0:/a.txt  flash:/b.txt
```

这时执行 dir　命令就可以看到设备上已经增加了文件 b.txt。

其他的操作命令参见“文件系统管理”一章。

RGOS 系统只能使用支持标准 SCSI 指令的设备（一般通用的 U 盘），不支持标准 SCSI 指令的设备在系统中无法使用（比如 USB 上网卡附带的 U 盘，附带虚拟 USB 光驱的 U 盘）。

U 盘仅支持 FAT 文件系统，其他文件系统的 U 盘需要在 PC 上格式成 FAT 文件系统后，才能在设备上使用。

- 当 U 盘上有多个分区的时候，在设备上仅能访问第一个 FAT 分区。
- RGOS 不支持 USB 移动硬盘（USB-HDD）。
- U 盘的路径不存在上层目录的概念。通过“cd usbX:\”进入 U 盘后，通过“cd flash:\”返回 flash 文件系统。
- U 盘的使用场景，见各个应用的命令配置指南。（拷贝的案例在 copy 或是 FS 的命令配置指南中；syslog 重定项，在 SYSLOG 模块的命令配置指南中；“指定通过 USB 上的文件启动系统”在多重引导的命令配置指南中）
- 在 CTRL 中 U 盘只为多重引导功能服务，在多重引导的命令配置指南有具体描述。
- 支持使用 URL 访问 U 盘。在此之前的版本请使用路径进行定位和访问。例如:

进入 U 盘分区：

```
Ruijie# cd /mnt/usb0
```

将根目录下的 a.txt 复制到 U 盘上。

```
Ruijie# copy  flash:/a.txt  usb0:/a.txt
```

10.2.2 显示 USB信息

命令	作用
show usb	显示系统 usb 设备信息。

在 CLI 命令模式下，可以使用 **show usb** 查看系统的 USB 信息。显示的信息如下：

```
Ruijie# show usb
Device: Mass Storage:
ID: 0
URL prefix: usb0
Disk Partitions:
usb0(type:FAT32)
Size : 131,072,000B(125MB)
Available size： 1,260,020B (1.2MB)
```

以上信息中，USB Mass Storage Device 是设备的名称。

URL 表示该 U 盘可以使用怎样的前缀访问 U 盘。

Size 表示 U 盘上可访问的空间。

Available size 表示 U 盘上的剩余空间。

10.2.3 卸载USB设备

在拔出 USB 设备之前，需使用 CLI 命令先将设备卸载，以防系统正在使用设备，导致出错。

命令	作用
Ruijie# **usb remove** *Device_ID*	卸载设备号为 *Device_ID* 的 USB 设备。

如上面所示，ID0 代表的是 USB 设备，以下命令可以卸载相应的 USB

```
Ruijie# usb remove 0
```

执行了卸载命令后，系统会打印出：

```
OK, now you can pull out the device 0.
*Jan  1 00:18:16: %USB-5-USB_DISK_REMOVED: USB Disk <Mass Storage> has been removed from USB port 0!
```

这时便可拔出 USB 设备。

有时候，由于系统正在使用设备，导致暂时无法卸载设备，则需等待一定时间后再执行该卸载命令，拔出设备。

一定要先卸载设备后再拔出，以免系统出现错误

10.2.4 USB故障

当打印如下信息：

```
*Jan  2 00:00:39: %USB-3-OHCI_ERR: USB1.0 controller is not available now.
```

这时候，USB 的 1.0 控制器将不可用，但 2.0 的 U 盘依然可用。这种情况下，需要整机复位方可使用对应版本的 U 盘。

当打印信息如下：

```
*Jan  2 00:00:39: %USB-3-EHCI_ERR: USB2.0 controller is not available now.
```

这时候，USB 的 2.0 控制器将不可用，但 1.0 的 U 盘依然可用。这种情况下，需要整机复位方可使用对应版本的 U 盘。

11 集群管理

11.1 集群管理概述

11.1.1 集群定义

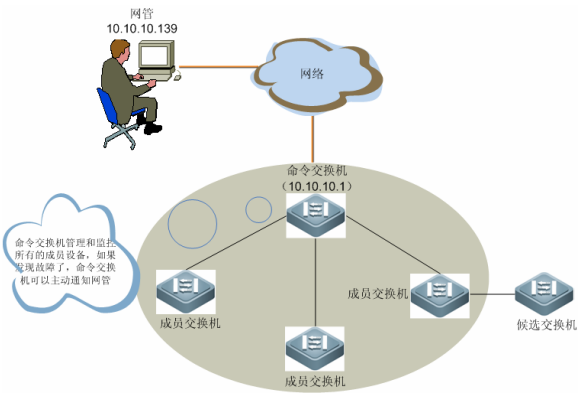
随着网络技术的发展，网络的规模越来越大，设备的数量越来越多，这给网络的管理工作带来了困难。一般，在目前的数字网络环境下，对网络设备的管理主要有两种方式，一是直接到网络设备布放的地点，通过串口直接连接网络设备，对设备进行配置管理；二是通过 SNMP 协议或者使用 Telnet 协议，在远端管理网络设备。

对于第一种方式，优点是管理手段相对简单，而且通过串口直接连接被管设备，不需要配置相应的管理 IP 地址，节省了 IP 资源；主要的问题是当网络设备比较多，配置工作非常繁琐，需要大量的人力物力，维护也比较困难，尤其当网络设备比较分散时，维护人员需要四处奔走，不仅工作量大，而且维护十分不方便。

对于第二种方式，优点是日常维护工作量小，工作人员可以在远端，通过网管终端，或者 Telnet 仿真终端，远程对被管理设备进行维护；主要的问题是需要为每一台被管设备分配一个 IP 地址，目前 IP 地址资源越来越缺乏，当设备数量非常大时，这种管理方式的缺陷显得尤为明显。

集群管理的主要目的就是解决大量分散网络设备的集中管理问题。集群是由一组交换机组成，构成一个统一的管理域（或者广播域），对外提供一个 IP 地址和一个管理接口，并提供对集群每个成员的管理和访问能力。网络管理员只需要在集群中的一个设备配置公网 IP 地址就可以实现对集群中其他设备的管理和维护；配置公网 IP 地址的设备被称为管理设备（或命令设备），其他被管理的设备称为成员设备；一般情况下，成员设备不需要配置公网 IP 地址，管理设备会自动为每一台成员设备分配一个集群编号和私有 IP 地址；这样管理设备与成员设备共同组成集群（私网），管理设备完成公网和私网之间广播域的隔离，屏蔽对私有地址的直接访问，由管理设备对外提供一个管理维护通道，实现了设备的集中、统一管理。典型组网应用如下图所示：

图 11-1 集群管理应用的典型拓扑图



集群管理的优点如下：

- 节省公网 IP；只需要给管理设备分配一个公网 IP 地址；
- 简化配置管理；通过管理设备就可实现对多个成员设备的配置和管理，不需要登录到每个成员设备上进行配置；
- 提供拓扑发现和显示功能，有助于监视和调试网络；

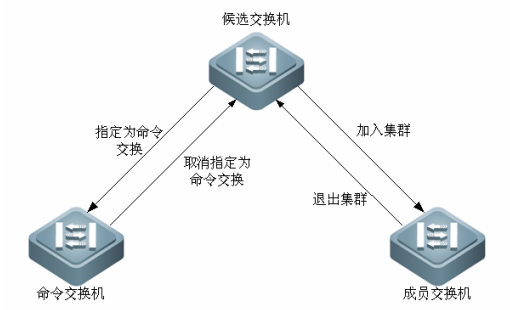
- 集群管理与配置不受网络拓扑结构和距离的限制，具有很大的灵活性。

11.1.2 集群角色

根据各设备在集群中所处的地位和功能不同，形成了不同的角色，用户可以通过配置来指定角色，集群中设备的角色可以分为三种：

- 管理设备（Administrator）：提供对整个集群的管理接口作用的设备，也称为命令设备，它是集群中惟一需要配置公网 IP 地址的设备（同时也会存在一个私网地址和成员设备互通）。对集群中的成员进行配置、管理、监控都必须通过管理设备来进行，管理设备对接收到的配置命令等进行重定向，把它发送到相应的成员设备中。
- 成员设备（Member）：集群中的成员。对成员设备的管理是通过管理设备代理完成，它可以不设置公网 IP 地址。
- 候选设备（Candidate）：指未加入任何集群管理、且具有集群能力的设备。

图 11-2 集群角色切换规则



三种角色的切换规则如图所示，说明如下：

- 用户在候选设备上创建集群的同时，将当前候选设备指定为集群管理设备。每一个集群必须指定一个（且只能指定一个）管理设备。管理设备被指定后，通过收集相关信息，发现和确定候选设备，并自动将候选设备加入集群中。
- 候选设备给加入集群后，成为成员设备。
- 集群内的成员设备被删除后将恢复为候选设备。
- 管理设备只有在删除集群时才能恢复为候选设备。

11.1.3 集群工作原理

集群管理由以下两个协议组成：

- LLDP 协议（Link Layer Discovery Protocol，链路层发现协议）
- Cluster（集群管理协议）

集群通过以上两个协议，对集群内部的设备进行配置和管理。其中 LLDP 协议遵循 IEEE 802.1AB-2005 标准。

集群的工作过程包括邻居发现、拓扑收集以及集群的建立与维护；拓扑收集过程和集群维护过程相对独立，工作原理如下所述：

- 所有设备通过 LLDP 协议来获取邻居设备的信息，包括邻居设备的 MAC 地址、端口信息等。

- 管理设备通过 LLDP 协议的私有属性来收集用户指定跳数范围内的设备信息以及各个设备的连接情况，并从收集到的拓扑信息中确定集群的候选设备和拓扑结构。

- 管理设备根据收集到的候选设备信息完成将候选设备加入集群、成员设备离开集群的操作。

1) LLDP 协议简介

LLDP 协议由链路层提供，能够发现邻居的设备信息，包括设备的端口信息、MAC 地址信息等。LLDP 协议本身只能发现一跳以内直接相连的邻居信息，集群管理可以利用 LLDP 协议的邻居信息来组织拓扑，以及利用 LLDP 报文中的厂商私有属性来传递集群信息。因此邻居发现是 LLDP 协议模块的功能，集群管理和拓扑收集都依赖于 LLDP 模块。

有关 LLDP 的配置，具体详见“LLDP”中相关的章节。

管理设备利用 LLDP 报文的私有属性进行拓扑收集，在一定网络范围内收集每个设备的信息以及设备间的连接情况，从而获取到集群的候选设备信息。

管理设备可以定时在网络内进行拓扑收集，用户也可以通过手工配置命令启动一次拓扑收集。管理设备收集拓扑信息过程如下：

- 管理设备从使能 LLDP 功能的端口定时发送拓扑收集请求报文

- 收到请求报文的设备立即发送拓扑响应报文至管理设备，复制此请求报文并发送到邻居设备；拓扑响应报文包含本设备的基本信息和所有邻接设备的信息

- 邻接设备收到请求报文后将执行同样操作，直至拓扑收集请求报文扩散到指定跳数范围内的所有设备

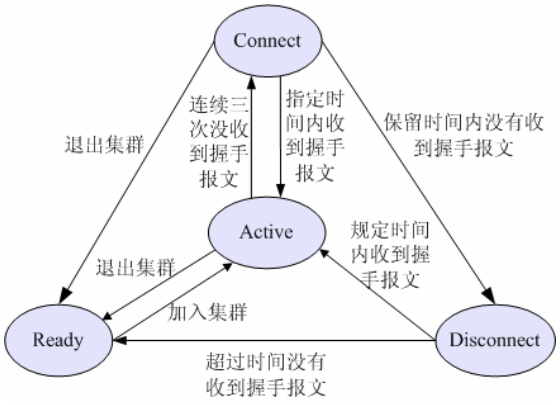
2) 集群管理维护

- 将候选设备加入集群：用户在建立集群前首先指定管理设备，管理设备通过 LLDP 协议发现和确定候选设备，将候选设备自动加入集群，用户也可以通过手工配置将候选设备加入到集群中。候选设备加入集群后，将获得管理设备为它分配的集群编号 SN、集群管理使用的私有 IP 地址等。

- 成员设备退出集群：设备加入集群后，管理设备可以对其进行管理与配置；用户可以手动删除成员设备、添加黑名单、为成员设备指定不同的管理设备、关闭成员设备的集群功能等操作使成员设备退出集群变成候选设备。

- 集群内部通讯：在集群内部，管理设备与成员设备通过握手报文进行实时通信，以维护他们之间的连接状态，管理设备和成员设备的连接状态如图所示：

图 11-3 管理设备与成员设备的连接状态



1) 候选设备加入集群成为成员设备后，状态从 Ready 迁移至 Active；成员设备定时发送握手报文给管理设备，管理设备收到成员设备的握手报文后，做出应答，将成员设备保持为 Active；成员设备收到握手应答后，也将自身状态保持为 Active。

2) 若管理设备在三倍握手报文发送时间间隔内没有收到成员设备发送的握手报文，则将成员设备状态从 Active 迁移至 Connect；同样的，若成员设备三倍握手报文发送时间间隔内没有收到管理设备发送的握手应答，将自身状态从 Active 迁移至 Connect。

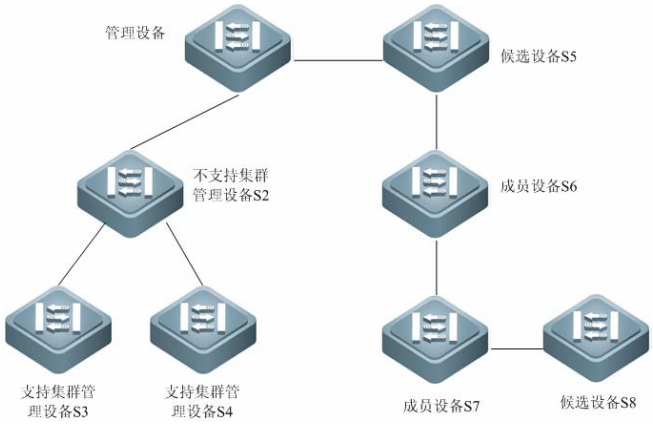
3) 若管理设备在有效保留时间内收到成员设备发送的握手报文，则将成员设备的状态迁移回 Active，否则将其迁移至 Disconnect；处于 Connect 状态的成员设备若在有效保留时间内收到管理设备发送的握手应答后，将其自身状态迁移回 Active，否则将其迁移至 Disconnect。

4) 当被中断的通信恢复时，管理设备和成员设备进行恢复过程，恢复成功后，成员设备在管理设备以及本地的状态都将恢复为 Active；如果超过时间没有收到恢复报文，管理设备将该成员设备退出集群，成员设备本身也将其自己的状态恢复为候选设备角色，即 Ready 状态。

- 集群管理资源：集群管理资源包括管理 VLAN 和管理 IP 地址池。管理 VLAN 限制集群管理的范围，提高安全性，默认在创建集群时，会从指定的 VLAN 2049-3000 范围内自动获取一个空闲管理 VLAN，从指定的私有 IP 地址池 192.168.168.0/24-192.168.254.0/24 范围内获取一个空闲管理 IP 地址池；在退出集群时，会将该管理 VLAN 和管理 IP 删除。

- 集群管理范围：管理设备借助 LLDP 协议来发现其他设备，因此，不支持该链路协议（或者关闭 LLDP 功能）的设备无法被发现，并且与之相连的其他设备也无法被发现。每台设备到管理设备之间经过了多少设备，这个称为拓扑跳数，管理设备只能发现并管理在有限拓扑跳数之内的设备，这个也称为集群范围。从集群管理设备开始，最多可以发现 16 跳以内的设备（默认只发现 5 跳）。集群管理范围如图所示

图 11-4 拓扑发现的跳数



假设当前的发现跳数是 3，则 S5、S6、S7 都能被发现，它们都在 3 跳范围之内；S8 则不能被发现，因为它距离管理设备的跳数已经超过 3。S2 不支持集群功能，不能被管理设备识别，S3 和 S4 虽然也在 3 跳之内并且也支持集群功能 ，但是由于 S2 不支持集群，因此这两台设备也不能被发现。

- 零配置即插即用：新安装的（支持集群功能的）设备，默认已经打开了 LLDP 功能和集群功能，因此不需要进行任何配置，就可以被管理设备发现，管理设备能自动将其加入集群并对其进行管理。

管理设备添加成员设备过程、管理设备与成员设备内部的握手报文都是基于 UDP 协议通信，因此，如果 UDP 协议在集群管理 SVI 接口 PING 不通，管理设备添加成员设备会失败，并给出 udp unreachable 的日志提示。

11.1.4 集群管理VLAN

管理 VLAN 能限制集群管理的范围，通过配置管理 VLAN，可实现如下功能：

- 集群的管理报文（不包括 LLDP 报文）都将限制在管理 VLAN 内，与其他报文隔离，增加了安全性。
- 管理设备和成员设备通过管理 VLAN 实现内部通讯。

集群管理提供管理 VLAN 自协商修改机制。集群在建立后，在拓扑收集的过程中，会判断管理设备和成员/候选设备相连的端口是否允许管理 VLAN 通过；因此，如果端口不允许管理 VLAN 通过时：

- 当端口是 access 模式，集群会将端口改成 trunk 模式，同时配置 Native Vlan 与 PVID 相等；
- 当端口是 trunk 模式，管理 VLAN 不在许可列表中，集群会将管理 VLAN 加入端口的带 tagged 的 VLAN 许可列表中；
- 当端口是 hybrid 模式，管理 VLAN 不在许可列表中，集群会将管理 VLAN 加入端口的带 tagged 的 VLAN 许可列表中。

11.1.5 集群应用

为了便于集群识别，成员设备和管理设备的命令提示符增加集群前缀，前缀形式为“集群名称_N.”，其中 N 为该设备的集群编号。

1) 集群内部成员互访

集群命令设备和成员设备可以直接通过 **cluster login** 互相登陆。即可以在管理设备上切换到指定的成员设备操作界面上对该成员设备进行配置管理；也可以从成员设备操作界面切换到管理设备操作界面上对管理设备进行管理。管理设备登陆到成员设备时，直接进入特权模式；成员设备登陆到管理设备，默认进入的是用户模式，只有经过管理设备的本地口令验证才能进入特权模式。

> 集群 **cluster login** 是使用 Telnet 进行连接，因此执行切换前，对端设备需要执行” enable service telnet-server”使能 telnet 功能，否则将导致切换失败。

2) TFTP 代理

只要在管理设备上设置了共用的 TFTP 服务器，成员设备就可以通过管理设备 TFTP 代理功能从 TFTP 服务器上下载文件，或者向 TFTP 服务器上传文件。

> 有关 TFTP 的配置，具体详见“系统升级维护配置”中“通过 TFTP 协议传输文件”章节。
>
> 管理设备同时只能为一个成员设备提供 TFTP 传输代理服务，其他成员设备必须等待前一个成员设备 TFTP 传输完毕才能进行代理传输。

3) SNMP 代理

只要在管理设备上设置了 SNMP Agent，网络上的管理工作站就可以使用管理设备的公网 IP 地址，通过 SNMP 访问整个集群，无需为每个成员设备进行 SNMP Agent 设置。管理工作站将 SNMP 请求发送给管理设备，管理设备将识别这个请求，转到相应的成员设备上，并将成员设备的响应信息转给管理工作站。管理设备是通过 Community 或者用户名加入后缀来识别成员，具体如下：

- 当使用 SNMPv1 和 SNMPv2 时，管理工作站在 SNMP 报文的 Commnunity 中增加后缀（@esN，其中 N 为成员设备编号），可以指定访问集群中的成员设备；

- 当使用 SNMPv3 时，管理工作站在 SNMP 报文的用户名中增加后缀（@esN，其中 N 为成员设备编号），可以指定访问集群中的成员设备；

有关 SNMP Agent 的配置，具体详见“SNMP”中相关的章节。

4) Trap 代理

只要在管理设备上设置了接收 Trap 的主机（即管理工作站），成员设备就可以通过管理设备代理向管理工作站发送 Trap：

- 当使用 SNMPv1 和 SNMPv2 时，成员设备在 Trap 报文中的 Community 中增加后缀（@esN，其中 N 为成员设备编号）；
- 当使用 SNMPv3 时，成员设备在 Trap 报文中用户名中增加后缀（@esN，其中 N 为成员设备编号），可以指定访问集群中的成员设备；

有关 SNMP Trap 的配置，具体详见“SNMP”中相关的章节。

5) Syslog 代理

只要在管理设备上设置了接收日志的主机（即 Syslog Server），成员设备就可以通过管理设备代理向管理工作站发送日志。同时，管理设备默认配置 service sysname，在打印 syslog 时，会在设备主机名前增加前缀，前缀形式为：“集群名称_N.”，其中 N 为该设备的集群编号。

有关 Syslog 的配置，具体详见“系统日志”中相关的章节。

管理设备会定时将其自身相关的 Log 配置命令同步到所有成员设备中。

11.2 配置管理设备

11.2.1 缺省配置

下表用来描述集群管理设备的缺省配置。

功能特性	缺省值
集群功能	默认打开
集群成员状态	默认是候选设备
集群自动添加功能	默认打开
集群拓扑收集的范围	默认为 5 跳
集群 timer 值	默认为 60 秒
集群 timer-hello 值	默认为 30 秒
集群 timer-hold 值	默认为 90 秒

11.2.2 配置任务简介

集群管理设备配置任务简介

步骤	配置任务	说明

1	使能设备和端口的 LLDP 功能	“必选”，缺省情况下，LLDP 功能是打开。
2	使能设备的集群功能	“必选”，缺省情况下，集群功能是打开。
3	启动设备的集群功能	“必选”
4	拓扑发现相关参数	“可选”，用户需要改变低拓扑收集的收敛性或改变拓扑收集范围时，需要配置。
5	集群参数	“必选”
6	集群内外交互	“可选”，在需要使用集群代理功能时，需要进行相关配置。

11.2.3 打开/关闭设备或接口的LLDP功能

缺省配置下设备的 LLDP 功能是打开的，如果想要关闭 LLDP 功能，按如下步骤进行配置：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **no lldp enable**	关闭设备 LLDP 功能。
Ruijie(config)# **end**	回到特权模式。

缺省配置下设备的接口 LLDP 功能是打开的，如果想要关闭接口 LLDP 功能，按如下步骤进行配置：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **interface** *gigabitethernet 0/1*	进入接口模式
Ruijie(config-GigabitEthernet 0/1)# **no lldp enable**	关闭设备接口的 LLDP 功能。
Ruijie(config-GigabitEthernet 0/1)# **end**	回到特权模式。

配置举例：

#关闭全局和接口的 LLDP 功能开关。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# no lldp enable
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-GigabitEthernet 0/1)# no lldp enable
```

11.2.4 打开/关闭集群功能

缺省配置下集群功能是打开的，如果想要关闭集群功能，按如下步骤进行配置：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **no cluster enable**	关闭集群管理功能。
Ruijie(config)# **end**	回到特权模式。

如果是管理设备，关闭集群功能将删除集群和相关配置。如果是成员设备，关闭集群功能将使之退出集群。

如果是候选设备，关闭集群功能将使之不再能成为任何集群的成员设备。

如果需要重新打开集群功能，在全局配置模式下，执行 **cluster enable** 命令。

配置举例：

关闭设备上的集群管理功能。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# no cluster enable
```

11.2.5 建立或删除集群

一个集群只能有一个管理设备；在设备上建立集群，同时使该设备成为集群的管理设备。如果想要建立集群，按如下步骤进行配置：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **cluster** [*name*]	在设备上建立集群，并将该设备设置为管理设备，集群编号为 1，并进入集群配置模式。 *name*：集群的名字，未配置默认是 CLUSTER。
name_1.Ruijie(config-cluster)# **end**	回到特权模式。
name_1.Ruijie# **show cluster**	验证配置。

集群已经建立，若要删除集群，可以在全局配置模式下执行 **no cluster** 命令。只有管理设备才能够删除集群。

配置举例：

建立一个集群，名称为 clus0：

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# cluster clus0
```

11.2.6 配置拓扑收集参数

集群建立后，管理设备默认会每隔 60s 进行一次拓扑收集，收集范围默认是 5 跳；如果想要修改拓扑收集参数，用户可以按照以下步骤进行配置：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **cluster** *clus*	进入集群模式
clus_1.Ruijie(config-cluster)#**timer** *topo-seconds*	配置拓扑收集时间间隔；默认 60s *topo-seconds*：拓扑收集 timer 时间，范围是 10-300，单位秒。
clus_1.Ruijie(config-cluster)# **hops-limit** *hop-number*	配置拓扑收集范围；默认 5 跳 *hop-number*：集群发现设备的范围（跳数），范围 1-16
clus_1.Ruijie(config-cluster)#**end**	回到特权模式。
clus_1.Ruijie# **show cluster**	验证配置。

配置举例：

修改拓扑收集时间间隔为 30s，同时拓扑收集范围为 7 跳

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# cluster clus0
clus_1.Ruijie(config-cluster)#timer 30
clus_1.Ruijie(config-cluster)#hops-limit 7
```

11.2.7 手动拓扑收集

当集群拓扑发生变化后，用户可以手动进行一次拓扑收集，获取到最新的拓扑信息，操作步骤如下：

命令	作用
clus_1.Ruijie# **cluster explore**	手动进行拓扑收集

配置举例：

手动指定管理设备立即进行拓扑收集

```
Ruijie# cluster explore
```

11.2.8 增加或删除成员设备

集群添加成员设备有两种方式：自动添加和手动添加。

集群在建立时，自动添加功能默认是打开的，管理设备能将发现的所有候选设备加入集群；如果需要关闭自动添加功能，可按以下步骤进行配置：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **cluster** clus	进入集群配置模式。
clus_1.Ruijie(config-cluster)# **no member auto-add**	关闭集群自动添加功能
clus_1.Ruijie(config-cluster)# **end**	回到特权模式。

在关闭自动添加功能时，会询问是否要将当前的所有动态成员设备转为静态成员；用户如果选择 YES，转为静态成员；选择 NO 或者输入其他字符，将删除当前所有的动态成员设备。

用户还可以通过手动添加成员设备、将成员设备从动态添加转为静态添加或者改变成员设备的集群编号 SN；这些功能都通过 **member add** 来实现。增加成员设备按如下步骤进行配置：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **cluster** clus	进入集群配置模式。

clus_1.Ruijie(config-cluster)# **member add** [*member-id*] **mac-address** *H.H.H*	将一个候选设备添加为成员设备；可以为其指定一个集群编号。 *member-id*：成员设备在集群中的编号，未配置集群会分配一个空闲编号。当集群管理 ip 的掩码长度小于等于 24 位时，编号范围是 2-240；当掩码长度大于 24 位时，比如 255.255.255.128，扣除全 0、全 1 和管理设备 ip，成员设备可分配 ip 范围是 2-126，则编号范围是 2-126。 *H.H.H*：要添加的设备 MAC 地址。
clus_1.Ruijie(config-cluster)# **end**	回到特权模式。
clus_1.Ruijie# **show cluster members**	查看集群成员，验证配置。

若要删除一个静态成员设备，可以在全局配置模式下执行命令 **no member add** *member-id*。该命令只能在管理设备上执行。

配置举例：

关闭自动添加功能，并将 MAC 地址为 00d0.f8fe.1007 的设备加入集群 clus，并指定其集群编号为 2。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# cluster clus
clus_1.Ruijie(config-cluster)#no member auto-add
clus_1.Ruijie(config-cluster)#member add 2 mac-address 00d0.f8fe.1007
```

11.2.9 配置集群管理资源

建立集群时，设备会默认为集群配置管理资源；从指定的 VLAN 2049-3000 范围内自动获取一个空闲管理 VLAN，从指定的 IP 地址池 192.168.168.0/24-192.168.254.0/24 范围内获取一个空闲管理 IP 地址池。建立集群后，执行该命令可以手动为管理设备配置新集群管理资源；使用该命令的 **no** 选项将集群管理资源恢复为默认值；可以通过以下步骤来完成：

命令	作用
clus_1.Ruijie# **configure terminal**	进入全局配置模式。
clus_1.Ruijie(config)# **cluster**	进入集群配置模式。
clus_1.Ruijie(config-cluster)# **management** { **vlan** *vlan-id* | **ip-pool** *ip-address ip-mask* | **vlan** *vlan-id* **ip-pool** *ip-address ip-mask* }	配置集群管理资源。 *vlan-id*: 集群管理 VLAN ID，范围是 1-4094。 *ip-address:* 集群管理 IP。 *ip-mask:* 集群管理 IP 地址池掩码。
clus_1.Ruijie(config-cluster)#**exit**	回到配置模式。
clus_1.Ruijie (config)# **end**	回到特权模式。
clus_1.Ruijie # **show cluster**	验证配置。

该命令会先删除集群，在按照新的管理 VLAN 和新的管理 IP 地址池重建集群，因此会造成震荡，建议用户一旦指定了管理资源就不要随意改变。

配置举例：

#下面的命令配置一个集群管理 VLAN 为 3333，管理 IP 地址池为 10.10.10.0 255.255.255.128。

```
clus_1.Ruijie# configure terminal                    //在管理设备的命令行界面执行
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
clus_1.Ruijie(config)# cluster
clus_1.Ruijie(config-cluster)# management vlan 3333 ip-pool 10.10.10.0 255.255.255.128
```

11.2.10 配置集群定时器

集群定时器设置包括握手报文定时发送的时间间隔和设备信息保留时间；握手报文是管理设备和成员设备的心跳包，维护管理设备和成员设备的连接通道；设备保留时间是当管理设备和成员设备连接通道异常时，成员设备信息在管理设备和其本身的保留时间。用户要修改定时器默认值，可以通过以下步骤来完成：

命令	作用
clus_1.Ruijie# **configure terminal**	进入全局配置模式。
clus_1.Ruijie(config)# **cluster**	进入集群配置模式。
clus_1.Ruijie(config-cluster)#**timer hold** *hold-seconds*	设置拓扑请求报文保留时间 timer-hold 值，范围是 10-300，单位秒，默认为 90 秒。
clus_1.Ruijie(config-cluster)#**timer hello** *hello-seconds*	设置成员设备状态更新时间 timer-hello 值，范围 10-300，单位为秒，默认为 30。
clus_1.Ruijie(config-cluster)#**exit**	回到配置模式。
clus_1.Ruijie (config)# **end**	回到特权模式。
clus_1.Ruijie # **show cluster**	验证配置。

配置集群定时器功能只能在管理设备上执行。使用该命令的 **no** 选项将恢复为缺省值。

配置举例：

管理设备上配置集群定时器时间。

```
clus_1.Ruijie# configure terminal                    //在管理设备的命令行界面执行
Enter configuration commands, one per line.  End with CNTL/Z.
clus_1.Ruijie(config)# cluster
clus_1.Ruijie(config-cluster)# timer hold  95        //设置信息保存时间为 95 秒
clus_1.Ruijie(config-cluster)# timer hello 30        //设置成员设备状态更新间隔时间为 30 秒
```

11.2.11 配置集群鉴权密码

管理设备添加成员设备支持鉴权方式和非鉴权方式。当候选设备配置了静态口令时，管理设备在添加成员设备采用鉴权方式；当候选设备没有配置静态口令，管理设备采用非鉴权方式添加。因此为了鉴权能通过，用户需要为管理设备配置全局鉴权密码池或者为指定的设备配置单机鉴权密码。可以通过以下步骤来完成：

命令	作用
clus_1.Ruijie# **configure terminal**	进入全局配置模式。
clus_1.Ruijie(config)# **cluster**	进入集群配置模式。

clus_1.Ruijie(config-cluster)# **member password** { *password-id* **|** *H.H.H* } { *password* **|** *encryption-type encrypted-password* }	配置鉴权密码。 *password-id:* 集群管理的密码编号 *H.H.H:* 设备 MAC 地址 *password:* 明文密码 *encryption-type:* 鉴权密码加密方式 (0 表示未加密形式，7 表示加密形式) *encrypted-password:* 指定加密方式后的鉴权密码。
clus_1.Ruijie(config-cluster)#**end**	回到特权模式。
clus_1.Ruijie # **show run**	验证配置。

集群鉴权不支持安全口令；即当用户配置了安全口令，但没有配置静态口令，管理设备仍采用非鉴权方式添加成员设备。

鉴权顺序为： **member password** *H.H.H*（单机密码）---》**member password** *password-id*（全局密码或密码池）、管理设备本身的密码（特指静态口令）、空密码；只有所有密码鉴权都失败后，候选设备才会添加失败。

配置举例：

MAC 地址为 00d0.f8fe.1007 的设备，鉴权密码配置为明文密码 aaa。

```
clus_1.Ruijie# configure terminal                    //在管理设备的命令行界面执行
Enter configuration commands, one per line.  End with CNTL/Z.
clus_1.Ruijie(config)# cluster
clus_1.Ruijie(config-cluster)# member password 00d0.f8fe.1007 aaa
```

#将明文密码 bbb 添加到集群鉴权密码池，并为其指定密码池编号为 12。

```
clus_1.Ruijie# configure terminal                    //在管理设备的命令行界面执行
Enter configuration commands, one per line.  End with CNTL/Z.
clus_1.Ruijie(config)# cluster
clus_1.Ruijie(config-cluster)# member password 12 bbb
```

11.2.12 配置集群黑名单

为保证集群的稳定性和安全性，用户可以使用黑名单的方式对加入集群的设备进行限制。将被限制设备的 MAC 地址添加到黑名单后，即使该设备已经启动集群功能，且正常连接到现有集群中，其设备本身和下联设备都无法加入到集群中参与集群的统一管理与配置。黑名单添加可以通过以下步骤来完成：

命令	作用
clus_1.Ruijie# **configure terminal**	进入全局配置模式。
clus_1.Ruijie(config)# **cluster**	进入集群配置模式。
clus_1.Ruijie(config-cluster)# **member black-list** *H.H.H*	将指定设备添加到集群黑名单中。 *H.H.H*：需要添加到黑名单内的设备 MAC 地址。
clus_1.Ruijie(config-cluster)#**end**	回到特权模式。
clus_1.Ruijie # **show cluster black-list**	验证配置。

通过此命令的 **no** 选项可以删除黑名单；当指定 *H.H.H* 时表示删除指定黑名单，否则删除所有黑名单。设备从黑名单中删除后，后续可以继续加入集群，成为成员设备。

配置举例：

管理设备上配置集群黑名单。将 MAC 地址为 0010-3500-e001 的设备添加到黑名单中。

```
clus_1.Ruijie# configure terminal                    //在管理设备的命令行界面执行
Enter configuration commands, one per line.  End with CNTL/Z.
clus_1.Ruijie(config)# cluster
clus_1.Ruijie(config-cluster)#member black-list 0010-3500-e001
```

#释放当前集群黑名单中的所有设备。

```
clus_1.Ruijie# configure terminal                    //在管理设备的命令行界面执行
Enter configuration commands, one per line.  End with CNTL/Z.
clus_1.Ruijie(config)# cluster
clus_1.Ruijie(config-cluster) # no member black-list
```

11.2.13 集群内操作

集群提供 **cluster login** 命令，允许管理设备直接登录到指定成员设备、或从成员设备登录到管理设备上。

如果由于某些错误的配置造成成员设备发生故障时，可以利用管理设备指定该台成员设备重启，通过 **cluster reload** 命令实现。通过以下步骤来完成：

命令	作用
clus_1.Ruijie# **cluster login** { **administrator** | **member** {*member-id* | *H.H.H* } }	从管理设备登录到一台成员设备，或从成员设备登录到管理设备。 *member-id*：成员设备的集群编号。 **administrator**：由成员设备登录到管理设备。 *H.H.H*：要登录的成员设备 MAC 地址。
clus_1.Ruijie#**cluster reload member** { *member-id* | *H.H.H* }	重启成员设备。 *member-id*：要重启的成员设备的集群编号。 *H.H.H*：要重启的成员设备的 MAC 地址。

如果要从被登录的设备上返回，请在特权模式下执行 **exit** 命令。

配置举例：

从管理设备登录到成员设备 2 上去。

```
clus_1.Ruijie# cluster login member 2
clus_2.Ruijie#             //进入成员设备的命令行界面
clus_2.Ruijie# exit       //退出成员设备的命令行界面
clus_1.Ruijie#
```

管理设备登录指定成员设备 3 重启。

```
clus_1.Ruijie# cluster reload member 3
```

11.2.14 配置集群内外交互

集群建立后，可以在管理设备上为集群统一配置 TFTP 服务器、网管主机和日志主机。

- 为集群统一配置 TFTP 服务器后，集群内部成员设备就可以通过管理设备的 TFTP 代理来访问 TFTP 服务器。
- 为集群统一配置日志主机后，集群内部成员设备的所有日志信息都将输出到配置的日志主机上
- 为集群统一配置网管主机后，集群内部成员设备通过管理设备向公用的 SNMP 网管站发送 Trap 信息。

具体配置可以参照如下步骤：

命令	作用
clus_1.Ruijie# **configure terminal**	进入全局配置模式。
clus_1.Ruijie(config)# **log server** *ip*	配置日志主机地址
clus_1.Ruijie(config)# **log trap**	允许管理设备向日志主机发送日志信息
clus_1.Ruijie(config)# **snmp-server community** *public* **rw**	指定 SNMP 团体的访问字符
clus_1.Ruijie(config)# **snmp-server enable traps**	启用 SNMP 主动给 NMS 发送 Trap 消息
clus_1.Ruijie(config)# **snmp-server host** *host-addr*	指定发送 Trap 的 SNMP 主机（NMS）
clus_1.Ruijie(config)# **cluster**	进入集群配置模式。
clus_1.Ruijie(config-cluster)# **proxy tftp-server** *ip-address*	设置集群共用的 TFTP 服务器。 *ip-address*：集群共用 TFTP 服务器地址（IPv4）。
clus_1.Ruijie(config-cluster)# **exit**	回到配置模式
clus_1.Ruijie (config)# **exit**	回到特权模式。
clus_1.Ruijie# **cluster login member** 2	登录到成员设备 2
clus_2.Ruijie# **cluster tftp server:** *source-file* **flash:** [*destination-file*]	成员设备 2 从 TFTP 服务器下载文件到本地。 *source-file*：需要传输的源文件，在远程 TFTP 服务器上； *destination-file*：传输的目的文件，在本地 FLASH 上，如果没有指定，则使用源文件名作为目的文件名；
clus_2.Ruijie# **cluster tftp flash:***source-file* **server:** [*destination-file*]	成员设备 2 从本地上传文件到 TFTP 服务器。 *source-file*：需要传输的源文件，在本地 FLASH 上； *destination-file*：传输的目的文件，在远程 TFTP 服务器上，如果没有指定，则使用源文件名作为目的文件名。

配置举例：

管理设备设置集群共用的 TFTP 服务器为 172.10.1.1。然后进入成员设备 2，使用集群共用的 TFTP 服务器传输 config.text 文件到本地。

```
clus_1.Ruijie# configure terminal                                    //在管理设备的命令行界面执行
Enter configuration commands, one per line.  End with CNTL/Z.
clus_1.Ruijie(config)# cluster
clus_1.Ruijie(config-cluster)# proxy tftp-server 172.10.1.1
clus_1.Ruijie(config-cluster)#exit
clus_1.Ruijie(config)#exit
clus_1.Ruijie# cluster login member 2                                 //登录到成员设备 2 的命令行界面
clus_2.Ruijie# cluster tftp server://config.text flash:config.text    //使用集群 TFTP 代理
```

11.3 配置成员设备

11.3.1 配置任务简介

集群成员设备配置任务简介

步骤	配置任务	说明
1	使能设备和端口的 LLDP 功能	“必选”，缺省情况下，LLDP 功能是打开。
2	使能设备的集群功能	“必选”，缺省情况下，集群功能是打开。
3	指定管理设备	“可选”，当需要该设备被指定集群进行管理时，需要配置集群名称或者管理设备的 MAC 地址。
4	集群内外交互	“可选”，可使用集群代理功能，进行相关操作。

11.3.2 配置成员设备的管理设备信息

指定成员设备可被管理的集群信息。指定集群信息按如下步骤进行配置：

命令	作用
clus_2.Ruijie# **configure terminal**	进入全局配置模式。
clus_2.Ruijie(config)# **cluster member** { **cluster-name** *name* | **admin-address** *H.H.H* }	指定可以管理该设备的集群名称或者管理设备 MAC 地址。 *name*：集群名称。 *H.H.H*：管理设备的 MAC 地址。
Ruijie(config)# **end**	回到特权模式。

执行 **no cluster member** 则删除相关信息，设备可以被任意集群加入。

如果设备是成员设备，执行该命令时，如果指定的集群与当前加入的集群不一致，则设备会退出集群变成候选设备。

配置举例：

指定管理成员设备的集群名称是 cluster。

```
clus_2.Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
clus_2.Ruijie(config)#cluster member cluster-name cluster
Ruijie#                                  //成员设备 2 变成了候选设备
```

11.4 配置候选设备

11.4.1 配置任务简介

集群候选设备配置任务简介

步骤	配置任务	说明

1	使能设备和端口的 LLDP 功能	“必选”，缺省情况下，LLDP 功能是打开。
2	使能设备的集群功能	“可选”，当不需要候选设备被集群管理时，可以关闭集群功能。
5	指定管理设备	“可选”，当需要该设备被指定集群进行管理时，需要配置集群名称或者管理设备的 MAC 地址。

11.4.2 配置候选设备的管理设备信息

指定候选设备可被管理的集群信息。指定集群信息按如下步骤进行配置：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **cluster member** { **cluster-name** *name* | **admin-address** *H.H.H* }	指定可以管理该设备的集群名称或者管理设备 MAC 地址。 *name*：集群名称。 *H.H.H*：管理设备的 MAC 地址。
Ruijie(config)# **end**	回到特权模式。

执行 **no cluster member** 则删除相关信息，设备可以被任意集群加入。

如果管理设备信息后，候选设备不会主动加入集群成为成员设备，添加过程必须有管理设备主动发起。

配置举例：

指定管理候选设备的集群名称是 cluster。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#cluster member cluster-name cluster
```

11.5 监视与维护

11.5.1 查看集群的配置和状态

在特权模式下，可以使用下表所列的命令来显示关于集群的各种信息：

命令	作用
show cluster	显示设备所属集群的基本信息。
show cluster members [*member-id* | **detail**]	显示成员设备的信息，在管理设备上将显示所有成员信息，在成员设备上只能显示自己和管理设备的信息。 *member-id*：成员设备在集群中的编号。
show cluster candidates [**detail** | *H.H.H*]	显示候选设备的信息，只有在管理设备上才能显示信息。 *H.H.H*：候选设备的 MAC 地址。
show cluster topology [*H.H.H* | *member-id*]	显示集群的拓扑信息。 *H.H.H*：集群设备的 MAC 地址。 *member-id*：成员设备在集群中的编号。

show cluster black-list	显示所有黑名单信息。

配置举例：

显示设备所属集群的基本配置信息。

```
clus_1.Ruijie#show cluster
Cluster:                        CLUSTER <Administrator>
Member-id:                      1
Administrator mac address:      00d0.f822.33ac
Administrator name:             Ruijie
Management vlan:                2056
Management ip:                  192.168.176.1
Management ip-pool:             192.168.176.0/24
Total number of members:        2
Status:                         0 members are unreachable
Run time:                       0 days, 1 hours, 5 minutes, 37 seconds
Timer:                          60 seconds
Timer hello:                    30 seconds
Timer hold:                     90 seconds
Hops-limit:                     5
Proxy tftp-server:              Not configured!
```

显示成员设备的信息

```
clus_1.Ruijie# show cluster member
SN          MAC         Name        Hops State    LcPort     UpSN       UpMAC      UpPort
---- -------------- ----------- ---- -------- ---------- ---- -------------- ---------
1    00d0.f8fe.1007 switch-1       0    <Admin>
2    00d0.f8fe.43d2 switch-2       1    up       Fa0/2      1    00d0.f8fe.1007 Fa0/3
3    00d0.f8fe.a861 switch-3       2    up       Fa0/5      2    00d0.f8fe.43d2 Fa0/12
```

显示候选设备的信息

```
clus_1.Ruijie# show cluster candidates
      MAC       Hops LcPort     UpSN       UpMAC      UpPort     STATUS
-------------- ---- ---------- ---- -------------- ---------- ------
00d0.f8fe.43d2 1    Fa0/2      1    00d0.f8fe.1007  Fa0/3      ready
00d0.f8fe.a861 2    Fa0/5      -    00d0.f8fe.43d2  Fa0/12     ready
```

显示集群的拓扑信息

```
clus_1.Ruijie#show cluster topology
-----------------------------------------------------------------------
    (PeerPort) ConnectFlag (LocalPort) [HostName:DeviceMac]
-----------------------------------------------------------------------
ConnectFlag:
    <--> normal connect   **** cluster unenable  -||- in blacklist
    ???? status down
```

```
------------------------------------------------------------------
[CLUSTER_1.Ruijie:00d0.f822.33c8]
    |
    +--(Fa0/11) <--> (Fa0/13)[CLUSTER_3.Ruijie:001a.a97b.d3ac]
    |   |
    |   +--(Fa0/23) <--> (Fa0/21)[CLUSTER_4.Ruijie:001a.a97e.043b]
    |       (Fa0/7) <--> (Fa0/7)
```

显示黑名单信息

```
clus_1.Ruijie#show cluster black-list
      MAC       Hops LcPort    UpSN      UpMAC     UpPort
-------------- ---- --------- ---- -------------- ---------
00d0.f8fe.43d2 1    Fa0/2     1    00d0.f8fe.1007  Fa0/3
00d0.f8fe.a861 -    -         -    -               -
```

11.6 集群管理典型配置举例

11.6.1 集群管理设备配置举例一

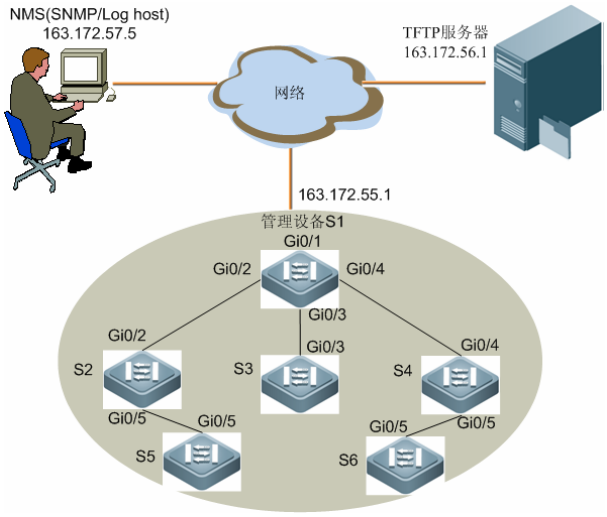
组网需求

为了管理新接入的 4 台交换机，要求：

- IP 资源比较紧张，只能分配一个公网 IP：163.172.55.1/24
- 能查看网络拓扑结构，验证网线连接是否正确，运行过程中，有没有出现网络故障
- 能监视 4 台交换机的运行状态，包括 Log 日志和 Trap 信息
- 能通过管理工作站 NMS 对 4 台交换机进行简单管理与配置
- 能对任意一台交换机进行升级

组网拓扑

图 11-5 组网拓扑图



配置步骤

■ 配置要点如下：

将配置有公网 IP 的设备作为集群管理设备；

管理设备通过端口 Gi0/1 接入到外部网络，通过端口 Gi0/2、端口 Gi0/3 和端口 Gi0/4；连接三台成员设备；

管理设备的 Gi0/1 属于 VLAN2，VLAN2 的接口 IP 地址为 163.172.55.1/24，管理设备的网管接口为 SVI2，外部网络的网络管理设备通过 VLAN2 登陆到管理设备

网管工作站及日志主机的 IP 地址为 163.172.57.5/24

整个集群使用一台设备作为 TFTP 服务器，IP 地址为 163.172.56.1/24

集群管理 VLAN 为 VLAN30，管理 IP 地址池为 192.168.176.0/24

■ 配置管理设备

#将端口 Gi0/1 加入 VLAN2，并创建 SVI2，接口地址为 163.172.55.1

```
Ruijie# config
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# vlan 2
Ruijie(config-vlan)# add interface gigabitEthernet 0/1
Ruijie(config-vlan)#exit
Ruijie(config)#interface vlan 2
Ruijie(config-VLAN 2)#ip address 163.172.55.1 255.255.255.0
```

#启用集群功能，创建集群 CLUSTER，管理 VLAN2050，IP 地址池 192.168.168.0/24

```
Ruijie# config
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# cluster                          //集群默认名称为 CLUSTER
Create Cluster [CLUSTER]
  Management (vlan = [2050], ip-pool = [192.168.168.0/24]).
```

```
CLUSTER_1.Ruijie(config-cluster)#
```

#修改集群管理 VLAN 为 30，IP 地址池为 192.168.176.0/24

```
CLUSTER_1.Ruijie # config
Enter configuration commands, one per line.  End with CNTL/Z.
CLUSTER_1.Ruijie (config)# cluster                //进入集群模式
CLUSTER_1.Ruijie (config-cluster)#management vlan 30 ip-pool 192.168.176.0 255.255.255.0
Proceed with rebuilding Cluster [CLUSTER] and change management? [NO/YES]yes
CLUSTER_1.Ruijie(config-cluster)#
```

#修改集群拓扑收集时间间隔为 50s

```
CLUSTER_1.Ruijie # config
Enter configuration commands, one per line.  End with CNTL/Z.
CLUSTER_1.Ruijie (config)# cluster                //进入集群模式
CLUSTER_1.Ruijie (config-cluster)#timer 50
```

#修改管理设备拓扑收集范围为 3 跳

```
CLUSTER_1.Ruijie # config
Enter configuration commands, one per line.  End with CNTL/Z.
CLUSTER_1.Ruijie (config)# cluster                //进入集群模式
CLUSTER_1.Ruijie (config-cluster)# hops-limit 3
```

#修改集群握手报文时间间隔为 20s，设备信息保留时间为 100s

```
CLUSTER_1.Ruijie # config
Enter configuration commands, one per line.  End with CNTL/Z.
CLUSTER_1.Ruijie (config)# cluster                //进入集群模式
CLUSTER_1.Ruijie (config-cluster)#timer hello 20
CLUSTER_1.Ruijie (config-cluster)#timer hold 100
```

#配置集群公用的 TFTP 服务器

```
CLUSTER_1.Ruijie # config
Enter configuration commands, one per line.  End with CNTL/Z.
CLUSTER_1.Ruijie (config)# cluster                //进入集群模式
CLUSTER_1.Ruijie (config-cluster)# proxy tftp-server 163.172.56.1
```

#配置集群管理工作站，包括 SNMP 的访问字符和 SNMP host

```
CLUSTER_1.Ruijie # config
Enter configuration commands, one per line.  End with CNTL/Z.
CLUSTER_1.Ruijie (config)# snmp-server community public rw
CLUSTER_1.Ruijie (config)# snmp-server enable traps
CLUSTER_1.Ruijie (config)# snmp-server host 163.172.57.5
```

#配置日志主机

```
CLUSTER_1.Ruijie # config
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
CLUSTER_1.Ruijie (config)# logging server 163.172.57.5
CLUSTER_1.Ruijie (config)# logging traps
```

#利用集群公用的 TFTP 服务器升级成员设备 S2

```
CLUSTER_1.Ruijie# cluster login member 2
CLUSTER_2.Ruijie# cluster tftp server:ngsa-maincompress-s5750e-ppc.bin_ flash:rgos.bin
CLUSTER_2.Ruijie# exit
CLUSTER_1.Ruijie# cluster reload member 2
Proceed with reloading Member (sn = [2], mac = [00d0.f822.33c8])? [NO/YES]yes
CLUSTER_1.Ruijie#
```

#利用管理工作站直接访问成员设备 2

在管理工作站中，将目的 IP 设置为 S1 的公网 IP：163.172.55.1 ，访问字符串为 public@es2

- 验证配置

通过 **show cluster、show cluster member** 查看相关集群信息。

通过 **show cluster topology** 查看网络的拓扑结构。

11.6.2 集群管理设备配置举例二

组网需求

完成举例一的配置步骤后，现在网络已经运行稳定，要求：

- 设备 S4、设备 S2 及其下联设备都不能被外网登陆，也不能被管理工作站 NMS 配置与监控
- 设备 S4 的下联设备要能正常被外网登陆访问
- 交换机异常重启后，能正确恢复之前的配置

2 配置步骤

- 配置要点：

要是设备 S2 及其下联设备不能被外网访问，可以在管理设备上将其加入黑名单，也可以登陆到该设备，指定不同的管理设备；

设备 S4 不能被外网访问，但是又不能影响其下联设备，可以关闭该设备的集群功能；

关闭自动添加功能，将所有的动态添加转为静态添加，并且将管理设备 s1 配置信息保存到 TFTP 服务器中。

- 要让设备 S2 及其下联设备不能被外网访问，有两种方式

方式一：在设备 S2 上进行配置

#指定成员设备 S2 的管理设备信息

```
CLUSTER_2.Ruijie # config
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
CLUSTER_2.Ruijie (config)# cluster member cluster-name clus1          //指定该设备只能被集群 clus1 管理
Ruijie (config)#
```

方式二：在管理设备上将设备 S2 加入黑名单

```
CLUSTER_1.Ruijie # config
Enter configuration commands, one per line.  End with CNTL/Z.
CLUSTER_1.Ruijie (config)# cluster                                    //进入集群模式
CLUSTER_1.Ruijie (config-cluster)# member black-list  001a.a9c4.48d2   //设备 S2 的 MAC 地址加入黑名单
```

- 设备 S4 不能被外网访问

#在设备 S4 上关闭集群功能

```
CLUSTER_4.Ruijie # config
Enter configuration commands, one per line.  End with CNTL/Z.
CLUSTER_4.Ruijie (config)# no cluster enable
Ruijie (config)#
```

- 保存配置

#关闭自动添加功能，将静态添加转为动态添加

```
CLUSTER_1.Ruijie # config
Enter configuration commands, one per line.  End with CNTL/Z.
CLUSTER_1.Ruijie (config)# cluster
CLUSTER_1.Ruijie(config-cluster)#no member auto-add
Disable auto-add.There are [3] auto-add Members,Make sure to keep Members with static? [NO/YES]yes
CLUSTER_1.Ruijie (config-cluster)# end
CLUSTER_1.Ruijie# write                                          //保存配置信息
```

#将管理设备 S1 的配置保存到 TFTP 服务器中

```
CLUSTER_1.Ruijie # cluster tftp flash:config_text server:CLUSTER_1.text
```

12 设备冗余

本章说明如何配置设备板冗余以实现不间断转发（NSF，nonstop forwarding），以及设备的文件系统管理方法。

12.1 设备冗余的NSF概述

NSF 是指采用控制面与转发面分离结构实现的网络设备，在控制面出现有计划停机（如软件升级）或未计划停机（如软硬件缺陷）时，转发面能够继续进行转发工作，并且在控制面重新启动过程中，不会出现转发停止或者拓扑波动。NSF 中 High Availability Architecture 的重要组成部分。

在双机热备中，其中一台设备作为主设备，另外一台设备作为从设备。在主设备发生故障或主动要求切换时，从设备接替成为新的主设备。在设备运行过程中，如果主设备出现异常不能正常工作，系统将自动切换到从设备工作，不丢失用户的相应配置，从而保证网络能够正常运行。在一般状况下，从设备不参与交换机的管理，而是监控主设备的运行状态，下列事件会触发设备的切换：

主设备的硬件故障，导致系统挂起或复位

两台设备之间的 heartbeat 消失

手工切换

- 两台设备同时起机（或一台设备已启动时热加入另一设备）时，会进行一些配置同步的操作（批量同步），同步完成后两台设备进入热备状态（Active/Standby Hot）。
- 目前在 VSU 模式下，仅支持 1:1 的热备关系，即全局主设备和全局从设备进行热备，其余设备为候选设备，候选设备在全局主从设备）之一故障时加入热备管理。VSU 模式下全局主设备和全局从设备之间进行的信息备份和配置备份等处理基本同单机模式下主从设备之间热备处理一致，热备的状态显示命令查看的仅为自己和对端的热备状态。
- 若是起机后系统检测到主从设备上的软件版本不一致，此时热备跑起来后会使两设备进入 Boot Cold 状态（Boot Cold/Boot Cold），即两设备分别检测到对方，但双方并不成为热备份关系。之后，热备份不再往下走，直到自动升级完成将从设备复位后（此时两设备软件版本一致），两设备才进入正常的热备份状态。

12.1.1 NSF的优点及限制

NSF 技术的实现可为网络服务提供以下便利：

1) 提高了网络的可用性

NSF 技术在设备转换过程中维持了数据转发及用户会话的状态信息。

2) 避免邻居检测到 link flap

在切换过程中转发面并未重新启动，因此邻居不会检测到链路先 Down 后 UP 的状态变化。

3) 避免 routing flaps

在切换过程中转发面维持转发通信，并且控制面快速构造新的转发表，没有明显的新旧转发表替换过程，从而避免出现routing flaps。

4) 用户会话(user sessions)不会丢失

在切换前已建立的用户会话由于状态进行了实时同步而不会丢失。

在交换机上使用 NSF 技术需要注意有以下限制：

在主从设备的软硬件构成完全一致的前提下方能保持 NSF 的正常工作；

在启动过程中，主/从设备之间需要先进行批量同步，以使两设备达到状态一致，在这个过程完成以前是 NSF 不能发挥作用的窗口期；

并非所有与转发相关的功能都进行了同步，按照对 NSF 的支持程度，交换机功能可分为以下几类：

- 可高用性支持功能
- 在主设备与从设备之间进行了状态信息的实时同步，如与二层转发直接相关的控制面功能都进行了实时同步；
- 可高用性兼容功能
- 这些特性不支持高可用性，它们的状态数据没有进行同步，但是在高可用性启用时，这些功能仍然可以使用，在切换后，这些功能从初始化状态开始运行；
- 可高用性不兼容功能

这些特性（可高用性不兼容功能）不支持高可用，它们的状态数据没有进行同步，在高可用性启用时，这些特性不能使用，否则可能导致系统行为的不正常。当这些功能启用时，系统就热备份状态降至 BOOT HOT 状态，此时系统只进行 running-config 的同步。

12.1.2 NSF的关键组成技术

实现 NSF 的关键技术包括：

状态同步

主设备将其运行状态实时同步至从设备，以使从设备能够在任意时刻接替主设备的功能，而不至产生可觉察的变化。

配置同步

对于一些与不间断转发没有直接关联的功能，只将它们的配置同步过来。通过 running-config 与 startup-config 的同步，可以使用户配置在切换过程中保持一致。

running-config 在用户配置从全局模式退出到特权模式时进行，而 startup-config 的同步则是用户在使用 write 或 copy 命令保存配置时进行。

采用 SNMP 进行的配置未进行自动同步，直到由 CLI 配置方式触发了 running-config 的同步，它们才会被同步。

用户可以配置自动同步的模式（全局配置模式下敲入 redundancy 命令后敲入 auto-sync { standard | startup-config | running-config }），并通过命令查看目前的同步自动同步模式是那种（特权模式下敲入命令 show redundancy auto-sync），也可以配置自动同步的时间间隔（全局配置模式下敲入 redundancy 命令后敲入 auto-sync time-period value，单位为秒）。

自动同步的模式包含以下 3 种:

standard：同步所有系统文件（既同步 startup-config，又同步 running-config）。

startup-config：同步运行时间的配置文件。

running-config：同步启动配置文件。

也可通过 no 命令将各模式都关闭，使得各配置文件都不自动同步。在未配置自动同步模式的情况下，默认配置是采用 standard 模式，即同步 startup-config 和 running-config 配置文件。

12.2 NSF配置

在设备冗余构成方式中，只有主设备支持所有的 CLI 命令，而从设备只支持用户模式及特殊模式下的少量命令。

12.2.1 配置冗余管理

主设备的自动选择

在 VSU 系统建立后，VSU 的主设备作为双机热备的主设备，VSU 的从设备作为双机热备的从设备。您可以在设备的运行中对 VSU 进行进行设备加入和设备退出操作。VSU 将根据系统当前的情况，自动选择相应的设备进行正常工作，同时不影响正常的数据交换，您在使用过程中可能遇到以下情况，主设备将做相应的选择：

如果在系统启动的时候，有两台设备，在运行过程中，退出其中一台设备（或者其中一台设备工作异常），如果该设备在退出（或者异常）之前为从设备，则退出（或者异常）后系统仅仅提示从设备退出；如果该设备在退出（或者异常）之前为主设备，那么另外一台设备将从从设备状态升级到主设备状态，并输出相应提示信息。

在设备的运行过程中，用户在配置完成后必须进行参数保存，否则相应的配置在主从设备切换的时候将失效。

在主从设备的批量备份期间，严禁拔掉主设备，这样会引起整个系统复位导致数据流中断。如果在批量备份期间，主设备软件出现异常，也会引起整个系统复位，导致数据流中断。

主设备的手动选择

允许您通过 CLI 所提供的命令来选择主从设备；

在特权用户模式下，执行如下命令可以强制切换主设备：

命令	作用
Ruijie# **redundancy forceswitch**	不需要进入全局配置模式，直接执行。

例如，当前的主设备主设备为设备 1，从设备为设备 2，执行如下命令后，设备 1 将复位，设备 2 将升级为主设备：

```
Ruijie# redundancy forceswitch
```

多台设备构成 VSU 时的 1:1 热备关系，切换操作后，新全局从设备不一定是原来的全局主设备，也可能是某天全局候选设备。

12.2.2 配置同步模式

执行以下命令可以配置需要同步的配置文件。

命令	作用
Ruijie(config)# **redundancy**	进入冗余配置模式
Ruijie(config-rdnd)# **auto-sync** {**standard	running-config	startup-config**}	配置需要同步的配置文件
Ruijie# **show running-config**	确认热备份已启动
Ruijie# **show redundancy states**	显示当前冗余操作模式

12.2.3 配置心跳检测时间

执行以下命令可以配置主从设备的心跳检测时间。

命令	作用
Ruijie(config)# **redundancy**	进入冗余配置模式
Ruijie(config-rdnd)# **switchover** *timeout timerout-period*	控制主从之间的心跳检测时间
Ruijie# **show running-config**	确认配置已生效
Ruijie# **show redundancy states**	显示当前冗余操作模式

12.2.4 复位设备

执行以下命令可以指定复位指定设备

命令	作用
Ruijie> **enable**	进行特权配置模式
Ruijie# **redundancy reload** { **peer	shelf** }	peer 是仅复位 slave；VSU 模式下需指定待复位的设备号：**redundancy reload shelf** *switchid*）

13 SRM

13.1 SRM概述

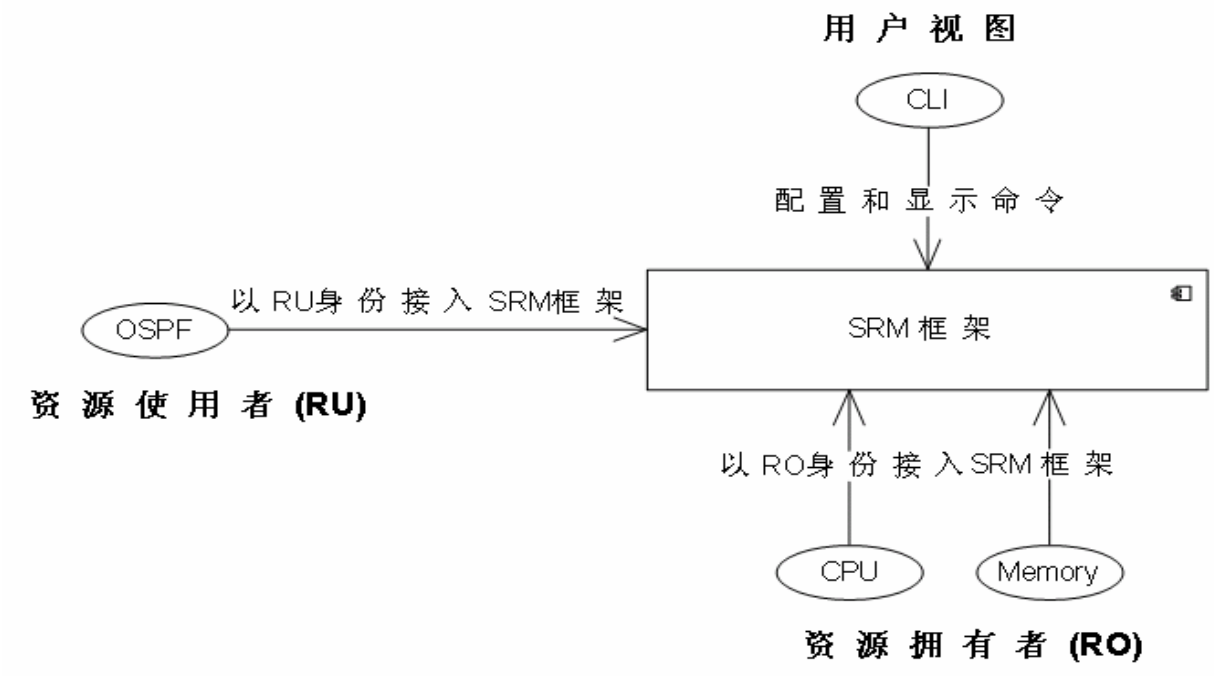
SRM（System Resources Manager，系统资源管理）用于监控嵌入式系统中有限内部资源的使用情况。通过对监控信息的分析，网管人员能够对设备的运行状态有更加全面的了解，对系统性能可以有更准确的衡量，并据此采取相应措施以提升可用性。

SRM 主要包括统计和监控功能：

- 统计：通过查阅资源使用情况的统计信息，用户可以了解到资源的当前分布情况以及历史记录，为系统优化、故障排查等提供有效依据。
- 监控：通过合理设置监控值，用户可以及时了解系统状态的变化，系统内部也可以根据状态变化执行特定的行为，以维持系统的稳定性和可靠性。

RGOS 的 SRM 构架如下图所示，SRM 将各类系统资源抽象成资源拥有者（Resource Owner，简称 RO），使用这些资源的模块被抽象成资源使用者（Resource User，简称 RU），SRM 框架则是资源拥有者、资源使用者以及外部用户之间的桥梁，同时也是整个 SRM 构架的核心。

图 13-1 SRM 构架



13.1.1 基本概念

资源使用者

资源使用者（Resource User，简称 RU），接入 SRM 框架中以对其资源使用情况进行监控。

RGOS 中只支持 Task 类型的 RU，即 RU 和 Task 是一一对应的关系。

资源拥有者

资源拥有者（Resource Owner，简称 RO），对应于 RGOS 中已有的资源管理模块，接入到 SRM 框架中通知资源变动并提供资源分配情况的统计信息。

当前，RO 包括 cpu 和 memory 这两类资源。

SRM 框架

SRM 框架，它构筑于具体 RO 之上，负责资源使用者、资源拥有者、监控策略等信息的维护以及资源占用率的监控。引入 SRM 框架的目的在于对用户屏蔽资源管理模块的差别，对外提供统一的 SRM 配置命令。

RU 组

为了支持对某类相似的 RU 进行统一的监控，在 RU 的基础上引入“组”的概念，允许用户自由的将多个 RU 组成一个 RU 组。当监控事件发生时，SRM 框架会把通告发给 RU 组中所有的成员。

SRM 中存在以下三类 RU 组：

- 全局组：它是系统中默认存在的 RU 组，表示对 RO 的全局占用率的监控。系统中只能存在一个全局组。
- 单元组：这类组中只包含单独的一个 RU，当用户对单个 RU 进行监控时，SRM 自动生成一个与 RU 同名的单元组，这个单元组将替代 RU 作为监控操作的对象。
- 多元组：这类组中允许包含多个 RU，用户可以根据自己的需要定义这类组，并增加或删除组中的 RU 成员。

一个 RU 只能属于某个 RU 组，不能同时属于多个不同的 RU 组，否则会发生一个 RU 使用多个策略的情况，这在策略关联中是不允许的。

策略

策略用来指明监控的对象和行为。一个策略由一个或者多个 RO 监控规则组成，而每个 RO 监控规则由一条或者多条不同级别的监控水线组成。

一条策略可以应用在多个 RU 组上。当策略被应用到 RU 组时，称策略与 RU 组发生关联，此时会产生一个监控实例，它会监控对应的资源使用状况。

策略分为两种：

- 全局策略：全局策略中的水线监控的是 RO 的全局占用率。因此全局策略只能和全局组关联，同时全局组也只能应用全局策略。
- 用户策略：用户策略中的水线监控的是由用户指定的 RU 的资源占用率总和。用户策略只能与单元组或多元组关联。

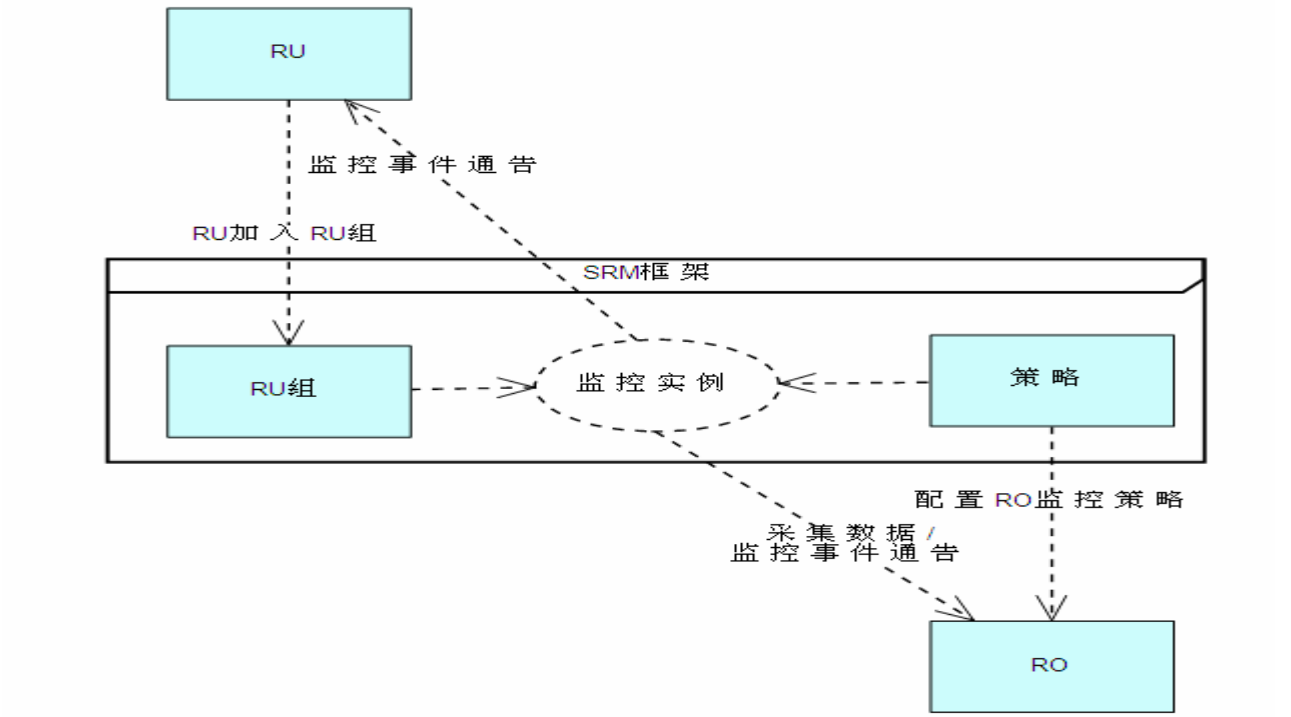
水线

水线包含如下属性：

- level：水线级别，用于指明水线的紧急程度，分为紧急（critical）、重要（major）、次要（minor），不同紧急程度的水线产生的监控事件通告也不同，用户通过查看通告的历史信息可以了解系统的运行状况。
- rising value：rising 水线值，有效值为 1~100。当资源占用率从低于 rising value 升至高于 rising value 且维持时间超过 interval 时，将产生一个 up 监控事件。
- falling value：falling 水线值，有效值为 1~100，且 falling value 必须小于 rising value。当资源占用率从高于 rising value 降至低于 falling value 且维持时间超过 interval 时，如果此前产生过同级别的 up 监控事件，将产生一个 down 监控事件，否则不会产生 down 监控事件。如果不配置 falling value，将不会产生和 up 监控事件对应的 down 事件。
- interval：维持时间，以秒为单位，最小值为 5s，最大值为 86400s。当占用率越过水线并稳定在水线一侧的时间超过 interval 时，才会产生一个监控事件。这就避免资源占用率在水线上下抖动时产生大量无效事件通告。

13.1.2 工作原理

图 13-2 工作原理



如图所示，SRM 框架通过策略和 RU 组关联产生的监控实例来监控 RU/RO 的资源状况。监控实例周期性的监控 RU/RO 资源状况，并和策略中的水线进行比较，当发现资源占用率穿越过水线并且稳定在水线一侧的时间超过规定的时间时，会触发相应的监控事件。

13.2 配置SRM

以下章节描述如何配置 SRM 特性：

- （必选）配置策略

- （必选）应用策略
- （必选）配置 RU 组
- 查看 SRM 配置与状态

13.2.1 配置监控策略

命令	作用
Ruijie>**enable**	进入特权模式。
Ruijie#**configure terminal**	进入全局模式。
Ruijie(config)#**resource manager** [**slot** *slot-id* [**subsystem** *subsystem-id*]]	进入 srm 配置模式。 默认进入本板的 srm 配置模式。 **slot** *slot-id*：指定要配置的板卡。 subsystem *subsystem-id*：子系统编号。
Ruijie(config-srm)#**policy** *policy-name* [**global**]或 Ruijie(config-srm-slot-slotnum)#**policy** *policy-name* [**global**]	配置策略并进入 srm-policy 配置模式。 *policy-name*：监控策略名称。 global：如果添加了 global 参数，则表示这是一个全局策略，否则表示这是一个用户策略。
Ruijie(config-srm-policy)#{**memory	cpu**}	进入 owner 配置模式。 目前支持 memory 和 cpu 两种 RO。
Ruijie(config-owner-memory)#{**critical	major	minor**} **rising** *rising-waterline-value* [**interval** *interval-value*] [**falling** *falling-waterline-value* [**interval** *interval-value*]]	设置水线。水线的数值单位为百分比，配置范围 1-100。 注：major 的 rising 水线必须大于 minor 的 rising 水线，critical 的 rising 水线必须大于 major 的 rising 水线。

如果要删除策略配置，在 SRM 模式下使用 **no policy** *policy-name* 命令进行设置。

配置举例：

配置一个名为 rgos_policy 的 global 类型的 policy，并对该 policy 的 memory 项进行配置。

```
Ruijie#configure terminal
Ruijie(config)#resource manager
Ruijie(config-srm)#policy rgos_policy global
Ruijie(config-srm-policy)#memory
Ruijie(config-owner-memory)#major rising 30 falling 15 interval 10
```

13.2.2 应用监控策略

命令	作用
Ruijie>**enable**	进入特权模式。
Ruijie# **configure terminal**	进入全局模式。
Ruijie(config)# **resource manager**	进入 srm 配置模式。
Ruijie(config-srm)#**user global** *global-policy-name*	全局组应用全局监控策略。
Ruijie(config-srm)#**user** *resource-user-name resource-policy-name*	某个资源使用者应用用户监控策略。

配置举例：

#配置一个名为 rgos_policy 的全局策略，并应用到全局组上。

```
Ruijie#configure terminal
Ruijie(config)#resource manager
Ruijie(config-srm)#policy rgos_policy global
Ruijie(config-srm-policy)#exit
Ruijie(config-srm)#user global rgos_policy
```

#配置一个名为 rgos_policy 的用户策略，并应用到 snmpd 上。

```
Ruijie#configure terminal
Ruijie(config)#resource manager
Ruijie(config-srm)#policy rgos_policy
Ruijie(config-srm-policy)#exit
Ruijie(config-srm)#user snmpd rgos_policy
```

#对 Group 应用 policy 的方式参见“配置 RU 组。

13.2.3 配置RU组

命令	作用
Ruijie>**enable**	进入特权模式
Ruijie# **configure terminal**	进入全局模式
Ruijie(config)# **resource manager**	进入 srm 配置模式
Ruijie(config-srm)#**user group** *resource-group-name*	配置 RU 组并进入 res-group 配置模式，*resource-group-name* 为 RU 组的名称
Ruijie(config-res-group)#**instance** *resource-user-name*	添加 RU，*resource-user-name* 为 RU 的名称，通过 **show resource database** 可以查看系统所有的 RU。
Ruijie(config-res-group)#**policy** *policy-name*	应用策略，*policy-name* 为策略名称

配置举例：

配置一个名为 rgos_group 的 RU 组，将 snmpd 添加到组中，最后组应用策略。

```
Ruijie#configure terminal
Ruijie(config)#resource manager
Ruijie(config-srm)#user group rgos_group
Router(config-res-group)#instance snmpd
Router(config-res-group)#policy rgos_policy
```

13.2.4 查看SRM配置与状态

命令	作用
show resource database [**slot** *slot-id* [**subsystem** *subsystem-id*]]	查看 srm 数据库，包括：RU 信息，RO 信息，策略信息。 默认显示主管理板的 srm 数据库信息； slot *slot-id*：指定要查看的板卡； subsystem *subsystem-id*：子系统编号。

show resource notification owner {**all	cpu	memory**} [**slot** *slot-id* [**subsystem** *subsystem-id*]]	查看监控事件通告统计。 all：查看所有 RO 的统计； cpu：查看和 cpu 有关的统计； memory：查看和 memory 有关的统计。 默认显示主管理板的监控事件通告统计； slot *slot-id*：指定要查看的板卡； subsystem *subsystem-id*：子系统编号。
show resource owner {**all	cpu	memory**} [**slot** *slot-id* [**subsystem** *subsystem-id*]]	查看 RO 的使用情况。 all: 所有的 RO 资源； cpu: cpu 资源； memory: memory 资源。 默认显示主管理板的 RO 的使用情况； slot *slot-id*：指定要查看的板卡； subsystem *subsystem-id*：子系统编号。
show resource policy {**all**	*policy-name*} [**slot** *slot-id* [**subsystem** *subsystem-id*]]	查看 policy 信息。 all: 表示所有的策略； *policy-name*:具体的策略名。 默认显示主管理板的 policy 信息； slot *slot-id*：指定要查看的板卡； subsystem *subsystem-id*：子系统编号。
show resource relationship [**slot** *slot-id* [**subsystem** *subsystem-id*]]	查看策略与 RU 组的关联。 默认显示主管理板的关联信息； slot *slot-id*：指定要查看的板卡； subsystem *subsystem-id*：子系统编号。
**show resource user {all	group** {**all**	*group-name*}	*resource-user-name*} [**slot** *slot-id* [**subsystem** *subsystem-id*]]	查看 RU 配置。 all: 表示所有的 RU 和 RU 组； group {all	*group-name}*: RU 组，all 表示所有的 RU 组，*group-name* 为 RU 组的名称； *resource-user-name*: RU 的名称。 默认显示主管理板 RU 配置； slot *slot-id*：指定要查看的板卡； subsystem *subsystem-id*：子系统编号。

13.3 SRM典型配置举例

组网需求

监控整机内存使用率，CPU 使用率；监控特定业务模块（比如 SNMPD、802.1X）内存使用率，CPU 使用率。

配置步骤

1) 配置一个全局策略对内存的使用进行监控，当系统的内存使用率达到 60%且超过 10 秒时触发 major 事件，SRM 会记录有关日志信息（请查看 SYSLOG 文档 SRM.txt）。

#配置一个全局策略对内存的使用进行监控

```
Ruijie#configure terminal
Ruijie(config)#resource manager
Ruijie(config-srm)#policy rgos_global_policy global
Ruijie(config-srm-policy)#memory
Ruijie(config-owner-memory)#major rising 60 interval 10
Ruijie(config-owner-memory)#exit
Ruijie(config-srm-policy)# exit
Ruijie(config-srm)#user global rgos_global_policy
```

配置一个用户策略并应用到 snmpd。

```
Ruijie#configure terminal
Ruijie(config)#resource manager
Ruijie(config-srm)#policy rgos_user_policy
Ruijie(config-srm-policy)#memory
Ruijie(config-owner-memory)#major rising 30 falling 15 interval 10
Ruijie(config-owner-memory)#exit
Ruijie(config-srm-policy)#exit
Ruijie(config-srm)#user snmpd rgos_user_policy
```

15. 配置 RU 组，将具体的 RU 加入该组，将策略应用在 RU 组上，以实现对 RU 的资源使用进行监控。

配置策略和组，并关联

```
Ruijie#configure terminal
Ruijie(config)#resource manager
Ruijie(config-srm)#policy rgos_grp_policy
Ruijie(config-srm-policy)#memory
Ruijie(config-owner-memory)#major rising 30
Ruijie(config-owner-memory)#exit
Ruijie(config-srm-policy)#exit
Ruijie(config-srm)#user group rgos_group
Router(config-res-group)#instance dlx_task
Ruijie(config-res-group)#policy rgos_grp_policy
```

显示验证

16. 查看 SRM 数据库信息

```
Ruijie#show resource database
Resource Owners                 ID
------------------------------------------------------------------
Cpu                                 0x0
Memory                              0x1
Resource Users                  ID                Priority
------------------------------------------------------------------
```

```
Ktimer                              0x1              PROT_TASK
atimer                          0x2              APP_TASK
printk_task                 0x3              APP_TASK_TS
waitqueue_process           0x4          PROT_TASK
tasklet_task                    0x5              PROT_TASK
cmic_pause_detect           0x6              PROT_TASK
idle                            0x7          IDLE
kevents                         0x8          PROT_TASK
snmpd                           0x9          PROT_TASK
snmp_trapd                  0xa          APP_TASK
mtdblock                        0xb              PROT_TASK
gc_task                         0xc              ROT_TASK
Context                         0xd          PROT_TASK
kswapd                          0xe              PROT_TASK
bdflush                         0xf              PROT_TASK
kupdate                         0x10             PROT_TASK
UPGRADE_TASK                    0x11             HAPP_TASK_TS
ll_mt                           0x12             PROT_TASK
ll main process             0x13         PROT_TASK
bridge_relay                    0x14             PROT_TASK
d1x_task                    0x15             HAPP_TASK_TS
secu_policy_task            0x16             APP_TASK_TS
```

17. 查看监控事件通告统计

```
Ruijie#show resource notification owner all
Owner: cpu
Global                      Global Notif.(cr(U/D):ma(U/D):mi(U/D))
------------------------------------------------------------------------
global                                  Not in monitored
Multi-User Group            User Notif.(cr(U/D):ma(U/D):mi(U/D))
------------------------------------------------------------------------
rgnos_group                             (cr(0/0):ma(0/0):mi(0/0))
Single-User Group           User Notif.(cr(U/D):ma(U/D):mi(U/D))
------------------------------------------------------------------------
ktimer                                  (cr(0/0):ma(0/0):mi(0/0))
Owner: memory
Global                      Global Notif.(cr(U/D):ma(U/D):mi(U/D))
------------------------------------------------------------------------
global                                  Not in monitored
Multi-User Group            User Notif.(cr(U/D):ma(U/D):mi(U/D))
------------------------------------------------------------------------
rgnos_group                             (cr(0/0):ma(0/0):mi(0/0))
Single-User Group           User Notif.(cr(U/D):ma(U/D):mi(U/D))
------------------------------------------------------------------------
ktimer                                  (cr(0/0):ma(0/0):mi(0/0))
```

18. 查看 RO 信息

```
Ruijie#show resource owner all
Resource Owner: CPU
Used Ratio(%): 5Sec -- 93, 1Min -- 93, 5Min – 93
RU Group                    Runtime(ms)   5Sec     1Min     5Min
-------------------------------------------------------------------
rgnos_group                 1590380       0          0          0
RU                              Runtime(ms)   5Sec     1Min     5Min
-------------------------------------------------------------------
rl_con                          171420            0            0            0
stat_get_and_send           1585180       1        1        1
cmic_pause_detect               1585180       0            0            0
mem_info_task               1602670           0        0            0
idle_vlan_proc_thread       1602670       0          0          0
rerp_msg_recv_thread        1602760       0          0          0
ssp_mc_trap_task            1602920       0          0          0
ssp_flow_rx_task            1604410       0            0            0
flow_warn_msg_task          1604440       0            0            0
flow_age_task               1604440       0            0            0
temperature_handler_task    1604650       0          0          0
keepalive_link_notify       1604700       0          0          0
datapkt_rcv_thread          1604700       0          0          0
rdp_slot_change_thread      1604700       0          0            0
printk_task                     2172590       92           92           92
idle                            2172590       7            7          7
Resource Owner: memory
Total Size(B): 536870912
Used  Size(B): 143081472
Used  Ratio(%): 27
RU Group                        Allocated Size(B)  Alloc Cnt     Free Cnt
-------------------------------------------------------------------
local-1                         0                    0            0
RU                                  Allocated Size(B)   Alloc Cnt        Free Cnt
-------------------------------------------------------------------
Ktimer                          0                    7065         14
atimer                      92                       2343         3
printk_task                     0                    0            0
waitqueue_process           0                    0            0
tasklet_task                    2656                     21           4
idle                            0                    0            0
ttipc_timer                     0                    1610         1610
kevents                         0                    0            0
iftp_server                     0                    0            0
snmpd                               45312                    53           47
```

snmp_trapd	0	0	0	
mtdblock	0	0	0	
gc_task	4	13	13	
context	0	0	0	
kswapd	0	0	0	
bdflush	0	0	0	
kupdate	0	2	2	

19. 查看策略信息

```
Ruijie#show resource policy all
policy Name: rgnos_global_policy
-----------------------------------------------------------------------
Type: Global
In Use: No
RO memory:
critical rising 98 interval 2600 falling 40 interval 2600
major rising 80 interval 4000 falling 30 interval 4000
minor rising 45 interval 6600 falling 10 interval 6600
RO cpu:
critical rising 99 interval 1800 falling 20 interval 1800
major rising 85 interval 3800 falling 40 interval 3800
minor rising 60 interval 6900 falling 10 interval 6900
policy Name: rgnos_policy4
-----------------------------------------------------------------------
Type: User
In Use: No
RO memory:
critical rising 92 interval 2500 falling 20 interval 2500
major rising 79 interval 3000 falling 40 interval 3000
minor rising 63 interval 5000 falling 10 interval 5000
RO cpu:
critical rising 89 interval 2900 falling 20 interval 2900
major rising 86 interval 3800 falling 40 interval 3800
minor rising 61 interval 5900 falling 10 interval 5900
policy Name: rgnos_policy3
-----------------------------------------------------------------------
Type: User
In Use: No
RO memory:
critical rising 92 interval 2500 falling 20 interval 2500
major rising 79 interval 3000 falling 40 interval 3000
minor rising 63 interval 5000 falling 10 interval 5000
RO cpu:
critical rising 89 interval 2900 falling 20 interval 2900
major rising 86 interval 3800 falling 40 interval 3800
```

```
minor rising 61 interval 5900 falling 10 interval 5900
```

20. 查看关联信息

```
Ruijie#show resource relationship
Policy                  Resource User      User Type
------------------------------------------------------------------------
global                       global                Global Group
rgnos_policy1           rgnos_group        Multi-User Group
rgnos_policy            ktimer             Single-User Group
```

21. 查看 RU 信息

```
Ruijie#show resource user all
Total resource user group: 2.
Multi-User Group: rgnos_group
------------------------------------------------------------
        Policy: rgnos_policy1
        User:
        Resource Owner: memory
                Allocated Size(B): 0
                Alloc Cnt: 0
                Free Cnt: 0
        Resource Owner: cpu
        Runtime(ms)         5Sec      1Min      5Min
        1735980             0           0           0
Single-User Group: ktimer
------------------------------------------------------------
        Policy: rgnos_policy
        User:   ktimer
        Resource Owner: memory
                Allocated Size(B): 0
                Alloc Cnt: 0
                Free Cnt: 0
        Resource Owner: cpu
        Runtime(ms)     5Sec          1Min          5Min
        1760120             0           0           0
```

14 硬件表项容量

14.1 概述

为了灵活应用硬件表项资源，以满足不同业务场景需求，提供了硬件容量配置功能。

14.2 配置硬件表项容量

用户可以自行指定如下几种硬件表项的最大条目数。

- 策略路由最大条目数
- IPv6 隧道接口最大数目
- 共享池（shared-pool）最大数目

以上配置，需保存，并重启设备后才会生效。

14.2.1 配置策略路由最大条目数

命令	作用
Ruijie(config)# **initialization route pbr** *max-num*	设置策略路由最大条目数，缺省值 64
Ruijie(config)# **no initialization route pbr**	恢复为缺省配置
Ruijie(config)# **initialization route pbr** ？	查看当前允许配置的最大数目合法值

14.2.2 配置IPv6 隧道接口最大数目

命令	作用
Ruijie(config)# **initialization route tunnel-termination** *max-num*	设置 IPv6 隧道接口最大数目，缺省值 32
Ruijie(config)# **no initialization route tunnel-termination**	恢复为缺省配置
Ruijie(config)# **initialization route tunnel-termination** ？	查看当前允许配置的最大数目合法值

14.2.3 配置共享池最大数目

命令	作用
Ruijie(config)# **initialization route shared-pool** *max-num*	设置共享池最大数目，缺省值 200。共享池资源供 MPLS,vlan-mapping,mac-vlan,subnet-vlan,qinq-adv 业务使用
Ruijie(config)# **no initialization route shared-pool**	恢复为缺省配置
Ruijie(config)# **initialization route shared-pool** ？	查看当前允许配置的最大数目合法值

14.3 查看硬件表项容量

命令	作用
Ruijie# **show initialization route**	查看硬件表项容量的相关信息

“config”列表示当前设置值，未生效；“running”列表示当前运行值，已生效；“default”列表示系统缺省值。

```
Ruijie #show initialization route



                           config  running  default

 policy-based route entry:  64      64       64

 tunnel termination entry:  32      32       32

 shared-pool entry:         200     200      200
```

配置指南-以太网交换

本分册介绍以太网交换配置指南相关内容，包括以下章节：

1. 接口
2. MAC 地址
3. Aggregate Port
4. 链路聚合控制协议（LACP）
5. VLAN
6. Super-VLAN
7. Protocol VLAN
8. Private VLAN
9. SHARE VLAN
10. Voice VLAN
11. MAC VLAN
12. MSTP
13. 协议帧透传
14. GVRP
15. LLDP
16. QinQ
17. ERPS
18. BUFFER

1 接口

本章主要对锐捷设备的接口类型进行划分，并对每种接口类型进行详细定义。锐捷设备的接口类型可分为以下两大类：

- 二层接口(L2 interface)
- 三层接口(L3 interface)

1.1 二层接口(L2 interface)

本节主要描述二层接口的类型及相关的定义，可分为以下几种类型

- Switch Port
- L2 Aggregate Port

1.1.1 Switch Port

Switch Port由设备上的单个物理端口构成，只有二层交换功能。该端口可以是一个 Access Port或一个 Trunk Port，您可以通过Switch Port接口配置命令，把一个端口配置为一个 Access Port或者 Trunk Port。Switch Port被用于管理物理接口和与之相关的第二层协议，并且不处理路由和桥接。

Access Port

每个 Access Port 只能属于一个 VLAN，它只传输属于这个 VLAN 的帧。一般用于连接计算机。

- 缺省 VLAN

每个 Access Port 只属于一个 VLAN，所以它的缺省 VLAN 就是它所在的 VLAN，可以不用设置。

- 帧的接收与发送

Access Port 发送出的数据帧是不带 TAG 的，且它只能接收以下三种格式的帧：Untagged 帧、VID 为 Access Port 所属 VLAN 的 Tagged 帧、VID 为 0 的 Tagged 帧。具体发送发式如下表所示：

帧格式	接收	发送
Untagged 帧	为数据帧添加缺省 VLAN 的 TAG。	去掉 TAG 再发送。
Tagged 帧	当 TAG 的 VID（VLAN ID）与缺省 VLAN ID 相同时，接收该数据帧	
	当 TAG 的 VID（VLAN ID）为 0 时，接收该数据帧。在 TAG 中，VID＝0 用于识别帧优先级。	
	当 TAG 的 VID（VLAN ID）与缺省 VLAN ID 不同且不为 0 时，丢弃该帧。	NA

Trunk Port

每个 Trunk port 可以属于多个 VLAN，能够接收和发送属于多个 VLAN 的帧，一般用于设备之间的连接，也可以用于连接用户的计算机。

■ 缺省 VLAN

因为 Trunk Port 可以属于多个 VLAN，所以需要设置一个 Native vlan 作为缺省 VLAN。缺省情况下 Trunk port 将传输所有 VLAN 的帧，为了减轻设备的负载，减少对带宽的浪费，可通过设置 VLAN 许可列表来限制 Trunk port 传输哪些 VLAN 的帧。

建议将本端设备 Trunk 端口的 native vlan 和相连的对端设备 Trunk 端口的 native vlan 配置为一致，否则端口可能无法正确转发报文。

■ 帧的接收与发送

Trunk port 可接收 Untagged 帧和端口允许 VLAN 范围内的 tagged 帧。Trunk Port 发送的非 Native vlan 的帧都是带 TAG 的，而发送的 Native vlan 的帧都不带 TAG。

帧格式	接收	发送
Untagged 帧	为数据帧添加 Native VLAN 的 TAG。	在发送该帧时，将去掉 TAG 后再发送。
Tagged 帧	当 Trunk Port 接收到的帧所带 TAG 的 VID 等于该 Trunk port 的 Native vlan 时，允许接收该数据帧；	在发送该帧时，将去掉 TAG 后再发送。
	当 Trunk Port 接收到的帧所带 TAG 的 VID 不等于该 Trunk port 的 Native vlan，但 VID 是该端口允许通过的 VLAN ID 时，接收该数据帧；	发送时，将保持原有 TAG。
	当 Trunk Port 接收到的帧所带 TAG 的 VID 不等于该 Trunk port 的 Native vlan，且 VID 是该端口不允许通过的 VLAN ID 时，丢弃该报文。	NA

Untagged 报文就是普通的 Ethernet 报文，普通 PC 机的网卡是可以识别这样的报文进行通讯；TAG 报文结构的变化是在源 MAC 地址和目的 MAC 地址之后，加上了 4bytes 的 VLAN 信息，也就是 VLAN TAG 头。

Hybrid 端口

Hybrid 类型的端口可以属于多个 VLAN，可以接收和发送多个 VLAN 的报文，可以用于设备之间连接，也可以用于连接用户的计算机。Hybrid 端口和 Trunk 端口的不同之处在于 Hybrid 端口可以允许多个 VLAN 的报文发送时不打标签，而 Trunk 端口只允许缺省 VLAN 的报文发送时不打标签， 需要注意的是：Hybrid 端口加入的 VLAN 必须已经存在。

1.1.2 L2 Aggregate Port

Aggregate port 是由多个物理成员端口聚合而成的。我们可以把多个物理链接捆绑在一起形成一个简单的逻辑链接，这个逻辑链接我们称之为一个 Aggregate Port（以下简称 AP ）。

对于二层交换来说 AP 就好像一个高带宽的 Switch port，它可以把多个端口的带宽叠加起来使用，扩展了链路带宽。此外，通过 L2 Aggregate port 发送的帧还将在 L2 Aggregate port 的成员端口上进行流量平衡，如果 AP 中的一条成员链路失效，L2 Aggregate port 会自动将这个链路上的流量转移到其他有效的成员链路上，提高了连接的可靠性。

L2 Aggregate Port 的成员端口类型可以为 Access port 或 Trunk Port，但同一个 AP 的成员端口必须为同一类型，要么全是 Access Port，要么全是 Trunk port。

1.2 三层接口(L3 interface)

本节主要描述三层接口的类型及相关的定义，可分为以下几种类型

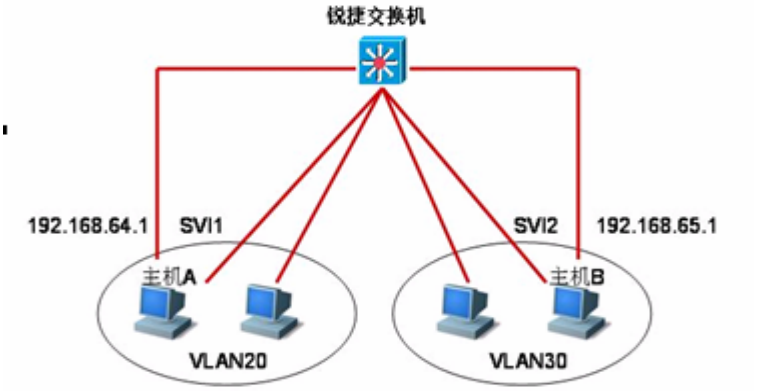
- SVI (Switch virtual interface)
- Routed Port
- L3 Aggregate Port

1.2.1 SVI

SVI(Switch virtual interface，交换虚拟接口)，用来实现三层交换的逻辑接口。SVI 可以做为本机的管理接口，通过该管理接口管理员可管理设备。您也可以创建 SVI 为一个网关接口，就相当于是对应各个 VLAN 的虚拟的子接口，可用于三层设备中跨 VLAN 之间的路由。创建一个 SVI 很简单，您可通过 **interface vlan** 接口配置命令来创建 SVI，然后给 SVI 分配 IP 地址来建立 VLAN 之间的路由。

如图所示，VLAN20 的主机可直接互相通讯，无需通过三层设备的路由，若 VLAN20 内的主机 A 想和 VLAN30 内的主机 B 通讯必须通过 VLAN20 对应的 SVI1 和 VLAN30 对应的 SVI2 才能实现。

图 1-1



1.2.2 Routed Port

一个 Routed Port 是一个物理端口，就如同三层设备上的一个端口，能用一个三层路由协议配置。在三层设备上，可以把单个物理端口设置为 Routed port，作为三层交换的网关接口。一个 Routed Port 与一个特定的 Vlan 没有关系，而是作为一个访问端口。Routed port 不具备二层交换的功能。您可通过 no switchport 命令将一个二层接口 Switch port 转变为 Routed port，然后给 Routed port 分配 IP 地址来建立路由。注意的是，当使用 no switchport 接口配置命令时，该端口关闭并重启，将删除该端口的所有二层特性。

当一个端口是 L2 Aggregate Port 的成员端口或者是未认证成功的 DOT1X 认证口时，是不能用 **switchport/ no switchport** 命令进行层次切换的。

1.2.3 L3 Aggregate Port

L3 Aggregate port 同 L2 Aggregate Port 一样，也是由多个物理成员端口汇聚构成的一个逻辑上的聚合端口组。汇聚的端口必须为同类型的三层接口。对于三层交换来说，AP 作为三层交换的网关接口，它相当于把同一聚合组内的多条物理链路视为一条逻辑链路，是链路带宽扩展的一个重要途径。此外，通过 L3 Aggregate port 发送的帧同样能在 L3 Aggregate port 的成员端口上进行流量平衡，当 AP 中的一条成员链路失效后，L3 Aggregate port 会自动将这个链路上的流量转移到其他有效的成员链路上，提高了连接的可靠性。

L3 Aggregate port 不具备二层交换的功能。您可通过 no switchport 将一个无成员二层接口 L2 Aggregate port 转变为 L3 Aggregate Port，接着将多个 Routed Port 加入此 L3 Aggregate port，然后给 L3 Aggregate Port 分配 IP 地址来建立路由。

1.3 配置接口

1.3.1 缺省配置

属性	缺省设置
工作模式	二层交换模式
Switch port 模式	access port
允许的 VLAN 范围	VLAN 1～4094
缺省 VLAN（对于 access port 而言）	VLAN 1
Native VLAN（对于 trunk port 而言）	VLAN 1
介质类型	copper
接口管理状态	Up
接口描述	空
速度	自协商
双工模式	自协商
流控	自协商
自协商模式	off
Aggregate port	无
风暴控制	关闭
保护端口	关闭
端口安全	关闭
光模块防伪检测	开启

1.3.2 接口编号规则

对于 Switch Port，其编号由两个部分组成：插槽号，端口在插槽上的编号。例如端口所在的插槽编号为 2，端口在插槽上的编号为 3，则端口对应的接口编号为 2/3。插槽的编号是从 0－插槽的个数。插槽的编号规则是：面对设备的面板，插槽按照从前至后，从左至右，从上至下的顺序一次排列，对应的插槽号从 1 开始依次增加。插槽上的端口编号是从 1－插槽上的端口数，编号顺序是从左到右。对于可以选择介质类型的设备，端口包括两种介质（光口和电口），无论使用那种介质，都使用相同的端口编号。您也可以通过命令行中的 show 命令来查看插槽以及插槽上的端口信息。

- 对于 Aggregate Port，其编号的范围为 1－设备支持的 Aggregate Port 个数。
- 对于 SVI，其编号就是这个 SVI 对应的 VLAN 的 VID。

设备上的静态插槽的编号固定为 0，而动态插槽(可插拔模块或线卡)的编号从 1 开始。

1.3.3 接口配置命令的使用

您可在全局配置模式下使用 interface 命令进入接口配置模式。

命令	作用
Ruijie(config)# **interface** interface-id	在全局配置模式下输入 interface 命令，进入接口配置模式。用户也可以在全局配置模式下使用 interface range 或 interface range macro 命令配置一定范围的接口。但是定义在一个范围内的接口必须是相同类型和具有相同特性的

下例给出了进入 Gigabitethernet 2/1 接口的示例：

```
Ruijie(config)# interface gigabitethernet 2/1
Ruijie(config-if)#
```

在接口配置模式下您可配置接口的相关属性。

1.3.4 配置一定范围的接口

用户可以使用全局配置模式下的 **interface range** 命令同时配置多个接口。当进入 **interface range** 配置模式时，此时设置的属性适用于所选范围内的所有接口。

命令	作用
Ruijie(config)# **interface range** {*port-range* | **macro** *macro_name*}	输入一定范围的接口。 **interface range** 命令可以指定若干范围段。 macro 参数可以使用范围段的宏定义，参见配置和使用端口范围的宏定义。 每个范围段可以使用逗号（，）隔开。 同一条命令中的所有范围段中的接口必须属于相同类型。

当使用 **interface range** 命令时，请注意 range 参数的格式：

有效的接口范围格式：

- **vlan** *vlan-ID - vlan-ID*， VLAN ID 范围 1～4094；
- **Gigabitethernet** slot/{第一个 port} - {最后一个 port}；

Aggregate Port Aggregate port 号 - Aggregate port 号， 范围 1～MAX；

在一个 **interface range** 中的接口必须是相同类型的，即或者全是 fastethernet，gigabitethernet 或者全是 Aggregate Port，或者全是 SVI。

下面的例子是在全局配置模式下使用 **interface range** 命令：

```
Ruijie# configure terminal
Ruijie(config)# interface range gigabitethernet 1/1 - 10
Ruijie(config-if-range)# no shutdown
Ruijie(config-if-range)#
```

下面的例子是如何使用分隔符号（,）隔开多个 range：

```
Ruijie# configure terminal
Ruijie(config)# interface range gigabitethernet 1/1-5, 1/7-8
Ruijie(config-if-range)# no shutdown
Ruijie(config-if-range)#
```

配置和使用端口范围的宏定义

用户可以自行定义一些宏来取代端口范围的输入。但在用户使用 **interface range** 命令中的 **macro** 关键字之前，必须先在全局配置模式下使用 **define interface-range** 命令定义这些宏。

命令	作用
Ruijie(config)# **define interface-range** *macro_name interface-range*	定义接口范围的宏定义。 macro_name－宏定义的名字，不超过 32 个字符。 宏定义的内部可以包括多个范围段。 同一宏定义中的所有范围段中的接口必须属于相同类型。
Ruijie(config)# **interface range macro** *macro_name*	宏定义的字符串将被保存在内存中，使用 **interface range** 命令时，可以使用宏定义的名字来取代需要输入的表示接口范围的字符串。

在全局配置模式下使用 no define interface-range macro_name 命令来删除设置的宏定义。

当使用 define interface-range 命令来定义接口范围时，注意：

有效的接口范围格式：

- – **vlan** *vlan-ID - vlan-ID*， VLAN ID 范围 1～4094；
- – **gigabitethernet** *slot*/{*第一个 port*} - {*最后一个 port*}；
- – **Aggregate Port** *Aggregate port 号 - Aggregate port 号*， 范围 1～MAX；

在一个 **interface range** 中的接口必须是相同类型的，即或者全是 switch port，或者全是 Aggregate Port，或者全是 SVI。

下面的例子是如何使用 **define interface-range** 命令来定义 gigabitethernet1/1-4 的宏定义：

```
Ruijie# configure terminal
Ruijie(config)# define interface-range resource
gigabitethernet 1/1-4
Ruijie(config)# end
```

下面的例子显示如何定义多个接口范围段的宏定义：

```
Ruijie# configure terminal
Ruijie(config)# define interface-range ports1to2N5to7
gigabitethernet 1/1-2, 1/5-7
Ruijie(config)# end
```

下面的例子显示使用宏定义 ports1to2N5to7 来配置指定范围的接口：

```
Ruijie# configure terminal
Ruijie(config)# interface range macro ports1to2N5to7
Ruijie(config-if-range)#
```

下面的例子显示如何删除宏定义 ports1to2N5to7：

```
Ruijie# configure terminal
Ruijie(config)# no define interface-range ports1to2N5to7
Ruijie# end
```

1.3.5 选择接口介质类型

有些接口，可以有多种介质类型供用户选择。您可以选择其中一种介质使用。一旦您选定介质类型，接口的连接状态、速度、双工、流控等属性都是指该介质类型的属性，如果您改变介质类型，新选介质类型的这些属性将使用默认值，您可以根据需要重新设定这些属性。

有多种介质类型的接口支持接口介质自动选择。如果您配置接口介质自动选择，在接口只有一种介质连接上时，设备使用当前连接的介质；在接口的两种介质都连接上时，设备将使用您配置的优先介质。介质自动选择优先介质默认为电口，您可以通过配置 medium-type auto-select prefer fiber 来设置优先介质为光口。在自动选择模式下，接口的速度、双工、流控等属性将使用默认值。

配置为介质自动选择的端口，对方端口需要设置为自动协商，不能 disable，否则会出现介质切换错误。

此配置命令只对物理端口有效。Aggregate Port 和 SVI 接口不支持介质类型设置。

此配置命令只对支持介质选择的端口有效。

配置为 Aggregate Port 成员口的端口，其介质类型必须一致，否则无法加入到 AP 中。Aggregate Port 成员口的端口类型不能改变。配置为介质自动选择的接口不能加入 AP。

命令	作用
Ruijie(config-if)# **medium-type { auto-select [prefer [fiber | copper]] | fiber | copper }**	设置端口的介质类型

下面的例子显示了如何设置接口 Gigabitethernet 1/1 的介质类型：

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# medium-type fiber
Ruijie(config-if)# end
```

接口介质切换功能不支持百兆光模块。

1.3.6 配置接口的描述和管理状态

为了有助于您记住一个接口的功能，您可以为一个接口起一个专门的名字来标识这个接口，也就是接口的描述(Description)。您可以根据要表达的含义来设置接口的具体名称，比如，您想将 Gigabitethernet 1/1 分配给用户 A 专门使用，您就可以将这个接口的描述设置为“Port for User A”。

命令	作用
Ruijie(config-if)# **description** *string*	设置接口的描述，最多 32 个字符。

下面的例子显示了如何设置接口 Gigabitethernet 1/1 的描述：

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# description PortForUser A
Ruijie(config-if)# end
```

在某些情况下，您可能需要禁用某个接口。您可以通过设置接口的管理状态来直接关闭一个接口。如果关闭一个接口，则这个接口上将不会接收和发送任何帧，这个接口将丧失这个接口对应的所有功能。您也可以通过设置管理状态来重新打开一个已经关闭的接口。接口的管理状态有两种：Up 和 Down，当端口被关闭时，端口的管理状态为 down，否则为 up。

命令	作用
Ruijie(config-if)# **shutdown**	关闭一个接口

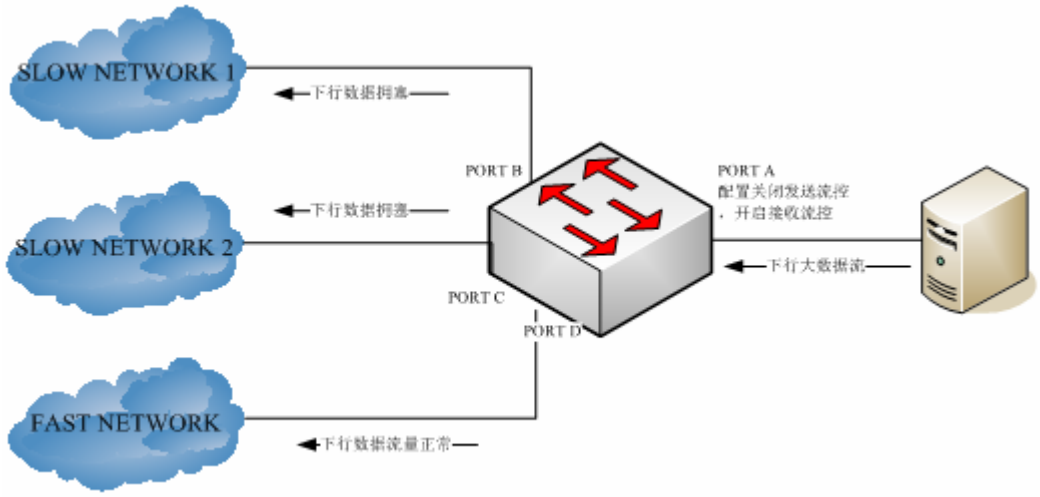
下面的例子描述如何关闭接口 Gigabitethernet 1/2：

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitethernet 1/2
Ruijie(config-if)# shutdown
Ruijie(config-if)# end
```

1.3.7 配置接口的速度、双工、流控和自协商模式

本节描述如何配置接口的速率、双工、流控模式和自协商。流控模式分为非对称流控模式和对称流控模式。在一般情况下，接口开启流控模式后，接口上将会处理接收到的流控帧，并在接口出现拥塞时发送流控帧，接收，发送流控帧的处理是一致的，这就是对称流控模式。但是，在一些情况下，设备希望某个接口能够处理接收到的流控帧保证报文不会因为拥塞而丢弃，又不想发出流控帧而导致整个网络速率下降，这个时候，就要通过配置非对称流控，将接收流控帧和发送流控帧的处理步调分开。如图 2 所示：设备的端口 A 为上联口，端口 B-D 为下联端口，其中端口 B 和 C 对应的是一个慢速网络，假如端口 A 上开启了接收流控和发送流控功能，由于端口 B 和 C 对应的是一个慢速网络，在发送端口 B 的数据流过大，导致端口 B 和 C 拥塞，进而导致端口 A 上的入口拥塞，端口 A 上就会发送流控帧，当上联设备响应流控帧时，就会降低往端口 A 的数据流，间接导致端口 D 上的网速下降。这个时候，可以配置端口 A 的发送流控功能关闭，来保障整个网络带宽利用率。

图 1-2



接口的速率、双工、流控和接口的自协商模式一起决定接口的自协商工作状态。通过参加自动协商的设备发送和接收快速连接脉冲(对于电口)或者编码后的协商信号(对于光口)，设备可以向链路远端的设备通告自己所运行的工作方式，并且侦测远端设备通告的运行方式，通过这些信息的交换，设备自动配置它们工作在最优能力下。

以下配置命令只对 Switch Port，Routed Port 有效。

命令	作用
Ruijie(config-if)# **speed** {**10** | **100** | **1000** | **auto** }	设置接口的速率参数，或者设置为 auto。 1000 只对千兆口有效;
Ruijie(config-if)# **duplex** {**auto** | **full** | **half** }	设置接口的双工模式。 光口支持半双工设置。
Ruijie(config-if)# **flowcontrol** {**auto** | **on** | **off** }	设置接口的流控模式。 当 speed，duplex，flowcontrol 都设为非 auto 模式时，且设置接口的自协商模式为 off 模式时，该

	接口关闭自协商过程。
Ruijie(config-if)# **flowcontrol** {**receive** | **send**} {**auto** | **on** | **off**}	支持非对称流控设备设置非对称流控模式。 当 receive 和 send 模式设置一致时，将同该模式下的 flowcontrol 命令，并显示为同模式下的 flowcontrol 命令
Ruijie(config-if)# **negotiation mode** { **on** | **off** }	设置接口的自协商模式。 接口的自协商模式和接口的自协商工作状态不完全等同，接口的自协商工作状态由接口的速率、双工、流控和自协商模式共同决定。 一般情况下，只要接口的速率、双工和流控中的一种属性为 auto 模式，或者接口的自协商模式为 on 模式，那么接口的自协商工作状态就是 on 的，即接口的自协商功能是打开的；反之，当接口的速率、双工和流控中的属性全部为非 auto 模式，并且接口的自协商模式为 off 模式时，那么接口的自协商工作状态就是 off 的，即接口的自协商功能是关闭的。 对于百兆光口，接口的自协商功能永远都是关闭的，即百兆光口的自协商工作状态永远都是 off 的；对于千兆电口，接口的自协商功能永远都是开启的，即千兆电口的自协商工作状态永远都是 on 的。

在接口配置模式下使用 **no speed**、**no duplex**、**no flowcontrol** 和 **no negotiation mode** 命令，将接口的速率、双工、流控和自协商模式配置恢复为缺省值（自协商）。下面的例子显示如何将 Gigabitethernet 1/1 的速率设为 1000M、双工模式设为全双工、流控关闭，并且设置接口的自协商模式为 on 模式：

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# speed 1000
Ruijie(config-if)# duplex full
Ruijie(config-if)# flowcontrol off
Ruijie(config-if)# negotiation mode on
Ruijie(config-if)# end
```

根据 IEEE 相关标准，千兆电口必须通过协商的方式来确定端口的 Master 或 Slave 状态。

1.3.8 配置接口的MTU

当端口进行大吞吐量数据交换时，可能会遇到大于以太网标准帧长度的帧，这种帧被称为 jumbo 帧。用户可以通过设置端口的 MTU 来控制该端口允许收发的最大帧长。

MTU 是指帧中有效数据段的长度，不包括以太网封装的开销。

端口收到或者转发的帧，如果长度超过设置的 MTU，将被丢弃。

MTU 允许设置的范围为 64~9216 字节，粒度为 4 字节，缺省为 1500 字节。

此配置命令只对物理端口有效。SVI 接口暂时不支持 MTU 设置。

命令	作用
Ruijie(config-if)# **mtu** *num*	设置端口的 MTU Num：<64-9216>

下面的例子显示了如何设置接口 Gigabitethernet 1/1 的 MTU：

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# mtu 64
Ruijie(config-if)# end
```

1.3.9 配置access/trunk port

本节主要讲述配置 Switchport 的操作模式(access/trunk port)及每种模式下的相关配置。

您可在接口配置模式下通过 **switchport** 或其他命令来配置 Switch Port 的相关属性：

命令	作用
Ruijie(config-if)# **switchport mode** {**access** | **trunk** }	配置接口的操作模式。

下例显示如何配置 gigabitethernet 1/2 的操作模式为 access port。

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitethernet 1/2
Ruijie(config-if)# switchport mode access
Ruijie(config-if)# end
```

命令	作用
Ruijie(config-if)# **switchport access vlan** *vlan-id*	配置 access port 所属的 VLAN。

下例显示如何配置 access port gigabitethernet 2/1 所属 vlan 为 100。

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitethernet 2/1
Ruijie(config-if)# switchport access vlan 100
Ruijie(config-if)# end
```

配置 trunk port 的 native VLAN

命令	作用
Ruijie(config-if)# **switchport trunk native vlan** *vlan-id*	配置 trunk port 的 NATIVE VLAN。

下例显示如何配置 Trunk Port Gigabitethernet 2/1 的 Native vlan 为 10。

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitethernet 2/1
Ruijie(config-if)# switchport trunk native vlan 10
Ruijie(config-if)# end
```

配置接口的端口安全，有关端口安全更详细的信息请参照“基于端口的流量控制”：

命令	作用
Ruijie(config-if)# **switchport port-security**	配置接口的端口安全。

下例显示如何打开 Gigabitethernet 2/1 的端口安全。。

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitethernet 2/1
Ruijie(config-if)# switchport port-security
Ruijie(config-if)# end
```

配置接口的速度，双工，流控请参照“配置接口的速度，双工，流控”。

下例显示如何配置 Gigabitethernet 2/1 为 access port，所属 VLAN 为 100，速度，双工，流控为自协商模式，端口安全打开：

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitethernet 2/1
Ruijie(config-if)# switchport access vlan 100
Ruijie(config-if)# speed auto
Ruijie(config-if)# duplex auto
Ruijie(config-if)# flowcontrol auto
Ruijie(config-if)# switchport port-security
Ruijie(config-if)# end
```

1.3.10 配置Hybrid端口

您可以通过以下步骤配置 Hybrid 端口：

命令	作用
configure terminal	进入配置模式
interface *interface-id*	进入接口配置模式 百兆,千兆，万兆
switchport mode hybrid	配置为端口为 hybrid 口
no switchport mode	删除端口模式
switchport hybrid native vlan *id*	设置 hybrid 口的默认 VLAN
switchport hybrid allowed vlan [[**add**] [**tagged** | **untaged**]] |**remove**] **vlist**	设置端口的输出规则

配置举例：

```
Ruijie# configure terminal
Ruijie(config)# interface g 0/1
Ruijie(config-if)# switchport mode hybrid
Ruijie(config-if)# switchport hybrid native vlan 3
Ruijie(config-if)# switchport hybrid allowed vlan untagged 20-30
Ruijie(config-if)# end
Ruijie# show running interface g 0/1
```

1.3.11 配置L2 Aggregate Port

本节主要讲述如何创建 L2 Aggregate Port 及和 L2 Aggregate Port 相关的一些配置。

您可以在接口配置模式下使用 **aggregateport** 来创建 L2 Aggregate Port，具体的配置过程请参照“配置 Aggregate Port”。

1.3.12 配置三层接口

配置三层接口：

命令	作用
Ruijie(config-if)# **no switchport**	将该接口 Shut Down 并且重新转换成三层模式。该命令只适用于 Switch Port 和 L2 Aggregrate port。
Ruijie(config-if)# **ip address** *ip_address subnet_mask* {[**secondary** | **tertiary** | **quartus**][**broadcast**]}	配置 IP 地址和子网掩码。

删除一个三层接口的 IP 地址可以使用接口配置模式的 **no ip address** 命令。

一个 L2 Aggregate Port 的成员口，不能进行 **no switchport** 操作。

下面的例子是描述如何将一个二层接口配置成 Routed Port，并且给该接口分配 IP 地址：

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitethernet 2/1
Ruijie(config-if)# no switchport
Ruijie(config-if)# ip address 192.20.135.21 255.255.255.0
Ruijie(config-if)# no shutdown
Ruijie(config-if)# end
```

1.3.13 配置SVI

本节主要描述如何创建 SVI 及和 SVI 的一些相关配置。

您可在通过 **interface vlan** *vlan-id* 创建一个 SVI 或修改一个已经存在的 SVI。

命令	作用
Ruijie(config)# **interface vlan** *vlan-id*	进入 SVI 接口配置模式。

然后可对 SVI 的相关属性进行配置，详细的信息请参考“配置 IP 单址路由”。

下面的例子显示如何进入接口配置模式，并且给 SVI 100 分配 IP 地址：

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface vlan 100
Ruijie(config-if)# ip address 192.168.1.1 255.255.255.0
Ruijie(config-if)# end
```

1.3.14 配置Routed port

本节描述如何创建 Routed Port 及和 Routed Port 的一些相关配置。

您可在接口模式下，进入某个接口后，使用 **no switchport** 来创建 Routed port。

创建一个 Routed port 并给该 Routed port 分配 IP 地址：

命令	作用
Ruijie(config-if)# **no switchport**	将该接口 Shut Down 并转换成三层模式
Ruijie(config-if)# **ip address** *ip_address subnet_mask*	配置 IP 地址和子网掩码。

当一个接口是 L2 Aggregate Port 的成员口时，是不能用 **switchport/ no switchport** 命令进行层次切换的。

下面的例子显示如何将一个二层接口配置成 Routed Port，并且给该接口分配 IP 地址：

```
Ruijie# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface fastethernet 1/6
Ruijie(config-if)# no switchport
Ruijie(config-if)# ip address 192.168.1.1 255.255.255.0
Ruijie(config-if)# no shutdown
Ruijie(config-if)# end
```

1.3.15 配置L3 Aggregate Port

本节描述如何创建 L3 Aggregate Port 及和 L3 Aggregate Port 的一些相关配置。

您可在接口模式下使用 **no switchport** 将某个 L2 Aggregate Port 转化为 L3 Aggregate Port:

命令	作用
Ruijie(config-if)# **no switchport**	将该接口 Shut Down 并转换成三层模式
Ruijie(config-if)# **ip address** *ip_address subnet_mask*	配置 IP 地址和子网掩码。

下面的例子显示如何创建 L3 Aggregate Port，并且给该接口分配 IP 地址：

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface aggregateport 2
Ruijie(config-if)# no switchport
Ruijie(config-if)# ip address 192.168.1.1 255.255.255.0
Ruijie(config-if)# no shutdown
Ruijie(config-if)# end
```

1.3.16 清除接口的统计值并复位该接口

在特权模式下您可通过 **clear** 命令清除接口的统计值并复位该接口。该命令只对 Switch Port，L2 Aggregrate port 的成员端口，Routed port，L3 Aggregate port 的成员端口有效，以下为 clear 命令：

命令	作用
Ruijie# **clear counters** [*interface-id*]	清除接口统计值。
Ruijie# **clear interrface** *interface-id*	接口硬件复位

接口的统计值可以通过特权模式命令 **show interfaces** 查看，在特权模式下使用 **clear counters** 命令，可以将接口的统计值清零。如果不指定接口，则将所有的 L2 接口计数器清零。

下面的例子显示如何清除 Gigabitethernet 1/1 的计数器：

```
Ruijie# clear counters gigabitethernet 1/1
```

1.3.17 显示接口配置和状态

本节描述接口的显示内容，显示实例。您可在特权模式下通过 **show** 命令可来查看接口状态。在特权模式下您可使用以下命令显示接口状态：

命令	作用
Ruijie# **show interfaces** [*interface-id*]	显示指定接口的全部状态和配置信息。
Ruijie# **show interfaces** *[interface-id]* **status**	显示接口的状态。
Ruijie# **show interfaces** [*interface-id*] **switchport**	显示可交换接口（非路由接口）的 administrative 和 operational 状态信息。
Ruijie# **show interfaces** [*interface-id*] **description**	显示指定接口的描述配置和接口状态。
Ruijie# **show interfaces** [*interface-id*] **counters**	显示指定端口的统计值信息，其中速率显示可能有0.5%内的误差。
Ruijie# **show interfaces** [*interface-id*] **mtu**	显示接口的 MTU 值。
Ruijie# **show interfaces** [*interface-id*] **usage**	显示接口的带宽利用率。
Ruijie# **show interfaces counters vlan** *vlan-id*	显示指定 VLAN 下的成员口的报文统计信息。
Ruijie# **show interfaces counters module** *module-id*	显示指定模块上所有端口的报文统计信息。
Ruijie# **show interfaces counters nonzero**	显示所有报文统计值为非零的端口的报文统计信息。
Ruijie# **show interfaces status vlan** *vlan-id*	显示指定 VLAN 下的成员口的端口状态信息。
Ruijie# **show interfaces status module** *module-id*	显示指定模块上所有端口的端口状态信息。

以下例子为显示接口 Gigabitethernet 1/1 的接口状态：

```
SwitchA#show interfaces gigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is DOWN  , line protocol is DOWN
Hardware is Broadcom 5464 GigabitEthernet
Interface address is: no ip address
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Bridge, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  RXload is 1 ,Txload is 1
  Queueing strategy: FIFO
    Output queue 0/0, 0 drops;
    Input queue 0/75, 0 drops
  Switchport attributes:
    interface's description:""
    medium-type is copper
    lastchange time:0 Day: 0 Hour: 0 Minute:13 Second
    Priority is 0
    admin duplex mode is AUTO, oper duplex is Unknown
    admin speed is AUTO, oper speed is Unknown
```

```
    flow receive control admin status is OFF,flow send control admin status is OFF,flow receive control
oper status is Unknown,flow send control oper status is Unknown
    admin negotiation mode is OFF, oper negotiation status is ON
broadcast Storm Control is OFF,multicast Storm Control is OFF,unicast Storm Control is OFF
 Port-type: trunk
   Native vlan:1
Allowed vlan lists:1-4094                    //Trunk 口的许可 VLAN 列表
Active vlan lists:1, 3-4  //实际生效的 vlan（即该设备上仅创建了 VLAN1、3 和 4）
  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 underruns , 0 dropped
0 output errors, 0 collisions, 0 interface resets
```

以下例子为显示接口 Aggregate Port 3 的接口状态：

```
Ruijie# show interfaces aggregateport 3
Interface   : AggreatePort 3
Description :
AdminStatus : up
OperStatus  : down
Hardware    : -
Mtu         : 1500
LastChange  : 0d:0h:0m:0s
AdminDuplex : Auto
OperDuplex  : Unknown
AdminSpeed  : Auto
OperSpeed   : Unknown
FlowControlAdminStatus : Autonego
FlowControlOperStatus  : Disabled
Priority    : 0
```

以下例子显示接口 GigabitEthernet 1/1 的接口配置信息：

```
Ruijie# show interfaces gigabitEthernet 1/1 switchport
Interface  Switchport Mode      Access    Native    Protected VLAN lists
---------- ---------- --------- --------- --------- --------- ------------
gigabitethernet 1/1      Enabled  Access      1         1         Enabled   All
```

以下例子为显示接口 Gigabitethernet 2/1 的接口描述：

```
Ruijie# show interfaces gigabitethernet 2/1 description
Interface           Status     Administrative    Description
------------  ---------       -----------    -----------------
```

```
gigabitethernet 2/1      down        down         Gi 2/1
Ruijie# show interfaces gigabitethernet 1/2 counters
Interface : gigabitethernet 1/2
5 minute input rate  : 9144 bits/sec, 9 packets/sec
5 minute output rate : 1280 bits/sec, 1 packets/sec
InOctets             : 17310045
InUcastPkts          : 37488
InMulticastPkts      : 28139
InBroadcastPkts      : 32472
OutOctets            : 1282535
OutUcastPkts         : 17284
OutMulticastPkts     : 249
OutBroadcastPkts     : 336
Undersize packets    : 0
Oversize packets     : 0
collisions           : 0
Fragments            : 0
Jabbers              : 0
CRC alignment errors : 0
AlignmentErrors      : 0
FCSErrors            : 0
dropped packet events (due to lack of resources): 0
packets received of length (in octets):
64:46264, 65-127: 47427, 128-255: 3478,
256-511: 658, 512-1023: 18016, 1024-1518: 125
```

以下例子为显示指定端口 GigabitEthernet 0/1 的 MTU 值：

```
Ruijie# show interfaces gigabitethernet 0/1 mtu
Interface                        MTU
-------------------------------- ------
GigabitEthernet 0/1              1500
```

以下例子为显示端口的 MTU 值(仅显示其中部分端口的信息，未显示出全部端口信息)：

```
Ruijie# show interfaces mtu
Interface                        MTU
-------------------------------- ------
GigabitEthernet 1/0/1            1500
GigabitEthernet 1/0/2            1500
GigabitEthernet 1/0/3            1500
GigabitEthernet 1/0/4            1500
GigabitEthernet 1/0/5            1500
```

以下例子为显示指定端口 GigabitEthernet 0/1 的带宽利用率值：

```
Ruijie# show interfaces gigabitethernet 0/1 usage
Interface                         Bandwidth     Bandwidth Usage
--------------------------------- ------------- -----------------
GigabitEthernet 0/1               100000   Kbit 0.0%
```

以下例子为显示端口的带宽利用率值(仅显示其中部分端口的信息，未显示出全部端口信息)：

```
Ruijie# show interfaces usage
Interface                         Bandwidth     Bandwidth Usage
--------------------------------- ------------- -----------------
GigabitEthernet 1/0/1             100000   Kbit 0.0%
GigabitEthernet 1/0/2             1000000  Kbit 0.0%
GigabitEthernet 1/0/3             1000000  Kbit 0.0%
GigabitEthernet 1/0/4             1000000  Kbit 0.0%
GigabitEthernet 1/0/5             1000000  Kbit 0.0%
```

以下例子为显示 VLAN 1 中所有成员端口的报文统计值(仅显示其中部分端口的信息，未显示出全部端口信息)：

```
Ruijie# show interfaces counters vlan 1
Interface : GigabitEthernet 1/0/1
5 minutes input rate  :0 bits/sec, 0 packets/sec
5 minutes output rate :0 bits/sec, 0 packets/sec
InOctets             : 408
InUcastPkts          : 4
InMulticastPkts      : 0
InBroadcastPkts      : 0
OutOctets            : 408
OutUcastPkts         : 4
OutMulticastPkts     : 0
OutBroadcastPkts     : 0
Undersize packets    : 0
Oversize packets     : 0
collisions           : 0
Fragments            : 0
Jabbers              : 0
CRC alignment errors : 0
AlignmentErrors      : 0
FCSErrors            : 0
dropped packet events (due to lack of resources): 0
packets received of length (in octets):
  64 : 0
  65-127 : 4
  128-255 : 0
  256-511 : 0
  512-1023 : 0
```

```
  1024-1518 : 0

Interface : GigabitEthernet 1/0/2
5 minutes input rate  :0 bits/sec, 0 packets/sec
5 minutes output rate :0 bits/sec, 0 packets/sec
InOctets             : 408
InUcastPkts          : 4
InMulticastPkts      : 0
InBroadcastPkts      : 0
OutOctets            : 408
OutUcastPkts         : 4
OutMulticastPkts     : 0
OutBroadcastPkts     : 0
Undersize packets    : 0
Oversize packets     : 0
collisions           : 0
Fragments            : 0
Jabbers              : 0
CRC alignment errors : 0
AlignmentErrors      : 0
FCSErrors            : 0
dropped packet events (due to lack of resources): 0
packets received of length (in octets):
  64 : 0
  65-127 : 4
  128-255 : 0
  256-511 : 0
  512-1023 : 0
  1024-1518 : 0
```

以下例子为显示报文统计值为非零值的端口报文统计信息值(仅显示其中部分端口的信息，未显示出全部端口信息)：

```
Ruijie# show interfaces counters nonzero
Interface : GigabitEthernet 1/0/1
5 minutes input rate  :0 bits/sec, 0 packets/sec
5 minutes output rate :0 bits/sec, 0 packets/sec
InOctets             : 408
InUcastPkts          : 4
InMulticastPkts      : 0
InBroadcastPkts      : 0
OutOctets            : 408
OutUcastPkts         : 4
OutMulticastPkts     : 0
OutBroadcastPkts     : 0
```

```
Undersize packets    : 0
Oversize packets     : 0
collisions           : 0
Fragments            : 0
Jabbers              : 0
CRC alignment errors : 0
AlignmentErrors      : 0
FCSErrors            : 0
dropped packet events (due to lack of resources): 0
packets received of length (in octets):
  64 : 0
  65-127 : 4
  128-255 : 0
  256-511 : 0
  512-1023 : 0
  1024-1518 : 0

Interface : GigabitEthernet 1/0/2
5 minutes input rate  :0 bits/sec, 0 packets/sec
5 minutes output rate :0 bits/sec, 0 packets/sec
InOctets             : 408
InUcastPkts          : 4
InMulticastPkts      : 0
InBroadcastPkts      : 0
OutOctets            : 408
OutUcastPkts         : 4
OutMulticastPkts     : 0
OutBroadcastPkts     : 0
Undersize packets    : 0
Oversize packets     : 0
collisions           : 0
Fragments            : 0
Jabbers              : 0
CRC alignment errors : 0
AlignmentErrors      : 0
FCSErrors            : 0
dropped packet events (due to lack of resources): 0
packets received of length (in octets):
  64 : 0
  65-127 : 4
  128-255 : 0
  256-511 : 0
  512-1023 : 0
```

```
  1024-1518 : 0
```

以下例子为显示模块 1/0 上端口报文统计值(仅显示其中部分端口的信息，未显示出全部端口信息)：

```
Ruijie# show interfaces counters module 1/0
Interface : GigabitEthernet 1/0/1
5 minutes input rate  :0 bits/sec, 0 packets/sec
5 minutes output rate :0 bits/sec, 0 packets/sec
InOctets             : 408
InUcastPkts          : 4
InMulticastPkts      : 0
InBroadcastPkts      : 0
OutOctets            : 408
OutUcastPkts         : 4
OutMulticastPkts     : 0
OutBroadcastPkts     : 0
Undersize packets    : 0
Oversize packets     : 0
collisions           : 0
Fragments            : 0
Jabbers              : 0
CRC alignment errors : 0
AlignmentErrors      : 0
FCSErrors            : 0
dropped packet events (due to lack of resources): 0
packets received of length (in octets):
  64 : 0
  65-127 : 4
  128-255 : 0
  256-511 : 0
  512-1023 : 0
  1024-1518 : 0

Interface : GigabitEthernet 1/0/2
5 minutes input rate  :0 bits/sec, 0 packets/sec
5 minutes output rate :0 bits/sec, 0 packets/sec
InOctets             : 408
InUcastPkts          : 4
InMulticastPkts      : 0
InBroadcastPkts      : 0
OutOctets            : 408
OutUcastPkts         : 4
OutMulticastPkts     : 0
OutBroadcastPkts     : 0
```

```
Undersize packets    : 0
Oversize packets     : 0
collisions           : 0
Fragments            : 0
Jabbers              : 0
CRC alignment errors : 0
AlignmentErrors      : 0
FCSErrors            : 0
dropped packet events (due to lack of resources): 0
packets received of length (in octets):
  64 : 0
  65-127 : 4
  128-255 : 0
  256-511 : 0
  512-1023 : 0
  1024-1518 : 0
```

以下例子为显示 VLAN 1 中所有成员端口的状态值(仅显示其中部分端口的信息，未显示出全部端口信息)：

```
Ruijie# show interfaces status vlan 1
Interface                      Status    Vlan  Duplex   Speed     Type
------------------------------ --------  ----  -------  --------- ------
GigabitEthernet 1/0/18         down      1     Unknown  Unknown   copper
GigabitEthernet 1/0/21         down      1     Unknown  Unknown   copper
GigabitEthernet 1/0/22         down      1     Unknown  Unknown   copper
GigabitEthernet 1/0/23         down      1     Unknown  Unknown   copper
GigabitEthernet 1/0/24         down      1     Unknown  Unknown   copper
GigabitEthernet 1/0/25         down      1     Unknown  Unknown   copper
```

以下例子为显示模块 1/0 中所有端口的状态值(仅显示其中部分端口的信息，未显示出全部端口信息)：

```
Ruijie# show interfaces status module 1/0
Interface                      Status    Vlan  Duplex   Speed     Type
------------------------------ --------  ----  -------  --------- ------
GigabitEthernet 1/0/18         down      1     Unknown  Unknown   copper
GigabitEthernet 1/0/21         down      1     Unknown  Unknown   copper
GigabitEthernet 1/0/22         down      1     Unknown  Unknown   copper
GigabitEthernet 1/0/23         down      1     Unknown  Unknown   copper
GigabitEthernet 1/0/24         down      1     Unknown  Unknown   copper
GigabitEthernet 1/0/25         down      1     Unknown  Unknown   copper
```

1.3.18 显示光模块信息

本节描述光模块信息查看命令，显示实例。您可在特权模式下通过 **show** 命令可来查看光模块信息。在特权模式下您可使用以下命令显示光模块信息：

命令	作用
Ruijie# **show interfaces** [*interface-id*] **transceiver**	显示指定接口的光模块基本信息
Ruijie# **show interfaces** [*interface-id*] **transceiver alarm**	显示指定接口的光模块当前故障告警信息，当没有故障时显示“None”。
Ruijie#**show interfaces** [*interface-id*] **transceiver diagnosis**	显示指定接口的光模块诊断参数的当前测量值。

以下例子显示千兆接口 Gigabitethernet 5/4 的光模块信息：

```
Ruijie#show interfaces gigabitEthernet 5/4 transceiver
Transceiver Type    :  1000BASE-SX-SFP
Connector Type      :  LC
Wavelength(nm)      :  850
Transfer Distance   :
    50/125 um OM2 fiber
        -- 550m
    62.5/125 um OM1 fiber
        -- 270m
Digital Diagnostic Monitoring  : YES
Vendor Serial Number           : 101680093602489
```

以下例子显示千兆接口 Gigabitethernet 5/4 的光模块当前故障告警信息：

```
Ruijie#show interfaces gigabitEthernet 5/4 transceiver alarm
RX  loss of signal
```

下表是 SFP 光模块和 XFP 光模块可能出现的告警信息描述表：

字段	说明
SFP	
RX loss of signal	接收信号丢失
RX power high	接收光功率高告警
RX power low	接收光功率低告警
TX fault	发送错误
TX bias high	偏置电流高告警
TX bias low	偏置电流低告警
TX power high	发送光功率高告警
TX power low	发送光功率低告警
Temp high	温度高告警
Temp low	温度低告警

Voltage high	电压高告警
Voltage low	电压低告警
Transceiver info checksum error	模块信息校验和错误
Transceiver info I/O error	模块信息读写错误
Transceiver type and port configuration mismatch	模块类型和端口速率配置不匹配
Transceiver type not supported by port hardware	端口不支持该类型模块
XFP	
RX loss of signal	接收信号丢失
RX not ready	接收状态未就绪
RX CDR loss of lock	RX CDR 时钟失锁
RX power high	接收光功率高告警
RX power low	接收光功率低告警
TX fault	发送错误
TX CDR loss of lock	TX CDR 时钟失锁
TX bias high	偏置电流高告警
TX bias low	偏置电流低告警
TX power high	发送光功率高告警
TX power low	发送光功率低告警
Module not ready	模块状态未就绪
Temp high	温度高告警
Temp low	温度低告警
Voltage high	电压高告警
Voltage low	电压低告警
Transceiver info checksum error	模块信息校验错误
Transceiver info I/O error	模块信息读写错误
Transceiver type and port configuration mismatch	模块类型和端口速率配置不匹配
Transceiver type not supported by port hardware	端口不支持该类型该模块

以下例子显示千兆接口 Gigabitethernet 5/4 的光模块诊断参数的当前测量值：

```
Ruijie#show interfaces gigabitEthernet 5/4 transceiver diagnosis
Current diagnostic parameters[AP:Average Power]:
Temp(Celsius)   Voltage(V)      Bias(mA)            RX power(dBm)       TX power(dBm)
38(OK)          3.20(OK)        0.04(OK)            -40.00(alarm)[AP]   -40.00(alarm)
```

下表是光模块诊断参数显示信息描述表：

字段	说明
diagnostic information	接口携带的光模块的数字诊断信息
Current diagnostic parameters	当前的诊断参数
Temp.(°C)	数字诊断参数——温度，单位为°C，精确到 1°C。
Voltage(V)	数字诊断参数——电压，单位为 V，精确到 0.01V。
Bias(mA)	数字诊断参数——偏置电流，单位为 mA，精确到 0.01mA。

RX power(dBM)	数字诊断参数——接收光功率，单位为 dBM。
TX power(dBM)	数字诊断参数——发送光功率，单位为 dBM，精确到 0.01dBM。
OK	表示当前状态正常，无需用户干预
warning	表示当前状态超过设备允许状态，需要用户注意。
alarm	表示当前状态严重超过设备允许状态，需要用户立即采取行动

☑ 光模块信息显示，故障告警和诊断参数测量功能需要配合锐捷网络的光模块使用。

☑ 光模块故障告警(光模块类型和端口速率配置不匹配告警、端口不支持该类型光模块告警除外)和诊断参数测量需要光模块支持 Digital Diagnostic Monitoring 功能才能显示。

1.3.19 光模块防伪检测

为了防止非我司原厂认证的光模块在使用过程中可能出现质量问题(非我司原厂认证的光模块质量无法得到保障)，导致用户数据通信质量受到影响，我司提供了光模块防伪检测功能，针对非我司原厂认证的光模块插入到我司设备上后，将会被自动识别出来并进行告警。我司设备的光模块防伪检测功能缺省是开启的，用户也可以通过配置来关闭设备的光模块防伪检测功能。

关闭设备的光模块防伪检测功能的命令必须在全局配置模式下执行，具体配置如下：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式
Ruijie(config)# **fiber antifake ignore**	关闭设备的光模块防伪检测功能

用户也可以通过执行 **no fiber antifake ignore** 命令来重新开启设备的光模块防伪检测功能。

以下是关闭设备的光模块防伪检测功能的例子：

```
Ruijie# configure terminal
Ruijie(config)# fiber antifake ignore
```

1.3.20 line-detect线缆检测

管理员可以通过线缆检测命令来检测线缆的工作状况。在线缆处于短路、断路等异常状态时，线缆检测有助于正确判断线缆的工作状况。

此命令必须在接口模式下执行，具体配置如下：

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **interface** *interface*	进入接口模式
Ruijie(config-if)# **line-detect**	执行线缆检测

1. 只有电介质的物理口才支持线缆检测，光介质物理口、AP 口不支持线缆检测。

2. 在正常连接的接口执行线缆检测，会导致连接暂时断掉，然后再重新建立连接。

以下是利用此命令进行线缆检测的例子：

```
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#line-detect
Interface : GigabitEthernet 0/1
start cable-diagnoses,please wait...
cable-daignoses end!this is result:
4 pairs
pair state      length(meters)
---- ---------- --------------
A    Ok         1
pair state      length(meters)
---- ---------- --------------
B    Ok         2
pair state      length(meters)
---- ---------- --------------
C    Short      1
pair state      length(meters)
---- ---------- --------------
D    Short      1
```

显示项解释：

显示项	说明
pairs	是指线缆里面包含的线对数目，如双绞线是由四对线组合而成。
State	当前线对的状态，共有四个值：OK（正常），Short（短路），Open（断路），Crosstalk（若即若离）。正常情况下，百兆双绞线 A、B 两对为 OK，C、D 两对为 Short。千兆双绞线 A、B、C、D 四对均为 OK。 Crosstalk 表示线路的信号存在不稳定的状况，信号时有时无。
Length	线缆的长度，单位为米。只有 state 为非 OK 的线对的长度才有效。另外，由于线缆长度是根据信号的传递时间来计算的，所以可能存在一定的误差。状态为 Short 或者 Open 对应的 length 是指端口到线缆故障点的长度。

管理员还可以通过线缆检测 show interface 命令来查看指定端口或全部端口的线缆检测状态。

1.3.21 配置LinkTrap策略

在设备中可以基于接口配置是否发送该接口的 LinkTrap，当功能打开时，如果接口发生 Link 状态变化，SNMP 将发出 LinkTrap,反之则不发。缺省情况下，该功能打开。

配置命令

命令	作用
Ruijie(config-if)# **[no] snmp trap link-status**	打开或者关闭发送该接口 link trap 的功能.

配置举例

下面配置将配置接口为不发送 Link trap：

```
Ruijie(config)# interface gigabitEthernet 1/1
Ruijie(config-if)# no snmp trap link-status
```

2 MAC 地址

2.1 概述

通过识别报文的数据链路层信息对报文转发是以太网交换机的主要功能（称为二层转发功能），以太网交换机通过报文所携带的目的 MAC 地址信息将报文转发到相应的端口，以太网交换机采用 MAC 地址表存储报文转发时所需要的目的 MAC 地址与端口信息关系。

以太网交换机的 MAC 地址表中所有的 MAC 地址都和 VLAN 相关联，不同的 VLAN 允许相同的 MAC 地址。每个 VLAN 都维护它自己逻辑上的一份地址表。一个 VLAN 已学习的 MAC 地址，对于其他 VLAN 而言可能是未知的，仍然需要学习。

以太网交换机的 MAC 地址包含以下信息：

图 2-1 MAC 地址表项构成

- 状态：表示地址表项为动态地址、静态地址或过滤地址。
- VLAN：MAC 地址所属的 VLAN
- MAC 地址：表项的 MAC 地址信息
- 端口：MAC 地址对应的端口信息

以太网交换机的 MAC 地址表中的表项通过以下两种方式进行更新和维护：

- 动态地址学习
- 手工配置地址

以太网交换机在转发报文时通过报文的目的 MAC 地址以及报文所属的 VLAN ID 的信息在 MAC 地址表中查找相应的转发输出端口，根据查找的结果采取单播、组播或广播的方式转发报文：

- 单播转发：以太网交换机能够在 MAC 地址表中查到与报文的目的 MAC 地址和 VLAN ID 相对应的表项并且表项中的输出端口是唯一的，报文直接从表项对应的端口输出。
- 组播转发：以太网交换机能够在 MAC 地址表中查到与报文的目的 MAC 地址和 VLAN ID 相对应的表项并且表项中对应一组输出端口，报文直接从这组端口输出。
- 广播转发：以太网交换机收到目的地址为 ffff.ffff.ffff 的报文或者在 MAC 地址表中查找不到对应的表项时，报文被送到所属的 VLAN 中除报文输入端口外的其他所有端口输出。

本文只涉及动态地址、静态地址与过滤地址的管理，组播地址的管理不在本文内描述，请参看 IGMP Snooping 配置指南。

2.1.1 动态地址学习

动态地址

通过以太网交换机的自动地址学习过程产生的 MAC 地址表项被称为动态地址，只有动态地址才会被地址表的老化机制所删除。

地址学习过程

通常情况下 MAC 地址表的维护都是通过动态地址学习的方式进行，其工作原理如下：

1) 以太网交换机的 MAC 地址表为空的情况下，UserA 要与 UserB 进行通讯，UserA 首先发送报文到交换机的端口 GigabitEthernet 0/2，此时以太网交换机将 UserA 的 MAC 地址学习到 MAC 地址表中。
由于地址表中没有 UserB 的源 MAC 地址，因此以太网交换机以广播的方式将报文发送到除了 UserA 以外的所有端口，包括 User B 与 User C 的端口，此时 UserC 能够收到 UserA 所发出的不属于它的报文。

图 2-2 动态地址学习步骤一

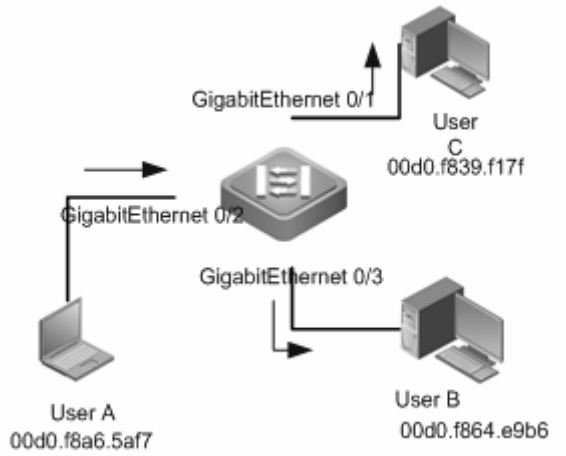


图 2-3 以太网交换 MAC 地址表一

Status	VLAN	MAC地址	端口
动态	1	00d0.f8a6.5af7	GigabitEthernet 0/2

2) UserB 收到报文后将回应报文通过以太网交换机的端口 GigabitEthernet 0/3 发送 UserA，此时以太网交换机的 MAC 地址表中已存在 UserA 的 MAC 地址，所以报文被以单播的方式转发到 GigabitEthernet 0/2 端口，同时以太网交换机将学习 UserB 的 MAC 地址，与步骤 1 中所不同的是 UserC 此时接收不到 UserB 发送给 UserA 的报文。

图 2-4 动态地址学习步骤二

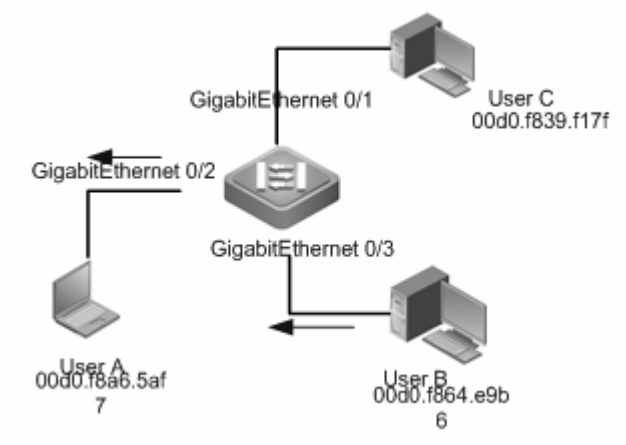


图 2-5 以太网交换机 MAC 地址表二

Status	VLAN	MAC地址	端口
动态	1	00d0.f8a6.5af7	GigabitEthernet 0/2
动态	1	00d0.f864.e9b6	GigabitEthernet 0/3

3) 通过 UserA 与 UserB 的一次交互过程后，以太网交换机学习到了 UserA 与 UserB 的源 MAC 地址，之后 UserA 与 UserB 之间的报文交互则采用单播的方式进行转发，此后 UserC 将不再接收到 UserA 与 UserB 之间的交互报文。

地址老化

以太网交换机的 MAC 地址表是有容量限制的，以太网交换机采用地址表老化机制进行不活跃的地址表项淘汰。

以太网交换机在学习到一个新的地址的同时启动该地址的老化记时，在达到老化记时前，如果以太网交换机没有再一次收到以该地址为源 MAC 地址的报文，那该地址在达到老化时间后会从 MAC 地址表中删除。

2.1.2 VLAN 的动态地址个数限制

以太网交换机的 MAC 地址表的容量是有限制的并且所有的 VLAN 共享整个 MAC 地址表容量，为避免一个 VLAN 内大量动态地址将整个 MAC 地址表所占用而使其他 VLAN 无法学习动态地址，导致其他 VLAN 的报文都采用广播方式转发，锐捷以太网交换机提供了 VLAN 的动态地址个数限制功能，用户可以规划各个 VLAN 内可学习的动态地址数，为每个 VLAN 配置可动态学习的地址的个数上限。

配置了 VLAN 的动态地址个数限制功能的 VLAN 只能够学到用户所指定个数的 MAC 地址，对超出用户配置上限部份的地址将不再学习，以这些地址为目的地址的报文将以广播方式转发。

- 如果配置 VLAN 的动态地址学习个数限制的上限小于当前 VLAN 中已学习到的动态地址数，此时以太网交换机不再学习该 VLAN 中的地址，直到 VLAN 内的地址数通过地址老化删除到小于上限后，设备才会重新学习。
- MAC 地址复制功能，复制到指定 VLAN 的 MAC 地址表项，不受该 VLAN 下动态 MAC 地址学习个数的限制。

2.1.1 接口的动态地址个数限制

工作原理

配置了接口的动态地址个数限制功能的接口只能够学到用户所指定个数的 MAC 地址，对超出用户配置上限部份的地址将不再学习，以这些地址为目的地址的报文将以广播方式转发。

> 如果配置接口的动态地址学习个数限制的上限小于当前接口下已学习到的动态地址数，此时设备不再学习该接口下的地址，直到接口下的地址数通过地址老化删除到小于上限后，设备才会重新学习。

2.1.2 静态地址

手工配置的 MAC 地址表项，用于绑定 MAC 地址与端口关系，这类地址只能通过手工配置添加和删除，保存配置后设备重启，静态地址也不会丢失。

通过手工配置静态地址的方式可以在 MAC 地址表中绑定设备下接的网络设备的 MAC 地址与端口关系。

2.1.3 过滤地址

手工配置的 MAC 地址表项，用于在以太网交换机上丢弃以所配置的 MAC 地址为源地址或目的地址的报文，这类地址只能通过手工配置添加和删除，保存配置后设备重启，过滤地址也不会丢失。

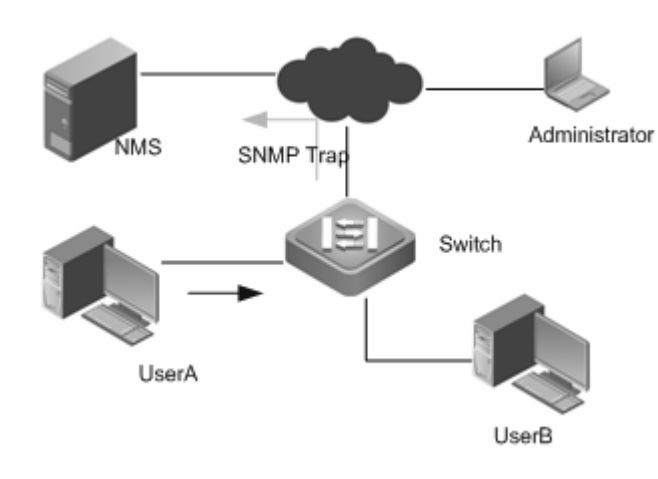
通过手工将网络中的非法接入用户的源 MAC 地址配置为过滤地址的方式可以实现过滤非法接入用户。

> 过滤地址对送 CPU 的报文无效。如：某个 ARP 报文的二层源 MAC 为一过滤地址，此时该 ARP 报文仍然会被送往 CPU，但其并不会被转发。

2.1.4 MAC 地址变化通知

以太网交换机的 MAC 地址通知功能通过与网络管理工作站（NMS）的协作为网络管理提供了监控网络以太网交换机下用户变化的机制。

图 2-6 地址变化通告



打开 MAC 地址通知的功能后，当以太网交换机学习到一个新的 MAC 地址或老化掉一个已学习到的 MAC 地址时，一个反映 MAC 地址变化的通知信息就会产生，并以 SNMP Trap 的方式将通知信息发送给指定的 NMS(网络管理工作站)。

当一个 MAC 地址增加的通知产生，就可以知道一个由此 MAC 地址标识的新用户开始使用网络，当一个 MAC 地址删除的通知产生，则表示一个用户在地址老化时间内没有新的报文发送，通常可以认为此用户已经停止使用网络了。

当使用以太网交换机下接的用户较多时，可能会出现在短时间内会有大量的 MAC 地址变化产生，导致网络流量增加。为了减轻网络负担，可以设置发送 MAC 地址通知的时间间隔。在达到配置的时间间隔之后，系统将这个时间内的通知信息封装成多个通知信息，此时在每条地址通知信息中，就包含了若干个 MAC 地址变化的信息，从而可以会有效地减少网络流量。

当 MAC 地址通知产生时，通知信息同时会记录到 MAC 地址通知历史记录表中。此时即便没有配置接收 Trap 的 NMS，管理员也可以通过查看 MAC 地址通知历史记录表来了解最近 MAC 地址变化的消息。

MAC 地址通知仅对动态地址有效，对于配置的静态地址与过滤地址的变化将不会产生通知信息。

2.1.5 IP 和 MAC 地址绑定

概述

通过手动配置 IP 和 MAC 地址绑定功能，可以对输入的报文进行 IP 地址和 MAC 地址绑定关系的验证。如果将一个指定的 IP 地址和一个 MAC 地址绑定，则设备只接收源 IP 地址和 MAC 地址均匹配这个绑定地址的 IP 报文；否则该 IP 报文将被丢弃。

利用地址绑定这个特性，可以严格控制设备的输入源的合法性。需要注意的是，通过地址绑定控制交换机的输入，将优先于 802.1X、端口安全以及 ACL 生效。

地址绑定模式

地址绑定的模式分为:兼容，宽松，严格三种模式，默认模式为严格模式。其相应的转发规则，见下表所示：

模式	IPv4 报文转发规则	IPv6 报文转发规则

严格	符合 IPV4+MAC 条件的报文转发	所有 IPV6 报文均不转发
宽松	符合 IPV4+MAC 条件的报文转发	所有 IPV6 报文均可转发
兼容	符合 IPV4+MAC 条件的报文转发	源 MAC 为绑定地址的 MAC 地址的 IPV6 报文转发

地址绑定例外端口

IP 地址和 MAC 地址绑定功能缺省对设备上的所有端口都生效，通过配置例外口的方式可以在使绑定功能在部份端口上不生效。

在应用中设备的上链端口的 IP 报文的绑定关系是不确定的，通常将设备的上链端口配置为例外口，此时上链端口则不进行 IP 地址与 MAC 地址的绑定检查。

2.1.6 认证失败用户的地址

在设备开启 WEB 认证、MAB 认证或 802.1X 认证时，如果下联终端用户发起认证，并没有通过认证，该用户的 MAC 地址会被设备记录下来，以备查看。

这些认证失败用户的地址，被记录在设备上是有时间限度的，超过时间限度后，记录被清除。目前，这个时间限度和 MAC 地址老化时间相同。

2.2 协议规范

《IEEE Std 802.3™ Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications》

《IEEE Std 802.1Q™ Virtual Bridged Local Area Networks》

2.3 配置MAC地址

2.3.1 缺省配置

功能特性	缺省值
动态地址老化时间	300 秒
端口 MAC 地址学习能力	开启
动态地址同步功能	关闭
MAC 地址变化通知功能	关闭
地址绑定模式	compatible

2.3.2 配置动态地址

配置端口 MAC 地址学习能力

命令	作用
Ruijie(config-if)# **no mac-address-learning**	关闭端口 MAC 地址学习能力，通过 show mac-address-learning 命令查看端口学习能力配置

MAC 地址学习能力缺省开启，如果端口上配置了 DOT1X，IP SOURCE GUARD 绑定，端口安全功能，端口的学习能力不能开启；同样，关闭端口学习能力的端口不能开启接入控制功能。

清除动态地址

命令	作用
Ruijie#**clear mac-address-table dynamic**	删除设备上所有的动态地址
Ruijie#**clear mac-address-table dynamic address** *mac-address* **vlan** *vlan-id*	删除特定 MAC 地址 *mac-address*：指定要删除的 MAC 地址。 *vlan-id*：指定要删除的 MAC 地址所在的 VLAN。
Ruijie#**clear mac-address-table dynamic interface** *interface-id* [**vlan** *vlan-id*]	删除特定物理接口或 Aggregate Port 上的特定 VLAN 中的所有动态地址或接口上所有动态地址。 *interface-id*：指定的物理接口或是 Aggregate Port。 *vlan-id*：指定删除动态地址所属的 VLAN。
Ruijie#**clear mac-address-table dynamic vlan** *vlan-id*	删除特定 VLAN 上的所有动态地址 *vlan-id*：指定所要删除的动态地址所属的 VLAN。

下面的例子说明了如何配置删除设备接口 GigabitEthernet 0/1 下 VLAN 1 中的所有动态地下。

```
Ruijie#clear mac-address-table dynamic interface GigabitEthernet 0/1 vlan 1
```

查看配置

命令	作用
Ruijie#**show mac-address-table dynamic**	查看设备上所有的动态地址信息。
Ruijie#**show mac-address-table dynamic address** *mac-address* [**vlan** *vlan-id*]	查看设备上特定动态 MAC 地址信息。 *mac-address*：查看的 MAC 地址。 vlan-id：查看特定的 VLAN 中的特定 MAC 地址。
Ruijie#**show mac-address-table dynamic interface** *interface-id* [**vlan** *vlan-id*]	查看设备上指定物理接口或 Aggregate Port 下的动态地址信息。 *interface-id*：指定的物理接口或是 Aggregate Port。 *vlan-id*：查看特定的 VLAN 中的动态地址。
Ruijie#**show mac-address-table dynamic vlan** *vlan-id*	查看设备上指定 VLAN 下的动态地址信息。 *vlan-id*：查看特定的 VLAN 中的动态地址。

Ruijie# **show mac-address-table count [interface** *interface-id* **| vlan** *vlan-id***]**	查看地址表的统计信息。 *interface-id*：查看指定接口的地址表项统计信息。 *vlan-id*：查看指定 VLAN 下的地址表项统计信息。

下面的例子说明了如何查看设备上物理接口 GigabitEthernet 0/1 下 VLAN 中的所有动态 MAC 地址信息。

```
Ruijie#show mac-address-table dynamic interface gigabitEthernet 0/1 vlan 1
Vlan          MAC Address           Type      Interface
----------  -------------------- -------- --------------------
   1          0000.5e00.010c        DYNAMIC  GigabitEthernet 0/1
   1          00d0.f822.33aa        DYNAMIC  GigabitEthernet 0/1
   1          00d0.f822.a219        DYNAMIC  GigabitEthernet 0/1
   1          00d0.f8a6.5af7        DYNAMIC  GigabitEthernet 0/1
```

下面的例子说明了如何查看设备上的地址表统计信息：

例 1：显示 MAC 地址各类型的表项数量：

```
Ruijie# show mac-address-table count
Dynamic Address Count  : 30
Static  Address Count  : 0
Filtering Address Count: 0
Total Mac Addresses    : 30
Total Mac Address Space Available: 8159
```

例 2：显示 VLAN 1 下的 MAC 地址数量：

```
Ruijie# show mac-address-table count vlan 1
Dynamic Address Count  : 7
Static  Address Count  : 0
Filter  Address Count  : 0
Total Mac Addresses     : 7
```

例 3：显示 interface g0/1 下的 MAC 地址数量：

```
Ruijie# show mac-address-table interface g0/1
Dynamic Address Count  : 10
Static  Address Count  : 0
Filter  Address Count  : 0
Total Mac Addresses     : 10
```

MAC 地址表的总有效地址空间为 16384。

2.3.3 配置动态地址老化时间

配置老化时间

命令	作用
Ruijie(config)# **mac-address-table agint-time** [*0*|*10-1000000*]	设置一个地址被学习后将保留在动态地址表中的时间长度，单位是秒，范围是 10－1000000 秒，缺省为 300 秒。当你设置这个值为 0 时，地址老化功能将被关闭，学习到的地址将不会被老化。
Ruijie(config)# **no mac-address-table agint-time**	恢复地址老化时间为缺少值。

下面的例子说明了如何配置设备的地址老化时间为 180 秒。

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#mac-address-table aging-time 180
```

查看配置

命令	作用
Ruijie#**show mac-address-table aging-time**	查看所有的地址老化配置信息

下面的例子说明了如何查看设备上的地址老化时间配置。

```
Ruijie#show mac-address-table aging-time
Aging time    : 180 seconds
```

地址表的实际老化时间会与设定值存在一定偏差，但不会超过设定值的 2 倍。老化时间范围为 10－630 秒。

2.3.4 配置 VLAN 的动态地址个数限制

配置 VLAN 动态地址个数限制

命令	作用
Ruijie(config)#**vlan** *vlan-id*	进入指定的 VLAN 配置模式
Ruijie (config-vlan)# **max-dynamic-mac-count** <1-32768>	配置 VLAN 可动态学习的地址数目

VLAN 的动态地址学习个数限制通过 no max-dynamic-mac-count 命令关闭，下面的例子说明了如何配置 VLAN1 的动态地址学习个数为 160 个：

```
Ruijie#configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#vlan 1
Ruijie(config-vlan)#max-dynamic-mac-count 160
```

查看配置

- 查看指定 VLAN 的动态地址学习个数限制

```
Ruijie#show mac-address-table max-dynamic-mac-count vlan 1
vlan limit   mac count learning
---- ------- --------- --------
1    160        6         YES
```

- 查看所有 VLAN 的动态地址学习个数限制

```
Ruijie#show mac-address-table max-dynamic-mac-count
vlan limit   mac count learning
---- ------- --------- --------
1    160      6         YES
3    500      124       YES
```

2.3.5 配置端口的动态地址个数限制

配置端口动态地址个数限制

命令	作用
Ruijie(config) int GigabitEthernet 0/1	进入指定的端口配置模式
Ruijie (config-if)# **max-dynamic-mac-count** <1-32768>	配置端口可动态学习的地址数目

端口的动态地址学习个数限制通过 no max-dynamic-mac-count 命令关闭，下面的例子说明了如何配置端口 0/1 的动态地址学习个数为 160 个：

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#int GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#max-dynamic-mac-count 160
```

查看配置

- 查看指定端口的动态地址学习个数限制

```
Ruijie#show mac-address-table max-dynamic-mac-count interface GigabitEthernet 0/1
```

```
Interface                Limit   MAC count Learning
------------------------ ------- --------- --------
GigabitEthernet 0/1      1000     0          YES
```

■ 查看所有端口的动态地址学习个数限制

```
Ruijie#show mac-address-table max-dynamic-mac-count interface
Interface                Limit   MAC count Learning
------------------------ ------- --------- --------
GigabitEthernet 0/1      1000     0          YES
GigabitEthernet 0/2      1000     0          YES
```

2.3.6 配置静态地址

管理静态地址

命令	作用
Ruijie(config)# **mac-address-table static** *mac-address* **vlan** *vlan-id* **interface** *interface-id*	*mac-address*：指定表项对应的目的 MAC 地址。 *vlan-id*：指定该地址所属的 VLAN。 *interface-id*：包将转发到的接口(可以是物理端口或 Aggregate Port)。 当设备在 vlan-id 指定的 VLAN 上接收到以 mac-address 为目的地址的报文时，这个报文将被转发到 interface-id 所指定的接口上。
Ruijie(config)# **no mac-address-table static** *mac-address* **vlan** *vlan-id* **interface** *interface-id*	删除静态地址表项，参数与添加命令一致。

下面的例子说明了如何配置添加一个静态地址 00d0.f800.073c，当在 VLAN 4 中接收到目的地址为该地址的报文时，这个报文将被转发到指定的接口 Gigabitethernet 0/3 上。

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# mac-address-table static 00d0.f800.073c vlan 4 interface gigabitethernet 0/3
```

下面的例子说明了如何配置删除上一例子中添加的静态地址 00d0.f800.073c。

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#no mac-address-table static 00d0.f800.073c vlan 4 interface gigabitethernet 0/3
```

查看配置

命令	作用
Ruijie# **show mac-address-table static**	查看所有的静态地址信息

下面的例子说明了如何查看设备上的所有静态地址信息。

```
Vlan          MAC Address           Type       Interface
----------  -------------------- -------- --------------------
   4        00d0.f800.073c        STATIC    GigabitEthernet 0/3
```

2.3.7 配置过滤地址

管理过滤地址

命令	作用
Ruijie(config)# **mac-address-table filtering** *mac-address* **vlan** *vlan-id*	*mac-address*：指定表项对应的 MAC 地址 *vlan-id*：指定该地址所属的 VLAN 当设备在 vlan-id 指定的 VLAN 上接收到以 mac-address 指定的地址为源地址或目的地址的报文将被丢弃。
Ruijie(config)# **no mac-address-table filtering** *mac-address* **vlan** *vlan-id*	删除过滤地址表项，参数与添加命令一致。

下面的例子说明了如何配置添加过滤地址。当在 VLAN 4 中接受到源地址或目的地址为 00d0.f800.073c 的报文时，将丢弃此报文。

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#mac-address-table filtering 00d0.f800.073c vlan 4
```

下面的例子说明了如何配置删除上一例子中的过滤地址 00d0.f800.073c。

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#no mac-address-table filtering 00d0.f800.073c vlan 4
```

查看配置

命令	作用
Ruijie#**show mac-address-table filtering**	查看过滤地址信息

下面的例子说明了如何查看设备上的所有静态地址信息。

```
Vlan          MAC Address           Type       Interface
-------  --------------- -------------------     -------------------
 4       00d0.f800.073c    FILTER                    GigabitEthernet 0/3
```

2.3.8 配置 MAC 地址变化通知

配置 MAC 地址变化通知

缺省情况下，MAC 地址的全局开关被关闭，所有接口的 MAC 地址通知功能也均被关闭。

配置设备 MAC 地址通知功能：

命令	作用
Ruijie(config)# **snmp-server host** *host-addr* **traps** [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**] }] *community-string*	配置接收 MAC 地址通知的 NMS。 *host-addr*：指明接收者的 IP。 **version**：指明发送哪种版本的 snmp trap 报文，对 v3 版本还可以指定是否认证以及安全等级参数。
Ruijie (config)#**snmp-server enable traps**	使能设备发送 trap 功能 。
Ruijie(config)#**mac-address-table notification**	打开 MAC 地址通知功能开关。
Ruijie(config)# **mac-address-table notification** { **interval** *value* | **history-size** *value*}	配置 MAC 地址通知的时间间隔与历史记录容量。 **interval** *value* ：设置产生 MAC 地址通知的时间间隔(可选)。时间间隔的单位为秒，范围为 1－3600，缺省为 1 秒。 **history-size** *value* ：MAC 通知历史记录表中记录的最大个数，范围 1－200，缺省为 50。
Ruijie(config-if)# **snmp trap mac-notification** {**added** |**removed**}	打开接口的 MAC 地址通知功能。 **added**：当地址增加时通知。 **removed**：当地址被删除时通知。

下面的例子说明了如何打开 MAC 地址通知功能，并以 public 为认证名向 IP 地址为 192.168.12.54 的 NMS 发送 MAC 地址变化通知的 Trap，产生 MAC 地址变化通知的间隔时间为 40 秒，MAC 地址通知历史记录表的大小为 100，打开接口 Gigabitethernet 0/1 上当 MAC 地址增加和减少时进行通知的功能：

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#snmp-server host 192.168.12.54 traps public
Ruijie(config)#snmp-server enable traps
Ruijie(config)#mac-address-table notification
Ruijie(config)#mac-address-table notification interval 40
Ruijie(config)#mac-address-table notification  history-size 100
Ruijie(config)#interface GigabitEthernet 0/1
Ruijie(config-if)#snmp trap mac-notification added
Ruijie(config-if)#snmp trap mac-notification removed
```

查看配置

在特权模式下，使用下表所列的命令来查看设备的 MAC 地址表信息：

命令	作用
Ruijie# **show mac-address-table notification**	查看 MAC 地址变化通知功能的全局配置信息。
Ruijie# **show mac-address-table notification interface**	查看接口的 MAC 地址变化通知的使能状况。
Ruijie# **show mac-address-table notification history**	查看 MAC 地址变化通知信息的历史记录表。

下面是查看 MAC 地址变化通知信息的例子。

查看 MAC 地址通知功能的全局配置信息：

```
Ruijie#show mac-address-table notification
MAC Notification Feature : Enabled
Interval(Sec): 2
Maximum History Size : 154
Current History Size : 2
Ruijie# show mac-address-table notification interface
Interface           MAC Added Trap  MAC Removed Trap
----------------- -------------- ----------------
Gi0/1                Disabled        Enabled
Gi0/2                Disabled        Disabled
Gi0/3                Enabled         Enabled
Gi0/4                Disabled        Disabled
Gi0/5                Disabled        Disabled
Gi0/6                Disabled        Disabled
Ruijie#show mac-address-table notification history
History Index:1
Entry Timestamp: 15091
MAC Changed Message :
Operation   VLAN  MAC Address    Interface
----------- ---- -------------- --------------------
Added         1    00d0.f808.3cc9  Gi0/1
Removed      1     00d0.f808.0c0c  Gi0/1
History Index:2
Entry Timestamp: 21891
MAC Changed Message :
Operation   VLAN  MAC Address    Interface
----------- ---- -------------- --------------------
Added       1      00d0.f80d.1083 Gi0/1
```

2.3.9 配置 IP 地址和 MAC 地址绑定

配置 IP 地址和 MAC 地址绑定

在全局模式下，可以通过以下步骤来设置地址绑定：

命令	作用
Ruijie(config)# **address-bind** *ip-address mac-address*	配置 IP 地址和 MAC 地址的绑定关系 *ip-address*：绑定的 IP 地址 *mac-address*：绑定的 MAC 地址
Ruijie(config)# **address-bind install**	使 IP 和 MAC 地址绑定生效

在全局配置模式下使用 **no address-bind** *ip-address mac-address* 删除一个 IP 地址和 MAC 地址的绑定项。

通过 **no address-bind install** 命令可关闭绑定功能，使地址绑定配置不生效。

下面是配置 IP 地址和 MAC 地址绑定模式的例子：

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#address-bind 192.168.5.1 00d0.f800.0001
Ruijie(config)#address-bind install
```

如果执行 address-bind install 之后，没有配置 IP+MAC 绑定，则所有 IP+MAC 绑定功能不生效，所有报文可以通过。

在全局 IP+MAC 绑定和 DOT1X 基于用户认证共用，并且安全通道开启时，全局 IP+MAC 绑定和 DOT1X 认证用户是并集关系，即符合全局绑定或者 DOT1X 的用户都可以通信。

配置地址绑定模式

命令	作用
Ruijie(config)# **address-bind ipv6-mode { compatible | loose | strict }**	配置地址绑定模式 **compatible**：兼容模式 **loose**：宽松模式 **strict**：严格模式
Ruijie(config)# **no adress-bind ipv6-mode**	恢复地址绑定模式为缺省值

下面是配置地址绑定模式为严格模式的例子：

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#address-bind ipv6-mode strict
```

设置 IPV6 模式对 **DHCP Snooping** 的地址绑定，端口安全的 MAC+IP 等多种 MAC+IP 绑定功能同时生效。对于某些产品的端口安全等功能支持 IPV6 的安全地址，IPV6 模式下的转发规则，如下表所示：

模式	Ipv4 转发规则	IPV6 转发规则
严格模式	只允许符合 IPV4+MAC 条件的报文转发。	只允许符合 IPV6 安全地址配置的 IPV6 报文转发。

宽松模式	只允许符合 IPV4+MAC 条件的报文转发。	允许所有的 IPV6 报文转发。
兼容模式	只允许符合 IPV4+MAC 条件的报文转发。	只允许源 MAC 为绑定的 MAC 地址，或符合 IPV6 安全地址配置的 IPV6 报文转发。 当安全通道开启时，IPV6 兼容模式与端口安全/DOT1X 基于端口认证共用时，所有符合绑定用户的 MAC 地址的 IPV6 报文都可以通行。

配置地址绑定例外端口

命令	作用
Ruijie(config)# **address-bind uplink** *interface-id*	配置地址绑定的例外端口 *interface-id*：端口或 Aggregate Port

通过 **no address-bind uplink** *interface-id* 命令取消指定例外口配置。

下面是配置端口 GigabitEthernet 0/1 为例外端口的例子：

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#address-bind uplink GigabitEthernet 0/1
```

查看配置

在特权模式下使用下列命令查看设备上的 IP 地址和 MAC 地址绑定的相关配置

命令	作用
Ruijie# **show address-bind**	查看设备上的 IP 地址与 MAC 地址绑定配置
Ruijie# **show address-bind uplink**	查看设备上的例外口信息

下面是查看设备的 IP 地址和 MAC 地址绑定配置的例子：

```
Ruijie#show address-bind
Total Bind Addresses in System : 1
IP Address          Binding MAC Addr
---------------     ----------------
    192.168.5.1     00d0.f800.0001
```

2.3.10 查看认证失败用户的地址

查看配置

命令	作用
Ruijie# **show mac-address-table drop**	查看所有认证失败用户的 MAC 地址

下面的例子说明了如何查看设备上的所有静态地址信息。

```
Vlan           MAC Address            Type        Interface
----------   -------------------- --------- --------------------
   3         00d0.f800.073c         DROP       GigabitEthernet 0/3
```

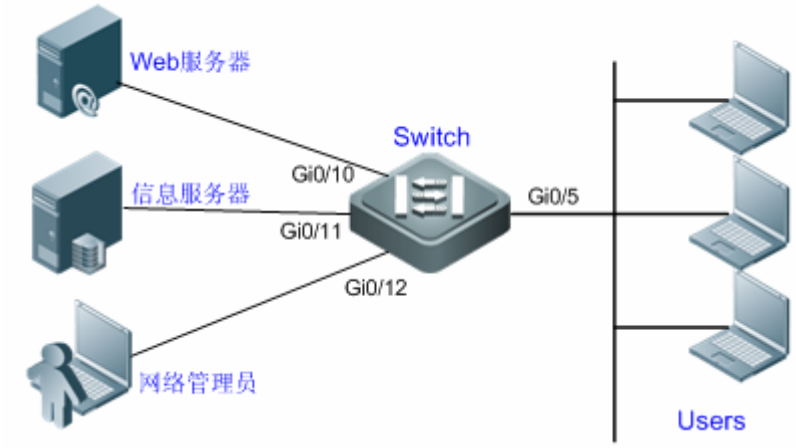
2.4 MAC地址表管理典型配置举例

2.4.1 静态 MAC 地址配置举例

拓扑图

下图为某信息系统组网图。Web 服务器、数据库服务器分别通过 Gi0/10、Gi0/11 连接到以太网交换机，服务器管理员通过 Gi0/12 口连接到以太网交换机，其他的一般用户通过以太网交换机的 Gi0/5 口接入访问 Web 服务器。所有的数据均在 VLAN 10 中转发。

图 2-7 静态 MAC 地址应用组网拓扑



应用需求

为保障 WEB 服务器与数据库之间交互的信息安全以及管理员与服务器之间交互的信息的安全，通过配置静态地址的方式保证 WEB 服务器与数据库服务器之间、管理员与各服务器之间的数据转发采用单播方式。这样可以有效的避免这些数据被以广播的方式转发到一般用户所使用的网络中。

配置要点

配置静态 MAC 地址表项，明确以下三个要素：

- 指定表项对应的目的 MAC 地址（Mac-address）
- 指定该地址所属的 VLAN（vlan-id）
- 接口 ID（Interface-id）

当交换机在 Vlan-id 指定的 VLAN 上接收到以 Mac-address 为目的地址的报文时，这个报文将被转发到 Interface-id 所指定的接口上。

本例的 MAC 地址同 VLAN、接口对应关系如下表所示：

角色	MAC 地址	VLAN ID	接口 ID
Web 服务器	00d0.3232.0001	VLAN2	Gi0/10
信息服务器	00d0.3232.0002	VLAN2	Gi0/11
网络管理员	00d0.3232.1000	VLAN2	Gi0/12

配置步骤

！进入交换机的全局配置模式

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

！添加静态 MAC 地址（指出所属 VLAN、接口）

```
Ruijie(config)#mac-address-table static 00d0.f8003232.0001 vlan 110 interface gigabitEthernet 0/10
Ruijie(config)#mac-address-table static 00d0.f8003232.0002 vlan 110 interface gigabitEthernet 0/211
Ruijie(config)#mac-address-table static 00d0.f800.00033232.1000 vlan 110 interface gigabitEthernet 0/312
```

查看设备配置

配置验证

在交换机上查看配置的静态 MAC 地址

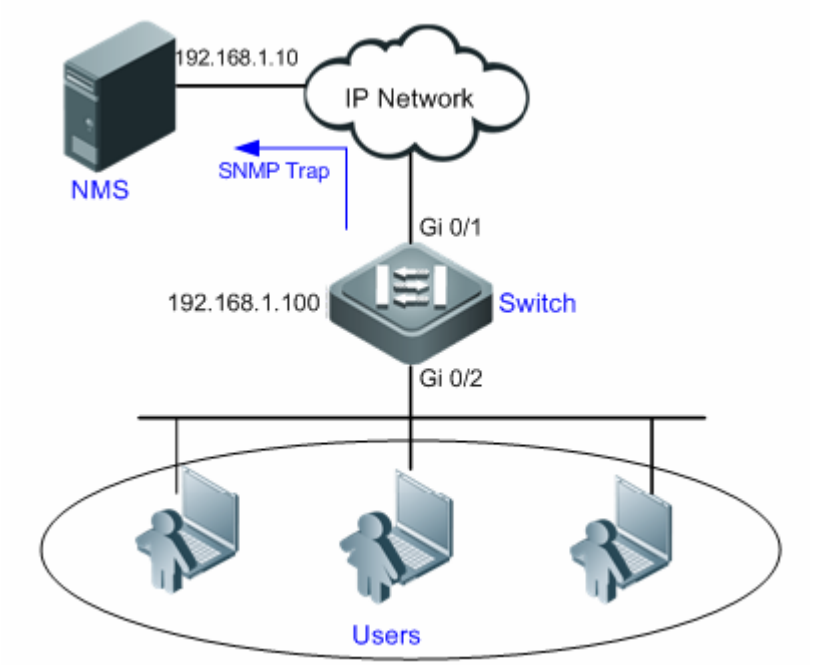
```
Ruijie#show mac-address-table static
Vlan        MAC Address          Type     Interface
----------  -------------------- -------- -------------------
   110        00d0.f8003232.0001       STATIC   GigabitEthernet 0/10
   110        00d0.f8003232.0002       STATIC   GigabitEthernet 0/211
   110        00d0.f800.3232.1000     STATIC   GigabitEthernet 0/312
```

2.4.2 动态 MAC 地址变化通知配置举例

拓扑图

下图为某企业内部网络示意图。下联用户通过 Gi0/2 口连接到交换机。

图 2-8 MAC 地址变化通知组网拓扑图



应用需求

为了便于管理员对下联用户使用网络情况信息的掌控，希望通过配置达到以下目的：

- 当交换机下联用户的接口学习到一个新的 MAC 地址或老化掉一个已学习到的地址时，将地址变化信息记录到 MAC 地址通知历史记录表中，供管理员了解最近的 MAC 地址变化信息。
- 同时，交换机能将 MAC 地址变化通知以 SNMP Trap 的方式将通知信息发送给指定的 NMS(网络管理工作站)
- 当交换机下联用户较多时，能尽量避免短时间内产生大量的 MAC 地址变化信息，减轻网络的负担。

配置要点

- 打开交换机全局 MAC 地址通知开关，在 Gi0/2 接口上配置 MAC 地址通知功能。
- 配置 NMS 主机地址，使能交换机主动发送 SNMP Trap 通知。交换机到 NMS（网络管理工作站）的路由可达。
- 设置交换机发送 MAC 地址通知的时间间隔为 300 秒（默认时间间隔为 1 秒）。交换机将该时间间隔内的通知信息封装成多个通知信息，这样，在每条地址通知信息中，就包含了若干个 MAC 地址变化的信息，从而达到减少网络流量的目的。

配置步骤

设备 IP 地址如图所示，具体配置过程此处省略。

第一步，打开交换机全局 MAC 地址变化通知开关

```
Ruijie>enable
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#mac-address-table notification
```

第二步，设置备发送 MAC 地址通知的时间间隔为 30 秒

```
Ruijie(config)#mac-address-table notification
```

第三步，打开 Gi0/2 接口的 MAC 地址通知功能

```
Ruijie(config)#mac-address-table notification interval 300
```

！进入 Gi0/2 接口配置模式

```
Ruijie(config)#interface gigabitEthernet 0/2
```

！设置当接口上有地址增加时发送通知

```
Ruijie(config-if-GigabitEthernet 0/2)# snmp trap mac-notification added
```

！设置当接口上有地址老化时也发送通知

```
Ruijie(config-if-GigabitEthernet 0/2)# snmp trap mac-notification removed
Ruijie(config-if-GigabitEthernet 0/2)#exit
```

第四步，配置接收 MAC 地址通知 Trap 信息的 NMS；NMS 地址为“192.168.1.10”，消息格式为 Version 2c，认证名为“comefrom2”

```
Ruijie(config)#snmp-server host 192.168.1.10 traps version 2c comefrom2
```

第五步，使能交换机主动发送 Trap 消息。

```
Ruijie(config)# snmp-server enable traps
```

配置验证

第一步，查看 MAC 地址通知功能的全局配置信息

```
Ruijie#show mac-address-table notification
MAC Notification Feature : Enabled
Interval(Sec): 300                    //发送 MAC 地址通知的时间间隔为 300 秒
Maximum History Size : 50   //默认 MAC 通知历史记录表的最大表项为 50 条
Current History Size : 0   //当前记录条目数
```

第二步，查看接口的 MAC 地址变化通知的使能状况

```
Ruijie#show mac-address-table notification interface gigabitEthernet 0/2
Interface               MAC Added Trap     MAC Removed Trap
-----------             --------------     --------------
GigabitEthernet 0/2    Enabled            Enabled
```

第三步，查看接口 MAC 地址表

```
Ruijie#show mac-address-table interface gigabitEthernet 0/2
Vlan        MAC Address          Type     Interface
----------  -------------------- -------- --------------------
   1        00d0.3232.0001       DYNAMIC  GigabitEthernet 0/2
   1        00d0.3232.0002       DYNAMIC  GigabitEthernet 0/2
   1        00d0.3232.0003       DYNAMIC  GigabitEthernet 0/2
```

第四步，功能验证。

使用 **clear mac-address-table dynamic address** *00d0.3232.0003* 模拟 00d0.3232.0003 地址的老化。

! 查看 MAC 地址通知功能的全局配置信息

```
Ruijie#show mac-address-table notification
MAC Notification Feature : Enabled
Interval(Sec): 300
Maximum History Size : 50
Current History Size : 1  // MAC 地址变化通知记录数，当前 1 条。
```

! 查看 MAC 地址变化通知信息的历史记录表

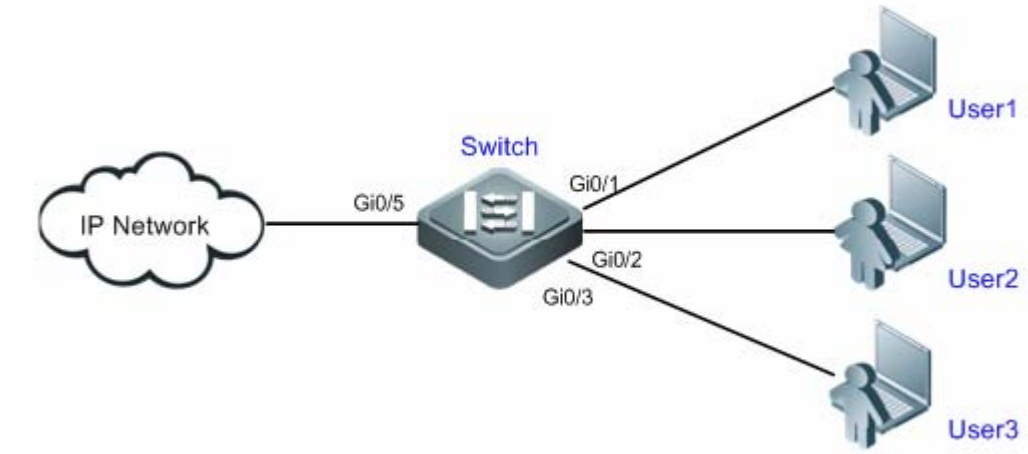
```
Ruijie#show mac-address-table notification history
History Index : 0
Entry Timestamp: 221683
MAC Changed Message :
Operation:DEL Vlan:1 MAC Addr: 00d0.3232.0003 GigabitEthernet 0/2
```

2.4.3 全局 IP/MAC 绑定配置举例

拓扑图

下图为某企业内部网络示意图。为了方便管理，企业为每台主机固定分配了一个 IP 地址。

图 2-9 全局 IP/MAC 绑定组网示意图



应用需求

- 防止员工非法盗用 IP，例如盗用权限更高人员的 IP 地址，以获得权限外的信息。
- 员工可在部门内实现移动办公。

配置要点

通过在交换机上手动配置全局 IP 和 MAC 地址绑定功能即可满足上述要求。配置要点如下：

- 手动配置全局 IP 和 MAC 地址绑定（本例列举 3 个用户）

用户	所属主机 MAC 地址	分配的 IP 地址
User1	00d0.3232.0001	192.168.1.10
User2	00d0.3232.0002	192.168.1.20
User3	00d0.3232.0003	192.168.1.30

- 全局使能 IP 和 MAC 地址绑定功能
- 将交换机的上链口（本例为 Gi0/5 口）配置为例外口

在应用中，由于交换机的上链口的 IP 报文的绑定关系是不确定的，通常将交换机的上链端口配置为例外口，此时上链端口则不进行 IP 地址与 MAC 地址的绑定检查。

配置步骤

第一步，配置全局 IP 和 MAC 地址绑定

```
Ruijie#configure terminal
```

！配置 User1 的 IP 和 MAC 地址绑定

```
Ruijie(config)#address-bind 192.168.1.10 00d0.3232.0001
```

！配置 User2 的 IP 和 MAC 地址绑定

```
Ruijie(config)#address-bind 192.168.1.20 00d0.3232.0002
```

！配置 User3 的 IP 和 MAC 地址绑定

```
Ruijie(config)#address-bind 192.168.1.30 00d0.3232.0003
```

第二步，全局使能 IP 和 MAC 地址绑定功能

```
Ruijie(config)#address-bind install
```

第三步，将交换机的上链口（本例为 Gi0/5 口）配置为例外口

```
Ruijie(config)#address-bind uplink gigabitEthernet 0/5
```

配置验证

第一步，查看交换机上的 IP 地址和 MAC 地址绑定配置。关注点：绑定关系是否正确。

```
Ruijie#show address-bind
IP Address          Binding MAC Addr
---------------     -----------------
   192.168.1.10     00d0.3232.0001
   192.168.1.20     00d0.3232.0002
   192.168.1.30     00d0.3232.0003
```

第二步，查看交换机上地址绑定例外口的配置

```
Ruijie#show address-bind uplink
Ports        State
------------ ------
Gi0/5        Enabled
```

第三步，测试验证。

交换机（除 Gi0/5 接口外）只接收源 IP 地址和 MAC 地址均匹配这些绑定地址的 IP 报文；对于不符合绑定条件的 IP 报文被丢弃。

3 Aggregate Port

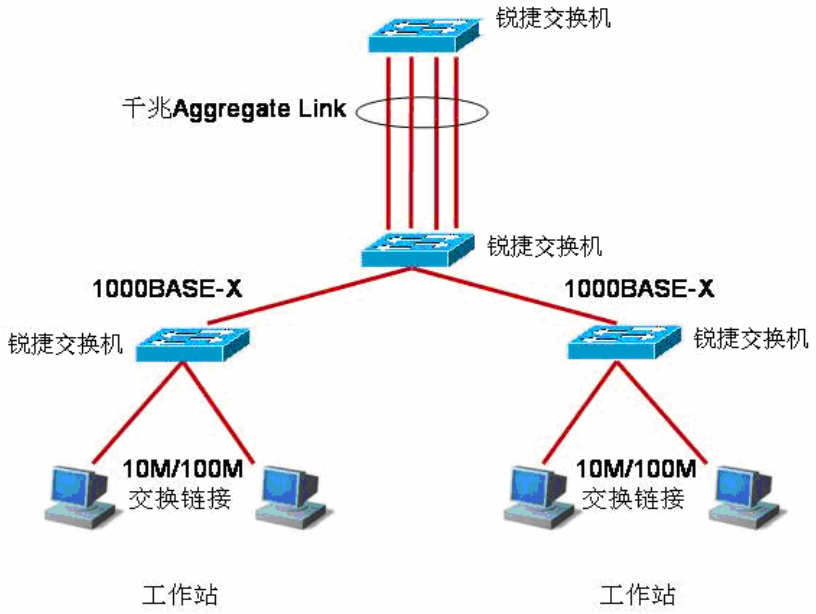
3.1 概述

将多个物理链接捆绑在一起形成一个逻辑链接，这个逻辑链接称为 Aggregate Port（简称 AP）。锐捷设备所提供的 AP 功能符合 IEEE802.3ad 标准，它可以用于扩展链路带宽，提供更高的连接可靠性。

AP 功能支持流量平衡，可以把流量均匀地分配给各成员链路。AP 功能还实现了链路备份，当 AP 中的一条成员链路断开时，系统会将该成员链路的流量自动地分配到 AP 中的其它有效成员链路上。AP 中一条成员链路收到的广播或者多播报文，将不会被转发到其它成员链路上。

每个 AP 口最多包含的成员口数量为 8 个，支持的最大 AP 数量为 120。

图 3-1 典型的 AP 配置



3.1.1 流量平衡

AP 可以根据报文的源 MAC 地址、目的 MAC 地址，源 MAC 地址+目的 MAC 地址、源 IP 地址，目的 IP 地址以及源 IP 地址+目的 IP 地址等特征值把流量平均地分配到 AP 的成员链路中。您可以用 **aggregateport load-balance** 设定流量分配方式。

源 MAC 地址流量平衡是根据报文的源 MAC 地址把报文分配到 AP 的各个成员链路中。不同源 MAC 的报文，根据源 MAC 地址在各成员链路间平衡分配；相同源 MAC 的报文，固定从同一个成员链路转发。

目的 MAC 地址流量平衡是根据报文的目的 MAC 地址把报文分配到 AP 的各个成员链路中。相同目的 MAC 的报文，固定从同一个成员链路转发；不同目的 MAC 的报文，根据目的 MAC 地址在各成员链路间平衡分配。

源 MAC+目的 MAC 地址流量平衡是根据报文的源 MAC 和目的 MAC 地址把报文分配到 AP 的各个成员链路中。具有不同的源 MAC+目的 MAC 地址的报文根据源 MAC+目的 MAC 地址在各成员链路间平衡分配，而具有相同的源 MAC+目的 MAC 地址的报文则固定分配给同一个成员链路。

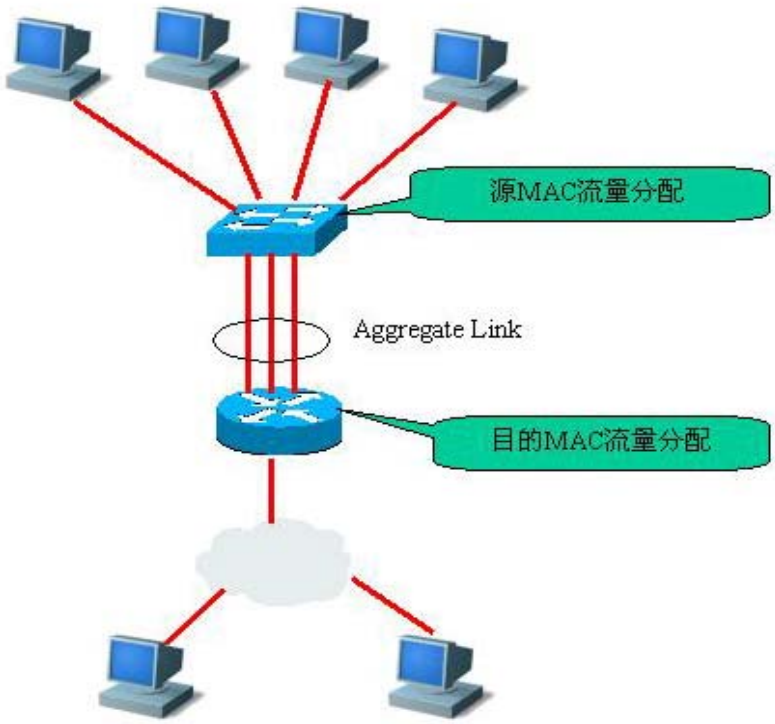
源 IP 地址或目的 IP 地址流量平衡是根据报文源 IP 或目的 IP 进行流量分配。不同源 IP 或目的 IP 的报文根据源 IP 或目的 IP 在各成员链路间平衡分配，相同源 IP 或目的 IP 的报文则固定通过相同的成员链路转发。该流量平衡方式用于三层报文，如果在此流量平衡模式下收到二层报文，则自动根据设备的默认方式进行流量平衡。

源 IP 地址+目的 IP 地址流量平衡是根据报文源 IP 和目的 IP 进行流量分配。该流量平衡方式用于三层报文，如果在此流量平衡模式下收到二层报文，则自动根据设备的默认方式进行流量平衡。具有不同的源 IP+目的 IP 地址的报文根据源 IP+目的 IP 地址在各成员链路间平衡分配，具有相同的源 IP+目的 IP 地址的报文则固定分配给相同的成员链路。

以上所有平衡模式都适用于二层 AP 和三层 AP，即源 IP 地址流量平衡、目的 IP 地址流量平衡、源 IP 地址+目的 IP 地址流量平衡模式也适用于二层 AP。用户应根据不同的网络环境设置合适的流量分配方式，以便能把流量较均匀地分配到各个链路上，充分利用网络的带宽。

在下图中，一个交换机通过 AP 与路由器进行通讯，所有内网中的设备（如图中的上面 4 台 PC 机）以路由器为网关，所有外网（如图中的下面 2 台 PC 机）经路由器发出的报文的源 MAC 都是网关的 MAC 地址，为了让路由器与其他主机之间的通讯流量能由其他链路来分担，应设置为根据目的 MAC 地址进行流量平衡；而在交换机处，则需要设置为根据源 MAC 地址进行流量平衡。

图 3-2 AP 流量平衡示意图



3.2 配置Aggregate Port

3.2.1 缺省配置

功能特性	缺省值
二层 AP 接口	无
三层 AP 接口	无
流量平衡	根据输入报文的源 MAC 和目的 MAC 进行流量分配。

3.2.2 配置指导

- AP 成员端口的端口速率必须一致。
- 二层端口只能加入二层 AP，三层端口只能加入三层 AP；包含成员口的 AP 口不允许改变二层/三层属性。
- AP 不能设置端口安全功能。
- 一个端口加入 AP，端口的属性将被 AP 的属性所取代。
- 一个端口从 AP 中删除，则端口的属性将恢复为加入 AP 前的属性。

当一个端口加入 AP 后，不能在该端口上进行任何配置，直到该端口退出 AP。

3.2.3 配置 L2 Aggregate Port

1) （可选）创建一个 L2 AP。

命令	作用
Ruijie(config)# **interface aggregateport** *ap-number*	创建一个 L2 AP。

2) 向该 AP 中添加成员口。

命令	作用
Ruijie(config)# **interface** *interface-type interface-number*	进入某二层接口。
Ruijie(config-if)# **port-group** *ap-number*	将二层接口加入 L2 AP。

通过 **port-group** 命令将二层接口加入一个 AP 时，如果该 AP 不存在，则同时创建这个 AP。

在接口配置模式下使用 **no port-group** 命令将此成员口退出 AP。

例：将二层的以太网接口 0/1 配置成二层 AP 5 的成员口（同时创建 AP5）。

```
Ruijie# configure terminal
Ruijie(config)# interface range gigabitEthernet 0/1
Ruijie(config-if-range)# port-group 5
Ruijie(config-if-range)# end
```

将普通端口加入某个 AP 口后，当该端口再次从 ap 口退出时，普通端口上的原先相关的配置可能会恢复为缺省的配置。不同功能对 ap 口的成员的原有配置的处理方式有所不同，因此建议在端口从 ap 口退出后，应查看并确认端口的配置。

3.2.4 配置 L3 Aggregate Port

1) 创建一个 L3 AP。

命令	作用
Ruijie(config)# **interface aggregateport** *ap-number*	创建一个 L2 AP。
Ruijie(config-if)# **no switchport**	将 L2 AP 转化为 L3 AP。

通过 **port-group** 命令将三层接口加入一个 AP 时，如果该 AP 不存在，则不能加入成功。因此，必须先创建 L3 AP，再将各三层接口加入。

2) 向该 AP 中添加成员口。

命令	作用
Ruijie(config)# **interface** *interface-type interface-number*	进入某二层接口。
Ruijie(config-if)# **no switchport**	将二层接口转化为三层接口。
Ruijie(config-if)# **port-group** *ap-number*	将三层接口加入 L3 AP。

例：创建一个 L3 AP 接口（AP 3），配置 IP 地址（192.168.1.1）。将 gigabitEthernet 0/1-3 加入 AP 3。

```
Ruijie# configure terminal
Ruijie(config)# interface aggretegateport 3
Ruijie(config-if)# no switchport
Ruijie(config-if)# ip address 192.168.1.1 255.255.255.0
Ruijie(config-if)# exit
Ruijie(config)# interface range gigabitEthernet 0/1-3
Ruijie(config-if-range)# no switchport
Ruijie(config-if-range)# port-group 3
```

3.2.5 配置 Aggregate Port 的流量平衡

命令	作用
Ruijie(config)# **aggregateport load-balance** {**dst-mac** | **src-mac** | **src-dst-mac** | **dst-ip** | **src-ip** | **src-dst-ip** | **src-port** | **src-dst-ip-l4port** }	设置 AP 的流量平衡算法。缺省为 src-dst-mac。 **dst-mac**：根据输入报文的目的 MAC 地址进行流量分配。 **src-mac**：根据输入报文的源 MAC 地址进行流量分配。 **src-dst-ip**：根据源 IP 与目的 IP 进行流量分配。 **dst-ip**：根据输入报文的目的 IP 地址进行流量分配。 **src-ip**：根据输入报文的源 IP 地址进行流量分配。 **src-dst-mac**：根据源 MAC 与目的 MAC 进行流量分配。 **src-port**：根据输入报文的源端口号进行流量分配。 **src-dst-ip-l4port**：根据源 IP 与目的 IP 和源 L4 端口号与目的 L4 端口号进行流量分配。

要将 AP 的流量平衡设置恢复到缺省值，可以在全局配置模式下使用 **no aggregateport load-balance** 命令。

3.2.6 显示 Aggregate Port

命令	作用
Ruijie# **show aggregateport** [*ap-number*] { **load-balance** | **summary** }	显示 AP 设置。

例：显示 AP 设置

```
Ruijie# show aggregateport load-balance
Load-balance : Source MAC address
Ruijie#show aggregateport 1 summary
AggregatePort MaxPorts SwitchPort Mode   Ports
------------- -------- ---------- ------
Ag1           8        Enabled    ACCESS
```

4 链路聚合控制协议(LACP)

4.1 概述

IEEE 802.3ad 标准的 LACP(Link Aggregation Control Protocol，链路聚合控制协议)是一个关于动态链路聚合的协议，它通过协议报文 LACPDU(Link Aggregation Control Protocol Data Unit，链路聚合控制协议数据单元)和相连的设备交互信息。

当端口启用 LACP 协议后，端口通过发送 LACPDU 来通告自己的系统优先级，系统 MAC，端口的优先级，端口号和操作 key 等。相连设备收到该报文后，根据所存储的其他端口的信息，选择端口进行相应的聚合操作，从而可以使双方在端口退出或者加入聚合组上达到一致。

4.1.1 动态链路聚合的模式

端口有 3 种聚合模式：主动(Active)模式、被动模式(Passive)和静态模式。

其中主动模式的端口会主动发起 LACP 报文协商；被动模式的端口则只会对收到的 LACP 报文做应答；静态模式不会发出 LACP 报文进行协商，具体配置请参见静态 AP 配置指南的说明。各个聚合模式的相邻端口聚合模式要求如下：

端口模式	相邻端口聚合模式要求
主动模式	主动模式或者被动模式
被动模式	主动模式
静态模式	静态模式

4.1.2 LACP端口的状态

聚合组内的成员有可能处于 3 种状态：

- 当端口的链路状态处于 Down 时，端口不可能转发任何数据报文，显示为”down”状态。
- 端口链路处于 Up 状态，并经过 LACP 协商后，端口被置于聚合状态(端口被作为一个聚合组的一个成员参与聚合组的数据报文转发)，显示为“bndl”状态。
- 当端口链路处于 UP 状态，但是由于对端没有启用 LACP，或者因为端口属性和主端口不一致等一些因素导致经过报文协商端口被置于挂起状态（处于挂起状态的端口不参与数据报文转发），显示为“susp”状态。

只有全双工的端口才能进行聚合

成员端口的速率、流控、介质类型以及成员端口的二、三层属性必须一致才能聚合

端口聚合后修改端口的上述属性将导致同聚合组内的其他端口也无法聚合

☑ 已经启用禁止成员口加入或者退出 AP 功能的端口不能启用 LACP；同时 LACP 成员口上不能启用禁止成员口加入或者退出 AP 功能。启用禁止成员口加入或者退出功能的 AP，不能被配置为 LACP AP；LACP AP 不能启用禁止成员口加入或者退出 AP 的功能。

☑ 由于外部功能限制而导致 LACP 退出 AP 失败时，会打印成员口退出 AP 失败的 SYSLOG（比如，端口 FastEthernet 0/1 退出 AP1 失败的 SYSLOG：“%LACP-5-UNBUNDLE_FAIL: Interface FastEthernet 0/1 failed to leave the AggregatePort 1”）。请修改配置，去掉禁止成员口退出 AP 的相关配置，否则会影响 AP 的正常报文传输。

4.2 动态链路聚合的优先级关系

4.2.1 LACP的系统ID

每台设备仅能配置一个 LACP 聚合系统。每个 LACP 聚合系统都有唯一的系统优先级。系统 ID 由 LACP 的系统优先级和设备 MAC 地址组成。系统优先级越小，系统 ID 的优先级越高；在系统优先级相同的情况下，比较设备的 MAC 地址，设备 MAC 地址越小，系统 ID 的优先级越高。系统 ID 优先级较高的系统决定端口状态，低优先级系统的端口状态随高优先级系统的端口状态变化而变化。

4.2.2 LACP的端口ID

每个端口有独立的 LACP 端口优先级，这是一个可配置的数值。端口 ID 由 LACP 的端口优先级和端口号组成。端口优先级数值越小，端口 ID 的优先级越高；在端口优先级相同的情况下，端口号越小，端口 ID 的优先级越高。

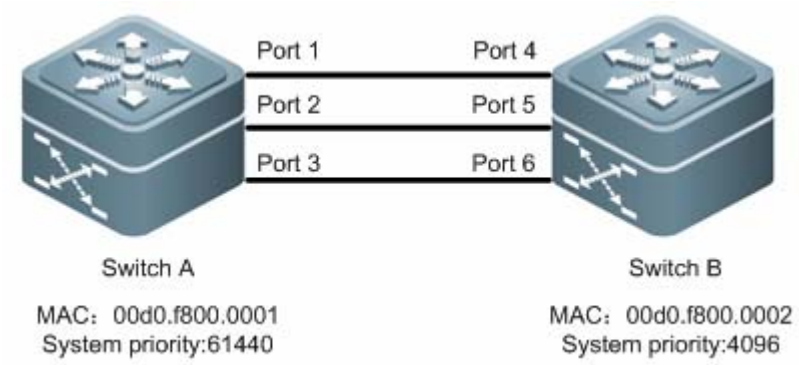
4.2.3 LACP的主端口

当有动态成员处于 up 状态时，LACP 会根据端口的速率，双工速率等关系，选择一个聚合组内端口 ID 优先级最高的端口作为主端口。只有和主端口属性相同的端口才能处于聚合状态，参与聚合组的数据转发。当端口的属性变化时，LACP 会重新选择主端口；当新的主端口不处于聚合状态时，LACP 会把同一个聚合组内的成员解聚合，重新聚合。

4.2.4 LACP的协商过程

在收到对端的 LACP 报文后，选取系统 ID 优先级比较高的系统。在系统 ID 优先级较高的一端，按照端口 ID 优先级从高到低的顺序，设置聚合组内端口的处于聚合状态。对端收到更新后的 LACP 报文后，也会把相应的端口设置成聚合状态。

图 4-1 LACP 协商



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

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

4.3 动态链路聚合的要求

动态链路聚合是 LACP 协议自动地添加和删除聚合组内的端口，两个端口被自动地聚合在一起有一定的要求。

- 只有相同的操作 key 才能被聚合在一起。
- 只有和主端口具有相同的速率和双工等基本属性的端口才能被动态聚合在一起。
- 端口链路处于 UP 状态，相连的端口启用 LACP，并且端口或者相连端口必须处于主动模式(Active)。

4.4 配置动态链路聚合(LACP)

你可以配置 LACP 的系统优先级，端口的优先级以及聚合组的管理 key。一台交换机所有的动态链路组只能有一个 LACP 系统优先级，修改这个值会影响到交换机上的所有聚合组。

在配置模式下，按如下步骤配置动态链路聚合：

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **lacp system-priority** *system-priority*	(可选)配置 LACP 系统的优先级，可选范围为 0-65535，默认优先级为 32768。
Ruijie(config)# **interface** *interface-id*	进入接口模式。
Ruijie(config-if)# **lacp port-priority** *port-priority*	(可选)配置端口的优先级，可选范围为 0-65535， 默认优先级为 32768。

Ruijie(config-if)# **port-group *key* mode active | passive**	把端口加入聚合组并指定端口的动态聚合模式，如果聚合组不存在，则会创建一个聚合组。 key 为聚合组的管理 key，key 取值范围根据不同产品支持的聚合组数量不同而变。 active 表示端口以主动模式加入动态聚合组，passive 表示端口以被动模式加入聚合组。
Ruijie(config-if)# **end**	退回特权模式。

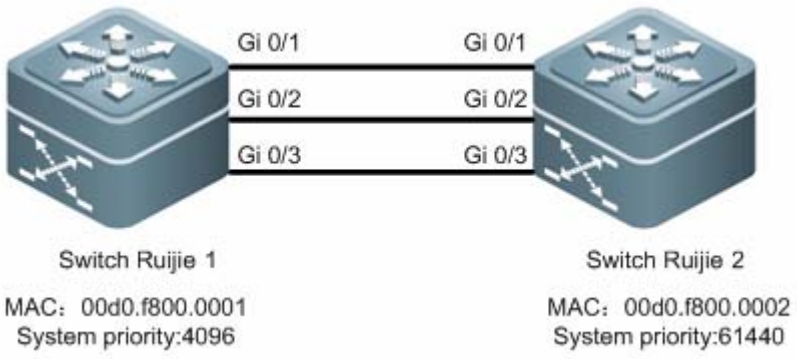
4.5 查看端口的动态链路聚合状态

在特权模式下使用如下命令来查看动态链路聚合的状态：

命令	作用
Ruijie# **show lacp summary [*key*]**	查看 LACP 系统的动态链路聚合状态.可指定显示特定聚合组的信息，参数 *key* 表示聚合组的 ID

4.6 LACP的配置用例

图 4-2 LACP 链路聚合



例如，如上图 2 所示拓扑，在交换机 Ruijie1 上设置 LACP 系统优先级为 4096，在端口 Gi 0/1、Gi 0/2、 Gi 0/3 上启用动态链路聚合协议，并设置端口的 LACP 端口优先级为 4096。

```
Ruijie1# configure terminal
Ruijie1(config)# lacp system-priority 4096
Ruijie1(config)# interface range GigabitEthernet 0/1-3
Ruijie1(config-if-range)# lacp port-priority 4096
Ruijie1(config-if-range)# port-group 3 mode active
Ruijie1(config-if-range)# end
```

在 Ruijie2 上设置 LACP 系统优先级为 61440，在端口 Gi 0/1、Gi 0/2、Gi 0/3 启用动态链路聚合协议，并设置端口的 LACP 端口优先级为 61440。

```
Ruijie2# configure terminal
Ruijie1(config)# lacp system-priority 61440
```

```
Ruijie2(config)# interface range GigabitEthernet 0/1-3
Ruijie2(config-if-range)# lacp port-priority 61440
Ruijie2(config-if-range)# port-group 3 mode active
Ruijie2(config-if-range)#end
```

配置完相关配置后，如果 LACP 协商成功，则会打印相应的 log：

```
*Feb 25 17:11:31: %LACP-5-BUNDLE: Interface Gi0/1 joined AggregatePort 3.
*Feb 25 17:11:32: %LACP-5-BUNDLE: Interface Gi0/2 joined AggregatePort 3.
*Feb 25 17:11:32: %LACP-5-BUNDLE: Interface Gi0/3 joined AggregatePort 3.
*Feb 25 17:11:32: %LINEPROTO-5-UPDOWN: Line protocol on Interface AggregatePort 3, changed state to up
```

表示端口 Gi 0/1、Gi 0/2、Gi 0/3 已经被成功地加入聚合组 3 了，这时在交换机 Ruijie1 上查看聚合组内成员口的状态。

```
Ruijie(config)#show LACP summary
Flags:  S - Device is requesting Slow LACPDUs
 F - Device is requesting Fast LACPDUs.
A - Device is in active mode.        P - Device is in passive mode.
Aggregate port 3:
Local information:
LACP port       Oper    Port     Port
Port     Flags     State     Priority        Key     Number  State
---------------------------------------------------------------
Gi0/1     SA        bndl        4096            0x3     0x1      0x3d
Gi0/2     SA        bndl        4096            0x3     0x2      0x3d
Gi0/3     SA        bndl        4096            0x3     0x3      0x3d
Partner information:
                    LACP port                   Oper    Port     Port
Port     Flags     Priority      Dev ID       Key     Number  State
---------------------------------------------------------------
Gi0/1     SA        61440     00d0.f800.0002   0x3     0x1     0x3d
Gi0/2     SA        61440     00d0.f800.0002   0x3     0x2     0x3d
Gi0/3     SA        61440     00d0.f800.0002   0x3     0x3     0x3d
```

其中，

“Local information”部分，显示的是本系统维护的端口的 LACP 信息。

“Port” 显示的是本系统内端口的 ID。

“Flags” 显示的是端口的一些状态标志：

‘S’标志着端口处于长超时状态，需要邻居慢速(每 30 秒发送一个)发送 LACPDU 报文。

‘F’标志着端口处于短超时状态，需要邻居快速(每秒发送一个) 发送 LACPDU 报文。

‘A’标志着端口是主动模式，‘P’标志着端口是被动模式。

“State” 显示的是端口状态：“bndl”标志着端口已经处于聚合状态了；其它状态说明参见前述“LACP 端口的状态”一节。

“LACP Port Priority” 显示的是端口的 LACP 优先级信息。

“Oper Key” 显示的是端口的操作 Key。

“Port Number” 显示的是端口的端口号。

“Port State” 显示的是端口的 LACP 协议状态。

“Partner infomation”部分，显示的是相连端口的 LACP 信息。

“Dev ID”部分显示的是端口相邻端口的系统 MAC 信息。

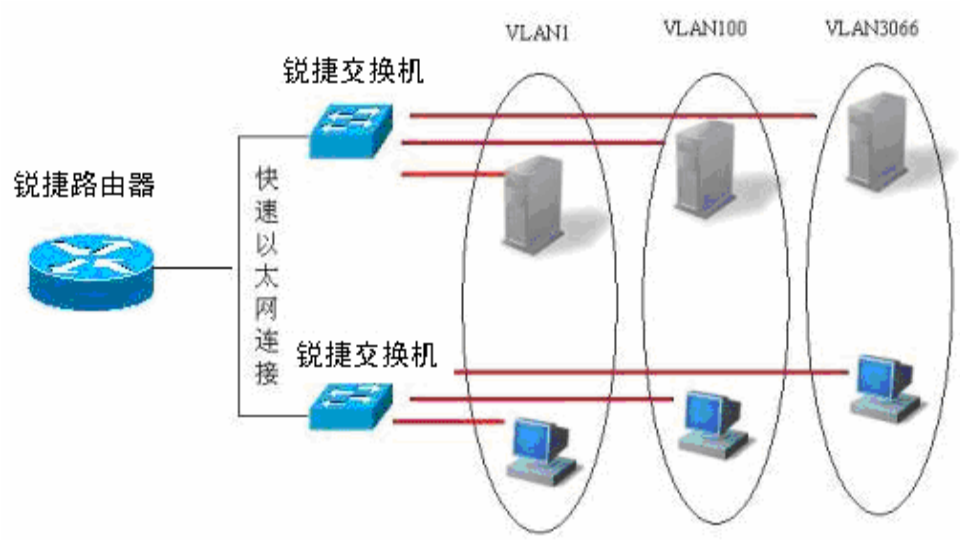
5 VLAN

5.1 概述

VLAN 是虚拟局域网（Virtual Local Area Network）的简称，它是在一个物理网络上划分出来的逻辑网络。这个网络对应于 ISO 模型的第二层网络。VLAN 的划分不受网络端口的实际物理位置的限制。VLAN 有着和普通物理网络同样的属性，除了没有物理位置的限制，它和普通局域网一样。第二层的单播、广播和多播帧在一个 VLAN 内转发、扩散，而不会直接进入其他的 VLAN 之中。所以，如果一个端口所连接的主机想要和其它不在同一个 VLAN 的主机通讯，则必须通过一个三层设备，见下图。

可以把一个端口定义为一个 VLAN 的成员，所有连接到这个特定端口的终端都是虚拟网络的一部分，并且整个网络可以支持多个 VLAN。当在 VLAN 中增加、删除和修改用户的时候，不必从物理上调整网络配置。

图 5-1



和一个物理网络一样，VLAN 通常和一个 IP 子网联系在一起。一个典型的例子是，所有在同一个 IP 子网中的主机属于同一个 VLAN，VLAN 之间的通讯必须通过三层设备。锐捷的三层设备可以通过 SVI 接口（Switch Virtual Interfaces）来进行 VLAN 之间的 IP 路由。关于 SVI 的配置，请见接口管理配置及 IP 单播路由配置。

5.1.1 支持的VLAN

产品支持的 VLAN 遵循 IEEE802.1Q 标准，最多支持 4094 个 VLAN(VLAN ID 1-4094)，其中 VLAN 1 是不可删除的默认 VLAN。

- 许可配置的 VLAN ID 范围为 1-4094
- 当硬件资源不足的情况下，系统将返回创建 VLAN 失败信息。

5.1.2 VLAN成员类型

可以通过配置一个端口的 VLAN 成员类型，来确定这个端口能通过怎样的帧，以及这个端口可以属于多少个 VLAN。关于 VLAN 成员类型的详细说明，请看下表：

命令	作用
Access	一个 Access 端口，只能属于一个 VLAN，并且是通过手工设置指定 VLAN 的。
Trunk（802.1Q）	一个 Trunk 口，在缺省情况下是属于本设备所有 VLAN 的，它能够转发所有 VLAN 的帧。也可以通过设置许可 VLAN 列表(Allowed-VLANs)来加以限制。

5.2 配置VLAN

一个 VLAN 是以 VLAN ID 来标识的。在设备中，用户可以添加、删除、修改 VLAN 2-4094，而 VLAN 1 是由设备自动创建，并且不可被删除。

可以在接口配置模式下配置一个端口的 VLAN 成员类型或加入、移出一个 VLAN。

5.2.1 VLAN配置信息的保存

当用户在特权命令模式下输入 **copy running-config startup-config** 命令后，VLAN 的配置信息便被保存进配置文件。要查看 VLAN 配置信息，可以使用 **show vlan** 命令。

5.2.2 缺省的VLAN配置

参数	缺省值	范围
VLAN ID	1	1－4094
VLAN Name	VLAN xxxx，xxxx 是 VLAN ID 数	无范围
VLAN State	Active	Active，Inactive

5.2.3 创建、修改一个VLAN

在全局配置模式下，用户可以创建或者修改一个 VLAN：

命令	作用
Ruijie(config)# **vlan** *vlan-id*	输入一个 VLAN ID。如果输入的是一个新的 VLAN ID，则设备会创建一个 VLAN，如果输入的是已经存在的 VLAN ID，则修改相应的 VLAN。
Ruijie(config-vlan)# **name** *vlan-name*	（可选）为 VLAN 取一个名字。如果没有进行这一步，则设备会自动为它起一个名字 VLAN xxxx，其中 xxxx 是用 0 开头的四位 VLAN ID 号。比如，VLAN 0004 就是 VLAN 4 的缺省名字。

如果用户想把 VLAN 的名字改回缺省名字，只需输入 **no name** 命令即可。

下面是一个创建 VLAN 888，将它命名为 Test888 的例子：

```
Ruijie# configure terminal
```

```
Ruijie(config)# vlan 888
Ruijie(config-vlan)# name test888
Ruijie(config-vlan)# end
```

5.2.4 删除一个VLAN

缺省 VLAN（VLAN 1）不允许删除。

在全局配置模式下删除一个已存在的 VLAN：

命令	作用
Ruijie(config)# **no vlan** *vlan-id*	输入一个 VLAN ID，删除它。

5.2.5 将当前Access口加入到指定VLAN

如果把一个接口分配给一个不存在的 VLAN，那么这个 VLAN 将自动被创建。

在接口配置模式下，将一个端口分配给一个 VLAN：

命令	作用
Ruijie(config-if)# **switchport mode access**	定义该接口的 VLAN 成员类型（二层 ACCESS 口）
Ruijie(config-if)# **switchport access vlan** *vlan-id*	将这个口分配给一个 VLAN

下面这个例子把 **GigabitEthernet** 0/10 作为 Access 口加入了 VLAN20：

```
Ruijie# configure terminal
Ruijie(config)# interface GigabitEthernet 0/10
Ruijie(config-if)# switchport mode access
Ruijie(config-if)# switchport access vlan 20
Ruijie(config-if)# end
```

下面这个例子显示了如何检查配置是否正确：

```
Ruijie# show interface GigabitEthernet 0/10 switchport
Interface         Switchport   Mode  Access Native Protected  VLAN lists
----------        --------     -----  ----- ------ ---------- -------
GigabitEthernet 0/10 enabled  ACCESS  20      1    Disabled  ALL
```

5.2.6 向当前VLAN添加Access口

在 VLAN 配置模式下，将指定的 Access 口加入该 VLAN。该命令的配置效果同在接口模式下指定该接口所属 VLAN 的命令（即 **switchport access vlan** *vlan-id*）效果一致。

命令	作用
Ruijie(config)# **vlan** *vlan-id*	输入一个 VLAN ID。如果输入的是一个新的 VLAN ID，则设备会创建一个 VLAN，如果输入的是已经存在的 VLAN ID，则修改相应的 VLAN。

Ruijie(config-vlan)# **add interface** { *interface-id* | **range** *interface-range* }	向当前 VLAN 中添加一个或一组 Access 接口。 缺省情况下，所有二层以太网口都属于 VLAN1
Ruijie(config-vlan)# ［**no**］**add interface** { *interface-id* | **range** *interface-range* }	从当前 VLAN 中删除一个或一组 Access 接口
Ruijie(config-vlan)#**show interface** *interface-id* **switchport**	查看二层接口信息

该命令只对 Access 口有效

对于两种形式的接口加入 VLAN 命令，配置生效的原则是后配置的命令覆盖前面配置的命令

下面这个例子把 Access 口 (GigabitEthernet 0/10)添加到 VLAN20：

```
Ruijie# configure terminal
SwitchA(config)#vlan 20
SwitchA(config-vlan)#add interface GigabitEthernet 0/10
```

下面这个例子显示了如何检查配置是否正确：

```
Ruijie# show interface GigabitEthernet 0/10 switchport
Interface         Switchport   Mode  Access Native Protected  VLAN lists
----------        --------     -----  ----- ------ ---------- -------
GigabitEthernet 0/10 enabled  ACCESS  20      1    Disabled   ALL
```

5.2.7 配置Dot1qVlanCurrentEntry表中的MIB节点dot1qVlanIndex的访问权限

在全局配置模式下，用户可以修改 Dot1qVlanCurrentEntry 表中的 MIB 节点 dot1qVlanIndex 的最大访问权限：

命令	作用
Ruijie(config)# **dot1q-vlan-current-entry mib dot1q-vlan-index max-access mode read-only**	修改 Dot1qVlanCurrentEntry 表中的 MIB 节点 dot1qVlanIndex 的最大访问权限为“只读”模式。配置该命令后，MIB 节点 dot1qVlanIndex 支持通过 SNMP 软件进行读取操作。

如果用户需要将 MIB 节点 dot1qVlanIndex 的最大访问权限恢复到缺省的“禁止访问”模式，只需输入 **no dot1q-vlan-current-entry mib dot1q-vlan-index max-access mode** 命令即可。

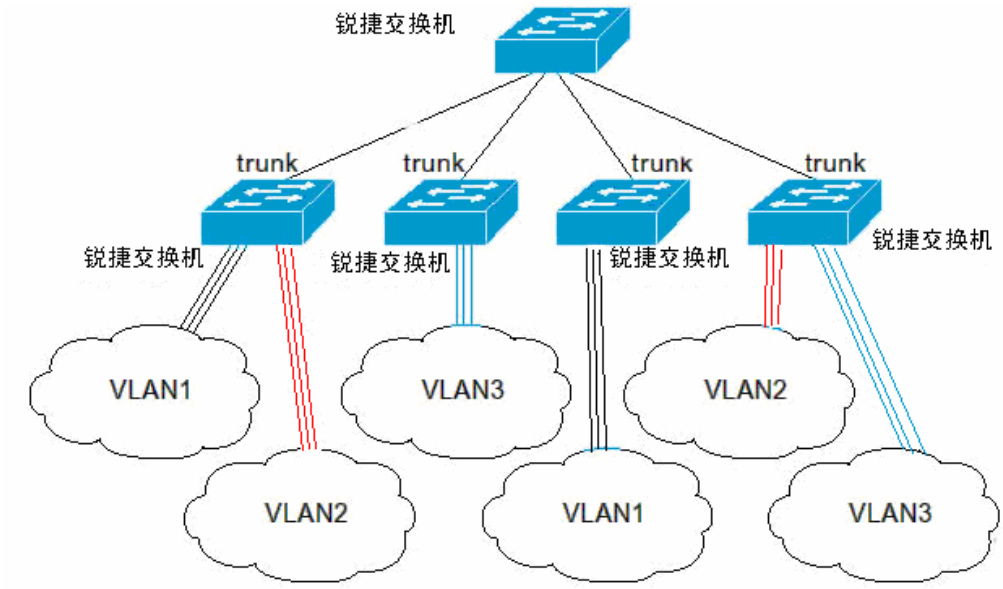
5.3 配置VLAN Trunks

5.3.1 Trunking概述

一个 Trunk 是将一个或多个以太网交换接口和其他的网络设备（如交换机）进行连接的点对点链路，一条 Trunk 链路可以传输属于多个 VLAN 的流量。

锐捷设备的 Trunk 采用 802.1Q 标准封装。下图显示了一个采用 Trunk 连接的网络。

图 5-2



用户可以把一个普通的以太网端口，或者一个 Aggregate Port 设为一个 Trunk 口（关于 Aggregate Port 的详细说明，请见配置 Aggregate Port）。

如果要把一个接口在 ACCESS 模式和 TRUNK 模式之间切换，请用 **switchport mode** 命令：

命令	作用
Ruijie(config-if)# **switchport mode access**	将一个接口设置成为 Access 模式
Ruijie(config-if)# **switchport mode trunk**	将一个接口设置成为 Trunk 模式

必须为 Trunk 口指定一个 Native VLAN。所谓 Native VLAN，就是指在这个接口上收发的 UNTAG 报文，都被认为是属于这个 VLAN 的。显然，这个接口的缺省 VLAN ID（即 IEEE 802.1Q 中的 PVID）就是 Native VLAN 的 VLAN ID。同时，在 Trunk 上发送属于 Native VLAN 的帧，则必然采用 UNTAG 的方式。每个 Trunk 口的缺省 Native VLAN 是 VLAN 1。

在配置 Trunk 链路时，请确认连接链路两端的 Trunk 口使用相同的 Native VLAN。

5.3.2 配置一个Trunk口

Trunk 口基本配置

在接口配置模式下，可以将一个接口配置成一个 Trunk 口。

命令	作用
Ruijie(config-if)# **switchport mode trunk**	定义该接口的类型为二层 Trunk 口
Ruijie(config-if)# **switchport trunk native vlan** *vlan-id*	为这个口指定一个 Native VLAN

如果想把一个 Trunk 口的所有 Trunk 相关属性都复位成缺省值，请使用 **no switchport mode** 配置命令。

5.3.3 定义Trunk口的许可VLAN列表

一个 Trunk 口缺省可以传输本设备支持的所有 VLAN（1－4094）的流量。但是，用户也可以通过设置 Trunk 口的许可 VLAN 列表来限制某些 VLAN 的流量不能通过这个 Trunk 口。

在接口配置模式下，可以修改一个 Trunk 口的许可 VLAN 列表。

命令	作用
Ruijie(config-if)# **switchport trunk allowed vlan** {**all** | [**add** | **remove** | **except**] } *vlan-list*	（可选）配置这个 Trunk 口的许可 VLAN 列表。参数 *vlan-list* 可以是一个 VLAN，也可以是一系列 VLAN，以小的 VLAN ID 开头，以大的 VLAN ID 结尾，中间用-号连接。如：10–20。 all 的含义是许可 VLAN 列表包含所有支持的 VLAN； add 表示将指定 VLAN 列表加入许可 VLAN 列表； remove 表示将指定 VLAN 列表从许可 VLAN 列表中删除； except 表示将除列出的 VLAN 列表外的所有 VLAN 加入许可 VLAN 列表；

如果想把 Trunk 的许可 VLAN 列表改为缺省的许可所有 VLAN 的状态，请使用 **no switchport trunk allowed vlan** 接口配置命令。

下面是一个把 VLAN 2 从端口 FastEthernet 1/15 的许可列表中移出的例子：

```
Ruijie(config)# interface fastethernet 1/15
Ruijie(config-if)# switchport trunk allowed vlan remove 2
Ruijie(config-if)# end
Ruijie# show interfaces fastethernet 1/15 switchport
Interface Switchport Mode  Access Native Protected VLAN lists
--------- ---------- ----  ------ ------ -------- ----------
Fa1/15     enabled    TRUNK  1      1     Disabled   1,3－4094
```

5.3.4 配置Native VLAN

一个 Trunk 口能够收发 TAG 或者 UNTAG 的 802.1Q 帧。其中 UNTAG 帧用来传输 Native VLAN 的流量。缺省的 Native VLAN 是 VLAN 1。

在接口配置模式下，可以为一个 Trunk 口配置 Native VLAN。

命令	作用
Ruijie(config-if)# **switchport trunk native vlan** *vlan-id*	配置 Native VLAN

如果想把 Trunk 的 Native VLAN 列表改回缺省的 VLAN 1，请使用 **no switchport trunk native vlan** 接口配置命令。

如果一个帧带有 Native VLAN 的 VLAN ID，在通过这个 Trunk 口转发时，会自动被剥去 TAG。

把一个接口的 Native VLAN 设置为一个不存在的 VLAN 时，设备不会自动创建此 VLAN。此外，一个接口的 Native VLAN 可以不在接口的许可 VLAN 列表中。此时，Native VLAN 的流量不能通过该接口。

5.3.5 显示VLAN

在特权模式下，才可以查看 VLAN 的信息。显示的信息包括 VLAN VID、VLAN 状态、VLAN 成员端口以及 VLAN 配置信息。以下罗列了相关的显示命令：

命令	作用
show vlan [*vlan-id*]	显示所有或指定 VLAN 的参数

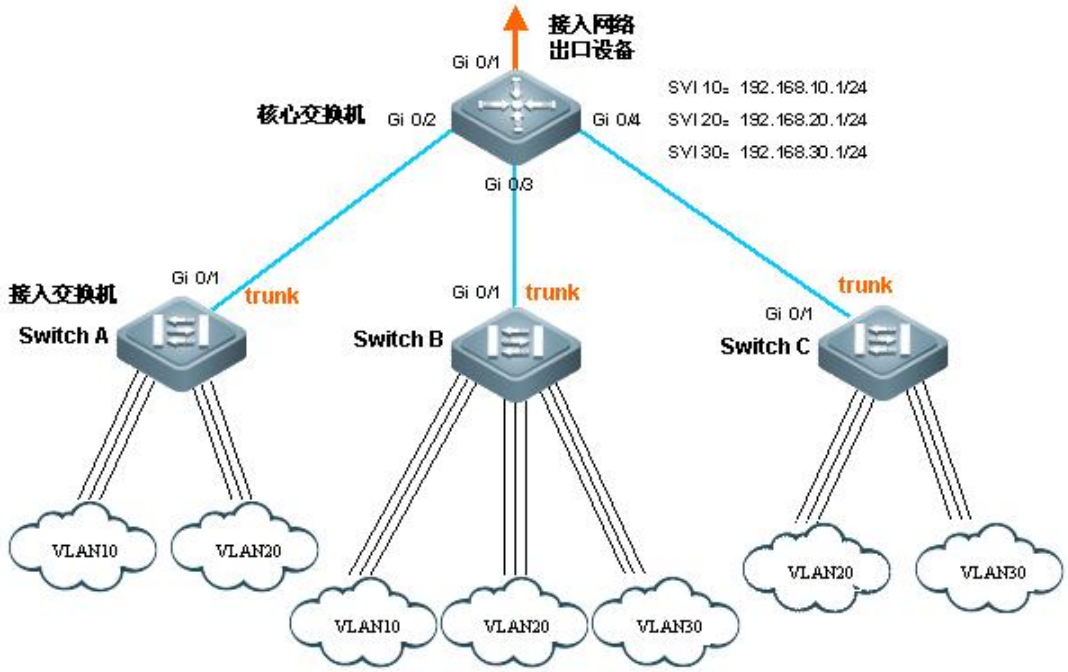
下面是一个显示 VLAN 的例子：

```
Ruijie# show vlan
VLAN Name                              Status    Ports
---------- ----------- ---------- ---------- ----------
   1 VLAN0001        STATIC    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                  Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                  Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                  Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                  Fa0/17, Fa0/19, Fa0/20, Fa0/21
                                  Fa0/22, Fa0/23, Fa0/24, Gi0/25
                                  Gi0/26, Gi0/27, Gi0/28
   2 VLAN0002        STATIC    Fa0/1, Fa0/2, Fa0/3
   3 VLAN0003        STATIC    Fa0/1, Fa0/2, Fa0/3
   4 VLAN0004        STATIC    Fa0/1, Fa0/2, Fa0/3
   5 VLAN0005        STATIC    Fa0/1, Fa0/2, Fa0/3
   6 VLAN0006        STATIC    Fa0/1, Fa0/2, Fa0/3
```

5.4 配置举例

组网拓扑

图 5-3



组网需求

如上图所示，某用户内网被划分为 VLAN 10、VLAN 20、VLAN 30，以实现相互间的 2 层隔离；3 个 VLAN 对应的 IP 子网分别为 192.168.10.0/24、192.168.20.0/24、192.168.30.0/24，3 个 VLAN 通过 3 层核心交换机的 IP 转发能力实现子网互连。

配置要点

本用例以核心交换机和 1 台接入交换机为例说明配置过程。要点如下：

- 在核心交换机配置 3 个 VLAN，配置下连接入交换机的端口为 trunk 口，并指定许可 vlan 列表，实现 2 层隔离；
- 在核心交换机配置 3 个 SVI 口，分别作为 3 个 VLAN 对应 IP 子网的网关接口，配置对应的 IP 地址；
- 分别在 3 台接入交换机创建 VLAN，为各 VLAN 分配 Access 口，指定上连核心交换机的 trunk 口。本用例以接入交换机 Switch A 为例说明配置步骤。

配置步骤

- 核心交换机上的配置

创建 VLAN

进入全局配置模式

```
Ruijie#configure terminal
```

创建 VLAN 10

```
Ruijie(config)#vlan 10
```

创建 VLAN 20

```
Ruijie(config-vlan)#vlan 20
```

创建 VLAN 30

```
Ruijie(config-vlan)#vlan 30
```

退回到全局配置模式

```
Ruijie(config-vlan)#exit
```

配置各下连 trunk 口，指定许可 vlan 列表

进入端口范围 Gi 0/2-4

```
Ruijie(config)#interface range GigabitEthernet 0/2-4
```

配置该端口 Gi 0/2-4 都为 trunk 口

```
Ruijie(config-if-range)#switchport mode trunk
```

退回到全局配置模式

```
Ruijie(config-if-range)#exit
```

进入端口 Gi 0/2

```
Ruijie(config)#interface GigabitEthernet 0/2
```

将所有 vlan 从该端口的许可 vlan 中删除

```
Ruijie(config-if)#switchport trunk allowed vlan remove 1-4094
```

重新添加该端口的许可 vlan 为 10、20

```
Ruijie(config-if)#switchport trunk allowed vlan add 10,20
```

进入端口 Gi 0/3

```
Ruijie(config-if)#interface GigabitEthernet 0/3
```

将所有 vlan 从该端口的许可 vlan 中删除

```
Ruijie(config-if)#switchport trunk allowed vlan remove 1-4094
```

重新添加该端口的许可 vlan 为 10、20、30

```
Ruijie(config-if)#switchport trunk allowed vlan add 10,20,30
```

进入端口 Gi 0/4

```
Ruijie(config-if)#interface GigabitEthernet 0/4
```

将所有 vlan 从该端口的许可 vlan 中删除

```
Ruijie(config-if)#switchport trunk allowed vlan remove 1-4094
```

重新添加该端口的许可 vlan 为 20、30

```
Ruijie(config-if)#switchport trunk allowed vlan add 20,30
```

退回到全局配置模式

```
Ruijie(config-if)#exit
```

在核心交换机上查看 vlan 配置

查看 vlan 信息，包括 vlan id、名称、状态、包括的端口

```
Ruijie#show vlan
VLAN  Name       Status                Ports
---- --------  --------   --------------------------------
   1 VLAN0001   STATIC     Gi0/1, Gi0/5, Gi0/6, Gi0/7
                           Gi0/8, Gi0/9, Gi0/10, Gi0/11
                           Gi0/12, Gi0/13, Gi0/14, Gi0/15
                           Gi0/16, Gi0/17, Gi0/18, Gi0/19
                           Gi0/20, Gi0/21, Gi0/22, Gi0/23
                           Gi0/24
  10 VLAN0010  STATIC      Gi0/2, Gi0/3
  20 VLAN0020  STATIC      Gi0/2, Gi0/3, Gi0/4
  30 VLAN0030  STATIC      Gi0/3, Gi0/4
```

查看端口 Gi 0/2 的 vlan 状态

```
Ruijie#show interface GigabitEthernet 0/2 switchport
Interface Switchport Mode  Access Native Protected VLAN lists
--------- ---------- -----  ------ ------ --------- ---------
Gi0/2      enabled   TRUNK    1       1      Disabled  10,20
```

查看端口 Gi 0/3 的 vlan 状态

```
Ruijie#show interface GigabitEthernet 0/3 switchport
Interface Switchport Mode  Access Native Protected VLAN lists
--------- ---------- -----  ------ ------ --------- ----------
Gi0/3      enabled   TRUNK    1       1      Disabled  10,20,30
```

查看端口 Gi 0/4 的 vlan 状态

```
Ruijie#show interface GigabitEthernet 0/4 switchport
Interface Switchport Mode  Access Native Protected VLAN lists
--------- ---------- -----  ------ ------ --------- ----------
Gi0/4      enabled   TRUNK    1       1      Disabled  20,30
```

创建 SVI 口，指定 IP 地址

进入全局配置模式

```
Ruijie#configure terminal
```

创建 SVI 10

```
Ruijie(config)#interface vlan 10
```

配置 SVI 10 的 IP 地址

```
Ruijie(config-if)#ip address 192.168.10.1 255.255.255.0
```

创建 SVI 20

```
Ruijie(config-if)#interface vlan 20
```

配置 SVI 20 的 IP 地址

```
Ruijie(config-if)#ip address 192.168.20.1 255.255.255.0
```

创建 SVI 30

```
Ruijie(config-if)#interface vlan 30
```

配置 SVI 30 的 IP 地址

```
Ruijie(config-if)#ip address 192.168.30.1 255.255.255.0
```

退回到全局配置模式

```
Ruijie(config-if)#exit
```

- 接入交换机 Switch A 上的配置

创建 VLAN

进入全局配置模式

```
Ruijie#configure terminal
```

创建 VLAN 10

```
Ruijie(config)#vlan 10
```

创建 VLAN 20

```
Ruijie(config-vlan)#vlan 20
```

退回到全局配置模式

```
Ruijie(config-vlan)#exit
```

- 为各 VLAN 分配 Access 口

进入端口范围 Gi 0/2-12

```
Ruijie(config)#interface range GigabitEthernet 0/2-12
```

将端口 Gi 0/2-12 配置为 Access 口

```
Ruijie(config-if)#switchport mode access
```

将端口 Gi 0/2-12 分配给 VLAN 10

```
Ruijie(config-if)#switchport access vlan 10
```

进入端口范围 Gi 0/13-24

```
Ruijie(config-if)#interface range GigabitEthernet 0/13-24
```

将端口 Gi 0/13-24 配置为 Access 口

```
Ruijie(config-if)#switchport mode access
```

将端口 Gi 0/13-24 分配给 VLAN 20

```
Ruijie(config-if)#switchport access vlan 20
```

退回到全局配置模式

```
Ruijie(config-if)#exit
```

指定上连核心交换机的 trunk 口

进入端口 Gi 0/1

```
Ruijie(config)#interface GigabitEthernet 0/1
```

配置该端口 Gi 0/1 都为 trunk 口

```
Ruijie(config-if)#switchport mode trunk
```

退回到全局配置模式

```
Ruijie(config-if)#exit
```

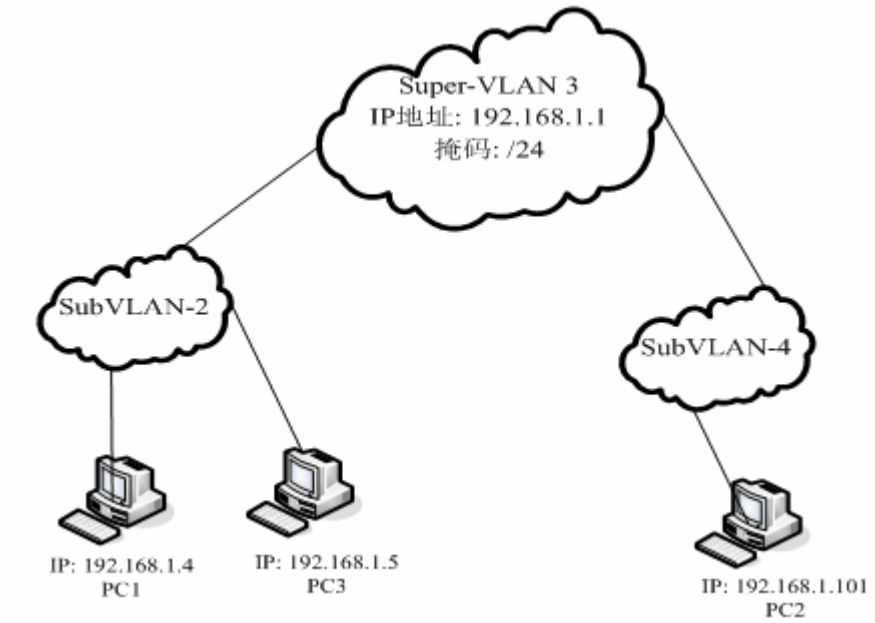
6 Super VLAN

6.1 概述

Super VLAN 是 VLAN 划分的一种方式。Super VLAN 又称为 VLAN 聚合，是一种专门优化 IP 地址的管理技术。其原理是将一个网段的 IP 分给不同的子 VLAN(Sub VLAN)，这些 Sub VLAN 同属于一个 Super VLAN。而每一个 Sub VLAN 都是独立的广播域，不同 Sub VLAN 之间二层相互隔离。当 Sub VLAN 内的用户需要进行三层通信时，将使用 Super VLAN 的虚接口的 IP 地址作为网关地址，这样多个 VLAN 共享一个 IP 地址，从而节省了 IP 地址资源。同时，为了实现不同 Sub VLAN 间的三层互通及 Sub VLAN 与其他网络的互通，需要利用 ARP 代理功能。通过 ARP 代理可以进行 ARP 请求和响应报文的转发与处理，从而实现了二层隔离端口间的三层互通。缺省状态下，Super VLAN 和 Sub VLAN 的 ARP 代理功能是打开的。

采用 Super VLAN 技术可以极大的节省 IP 地址，它只需对包含多个 Sub VLAN 的 Super VLAN 分配一个 IP 地址，既节省地址又方便网络管理。

图 6-1



下面描述一下 VLAN 聚合情况下，两个聚合的 Sub-VLAN 之间通信的过程，如上图所示：

Sub VLAN2 和 Sub VLAN4 聚合成 Super VLAN3，为 Super VLAN3 分配一个 IP 子网， Sub VLAN2 和 Sub VLAN4 都位于此子网。假设 Sub VLAN2 中的一台主机 PC1 要与子网中的另一台主机 PC2 通信，PC1 发现对方与自己处于同一网段，则直接发出目的 IP 的 ARP 请求报文。那么三层设备收到该 ARP 请求报文后，将其在 Sub VLAN2 的范围内直接通过二层广播此报文，并送一份给设备本身的 ARP 模块，设备的 ARP 模块首先看 ARP 请求报文中的目的 IP 地址是不是在 Sub-VLAN2 中，如果是就丢弃该报文，因为表明它和 PC1 在同一个广播域里面，那么目的主机将直接应答给 PC1；如果不是就将 SuperVLAN3 的 MAC 地址应答给 PC1，完成 ARP 的代理工作。比如 PC1 和 PC2 的通信就需要通过 ARP 代理，由设备转发 PC1 发给 PC2 的数据包； 而 PC1 和 PC3 的通信则直接进行无需通过设备转发。

限制：

- Super VLAN 不能包含任何成员口，只能包含 Sub VLAN，由 Sub VLAN 包含实际的物理接口。
- Super VLAN 不能做为其它 Super VLAN 的 Sub VLAN。
- Super VLAN 不能当正常的 1Q vlan 来使用。
- VLan 1 不能作为 SuperVLAN。
- Sub VLAN 不能配置为网络接口，不能配置 IP 地址。
- SVLAN 不能使用 VRRP，不支持多播。
- 基于 Super VLAN 接口的 ACL 和 QOS 配置不对 Sub VLAN 生效。

Sub VLAN 容量相关配置，参见《硬件表项容量》文档“配置共享池最大数目”章节。

6.2 配置Super VLAN

6.2.1 创建Super VLAN

可以使用下面的命令来设置 Super VLAN。

命令	作用
Ruijie# **configure terminal**	进入全局配置模式
Ruijie(config)# **vlan** *vlan-id*	进入 VLAN 配置模式
Ruijie(config-vlan)# **supervlan**	打开 SuperVLAN 的功能
Ruijie(config-vlan)# **end**	回到特权模式

缺省情况下，Super VLAN 功能是关闭的，使用 **no supervlan** 可以关闭已经打开得 supervlan 的功能。

6.2.2 配置Super VLAN的Sub VLAN

必须为 SuperVLAN 配置 SubVLAN，该 SuperVLAN 才有意义。

可以使用下面的命令来使一个 VLAN 属于 Super VLAN 的 SubVLAN。

可能由于资源不足导致设置 SubVLAN 失败

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **vlan** *vlan-id*	进入 VLAN 配置模式
Ruijie(config-vlan)# **supervlan**	设置该 vlan 为 SuperVLAN
Ruijie(config-vlan)# **subvlan** *vlan-id-list*	指定若干个 sub vlan 并把它们加入 supervlan 中。
Ruijie(config-vlan)# **exit**	退出到全局模式

使用 **no subvlan** [*vlan-id-list*] 命令删除 SuperVLAN 的 SubVLAN。

不能使用 **no vlan** 命令删除 SubVLAN，必须先转成普通 VLAN 才能删除。

6.2.3 设置Sub VLAN的地址范围

用户可以为每个 SubVLAN 配置其地址空间范围，以便设备区分给定的 IP 地址属于哪个 SubVLAN. 同一个 SuperVLAN 下的 SubVLAN 配置的地址空间范围不可以有交叉重叠或者互相包含的关系.

请在全局模式下进行下列配置。

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **vlan** *vlan-id*	进入 vlan 配置模式
Ruijie(config-vlan)# **subvlan-address-range** *start-ip end-ip*	设置子 VLAN 的地址范围，start-ip 为该 SubVLAN 的 IP 起始地址 end-ip 为该 SubVLAN 的 IP 结束地址
Ruijie(config-vlan)# **end**	回到特权模式
Ruijie# **show running-config**	验证前面各步骤的配置

用户可以通过执行 no subvlan-address-range 删除之前配置

6.2.4 设置Super VLAN的虚拟接口

当 Sub VLAN 内的用户需要进行三层通信时,首先要创建 SuperVLAN 对应的虚拟三层接口进行。

使用 SuperVLAN 自身对应的 SVI 作为虚拟接口

请在全局模式下进行下列配置。

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **interface vlan** *vlan-id*	进入 SVI 模式
Ruijie(config-vlan)# **ip address** *ip mask*	设置虚拟接口的 IP 地址
Ruijie(config-vlan)# **end**	回到特权模式
Ruijie# **show running-config**	验证前面各步骤的配置

6.2.5 设置VLAN的代理ARP功能

可以使用下面的命令来设置 VLAN 的代理 ARP 功能，从而允许 SubVLAN 之间互相通信。缺省情况下该功能是打开的。

请在全局模式下进行下列配置。

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **vlan** *vlan-id*	进入 VLAN 模式
Ruijie(config-vlan)# **proxy-arp**	打开 VLAN 的 ARP 代理功能
Ruijie(config-vlan)# **end**	回到特权模式
Ruijie# **show running-config**	验证前面各步骤的配置

使用 **no proxy-arp** 关闭 Vlan 的代理 ARP 功能。

6.2.6 显示supervlan设置

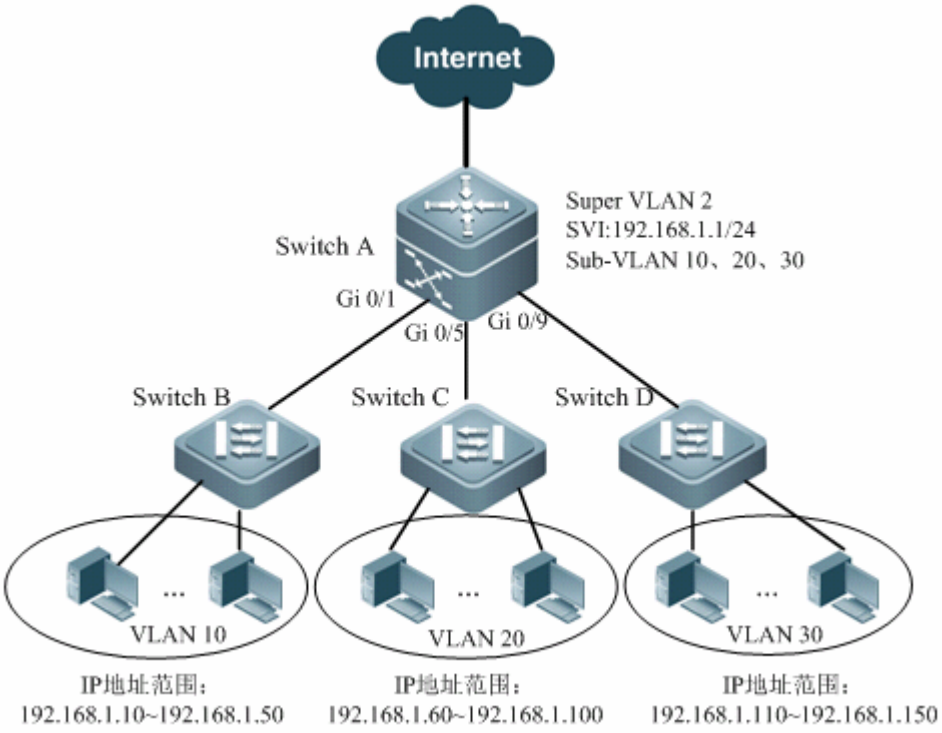
可以使用下面的命令来显示设置 SuperVLAN 的配置

命令	作用
show supervlan	显示 supervlan 配置

6.3 Super VLAN典型配置用例

组网拓扑

图 6-2 Super VLAN 应用拓扑



应用需求

如上图所示，Switch A 作为汇聚设备，通过 Trunk 口下联接入设备 Switch B、Switch C、Switch D。

应用需求如下：

- 接入用户通过划分 VLAN 实现二层隔离。
- 所有 VLAN 用户共享一个 IP 网关，实现三层通信以及与外网通信。

配置要点

- 在接入设备（本例为 Switch B、Switch C、Switch D）上仅需按照普通 VLAN （本例为 VLAN 10、VLAN 20、VLAN 30）实现二层通信隔离。
- 在汇聚设备（本例为 Switch A）上配置 Super VLAN（本例为 VLAN 2）功能，将接入设备上的 VLAN（本例为 VLAN 10、VLAN 20、VLAN 30）设置为 Sub-VLAN。
- 为 Super VLAN 设置 SVI（本例为 192.168.1.1/24），并且为各个 Sub-VLAN 分配 IP 地址范围（本例如上图所示）。

配置步骤

以下仅针对 Switch A 进行配置举例，对于接入设备 Switch B、Switch C、Switch D 的 VLAN 划分情况不再列举。

- 配置 Switch A

第一步，进入全局配置模式，创建 VLAN 2、VLAN 10、VLAN 20、VLAN 30。

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#vlan 2
Ruijie(config-vlan)#exit
Ruijie(config)#vlan 10
Ruijie(config-vlan)#exit
Ruijie(config)#vlan 20
Ruijie(config-vlan)#exit
Ruijie(config)#vlan 30
Ruijie(config-vlan)#exit
```

第二步，设置 VLAN 2 为 Super VLAN，对应的 Sub-VLAN 为 VLAN 10、VLAN 20、VLAN 30。

```
Ruijie(config)#vlan 2
Ruijie(config-vlan)#supervlan
Ruijie(config-vlan)#subvlan 10,20,30
Ruijie(config-vlan)#exit
```

第三步，设置 Super VLAN 2 对应的三层虚拟接口，与 Super VLAN 2 关联的所有 Sub-VLAN 用户将通过该接口进行三层通信。

```
Ruijie(config)#interface vlan 2
Ruijie(config-if-VLAN 2)#ip address 192.168.196.1 255.255.255.0
```

第四步，设置 Sub-VLAN 10 的 IP 地址范围为 192.168.196.10~192.168.196.50，Sub-VLAN 20 的 IP 地址范围为 192.168.196.60~192.168.196.100，Sub-VLAN 30 的 IP 地址范围为 192.168.196.110~192.168.196.150。

```
Ruijie(config)#vlan 10
Ruijie(config-vlan)#subvlan-address-range 192.168.196.10 192.168.196.50
Ruijie(config-vlan)#exit
Ruijie(config)#vlan 20
Ruijie(config-vlan)#subvlan-address-range 192.168.196.60 192.168.196.100
Ruijie(config-vlan)#exit
Ruijie(config)#vlan 30
```

```
Ruijie(config-vlan)#subvlan-address-range 192.168.196.110 192.168.196.150
```

第五步，设置端口 Gi 0/1、Gi 0/5、Gi 0/9 为 Trunk 口，用于连接 Switch B、Switch C、Switch D。

```
Ruijie(config)#interface range gigabitEthernet 0/1,0/5,0/9
Ruijie(config-if-range)#switchport mode trunk
```

验证结果

第一步，查看 Switch A 的配置信息，关注点：Super VLAN 和 Sub-VLAN 的映射关系、Sub-VLAN 的 IP 地址范围、Super VLAN 的网关地址是否配置正确。

```
Ruijie#show running-config
!
vlan 1
!
vlan 2
 supervlan
 subvlan 10,20,30
!
vlan 10
 subvlan-address-range 192.168.196.10 192.168.196.50
!
vlan 20
 subvlan-address-range 192.168.196.60 192.168.196.100
!
vlan 30
 subvlan-address-range 192.168.196.110 192.168.196.150
!
interface GigabitEthernet 0/1
 switchport mode trunk
!
interface GigabitEthernet 0/5
 switchport mode trunk
!
interface GigabitEthernet 0/9
 switchport mode trunk
!
interface VLAN 2
 no ip proxy-arp
 ip address 192.168.196.1 255.255.255.0
!
```

第二步，查看 Super VLAN 的配置情况，如显示信息所示：Super VLAN 和 Sub-VLAN 的 ARP 代理功能默认是开启的。

```
Ruijie(config-if-range)# show supervlan
supervlan id  supervlan arp-proxy  subvlan id  subvlan arp-proxy  subvlan ip range
```

```
-----------  -----------------  ------------------------
2        ON          10         ON       192.168.196.10 - 192.168.196.50
                     20         ON       192.168.196.60 - 192.168.196.100
                     30         ON      192.168.196.110 - 192.168.196.150
```

7 Protocol VLAN

7.1 Protocol VLAN概述

设备端口接收到的报文，都需要进行 VLAN 分类，使报文属于唯一的一个 VLAN，有以下三种可能：

- 如果报文是空 VLAN ID 报文（UNTAG 或 Priority 报文），而设备仅支持基于端口的 VLAN 分类的话，报文所添加 TAG 的 VLAN ID 将是输入端口的 PVID。
- 如果报文是空 VLAN ID 报文（UNTAG 或 Priority 报文），而设备支持基于报文协议类型的 VLAN 分类的话，报文所添加 TAG 的 VLAN ID 将会从输入端口上的协议组配置相对应的 VLAN ID 集中选取，而如果报文的协议类型与输入端口上的所有协议组配置都不相符的话，将按照基于端口的 VLAN 分类来分配 VLAN ID。
- 如果报文是 TAG 报文，其所属 VLAN 分类由 TAG 中的 VLAN ID 决定。

Protocol VLAN 技术就是基于报文协议类型的 VLAN 分类技术，其可以将某一协议类型的空 VLAN ID 报文都划分到同一个 VLAN。

Protocol VLAN 配置只对 Trunk 口和 Hybrid 口生效，对于 Access 口没有作用。

我司产品支持端口上的基于报文类型和以太网类型的 VLAN 分类两种 VLAN 分类技术。

您最好在配置好 VLAN、端口的 Trunk、Hybrid 、Access 和 AP 属性后，再配置 Protocol VLAN，如果您在 Trunk 或 Hybrid 口上配置了 Protocol VLAN，那么您需要报文 Trunk 和 Hybrid 口的许可 VLAN 列表包含 Protocol VLAN 相关的所有 VLAN。

7.2 配置Protocol VLAN

7.2.1 缺省Protocol VLAN

缺省情况下，没有 Protocol VLAN 的配置。

7.2.2 配置报文类型和以太网类型的profile

按如下方式配置报文类型和以太网类型：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式
Ruijie(config)# **protocol-vlan profile** *id* **frame-type** [*type*] **ether-type** [*type*]	配置报文类型和以太网类型的 profile
Ruijie(config)# **no protocol-vlan profile** *id*	删除某 profile 配置
Ruijie(config)# **no protocol-vlan profile**	清除所有的 profile 配置
Ruijie(config-vlan)# **show protocol-vlan profile** [*id*]	显示 profile 配置

举例如下：

```
Ruijie# configure terminal
Ruijie(config)# protocol-vlan profile 1 frame-type ETHERII ether-type EHTER_AARP
Ruijie(config)# protocol-vlan profile 2 frame-type SNAP ether-type 0x809b
Ruijie(config-vlan)# show protocol-vlan profile
profile           frame-type  ether-type        Interfaces|vid
-------      ---------   ----------         -----------
1             ETHERII      EHTER_AARP         NULL|NULL
2             SNAP          ETHER_APPLETALK  NULL|NULL
```

Profile 应用到端口上之后，配置才能生效;

在更新某个 Profile 配置时，必须先删除该 Profile，再重新配置该 Profile;

最大支持 12 个 profile。

7.2.3 应用profile

您可以通过下面的设置步骤来完成：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式
Ruijie(config)# **interface** *interface-id*	进入接口配置模式
Ruijie(config-if)# **protocol-vlan profile** *id* **vlan** *vid*	应用某 profile 到该接口
Ruijie(config-if)# **no protocol-vlan profile** *id*	清除该端口上的某个 profile
Ruijie(config-if)# **no protocol-vlan profile**	清除该端口上的所有 profile
Ruijie(config-if)# **show protocol-vlan profile**	显示 profile 配置

下面例子将 profile 1 和 profile 2 应用到插槽 3 的 GE 口 1，VLAN 分类为 VLAN 101 和 102:

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 3/1
Ruijie(config-if)# protocol-vlan profile 1 vlan 101
Ruijie(config-if)# protocol-vlan profile 2 vlan 102
Ruijie(config-if)# show protocol-vlan profile
profile      frame-type  ether-type       Interfaces|vid
-------      ---------   ----------       --------------
1             ETHERII    EHTER_AARP       gi3/1|101
2             SNAP       ETHER_APPLETALK  gi3/1|102
```

每个接口上都可以应用所有的 profile。

相同的 profile 在不同的接口上可以指定不同的 vid。

最大支持 4094 个 VID。

7.2.4 显示Protocol VLAN配置

您可以通过以下步骤显示 Protocol VLAN 内容：

命令	作用
show protocol-vlan	显示 Protocol VLAN 的内容

举例如下：

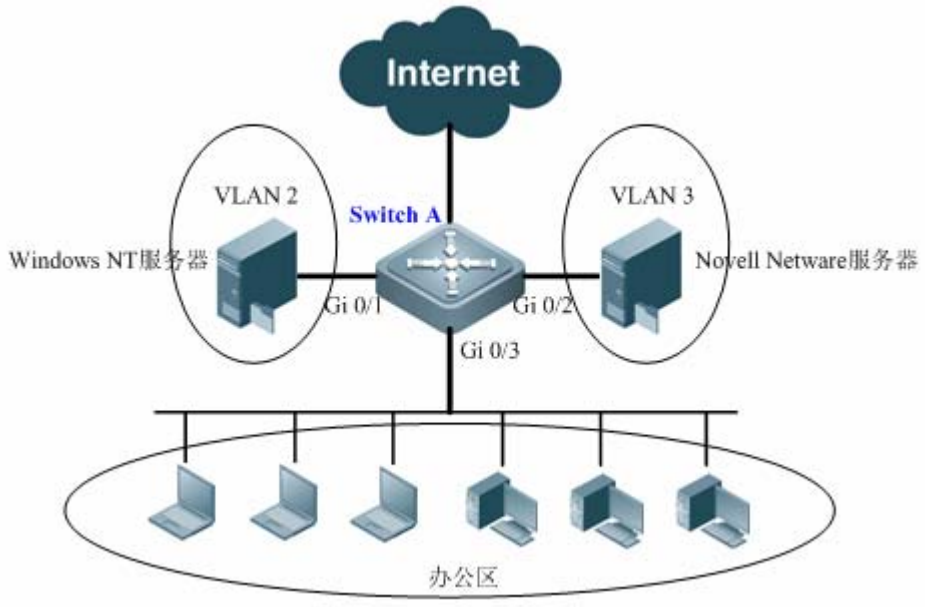
```
Ruijie# show protocol-vlan
ip               mask            vlan
-------------    --------------   ----
192.168.100.3    255.255.255.0    100
profile      frame-type  ether-type           Interfaces|vid
-------      ---------   ------------------   --------------
1             ETHERII      EHTER_AARP          gi3/1|101
2             SNAP         ETHER_APPLETALK     gi3/1|1
```

7.3 Protocol VLAN典型配置用例

7.3.1 基于协议的VLAN配置用例

组网拓扑

图 7-1 基于协议的 VLAN 配置用例示意图



应用需求

上图是由 Windows NT 和 Novell Netware 操作系统互联的网络结构，办公区通过 HUB 与三层设备 Switch A 相连。在办公区内分散着不同的 PC 用户，一部分采用 Windows NT 操作系统，支持 IP 协议；一部分采用 Novell Netware 操作系统，支持 IPX 协议。整个办公区通过上链口 Gi 0/3 与外网以及服务器通信。

组网需求如下：

- 实现 Windows NT 和 Novell Netware 操作系统的 PC 用户二层通信隔离，减少网络流量。

配置要点

1、配置报文类型和以太网类型的 profile（本例将支持 IP 协议的报文对应 Profile 1，支持 IPX 协议的报文对应 Profile 2）

2、将 Profile 应用到上链口（配合为 Gi 0/3）上，并与 VLAN 关联（本例将 Profile 1 关联 VLAN 2，Profile 2 关联 VLAN 3）。

配置基于协议划分 VLAN 的端口仅针对 Trunk 口和 Hybrid 口生效，可以连接 HUB 或直连用户 PC。

PC 用户可以根据协议指定的 VLAN 确认各自所属的 IP 网段（各 VLAN 的网段配置此处不列举）。

配置步骤

- 配置 Switch A

第一步，进入全局配置模式，创建 VLAN 2、VLAN 3。

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#vlan range 2,3
Ruijie(config-vlan-range)#exit
```

第二步，由于 Windows NT 服务器和 Novell Netware 服务器直连端口 Gi 0/1 和 Gi 0/2，可以直接配置基于端口的 VLAN 划分。

```
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-GigabitEthernet 0/1)#switchport access vlan 2
Ruijie(config-GigabitEthernet 0/1)#exit
Ruijie(config)#interface gigabitEthernet 0/2
Ruijie(config-GigabitEthernet 0/2)#switchport access vlan 3
Ruijie(config-GigabitEthernet 0/2)#exit
```

第三步，配置上链口 Gi 0/3 为 Trunk 口。

```
Ruijie(config)#interface gigabitEthernet 0/3
Ruijie(config-GigabitEthernet 0/3)#switchport mode trunk
```

第四步，将 IP、IPX 协议配置相应的 Profile 1、2。（此处假设报文使用 EthernetII 封装，IP 和 IPX 分别对应的以太网类型为 0X0800、0X8137）

```
Ruijie(config)#protocol-vlan profile 1 frame-type eTHERII ether-type 0x0800
Ruijie(config)#protocol-vlan profile 2 frame-type eTHERII ether-type 0x8137
```

第五步，将 Profile 1、2 应用到端口 Gi 0/3 上，划分为 VLAN 2 和 VLAN 3。如果端口收到 IP 协议报文将划分属于 VLAN 2，如果端口收到 IPX 协议报文将划分属于 VLAN 3。

```
Ruijie(config-GigabitEthernet 0/3)#protocol-vlan profile 1 vlan 2
Ruijie(config-GigabitEthernet 0/3)#protocol-vlan profile 2 vlan 3
Ruijie(config-GigabitEthernet 0/3)#exit
```

验证结果

第一步，查看 Switch A 的配置信息，关注点：Protocol VLAN 的 Profile 是否配置正确、应用 Profile 的端口是否配置正确。

```
Ruijie#show running-config
!
vlan 2
!
vlan 3
!
protocol-vlan profile 1 frame-type ETHERII ether-type 0x800
protocol-vlan profile 2 frame-type ETHERII ether-type 0x8137
!
interface GigabitEthernet 0/1
 switchport access vlan 2
!
interface GigabitEthernet 0/2
 switchport access vlan 3
!
interface GigabitEthernet 0/3
 switchport mode trunk
protocol-vlan profile 1 vlan 2
 protocol-vlan profile 2 vlan 3
!
```

第二步，查看配置的 Profile 匹配的协议报文类型，以及应用的端口号、VLAN ID。

```
Ruijie#show protocol-vlan profile
profile frame-type ether-type/DSAP+SSAP interface   vlan
------- ---------- -------------------- --------------------
1       ETHERII    0x800                      Gi0/3         2
2       ETHERII    0x8137                     Gi0/3         3
```

8 Private VLAN

8.1 Private VLAN技术

服务提供商如果给每个用户一个 VLAN，则由于一台设备支持的 VLAN 数最大只有 4096 而限制了服务提供商能支持的用户数；在三层设备上，每个 VLAN 被分配一个子网地址或一系列地址，这种情况导致 IP 地址的浪费，一种解决方法就是应用 Private VLAN 技术。

私有 VLAN(Private VLAN)将一个 VLAN 的二层广播域划分成多个子域，每个子域都由一个私有 VLAN 对组成：主 VLAN(Primary VLAN)和辅助 VLAN(Secondary VLAN)。

一个私有 VLAN 域可以有多个私有 VLAN 对，每一个私有 VLAN 对代表一个子域。在一个私有 VLAN 域中所有的私有 VLAN 对共享同一个主 VLAN。每个子域的辅助 VLAN ID 不同。

一个私有 VLAN 域中只有一个主 VLAN，辅助 VLAN 实现同一个私有 VLAN 域中的二层隔离，有两种类型的辅助 VLAN：

- 隔离 VLAN(Isolated VLAN)：同一个隔离 VLAN 中的端口不能互相进行二层通信。一个私有 VLAN 域中只有一个隔离 VLAN。
- 群体 VLAN(Community VLAN)：同一个群体 VLAN 中的端口可以互相进行二层通信，但不能与其它群体 VLAN 中的端口进行二层通信。一个私有 VLAN 域中可以有多个群体 VLAN。

混杂端口（Promiscuous Port），属于主 VLAN 中的端口，可以与任意端口通讯，包括同一个私有 VLAN 域中辅助 VLAN 的隔离端口和群体端口。

混杂 TRUNK 端口（Promiscuous Trunk Port），可以同时是多个普通 VLAN 和多个私有 VLAN 的成员端口，可以和同一 VLAN 内的任意端口通讯。在普通 VLAN 中，报文转发遵循 802.1Q 规则，在私有 VLAN 中，从混杂 TRUNK 端口转发出的带 TAG 报文，其 VID 如果是辅助 VLAN ID，会转成相应主 VLAN 的 VID 后，再输出。

隔离端口(Isolated Port)，隔离 VLAN 中的端口，只能与混杂口通讯。隔离端口接收到的报文可允许转发到 Trunk Port，但 Trunk Port 接收到 vid 是隔离 VLAN 的报文不能向隔离端口转发。

隔离 TRUNK 端口（Isolated Trunk Port），可以同时是多个普通 VLAN 和多个 PVLAN 的成员端口。在隔离 VLAN 中，只能与混杂口通讯；在群体 VLAN 中，可以与同一个群体 VLAN 的群体端口通讯，也可以同混杂口通讯；在普通 VLAN 中，遵循 802.1Q 规则。隔离 TRUNK 端口接收到的隔离 VLAN ID 的报文可允许转发到 Trunk Port，但 Trunk Port 接收到 vid 是隔离 VLAN 的报文不能向隔离端口转发。

从隔离 TRUNK 端口转发出的带 TAG 报文，其 VID 如果是主 VLAN ID，会转成相应辅助 VLAN 的 VID 后，再输出。

群体端口(Community port)，属于群体 VLAN 中的端口，同一个群体 VLAN 的群体端口可以互相通讯，也可以与混杂口通讯。不能与其它群体 VLAN 中的群体端口及隔离 VLAN 中的隔离端口通讯。

各种端口类型间的报文转发关系：

输出端口 / 输入端口	混杂端口	隔离端口	群体端口	隔离 TRUNK 端口（同 VLAN 内）	混杂 TRUNK 端口（同 VLAN 内）	TRUNK 端口（同 VLAN 内）
混杂端口	通	通	通	通	通	通
隔离端口	通	不通	不通	不通	通	通

群体端口	通	不通	通	通	通	通
隔离 TRUNK 端口（同 VLAN 内）	通	不通	通	不通（隔离 VLAN 内不通，非隔离 VLAN 内通）	通	通
混杂 TRUNK 端口（同 VLAN 内）	通	通	通	通	通	通
TRUNK 端口（同 VLAN 内）	通	不通	通	不通（隔离 VLAN 内不通，非隔离 VLAN 内通）	通	通

各种端口类型间的报文转发后 VLAN TAG 变化关系：

输出端口 / 输入端口	混杂端口	隔离端口	群体端口	隔离 TRUNK 端口（同 VLAN 内）	混杂 TRUNK 端口（同 VLAN 内）	TRUNK 端口（同 VLAN 内）
混杂端口	不变	不变	不变	加上辅助 VLAN ID	加上主 VLAN ID TAG，其它非私有 VLAN 内不变。	加上主 VLAN ID TAG
隔离端口	不变	NA	NA	NA	加上主 VLAN ID TAG，其它非私有 VLAN 内不变。	加上隔离 VLAN ID TAG
群体端口	不变	NA	不变	加上群体 VLAN ID TAG	加上主 VLAN ID TAG，其它非私有 VLAN 内不变。	加上群体 VLAN ID TAG
隔离 TRUNK 端口（同 VLAN 内）	去掉 VLAN TAG	NA	去掉 VLAN TAG	非隔离 VLAN 内不变。	加上主 VLAN ID TAG，其它非私有 VLAN 内不变。	不变
混杂 TRUNK 端口（同 VLAN 内）	去掉 VLAN TAG	不变	不变	加上辅助 VLAN ID	加上主 VLAN ID TAG，其它非私有 VLAN 内不变。	不变
TRUNK 端口（同 VLAN 内）	去掉 VLAN TAG	NA	去掉 VLAN TAG	主 VLAN 内转成辅助 VLAN ID，其它非隔离 VLAN 内不变。	加上主 VLAN ID TAG，其它非私有 VLAN 内不变。	不变
交换机 CPU	Untag	Untag	Untag	加上辅助 VLAN ID TAG	加上主 VLAN ID TAG，其它非私有 VLAN 内不变。	加上主 VLAN ID TAG

私有 VLAN 中，只有主 VLAN 可以创建 SVI 接口，辅助 VLAN 不可以创建 SVI。

私有 VLAN 中的端口可以为 SPAN 源端口，不可以为镜像目的端口。

输出端口 / 输入端口	混杂端口	隔离端口	群体端口	隔离 TRUNK 端口（同 VLAN 内）	TRUNK 端口（同 VLAN 内）	TRUNK 端口（同 VLAN 内）
混杂端口	不变	不变	不变	加上主 VLAN ID TAG	加上主 VLAN ID TAG，其它非私有 VLAN 内不变。	加上主 VLAN ID TAG
隔离端口	不变	NA	NA	NA	加上主 VLAN ID TAG，其	加上隔离

					它非私有 VLAN 内不变。	VLAN ID TAG
群体端口	不变	NA	不变	加上群体 VLAN ID TAG	加上主 VLAN ID TAG，其它非私有 VLAN 内不变。	加上群体 VLAN ID TAG
隔离 TRUNK 端口(同 VLAN 内)	去掉 VLAN TAG	NA	去掉 VLAN TAG	非隔离 VLAN 内不变。	加上主 VLAN ID TAG，其它非私有 VLAN 内不变。	不变
混杂 TRUNK 端口（同 VLAN 内）	去掉 VLAN TAG	不变	不变	非隔离 VLAN 内不变。	加上主 VLAN ID TAG，其它非私有 VLAN 内不变。	不变
TRUNK 端口（同 VLAN 内）	去掉 VLAN TAG	NA	去掉 VLAN TAG	非隔离 VLAN 内都不变。	加上主 VLAN ID TAG，其它非私有 VLAN 内不变。	不变
交换机 CPU	Untag	Untag	Untag	加上主 VLAN ID TAG	加上主 VLAN ID TAG，其它非私有 VLAN 内不变。	加上主 VLAN ID TAG

8.2 Private VLAN配置

8.2.1 缺省Private VLAN设置

缺省情况下，没有 Private VLAN 的配置

8.2.2 配置VLAN作为私有VLAN

配置方法如下命令

命令	说明
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **vlan** *vid*	进入 VLAN 配置模式
Ruijie(config-vlan)# **private-vlan**{**community** | **isolated**| **primary**}	配置私有 VLAN 类型
Ruijie(config-vlan)# **no private-vlan**{**community** | **isolated** | **primary**}	取消私有 VLAN 配置
Ruijie(config-vlan)# **end**	退出 VLAN 模式
Ruijie# **show vlan private-vlan** [*type*]	显示私有 VLAN

在 802.1Q Vlan 中具有成员口情况不能声明为私有 VLAN,VLAN 1 不能声明为私有 VLAN,对于具有 Trunk 口或 Uplink 口的 802.1Q VLAN 中，先将该 VLAN 从许可 VLAN 列表中删除，对 Private VLAN 处于 ACTIVE 状态必须满足以下条件：1）具有 Priamry VLAN；2）具有 Secondary VLAN；3）Secondary VLAN 与 Primary VLAN 关联

以下命令将 802.1Q VLAN 配置为 Private VLAN：

```
Ruijie# configure terminal
Ruijie(config)# vlan 303
Ruijie(config-vlan)# private-vlan community
```

```
Ruijie(config-vlan)# end
Ruijie# show vlan private-vlan community
VLAN Type  Status    Routed   Interface   Associated VLANs
--- ----   --------  ------   ---------   ------------------
303 comm   inactive  Disabled               no association
Ruijie# configure terminal
Ruijie(config)# vlan 404
Ruijie(config-vlan)# private-vlan isolated
Ruijie(config-vlan)# end
Ruijie# show vlan private-vlan
VLAN Type  Status    Routed   Interface   Associated VLANs
--- ----   --------  ------   ---------   ------------------
303 comm  inactive  Disabled               no association
404 isol  inactive  Disabled               no association
```

8.2.3 关联Secondary VLAN和Primary VLAN

按如下方式关联 Secondary VLAN 和 Primary VLAN：

命令	说明
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **vlan** *p_vid*	进入 Primary VLAN 配置模式
Ruijie(config-vlan)# **private-vlan association** {*svlist* | **add** *svlist* | **remove** *svlist*}	关联 Secondary VLAN
Ruijie(config-vlan)# **no private-vlan association**	清除与所有 Secondary VLAN 的关联
Ruijie(config-vlan)# **end**	退出 VLAN 模式
Ruijie# **show vlan private-vlan** [*type*]	显示私有 VLAN

举例如下：

```
Ruijie# configure terminal
Ruijie(config)# vlan 202
Ruijie(config-vlan)# private-vlan association 303-307,309,440
Ruijie(config-vlan)# end
Ruijie# show vlan private-vlan
VLAN Type  Status    Routed   Interface   Associated VLANs
--- ----   --------  ------   ---------   ------------------
202 prim  inactive  Disabled               303-307,309,440
303 comm  inactive  Disabled               202
304 comm  inactive  Disabled               202
305 comm  inactive  Disabled               202
306 comm  inactive  Disabled               202
307 comm  inactive  Disabled               202
309 comm  inactive  Disabled               202
```

```
440 comm  inactive  Disabled              202
```

该操作在声明为 Primary VLAN 的 VLAN 配置模式进行。

当启用 MSTP 时，请确认 Secondary vlan 和 Primary vlan 需要关联到同一个实例（instance）上。

8.2.4 映射Secondary VLAN和Primary VLAN的三层接口

您可以通过下面的设置步骤来完成：

命令	说明
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **interface vlan** *p_vid*	进入 Primary VLAN 的接口模式
Ruijie(config-if)# **private-vlan mapping** {*svlist* | **add** *svlist* | **remove** *svlist*}	映射 Secondary VLAN 到 Primary VLAN 的 SVI 三层交换。
Ruijie(config-if)# **end**	退出接口模式

下面例子配置 Secondary VLAN 路由：

```
Ruijie# configure terminal
Ruijie(config)# interface vlan 202
Ruijie(config-if)# private-vlan mapping add 303-307,309,440
Ruijie(config-if)# end
```

操作中的 Primary VLAN 和 Secondary VLAN 是相关联的。

8.2.5 配置二层接口作为私有VLAN的主机端口

按照以下步骤配置二层接口作为私有 VLAN 的主机端口(Host Port)：

命令	说明
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **interface** *interface-id*	进入接口配置模式 *fastethernet*, *gigabitethernet*, *tengigabitethernet*
Ruijie(config-if)# **switchport mode private-vlan host**	配置为二层交换模式
Ruijie(config-if)# **no switchport mode**	清除私有 VLAN 配置
Ruijie(config-if)# **switchport private-vlan host-association** *p_vid s_vid*	关联二层口与私有 VLAN
Ruijie(config-if)# **no switchport private-vlan host-association**	清除关联

举例如下：

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/2
Ruijie(config-if)# switchport mode private-vlan host
Ruijie(config-if)# switchport private-vlan host-association 202 203
Ruijie(config-if)# end
```

操作中的 Primary VLAN 和 Secondary VLAN 是相关联的。

8.2.6 配置二层接口作为PVLAN 隔离TRUNK端口

配置二层接口作为隔离 PVLAN TRUNK 端口，通过以下操作命令：

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config-if)# **interface** *interface-id*	进入接口配置模式 *fastethernet*, *gigabitethernet*, *tengigabitethernet*
Ruijie(config-if)# **switchport mode trunk**	配置为 trunk 模式
Ruijie(config-if)# **switchport private-vlan association trunk** *p_vid s_vid*	关联二层口与私有 VLAN，允许配置多对。p_vid 和 s_vid 参数分别是主 VLAN ID 和辅助 VLAN ID。
Ruijie(config-if)# **no switchport private-vlan association trunk** *p_vid s_vid*	清除关联
Ruijie(config-if)# **switchport trunk allowed vlan** {**all** | [**add** | **remove** | **except**] } *vlan-list*	（可选）配置这个 Trunk 口的许可 VLAN 列表。参数 *vlan-list* 可以是一个 VLAN，也可以是一系列 VLAN，以小的 VLAN ID 开头，以大的 VLAN ID 结尾，中间用-号连接。如：10–20。 all 的含义是许可 VLAN 列表包含所有支持的 VLAN； add 表示将指定 VLAN 列表加入许可 VLAN 列表； remove 表示将指定 VLAN 列表从许可 VLAN 列表中删除； except 表示将除列出的 VLAN 列表外的所有 VLAN 加入许可 VLAN 列表；
Ruijie(config-if)# **switchport trunk native vlan** *vlan-id*	配置 Native VLAN 如果想把 Trunk 的 Native VLAN 列表改回缺省的 VLAN 1，请使用 no switchport trunk native vlan 接口配置命令。

举例如下：

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/2
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# switchport private-vlan association trunk 202 203
Ruijie(config-if)# switchport trunk allowed vlan 100
Ruijie(config-if)# switchport trunk native vlan 100
Ruijie(config-if)# end
```

操作中的 Primary VLAN 和 Secondary VLAN 是相关联的

8.2.7 配置二层接口作为混杂TRUNK端口

配置二层接口作为混杂 PVLAN TRUNK 端口，通过以下操作命令：

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config-if)# **interface** *interface-id*	进入接口配置模式 *fastethernet*, *gigabitethernet*, *tengigabitethernet*
Ruijie(config-if)# **switchport mode trunk**	配置为 trunk 模式
Ruijie(config-if)# **switchport private-vlan promiscuous trunk** *p_vid s_list*	关联二层口与私有 VLAN，允许配置多对。p_vid 和 s_list 参数分别是主 VLAN ID 和辅助 VLAN ID 列表。
Ruijie(config-if)# **no switchport private-vlan promiscuous trunk** *p_vid s_list*	清除关联
Ruijie(config-if)# **switchport trunk allowed vlan** {**all** | [**add** | **remove** | **except**] } *vlan-list*	（可选）配置这个 Trunk 口的许可 VLAN 列表。参数 *vlan-list* 可以是一个 VLAN，也可以是一系列 VLAN，以小的 VLAN ID 开头，以大的 VLAN ID 结尾，中间用-号连接。如：10–20。 all 的含义是许可 VLAN 列表包含所有支持的 VLAN； add 表示将指定 VLAN 列表加入许可 VLAN 列表； remove 表示将指定 VLAN 列表从许可 VLAN 列表中删除； except 表示将除列出的 VLAN 列表外的所有 VLAN 加入许可 VLAN 列表；
Ruijie(config-if)# **switchport trunk native vlan** *vlan-id*	配置 Native VLAN 如果想把 Trunk 的 Native VLAN 列表改回缺省的 VLAN 1，请使用 no switchport trunk native vlan 接口配置命令。

举例如下：

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/2
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# switchport private-vlan promiscuous trunk 202 203
Ruijie(config-if)# switchport trunk allowed vlan 100
Ruijie(config-if)# switchport trunk native vlan 100
Ruijie(config-if)# end
```

操作中的 Primary VLAN 和 Secondary VLAN 是相关联的

8.2.8 配置二层接口作为私有VLAN的混杂端口

配置二层接口作为私有 VLAN 的端口，通过以下操作命令：

命令	说明
Ruijie# **configure terminal**	进入配置模式

Ruijie(config)# **interface** *interface-id*	进入接口配置模式 百兆,千兆，万兆
Ruijie(config-if)# **switchport mode private-vlan promiscuous**	配置为私有 VLAN 二层交换模式
Ruijie(config-if)# **no switchport mode**	删除端口私有 VLAN 配置
Ruijie(config-if)# **switchport private-vlan mapping** *p_vid*{*svlist* | **add** *svlist* | **remove** *svlist*}	配置私有 VLAN 混杂端口所在的 Primary VLAN 以 Secondary VLAN 列表
Ruijie(config-if)# **no switchport private-vlan mapping**	取消混杂所有的的 seconary VLAN.

下面例子描述配置过程：

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/2
Ruijie(config-if)# switchport mode private-vlan promiscuous
Ruijie(config-if)# switchport private-vlan mapping 202 add 203
Ruijie(config-if)# end
```

操作中的 Primary VLAN 和 Secondary VLAN 是相关联的

8.2.9 显示private VLAN

您可以通过以下步骤显示 Private VLAN 内容：

命令	说明
show vlan private-vlan [*type*]	显示 private VLAN 的内容

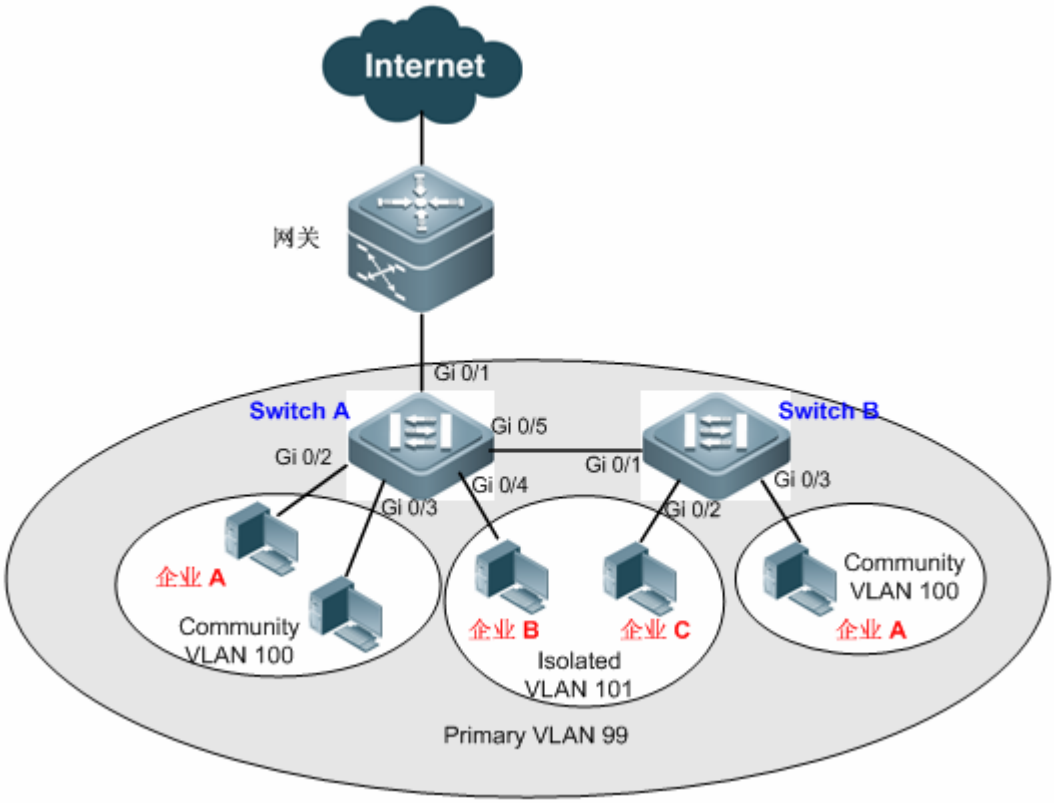
```
Ruijie# show vlan private-vlan
VLAN Type  Status    Routed   Interface   Associated VLANs
---- ----  --------  ------   ---------   ------------------
202 prim   active   Enabled    Gi0/1       303-307,309,440
303 comm   active   Disabled   Gi0/2       202
304 comm   active   Disabled   Gi0/3       202
305 comm   active   Disabled   Gi0/4       202
306 comm   active   Disabled                202
307 comm   active   Disabled                202
309 comm   active   Disabled                202
440 comm   active   Enabled    Gi0/5       202
```

8.3 PVLAN典型配置用例

8.3.1 PVLAN跨设备二层应用

拓扑图

图 8-1 PVLAN 跨设备二层应用拓扑



应用需求

如上图所示，在主机托管业务运营网络中，各企业用户通过设备 Switch A、Switch B 接入网络。主要需求如下：

- 企业内用户之间可以进行通信，企业间用户通信隔离
- 所有企业用户共享一个网关地址，可以与外网通信。

配置要点

- 将所有企业配置属于同一个 PVLAN（本例为 Primary VLAN 99），所有企业用户均通过该 VLAN 共享一个三层接口，实现外网通信。
- 如果企业内有多个用户，可以将各企业划分属于不同的 Community VLAN（本例将企业 A 划分属于 Community VLAN 100），实现企业内用户互相通信，企业间用户通信隔离。

- 如果企业内仅有一个用户，可以将这些企业划分属于同一个 Isolated VLAN（本例将企业 B 和 C 划分属于 Isolated VLAN 101），实现企业间用户通信隔离。

☑ 跨设备运行 PVLAN，需要将相连的端口配置为 Trunk Port。

☑ 与网关相连的端口需要配置为 Promiscuous Port；对端口网关设备接口可以配置为 Trunk Port 或 Hybrid Port，且 Native VLAN 是 PVLAN 的 Primary VLAN。

配置步骤

第一步，在设备上创建 Primary VLAN 和 Secondary VLAN。

！在 Switch A 上配置 Primary VLAN 99、Community VLAN 100、Isolated VLAN 101。

```
SwitchA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)#vlan 99
SwitchA(config-vlan)#private-vlan primary
SwitchA(config-vlan)#exit
SwitchA(config)#vlan 100
SwitchA(config-vlan)#private-vlan community
SwitchA(config-vlan)#exit
SwitchA(config)#vlan 101
SwitchA(config-vlan)#private-vlan isolated
SwitchA(config-vlan)#exit
```

！Switch B 的配置同上。

第二步，在设备上关联 Secondary VLAN 和 Primary VLAN。

！在 Switch A 上配置 Community VLAN 100、Isoated VLAN 101 和 Primary VLAN 99 关联。

```
SwitchA(config)#vlan 99
SwitchA(config-vlan)#private-vlan association 100-101
SwitchA(config-vlan)#exit
```

！Switch B 的配置同上。

第三步，配置上链口，用于连接网关设备。

！将 Switch A 的端口 Gi 0/1 设置为 Promiscuous Port

```
SwitchA(config)#interface gigabitEthernet 0/1
SwitchA(config-if-GigabitEthernet 0/1)#switchport mode private-vlan promiscuous
SwitchA(config-if-GigabitEthernet 0/1)#switchport private-vlan mapping 99 100-101
SwitchA(config-if-GigabitEthernet 0/1)#exit
```

第四步，将各企业用户接入端口划分属于相应的 Secondary VLAN（如上图所示）。

！在 Switch A 上配置端口 Gi 0/2、Gi 0/3 属于 Community VLAN 100，端口 Gi 0/4 属于 Isolated VLAN 101。

```
SwitchA(config)#interface range gigabitEthernet 0/2-3
```

```
SwitchA(config-if-range)#switchport mode private-vlan host
SwitchA(config-if-range)#switchport private-vlan host-association 99 100
SwitchA(config-if-range)#exit
SwitchA(config)#interface gigabitEthernet 0/4
SwitchA(config-if-GigabitEthernet 0/4)#switchport mode private-vlan host
SwitchA(config-if-GigabitEthernet 0/4)#switchport private-vlan host-association 99 101
```

！在 Switch B 上配置端口 Gi 0/2 属于 Isoated VLAN 101，端口 Gi 0/3 属于 Community VLAN 100。

```
SwitchB(config)#interface gigabitEthernet 0/2
SwitchB(config-if-GigabitEthernet 0/2)#switchport mode private-vlan host
SwitchB(config-if-GigabitEthernet 0/2)# switchport private-vlan host-association 99 101
SwitchB(config-if-GigabitEthernet 0/2)#exit
SwitchB(config)#interface gigabitEthernet 0/3
SwitchB(config-if-GigabitEthernet 0/3)#switchport mode private-vlan host
SwitchB(config-if-GigabitEthernet 0/3)# switchport private-vlan host-association 99 100
SwitchB(config-if-GigabitEthernet 0/3)#exit
```

第五步，配置 PVLAN 跨设备运行的连接口。

！配置 Switch A 的端口 Gi 0/5 为 Trunk Port

```
SwitchA(config)#interface gigabitEthernet 0/5
SwitchA(config-if-GigabitEthernet 0/5)#switchport mode trunk
SwitchA(config-if-GigabitEthernet 0/5)#exit
```

！配置 Switch B 的端口 Gi 0/1 为 Trunk Port。

```
SwitchB(config)#interface gigabitEthernet 0/1
SwitchB(config-if-GigabitEthernet 0/1)#switchport mode trunk
SwitchB(config-if-GigabitEthernet 0/1)#exit
```

配置验证

第一步，查看设备的配置信息。

！Switch A 的配置信息

```
SwitchA#show running-config
!
vlan 99
 private-vlan primary
 private-vlan association add 100-101
!
vlan 100
 private-vlan community
!
vlan 101
 private-vlan isolated
```

```
!
interface GigabitEthernet 0/1
 switchport mode private-vlan promiscuous
 switchport private-vlan mapping 99 add 100-101
!
interface GigabitEthernet 0/2
 switchport mode private-vlan host
 switchport private-vlan host-association 99 100
!
interface GigabitEthernet 0/3
 switchport mode private-vlan host
 switchport private-vlan host-association 99 100
!
interface GigabitEthernet 0/4
 switchport mode private-vlan host
 switchport private-vlan host-association 99 101
!
interface GigabitEthernet 0/5
 switchport mode trunk
!
```

！Switch B 的配置信息

```
SwitchB#show running-config
!
vlan 99
 private-vlan primary
 private-vlan association add 100-101
!
vlan 100
 private-vlan community
!
vlan 101
 private-vlan isolated
!
interface GigabitEthernet 0/1
 switchport mode trunk
!
interface GigabitEthernet 0/2
 switchport mode private-vlan host
 switchport private-vlan host-association 99 101
!
interface GigabitEthernet 0/3
 switchport mode private-vlan host
 switchport private-vlan host-association 99 100
!
```

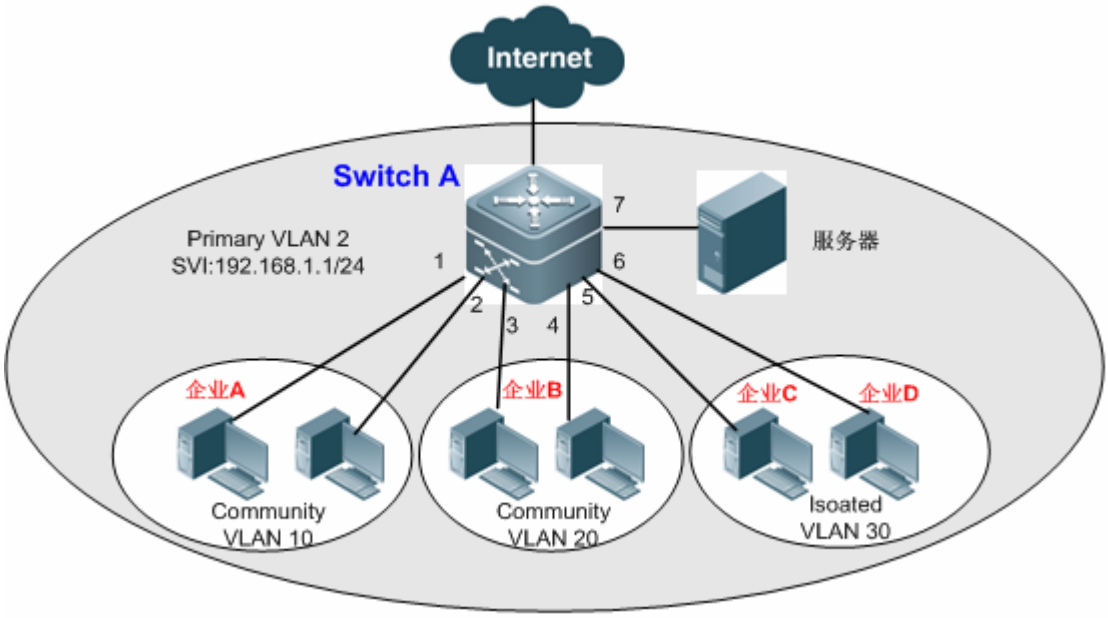
第二步，在设备上查看 PVLAN 的相关配置信息。

```
SwitchA#show vlan private-vlan
VLAN  Type       Status   Routed   Ports           Associated VLANs
------------------------------ ------------------
99    primary    active   Disabled Gi0/1, Gi0/5          100-101
100   community  active   Disabled Gi0/2, Gi0/3, Gi0/5       99
101   isolated   active   Disabled Gi0/4, Gi0/5                 99
```

8.3.2 PVLAN单台设备三层应用

拓扑图

图 8-2 PVLAN 单台设备三层应用拓扑



应用需求

如上图所示，在主机托管业务运营网络中，各企业用户通过三层设备 Switch A 接入网络。主要需求如下：

- 企业内用户之间可以通信，企业间用户通信隔离。
- 所有企业用户都可以访问服务器
- 所有企业用户共享一个网关地址，可以与外网通信。

配置要点

- 在设备上（本例为 Switch A）配置 PVLAN 功能，具体配置要点可参考“PVLAN 跨设备二层应用”章节的配置要点。

- 将直连服务器的端口（本例为端口 Gi 0/7）设置为 Promiscuous Port，所有企业用户都可以通过 Promiscuous Port 和服务器通信。
- 在三层设备(本例为 Switch A)配置 PVLAN 的网关地址(本例配置 VLAN 2 的 SVI 为 192.168.1.1/24)，并配置 Primary VLAN（本例为 VLAN 2）和 Secondary VLAN（本例为 VLAN 10、20、30）的三层接口映射关系，所有企业用户可以通过这个网关地址与外网通信。

配置步骤

第一步，在设备上创建 Primary VLAN 和 Secondary VLAN。

！在 Switch A 上配置 Primary VLAN 2、Community VLAN 10、Community VLAN 20、Isolated VLAN 30。

```
SwitchA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)#vlan 2
SwitchA(config-vlan)#private-vlan primary
SwitchA(config-vlan)#exit
SwitchA(config)#vlan 10
SwitchA(config-vlan)#private-vlan community
SwitchA(config-vlan)#exit
SwitchA(config)#vlan 20
SwitchA(config-vlan)#private-vlan community
SwitchA(config-vlan)#exit
SwitchA(config)#vlan 30
SwitchA(config-vlan)#private-vlan isolated
SwitchA(config-vlan)#exit
```

第二步，在设备上关联 Secondary VLAN 和 Primary VLAN。

！在 Switch A 上配置 Community VLAN 10、Community VLAN 20、Isoated VLAN 30 和 Primary VLAN 2 关联。

```
SwitchA(config)#vlan 2
SwitchA(config-vlan)#private-vlan association 10,20,30
SwitchA(config-vlan)#exit
```

第三步，将各企业用户接入端口划分属于相应的 Secondary VLAN（如上图所示）。

！在 Switch A 上配置端口 Gi 0/1、Gi 0/2 属于 Community VLAN 10，端口 Gi 0/3、Gi 0/4 属于 Community VLAN 20，端口 Gi 0/5、Gi 0/6 属于 Isloated VLAN 30。

```
SwitchA(config)#interface range gigabitEthernet 0/1-2
SwitchA(config-if-range)#switchport mode private-vlan host
SwitchA(config-if-range)#switchport private-vlan host-association 2 10
SwitchA(config-if-range)#exit
SwitchA(config)#interface range gigabitEthernet 0/3-4
SwitchA(config-if-range)#switchport mode private-vlan host
SwitchA(config-if-range)#switchport private-vlan host-association 2 20
SwitchA(config-if-range)#exit
```

```
SwitchA(config)#interface range gigabitEthernet 0/5-6
SwitchA(config-if-range)#switchport mode private-vlan host
SwitchA(config-if-range)#switchport private-vlan host-association 2 30
SwitchA(config-if-range)#exit
```

第四步，配置服务器连接端口。

！将 Switch A 的端口 Gi 0/7 配置为 Promiscuous Port

```
SwitchA(config)#interface gigabitEthernet 0/7
SwitchA(config-if-GigabitEthernet 0/7)#switchport mode private-vlan promiscuous
SwitchA(config-if-GigabitEthernet 0/7)#switchport private-vlan maping 2 10,20,30
SwitchA(config-if-GigabitEthernet 0/7)#exit
```

第五步，在三层设备配置 PVLAN 的网关地址

！在 Switch A 上配置 Primary VLAN 2 的 SVI 为 192.168.1.1/24，并配置映射 Community VLAN 10、Community VLAN 20 和 Isolated VLAN 30。

```
SwitchA(config)#interface vlan 2
SwitchA(config-if-VLAN 2)#ip address 192.168.1.1 255.255.255.0
SwitchA(config-if-VLAN 2)#private-vlan mapping 10,20,30
SwitchA(config-if-VLAN 2)#exit
```

配置验证

第一步，查看 Switch A 的配置信息。

```
SwitchA#show running-config
!
vlan 2
 private-vlan primary
 private-vlan association add 10,20,30
!
vlan 10
 private-vlan community
!
vlan 20
 private-vlan community
!
vlan 30
 private-vlan isolated
!
interface GigabitEthernet 0/1
 switchport mode private-vlan host
 switchport private-vlan host-association 2 10
!
interface GigabitEthernet 0/2
```

```
 switchport mode private-vlan host
 switchport private-vlan host-association 2 10
!
interface GigabitEthernet 0/3
 switchport mode private-vlan host
 switchport private-vlan host-association 2 20
!
interface GigabitEthernet 0/4
 switchport mode private-vlan host
 switchport private-vlan host-association 2 20
!
interface GigabitEthernet 0/5
 switchport mode private-vlan host
 switchport private-vlan host-association 2 30
!
interface GigabitEthernet 0/6
 switchport mode private-vlan host
 switchport private-vlan host-association 2 30
!
interface GigabitEthernet 0/7
 switchport mode private-vlan promiscuous
 switchport private-vlan mapping 2 add 10,20,30
!
interface VLAN 2
 no ip proxy-arp
 ip address 192.168.1.1 255.255.255.0
 private-vlan mapping add 10,20,30
!
```

第二步，查看 PVLAN 的相关配置信息

```
SwitchA#show vlan private-vlan
VLAN  Type   Status   Routed   Ports  Associated VLANs
------------------------------ ------------------
2     primary    active   Enabled  Gi0/7          10,20,30
10    community  active   Enabled  Gi0/1, Gi0/2    2
20    community  active   Enabled  Gi0/3, Gi0/4    2
30    isolated   active   Enabled  Gi0/5, Gi0/6    2
```

9 SHARE VLAN

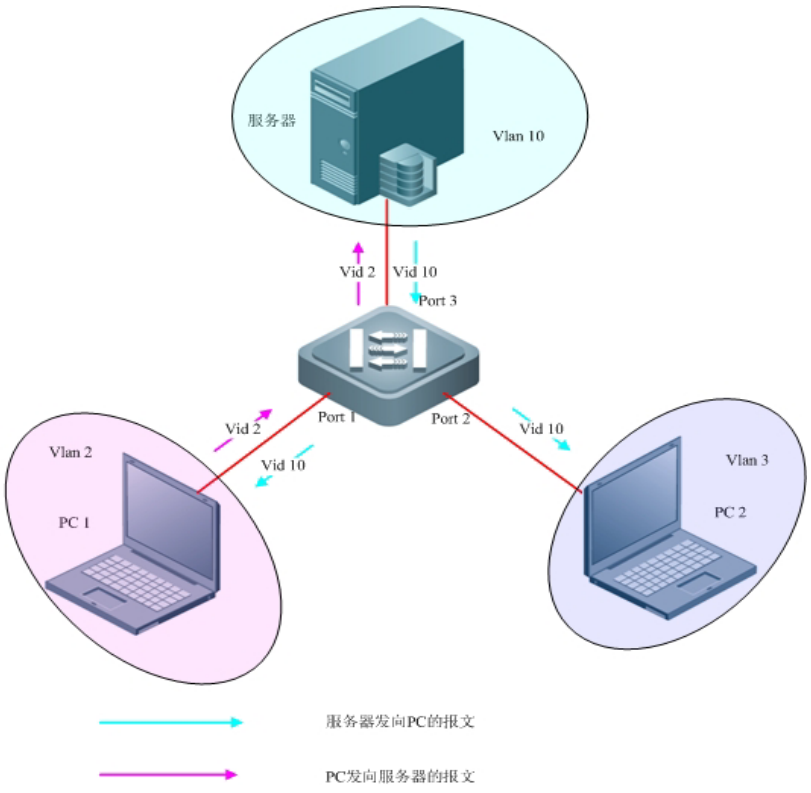
9.1 概述

SHARE VLAN 是一种共享地址的 VLAN，它可以解决交换机在一个 VLAN 上学习到一个 MAC 地址，但以这个地址为目的地址的报文在另一个 VLAN 内传输时会广播的问题。如果一个 VLAN 被配置成 SHARE VLAN，那么它会把自己学习到的动态 MAC 地址和静态 MAC 地址复制到其它存在的 VLAN，并且其它 VLAN 学习到的动态 MAC 地址和静态 MAC 地址也会复制一份到 SHARE VLAN。我们称地址复制过程中引发复制的地址为母地址，被复制出来的地址为子地址。子地址不会再引发复制。当母地址被删除或老化时，子地址也一同被删除或老化，但子地址的删除不会影响到母地址。

9.2 应用模型

报文是通过查找地址表进行转发的，如果地址表中没有报文的目的地址，则报文会在 VLAN 内广播。如图所示：

图 9-1



PC1 发往服务器的报文的 VID 为 2，这时交换机会学习到 PC1 的地址，如下表所示：

Vlan	MAC	Address Type	Interface
2	PC1-MAC	DYNAMIC	Port 1

假设服务器所有的应答报文都在 VLAN 10 中。由于交换机学到 PC1 的 MAC 地址的 VID 为 2，所以当服务器的 VID 为 10 的应答报文到交换机时，交换机找不到这个地址，所以会广播，那么 PC2 也就会收到服务器发到 PC1 的报文，这个报文对

于 PC2 来说是无用的，这样既浪费了带宽，也浪费了 PC2 的资源。那怎么样避免这个问题呢？网络管理员可以把 VLAN 10 设置为 SHARE VLAN，这样当交换机在学习到 VID 为 2 的地址时会复制这个地址到 VLAN 10，如表 2 所示：

Vlan	MAC	Address Type	Interface
2	PC1-MAC	DYNAMIC	Port 1
10	PC1-MAC	DYNAMIC	Port 1

这时服务器的应答报文到交换机后，交换机可以找到 VID 为 10 的地址，则只从 port 1 发出，也就不会广播了。

- 每台交换机只支持一个 SHARE VLAN。
- 只支持复制动态 MAC 地址和静态 MAC 地址。
- 如果交换机上已配置了 PROTLCOL VLAN、REMOTE VLAN 或接口地址表复制功能，那交换机上不能再配置 SHARE VLAN，反之亦然。
- 子地址一旦被删除，则它在母地址老化或被删除后再重新学习到时才会重新复制。
- 当 MAC 地址表资源不足时，MAC 地址会复制失败。当复制失败时，如果母地址是动态地址，则母地址和已复制成功的子地址都会被删除；如果母地址是静态地址，则只删除已复制成功的子地址。

9.3 配置SHARE VLAN

配置 SHARE VLAN：

命令	作用
Ruijie(config-vlan)# **share**	激活 SHARE VLAN
Ruijie(config-vlan)# **no share**	取消 SHARE VLAN

示例：

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# vlan 10
Ruijie(config-vlan)# share
Ruijie(config)# end
```

9.4 显示SHARE VLAN

查看 SHARE VLAN：

命令	作用
Ruijie(config-vlan)#**show mac-address-table share**	查看 MAC 地址状态
Ruijie# show vlan	查看 SHARE VLAN

示例：

查看 SHARE VLAN:

```
Ruijie#show vlan
```

```
VLAN  Name       Status     Ports
----  --------  -------  --- --------------------------------
   1   VLAN0001  STATIC    Gi0/1, Gi0/2, Gi0/3, Gi0/4
                           Gi0/5, Gi0/6, Gi0/7, Gi0/8
                           Gi0/9, Gi0/10, Gi0/11, Gi0/12
                           Gi0/13, Gi0/14, Gi0/15, Gi0/16
                           Gi0/17, Gi0/18, Gi0/19, Gi0/20
                           Gi0/21, Gi0/22, Gi0/23, Gi0/24
   2   VLAN0002  STATIC    Gi0/1
   4   VLAN0004  STATIC    Gi0/2
10   VLAN0010  SHARE     Gi0/1
```

查看 MAC 地址状态：

```
Ruijie# show mac-address-table share
Vlan  MAC Address     Type     Interface               Status
----  --------------- -------  ------------------- ----------
   2   0040.4650.1e1e DYNAMIC GigabitEthernet 0/1 original
  10   0040.4650.1e1e DYNAMIC GigabitEthernet 0/1 duplicated
```

9.5 SHARE VLAN典型配置用例

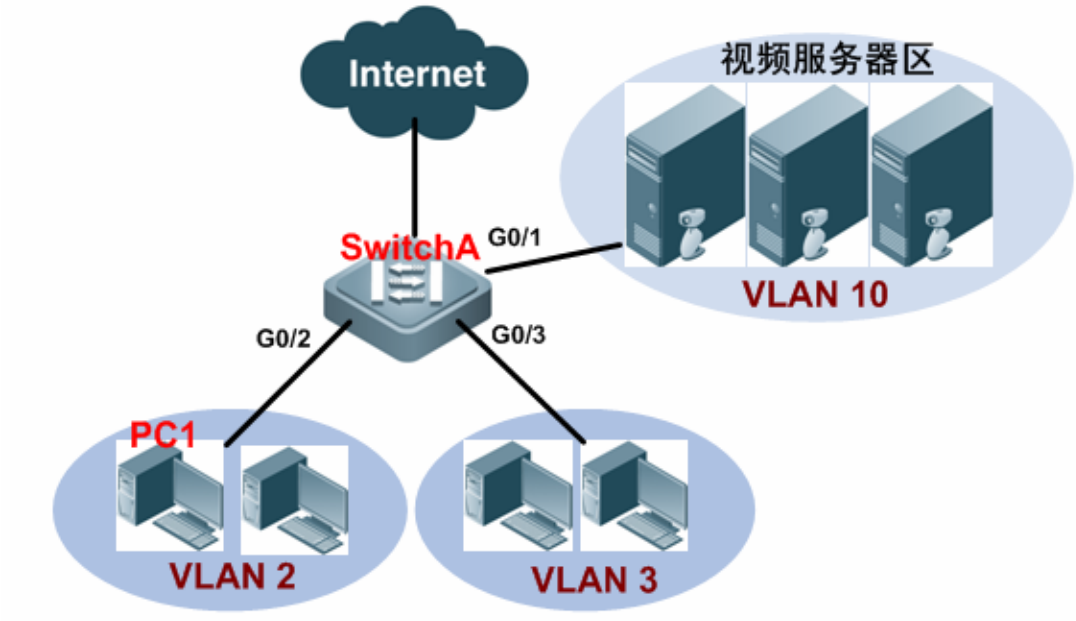
9.5.1 SHARE VLAN的视频点播应用

组网需求

在某办公网的应用环境中，SwitchA 下联所属的 VLAN 2 内的一个 PC 用户(PC1)进行视频点播。要求通过配置使得 VLAN2 内的用户访问视频服务器（属于 VLAN10）时，能够确保 VLAN 3 内的接入用户不受影响，确保其网络资源不被浪费（即 VLAN 3 内的用户不收到来自视频服务器发回的应答报文)。

组网拓扑

图 9-2 SHARE VLAN 的视频点播应用



配置要点

为满足需求，需要在 SwitchA 设备上将 VLAN 10 配置为 SHARE VLAN。分析如下：

PC1 用户进行视频点播，视频服务器在进行数据请求之后进行回包，数据在到达 SwitchA 时，交换机会根据其 PVID 值打上 VLAN 10 TAG。

在 SwitchA 上将 VLAN 10 配置为 SHARE VLAN，交换机学习到的地址为：

Vlan	MAC	Address Type	Interface
2	PC1-MAC	DYNAMIC	G0/2
10	PC1-MAC	DYNAMIC	G0/2

报文就会通过 G0/2 直接送到 PC1，其它用户不会收到这个应答报文。

配置步骤

1、配置 SwitchA 的 G0/2 为 hybrid 口（默认 VLAN 为 2，允许的 UNTAG VLAN 为 VLAN 2 和 VLAN10），G0/3 为 hybrid 口（默认 VLAN 为 3，允许的 UNTAG VLAN 为 VLAN 3 和 VLAN10），G0/1 为 hybrid 口（默认 VLAN 为 2，允许的 UNTAG VLAN 为所有 VLAN）。

```
Ruijie(config)#interface gigabitEthernet 0/2
Ruijie(config-GigabitEthernet 0/2)#switchport mode hybrid
Ruijie(config-GigabitEthernet 0/2)#switchport hybrid native vlan 2
Ruijie(config-GigabitEthernet 0/2)#switchport hybrid allowed vlan untagged 2,10
Ruijie(config)#interface gigabitEthernet 0/3
Ruijie(config-GigabitEthernet 0/3)#switchport mode hybrid
Ruijie(config-GigabitEthernet 0/3)#switchport hybrid native vlan 3
Ruijie(config-GigabitEthernet 0/2)#switchport hybrid allowed vlan untagged 3,10
Ruijie(config-GigabitEthernet 0/1)#switchport mode hybrid
```

```
Ruijie(config-GigabitEthernet 0/1)#switchport hybrid native vlan 10
Ruijie(config-GigabitEthernet 0/1)#switchport hybrid allowed vlan untagged 1-4094
```

2、在 SwitchA 上将 VLAN 10 配置成 SHARE VLAN：

```
Ruijie(config)#vlan 10
Ruijie(config-vlan)#share
```

显示验证

第一步：PC1（假设 IP 地址为 192.168.12.4）ping 服务器（假设 IP 地址为 192.168.12.6），结果可以 ping 通。

第二步，在 SwitchA 上查看 SHARE VLAN 信息：

```
Ruijie(config-vlan)#show vlan
VLAN  Name       Status     Ports
----  --------  -------  --- --------------------------------
   1   VLAN0001  STATIC    Gi0/1, Gi0/2, Gi0/3, Gi0/4
                           Gi0/5, Gi0/6, Gi0/7, Gi0/8
                           Gi0/9, Gi0/10, Gi0/11, Gi0/12
                           Gi0/13, Gi0/14, Gi0/15, Gi0/16
                           Gi0/17, Gi0/18, Gi0/19, Gi0/20
                           Gi0/21, Gi0/22, Gi0/23, Gi0/24
   2   VLAN0002  STATIC    Gi0/1, Gi0/2, Gi0/3
   3   VLAN0003  STATIC    Gi0/1, Gi0/2, Gi0/3
10  VLAN0010  SHARE     Gi0/1, Gi0/2, Gi0/3
```

第三步：在 SwitchA 上查看 MAC 地址状态（只显示端口 2 的信息，其他端口省略）：

```
Ruijie(config)#show mac-address-table share
Vlan  MAC Address     Type     Interface               Status
----  --------------- -------  ------------------- ----------
   2   00d0.f864.6909 DYNAMIC GigabitEthernet 0/2 original
  10   00d0.f864.6909 DYNAMIC GigabitEthernet 0/2 duplicated
```

10 Voice VLAN

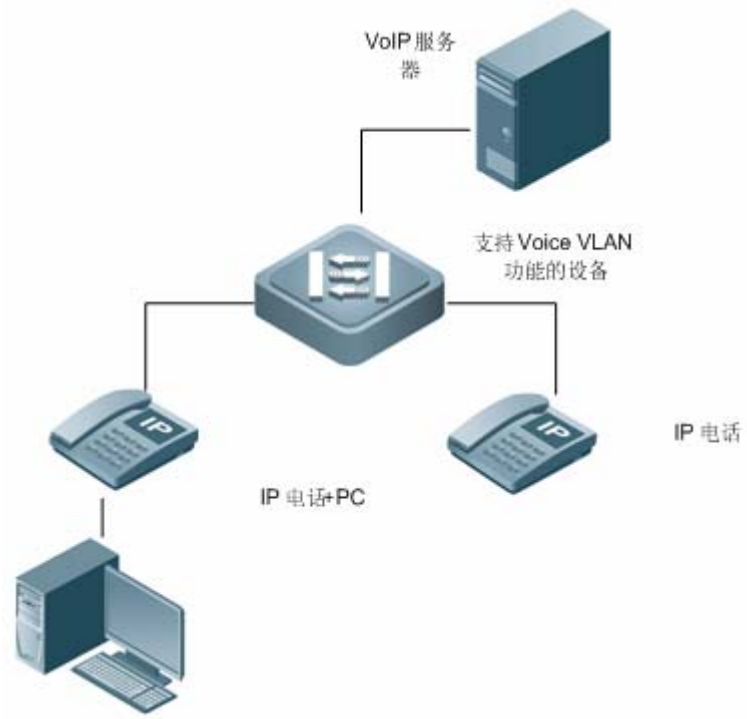
10.1 Voice VLAN概述

随着技术的日益发展，IP 电话应用越来越广泛。IP 电话可以将语音模拟信号转换成数字信号，通过 IP 网络传送到接收端，接收端收集数据包后语音解码得到模拟话音，配合其他语音设备向用户提供大容量、低费用的语音通信解决方案。

Voice VLAN 是为用户的语音数据流专门划分的 VLAN。用户通过创建 Voice VLAN 并将连接语音设备的端口加入 Voice VLAN，可以使语音数据集中在 Voice VLAN 中进行传输，并对语音流进行有针对性的 QoS（Quality of Service，服务质量）配置，提高语音流量的传输优先级，保证通话质量。

Voice VLAN 的基本组网如下图所示：

图 10-1 Voice VLAN 基本组网图



IP 电话和 Voice VLAN 的连接常用的有 2 种（参见上图）：

1. IP 电话单独接入 Voice VLAN 中，该链路中只有一条语音流。这类链接一般用于会议室部署 IP 电话，或无需用到 PC 进行数据业的场合。

2. PC 和 IP 电话组成菊花链接入网络。该链路中同时有语音流和数据流。此时，语音流和数据流分别在 Voice VLAN 和数据 VLAN 中，保证其互不干扰。一般办公人员需使用 PC 进行数据业务通信，同时也需通过 IP 电话进行语音通信时采用该种链接。

基本组网图中的各角色定义如下：

角色	作用
VoIP 服务器	通常 VoIP 应用中所需的服务器组（可以是 1 台承载多种应用服务的服务器，也可是多台提供不同服务的服务器），可能是 Call Agent、DHCP server（给 IP 电话自动分配 IP 地址、Voice VLAN ID 等信息）、录音服务器，等等。
互连设备	提供 Voice VLAN 功能的设备
用户终端设备	IP 电话与用户办公 PC

支持 Voice VLAN 功能的设备可以根据进入端口的数据报文中的源 MAC 地址字段，判断该数据流是否为指定语音设备的语音数据流，源 MAC 地址符合系统设置的语音设备 OUI（Organizationally Unique Identifier，全球统一标识符）地址的报文被认为是语音数据流，被划分到 Voice VLAN 中传输。

OUI 地址为 MAC 地址的前 24 位，是 IEEE（Institute of Electrical and Electronics Engineers，电气和电子工程师学会）为不同设备供应商分配的一个全球唯一的标识符，从 OUI 地址可以判断出该设备是哪一个厂商的产品。

10.1.1 Voice VLAN基本概念

10.1.1.1 Voice VLAN的自动模式与手动模式

Voice VLAN 中的端口可工作在 Voice VLAN 的自动模式或手动模式，在不同的工作模式下端口加入 Voice VLAN 的方式不同。

自动模式

当用户 IP 电话启动时，所发出的协议报文经支持 Voice VLAN 的设备时，设备通过识别该报文的源 MAC，匹配交换机上所配置的 Voice VLAN 的 OUI 地址。OUI 地址匹配成功后，设备自动将该语音报文的输入端口添加到 Voice VLAN，并下发策略，将语音报文的优先级修改为设备上所配置的 Voice VLAN 中语音流的优先级。

同时，用户可在设备上设置 Voice VLAN 的老化时间，当在老化时间内，系统没有从输入端口收到任何语音报文时，系统将把该端口从 Voice VLAN 中删除。端口加入 Voice VLAN 或从 Voice VLAN 中删除的过程由系统自动实现。端口的老化机制可以避免长时间不使用语音设备的端口一直驻留在 Voice VLAN 中。

手动模式

用户手工地在支持 Voice VLAN 的设备上将 IP 电话所连接的端口加入到 Voice VLAN 中。用户 IP 电话通讯过程中，设备通过识别该报文的源 MAC，匹配设备上所配置的 Voice VLAN 的 OUI 地址。OUI 地址匹配成功后，设备自动将该语音报文的输入端口添加到 Voice VLAN，并下发策略，将语音报文的优先级修改为设备上所配置的 Voice VLAN 中语音流的优先级。

手动模式下，端口加入 Voice VLAN 或从 Voice VLAN 中删除的过程由管理员手动进行配置。

对于 IP 电话发出的携带 tag 标签的报文，两种模式处理方式一致，与 VLAN 功能的转发规则相同，根据标签进行转发。

按照是否自动获取 IP 地址与 VLAN 信息来划分，一般来说，IP 电话有 2 种：

自动获取 IP 地址及 Voice VLAN 编号的电话，这类电话可以发送 untagged 或 tagged 的语音流。

手工设置 IP 地址及 Voice VLAN 编号的电话，这类电话只能发送 tagged 语音流。

Voice VLAN 功能支持使用 Access Port、Trunk Port 与 Hybrid Port 传输语音数据，依照连接的 IP 电话类型的不同，需要用户保证端口的类型、Voice VLAN 工作模式与 IP 电话类型能够匹配，具体匹配关系如下表所示：

Voice VLAN 工作模式	语音流类型	端口类型	支持条件
自动模式	Tagged 语音流	Access Port	不支持
		Trunk Port	支持，接入端口的 native VLAN 必须存在且不能是 Voice VLAN，同时该端口允许 native VLAN 通过
		Hybrid Port	支持，接入端口的 native VLAN 必须存在且不能是 Voice VLAN，同时该端口允许 native VLAN 通过
		Uplink 口	支持，接入端口的 native VLAN 必须存在且不能是 Voice VLAN，同时接入端口应允许 native VLAN 的报文通过
	Untagged 语音流	Access Port	不支持
		Trunk Port	不支持
		Hybrid Port	不支持
		Uplink 口	不支持
手动模式	Tagged 语音流	Access Port	不支持
		Trunk Port	支持，接入端口的 native VLAN 必须存在且不能是 Voice VLAN，同时接入端口允许 native VLAN 和 Voice VLAN 的报文通过
		Hybrid Port	支持，接入端口的 native VLAN 必须存在且不能是 Voice VLAN，同时该端口允许 native VLAN 通过，且 Voice VLAN 应在该端口允许通过的 tagged VLAN 列表中
		Uplink 口	支持，接入端口的 native VLAN 必须存在且不能是 Voice VLAN，同时接入端口应允许 native VLAN 和 Voice VLAN 的报文通过
	Untagged 语音流	Access Port	支持，Voice VLAN 须和接入端口所属 VLAN 一致

		Trunk Port	支持，接入端口的 native VLAN 必须是 Voice VLAN，且接入端口允许该 VLAN 通过
		Hybrid Port	支持，接入端口的 native VLAN 必须是 Voice VLAN，且在接入端口允许通过的 untagged VLAN 列表中
		Uplink 口	不支持

- 如果用户的 IP Phone 发出的是 tagged 语音流，且接入的端口上使能了 802.1x 认证和 Guest VLAN 功能，为保证各种功能的正常使用，请为 Voice VLAN、端口的缺省 VLAN 和 802.1x 的 Guest VLAN 分配不同的 VLAN ID。
- 由于 Protocol VLAN 只对 Trunk Port/Hybrid Port 输入的 untagged 报文生效，而 Voice VLAN 自动模式下的 Trunk/Hybrid Port 只能对 tagged 语音流进行处理，因此请不要将某个 VLAN 同时设置为 Protocol VLAN 与 Voice VLAN。
- 在使用自动模式时，请不要将 OUI 地址配置为静态地址，否则会影响自动模式的使用。
- 加入 Voice VLAN 的端口若绑定 IP+MAC 或仅 IP 的安全地址，该安全地址绑定对符合 Voice VLAN OUI 地址的语音流不生效，即不符合绑定但符合 Voice VLAN OUI 地址的语音流不被过滤。
- 配置全局 IP 地址和 MAC 地址绑定，对于加入 Voice VLAN 的端口，该绑定对符合 Voice VLAN OUI 地址的语音流不生效。
- 不支持 Voice VLAN 语音流的 CoS 值设置，输出报文的 COS 值为 DSCP 通过 QoS 映射表映射后的值。

10.1.1.2 Voice VLAN的安全模式

为了能够更好地进行用户语音流与数据流分离传输，Voice VLAN 提供安全模式功能。安全模式打开时，Voice VLAN 只允许传输语音流，设备会对报文的源 MAC 地址进行检查，当报文源 MAC 地址是可识别的 Voice VLAN OUI 地址时，允许该报文在 Voice VLAN 内传输，否则将该报文丢弃。安全模式关闭时，不对报文的源 MAC 地址进行检查，所有报文均可在 Voice VLAN 内进行传输。

- 安全模式下，仅对 untagged 报文及带有 Voice VLAN tag 的报文进行源 MAC 地址检查，对于带有其它非 Voice VLAN tag 的报文，设备按照 VLAN 规则对报文进行转发和丢弃的处理，不受 Voice VLAN 安全/普通模式的影响。
- 建议用户尽量不要在 Voice VLAN 中同时传输语音和业务数据。若的确有此需要，请确认 Voice VLAN 的安全模式已关闭。

10.2 Voice VLAN工作原理

支持 Voice VLAN 功能的设备，通过将数据流和语音流分别限制在数据 VLAN 和 Voice VLAN 中，从而保证语音通话与业务报文互不影响。同时下发优先级策略提高语音流的优先级，保证通话质量。其基本工作方式如下所述：

第一步，由用户在设备上创建 1 个专用传输语音报文的 VLAN，即 Voice VLAN，并使能连接 IP 电话的端口的 Voice VLAN 功能。

第二步，连接 IP 电话的端口加入 Voice VLAN，这是关键的一步。加入的方式视 Voice VLAN 的工作模式为自动模式或手动模式而有所不同，具体如下：

自动模式下，当设备从该端口收到一个 untagged 报文以后，会将其源 MAC 地址和合法 OUI 地址相匹配。如果该源 MAC 为 OUI 地址，即认为该报文为语音报文。设备将该端口自动加入到 Voice VLAN 中，同时在该端口上学习这个 MAC 地址。

手动模式下，由用户手动配置连接 IP 电话的端口加入到 Voice VLAN。

第三步，无论是自动模式还是手动模式，当端口加入 Voice VLAN 时，设备会下发策略，提高所有通过 Voice VLAN 的源 MAC 匹配该 OUI 的报文的优先级。将能够匹配该 OUI 地址的语音报文的优先级设置为 cos=6，dscp=46。

经过上述步骤后，连接 IP 电话的端口加入到专用的 Voice VLAN 中，语音报文在 Voice VLAN 中集中传输，同时语音报文以高优先级从设备中转发出去。

如果 IP 电话支持 LLDP 协议，则用户无需配置 OUI，设备可以通过捕捉 IP 电话发出的 LLDP 协议，对协议报文中的设备能力字段进行识别，对于标识其能力为“telephone”的设备识别为语音设备，将协议报文中的源 MAC 提取出来作为语音设备 MAC 进行处理，从而实现语音设备的自动识别。

LLDP 的配置方法请参见《LLDP》章节。

10.3 配置Voice VLAN基本特性

以下章节描述如何配置 Voice VLAN 的基本特性：

- （必选）使能 Voice VLAN 功能
- （必选）使能端口 Voice VLAN 功能
- （可选）配置端口的 Voice VLAN 工作模式
- （可选）配置 Voice VLAN 老化时间
- （可选）配置 Voice VLAN OUI 地址
- （可选）配置 Voice VLAN 的安全模式
- （可选）配置 Voice VLAN 的语音流优先级
- 查看 Voice VLAN 配置和状态

10.3.1 缺省配置

下表用来描述 Voice VLAN 的缺省配置。

功能特性	缺省值
Voice VLAN 使能状态	Disable，Voice VLAN 功能关闭
Voice VLAN 安全模式	打开
Voice VLAN 老化时间	1 天（1440 分钟），仅在自动模式下有效

Voice VLAN CoS	6
Voice VLAN DSCP	46
端口的 Voice VLAN 使能状态	关闭
端口的 Voice VLAN 工作模式	自动模式

10.3.2 使能Voice VLAN功能

缺省情况下，Voice VLAN 功能关闭，进入特权模式，按以下步骤开启 Voice VLAN 功能：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **vlan** *vlan-id*	创建 Voice VLAN。
Ruijie(config-vlan)# **exit**	退出 VLAN 配置模式。
Ruijie(config)# **voice vlan** *vlan-id*	使能 Voice VLAN，设置一个 VLAN 为 Voice VLAN。

如果要关闭 Voice VLAN 功能，可用 **no voice vlan** 全局配置命令进行设置。

配置举例：

全局使能 Voice VLAN 功能，并设置 VLAN 2 为 Voice VLAN。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# vlan 2
Ruijie(config-vlan)# exit
Ruijie(config)# voice vlan 2
```

当端口同时打开 802.1x 与 Voice VLAN 功能时，符合 Voice VLAN OUI 设置的 IP 电话无需认证即可使用 Voice VLAN 通信。譬如在同一个端口上接入 PC 和 IP 电话，打开 802.1x 认证功能后，PC 使用网络需进行 1x 认证，而 IP 电话不受影响。

配置 Voice VLAN 之前，须先创建对应的 VLAN。

VLAN 1 是默认 VLAN，无需创建，但 VLAN 1 不能被设置为 Voice VLAN。

如果接入的端口上开启了 802.1x VLAN 自动跳转功能，为保证功能的正常使用，请不要将下发的 VID 设置为 Voice VLAN ID。

不要将 RSPAN 的 Remote VLAN 与 Voice VLAN 配置成同 1 个 VLAN，否则可能会影响远程端口镜像功能与 Voice VLAN 功能。

10.3.3 使能端口Voice VLAN功能

缺省情况下端口的 Voice VLAN 功能关闭，进入特权模式，按以下步骤开启端口的 Voice VLAN 功能：

命令	作用

Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **interface** *interface-name*	进入端口的配置模式，可使能 Voice VLAN 的端口为物理端口。
Ruijie(config-if)# **voice vlan enable**	使能端口的 Voice VLAN 功能。 缺省情况下端口的 Voice VLAN 功能关闭。

如果要关闭端口的 Voice VLAN 功能，可用 **no voice vlan enable** 命令进行设置。

配置举例：

打开端口 FastEthernet 0/1 的 Voice VLAN 功能，并显示当前 Voice VLAN 正在工作中的端口

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# voice vlan enable
```

在全局 Voice VLAN 关闭的情况下，也允许使能端口的 Voice VLAN 功能，但不生效。

Voice VLAN 仅支持二层物理口（Access Port/Trunk Port/Hybrid Port/Uplink Port 端口等），不支持在 AP 口与 Routed Port 上打开 Voice VLAN 功能。

端口使能了 Voice VLAN 功能后，为保证功能运行正常，请不要切换端口的二层模式（Access Port/Trunk Port/Hybrid Port 等）。若需切换，请先关闭端口的 Voice VLAN 功能。

10.3.4 配置端口的Voice VLAN工作模式

Voice VLAN 的工作模式分为自动模式与手动模式,基于端口配置,关于自动模式与手动模式的概念请参见 Voice VLAN 的自动模式与手动模式部分说明。

缺省情况下，端口的 Voice VLAN 工作模式为自动模式，进入特权模式按以下步骤开启端口的 Voice VLAN 功能：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **interface** *interface-name*	进入端口的配置模式。
Ruijie(config-if)# **voice vlan mode auto**	设置端口的 Voice VLAN 模式为自动模式。 缺省情况下，Voice VLAN 工作在自动模式。 各个端口 Voice VLAN 的工作模式相互独立，不同的端口可以设置为不同的模式。

如果要设置端口的工作模式为手动模式，则使用 **no voice vlan mode auto** 命令进行设置。

配置举例：

设置端口 FastEthernet 0/1 的 Voice VLAN 模式为自动模式

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

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-vlan)# voice vlan mode auto
```

端口使能了 Voice VLAN 功能后，不允许进行手动模式和自动模式的切换，若需进行模式切换，请先关闭端口的 Voice VLAN 功能。

自动模式下，不允许通过手工配置命令将端口加入 Voice VLAN 或从 Voice VLAN 中删除。

当端口使能了 Voice VLAN 并工作在手工模式时，必须手工将端口加入 Voice VLAN，才能保证 Voice VLAN 功能生效。

当端口工作于自动模式时，为保证功能运行正常，请注意不要将端口的 native VLAN 设置为 Voice VLAN。

锐捷产品 Trunk Port/Hybrid Port 缺省可以传输所有 VLAN 的报文，请先将 Voice VLAN 从端口的 VLAN 许可列表中移出，再打开 Voice VLAN 功能，以保证未连接语音设备的端口不会加入 Voice VLAN，或长时间不使用的端口一直驻留在 Voice VLAN 中。

10.3.5 配置Voice VLAN老化时间

用户可在设备上设置 Voice VLAN 的老化时间，当在老化时间内，设备没有从输入端口收到任何语音报文时，将把该端口从 Voice VLAN 中删除。老化时间仅对自动模式生效。

进入特权模式，按以下步骤配置老化时间：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **voice vlan aging** *minutes*	配置 Voice VLAN 的老化时间，取值范围为 5-10000 分钟，缺省为 1440 分钟。

如果要将老化时间恢复到缺省值，可用 **no voice vlan aging** 全局配置命令进行设置。

配置举例：

设置 Voice VLAN 老化时间为 10 分钟

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# voice vlan aging 10
```

10.3.6 配置Voice VLAN OUI地址

锐捷产品提供 Voice VLAN 可识别的 OUI 地址设置，OUI 地址的说明请参见 Voice VLAN 概述部分。支持 Voice VLAN 功能的设备通过识别输入报文的源 MAC，是否匹配设备上所配置的 Voice VLAN 的 OUI 地址，来判断该数据流是否为指定语音设备的语音数据流。

进入特权模式，按以下步骤配置 Voice VLAN OUI 地址：

命令	作用

Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **voice vlan mac-address** *mac-addr* **mask** *oui-mask* [**description** *text*]	配置设备可识别的 Voice VLAN OUI 地址
Ruijie(config)# **show voice vlan oui**	查看 Voice VLAN OUI 地址

如果要删除设备上设置的某个 OUI 地址，可用 **no voice vlan mac-address** *oui* 全局配置命令进行设置。

配置举例：

设置 OUI 地址 0012.3400.0000 为 Voice VLAN 的合法地址，厂商为 Company A

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# voice vlan mac-address 0012.3400.0000 mask ffff.ff00.0000 description Company A
Ruijie(config)# show voice vlan oui
Oui Address     Mask              Description
0012.3400.0000  ffff.ff00.0000  Company A
```

10.3.7 配置Voice VLAN的安全模式

为了更好地进行用户语音流与数据流分离传输，锐捷产品的 Voice VLAN 提供安全模式功能，安全模式打开时 Voice VLAN 内只允许传输语音流，更好地保证语音流传输质量

进入特权模式，按以下步骤配置 Voice VLAN 的安全模式：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **voice vlan security enable**	打开 Voice VLAN 的安全模式。 缺省情况下，Voice VLAN 的安全模式打开。

如果要关闭 Voice VLAN 的安全模式，可用 **no voice vlan security enable** 全局配置命令进行设置。

配置举例：

打开 Voice VLAN 的安全模式

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# voice vlan security enable
```

10.3.8 配置Voice VLAN的语音流优先级

设备通过修改 Voice VLAN 的语音流的 DSCP 值来提高语音流的优先级，保证通话质量。关于 DSCP 的概念，请参见 QoS 配置章节的说明。

进入特权模式，按以下步骤配置 Voice VLAN 的语音流优先级：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **voice vlan dscp** *dscp-value*	设置 Voice VLAN 语音流的 DSCP 值。 缺省情况下，DSCP 为 46。

如果要将 DSCP 值恢复为缺省值，可使用 **no voice vlan dscp** 全局配置命令进行设置。

配置举例：

配置 Voice VLAN 的语音流优先级，DSCP 为 40。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# voice vlan dscp 40
```

Voice VLAN 所配置的 DSCP 值与 802.1x 功能下发的 DSCP 属性冲突时，以 Voice VLAN 配置的 DSCP 值生效。

10.3.9 查看Voice VLAN配置和状态

Voice VLAN 提供了如下的显示命令用于查看各种配置信息及运行时信息，各命令的功能说明如下：

命令	作用
show voice vlan	显示 Voice VLAN 的配置信息与当前状态，包括使能 Voice VLAN 功能的端口的工作模式。
show voice vlan oui	显示当前设备支持的 OUI 地址、OUI 地址掩码和描述信息。
show vlan	显示当前 Voice VLAN 正在工作中的端口，同普通 VLAN 的显示命令。

10.4 Voice VLAN典型配置举例

10.4.1 Voice VLAN自动模式配置举例

组网需求

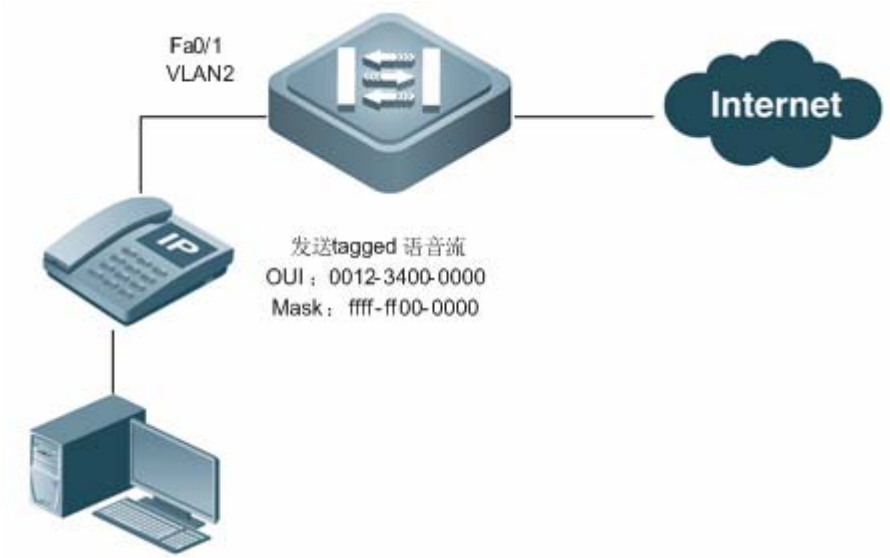
假设 Voice VLAN 自动模式配置有以下需求：

- 创建 VLAN2 为 Voice VLAN。
- Voice VLAN 老化时间为 1000 分钟。
- IP 电话 MAC 地址为 0012.3456.7890，发送 tagged 语音流，接入端口是 Trunk 类型端口 Fa0/1（此处为示例说明，在使用 Voice VLAN 功能时请参见 Voice VLAN 的自动模式与手动模式章节中的端口模式与 IP 电话语音流类型匹配关系表），端口的 native VLAN 为 VLAN 5。
- 设备允许 OUI 地址为 0012.3400.0000，掩码是 ffff.ff00.0000 的语音报文通过 Voice VLAN 转发。

- 接入端口 Fa0/1 下连的 PC 需要使用 802.1x 认证。

组网拓扑

图 10-2 Voice VLAN 自动模式配置组网图



配置要点

依据组网需求，设备的 Voice VLAN 配置需要注意：由于 Fa0/1 下连的是发送 tagged 语音流，且为 Trunk Port，Voice VLAN 模式为自动模式，依据匹配关系要求，Fa0/1 的 native VLAN 必须存在且不能是 Voice VLAN，同时该端口允许 native VLAN 通过。

组网需求中 Fa0/1 的 native VLAN 为 5，非 Voice VLAN（VLAN2），可满足上述要求。同时由于 Trunk Port 缺省包含所有 VLAN，为更好地使用自动模式，使不连接语音设备的端口不加入 Voice VLAN，需要先将 Voice VLAN（VLAN5）从 Fa0/1 的 VLAN 许可列表中移出。

配置步骤

1）创建 VLAN2 为 Voice VLAN

#创建 VLAN2，使能 VLAN2 的 Voice VLAN 功能

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# vlan 2
Ruijie(config-vlan)# exit
Ruijie(config)# voice vlan 2
```

2）Voice VLAN 老化时间为 1000 分钟

设置 Voice VLAN 的老化时间

```
Ruijie(config)# voice vlan aging 1000
```

3）设备允许 OUI 地址为 0012.3400.0000，掩码是 ffff.ff00.0000 的语音报文通过 Voice VLAN 转发。

设置 Voice VLAN OUI 地址

```
Ruijie(config)# voice vlan mac-address 0012.3400.0000 mask ffff.ff00.0000
```

4）接入端口是 Trunk 类型端口 Fa0/1，端口的 native VLAN 为 VLAN 5。

设置 Fa0/1 为 Trunk Port

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# switchport mode trunk
```

设置 Fa0/1 的 native VLAN 为 VLAN5

```
Ruijie(config-if)# switchport trunk native vlan 5
```

将 Voice VLAN 从加入 Fa0/1 的 VLAN 列表中移出

```
Ruijie(config-if)# switchport trunk allowed vlan remove 2
```

使能 Fa0/1 的 Voice VLAN 功能

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# voice vlan enable
```

5）若接入端口需同时打开 802.1x 功能，则需做如下配置。

802.1x 功能的设置 Fa0/1 为 802.1x 受控口

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# dot1x port-control auto
```

其余 802.1x 功能的配置方法，请参见 802.1x 配置章节

显示验证

查看设备当前的 Voice VLAN 状态

```
Ruijie(config)# show voice vlan
Voice Vlan status: ENABLE             // 全局 Voice VLAN 使能
Voice Vlan ID        : 2                // Voice VLAN ID 为 2
Voice Vlan security mode: Security  // 全局安全模式打开
Voice Vlan aging time: 1440minutes
Voice Vlan cos       : 6
Voice Vlan dscp      : 46
Current voice vlan enabled port mode:
PORT                 MODE
-------------------- ----------
```

```
Fa0/1                AUTO             // Fa0/1 使能 Voice VLAN，为自动模式
# 查看设备的 Voice VLAN OUI 地址
Ruijie(config)# show voice vlan oui
Oui Address     Mask              Description        Status
0012.3400.0000  ffff.ff00.0000                       static
```

10.4.2 Voice VLAN手动模式配置举例

组网需求

1）创建 VLAN2 为 Voice VLAN。

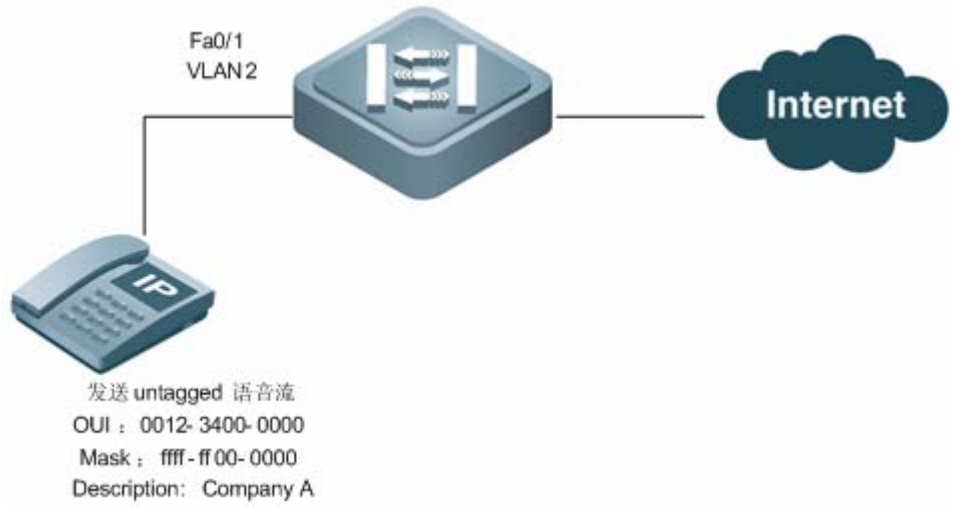
2）IP 电话 MAC 地址为 0012.3456.7890，发送 untagged 语音流，接入端口是 Hybrid 类型端口 Fa0/1。

3）Fa0/1 工作在手动模式。

4)设备允许 OUI 地址为 0012.3400.0000,掩码是 ffff.ff00.0000 的语音报文通过 Voice VLAN 转发,描述符为 Company A。

组网拓扑

图 10-3 Voice VLAN 手动模式配置组网图



配置要点

依据组网需求,设备的 Voice VLAN 配置需要注意:由于 Fa0/1 下连的是发送 untagged 语音流,且 Fa0/1 为 Hybrid Port，Voice VLAN 模式为手动模式，依据匹配关系要求，Fa0/1 的 native VLAN 必须是 Voice VLAN，且 Voice VLAN 须在端口的允许通过的 untagged VLAN 列表中。因此，组网需求中 Fa0/1 的 native VLAN 应设置为 2（Voice VLAN ID），同时配置时需要将 VLAN2 加入 Fa0/1 允许通过的 untagged VLAN 列表中。

配置步骤

1）创建 VLAN2 为 Voice VLAN

#创建 VLAN2，使能 VLAN2 的 Voice VLAN 功能

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# vlan 2
Ruijie(config-vlan)# exit
Ruijie(config)# voice vlan 2
```

2)设备允许 OUI 地址为 0012.3400.0000,掩码是 ffff.ff00.0000 的语音报文通过 Voice VLAN 转发,描述符为 Company A。

设置 Voice VLAN OUI 地址

```
Ruijie(config)# voice vlan mac-address 0012.3400.0000 mask ffff.ff00.0000 description Company A
```

3）接入端口是 Hybrid 类型端口 Fa0/1，端口的 native VLAN 为 VLAN 2

设置 Fa0/1 为 Hybrid Port

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# switchport mode hybrid
```

设置 Voice VLAN 为 Fa0/1 的 native VLAN

```
Ruijie(config-if)# switchport hybrid native vlan 2
```

将 Voice VLAN（即 VLAN2）加入 Fa0/1 的 untagged 列表

```
Ruijie(config-if)# switchport hybrid allowed vlan add untagged 2
```

使能 Fa0/1 的 Voice VLAN 功能

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# voice vlan enable
```

显示验证

查看设备当前的 Voice VLAN 状态

```
Ruijie(config)# show voice vlan
Voice Vlan status: ENABLE             // 全局 Voice VLAN 使能
Voice Vlan ID        : 2                // Voice VLAN ID 为 2
Voice Vlan security mode: Security  // 全局安全模式打开
Voice Vlan aging time: 1440minutes
Voice Vlan cos       : 6
Voice Vlan dscp      : 46
Current voice vlan enabled port mode:
PORT                 MODE
```

```
------------------- ----------
Fa0/1                MANUAL             // Fa0/1 使能 Voice VLAN，为手动模式
```

查看设备的 Voice VLAN OUI 地址

```
Ruijie(config)# show voice vlan oui
Oui Address     Mask              Description       Status
0012.3400.0000  ffff.ff00.0000  Company A         static
```

11 MAC VLAN

11.1 MAC VLAN 概述

随着移动办公的普及，终端设备不再通过固定端口接入设备，它可能本次使用端口 A 接入网络，下次使用端口 B 接入网络。如果端口 A 和端口 B 的 VLAN 配置不同，则终端设备第二次接入后就会被划分到不同 VLAN，导致无法使用原 VLAN 内的资源；如果端口 A 和端口 B 的 VLAN 配置相同，当端口 B 被分配给别的终端设备时，又会引入安全问题。如何在同一端口下，允许不同 VLAN 的主机自由接入呢？MAC VLAN 功能由此产生。

MAC VLAN 就是基于 MAC 地址划分的 VLAN，是一种新的 VLAN 划分方法。该功能通常会和 802.1X 下发 VLAN 功能结合使用，以实现 802.1X 终端的安全、灵活接入。当 802.1X 用户通过认证后，根据认证服务器下发的 VLAN 和用户 MAC 地址，由交换机自动生成 MAC VLAN 表项。网络管理员也可以预先在交换机上配置 MAC 地址和 VLAN 的关联关系。

MAC VLAN 的最大优点就是当用户物理位置发生移动时，即从一台交换机换到其它的交换机时，不需要重新配置用户所在端口的 VLAN。所以，可以认为这种根据 MAC 地址的 VLAN 划分方法是基于用户的 VLAN。

11.2 工作原理

当交换机收到报文时，将数据流的源 MAC 与 MAC VLAN 表项中指定的 MAC 地址进行匹配。如果匹配成功，则将该报文转发到 MAC VLAN 表项指定的 VLAN 中；如果匹配失败，则该数据流所属的 VLAN 仍然由端口的 VLAN 规则决定。

为了实现 PC 从任意交换机接入时，都会被划分到指定的 VLAN，可以通过如下二种方式进行配置：

- 通过命令行静态配置。用户通过命令行在本地交换机设备上配置 MAC 地址和 VLAN 的关联关系。
- 通过认证服务器来自动配置（802.1X VLAN 下发功能）。当用户认证通过后，交换机根据认证服务器提供的信息，动态创建 MAC 地址和 VLAN 的关联关系。用户下线时，交换机将自动删除该对应关系。该方式需要在认证服务器上配置 MAC 地址和 VLAN 的关联，有关“802.1X VLAN 下发功能”的详细介绍请参见“802.1X 配置”。

MAC VLAN 表项可以同时支持两种配置方式，即在本地设备和认证服务器上都进行了配置，但是这两种配置必须一致配置才能生效；如果不一致的话，则先执行的配置生效。

基于 MAC 的 VLAN 功能只能在 HYBRID 端口上配置；

MAC VLAN 表项仅针对 UNTAG 的报文生效，对携带 TAG 的报文不生效；

静态配置或动态生成 MAC VLAN 表项时，指定 VLAN 必需已经存在；

MAC VLAN 表项中指定的 VLAN 不能是 Super VLAN(可以是 Sub VLAN)、Remote VLAN、Primary VLAN（可以是 Secondary VLAN）；

如果指定 VLAN 已经存在相应的 MAC VLAN 表项，该 VLAN 不能被删除；该 VLAN 关联的所有 MAC VLAN 表项被删除后（包括静态配置和动态生成的 MAC VLAN 表项），才可以删除指定 VLAN；

MAC VLAN 表项中指定的 MAC 地址必须是单播地址；

MAC VLAN 表项对所有开启 MAC VLAN 功能的 HYBRID 端口生效；

11.3 配置 MAC VLAN

MAC VLAN 容量相关配置，参见《硬件表项容量》文档“配置共享池最大数目”章节。

以下章节描述如何配置 MAC VLAN 的基本特性：

- MAC VLAN 的缺省配置
- (必选)配置基于端口的 MAC VLAN 开关
- (可选)全局添加/删除 MAC VLAN 表项

11.3.1 MAC VLAN的缺省配置

下表用来描述 MAC VLAN 的缺省配置。

功能特性	缺省值
基于端口的开关	关闭
全局添加/删除静态 MAC VLAN 表项	不存在

11.3.2 基于端口开启/关闭MAC VLAN

缺省情况下，基于端口的 MAC VLAN 开关处于关闭状态，所有 MAC VLAN 表项均不会在端口上生效。

进入端口配置模式，按以下步骤在端口上开启 MAC VLAN 功能。

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **interface** *interface-id*	进入端口配置模式，首先配置为 hybrid 端口。
Ruijie(config-if)# **mac-vlan enable**	使能端口的 MAC VLAN 功能。
Ruijie(config-if)# **end**	退回到特权模式。
Ruijie# **show mac-vlan interface**	查看已经开启 MAC VLAN 的端口列表

举例如下：

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface fastethernet 0/10
Ruijie(config-if)# mac-vlan enable
Ruijie(config-if)# end
Ruijie# show mac-vlan interface
  MAC VLAN is enabled on following interface:
  ---------------------------------------
  fastethernet 0/10
```

11.3.3 全局添加/删除静态MAC VLAN表项

用户需要在全局模式下配置 MAC 地址和 VLAN 的关联关系。可选配置 802.1p 优先级，默认值为 0。

全局模式下按如下步骤配置 MAC VLAN：

命令	作用
Ruijie(config)# **mac-vlan mac-address** *mac-address* [**mask** *mac-mask*] **vlan** *vlan-id* {**priority** *pri_val*}	将 MAC 地址和 VLAN 关联起来，可选指定 MAC 地址掩码和优先级
Ruijie(config)# **no mac-vlan all**	删除所有的静态 MAC VLAN 表项
Ruijie(config)# **no mac-vlan mac-address** *mac-address* [**mask** *mac-mask*]	删除指定 MAC 的静态 MAC VLAN 表项
Ruijie(config)# **no mac-vlan vlan** *vlan-id*	删除指定 VLAN 的静态 MAC VLAN 表项

举例如下：

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# mac-vlan mac-address 0000.0000.0001 vlan 2 priority 3
Ruijie(config)# no mac-vlan mac-address 0000.0000.0001
Ruijie(config)# no mac-vlan vlan 2
Ruijie(config)# no mac-vlan all
Ruijie(config)# end
```

- UNTAG 的报文如果能够匹配 MAC VLAN 表项，由于 MAC VLAN 表项的优先级最高，报文一进入交换机就被修改为 MAC VLAN 表项指定的 VLAN，后续功能和协议都是按照修改后的 VLAN 进行处理。可能造成的影响，举例如下：
- 802.1x 用户认证失败后，Hybrid 端口跳转到 FAIL VLAN 功能指定的 VLAN 100 中，但是静态配置的 MAC VLAN 表项将该用户所有的报文重定向到 VLAN 200 中；导致该用户无法在 FAIL VLAN 100 中正常通讯；
- UNTAG 的报文匹配 MAC VLAN 表项后，触发 MAC 地址学习的 VLAN 是根据 MAC VLAN 表项重定向之后的 VLAN；
- 开启 MAC VLAN 的端口，如果接收报文可以同时匹配掩码不为全 F 和掩码为全 F 的 MAC VLAN 表项，报文处理按照掩码不为全 F 的 MAC VLAN 表项为准；
- UNTAG 的报文同时匹配 MAC VLAN 表项和 VOICE VLAN 表项时，同时修改报文优先级，报文优先级以 VOICE VLAN 为准；
- UNTAG 的报文同时匹配 MAC VLAN 表项和 PROTOCOL VLAN 表项时，报文携带 VLAN 以 MAC VLAN 为准；
- MAC VLAN 只适用于 UNTAG 的报文，对于 PRIORITY 报文（VLAN TAG 为 0，带 COS PRIORITY 信息的报文）不适用，处理行为不确定；
- ☑ 交换机上 QOS 的报文信任模式默认处于关闭状态，这会导致修改所有报文的 PRIORITY 信息为 0，从而覆盖 MAC VLAN 功能对报文 PRIORITY 的修改。可以在端口配置模式下执行：“mls qos trust cos”命令开启 QOS 信任模式，信任报文的 PRIORITY 信息；

11.3.4 查看MAC VLAN配置

查看 MAC VLAN 表项

查看静态配置和动态生成的 MAC VLAN 表项，特权模式下按如下步骤查看：

命令	作用
show mac-vlan all	显示所有的 MAC VLAN 表项，包括静态配置和动态生成的
show mac-vlan dynamic	显示动态生成的 MAC VLAN 表项
show mac-vlan static	显示静态配置的 MAC VLAN 表项
show mac-vlan vlan *vlan-id*	显示指定 VLAN 的 MAC VLAN 表项
show mac-vlan mac-address *mac-address* [**mask** *mac-mask*]	显示指定 MAC 地址的 MAC VLAN 表项

举例如下：

查看所有的 MAC VLAN 表项

```
Ruijie# show mac-vlan all
The following MAC VLAN address exist:
S: Static   D: Dynamic
MAC ADDR           MASK             VLAN ID   PRIO   STATE
-------------------------------------------------------
0000.0000.0001   ffff.ffff.ffff   2         0       D
0000.0000.0002   ffff.ffff.ffff   3         3       S
0000.0000.0003   ffff.ffff.ffff   3         3       S&D
Total MAC VLAN address count: 3
```

查看 MAC VLAN 基于端口的开关

查看 MAC VLAN 基于端口的开关状态，特权模式下按如下步骤查看：

命令	作用
show mac-vlan interface	显示所有端口的 MAC VLAN 开关状态

举例如下：

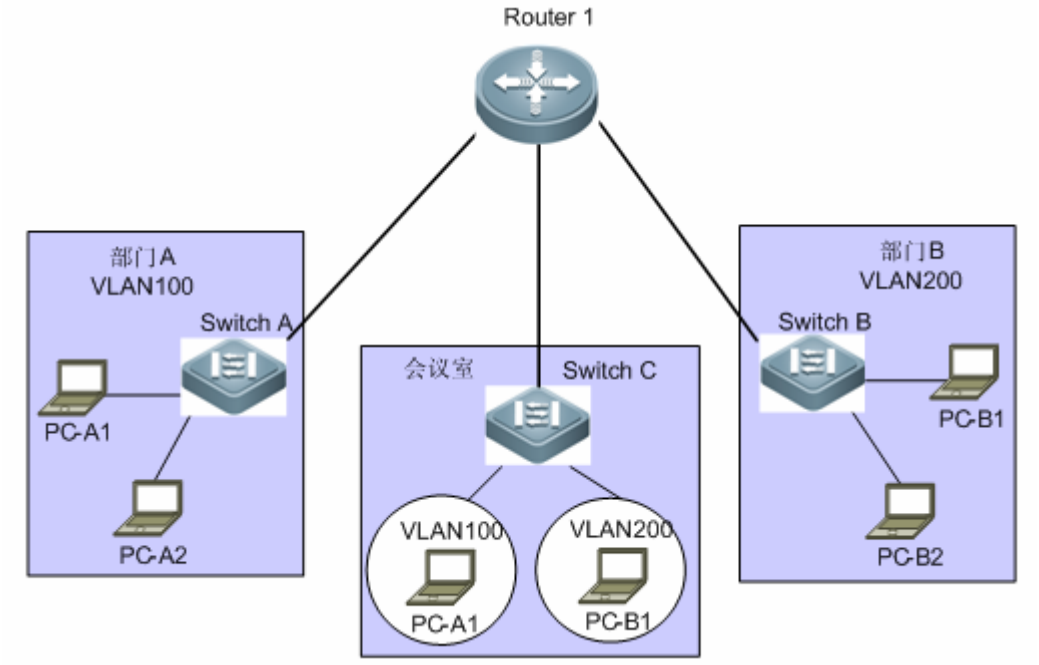
查看所有端口的 MAC VLAN 开关状态

```
Ruijie# show mac-vlan interface
  MAC VLAN is enabled on following interface:
  ---------------------------------------
  fastethernet 0/3
  fastethernet 0/10
```

11.4 MAC VLAN 典型配置举例

如图所示： PC-A1、PC-A2 属于 A 部门，规划为 VLAN 100；PC-B1、PC-B2 属于 B 部门，规划为 VLAN 200。因为人员流动关系，公司在会议室提供了临时办公场所，但是要求接入后只能划分到自己部门所在的 VLAN。如：PC-A1 接入后只能划分到 VLAN 100，PC-B1 接入后只能划分到 VLAN 200。

图 11-1 MAC VLAN 典型应用图



因为会议室 PC 接入网络的端口不固定，因此可能通过 MAC VLAN 功能，将员工 PC 的 MAC 地址和员工所在部门的 VLAN 关联起来。不管从哪个端口接入，均可以被自动划分到部门所在的 VLAN。

11.4.1 MAC VLAN静态配置过程

如果 PC 接入不需要进行认证，通过配置静态 MAC VLAN 表项，可以达到上述要求。

交换机 Switch C 上要求配置如下：

步骤 1、与 Router 1 相连的端口配置为 TRUNK 口：

```
Ruijie(config)# interface interface_name
Ruijie(config-if)# switchport mode trunk
```

步骤 2、所有与 PC 相连的端口配置为 HYBRID 口，开启 MAC VLAN 功能开关，并修改默认 UNTAG VLAN 列表；

```
Ruijie(config)# interface interface_name
Ruijie(config-if)# switchport mode hybrid
Ruijie(config-if)# switchport hybrid allowed vlan add untagged 100,200
Ruijie(config-if)# mac-vlan enable
```

步骤 3、配置 MAC VLAN 表项：

```
Ruijie(config)# mac-vlan mac-address PC-A1-mac vlan 100
Ruijie(config)# mac-vlan mac-address PC-B1-mac vlan 200
```

所有通过 Switch C 接入的 PC，通过步骤 3，配置相应的 MAC VLAN 表项。

11.4.2 MAC VLAN + 802.1x VLAN下发配置过程

如果 PC 接入需要进行 802.1x 认证，结合 802.1x VLAN 下发功能，可以动态生成 MAC VLAN 表项，可以达到上述接入要求。

交换机 Switch C 上要求配置如下：

步骤 1、2，同 MAC VLAN 静态配置过程；

步骤 3、在端口上开启 802.1x 受控，并允许 VLAN 下发；

```
Ruijie(config-if)# dot1x port-control auto
Ruijie(config-if)# dot1x dynamic-vlan enable
```

通过以上配置，即可达到要求。

12 MSTP

12.1 STP、RSTP概述

本设备既支持 STP 协议，也支持 RSTP 协议，遵循 IEEE 802.1D 和 IEEE 802.1w 标准。

STP 协议是用来避免链路环路产生的广播风暴、并提供链路冗余备份的协议。

对二层以太网来说，两个 LAN 间只能有一条活动着的通路，否则就会产生广播风暴。但是为了加强一个局域网的可靠性，建立冗余链路又是必要的，其中的一些通路必须处于备份状态，如果当网络发生故障，另一条链路失效时，冗余链路就必须被提升为活动状态。手工控制这样的过程显然是一项非常艰苦的工作，STP 协议就自动地完成这项工作。它能使一个局域网中的设备起以下作用：

- 发现并启动局域网的一个最佳树型拓朴结构。
- 发现故障并随之进行恢复，自动更新网络拓朴结构，使在任何时候都选择了可能的最佳树型结构。

局域网的拓朴结构是根据管理员设置的一组网桥配置参数自动进行计算的。使用这些参数能够生成最好的一棵拓朴树。只有配置得当，才能得到最佳的方案。

RSTP 协议完全向下兼容 802.1D STP 协议，除了和传统的 STP 协议一样具有避免回路、提供冗余链路的功能外，最主要的特点就是“快”。如果一个局域网内的网桥都支持 RSTP 协议且管理员配置得当，一旦网络拓朴改变而要重新生成拓朴树只需要不超过 1 秒的时间（传统的 STP 需要大约 50 秒）。

12.1.1 Bridge Protocol Data Units(简写为BPDU)：

要生成一个稳定的树型拓朴网络需要依靠以下元素：

- 每个网桥拥有的唯一的桥 ID（Bridge ID），由桥优先级和 Mac 地址组合而成。
- 网桥到根桥的路径花费（Root Path Cost），以下简称根路径花费。
- 每个端口 ID（Port ID），由端口优先级和端口号组合而成。

网桥之间通过交换 BPDU（Bridge Protocol Data Units，网桥协议数据单元）帧来获得建立最佳树形拓朴结构所需要的信息。这些帧以组播地址 01-80-C2-00-00-00（十六进制）为目的地址。

每个 BPDU 由以下这些要素组成：

- Root Bridge ID（本网桥所认为的根桥 ID）。
- Root Path Cost（本网桥的根路径花费）。
- Bridge ID（本网桥的桥 ID）。
- Message Age（报文已存活的时间）
- Port ID（发送该报文端口的 ID）。

Forward-Delay Time、Hello Time、Max-Age Time 三个协议规定的时间参数。

其他一些诸如表示发现网络拓朴变化、本端口状态的标志位。

当网桥的一个端口收到高优先级的 BPDU（更小的 Bridge ID，更小的 Root Path Cost 等），就在该端口保存这些信息，同时向所有端口更新并传播这些信息。如果收到比自己低优先级的 BPDU，网桥就丢弃该信息。

这样的机制就使高优先级的信息在整个网络中传播开，BPDU 的交流就有了下面的结果：

- 网络中选择了一个网桥为根桥（Root Bridge）。
- 除根桥外的每个网桥都有一个根口（Root Port），即提供最短路径到 Root Bridge 的端口。
- 每个网桥都计算出了到根桥（Root Bridge）的最短路径。
- 每个 LAN 都有了指派网桥（Designated Bridge），位于该 LAN 与根桥之间的最短路径中。指派网桥和 LAN 相连的端口称为指派端口（Designated Port）。
- 根口（Root port）和指派端口（Designated Port）进入 Forwarding 状态。
- 其他不在生成树中的端口就处于 Discarding 状态

12.1.2 Bridge ID

按 IEEE 802.1W 标准规定，每个网桥都要有单一的网桥标识（Bridge ID），生成树算法中就是以它为标准来选出根桥（Root Bridge）的。Bridge ID 由 8 个字节组成，后 6 个字节为该网桥的 mac 地址，前 2 个字节如下表所示，前 4 bit 表示优先级（Priority），后 8 bit 表示 System ID，为以后扩展协议而用，在 RSTP 中该值为 0，因此给网桥配置优先级就要是 4096 的倍数。

	Bit 位	值
Priority value	16	32768
	15	16384
	14	8192
	13	4096
System ID	12	2048
	11	1024
	10	512
	9	256
	8	128
	7	64
	6	32
	5	16
	4	8
	3	4
	2	2
	1	1

12.1.3 Spanning-Tree Timers（生成树的定时器）

以下描述影响到整个生成树性能的三个定时器。

- Hello timer：定时发送 BPDU 报文的时间间隔。
- Forward-Delay timer：端口状态改变的时间间隔。当 RSTP 协议以兼容 STP 协议模式运行时，端口从 Listening 转变向 Learning，或者从 Learning 转向 Forwarding 状态的时间间隔。
- Max-Age timer：BPDU 报文消息生存的最长时间。当超出这个时间，报文消息将被丢弃。

12.1.4 Port Roles and Port States

每个端口都在网络中有扮演一个角色（Port Role），用来体现在网络拓朴中的不同作用。

- Root port：提供最短路径到根桥（Root Bridge）的端口。
- Designated port：每个 LAN 的通过该口连接到根桥。
- Alternate port：根口的替换口，一旦根口失效，该口就立该变为根口。
- Backup port：Designated Port 的备份口，当一个网桥有两个端口都连在一个 LAN 上，那么高优先级的端口为 Designated Port，低优先级的端口为 Backup Port。
- Disable port：当前不处于活动状态的口，即 Operation State 为 Down 的端口都被分配了这个角色。

以下为各个端口角色的示意图 1、2、3：

R = Root Port　　D = Designated Port　　A = Alternate Port　　B = Backup Port

在没有特别说明情况下，端口优先级从左到右递减。

图 12-1

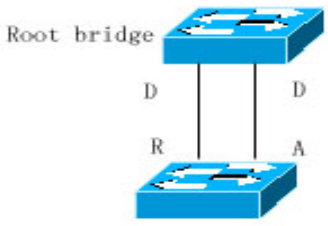


图 12-2

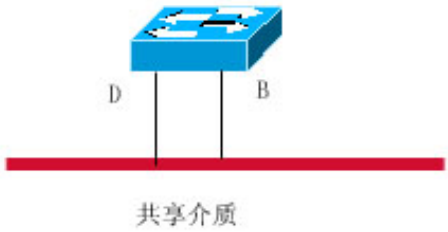
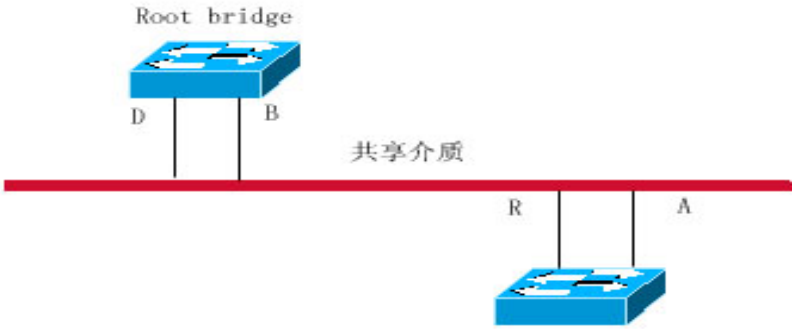


图 12-3



每个端口有三个状态（Port State）来表示是否转发数据包，从而控制着整个生成树拓朴结构。

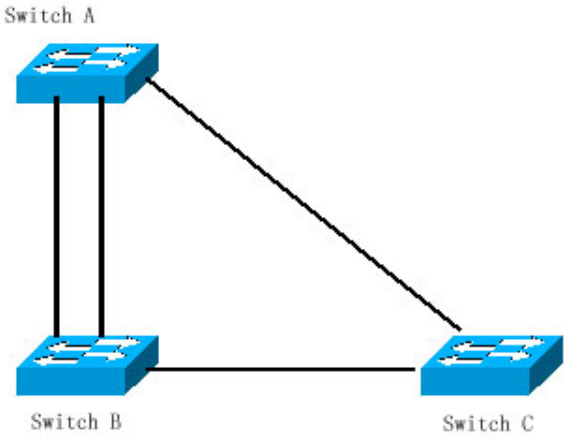
- Discarding：既不对收到的帧进行转发，也不进行源 Mac 地址学习。
- Learning：不对收到的帧进行转发，但进行源 Mac 地址学习，这是个过渡状态。
- Forwarding：既对收到的帧进行转发，也进行源 Mac 地址的学习。

对一个已经稳定的网络拓朴，只有 Root Port 和 Designated Port 才会进入 Forwarding 状态，其它端口都只能处于 Discarding 状态。

12.1.5 网络拓朴树的生成（典型应用方案）

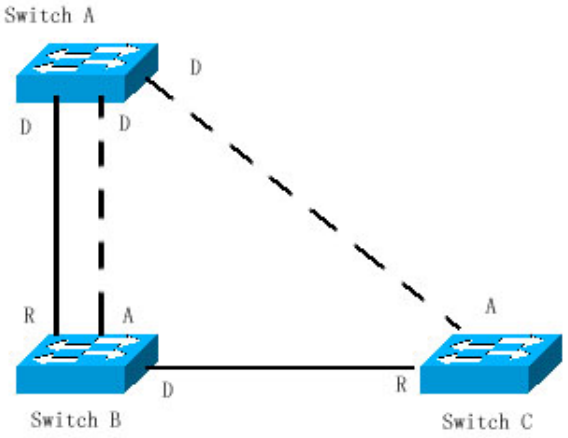
现在就可以说明 STP、RSTP 协议是如何把杂乱的网络拓朴生成一个树型结构了。如下图 4 所示，假设 Switch A、B、C 的 bridge ID 是递增的，即 Switch A 的优先级最高。A 与 B 间是千兆链路，A 和 C 间为十兆链路，B 和 C 间为百兆链路。Switch A 做为该网络的骨干设备，对 Switch B 和 Switch C 都做了链路冗余，显然，如果让这些链路都生效是会产生广播风暴的。

图 12-4



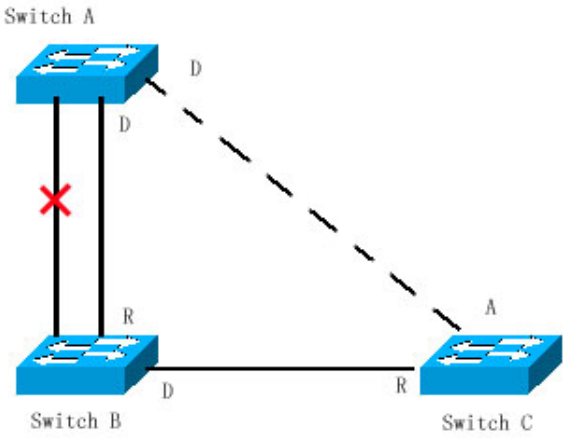
而如果这三台 Switch 都打开了 Spanning Tree 协议，它们通过交换 BPDU 选出根桥（Root Bridge）为 Switch A。Switch B 发现有两个端口都连在 Switch A 上，它就选出优先级最高的端口为 Root Port，另一个端口就被选为 Alternate Port。而 Switch C 发现它既可以通过 B 到 A，也可以直接到 A，但由于设备通过计算发现：就算通过 B 到 A 的链路花费（Path Cost）也比直接到 A 的低（各种链路对应的链路花费请查表），于是 Switch C 就选择了与 B 相连的端口为 Root port，与 A 相连的端口为 Alternate port。都选择好端口角色（Port Role）了，就进入各个端口相应的状态了，于是就生成了相应的图 5。

图 12-5



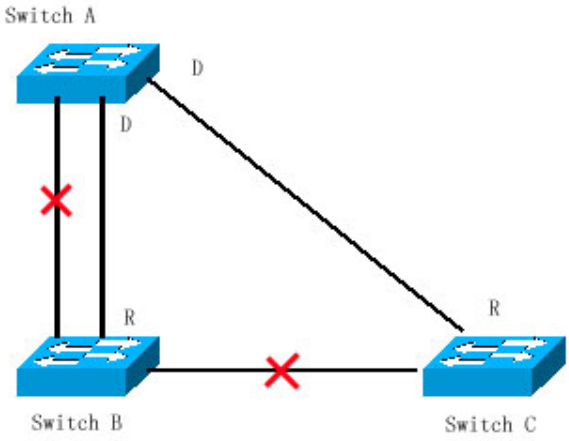
如果 Switch A 和 Switch B 之间的活动链路出了故障，那备份链路就会立即产生作用，于是就生成了相应的图 6。

图 12-6



如果 Switch B 和 Switch C 之间的链路出了故障，那 Switch C 就会自动把 Alternate port 转为 Root port，就生成了图 7 的情况。

图 12-7



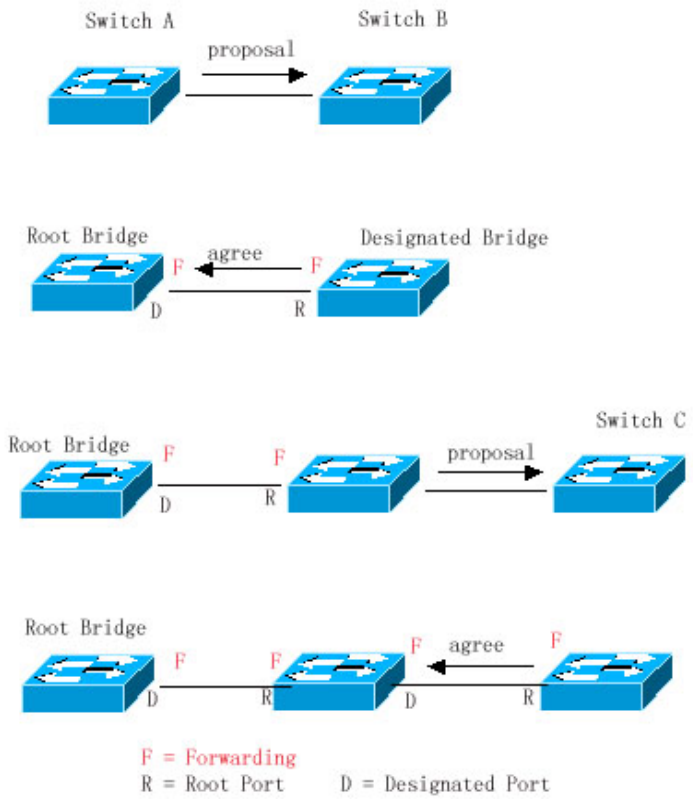
12.1.6 RSTP的快速收敛

现在开始介绍 RSTP 所特有的功能，即能让端口“快速”的 Forwarding。

STP 协议是选好端口角色（Port Role）后等待 30 秒(为 2 倍的 Forward-Delay Time，Forward-Delay Time 可配置，默认为 15 秒)再 Forwarding 的，而且每当拓朴发生变化后，每个网桥重新选出的 Root Port 和 Designated Port 都要经过 30 秒再 Forwarding，因此要等整个网络拓朴稳定为一个树型结构就大约需要 50 秒。

而 RSTP 端口的 Forwarding 过程就大不一样了，如图 8 所示，Switch A 发送 RSTP 特有“Proposal”报文，Switch B 发现 Switch A 的优先级比自身高，就选 Switch A 为根桥，收到报文的端口为 Root Port，立即 Forwarding，然后从 Root Port 向 Switch A 发送“Agree”报文。Switch A 的 Designated Port 得到“同意”，也就 Forwarding 了。然后 Switch B 的 Designated Port 又发送“Proposal”报文依次将生成树展开。因此在理论上，RSTP 是能够在网络拓朴发生变化的一瞬间恢复网络树型结构，达到快速收敛。

图 12-8



以上的“握手”过程是有条件的，就是端口间必须是“Point-to-point Connect（点对点连接）”。为了让设备发挥最大的功效，最好不要使设备间为非点对点连接。

本章中除图 9 外，其它示意图均为“点对点连接”，以下列出了“非点对点连接”的范例图。

非点对点连接范例：

图 12-9

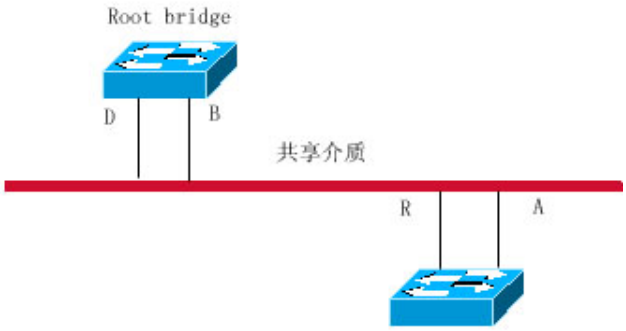
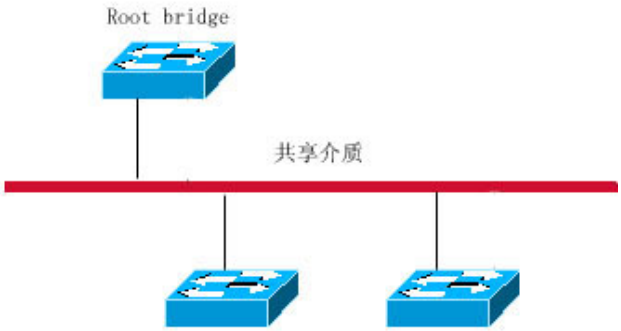
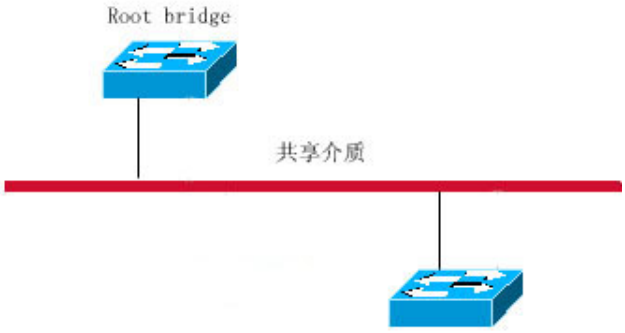


图 12-10



另外、下图为“点对点”连接，请用户注意区分

图 12-11



12.1.7 RSTP与STP的兼容

RSTP 协议可以与 STP 协议完全兼容，RSTP 协议会根据收到的 BPDU 版本号来自动判断与之相连的网桥是支持 STP 协议还是支持 RSTP 协议，如果是与 STP 网桥互连就只能按 STP 的 Forwarding 方法，过 30 秒再 Forwarding，无法发挥 RSTP 的最大功效。

另外，RSTP 和 STP 混用还会遇到这样一个问题。如图 12 所示，Switch A 是支持 RSTP 协议的，Switch B 只支持 STP 协议，它们俩互连，Switch A 发现与它相连的是 STP 桥，就发 STP 的 BPDU 来兼容它。但后来如果换了台 Switch C，它支持 RSTP 协议，但 Switch A 却依然在发 STP 的 BPDU，这样使 Switch C 也认为与之互连的是 STP 桥了，结果两台支持 RSTP 的设备却以 STP 协议来运行，大大降低了效率。

为此 RSTP 协议提供了 Protocol-migration 功能来强制发 RSTP BPDU (这种情况下，对端网桥必须支持 RSTP)，这样 Switch A 强制发了 RSTP BPDU，Switch C 就发现与之互连的网桥是支持 RSTP 的，于是两台设备就都以 RSTP 协议运行了，如图 13。

图 12-12

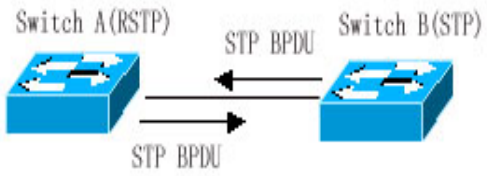
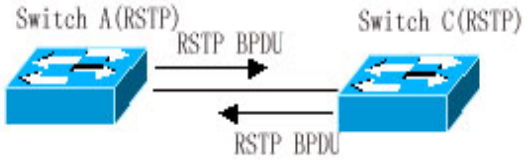


图 12-13



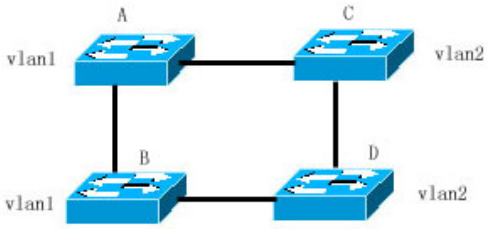
12.2 MSTP概述

本设备支持 MSTP，MSTP 是在传统的 STP、RSTP 的基础上发展而来的新的生成树协议，本身就包含了 RSTP 的快速 FORWARDING 机制。

由于传统的生成树协议与 Vlan 没有任何联系，因此在特定网络拓朴下就会产生以下问题：

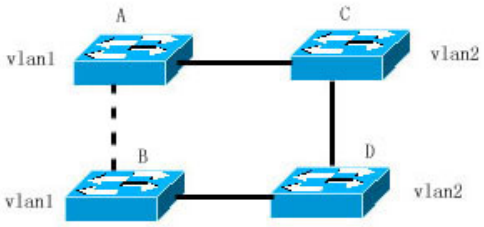
如图 14 所示，设备 A、B 在 Vlan1 内，设备 C、D 在 Vlan2 内，然后连成环路。

图 12-14



若从设备 A 依次通过设备 C、D 到达 B 的链路花费比从设备 A 直接到 B 的链路花费更少的情况下，会造成把设备 A 和 B 间的链路给 DISCARDING（如图 15 所示）。由于设备 C、D 不包含 Vlan1，无法转发 Vlan1 的数据包，这样设备 A 的 Vlan1 就无法与设备 B 的 Vlan1 进行通讯。

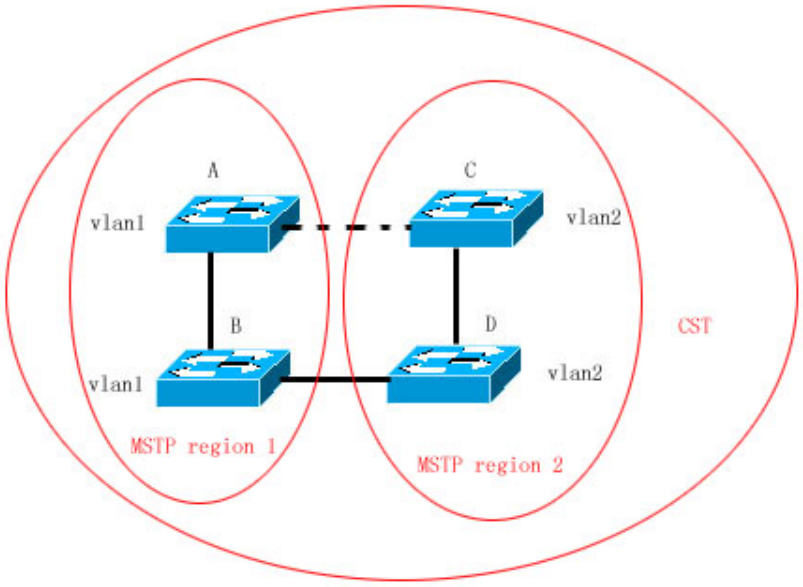
图 12-15



为了解决这个问题，MSTP 就产生了，它可以把一台设备的一个或多个 Vlan 划分为一个 Instance，有着相同 Instance 配置的设备就组成一个域（MST Region），运行独立的生成树（这个内部的生成树称为 IST，Internal Spanning-tree）；这个 MST region 组合就相当于一个大的设备整体，与其他 MST Region 再进行生成树算法运算，得出一个整体的生成树，称为 CST（Common Spanning Tree）。

按这种算法，以上网络就可以在 MSTP 算法下形成图 16 的拓朴：设备 A 和 B 都在 MSTP Region 1 内，MSTP Region 1 没能环路产生，所以没有链路 DISCARDING，同理 MSTP Region 2 的情况也是一样的。然后 Region 1 和 Region 2 就分别相当于两个大的设备，这两台“设备”间有环路，因此根据相关配置选择一条链路 DISCARDING。

图 12-16



这样，既避免了环路的产生，也能让相同 Vlan 间的通讯不受影响。

12.2.1 如何划分MSTP Region

根据以上描述，很明显，要让 MSTP 产生应有的作用，首先就要合理地划分 MSTP Region，相同 MSTP Region 内的设备“MST 配置信息”一定要相同。

MST 配置信息包括：

- MST 配置名称（Name）：最长可用 32 个字节长的字符串来标识 MSTP Region。
- MST Revision Number：用一个 16bit 长的修正值来标识 MSTP Region。
- MST Instance—vlan 的对应表：每台设备都最多可以创建 64 个 Instance（id 从 1 到 64），Instance 0 是强制存在的，所以系统总共支持 65 个 Instance。用户还可以按需要分配 1-4094 个 Vlan 属于不同的 Instance（0－64），未分配的 Vlan 缺省就属于 Instance 0。这样，每个 MSTI（MST Instance）就是一个“Vlan 组”，根据 BPDU 里的 MSTI 信息进行 MSTI 内部的生成树算法，不受 CIST 和其他 MSTI 的影响。

可在用 spanning-tree mst configuration 全局配置命令进入“MST 配置模式”配置以上信息。

MSTP BPDU 里附带以上信息，如果一台设备收到的 BPDU 里的 MST 配置信息和自身的一样，就会认为该端口上连着的设备和自己是属于同一个 MST Region，否则就认为是从另外一个 Region 来的。

建议在关闭 MSTP 模式后配置 Instance—vlan 的对应表，配置好后再打开 MSTP，以保证网络拓朴的稳定和收敛。

12.2.2 MSTP region内的生成树（IST）

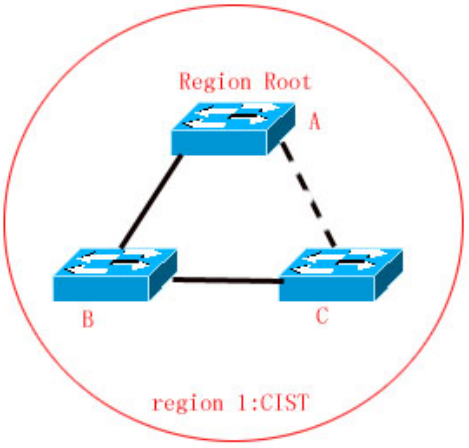
划分好 MSTP Region 后，每个 Region 里就按各个 Instance 所设置的 Bridge Priority、Port Priority 等参数选出各个 Instance 独立的 Root Bridge，以及每台设备上各个端口的 Port Role，然后就 Port Role 指定该端口在该 Instance 内是 FORWARDING 还是 DISCARDING 的。

这样，经过 MSTP BPDU 的交流，IST(Internal Spanning Tree) 就生成了，而各个 Instance 也独立的有了自己的生成树（MSTI），其中 Instance 0 所对应的生成树与 CST 共同称为 CIST（Common Instance Spanning Tree）。也就是说，每个 Instance 都为各自的“vlan 组”提供了一条单一的、不含环路的网络拓朴。

如下图所示，在 Region 1 内，设备 A、B、C 组成环路。

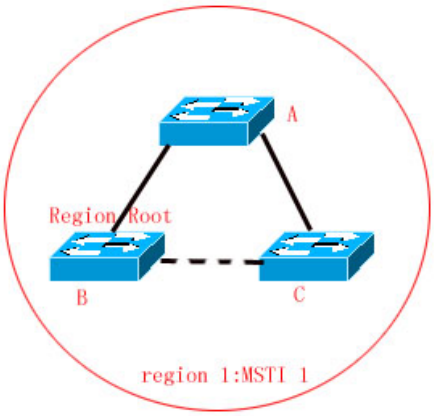
在 CIST（Instance 0）中，如图 17，因 A 的优先级最高，被选为 Region Root，再根据其他参数，把 A 和 C 间的链路给 DISCARDING。因此，对 Instance 0 的“Vlan 组”来说，只有 A 到 B、B 到 C 的链路可用，打断了这个“Vlan 组”的环路。

图 12-17



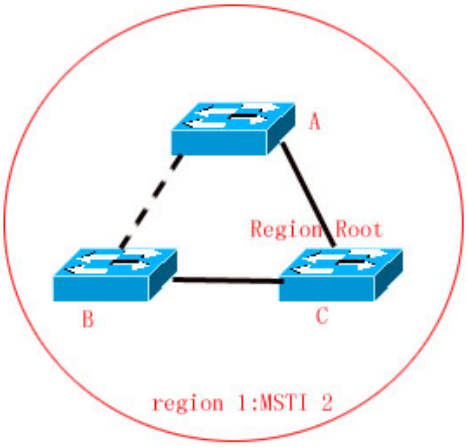
而对 MSTI 1（Instance 1）来说，如图 18，B 的优先级最高，被选为 Region Root，再根据其他参数，把 B 和 C 间的链路给 DISCARDING。因此，对 Instance 1 的“Vlan 组”来说，只有 A 到 B、A 到 C 的链路可用，打断了这个“Vlan 组”的环路。

图 12-18



而对 MSTI 2（Instance 2）来说，图 19，C 的优先级最高，被选为 Region Root，再根据其他参数，把 A 和 B 间的链路给 DISCARDING。因此，对 Instance 2 的“Vlan 组”来说，只有 B 到 C、A 到 C 的链路可用，打断了这个“Vlan 组”的环路。

图 12-19

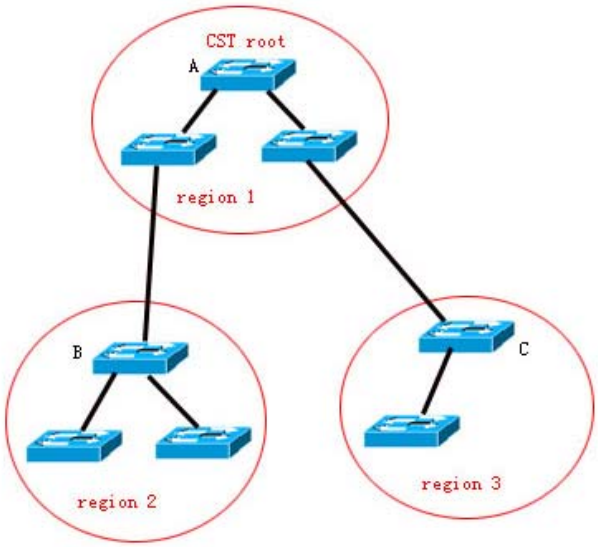


用户在这里要注意的是 MSTP 协议本身不关心一个端口属于哪个 Vlan，所以用户应该根据实际的 Vlan 配置情况来为相关端口配置对应的 Path Cost 和 Priority，以防 MSTP 协议打断了不该打断的环路。

12.2.3 MSTP region间的生成树（CST）

每个 MSTP region 对 CST 来说可以相当于一个大的设备整体，不同的 MSTP Region 也生成一个大的网络拓朴树，称为 CST(Common Spanning Tree) 。如图 20 所示，对 CST 来说，Bridge ID 最小的设备 A 被选为整个 CST 的根(CST Root)，同时也是这个 Region 内的 CIST Regional Root。在 Region 2 中，由于设备 B 到 CST Root 的 Root Path Cost 最短，所以被选为这个 Region 内的 CIST Regional Root。同理，Region 3 选设备 C 为 CIST Regional Root。

图 12-20



CIST Regional Root 不一定是该 Region 内 Bridge ID 最小的那台设备，它是指该 Region 内到 CST Root 的 Root Path Cost 最小的设备。

同时，CIST Regional Root 的 Root Port 对 MSTI 来说有了个新的 Port Role，为“Master port”，作为所有 Instance 对外的“出口”，它对所有 Instance 都是 FORWARDING 的。为了使拓朴更稳定，我们建议每个 Region 对 CST Root 的“出口”尽量只在该 Region 的一台设备上!

12.2.4 Hop Count

IST 和 MSTI 已经不用 Message Age 和 Max Age 来计算 BPDU 信息是否超时，而是用类似于 IP 报文 TTL 的机制来计算，它就是 Hop Count。

可以用 **spanning-tree max-hops** 全局配置命令来设置。在 Region 内，从 Region Root Bridge 开始，每经过一个设备，Hop Count 就会减 1，直到为 0 则表示该 BPDU 信息超时，设备收到 Hops 值为 0 的 BPDU 就要丢弃它。

为了和 Region 外的 STP、RSTP 兼容，MSTP 依然保留了 Message Age 和 Max Age 的机制。

12.2.5 MSTP和RSTP、STP协议的兼容

对 STP 协议来说，MSTP 会像 RSTP 那样发 STP BPDU 来兼容它，详细情况请参考“RSTP 与 STP 的兼容”章节。

而对 RSTP 协议来说，本身会处理 MSTP BPDU 中 CIST 的部分，因此 MSTP 不必专门的发 RSTP BPDU 以兼容它。

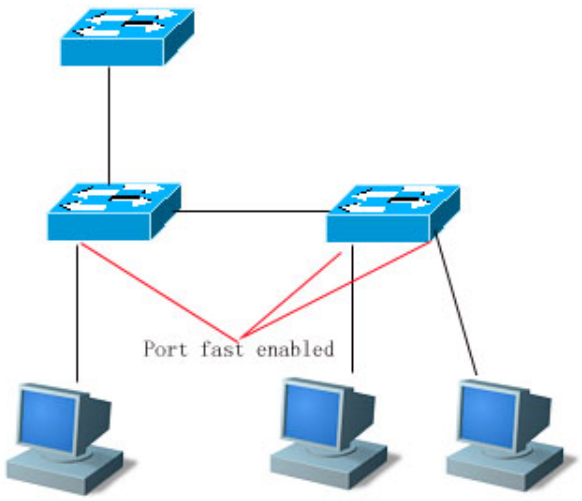
每台运行 STP 或 RSTP 协议的设备都是单独的一个 Region，不与任何一个设备组成同一个 Region。

12.3 MSTP可选特性

12.3.1 Port Fast

如果设备的端口直连着网络终端，那么就可以设置该端口为 Port Fast，端口直接 Forwarding，这样可免去端口等待 Forwarding 的过程（如果不配置 Port Fast 的端口，就要等待 30 秒 Forwarding）。下图表示了一个设备的哪些端口可以配置为 Port Fast enable。

图 12-21



如果在设了 Port Fast 的端口中还收到 BPDU，则它的 Port Fast Operational State 为 Disabled。这时该端口会按正常的 STP 算法进行 Forwarding。

12.3.2 BPDU Guard

BPDU Guard 既能全局的 enable，也能针对单个 Interface 进行 enable。这两者有些细小的差别。

可以在全局模式中用 **spanning-tree portfast bpduguard default** 命令打开全局的 BPDU Guard enabled 状态，在这种状态下，如果某个 Interface 打开了 Port Fast，或该接口自动识别为边缘口，而该 Interface 收到了 BPDU，该端口就会进入 Error-disabled 状态，以示配置错误；同时整个端口被关闭，表示网络中可能被非法用户增加了一台网络设备，使网络拓朴发生改变。

也可以在 Interface 配置模式下用 **spanning-tree bpduguard enable** 命令来打开单个 Interface 的 BPDU Guard（与该端口是否打开 Port Fast 无关）。在这个情况下如果该 Interface 收到了 BPDU，就进入 Error-disabled 状态。

12.3.3 BPDU Filter

BPDU Filter 既能全局的 enable，也能针对单个 Interface 进行 enable。这两者有些细小的差别。

可以在全局模式中用 **spanning-tree portfast bpdufilter default** 命令打开全局的 BPDU Filter enabled 状态，在这种状态下，Port Fast enabled 的 Interface 将既不收 BPDU，也不发 BPDU，这样，直连 Port Fast enabled 端口的主机

就收不到 BPDU。而如果 Port Fast enabled 的 Interface 因收到 BPDU 而使 Port Fast Operational 状态 disabled，BPDU Filter 也就自动失效。

也可以在 Interface 配置模式下用 **spanning-tree bpdufilter enable** 命令设置了单个 Interface 的 BPDU Filter enable（与该端口是否打开 Port Fast 无关）。在这个情况下该 Interface 既不收 BPDU，也不发 BPDU，并且是直接 Forwarding 的。

12.3.4 Tc-protection

TC-BPDU 报文是指携带 TC 标志的 BPDU 报文，交换机收到这类报文表示网络拓扑发生了变化，会进行 MAC 地址表的删除操作，对三层交换机，还会引发快转模块的重新打通操作，并改变 ARP 表项的端口状态。为避免交换机受到伪造 TC-BPDU 报文的恶意攻击时频繁进行以上操作，负荷过重，影响网络稳定，可以使用 TC-protection 功能进行保护。

Tc-protection 只能全局的打开和关闭，缺省情况下为打开此功能。

在打开相应功能时，收到 TC-BPDU 报文后的一定时间内（一般为 4 秒），只进行一次删除操作，同时监控该时间段内是否收到 TC-BPDU 报文。如果在该时间段内收到了 TC-BPDU 报文，则设备在该时间超时后再进行一次删除操作。这样可以避免频繁的删除 MAC 地址表项和 ARP 表项。

12.3.5 TC Guard

Tc-Protection 功能可以保证网络产生大量 tc 报文时减少动态 MAC 地址和 ARP 的删除，但在遇到 TC 报文攻击的时候还是会产生很多的删除操作，并且 TC 报文是可扩散的，将影响整个网络。使用 TC Guard 功能，我们允许用户在全局或者端口上禁止 TC 报文的扩散。当一个端口收到 TC 报文的时候，如果全局配置了 TC Guard 或者是端口上配置了 TC Guard，则该端口将屏蔽掉该端口接收或者是自己产生的 TC 报文，使得 TC 报文不会扩散到其它端口，这样能有效控制网络中可能存在的 TC 攻击，保持网络的稳定，尤其是在三层设备上，该功能能有效避免接入层设备的振荡引起核心路由中断的问题。

- 错误的使用 tc-guard 功能会使网络之间的通讯中断。
- 建议在确认网络当中有非法的 tc 报文攻击的情况下再打开此功能。
- 打开全局的 tc-guard，则所有端口都不会对外扩散 tc 报文。适用于桌面接入设备上开启。
- 打开接口的 tc-guard,则对于该接口产生的拓扑变化以及收到的 tc 报文，将不向其它端口扩散。适合在上链口，尤其是汇聚接核心的端口开启该功能。

12.3.6 TC过滤

配置 TC Guard 功能，端口将不扩散 TC 报文到本设备上其它参与生成树计算的端口，这里的不扩散包括了两种情况：一种是端口收到的 TC 报文不扩散，一种是端口自己产生的 TC 报文不扩散。端口自己产生的 TC 报文是指当端口转发状态发生变化时(例如从 block 到 forwarding 的转变)，端口会产生 TC 报文，此时表示拓扑可能发生了变化。

这样，可能引发的问题时，由于 TC Guard 阻止了 TC 报文的扩散，导致当发生拓扑变化的时候，设备没有清除相应端口的 MAC 地址，转发数据出错。

因此，引入了 TC 过滤的概念。TC 过滤是指对于端口收到的 TC 报文不处理，而正常的拓扑变化的情况，能够处理。这样，解决了未配置 Portfast 的端口频繁地 UP/DOWN 引起的清地址和核心路由中断的问题，又能保证发生拓扑变化时，核心路由表项能够得到及时地更新。

TC 过滤功能缺省情况下关闭。

12.3.7 BPDU源MAC检查

BPDU 源 MAC 检查是为了防止通过人为发送 BPDU 报文来恶意攻击交换机而使 MSTP 工作不正常。当确定了某端口点对点链路对端相连的交换机时，可通过配置 BPDU 源 MAC 检查来达到只接收对端交换机发送的 BPDU 帧，丢弃所有其他 BPDU 帧，从而达到防止恶意攻击。你可以在 interface 模式下来为特定的端口配置相应的 BPDU 源 MAC 检查 MAC 地址，一个端口只允许配置一个过滤 MAC 地址，通过 no bpdu src-mac-check 来禁止 BPDU 源 MAC 检查，此时端口接收任何 BPDU 帧。

12.3.8 BPDU非法长度过滤

BPDU 的以太网长度字段超过 1500 时，该 BPDU 帧将被丢弃，以防止收到非法 BPDU 报文。

12.3.9 边缘口的自动识别

指派口在一定的时间范围内(为 3 秒)，如果收不到下游端口发送的 BPDU，则认为该端口相连的是一台网络设备，从而设置该端口为边缘端口，直接进入 Forwarding 状态。自动标识为边缘口的端口因收到 BPDU 而自动识别为非边缘口。

可以通过 **spanning-tree autoedge disabled** 命令取消边缘口的自动识别功能。

该功能是缺省打开的。

边缘口的自动标识功能与手工的 Port Fast 冲突时，以手工配置的为准。

该功能作用于指派口与下游端口进行快速协商转发的过程中，所以 STP 协议不支持该功能。同时如果指派口已经处于转发状态，对该端口进行 Autoedge 的配置不会生效，只有在重新快速协商的过程中才生效，如拔插网线。

端口如果先打开了 BPDU Filter，则该端口直接 Forwarding，不会自动识别为边缘口。

该功能只适用与指派口。

12.3.10 ROOT Guard功能

在网络设计中常常将根桥和备份根桥划分在同一个域内，由于维护人员的错误配置或网络中的恶意攻击，根桥有可能收到优先级更高的配置信息，从而失去当前根桥的位置，引起网络拓扑的错误的变动。Root Guard 功能就是为了防止这种情况的出现。

接口打开 Root Guard 功能时，强制其在所有实例上的端口角色为指定端口，一旦该端口收到优先级更高的配置信息时，Root Guard 功能会将该接口置为 root-inconsistent (blocked)状态，在足够长的时间内没有收到更优的配置信息时，端口会恢复成原来的正常状态。

当端口因 Root Guard 而处于 blocked 状态时，可以通过手动恢复为正常状态，即关闭端口的 ROOT Guard 功能或关闭接口的保护功能（在接口模式下配置 spanning-tree guard none）。

- 错误的使用 ROOT Guard 特性会导致网络链路的断开。
- 在非指派口上打开 ROOT Guard 功能会强制其为指派口，同时端口会进入 BKN 状态，该状态表示端口因 Root 不一致而进入 blocked 状态。
- 如果端口在 MST0 因收到更优的配置消息而进入 BKN 状态，会强制端口在其它所有的实例中处于 BKN 状态。
- 端口的 ROOT Guard 和 LOOP Guard 同一时刻只能有一个生效。

12.3.11 LOOP Guard功能

由于单向链路的故障，根口或备份口由于收不到 BPDU 会变成指派口进入转发状态，从而导致了网络中环路的产生，LOOP Guard 功能防止了这种情况的发生。

对于配置了环路保护的端口，如果收不到 BPDU，会进行端口角色的迁移，但端口状态将一直被设成 discarding 状态。直到重新收到 BPDU 而进行生成树的重计算。

- 可以基于全局或接口打开 LOOP Guard 特性。
- 端口的 ROOT Guard 和 LOOP Guard 同一时刻只能有一个生效。

12.4 配置MSTP

12.4.1 缺省的Spanning Tree设置

下面列出 Spanning Tree 的缺省配置

项目	缺省值
Enable State	Disable，不打开 STP
STP MODE	MSTP
STP Priority	32768
STP port Priority	128
STP port cost	根据端口速率自动判断
Hello Time	2 秒
Forward-delay Time	15 秒
Max-age Time	20 秒
Path Cost 的缺省计算方法	长整型

Tx-Hold-Count	3
Link-type	根据端口双工状态自动判断
Maximum hop count	20
vlan 与 实例 对应关系	所有 vlan 属于实例 0，只存在实例 0

可通过 **spanning-tree reset** 命令让 Spanning Tree 参数恢复到缺省配置(不包括关闭 Span)。

12.4.2 打开、关闭Spanning Tree协议

打开 Spanning-tree 协议，设备即开始运行生成树协议，本设备缺省运行的是 MSTP 协议。

设备的缺省状态是关闭 Spanning-tree 协议。

进入特权模式，按以下步骤打开 Spanning Tree 协议：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **spanning-tree**	打开 Spanning Tree 协议。
Ruijie(config)# **end**	退回到特权模式。
Ruijie# **show spanning-tree**	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

如果要关闭 Spanning Tree 协议，可用 **no spanning-tree** 全局配置命令进行设置。

12.4.3 配置Spanning Tree的模式

按 802.1 相关协议标准，STP、RSTP、MSTP 这三个版本的 Spanning Tree 协议本来就无须管理员再多做设置，版本间自然会互相兼容。但考虑到有些厂家不完全按标准实现，可能会导致一些兼容性的问题。因此我们提供这么一条命令配置，以供管理员在发现其他厂家的设备与本设备不兼容时，能够切换到低版本的 Spanning Tree 模式，以兼容之。

从 MSTP 模式切换到 RSTP 或 STP 模式时，有关 MSTP Region 的所有的信息将被清空。

设备的缺省模式是 MSTP 模式。

进入特权模式，按以下步骤打开 Spanning Tree 协议：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **spanning-tree mode mstp / rstp / stp**	切换 Spanning Tree 模式。
Ruijie(config)# **end**	退回到特权模式。
Ruijie# **show spanning-tree**	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

如果要恢复 Spanning Tree 协议的缺省模式，可用 **no spanning-tree mode** 全局配置命令进行设置。

12.4.4 配置设备优先级（Switch Priority）

设置设备的优先级关系着到底哪个设备为整个网络的根，同时也关系到整个网络的拓朴结构。建议管理员把核心设备的优先级设得高些（数值小），这样有利于整个网络的稳定。可以给不同的 Instance 分配不同的设备优先级，各个 Instance 可根据这些值运行独立的生成树协议。对于不同 Region 间的设备，它们只关心 CIST（Instance 0）的优先级。

如 Bridge ID 所讲，优先级的设置值有 16 个，都为 4096 的倍数，分别是 0，4096，8192，12288，16384，20480，24576，28672，32768，36864，40960，45056，49152，53248，57344，61440。缺省值为 32768。

进入特权模式，按以下步骤配置设备优先级：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **spanning-tree** [**mst** *instance-id*] **priority** *priority*	针对不同的 instance 配置设备的优先级，如果不加 instance 参数时，表示对 instance 0 进行配置。 *instance-id*，范围为 0－64 *priority*，取值范围为 0 到 61440，按 4096 的倍数递增，缺省值为 32768。
Ruijie(config)# **end**	退回到特权模式。
Ruijie# **show running-config**	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

您如果要恢复到缺省值，可用 **no spanning-tree mst** *instance-id* **priority** 全局配置命令进行设置。

12.4.5 配置端口优先级（Port Priority）

当有两个端口都连在一个共享介质上，设备会选择一个高优先级（数值小）的端口进入 Forwarding 状态，低优先级（数值大）的端口进入 Discarding 状态。如果两个端口的优先级一样，就选端口号小的那个进入 Forwarding 状态。您可以在一个端口上给不同的 Instance 分配不同的端口优先级，各个 Instance 可根据这些值运行独立的生成树协议。

和设备的优先级一样，可配置的优先级值也有 16 个，都为 16 的倍数，分别是 0，16，32，48，64，80，96，112，128，144，160，176，192，208，224，240。缺省值为 128。

进入特权模式，按以下步骤配置端口优先级：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **interface** *interface-id*	进入该 interface 的配置模式，合法的 interface 包括物理端口和 Aggregate Link。
Ruijie(config-if)# **spanning-tree** [**mst** *instance-id*] **port-priority** *priority*	针对不同的 instance 配置端口的优先级，当您不加 instance 参数时，即对 instance 0 进行配置。 *instance-id*，范围为 0－64 *priority*，配置该 interface 的优先级，取值范围为 0 到 240，按 16 的倍数递增，缺省值为 128

Ruijie(config-if)# **end**	退回到特权模式。
Ruijie# **show spanning-tree** [**mst** *instance-id*] **interface** *interface-id*	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

您如果要恢复到缺省值，可用 **no spanning-tree mst** *instance-id* **port-priority** 接口配置命令进行设置。

12.4.6 配置端口的路径花费（Path Cost）

设备是根据哪个端口到根桥（Root Bridge）的 Path Cost 总和最小而选定 Root Port 的，因此 Port Path Cost 的设置关系到本设备 Root Port。它的缺省值是按 Interface 的链路速率（The Media Speed）自动计算的，速率高的花费小，如果管理员没有特别需要可不必更改它，因为这样算出的 Path Cost 最科学。您可以在一个端口上针对不同的 Instance 分配不同的路径花费，各个 Instance 可根据这些值运行独立的生成树协议。

进入特权模式，按以下步骤配置端口路径花费：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **interface** *interface-id*	进入该 interface 的配置模式，合法的 interface 包括物理端口和 Aggregate Link。
Ruijie(config-if)# **spanning-tree** [**mst** *instance-id*] **cost** *cost*	针对不同的 instance 配置端口的优先级，当您不加 instance 参数时，即对 instance 0 进行配置。 *instance-id*，范围为 0－64 *cost* ，配置该端口上的花费，取值范围为 1 到 200，000，000。缺省值为根据 interface 的链路速率自动计算。
Ruijie(config-if)# **end**	退回到特权模式。
Ruijie# **show spanning-tree** [**mst** *instance-id*] **interface** *interface-id*	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

您如果要恢复到缺省值，可用 no spanning-tree mst cost 接口配置命令进行设置。

12.4.7 配置Path Cost的缺省计算方法（path cost method）

当该端口 Path Cost 为缺省值时，设备会自动根据端口速率计算出该端口的 Path Cost。但 IEEE 802.1d-1998 和 IEEE 802.1t 对相同的链路速率规定了不同 Path Cost 值，802.1d-1998 的取值范围是短整型（short）（1—65535），802.1t 的取值范围是长整型（long）（1—200，000，000）。其中对于 AP 的 Cost 值有两个方案：我司的私有方案固定为物理口的 Cost 值*95%；标准推荐的方案为 20，000，000，000/(AP 的实际链路带宽)，其中 AP 的实际链路带宽为成员口的带宽*UP 成员口个数。请管理员一定要统一好整个网络内 Path Cost 的标准。缺省模式为私有长整型模式。

下表列出两种方法对不同链路速率自动设置的 Path Cost。

端口速率	Interface	IEEE 802.1d（short）	IEEE 802.1t（long）	IEEE 802.1t（long standard）

10M	普通端口	100	2000000	2000000
	Aggregate Link	95	1900000	2000000 ÷ linkupcnt
100M	普通端口	19	200000	200000
	Aggregate Link	18	190000	200000 ÷ linkupcnt
1000M	普通端口	4	20000	20000
	Aggregate Link	3	19000	20000 ÷ linkupcnt
10000M	普通端口	2	2000	2000
	Aggregate Link	1	1900	2000 ÷ linkupcnt

默认采用我司的私有长整型模式。修改成标准推荐方案的 path cost 方案后，AP 的 cost 会随着 UP 成员口数量的变化而变化，而端口 cost 值变化会导致网络拓扑发生变化。

AP 为静态 AP 时，表格中的 linkupcnt 为 UP 成员口个数；AP 为 LACP AP 时，表格中的 linkupcnt 为参与 AP 数据转发的成员口个数；当 AP 内没有任何成员口 linkup 时，linkupcnt 为 1。具体 AP 和 LACP 的配置，请参见《AP-SCG.doc》和《LACP-SCG.doc》的说明。

进入特权模式，按以下步骤配置端口路径花费的缺省计算方法：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **spanning-tree pathcost method** {{**long** [**standard**]} | **short**}	配置端口路径花费的缺省计算方法，设置值为私有长整型（long）、标准长整形(standard long)或短整型（short），缺省值为私有长整型（long）。
Ruijie(config)# **end**	退回到特权模式。
Ruijie# **show running-config**	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

您如果要恢复到缺省值，可用 **no spanning-tree pathcost method** 全局配置命令进行设置。

12.4.8 配置Hello Time

配置设备定时发送 BPDU 报文的时间间隔。缺省值为 2 秒。

进入特权模式，按以下步骤配置 Hello Time：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **spanning-tree hello-time** *seconds*	配置 hello_time，取值范围为 1 到 10 秒，缺省值为 2 秒。
Ruijie(config)# **end**	退回到特权模式。
Ruijie# **show running-config**	核对配置条目。

Ruijie# **copy running-config startup-config**	保存配置。

您如果要恢复到缺省值，可用 no spanning-tree hello-time 全局配置命令进行设置。

12.4.9 配置Forward-Delay Time

配置端口状态改变的时间间隔。缺省值为 15 秒。

进入特权模式，按以下步骤配置 Forward-Delay Time：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **spanning-tree forward-time** *seconds*	配置 forward delay time，取值范围为 4 到 30 秒，缺省值为 15 秒。
Ruijie(config)# **end**	退回到特权模式。
Ruijie# **show running-config**	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

您如果要恢复到缺省值，可用 **no spanning-tree forward-time** 全局配置命令进行设置。

12.4.10 配置Max-Age Time

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **spanning-tree max-age** *seconds*	配置 max age time，取值范围为 6 到 40 秒，缺省值为 20 秒。
Ruijie(config)# **end**	退回到特权模式。
Ruijie# **show running-config**	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

您如果要恢复到缺省值，可用 **no spanning-tree max-age** 全局配置命令进行设置。

Hello Time、Forward-Delay Time、Max-Age Time 除了有一个自身的取值范围外，这三个之间还有一个制约关系，就是：2*(Hello Time + 1.0 seconds) <= Max-Age Time <= 2*(Forward-Delay – 1.0seconds)。您配置的这三个参数必须满足这个条件，否则有可能导致拓扑不稳定。

12.4.11 配置Tx-Hold-Count

配置每秒钟最多发送的 BPDU 个数，缺省值为 3 个。

进入特权模式，按以下步骤配置 Tx-Hold-Count：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。

Ruijie(config)# **spanning-tree tx-hold-count** *numbers*	配置每秒最多发送 BPDU 个数，取值范围为 1 到 10 个，缺省值为 3 个。
Ruijie(config)# **end**	退回到特权模式。
Ruijie# **show running-config**	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

您如果要恢复到缺省值，可用 no spanning-tree tx-hold-count 全局配置命令进行设置。

12.4.12配置link-type

配置该端口的连接类型是不是“点对点连接”，这一点关系到RSTP是否能快速的收敛。请参照“RSTP的快速收敛”。当您不设置该值时，设备会根据端口的“双工”状态来自动设置的，全双工的端口就设link type为point-to-point，半双工就设为shared。您也可以强制设置link type来决定端口的连接是不是“点对点连接”。

进入特权模式，按以下步骤配置端口的 link type：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **interface** *interface-id*	进入接口配置模式
Ruijie(config-if)# **spanning-tree link-type point-to-point / shared**	配置该 interface 的连接类型，缺省值为根据端口“双工”状态来自动判断是不是“点对点连接”。全双工为“点对点连接”，即可以快速 FORWARDING。
Ruijie(config-if)# **end**	退回到特权模式。
Ruijie# **show running-config**	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

您如果要恢复到缺省值，可用 **no spanning-tree link-type** 接口配置命令进行设置。

12.4.13配置Protocol Migration处理

该设置是让该端口强制进行版本检查。相关说明请参看 RSTP与STP的兼容。

命令	作用
Ruijie# **clear spanning-tree detected-protocols**	对所有端口强制版本检查
Ruijie# **clear spanning-tree detected-protocols interface** *interface-id*	针对一个端口进行版本检查

12.4.14配置MSTP Region

要让多台设备处于同一个 MSTP Region，就要让这几台设备有相同的名称（Name）、相同的 Revision Number、相同的 Instance—Vlan 对应表。

你可以配置 0－64 号 Instance 包含哪些 Vlan，剩下的 Vlan 就自动分配给 Instance 0。一个 Vlan 只能属于一个 Instance。

我们建议您在关闭 STP 的模式下配置 Instance—Vlan 的对应表，配置好后再打开 MSTP，以保证网络拓朴的稳定和收敛。

进入特权模式，按以下步骤配置 MSTP Region：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **spanning-tree mst configuration**	进入 MST 配置模式。
Ruijie(config-mst)# **instance** *instance-id* **vlan** *vlan-range*	把 vlan 组添加到一个 MST instance 中 *instance-id*，范围为 0－64 *vlan-range*，范围为 1－4094 举例来说： instance 1 vlan 2-200 就是把 vlan 2 到 vlan 200 都添加到 instance 1 中。 instance 1 vlan 2，20，200 就是把 vlan 2、vlan 20，vlan 200 添加到 instance 1 中。 同样，您可以用 no 命令把 vlan 从 instance 中删除，删除的 vlan 自动转入 instance 0。
Ruijie(config-mst)# **name** *name*	指定 MST 配置名称，该字符串最多可以有 32 个字节。
Ruijie(config-mst)# **revision** *version*	指定 MST revision number，范围为 0－65535。缺省值为 0
Ruijie(config-mst)# **show spanning-tree mst configuration**	核对 MST 的配置条目。
Ruijie(config-mst)# **end**	退回到特权模式。
Ruijie# **copy running-config startup-config**	保存配置。

要恢复缺省的 MST Region Configuration 配置，您可以用 **no spanning-tree mst configuration** 全局配置命令。您也可以用 **no instance** *instance-id* 来删除该 instance。同样，**no name**、**no revision** 可以分别把 MST name、MST revision number 恢复到缺省值。

以下为配置实例：

```
Ruijie(config)# spanning-tree mst configuration
Ruijie(config-mst)# instance 1 vlan 10-20
Ruijie(config-mst)# name region1
Ruijie(config-mst)# revision 1
Ruijie(config-mst)# show spanning-tree mst configuration
Multi spanning tree protocol : Enable Name [region1]
Revision 1
Instance Vlans Mapped
-------- --------------------
0 1-9,21-4094
1 10-20
------------------------------
Ruijie(config-mst)# exit
```

```
Ruijie(config)#
```

在配置 vlan 和 instance 的映射关系前请务必确保所配置的 vlan 已经被创建，否则在部分产品上有可能会出现 vlan 和 instance 关联失败。

12.4.15 配置Maximum-Hop Count

配置 Maximum-Hop Count，指定了 BPDU 在一个 Region 内经过多少台设备后被丢弃。它对所有 Instance 有效。

进入特权模式，按以下步骤配置 Maximum-Hop Count：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **spanning-tree max-hops** *hop-count*	配置 Maximum-Hop Count，范围为 1－40，缺省值为 20
Ruijie(config)# **end**	退回到特权模式。
Ruijie# **show running-config**	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

您如果要恢复到缺省值，可用 **no spanning-tree max-hops** 全局配置命令进行设置。

12.4.16 配置接口的兼容性模式

配置接口的兼容性模式，可以使该端口发送 BPDU 时根据当前端口的属性有选择的携带不同的 MSTI 的信息，以实现与其它产商之间的互连。

进入特权模式，按以下步聚配置接口的兼容性模式：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **interface** *interface-id*	进入接口配置模式
Ruijie(config-if)# **spanning-tree compatible enable**	打开接口的兼容性模式
Ruijie(config-if)# **end**	退回到特权模式。
Ruijie# **show running-config**	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

您如果要取消该配置，可用 **no spanning-tree compatible enable** 接口配置命令进行设置。

12.4.17 清除STP统计信息

该设置是清除 STP 的收发包统计信息。收发包统计信息可以通过 **show spanning-tree counters** 命令查看。

命令	作用
Ruijie# **clear spanning-tree counters**	清除所有端口的收发包统计信息

Ruijie# **clear spanning-tree counters interface** *interface-id*	清除指定端口的收发包统计信息

12.5 配置MSTP可选特性

12.5.1 缺省的生成树可选特性设置

可选特性除了边缘口的自动识别功能缺省打开外，其它功能缺省都是关闭的。

12.5.2 打开Port Fast

打开 Port Fast 后该端口会直接 Forwarding。但会因为收到 BPDU 而使 Port Fast Operational State 为 disabled，从而正常的参与 STP 算法而 Forwarding。

进入特权模式，按以下步骤配置 Port Fast：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **interface** *interface-id*	进入该 interface 的配置模式，合法的 interface 包括物理端口和 Aggregate Link。
Ruijie(config-if)# **spanning-tree portfast**	打开该 interface 的 portfast。
Ruijie(config-if)# **end**	退回到特权模式。
Ruijie# **show spanning-tree interface** *interface-id* **portfast**	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

您如果要关闭 Port Fast，在 Interface 配置模式下用 **spanning-tree portfast disable** 命令进行设置。

您可以用全局配置命令 **spanning-tree portfast default** 来打开所有端口的 Portfast。

12.5.3 打开BPDU Guard

端口打开 BPDU Guard 后，如果在该端口上收到 BPDU，则会进入 Error-disabled 状态。

进入特权模式，按以下步骤配置 BPDU Guard：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **spanning**-tree **portfast Bpduguard default**	全局的打开 BPDU guard
Ruijie(config)# **interface** *interface-id*	进入该 interface 的配置模式，合法的 interface 包括物理端口和 Aggregate Link。
Ruijie(config-if)# **spanning-tree portfast**	打开该 interface 的 portfast。全局的 BPDU guard 配置

	才生效。
Ruijie(config-if)# **end**	退回到特权模式。
Ruijie# **show running-config**	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

您如果要关闭 BPDU Guard，可在全局配置命令 **no spanning-tree portfast bpduguard default** 进行设置。

您如果要针对单个 Interface 打开 BPDU Guard，您可用 Interface 配置命令 **spanning-tree bpduguard enable** 进行设置，用 **spanning-tree bpduguard disable** 关闭 BPDU guard。

12.5.4 打开BPDU Filter

打开 BPDU Filter 后，相应端口会既不发，也不收 BPDU。

进入特权模式，按以下步骤配置端口 BPDU Filter：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **spanning-tree portfast bpdufilter default**	全局的打开 BPDU filter
Ruijie(config)# **interface** *Interface-id*	进入该 interface 的配置模式，合法的 interface 包括物理端口和 Aggregate Link。
Ruijie(config-if)# **spanning-tree portfast**	打开该 interface 的 portfast。全局的 BPDU filter 配置才生效。
Ruijie(config-if)# **end**	退回到特权模式。
Ruijie# **show running-config**	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

您如果要关闭 BPDU Filter，可以用全局配置命令 **no spanning-tree portfast bpdufilter default** 进行设置。

您如果要针对单个 Interface 打开 BPDU Filter，您可以用 Interface 配置命令 **spanning-tree bpdufilter enable** 进行设置，用 **spanning-tree bpdufilter disable** 关闭 BPDU Guard。

12.5.5 打开Tc_Protection

进入特权模式，按以下步骤配置 Tc_Protection：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **spanning-tree tc-protection**	打开 tc-protection
Ruijie(config)# **end**	退回到特权模式。
Ruijie# **show running-config**	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

您如果要关闭 Tc_Protection，可以用全局配置命令 **no spanning-tree tc-protection** 进行设置。

12.5.6 打开TC Guard

进入特权模式，按以下步骤配置全局的 TC Guard

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **spanning-tree tc-protection tc-guard**	打开全局的 TC Guard
Ruijie(config)# **end**	退回到特权模式。
Ruijie# **show running-config**	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

进入特权模式，按以下步骤配置接口下的 TC Guard

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **interface** *Interface-id*	进入该 interface 的配置模式，合法的 interface 包括物理端口和 Aggregate Link。
Ruijie(config-if)# **spanning-tree tc-guard**	打开该 interface 的 TC Guard。
Ruijie(config-if)# **end**	退回到特权模式。
Ruijie# **show running-config**	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

12.5.7 打开TC过滤

进入特权模式，按以下步骤配置接口下的 TC 过滤功能

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **interface** *Interface-id*	进入该 interface 的配置模式，合法的 interface 包括物理端口和 Aggregate Link。
Ruijie(config-if)# **spanning-tree ignore tc**	打开该 interface 的 TC 过滤
Ruijie(config-if)# **end**	退回到特权模式。
Ruijie# **show running-config**	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

您如果需要关闭 TC 过滤功能，可以在接口模式下使用 **no spanning-tree ignore tc** 命令进行设置。

12.5.8 打开BPDU源MAC检查

打开 BPDU 源 MAC 检查，将只接受源 MAC 地址为指定 MAC 的 BPDU 帧，过滤掉其它所有接收的 BPDU 帧。

进入接口模式，您可以按以下步骤配置 BPDU 源 MAC 检查：

命令	作用

Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **interface** *Interface-id*	进入该 interface 的配置模式，合法的 interface 包括物理端口和 Aggregate Link。
Ruijie(config-if)#**bpdu src-mac-check** *H.H.H*	打开 bpdu 源 mac 检查。
Ruijie(config-if)# **end**	退回到特权模式。
Ruijie# **show running-config**	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

您如果要关闭 bpdu 源 mac 检查，可以用接口下配置命令 **no bpdu src-mac-check** 进行设置。

12.5.9 关闭边缘口的自动识别

如果在一定的时间范围内（为 3 秒），如果指派口没有收到 BPDU，则自动识别为边缘口。但会因为收到 BPDU 而使 Port Fast Operational State 为 disabled，该功能缺省是打开的。

进入特权模式，按以下步骤配置 Autoedge：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **interface** *interface-id*	进入该 interface 的配置模式，合法的 interface 包括物理端口和 Aggregate Link。
Ruijie(config-if)# **spanning-tree autoedge**	打开该 interface 的 autoedge。
Ruijie(config-if)# **end**	退回到特权模式。
Ruijie# **show spanning-tree interface** *interface-id*	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

您如果要关闭 Autoedge，在 Interface 配置模式下用 **spanning-tree autoedge disabled** 命令进行设置。

12.5.10打开Root Guard

进入特权模式，按以下步骤配置接口的 ROOT Guard

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **interface** Interface-id	进入该 interface 的配置模式，合法的 interface 包括物理端口和 Aggregate Link。
Ruijie(config-if)# **spanning-tree guard root**	打开接口的 ROOT Guard 特性
Ruijie(config-if)# **end**	退回到特权模式。
Ruijie# **show running-config**	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

12.5.11打开Loop Guard

进入特权模式，按以下步骤配置全局的 Loop Guard

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **spanning-tree Loopguard default**	打开全局的 LOOP Guard。
Ruijie(config)# **end**	退回到特权模式。
Ruijie# **show running-config**	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

进入特权模式，按以下步骤配置接口下的 LOOP Guard

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **interface** *Interface-id*	进入该 interface 的配置模式，合法的 interface 包括物理端口和 Aggregate Link。
Ruijie(config-if)# **spanning-tree guard loop**	打开该 interface 的 Loop Guard。
Ruijie(config-if)# **end**	退回到特权模式。
Ruijie# **show running-config**	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

12.5.12关闭接口的保护功能

进入特权模式，按以下步骤关闭接口的根或环路保护功能。

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **interface** *Interface-id*	进入该 interface 的配置模式，合法的 interface 包括物理端口和 Aggregate Link。
Ruijie(config-if)# **spanning-tree guard none**	关闭接口的 guard 功能
Ruijie(config-if)# **end**	退回到特权模式。
Ruijie# **show running-config**	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

12.6 显示MSTP配置和状态

MSTP 提供了如下的显示命令命令用于查看各种配置信息及运行时信息，各命令的功能说明如下：

命令	作用
show spanning-tree	显示 MSTP 的各项参数信息及生成树的拓扑信息
show spanning-tree counters [interface *interface-id***]**	显示 MSTP 的收发包统计信息
show spanning-tree summary	显示 MSTP 的各 instance 的信息及其端口转发状态信息

show spanning-tree inconsistentports	显示因根保护或环路保护而 block 的端口
show spanning-tree mst configuration	显示 MST 域的配置信息
show spanning-tree mst *instance-id*	显示该 instance 的 MSTP 信息
show spanning-tree mst *instance-id* **interface** *interface-id*	显示指定 interface 的对应 instance 的 MSTP 信息
show spanning-tree interface *interface-id*	显示指定 interface 的所有 instance 的 MSTP 信息
show spanning-tree forward-time	显示 forward-time
show spanning-tree hello time	显示 Hello time
show spanning-tree max-hops	显示 max-hops
show spanning-tree tx-hold-count	显示 tx-hold-count
show spanning-tree pathcost method	显示 pathcost method

13 协议帧透传

13.1 概述

协议帧透传功能是指在开启特定的协议后，保证协议帧可以继续转发到其他网络设备上。

支持的协议帧透传有：BPDU，GVRP，802.1X，保留组播协议，CISCO 私有 PVST 协议。各协议帧的说明如下：

BPDU 协议帧：生成树协议使用的协议帧，包括 IEEE 标准规定的协议帧和锐捷私有的协议帧。该配置文档中可配置透传的是锐捷私有的 BPDU 协议帧，协议帧通过二层目的 MAC 地址来标识，目的 MAC 地址为 01D0:F800:0000。

GVRP 协议帧：通用 VLAN 注册协议帧，包括 IEEE 标准规定的协议帧和锐捷私有的协议帧。该配置文档中可配置透传的是锐捷私有的 GVRP 协议帧，协议帧通过二层目的 MAC 地址来标识，目的 MAC 地址为 01D0:F800:0021。

802.1X 协议帧：IEEE 制定关于用户接入网络的认证标准协议帧，包括 IEEE 标准规定的协议帧和锐捷私有的协议帧。协议帧通过二层目的 MAC 地址来标识，标准协议帧的目的 MAC 地址为 0180:C200:0003，锐捷私有的 802.1X 协议帧的目的 MAC 地址为 01D0:F800:0003。

保留组播协议帧：IEEE 标准规定保留组地址。这些保留组地址通过二层目的 MAC 地址来标识，该配置文档中可配置透传的组地址范围为：0180:C200:0000 – 0180:C200:FFFF。对于该配置中同 802.1X 协议帧冲突部分地址，以 802.1X 协议帧配置为准。

PVST 协议帧：CISCO 私有的生成树协议帧。该协议帧通过目的 MAC 标识，目的 MAC 地址为：0100:0CCC:CCCD。

只支持 BPDU、GVRP、802.1X 这三种协议帧的透传。

13.2 配置协议帧透传

下面列出协议帧透传的缺省配置，在未开启对应协议情况下，这些协议帧将被认为是二层组播地址。

功能特性	缺省值
BPDU 协议帧透传	关闭
GVRP 协议帧透传	关闭
802.1X 协议帧透传	开启

13.2.1 BPDU 协议帧透传配置

在全局配置模式下，执行如下命令可以在设备上开启 BPDU 协议帧透传功能：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式
Ruijie(config)# **bridge-frame forwarding protocol bpdu**	开启 BPDU 协议帧透传功能
Ruijie(config)# **end**	退回到特权模式

13.2.2 GVRP 协议帧透传配置

在全局配置模式下，执行如下命令可以在设备上开启 GVRP 协议帧透传功能：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式
Ruijie(config)# **bridge-frame forwarding protocol gvrp**	开启 GVRP 协议帧透传功能
Ruijie(config)# **end**	退回到特权模式

13.2.3 802.1X 协议帧透传配置

在全局配置模式下，执行如下命令可以在设备上开启 802.1X 协议帧透传功能：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式
Ruijie(config)# **bridge-frame forwarding protocol 802.1x**	开启 802.1X 协议帧透传功能
Ruijie(config)# **end**	退回到特权模式

14 GVRP

14.1 概述

GVRP（GARP VLAN Registration Protocol）是一种动态配置和扩散 VLAN 成员关系的 GARP（Generic Attribute Registration Protocol，通用属性注册协议）应用。

通过 GVRP 协议，设备可以：

设备监听各端口上的 GVRP PDU，从 GVRP PDU 中学习到与之相连的 GVRP-aware 设备的 VLAN 信息，并据此配置接收 GVRP PDU 的端口上的 VLAN 成员。

通过发送 GVRP PDU 的方式，设备可以在各端口上通告端口的 VLAN 信息。通告的 VLAN 信息包括本机的静态配置及通过 GVRP 从其它设备上学习到的信息。

通过 GVRP，交换网内的设备可动态创建 VLAN，并且实时保持 VLAN 配置的一致性。通过在网络内部自动通告 VLAN ID，GVRP 降低了由于配置不一致而产生错误的可能性。而且，当一个设备上的 VLAN 配置发生变化时，GVRP 可以自动改变相连设备上的 VLAN 配置，从而减少用户的手工配置工作。

GARP 与 GVRP 是由下列标准定义的：

- IEEE standard 802.1D
- IEEE standard 802.1Q

14.2 配置GVRP

14.2.1GVRP 缺省配置

下表显示 GVRP 缺省配置：

功能特性	缺省值
GVRP global enable state	Disabled
GVRP dynamic creation of VLANs	Disabled
GVRP base vlan id	VLAN 1(仅在 MSTP 环境中起作用)
GVRP registration mode	Enable
GVRP applicant state	Normal, (Ports do not declare VLANs when in STP blocking state)
GVRP timers	Join Time: 200 ms Leave Time: 600 ms Leaveall Time: 10，000 ms

14.2.2 GVRP 配置指南

相互连接进行通信的两台设备都应启动 GVRP，GVRP 信息只在 Trunk Links 中传播，但传播的信息包括当前设备的所有 VLAN 信息，不管 VLAN 是动态学习的，或是手工设置的。

在运行 STP（Spanning-tree Protocol）的情况下，只有状态为 Forwarding 的端口才会参与 GVRP 的运行，如接收、发送 GVRP PDU，只有状态为 Forwarding 的端口的 VLAN 信息会被 GVRP 扩散。

所有由 GVRP 添加的 VLAN Port 都是 Tagged Port。

所有由 GVRP 动态学习的 VLAN 信息都未保存在系统中，当设备复位时，这些信息将全部丢失。用户也不可以保存这些动态学习到的 VLAN 信息。

由 GVRP 创建的动态 VLAN 的参数不能修改。

网络中所有需要交换 GVRP 信息的设备的 GVRP Timers（Join，Leave，Leaveall）必须保持一致。

14.2.3 启动 GVRP

只有在全局使能允许的情况下 GVRP 才会启动。

在 GVRP 未全局使能的状态下，其它 GVRP 参数可以进行配置，但只有在 GVRP 开始运行时，这些 GVRP 选项设置才能发生作用。

全局控制 GVRP：

命令	作用
Ruijie(config)# [**no**] **gvrp enable**	启用 GVRP(如果为关闭的话)

举例如下：

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# gvrp enable
Ruijie(config)# end
```

14.2.4 控制动态 VLAN 的创建

当一个端口接收到的信息（仅限于 Joinin Joinempty）中所指示的 VLAN 在本地设备不存在时，GVRP 可能会创建这个 VLAN。是否允许动态创建 VLAN 由用户控制。

控制创建动态 VLAN：

命令	作用
Ruijie(config)# [**no**] **gvrp dymanic-vlan-creation enable**	允许 GVRP 动态创建 VLAN (如果为关闭的话)

用户不能修改由 GVRP 创建的动态 VLAN 的参数。

举例如下：

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# gvrp dymanic-vlan-creation enable
Ruijie(config)# end
```

14.2.5 设置 GVRP 的运行 VLAN

在未运行 STP（Spanning-tree Protocol）的环境，所有可用端口都可以参与 GVRP 的运行。

在运行 SST（Single Spanning-tree）的环境中，只有在当前 SST Context 中处于 Forwarding 状态的端口才参与 GVRP 的运行。

在运行 MST（Multi Spanning-tree）的环境中，GVRP 可在 VLAN 1 所属的 Spanning-tree Context 中运行，用户不能指定其它 Spanning-tree Context。

14.2.6 配置端口的登记方式

端口有两种登记模式：

- GVRP Registration Normal
- GVRP Registration Disabled

将一个端口设置为 **normal registration** 模式，将允许动态创建（如果 Dynamic VLAN Creation Enabled）、登记或注销端口上的 VLAN。

当端口设置为 **disabled registration** 模式时，禁止任何动态登记或注销 VLAN 的行动。

设置端口的 GVRP Registration Mode：

命令	作用
Ruijie(config-if)# [**no**] **gvrp registration mode {normal | disabled}**	设置端口的 GVRP 登记模式

这两种登记模式不会影响端口上的静态 VLAN，用户创建的静态 VLAN 永远都是 Fixed Registrar。

打开端口 1 的 Registration Mode 的示例：

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# gvrp registration mode enable normal
Ruijie(config-if)# end
```

14.2.7 配置端口的通告模式

端口有两种通告模式，控制端口是否发送 GVRP 通告。

- GVRP Normal Applicant

允许在端口上通告本端口的 VLAN，包括所有动态及静态 VLAN。

- GVRP Non-Applicant

禁止在端口上通告本端口的 VLAN。

设置端口的通告模式：

命令	作用
Ruijie(config-if)# [**no**] **gvrp applicant state** {**normal** | **non-applicant**}	设置端口的 GVRP 通告模式

设置端口 1 的 Applicant State 的示例：

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# gvrp applicant state normal
Ruijie(config-if)# end
```

14.2.8 设置 GVRP 定时器

GVRP 中使用了三个定时器：

- Join Timer

Join Timer 控制端口发出通告前的最大时延，实际发送间隔在 0 到这个最大时延之间。缺省值是 200ms。

- Leave Timer

Leave Timer 控制端口在接收到 Leave Message 后，将端口从 VLAN 中删除前所要等待的时间，如果在这个时间段内端口重新收到 Join Message，则端口的 VLAN 成员关系仍然保留，同时定时器失效；如果在定时器超时前仍未收到 Join Message，则端口的状态变为 Empty，端口从 VLAN 成员表中删除。缺省值是 600ms。

- LeaveAll Timer

LeaveAll Timer 控制在端口上发送 LeaveAll Message 的最小间隔，如果在定时器超时前端口收到 LeaveAll Message，则定时器开始重新计时；如果定时器超时，则在端口上发送 LeaveAll Message，LeaveAll Message 同时也发送给端口本身，从而触发 Leave Timer 也开始计数。缺省值是 10，000ms。实际发送间隔在 Leaveall 与 Leaveall + Join 之间。

设置定时器时，必须保证 Leave Value 大于或等于三倍的 Join Value(Leave >= Join * 3)，同时 Leaveall 必须大于 Leave(Leaveall > Leave)。 如果不能满足以上条件，设置定时器操作将返回失败。例如，如果在设置 Leave

Timer 为 600ms 后，设置 Join Timer 为 320ms 将会显示出错提示。要使操作成功，当 Join Timer 为 350ms 时，Leave Timer 要不小于 1050ms。

在实际组网中，建议用户将 GVRP 定时器配置为以下的推荐值：

Join Timer：6000ms（6 秒钟）；

Leave Timer：30000ms（30 秒钟）；

LeaveAll Timer：120000ms（2 分钟）。

定时器设置的有效粒度是 10ms。

要保证所有互联的 GVRP 设备中的 GVRP Timer 设置保持一致，否则 GVRP 可能工作异常。

调整 GVRP Timer 的数值：

命令	作用
Ruijie(config)# [**no**] **gvrp timer** {**join** | **leave** | **leaveall**} *timer-value*	设置端口的定时器值

设置 GVRP Join Timer 的示例：

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# gvrp timer join 1000
Ruijie(config)# end
```

14.2.9 显示 GVRP 的配置和状态

显示 GVRP 的统计值

GVRP 的统计值是以端口为单位计算的，显示统计值命令的详细使用方法及各项统计值的含义请参照命令行接口 **show gvrp statistics**。

显示端口的 GVRP 统计值：

命令	作用
Ruijie# **show gvrp statistics** {*interface-id* | **all**}	显示端口的统计值

显示 GVRP 统计值的示例：

```
Ruijie# show gvrp statistics gigabitethernet 1/1
Interface  GigabitEthernet 3/1
RecValidGvrpPdu    0
RecInvalidGvrpPdu   0
RecJoinEmpty    0
RecJoinIn       0
```

```
RecEmpty        0
RecLeaveEmpty   0
RecLeaveIn      0
RecLeaveAll     0
SentGvrpPdu     0
SentJoinEmpty   0
SentJoinIn      0
SentEmpty       0
SentLeaveEmpty  0
SentLeaveIn     0
SentLeaveAll    0
JoinIndicated   0
LeaveIndicated  0
JoinPropagated  0
LeavePropagated  0
```

清除 GVRP 的统计值，使其重新开始计数：

命令	作用
Ruijie# **clear gvrp statistics** {*interface-id* | **all**}	清除端口的统计值

清除端口一上 GVRP 统计值的示例：

```
Ruijie# clear gvrp statistics gigabitethernet 1/1
```

显示 GVRP 的运行状态

GVRP 的当前运行状态可通过 **show gvrp status** 命令来察看。这条命令可以显示当前的动态创建的 VLAN，及静态 VLAN 的动态逻辑端口。

命令	作用
Ruijie# **show gvrp status**	显示当前 GVRP 的运行状态

举例如下：

```
Ruijie# show gvrp status
VLAN 1
Dynamic Ports:
DVLAN 5
Dynamic Ports:
Port:GigabitEthernet 3/1
```

显示 GVRP 的当前配置

GVRP 的当前运行状态可通过 **show gvrp configuration** 命令来察看。这条命令可以显示当前的动态创建的 VLAN，及静态 VLAN 的动态逻辑端口。

命令	作用
Ruijie# **show gvrp configuration**	显示当前 GVRP 的配置状态

举例如下：

```
Ruijie# show gvrp configuration
Global GVRP Configuration:
GVRP Feature:enabled
GVRP dynamic VLAN creation:enabled
Join Timers(ms):200
Join Timers(ms):600
Join Timers(ms):10000
Port based GVRP Configuration:
Port:GigabitEthernet 3/1 app mode:normal reg mode:normal
Port:GigabitEthernet 3/2 app mode:normal reg mode:normal
Port:GigabitEthernet 3/3 app mode:normal reg mode:normal
Port:GigabitEthernet 3/4 app mode:normal reg mode:normal
Port:GigabitEthernet 3/5 app mode:normal reg mode:normal
Port:GigabitEthernet 3/6 app mode:normal reg mode:normal
Port:GigabitEthernet 3/7 app mode:normal reg mode:normal
Port:GigabitEthernet 3/8 app mode:normal reg mode:normal
Port:GigabitEthernet 3/9 app mode:normal reg mode:normal
Port:GigabitEthernet 3/10 app mode:normal reg mode:normal
Port:GigabitEthernet 3/11 app mode:normal reg mode:normal
Port:GigabitEthernet 3/12 app mode:normal reg mode:normal
```

15 LLDP

15.1 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。

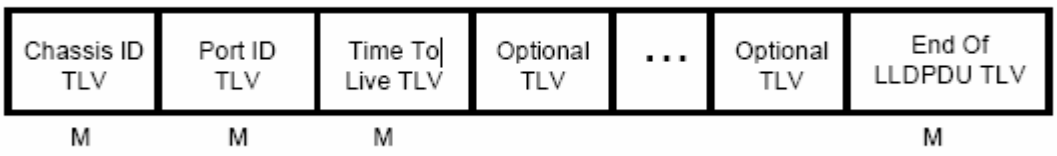
通过 LLDP，网络管理系统可以掌握拓扑的连接情况，比如设备的哪些端口与其它设备相连接，链路连接两端的端口的速率、双工是否匹配等，管理员可以根据这些信息快速地定位及排查故障。

15.1.1 基本概念

LLDPDU

LLDPDU 是指封装在 LLDP 报文中的协议数据单元，它由一系列的 TLV 封装而成。这些 TLV 集合包括了三个固定的 TLV 加上一系列可选的 TLVs 和一个 End Of TLV 组成。LLDPDU 的具体格式如图所示：

图 15-1 LLDPDU 格式



其中：

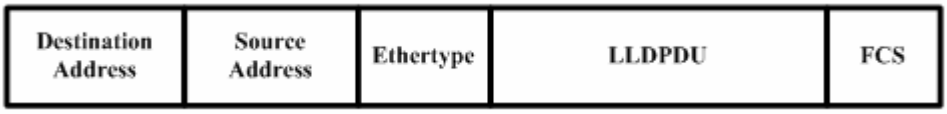
- M 表示是固定的 TLV。
- 在 LLDPDU 中，Chassis ID TLV、Port ID TLV、Time To Live TLV 和 End Of LLDPDU TLV 是必须携带的，而其它类型的 TLV 是可选携带。

LLDP 报文封装格式

LLDP 报文支持两种封装格式：Ethernet II 和 SNAP（Subnetwork Access Protocols，子网访问协议）。

其中 Ethernet II 格式封装的 LLDP 报文如图所示：

图 15-2 Ethernet II 格式封装的 LLDP 报文

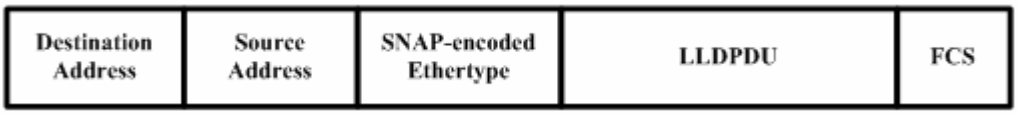


其中：

- Destination Address：目的 MAC 地址，为 LLDP 的组播地址 01-80-C2-00-00-0E。
- Source Address：源 MAC 地址，为设备的二层 MAC 地址。
- Ethertype：以太网类型，为 0x88CC。
- LLDPDU：LLDP 协议数据单元。
- FCS：帧校验序列。

SNAP 格式封装的 LLDP 报文如图所示：

图 15-3 SNAP 格式封装的 LLDP 报文



其中：

- Destination Address：目的 MAC 地址，为 LLDP 的组播地址 01-80-C2-00-00-0E。
- Source Address：源 MAC 地址，为设备的二层 MAC 地址。
- SNAP-encoded Ethertype：SNAP 封装的以太网类型，为 AA-AA-03-00-00-00-88-CC.。
- LLDPDU：LLDP 协议数据单元。
- FCS：帧校验序列。

TLV

LLDPDU 中封装的 TLV 可以分成二个大类：

- 基本管理 TLV
- 组织定义 TLV

基本管理 TLV 是一组用于网络管理的基础 TLV 集合。组织定义 TLV 是由标准组织和其它机构定义的 TLV，比如 IEEE 802.1 组织、IEEE 802.3 组织分别定义了各自的 TLV 集合。

3) 基本管理 TLV

基本管理 TLV 集合包含了两种类型的 TLV：固定 TLV 和可选 TLV。固定 TLV 是指该 TLV 信息必须包含在 LLDPDU 中发布，可选 TLV 是指根据需要确定 TLV 是否包含在 LLDPDU 中发布。

基本管理 TLV 的内容见表：

TLV 类型	TLV 说明	在 LLDPDU 中用法
End Of LLDPDU TLV	LLDPDU 的结束标志，占用 2 个字节	固定
Chassis ID TLV	用于标识设备，通常用 MAC 地址表示	固定
Port ID TLV	用于标识发送 LLDPDU 的端口	固定
Time To Live TLV	本地信息在邻居设备上的存活时间，当收到 TTL 为 0 的 TLV 时，此时需要删除掉对应的邻居信息。	固定
Port Description TLV	发送 LLDPDU 的端口描述符	可选
System Name TLV	描述设备的名称	可选
System Description TLV	设备描述信息，包括硬件/软件版本、操作系统等信息	可选
System Capabilities TLV	描述设备的主要功能，例如桥接、路由、中继等功能	可选
Management Address TLV	管理地址，同时包含了接口号和 OID（Object Identifier，对象标识）。	可选

☑ 锐捷交换机系列产品 LLDP 协议支持基本管理 TLV 的发布。

4) 组织定义 TLV

不同的组织（例如 IEEE 802.1、IEEE 802.3、IETF 或者设备供应商）定义特定的 TLV 信息去通告设备的特定信息。TLV 格式中通过 OUI（Organizationally Unique Identifier，组织唯一标识符）字段来区分不同的组织。

组织定义 TLV 属于可选的 TLV 集合，根据用户的实际需要在 LLDPDU 中发布。目前比较常见的组织定义 TLV 有以下三种：

5) IEEE 802.1 组织定义的 TLV

IEEE 802.1 组织定义的 TLV 见表：

TLV 类型	TLV 说明
Port VLAN ID TLV	端口的 VLAN 标识符
Port And Protocol VLAN ID TLV	端口的协议 VLAN 标识符
VLAN Name TLV	端口的 VLAN 名称
Protocol Identity TLV	端口支持的协议类型

☑ 锐捷交换机系列产品 LLDP 协议，不支持发送 Protocol Identity TLV，但支持接收该类型的 TLV。

6) IEEE 802.3 组织定义的 TLV

IEEE 802.3 组织定义的 TLV 见表：

TLV 类型	TLV 说明
MAC/PHY Configuration//Status TLV	端口的速率双工状态、是否支持并使能自动协商功能
Power Via MDI TLV	端口的供电能力
Link Aggregation TLV	端口的链路聚合能力及当前的聚合状态
Maximum Frame Size TLV	端口所能传输的最大的帧的大小

☑ 锐捷交换机系列产品 LLDP 协议支持 IEEE 802.3 组织定义的 TLV 的发布。

7) LLDP-MED TLV

LLDP-MED 以 IEEE 802.1AB LLDP 协议为基础，它扩展了 LLDP，使用户能够更方便地部署 VoIP（Voice Over IP，基于 IP 的语音传输）网络及进行故障检测。它提供了网络配置策略、设备发现、以太网供电管理和目录管理等应用，满足了节约成本、有效地管理和易于部署方面的需求，简化了语音设备地部署。

LLDP-MED 定义的 TLV 见表：

TLV 类型	TLV 说明
LLDP-MED Capabilities TLV	设备是否支持 LLDP-MED、LLDPDU 中封装的 LLDP-MED TLV 类型以及当前设备的类型（网络连接设备或终端）
Network Policy TLV	通告端口的 VLAN 的配置、支持的应用类型（如语音或视频）、二层的优先级信息等
Location Identification TLV	定位标识终端设备。在网络拓扑收集等应用中能够精确地定位出终端设备
Extended Power-via-MDI TLV	提供了更高级的供电管理
Inventory – Hardware Revision TLV	MED 设备的硬件版本
Inventory – Firmware Revision TLV	MED 设备的固件版本
Inventory – Software Revision TLV	MED 设备的软件版本
Inventory – Serial Number TLV	MED 设备的序列号
Inventory – Manufacturer Name TLV	MED 设备的制造商的名称
Inventory – Model Name TLV	MED 设备的模块名称
Inventory – Asset ID TLV	MED 设备的资产标识符，用于目录管理和资产跟踪

☑ 锐捷交换机系列产品 LLDP 协议支持 LLDP-MED 定义的 TLV 的发布。

15.1.2 工作原理

LLDP 工作模式

LLDP 提供了三种工作模式：

- TxRx：即发送也接收 LLDPDU。
- Rx Only：只接收不发送 LLDPDU。
- Tx Only：只发送不接收 LLDPDU。

当端口的 LLDP 工作模式发生变化时，端口将对协议状态机进行初始化操作，通过配置端口初始化的延迟时间，可以避免由于工作模式频繁改变而导致端口不断地进行初始化操作。

LLDP 报文的传输机制

LLDP 工作在 TxRx 或 Tx Only 模式时，会周期性的发送 LLDP 报文。当本地设备的信息发生变化时，会立即发送 LLDP 报文。为了避免本地信息的频繁变化引起的频繁发送 LLDP 报文，在发送完一个 LLDP 报文后需要延迟一定的时间后再发往下一个 LLDP 报文。该延迟时间可以手工配置。
LLDP 提供了两种报文类型：

- 标准 LLDP 报文：包含了本地设备的管理和配置信息。
- Shutdown 通告报文：当取消了 LLDP 的传输模式或者端口被管理 Shutdown 时，将触发 LLDP Shutdown 通告报文的发送。Shutdown 通告报文由 Chassis ID TLV、Port ID TLV、Time To Live TLV 和 End OF LLDP TLV 组成。其中 Time To Live TLV 中 TTL 等于 0。当设备收到 LLDP Shutdown 通告报文时，将认为邻居信息已经不再有效并立即删除邻居信息。

当 LLDP 工作模式由关闭或 Rx 转变为 TxRx 或 Tx，或者发现新邻居时（即收到新的 LLDP 报文且本地尚未保存该邻居信息），为了让邻居设备尽快学习到本设备的信息，将启动快速发送机制。快速发送机制调整 LLDP 报文的发送周期为 1 秒，并连续发送一定数量的 LLDP 报文。

LLDP 报文的接收机制

LLDP 工作在 TxRx 或 RxOnly 模式时，能够接收 LLDP 报文。当设备收到 LLDP 报文时，会进行有效性检查。通过报文校验后，判断是新的邻居信息还是已经存在的邻居信息更新，并将邻居信息保存在本地设备。同时根据报文中 TTL TLV 的值设置邻居信息在本地设备的存活时间。如果收到 TTL TLV 的值为 0，表示需要立即老化掉该邻居信息。

15.1.3 协议规范

LLDP 相关的协义规范和标准有：

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

15.2 配置LLDP基本功能

- （可选）使能LLDP
- （可选）配置LLDP工作模式
- （可选）配置允许发布的TLV类型
- （可选）配置LLDP报文中发布管理地址
- （可选）配置快速发送LLDP报文的个数
- （可选）配置TTL乘数和LLDP报文发送时间间隔
- （可选）配置LLDP报文的发送延迟时间
- （可选）配置端口初始化的延迟时间

- （可选）配置LLDP Trap功能
- （可选）配置LLDP错误检测功能
- （可选）配置LLDP报文封装格式
- （可选）配置 LLDP Network Policy 策略
- （可选）配置设备的普通地址信息
- （可选）配置设备的紧急电话号码信息
- 查看配置

15.2.1 缺省配置

下表用来描述 LLDP 的缺省配置。

功能特性	缺省值
全局使能 LLDP	缺省打开
端口使能 LLDP	缺省打开
LLDP 工作模式	TxRx
端口初始化的延迟时间	2 秒
LLDP 报文发送间隔	30 秒
LLDP 报文发送延迟时间	2 秒
邻居信息超时时间	120 秒
LLDP 报文封装格式	Ethernet II
使能 LLDP Trap	缺省关闭
LLDP 错误检测功能	缺省打开

15.2.2 使能 LLDP

缺省情况下，LLDP 全局开关处于打开状态，且接口使能 LLDP。全局和接口上均开启 LLDP 功能时，接口上的 LLDP 功能才生效。

按以下步骤关闭 LLDP 全局开关和接口的 LLDP 功能。

命令	作用
Ruijie(config)#**no lldp enable**	关闭全局的 LLDP 开关
Ruijie(config)# **interface** *interface-name*	进入接口配置模式。LLDP 运行在实际的物理接口上（对于 AP 口，则实际是运行在 AP 成员口上）。堆叠口，VSL 口不支持 LLDP。
Ruijie(config-if)#**no lldp enable**	关闭接口的 LLDP
Ruijie(config-if)#**show lldp status**	显示 LLDP 的状态信息

如果要重新打开全局和端口的 LLDP 开关，可以使用 **lldp enable** 命令。

全局关闭 LLDP 开关，将使设备的 LLDP 功能失效。同时，设备会发送 Shutdown 通告报文通知邻居设备将对应的 LLDP 信息删除。

端口学习到的邻居个数限制在 5 个，即端口最多只能学习到 5 个邻居。

如果邻居设备不支持 LLDP，但是邻居设备下连的设备支持 LLDP，由于邻居设备可能会转发 LLDP 的报文，这样，端口可能会学习到非直连的设备的信息。

配置举例：

关闭全局的 LLDP 开关并显示 LLDP 的状态信息。

```
Ruijie(config)#no lldp enable
Ruijie(config)#show lldp status
Global status of LLDP: Disable
```

15.2.3 配置 LLDP 工作模式

缺省情况下，接口的 LLDP 功能处于打开状态，且缺省工作在 TxRx 模式，用户可根据实际需要将工作模式修改为 Tx 或 Rx 模式。按以下步骤配置 LLDP 工作模式。

命令	作用
Ruijie(config)# **interface** *interface-name*	进入接口配置模式。LLDP 运行在实际的物理接口上（对于 AP 口，则实际是运行在 AP 成员口上）。堆叠口，VSL 口不支持 LLDP。
Ruijie(config-if)#**lldp mode** { **tx** | **rx** | **txrx** }	配置 LLDP 工作模式。可配置的工作模式为 tx、rx、txrx。
Ruijie(config-if)#**show lldp status interface** *interface-name*	显示接口的 LLDP 状态信息

配置举例：

配置接口上的 LLDP 工作模式为 Tx，并查看接口的 LLDP 状态信息

```
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#lldp mode tx
Ruijie(config-if-GigabitEthernet 0/1)#show lldp status interface gigabitethernet 0/1
Port [GigabitEthernet 0/1]
Port status of LLDP             : Enable
Port state                      : UP
Port encapsulation              : Ethernet II
Operational mode                : TxOnly
Notification enable             : NO
Error detect enable             : YES
Number of neighbors             : 0
```

```
Number of MED neighbors          : 0
```

15.2.4 配置允许发布的 TLV 类型

缺省情况下，接口上允许发布除 Location Identification TLV 之外的所有类型的 TLV。按以下步骤配置接口允许发布的 TLV 类型。

命令	作用
Ruijie(config)# **interface** *interface-name*	进入接口配置模式。LLDP 运行在实际的物理接口上（对于 AP 口，则实际是运行在 AP 成员口上）。堆叠口，VSL 口不支持 LLDP。
Ruijie(config-if)# **lldp tlv-enable** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** | **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] } | **dot3-tlv** { **all** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **location** { **civic-location** | **elin** } **identifier** *id* | **network-policy profile** [*profile-num*] | **power-over-ethernet** } }	缺省情况下，接口上允许发布除 Location Identification TLV 之外的所有类型的 TLV
Ruijie(config-if)# **show lldp tlv-config interface** *interface-name*	显示指定接口允许发布的 TLV 属性

- 配置基本管理 TLV、IEEE 802.1 组织定义 TLV、IEEE 802.3 组织定义 TLV 时，如果指定 **all** 参数，将发布该类型的所有可选 TLV。
- 配置 LLDP-MED TLV 时，如果指定 **all** 参数，将发布除 Location Identification TLV 之外的所有类型的 LLDP-MED TLV。
- 配置允许发布 LLDP-MED Capability TLV 时，需要先配置允许发布 LLDP 802.3 MAC/PHY TLV；取消发布 LLDP 802.3 MAC/PHY TLV 时，需要先取消发布 LLDP-MED Capability TLV。
- 配置 LLDP-MED TLV 时，必须先配置允许发布 LLDP-MED Capability TLV，才可以配置允许发布 LLDP-MED 其它类型的 TLV。
- 取消发布 LLDP-MED TLV，必须先取消发布 LLDP-MED 其它类型的 TLV，才允许取消发布 LLDP-MED Capability TLV。
- 关于 lldp tlv-enable 命令的各关键字的含义，请参见 LLDP 配置指导中的描述。
- 当设备下联 IP 电话，若 IP 电话支持 LLDP-MED，则可以通过配置 network policy TLV 下发策略给 IP 电话。

配置举例：

#配置取消发布 IEEE 802.1 组织定义的 Port And Protocol VLAN ID TLV。

```
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#no lldp tlv-enable dot1-tlv protocol-vlan-id
Ruijie(config-if-GigabitEthernet 0/1)#show lldp tlv-config interface gigabitethernet 0/1
LLDP tlv-config of port [GigabitEthernet 0/1]
               NAME                  STATUS DEFAULT
------------------------------ ------ -------
Basic optional TLV:
Port Description TLV              YES    YES
System Name TLV                    YES    YES
System Description TLV            YES    YES
System Capabilities TLV           YES    YES
Management Address TLV            YES    YES

IEEE 802.1 extend TLV:
Port VLAN ID TLV                   YES    YES
Port And Protocol VLAN ID TLV    NO     YES
VLAN Name TLV                        YES    YES

IEEE 802.3 extend TLV:
MAC-Physic TLV                       YES    YES
Power via MDI TLV                  YES    YES
Link Aggregation TLV               YES    YES
Maximum Frame Size TLV             YES    YES

LLDP-MED extend TLV:
Capabilities TLV                     YES    YES
Network Policy TLV                   YES    YES
Location Identification TLV       NO     NO
Extended Power via MDI TLV        YES    YES
Inventory TLV                          YES    YES
```

15.2.5 配置 LLDP 报文中发布管理地址

管理地址是提供给网络管理系统用于标识某台网络设备并能进行管理的地址。缺省情况下，在 LLDP 报文中发布管理地址，发布的管理地址为接口允许通过的最小 VLAN 的 IPv4 地址。

按以下步骤配置 LLDP 报文中发布管理地址：

命令	作用
Ruijie(config)# **interface** *interface-name*	进入接口配置模式。LLDP 运行在实际的物理接口上（对于 AP 口，则实际是运行在 AP 成员口上）。堆叠口，VSL 口不支持 LLDP。

Ruijie(config-if)#**lldp management-address-tlv** [*ip-address*]	配置 LLDP 报文中发布的管理地址
Ruijie(config-if)#**show lldp local-information interface** *interface-name*	显示指定接口的 LLDP 本地信息

缺省情况下，LLDP 报文发布管理地址。发布的管理地址为端口允许通过的最小 VLAN 的 IPv4 地址，如果该 VLAN 未配置 IPv4 地址，则继续查找下一个允许通过的最小 VLAN，直到找到 IPv4 地址为止。

如果未找到 IPv4 地址，则查找端口允许通过的最小 VLAN 的 IPv6 地址。

如果仍未找到 IPv6 地址，则采用本机地址 127.0.0.1 作为管理地址发布。

配置举例：

配置 LLDP 报文发布的管理地址为 192.168.1.1 并查看相应的配置信息。

```
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#lldp management-address-tlv 192.168.1.1
Ruijie(config-if-GigabitEthernet 0/1)#show  lldp local-information interface GigabitEthernet 0/1
Lldp local-information of port [GigabitEthernet 0/1]
  Port ID type                      : Interface name
  Port id                           : GigabitEthernet 0/1
  Port description                  :

  Management address subtype        : ipv4
  Management address                : 192.168.1.1
  Interface numbering subtype       : ifIndex
  Interface number                  : 0
  Object identifier                 :

  802.1 organizationally information
  Port VLAN ID                      : 1
  Port and protocol VLAN ID(PPVID)  : 1
      PPVID Supported               : YES
      PPVID Enabled                 : NO
  VLAN name of VLAN 1               : VLAN0001
  Protocol Identity                 :

  802.3 organizationally information
  Auto-negotiation supported        : YES
  Auto-negotiation enabled          : YES
  PMD auto-negotiation advertised   : 1000BASE-T full duplex mode, 100BASE-TX full duplex mode,
100BASE-TX half duplex mode, 10BASE-T full duplex mode, 10BASE-T half duplex mode
  Operational MAU type              : speed(100)/duplex(Full)
  PoE support                       : NO
```

```
Link aggregation supported        : YES
Link aggregation enabled          : NO
Aggregation port ID               : 0
Maximum frame Size                : 1500

LLDP-MED organizationally information
Power-via-MDI device type         : PD
Power-via-MDI power source        : Local
Power-via-MDI power priority      :
Power-via-MDI power value         :
Model name                        : Model name
```

15.2.6 配置快速发送 LLDP 报文的个数

当发现新的邻居，或者 LLDP 工作模式从关闭或 Rx 转变为 TxRx 或 Tx 时，为了让邻居设备尽快地学习到本设备的信息，将启动快速发送机制，快速发送机制缩短 LLDP 报文的发送周期为 1 秒，并连续发送一定数量的 LLDP 报文后再恢复正常的发送周期。

命令	作用
Ruijie(config)#**lldp fast-count** *count*	配置快速发送 LLDP 报文的个数，缺省为 3 个，可配置的范围为 1-10
Ruijie(config-if)#**show lldp status**	显示 LLDP 状态信息

配置举例：

配置快速发送 LLDP 报文的个数为 5 个。

```
Ruijie(config)#lldp fast-count 5
Ruijie(config)#show lldp status
Global status of LLDP                 : Enable
Neighbor information last changed time :
Transmit interval                     : 30s
Hold multiplier                       : 4
Reinit delay                          : 2s
Transmit delay                        : 2s
Notification interval                 : 5s
Fast start counts                     : 5
```

15.2.7 配置 TTL 乘数和 LLDP 报文发送时间间隔

LLDP 报文中 Time To Live TLV 的值=TTL 乘数×报文发送时间间隔+1。因此，通过调整 TTL 乘数可以控制本设备信息在邻居设备的存活时间。

而通过调整 LLDP 报文发送时间间隔，可以调整 LLDP 报文的发送周期。按以下步骤配置 TTL 乘数和 LLDP 报文的发送时间间隔：

命令	作用
Ruijie(config)#**lldp hold-multiplier** *value*	配置 TTL 乘数，缺省值为 4，可配置的范围为 2-10
Ruijie(config)#**lldp timer tx-interval** *seconds*	配置发送 LLDP 报文的时间间隔。缺省发送时间间隔为 30 秒，可配置的范围为 5-32768 秒
Ruijie(config-if)#**show lldp status**	显示 LLDP 状态信息

配置举例：

配置 TTL 乘数为 3，LLDP 报文的发送间隔为 20 秒，此时，本地设备信息在邻居设备的存活时间为 61 秒。

```
Ruijie(config)#lldp hold-multiplier 3
Ruijie(config)#lldp timer tx-interval 20
Ruijie(config)#show lldp status
Global status of LLDP                 : Enable
Neighbor information last changed time :
Transmit interval                     : 20s
Hold multiplier                       : 3
Reinit delay                          : 2s
Transmit delay                        : 2s
Notification interval                 : 5s
Fast start counts                     : 3
```

15.2.8 配置 LLDP 报文的发送延迟时间

当本地信息发生变化时，会立即向邻居设备发送 LLDP 报文。为了避免本地信息频繁变化引起的频繁地发送 LLDP 报文，可以配置 LLDP 报文的发送延迟时间来限制 LLDP 报文的频繁发送。缺省的发送延迟时间为 2 秒，按以下步骤配置 LLDP 报文的发送延迟时间：

命令	作用
Ruijie(config)#**lldp timer tx-delay** *seconds*	配置发送 LLDP 报文的延迟时间
Ruijie(config)#**show lldp status**	显示 LLDP 状态信息

配置举例：

配置发送 LLDP 报文的延迟时间为 3 秒，同时查看 LLDP 状态信息。

```
Ruijie(config)#lldp timer tx-delay 3
Ruijie(config)#show lldp status
Global status of LLDP                 : Enable
Neighbor information last changed time :
Transmit interval                     : 30s
Hold multiplier                       : 4
```

```
Reinit delay                          : 2s
Transmit delay                        : 3s
Notification interval                 : 5s
Fast start counts                     : 3
```

15.2.9 配置端口初始化的延迟时间

当端口的工作模式发生变化时，端口将对协议状态机进行初始化操作。为了避免端口的工作模式的频繁变化引起地频繁地初始化状态机，可以配置端口初始化的延迟时间。按以下步骤配置端口初始化的延迟时间：

命令	作用
Ruijie(config)#**lldp timer reinit-delay** *seconds*	配置端口初始化的延迟时间
Ruijie(config)#**show lldp status**	显示 LLDP 状态信息

配置举例：

#配置端口初始化的延迟时间为 3 秒，并显示 LLDP 的状态信息。

```
Ruijie(config)#lldp timer reinit-delay 3
Ruijie(config)#show lldp status
Global status of LLDP                 : Enable
Neighbor information last changed time :
Transmit interval                     : 30s
Hold multiplier                       : 4
Reinit delay                          : 3s
Transmit delay                        : 2s
Notification interval                 : 5s
Fast start counts                     : 3
```

15.2.10配置 LLDP Trap 功能

通过配置 Trap 功能，可以将本地设备的 LLDP 信息（例如发现新邻居、检测到与邻居的通信链路故障等信息）发送给网管服务器，管理员可以根据此信息监控网络的运行状况。

同时为了防止 LLDP Trap 信息地频繁发送，可以配置发送 LLDP Trap 的时间间隔。在这段时间间隔内，检测到 LLDP 信息变化，将发送 Trap 给网管服务器。

缺省情况下，LLDP Trap 功能处于关闭状态。

按以下步骤可配置 LLDP Trap 功能：

命令	作用
Ruijie(config)#**lldp timer notification-interval** *seconds*	配置发送 LLDP Trap 信息的时间间隔，缺省的时间间隔是 5 秒，可配置的范围是 5-3600

Ruijie(config)# **interface** *interface-name*	进入接口配置模式。LLDP 运行在实际的物理接口上（对于 AP 口，则实际是运行在 AP 成员口上）。堆叠口，VSL 口不支持 LLDP。
Ruijie(config-if)#**lldp notification remote-change enable**	使用 LLDP Trap 功能，缺省情况下，LLDP Trap 功能处于关闭状态。
Ruijie(config-if)#**show lldp status**	显示 LLDP 状态信息

配置举例：

#使能 LLDP Trap 功能，并配置 LLDP Trap 信息的发送时间间隔为 10 秒。

```
Ruijie(config)#lldp timer notification-interval 10
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#lldp notification remote-change enable
Ruijie(config-if-GigabitEthernet 0/1)#show lldp status
Global status of LLDP                 : Enable
Neighbor information last changed time :
Transmit interval                     : 30s
Hold multiplier                       : 4
Reinit delay                          : 2s
Transmit delay                        : 2s
Notification interval                 : 10s
Fast start counts                     : 3
------------------------------------------------------------
Port [GigabitEthernet 0/1]
------------------------------------------------------------
Port status of LLDP             : Enable
Port state                      : UP
Port encapsulation              : Ethernet II
Operational mode                : RxAndTx
Notification enable             : YES
Error detect enable             : YES
Number of neighbors             : 0
Number of MED neighbors         : 0
```

15.2.11配置 LLDP 错误检测功能

配置 LLDP 错误检测功能，错误检测包括链路两端的 VLAN 配置检测、端口状态检测、端口聚合配置检测、MTU 配置检测及环路检测。当 LLDP 检测到错误时，将打印 LOG 信息提示管理员。

按以下步骤配置 LLDP 错误检测功能：

命令	作用

Ruijie(config)# **interface** *interface-name*	进入接口配置模式。LLDP 运行在实际的物理接口上（对于 AP 口，则实际是运行在 AP 成员口上）。堆叠口，VSL 口不支持 LLDP。
Ruijie(config-if)#**lldp error-detect**	配置 LLDP 错误检测功能，缺省情况下，LLDP 错误检测功能打开。
Ruijie(config-if)#**show lldp status interface** *interface-name*	显示接口的 LLDP 状态信息

配置举例：

#配置 LLDP 错误检测功能。

```
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#lldp error-detect
Ruijie(config-if-GigabitEthernet 0/1)#show lldp status interface gigabitethernet 0/1
Port [GigabitEthernet 0/1]
Port status of LLDP             : Enable
Port state                      : UP
Port encapsulation              : Ethernet II
Operational mode                : RxAndTx
Notification enable             : NO
Error detect enable             : YES
Number of neighbors             : 0
Number of MED neighbors         : 0
```

15.2.12配置 LLDP 报文封装格式

缺省情况下，LLDP 报文采用 Ethernet II 格式封装。可配置的封装格式为 Ethernet II 和 SNAP。

配置成 Ethernet II 格式封装时，设备只能发送和接收 Ethernet II 格式的 LLDP 报文。

配置成 SNAP 格式封装时，设备只能发送和接收 SNAP 格式的 LLDP 报文。

按以下步骤配置 LLDP 报文封装格式：

命令	作用
Ruijie(config)# **interface** *interface-name*	进入接口配置模式。LLDP 运行在实际的物理接口上（对于 AP 口，则实际是运行在 AP 成员口上）。堆叠口，VSL 口不支持 LLDP。
Ruijie(config-if)#**lldp encapsulation snap**	配置 LLDP 报文封装格式为 SNAP。
Ruijie(config-if)#**show lldp status interface** *interface-name*	显示接口的 LLDP 状态信息

为了保证本地设备和邻居设备的正常通信，必须将 LLDP 报文配置成相同的封装格式。

配置举例：

#配置 LLDP 报文的封装格式为 SNAP 并查看相应的配置。

```
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#lldp encapsulation snap
Ruijie(config-if-GigabitEthernet 0/1)#show lldp status interface gigabitethernet 0/1
Port [GigabitEthernet 0/1]
Port status of LLDP             : Enable
Port state                      : UP
Port encapsulation              : Snap
Operational mode                : RxAndTx
Notification enable             : NO
Error detect enable             : YES
Number of neighbors             : 0
Number of MED neighbors         : 0
```

15.2.13配置 LLDP Network Policy 策略

缺省情况下，LLDP 报文采用无应用类型的 network policy tlv。

用户可以按以下步骤配置 network policy：

命令	作用
Ruijie(config)# **lldp network-policy profile** *profile-num*	进入 LLDP network-policy 配置模式。
Ruijie(config-lldp-network-policy)# **{ voice | voice-signaling } vlan { { *vlan-id* [cos *cvalue* | dscp *dvalue*] } | { dot1p [cos *cvalue* | dscp *dvalue*] } | none | untagged }** **no { voice | voice-signaling } vlan**	配置 LLDP network-policy 策略。

当设备下联 IP 电话，若 IP 电话支持 LLDP-MED，则可以通过配置 network policy TLV 下发策略给 IP 电话，由 IP 电话修改语音流 tag 和 QOS。在设备上，除配置上述策外，还需要配置步骤为：1.使能 voice vlan 功能，把连接 IP 电话的端口静态加入 voice vlan。2.把连接 IP 电话的端口配置为 QOS 信任口（推荐使用信任 dscp 模式）。3.如果在此端口上同时开启了 1X 认证，则还需要配置一条安全通道，允许 voice vlan 内的报文通过。若 IP 电话不支持 LLDP-MED，则必须使能 voice vlan 功能，并将话机 MAC 地址手动配置到 voice vlan OUI 列表中。

QOS 信任模式的配置方法请参见《IP QOS》章节；voice vlan 的配置方法请参见《Voice VLAN》章节；安全通道的配置方法请参见《ACL》章节。

配置举例：

#配置接口 1 发布的 LLDP 报文中 Network Policy TLV 策略为 1：voice 应用类型 vlan id 是 3，cos 是 4，dscp 是 6。

```
Ruijie#config
```

```
Ruijie(config)#lldp network-policy profile 1
Ruijie(config-lldp-network-policy)# voice vlan 3 cos 4
Ruijie(config-lldp-network-policy)# voice vlan 3 dscp 6
Ruijie(config-lldp-network-policy)#exit
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# lldp tlv-enable med-tlv network-policy profile 1
```

15.2.14配置设备的普通地址信息

用户可以按以下步骤配置设备的地址信息:

命令	作用
Ruijie(config)# **lldp location civic-location identifier** *id*	进入 LLDP Civic Address 配置模式。
Ruijie(config-lldp-civic)**# device-type** *device-type*	配置设备类型，缺省配置为交换机。
Ruijie(config-lldp-civic)# **{ country | state | county | city | division | neighborhood | street-group | leading-street-dir | trailing-street-suffix | street-suffix | number | street-number-suffix | landmark | additional-location-information | name | postal-code | building | unit | floor | room | type-of-place | postal-community-name | post-office-box | additional-code}** *ca-word*	配置 LLDP 普通地址信息。

配置举例：

#配置设备接口 1 的地址为：交换机设备，地址是国家：CH，城市：Fuzhou，邮编：350000。

```
Ruijie#config
Ruijie(config)#lldp location civic-location identifier 1
Ruijie(config-lldp-civic)# country CH
Ruijie(config-lldp-civic)# city Fuzhou
Ruijie(config-lldp-civic)# postal-code 350000
Ruijie(config-lldp-civic)# exit
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# lldp tlv-enable location civic-location identifier 1
```

15.2.15配置设备的紧急电话号码信息

用户可以按以下步骤配置设备的紧急电话号码信息：

命令	作用

Ruijie(config)# **lldp location elin identifier** *id* **elin-location** *tel-number*	配置紧急电话号码信息。

配置举例：

#配置设备接口 1 的紧急电话号码为：085285555556。

```
Ruijie#config
Ruijie(config)#lldp location elin identifier 1 elin-location 085283671111
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# lldp tlv-enable location elin identifier 1
```

15.2.16查看和清除配置

命令	作用
show lldp local-information [**global** | **interface** *interface-name*]	显示准备发给邻居的设备信息
show lldp location { **civic-location** | **elin** } { **identifier** *id* | **interface** *interface-name* | **static** }	显示本地设备的普通地址信息或者紧急电话号码信息
show lldp neighbors [**interface** *interface-name*] [**detail**]	显示该端口所连接的邻居的设备信息
show lldp network-policy profile [*profile-num*]	显示 LLDP network-policy 配置信息
show lldp statistics [**global** | **interface** *interface-name*]	显示 LLDP 统计信息
show lldp status [**interface** *interface-name*]	显示 LLDP 状态信息
show lldp tlv-config [**interface** *interface-name*]	显示可发布的可选 TLV 信息
clear lldp statistics [**interface** *interface-name*]	清除 LLDP 统计信息
clear lldp table [**interface** *interface-name*]	清除 LLDP 邻居信息

配置举例：

#显示指定端口连接的邻居设备的信息：

```
Ruijie# show lldp neighbors detail
Lldp neighbor-information of port [GigabitEthernet 0/1]
  Neighbor index                    : 1
  Device type                       : LLDP Device
  Update time                       : 12minutes 40seconds
Aging time                          : 5seconds
  Chassis ID type                   : MAC address
  Chassis id                        : 00d0.f822.33cd
  System name                       : System name
  System description               : System description
  System capabilities supported     : Repeater, Bridge, Router
  System capabilities enabled       : Repeater, Bridge, Router
```

```
  Management address subtype        : 802 mac address
  Management address                : 00d0.f822.33cd
  Interface numbering subtype       :
  Interface number                  : 0
  Object identifier                 :

  LLDP-MED capabilities             :
  Device class                      :
  HardwareRev                       :
  FirmwareRev                       :
  SoftwareRev                       :
  SerialNum                         :
  Manufacturer name                 :
  Asset tracking identifier         :

  Port ID type                      : Interface name
  Port id                           : GigabitEthernet 0/2
  Port description                  :

  802.1 organizationally information
  Port VLAN ID                      : 1
  Port and protocol VLAN ID(PPVID)  : 1
      PPVID Supported               : YES
      PPVID Enabled                 : NO
  VLAN name of VLAN 1               : VLAN0001
  Protocol Identity                 :
  802.3 organizationally information
  Auto-negotiation supported        : YES
  Auto-negotiation enabled          : YES
  PMD auto-negotiation advertised   : 1000BASE-T full duplex mode, 100BASE-TX full duplex mode,
100BASE-TX half duplex mode, 10BASE-T full duplex mode, 10BASE-T half duplex mode
  Operational MAU type              : speed(100)/duplex(Full)
  PoE support                       : NO
  Link aggregation supported        : YES
  Link aggregation enabled          : NO
  Aggregation port ID               : 0
  Maximum frame Size                : 1500

  LLDP-MED organizationally information
  Power-via-MDI device type         :
  Power-via-MDI power source        :
```

```
Power-via-MDI power priority      :
Power-via-MDI power value         :
```

关于 LLDP 显示信息的具体含义，请参见《LLDP 命令参考》中的描述。

15.3 LLDP典型配置举例

15.3.1 利用 LLDP 查看拓扑连接情况

组网需求

- 设备需求

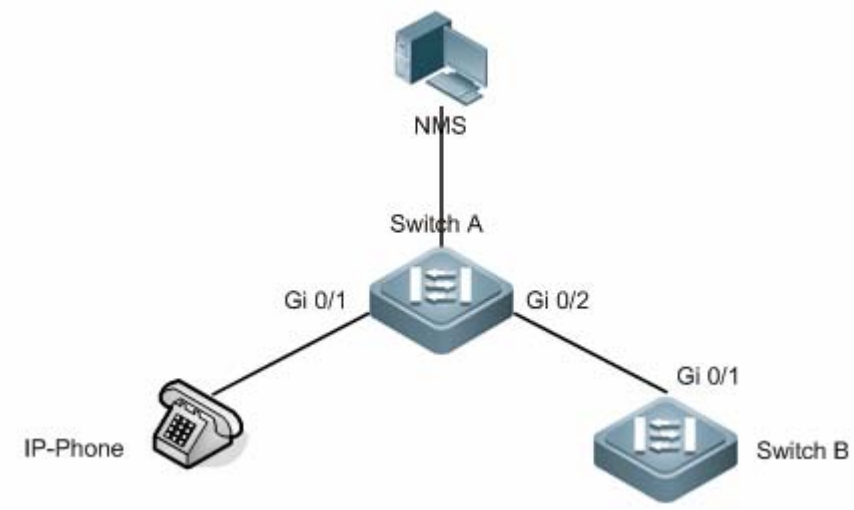
以太网交换机二台（分别以 Switch A 和 Switch B 表示）、MED 设备一台（以 IP Phone 为例）、NMS（Network Management System，网络管理系统）一台。

- 配置需求

LLDP 功能默认打开，不需要再行配置。

组网拓扑

图 15-4 LLDP 基本拓扑图



配置要点

- 端口上 LLDP 的工作模式为 TxRx。
- LLDP 报文的发送时间参数采用缺省值，即发送时间间隔为 30 秒、传输 LLDP 报文的延迟时间为 2 秒。

配置步骤

缺省情况下，LLDP 功能处于打开状态，不需要再行配置。

显示验证

- 显示 Switch A 所连接的邻居信息。

#Switch A 上显示所连接的邻居信息。

```
Ruijie# show lldp neighbors gigabitethernet 0/2
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Local Intf  Port ID  Capability   Aging-time
Gi 0/2       Gi 0/1   B,R           120

Total entries displayed: 1
```

上述信息表示交换机 A 的端口 2 连接的邻居设备的端口为 Gi 0/1，邻居具有桥接，路由功能。

#显示 Switch A 的端口 gi 0/2 连接的邻居的详细信息。

```
Ruijie# show lldp neighbors interface gigabitethernet 0/2 detail
Lldp neighbor-information of port [GigabitEthernet 0/2]
  Neighbor index                  : 1
  Device type                     : LLDP Device
Update time                      : 5minutes 39seconds
Aging time                         :  5seconds

  Chassis ID type                 : MAC address
  Chassis id                      : 00d0.f822.33cd
  System name                     : System name
  System description              : System description
  System capabilities supported   : Repeater, Bridge, Router
  System capabilities enabled     : Repeater, Bridge, Router

  Management address subtype      : 802 mac address
  Management address              : 00d0.f822.33cd
  Interface numbering subtype     :
  Interface number                : 0
  Object identifier               :
```

```
  LLDP-MED capabilities             :
  Device class                      :
  HardwareRev                       :
  FirmwareRev                       :
  SoftwareRev                       :
  SerialNum                         :
  Manufacturer name                 :
  Asset tracking identifier         :

  Port ID type                      : Interface name
  Port id                           : GigabitEthernet 0/1
  Port description                  :

  802.1 organizationally information
  Port VLAN ID                      : 1
  Port and protocol VLAN ID(PPVID)  : 1
      PPVID Supported               : YES
      PPVID Enabled                 : NO
  VLAN name of VLAN 1               : VLAN0001
  Protocol Identity                 :


  802.3 organizationally information
  Auto-negotiation supported        : YES
  Auto-negotiation enabled          : YES
  PMD auto-negotiation advertised   : 1000BASE-T full duplex mode, 100BASE-TX full duplex mode,
100BASE-TX half duplex mode, 10BASE-T full duplex mode, 10BASE-T half duplex mode
  Operational MAU type              : speed(1000)/duplex(Full
  PoE support                       : NO
  Link aggregation supported        : YES
  Link aggregation enabled          : NO
  Aggregation port ID               : 0
  Maximum frame Size                : 1500

  LLDP-MED organizationally information
  Power-via-MDI device type         :
  Power-via-MDI power source        :
  Power-via-MDI power priority      :
              Power-via-MDI power value         :
```

15.3.2 利用 LLDP 错误检测功能进行错误检测

组网需求

- 设备需求

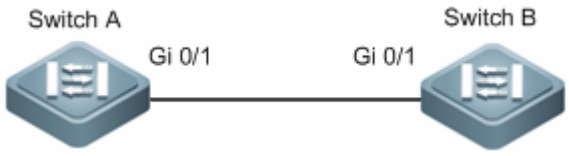
以太网交换机二台（分别以 Switch A 和 Switch B 表示）。

- 配置需求

LLDP 功能默认打开，不需要再行配置。

组网拓扑

图 15-5 LLDP 基本拓扑图



配置要点

- 端口上 LLDP 的工作模式为 TxRx。
- LLDP 报文的发送时间参数采用缺省值，即发送时间间隔为 30 秒、传输 LLDP 报文的延迟时间为 2 秒。
- LLDP 错误检测功能缺省打开，不需要再行配置。

配置步骤

交换机 A 的 gi 0/1 口配置速率为强制 100M.

```
Ruijie#configure terminal
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#speed 100
%Warning: the speed/duplex of port GigabitEthernet 0/1 may not match with it's neighbor.
```

以上信息表示端口 1 上的速率双工与相连邻居设备上的端口的速率双工不匹配。

显示验证

管理员在进行 VLAN 配置、端口速率双工配置、聚合端口配置和端口 MTU 配置时，如果配置的信息与相连接的邻居设备的配置不匹配，将提示相应的错误信息。

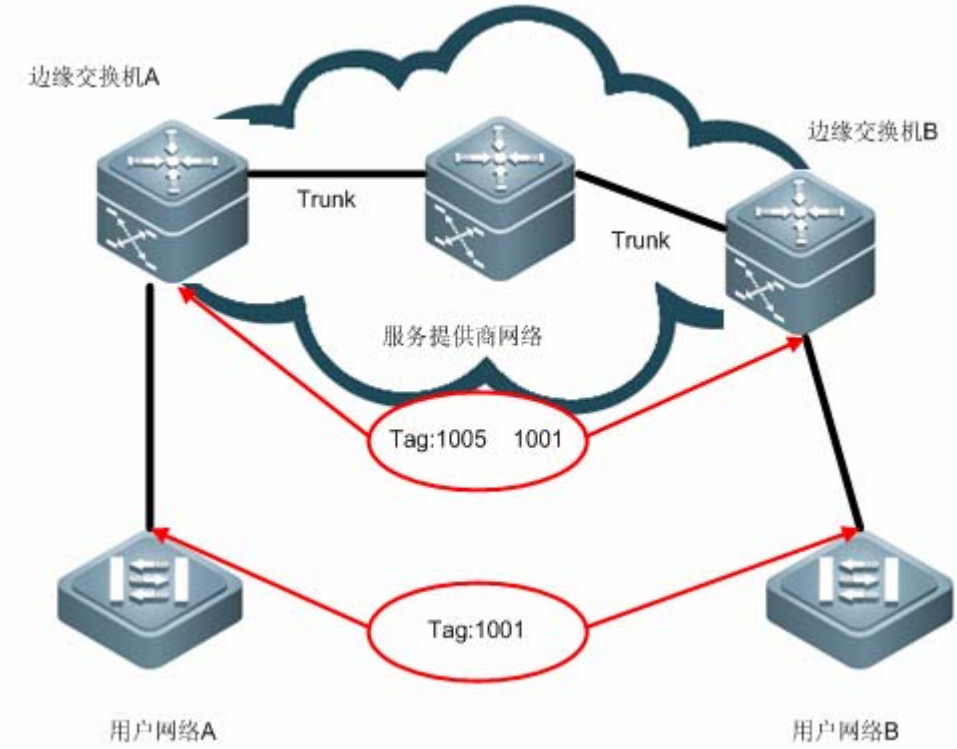
16 QinQ

16.1 QinQ概述

QinQ 其标准出自 IEEE 802.1ad，业界有多种不同的称呼，比如 dot1q-tunneling、Tag in Tag、VLAN VPN、Stack VLAN。因为 IEEE 802.1Q 中定义的 VLAN Tag 域只有 12 个比特用于表示 VLAN ID，所以设备最多只能支持 4094 个 VLAN。在城域网中需要大量的 VLAN 来隔离用户，4094 个 VLAN 远远不能满足需求。QinQ 的基本原理是在用户报文进入服务提供商网络之前封装上一个服务提供商网络的 VLAN Tag，而把用户报文中的原有的 VLAN Tag 当做数据，使报文带着两层 VLAN Tag 穿越服务提供商网络。在服务提供商网络中，报文只根据外层 VLAN Tag 传播，当用户报文离开服务提供商网络时，剥去外层 VLAN Tag，在用户网络中根据私网 VLAN Tag 传播，从而解决 VLAN 数目不足的问题。

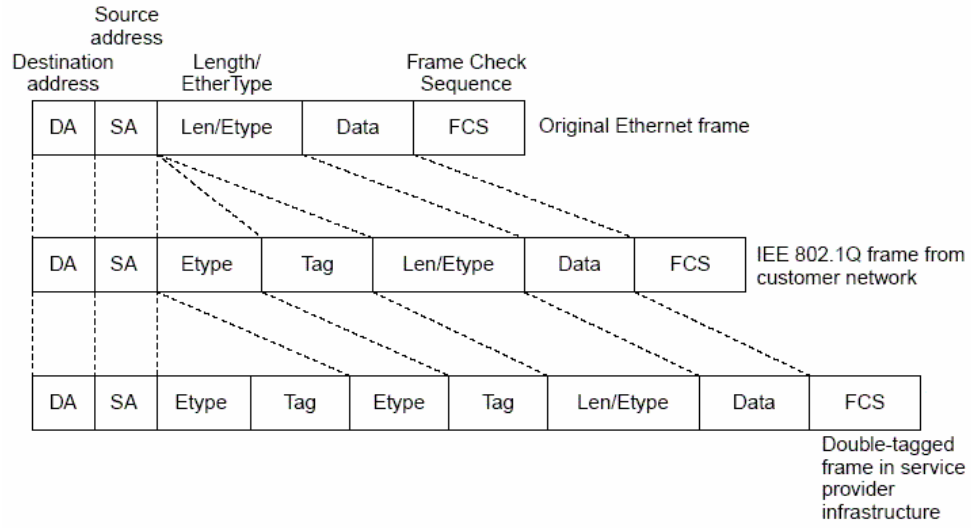
如下图所示，用户网络 A 的 VLAN 1001 的报文在进入服务提供商网络之前被添加上一层 vlan Tag 1005 的外层 Tag，使报文携带两层 Tag，在服务商网络中根据外层 Vlan Tag 1005 传播。当报文离开服务提供商网络时，外层 Vlan Tag 1005 将被剥去，报文在用户网络中仍然以 Vlan Tag 1001 进行传播。

图 16-1 QinQ 示意图



下图显示了双 Tag 添加的过程：边界设备的入口称为 dot1q-tunnel port 或简称 tunnel port，所有进入边界设备的帧都被当作是 Untagged 帧，而不管它实际上是 Untagged 还是已经带 802.1Q Tag 头的帧，都被封装上服务商的 Tag，VLAN 号为 Tunnel port 的缺省 VLAN。

图 16-2 双 Tag 报文的结构



16.1.1 基本 QinQ

基本 QinQ 是基于端口实现的。配置了 tunnel 口后，当该端口接收到报文，设备会为该报文打上 tunnel 口缺省 VLAN 的 VLAN Tag。如果接收到的是已经带有 VLAN Tag 的报文，该报文就成为双 Tag 的报文；如果接收到的是不带 VLAN Tag 的报文，该报文就成为带有端口缺省 VLAN Tag 的报文。基本 QinQ 简单，但外层 VLAN Tag 封装方式不够灵活。

16.1.2 灵活 QinQ

灵活 QinQ 可以为不同的数据流打上不同的外层 VLAN Tag：如根据用户 VLAN Tag、MAC 地址、IP 协议、源地址、目的地址、优先级、或应用程序的端口号等信息的不同，封装不同的外层 Tag。借助上述分类方法，实际实现了根据不同用户、不同业务、不同优先级等对报文进行外层 VLAN Tag 封装。

当前，在配置上可以使用的具体策略有：

- 根据内层 VLAN Tag 添加外层 VLAN Tag；
- 根据外层 VLAN Tag 修改外层 VLAN Tag；
- 根据内层 VLAN Tag 修改外层 VLAN Tag；
- 利用 ACL，根据 ACL 添加外层 VLAN Tag；
- 利用 ACL，根据 ACL 修改外层 VLAN Tag；
- 利用 ACL，根据 ACL 修改内层 VLAN Tag；

16.1.3 VLAN mapping

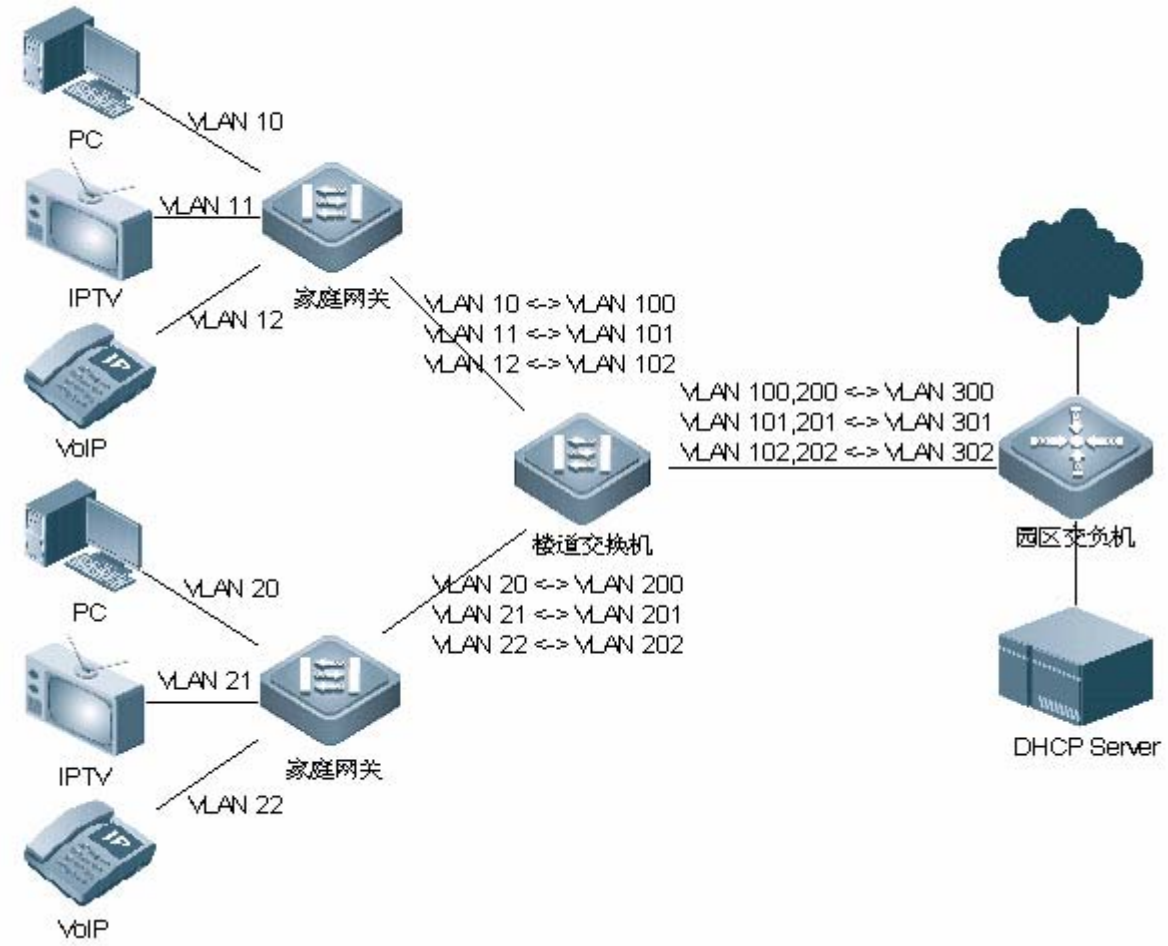
VLAN Mapping 也称为 VLAN 映射，其主要的功能是将用户报文中的私网 VLAN Tag 替换为公网的 VLAN Tag，使其按照公网的网络规划进行传输。在报文被发送回用户私网时，再按照同样的规则将 VLAN Tag 恢复为原有的用户私网 VLAN Tag，使报文正确到达目的地。VLAN mapping 支持以下两种映射关系：

- 一对一 VLAN mapping：将报文 Tag 的 VID 修改为另一个指定的 Tag 的 VID。

- 多对一 VLAN mapping：将来自多个 VLAN 的报文 Tag 的 VID 修改为同一个 Tag 的 VID。

如下图所示，1:1 VLAN MAPPING 主要用在楼道交换机处，以用不同的 VLAN 承载不同用户的相同业务，以区分不同的用户；N:1 VLAN MAPPING 主要用在园区交换机处，以用一个 VLAN 来承载原本由多个 VLAN 承载的不同用户的相同业务，以节约 VLAN 资源。

图 16-3 1:1 VLAN 映射和 N:1 VLAN 映射应用示意图



一对一 VLAN mapping 的实现方式一

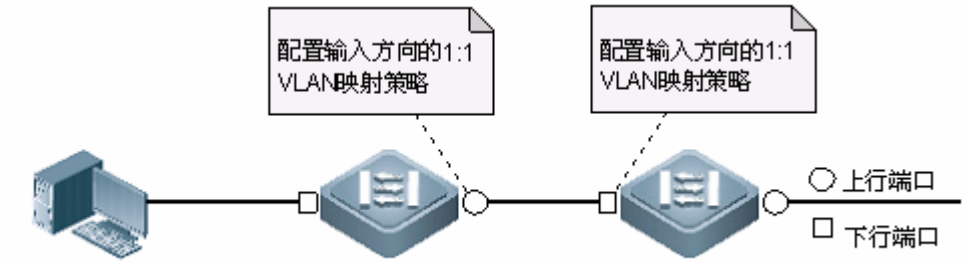
图 16-4 1:1 VLAN 映射实现方式一

- 对于上行数据流，通过在上图所示的下行端口上配置输入方向的 VLAN 映射策略，将原来的 VLAN Tag 映射为新的 VLAN Tag。

- 对于下行数据流，通过在上图所示的下行端口上配置输出方向的 VLAN 映射策略，将报文的 VLAN Tag 映射到原来的 VLAN Tag。

一对一 VLAN mapping 的实现方式二

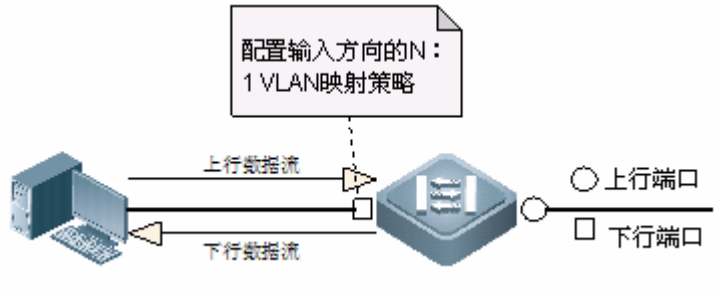
图 16-5 1:1 VLAN 映射实现方式二



- 对于上行数据流，通过在上图所示的下行端口上配置输入方向的 VLAN 映射策略，将原来的 VLAN Tag 映射为新的 VLAN Tag。
- 对于下行数据流，通过在上图所示的上行端口上配置输入方向的 VLAN 映射策略，将报文的 VLAN Tag 映射到原来的 VLAN Tag。

多对一 VLAN mapping 的实现方式

图 16-6 N:1 VLAN 映射实现方式



- 对于上行数据流，通过在上图所示的下行端口上配置输入方向的 VLAN 映射策略，将原来的 VLAN Tag 映射为新的 VLAN Tag。
- 对于下行数据流的映射，当前不支持。

16.1.4 TPID 设置及优先级的复制与映射

以太网帧 Tag 包含四个字段：TPID(Tag Protocol Identifier，标签协议标志)、 User Priority、CFI、VLAN ID。对于 TPID 值，缺省采用 IEEE802.1Q 协议规定的 0x8100。而某些厂商的设备将报文外层 Tag 的 TPID 值设置为 0x9100 或其他值。为了和这些设备兼容，提供了基于端口的报文 TPID 可配置功能。用户可自行配置端口的 TPID 值，那么这些端口在转发报文时，会将报文的外层 Vlan Tag 中的 TPID 替换为用户设定的值。

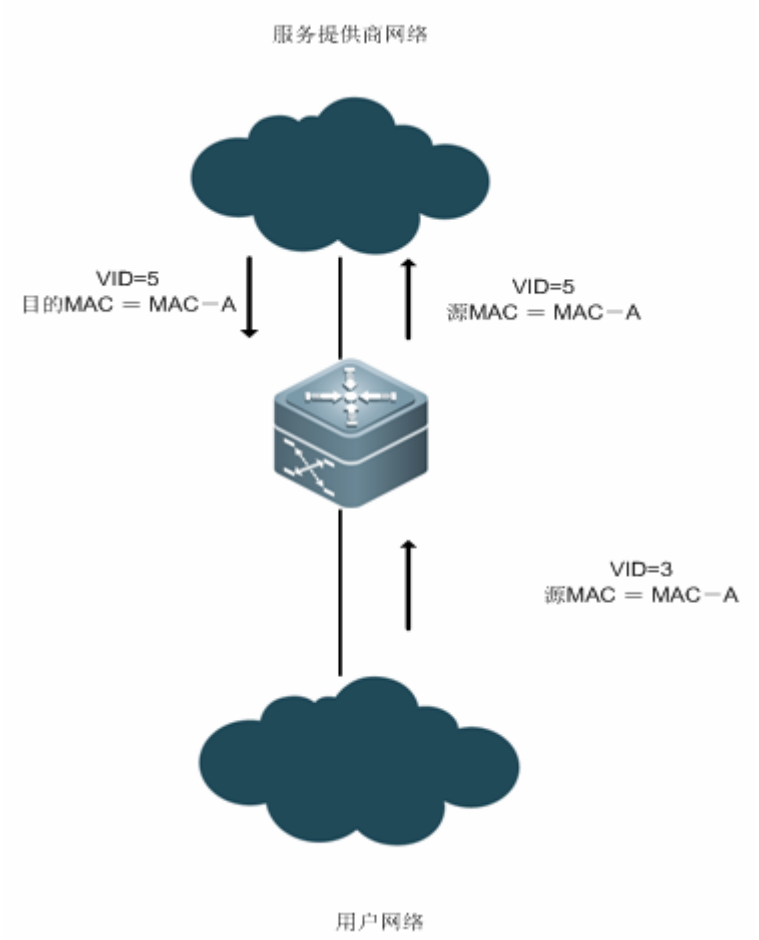
- 优先级复制：指的是在添加外层 Tag 的时候，将内层 Tag(用户 Tag)的优先级复制到外层 Tag(服务商 Tag)。

- 优先级映射：指的是在添加外层 Tag 的时候，根据内层 Tag(用户 Tag)的优先级将外层 Tag(服务商 Tag)的优先级设置为不同的值。

16.1.5 MAC 地址复制

由于采用基于数据流的灵活 QinQ 时， 交换机学到的 mac 的 vid 是 native vlan 的。故当采用基于数据流的 vlan 转换时，当报文从对端回来时候，就会发生无法查询到 mac 地址而泛洪的情况。

图 16-7 灵活 QinQ 报文的 MAC 地址学习示意图



如上图所示，假设交换机和用户网络相连端口是 dot1q-tunnel port，且在该端口上配置 native vlan 是 4，并且配置策略对源 MAC 为 A 的报文封装外层 Tag 为 vlan 5。当交换机收到用户网络 vlan 3 且源 MAC 为 A 的报文后，为其添加 vlan 5 的外层 Tag，同时由于接收端口的 native vlan 是 vlan 4，MAC-A 将被学习到 vlan 4 中。当响应报文返回时，由于其外层 Tag 的 vlan 是 vlan 5，将在 vlan 5 中查找 MAC-A，但是 MAC-A 并没有被学习到 vlan 5 中，此报文将被泛洪。

为此，可以将 native vlan 的 mac 地址复制到外层 Tag 所在的 vlan 中，解决从公网返回的报文被持续泛洪的问题。同样，也可以将外层 Tag 所在 vlan 的 mac 地址复制到 native vlan，解决从用户网络发往公网的报文被持续泛洪的问题。

16.1.6 二层协议透传

为了实现用户网络之间二层协议报文的传输而又不对运营商网络产生影响，可以使用二层报文透传功能。当用户网络中二层协议报文进入边缘设备后，将目的 mac 地址改成私有地址在运营商网络中转发，到了另外一端边缘设备后，再将目的 mac 地址改成公有地址回到另一端用户网络，以达到二层协议报文在运营商网络透传的效果。

16.1.7 Uplink 端口

Uplink 端口其实就是一种特殊的 Trunk 口，不同的是，从 Uplink 口输出的报文都是带 Tag 的，而从 Trunk Port 输出的报文，如果是 Native VLAN 转发过来的，则是不带 Tag 的。上链端口(如：用户网络中连接到服务商网络的端口)通常被配置成 Uplink 口。

16.2 配置QINQ

QINQ 容量相关配置，参见《硬件表项容量》文档“配置共享池最大数目”章节。

16.2.1 QinQ 的默认配置

默认配置下，基本 QinQ、灵活 QinQ 和 QinQ 其他功能均为关闭状态。

16.2.2 QinQ 配置的限制

QinQ 配置有如下限制：

- 路由口不能设置为 Tunnel Port。
- 配置为 Tunnel 的端口不能再启用 802.1x 功能。
- 配置为 Tunnel 的端口不能再启用端口安全功能。
- 配置 Tunnel Port 作为 RSPAN 的源口时，外部 TAG 中的 VID 等于 RSPAN VLAN 的报文视为监控数据流。
- 对于应用在 Tunnel Port 上的 ACL，若要匹配用户 TAG 中的 VID，需要使用 inner 关键词。
- 请将与服务商网络相连的用户网络的出口也配置为 Uplink 口，如果在用户网络中配置了 QinQ 端口的服务商 Tag 的 TPID 值，那么用户网络出口的 Uplink 口的服务商 Tag 的 TPID 值也需要配置为相同值。
- 接口的 MTU 值默认为 1500 字节。当为报文加上外层 VLAN Tag 后，报文的长度会增加 4 个字节，建议用户适当增加运营商网络中各接口的 MTU 值，至少为 1504 字节。
- 在设备上配置了 QinQ 口之后，若要在设备开启 igmp snooping，需要使用 SVGL 共享模式，否则 igmp snooping 在 QinQ 口上将无法正常工作。

16.2.3 配置基本 QinQ

在全局配置模式下使用 **Interface** 命令进入接口配置模式。按照下面的步骤进行 Tunnel Port 配置：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式
Ruijie(config)# **interface** *interface-id*	进入接口配置模式
Ruijie(config-if)# **switchport mode dot1q-tunnel**	接口设置成 dot1q-tunnel port
Ruijie(config-if)# **switchport dot1q-tunnel allowed vlan** [**add**] { **tagged** | **untagged** } *v_list*	添加 dot1q-tunnel 口的许可 vlan，并指明输出相应许可 vlan 的报文时，是否需要带 Tag
Ruijie(config-if)# **switchport dot1q-tunnel native vlan** *VID*	设置 dot1q-tunnel 口的缺省 vlan
Ruijie(config-if)# **end**	退出接口模式
Ruijie# **show running-config**	查看全局配置

如果要删除 dot1q-tunnel 口的许可 vlan，请配置 **switchport dot1q-tunnel allowed vlan remove** *v_list* 。

建议不要将服务商网络中 trunk 口的 native vlan 设置为 tunnel 口的缺省 vlan，因为 trunk 口会剥去 VID 为其 native vlan 的 Tag。

下例给出了如何配置一个 QinQ 端口的示例：

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# switchport mode dot1q-tunnel
Ruijie(config-if)# switchport dot1q-tunnel nativ vlan 20
Ruijie(config-if)# switchport dot1q-tunnel allowed vlan tagged 100-200
Ruijie(config-if)# end
```

16.2.4 配置灵活 QinQ

16.2.4.1 配置基于协议的vid变更策略表

配置 vid 添加策略表

对 **dot1q-tunnel** 端口的输入报文，有时需要能够由报文 Tag 中的不同 VID，指定在转发时为报文添加不同的外部 Tag 的 VID，使用 **dot1q outer-vid** 指定内部 VID 列表添加外部 Tag 时的外部 VID，**no dot1q outer-vid** 命令可以取消相应得配置。 按照该命令功能，可以通过指定内部 VLAN 添加与内部 VID 相同的外部 VID，并将出口加入该 VLAN 的 UnTag 端口集中，可以实现从出口输出的为原始内部 Tag 报文。具体命令详见命令参考。

配置步骤如下：

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **interface** *interface-id*	进入接口模式
Ruijie(config-if)# **switchport mode dot1q-tunnel**	接口配置为 dot1q-tunnel 口

Ruijie(config-if)# **dot1q outer-vid** *VID* **register inner-vid** *v_list*	配置基于协议添加外部 Tag 的 VID 策略
Ruijie(config-if)# **end**	退出接口模式
Ruijie# **show registration-table**	查看该配置。

如果要取消基于协议添加外部 Tag 的 VID 策略，请配置 **no dot1q outer-vid** *VID* **register inner-vid** *v_list*。

下面例子设置输入报文 Tag 中的 VID 为 4-22 时，增加外部 Tag 中的 VID 为 3。由于端口本身要属于外部 Tag 对应 VLAN，因此还要配置命令将端口加入该 VLAN。

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport mode dot1q-tunnel
Ruijie(config-if)# switchport dot1q-tunnel allowed vlan add tagged 3
Ruijie(config-if)# dot1q outer-vid 3 register inner-vid 4-22
Ruijie(config-if)# end
```

配置基于外层 Tag 的 vid 修改策略表

对 Access，Trunk，Hybrid，Uplink 端口的输入报文，有时需要能够由报文外部 Tag 中的不同 VID，指定在转发时修改为不同的外部 Tag 的 VID，使用 **dot1q relay-vid** *VID* **translate local-vid** *v_list* 指定本地 VID(修改前外部 Tag 中的 VID)列表修改为新的 VID，**no dot1q outer-vid** *VID* **translate local-vid** *v_list* 命令可以取消相应的配置。具体命令详见命令参考。

配置步骤如下：

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **interface** *interface-id*	进入接口模式
Ruijie(config-if)# **switchport mode** *port-type*	配置为 Access、Trunk、Uplink 或 Hybrid 口
Ruijie(config-if)# **dot1q relay-vid** *VID* **translate local-vid** *v_list*	配置基于外部 Tag 修改外部 Tag 的 VID 策略
Ruijie(config-if)# **end**	退出接口模式
Ruijie# **show translation-table**	查看该配置。

如果要取消基于外部 Tag 修改外部 Tag 的 VID 策略，请配置 **no dot1q relay-vid** *VID* **translate local-vid** *v_list*。

下面例子设置当输入报文外部 Tag 的 vid 为 10-20 时，修改该 vid 为 100

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# dot1q relay-vid 100 translate local-vid 10-20
Ruijie(config-if)# end
```

16.2.4.2 配置基于数据流的vid变更策略表

配置 vid 添加策略表

对 **dot1q-tunnel** 端口的输入报文，有时需要能够由报文内容的不同，转发时为报文添加外部 Tag 可以指定不同的 VID，使用 **traffic-redirect access-group** *acl* **nested-vlan** *VID* **in** 命令，**dot1q-tunnel** 口输入的报文匹配 acl 条件时，转发报文添加外部 Tag 指定其 VID 为改命令指定值，**no traffic-redirect access-group** acl **nested-vlan** 命令可以取消相应的配置。命令形式详见命令参考。

配置步骤如下：

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **interface** *intf-id*	进入接口模式
Ruijie(config-if)# **switchport mode dot1q-tunnel**	接口配置为 dot1q-tunnel 口
Ruijie(config-if)# **traffic-redirect access-group** *acl* **nested-vlan** *VID* **in**	配置基于数据流添加外部 Tag 的 VID 策略
Ruijie(config-if)# **end**	退出接口模式
Ruijie# **show traffic-redirect**	查看该配置。

如果要取消基于数据流添加外部 Tag 的 VID 策略，请配置 **no traffic-redirect access-group** *acl* **nested-vlan**。

- 基于数据流的 VID 变更策略表优先于基于协议的 VID 变更策略表生效。
- 当 AP 口添加或者删除成员口时，AP 上配置的 VID 添加策略或修改策略会被删除，需要重新配置。建议用户配置完 AP 成员后，再在 AP 上进行 VID 策略配置。
- 当 ACL 被删除时，与此 ACL 相关的策略会被自动删除。
- 当 dot1q-tunnel 口收到 >= 2 层 Tag 的报文时，无法采用基于数据的匹配规则来添加 Tag。
- 若某个报文同时匹配两个或两个以上数据流策略的规则，且数据流策略未指明优先级时，按配置时间优先。
- ☑ qinq tunnel 口上接收到的报文如果同时匹配了基于协议的 VID 添加策略和基于数据流的 VID 添加策略，最后转发的报文添加的是基于数据流策略的 VID。

下面例子设置将接口源地址为 1.1.1.3 输入报文添加 VID 为 10

```
Ruijie# configure terminal
Ruijie(config)# ip access-list standard 20
Ruijie(config-acl-std)# permit host 1.1.1.3
Ruijie(config-acl-std)# exit
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport mode dot1q-tunnel
Ruijie(config-if)# traffic-redirect access-group 20 nested-vlan 10 in
Ruijie(config-if)# end
```

配置外部 vid 修改策略表

对 Access，Trunk，Hybrid，Uplink 端口的输入报文，有时需要能够由报文内容修改外部 Tag 的 VID 。

使用 traffic-redirect access-group *acl* outer-vlan *VID* in 命令，对于符合 acl 条件的报文修改该报文外部 Tag 中的 VID 为命令指定的 VID，no traffic-redirect access-group *acl* outer-vlan 命令可以取消相应的配置。命令形式详见命令参考。

配置步骤如下：

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **interface** *intf-id*	进入接口模式
Ruijie(config-if)# **switchport mode trunk**	配置为 Access，Trunk 或 Hybrid 口
Ruijie(config-if)# **traffic-redirect access-group** *acl* **outer-vlan** *VID* **in**	配置基于数据流修改外部 Tag 的 VID 策略
Ruijie(config-if)# **end**	退出接口模式
Ruijie# **show traffic-redirect**	查看该配置。

如果要取消基于数据流修改外部 Tag 的 VID 策略，请配置 no traffic-redirect access-group *acl* outer-vlan。

- 基于数据流的外部 VID 修改策略表优先于基于协议的外部 VID 修改策略表生效
- 当 AP 口添加或者删除成员口时，AP 上配置的 VID 添加策略或修改策略会被删除，需要重新配置。建议用户配置完 AP 成员后，再在 AP 上进行 VID 策略配置。
- 当 ACL 被删除时，与此 ACL 相关的策略会被自动删除。
- 若某个报文同时匹配两个或两个以上数据流策略的规则，且数据流策略未指明优先级时，按配置时间优先。

下面例子设置将接口源地址为 1.1.1.1 输入报文的外部 VID 修改为 3

```
Ruijie# configure terminal
Ruijie(config)# ip access-list standard 2
Ruijie(config-acl-std)# permit host 1.1.1.1
Ruijie(config-acl-std)# exit
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# traffic-redirect access-group 2 outer-vlan 3 in
Ruijie(config-if)# end
```

16.2.5 配置 VLAN mapping

16.2.5.1 配置一对一VLAN mapping

在 access、trunk、hybrid 或 uplink 端口上，通过如下方式配置一对一 VLAN mapping。具体命令详见命令参考。

配置步骤如下：

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **interface** *intf-id*	进入接口模式
Ruijie(config-if)# **switchport mode** *port-type*	接口配置为 Access、Trunk、Uplink 或 Hybrid 口

Ruijie(config-if)# **vlan-mapping-in vlan** *cvlan* **remark** *svlan*	配置输入方向的一对一 vlan mapping 功能。它将从端口输入报文的 Customer VLAN ID 修改为指定的 Server VLAN ID。
Ruijie(config-if)# **no vlan-mapping-in vlan** *cvlan* **remark** *svlan*	取消输入方向上的一对一 vlan mapping 功能
Ruijie(config-if)# **vlan-mapping-out vlan** *svlan* **remark** *cvlan*	配置输出方向的一对一 vlan mapping 功能。它将从端口输出报文的 Server VLAN ID 修改回指定的 Customer VLAN ID。
Ruijie(config-if)# **no vlan-mapping-out vlan** *svlan* **remark** *cvlan*	取消输出方向上的一对一 vlan mapping 功能
Ruijie(config-if)# **end**	退出接口模式
Ruijie# **show interface**[*intf-id*] **vlan-mapping**	查看该配置。

下面例子设置输入报文 Tag 中的 VID 为 3 时，将其改成 4 再转发

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# vlan-mapping-in vlan 3 remark 4
Ruijie(config-if)# vlan-mapping-out vlan 4 remark 3
Ruijie(config-if)# end
```

16.2.5.2 配置多对一VLAN mapping

在 access、trunk、hybrid 或 uplink 端口上，通过如下方式配置多对一 VLAN mapping。具体命令详见命令参考。

配置步骤如下：

命令	作用
Ruijie#**configure terminal**	进入配置模式
Ruijie(config)# **interface** *intf-id*	进入接口模式
Ruijie(config-if)# **switchport mode** *port-type*	接口配置为 Access、Trunk、Uplink 或 Hybrid 口
Ruijie(config-if)# **vlan-mapping-in vlan** *cvlan-list* **remark** *svlan*	配置输入方向的多对一 vlan mapping 功能。它可同时将输入的多个 Customer VLAN ID 修改为同一个指定的 Server VLAN ID。
Ruijie(config-if)# **no vlan-mapping-in vlan** *cvlan-list* **remark** *svlan*	取消多对一 vlan mapping 功能
Ruijie(config-if)# **end**	退出接口模式
Ruijie# **show interface**[*intf-id*] **vlan-mapping**	查看该配置。

下面例子设置输入报文 Tag 中的 VID 为 3 到 7 时，将其改成 8 再转发

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# vlan-mapping-in vlan 3-7 remark 8
Ruijie(config-if)# end
```

配置 VLAN mapping 情况下，送 CPU 的报文 VLAN ID 为修改之后的 VLAN ID。

建议用户不要在同一端口上同时配置 VLAN 映射和灵活 QinQ。

16.2.6 配置 QinQ 其他功能

16.2.6.1 配置一个uplink端口

在全局配置模式下使用 **Interface** 命令进入接口配置模式。按照下面的步骤进行 Uplink Port 配置：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式
Ruijie(config)# **interface** <*interface*>	进入接口配置模式
Ruijie(config-if)# **switchport mode uplink**	配置端口为 Uplink 口
Ruijie(config-if)# **end**	退出接口模式
Ruijie(config-if)# **show running-config**	查看全局配置

下例给出了如何配置一个 Uplink 端口的示例：

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport mode uplink
Ruijie(config)# end
```

16.2.6.2 配置服务商Tag中的TPID值

在全局配置模式下按照下面的步骤进行配置：

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **frame-tag tpid** <*tpid*>	设置帧 Tag 中的 TPID。如果想设置为 0x9100。那么直接输入 frame-tag tpid 9100。注意默认是 16 进制。
Ruijie(config)# **end**	退出配置模式
Ruijie# **show frame-tag tpid**	查看端口的 tpid 值列表。

下例给出了如何配置 TPID 的示例：

```
Ruijie(config)# frame-tag tpid 9100
Ruijie(config)# end
Ruijie# show frame-tag tpid interface gigabitethernet 0/1
Port      tpid
--------- -------------
Gi0/1     0x9100
```

不允许将 tpid 指定为如下知名类型 0x0806(ARP)、0x0200(PUP)、0x8035(RARP)、0x0800(IP)、0x86DD(IPv6)、0x8863/0x8864(PPPoE) 、 0x8847/0x8848(MPLS) 、 0x8137(IPX/SPX) 、 0x8000(IS-IS) 、 0x8809(LACP) 、 0x888E(802.1x)、0x88A7(集群)、0x0789(我司保留)。

☑ S5750-S 只支持在全局配置模式下配置 TPID。

16.2.6.3 配置优先级复制

为了能够维持报文的优先级，需要在 tunnel 口上，将用户报文的内层 Tag 的优先级复制到外层 Tag 中。

配置步骤如下：

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **interface** <*interface*>	进入接口配置模式
Ruijie(config-if)# **mls qos trust cos**	配置端口信任模式为 trust CoS。
Ruijie(config-if)# **inner-priority-trust enable**	复制内层 Tag(用户 Tag)的 priority 字段值到外层 Tag 的 priority 字段值(服务商 Tag)。
Ruijie(config-if)# **end**	退出接口模式
Ruijie# **show inner-priority-trust**	查看复制的配置。

只有 dot1q-tunnel 端口允许配置用户 Tag 的优先级复制，其优先级高于信任模式的 QOS，低于基于数据流的 QOS。

优先级复制与优先级映射功能不能在同一接口上同时打开。

下例给出了如何配置用户 Tag 优先级复制的示例：

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if)#mls qos trust cos
Ruijie(config-if)# inner-priority-trust enable
Ruijie(config)# end
Ruijie# show inner-priority-trust interface gigabitethernet 0/1
Port      inner-priority-trust
------    --------------------
Gi0/1     enable
```

16.2.6.4 配置优先级映射

为了能够在 tunnel 口上，实现对报文优先级的灵活控制，可以根据报文内层优先级的不同，为报文封装 Tag 时候标记上不同优先级的外层标签。

配置步骤如下：

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **interface** <*interface*>	进入接口配置模式
Ruijie(config-if)# **dot1q-Tunnel cos** *inner-cos-value* **remark-cos** *outer-cos-value*	根据内层 Tag(用户 Tag)的 priority 字段值设置外层 Tag 的 priority 字段值(服务商 tag)。
Ruijie(config-if)# **end**	退出接口模式
Ruijie# **show interface intf-name remark**	查看优先级映射的配置。

- 只有 dot1q-tunnel 端口允许配置用户 Tag 的优先级复制，其优先于 QOS 生效。
- 优先级映射与优先级复制功能不能在同一接口上同时打开。
- 如果没有配置信任模式，即 trust none，则优先级映射的配置不生效；如果配置的信任模式和配置的映射不匹配，也不生效。

下例给出了如何配置用户 Tag 优先级复制的示例：

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if)#dot1q-Tunnel cos 3 remark-cos 5
Ruijie(config)# end
Ruijie# show interface gigabitethernet 0/1 remark
Ports          Type         From value  To value
-------------- ------------ ----------- --------
Gi0/1          Cos-To-Cos   3           5
```

16.2.6.5 配置地址复制

当一个端口学习到动态地址时，将其从一个 vlan 复制到另一个 vlan 中。

配置步骤如下：

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config-if)# **interface** <*interface*>	进入接口配置模式
Ruijie(config-if)# **mac-address-mapping** *x* **source-vlan** *src-vlan-list* **destination-vlan** *dst-vlan-id*	将接口在源 vlan 中学习到的动态地址复制到目的 vlan 中。
Ruijie(config-if)# **end**	退出接口模式
Ruijie(config-if)# **show interface** *intf-name* **mac-address-mapping** *x*	查看地址复制的配置。

- 关闭 VLAN 间 MAC 地址复制功能后，系统将删除目的 VLAN 中通过该功能学到的其他 VLAN 的所有 MAC 地址表项。
- VLAN 间 MAC 地址复制功能在一个端口下对某个目的 VLAN 只能配置一次。如果需要修改，必须先删除之前的配置，然后再重新进行配置。
- 不能和 share vlan 共用；不能将地址复制到动态 VLAN 中。
- 每个端口最多只能配置 8 个目的 VLAN。即使端口不在指定的目的 VLAN 中，该功能也会生效。
- 地址复制不能在 host/promiscuous 口上配置，不能在打开端口安全，镜像的目的口，打开 1x 功能的端口上配置。
- 只复制动态地址；静态地址不复制；地址表已满时，不复制；开启功能前，源地址已经存在的 mac 地址不复制。
- 复制地址的优先级比动态地址高，比其它类型地址的优先级低。
- 当 MAC 地址老化时候，由其复制出来的地址也要相应老化；当 MAC 地址被删除时，由其复制出来的地址也将被自动删除。

不支持热备，故当发生主从切换建议用户关闭复制功能，再重新打开。

用户不能手工删除通过 VLAN 间 MAC 地址复制功能获得的 MAC 地址表项，如果确实需要删除该表项，可以通过关闭 VLAN 间 MAC 地址复制功能实现。

下例给出了如何配置用户 Tag 优先级复制的示例：

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)#mac-address-mapping 1 source-vlan 1-3 destination-vlan 5
Ruijie(config)# end
Ruijie# show interface mac-address-mapping
Ports     destination-VID     Source-VID-list
-------------------------------------------
Gi0/1          5                   1-3
```

16.2.6.6 配置二层协议透传功能

STP 协议报文透传设置

要配置 STP 协议报文透传功能，在特权模式下按照下面的步骤进行配置：

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **l2protocol-tunnel stp**	配置全局使能 STP 协议报文透传功能
Ruijie(config-if)# **interface** *interface-name*	进入接口模式
Ruijie(config-if)# **l2protocol-tunnel stp enable**	在接口上使能 STP 协议报文透传功能
Ruijie# **show l2protocol-tunnel stp**	查看该配置。

下面的例子打开 STP 报文的透传功能

```
Ruijie# configure terminal
Ruijie(config)# l2protocol-tunnel stp
Ruijie(config)# interface fa 0/1
Ruijie(config-if)# l2protocol-tunnel stp enable
```

GVRP 协议报文透传设置

要配置 GVRP 协议报文透传功能，在特权模式下按照下面的步骤进行配置：

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **l2protocol-tunnel gvrp**	配置全局使能 GVRP 协议报文透传功能
Ruijie(config-if)# **interface** *interface-name*	进入接口模式
Ruijie(config-if)# **l2protocol-tunnel gvrp enable**	在接口上使能 GVRP 协议报文透传功能
Ruijie# **show l2protocol-tunnel gvrp**	查看该配置。

下面的例子打开 GVRP 报文的透传功能

```
Ruijie# configure terminal
Ruijie(config)# l2protocol-tunnel gvrp
Ruijie(config)# interface fa 0/1
Ruijie(config-if)# l2protocol-tunnel gvrp enable
```

当全局使能协议透传后，接口上使能协议透传时候才有效。当接口上协议透传功能生效时候，该接口不参与该协议计算。若透传口收到目的 MAC 为特殊组播地址的报文， 则表示组网出现错误，将直接丢弃该报文。

配置透传地址

相应协议的透传地址，在特权模式下按照下面的步骤进行配置：

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **l2protocol-tunnel** { **STP** | **GVRP** } **tunnel-dmac** *mac-address*	配置相应协议的透传地址
Ruijie(config)# **show l2protocol-tunnel stp**	查看该配置。

下面的例子打开 STP 报文的透传功能

```
Ruijie# configure terminal
Ruijie(config)#l2protocol-tunnel stp tunnel-dmac 011AA9 000005
```

其中 STP 报文可选地址范围: 01d0.f800.0005、011a.a900.0005、010f.e200.0003、0100.0ccd.cdd0、0100.0ccd.cdd1、0100.0ccd.cdd2; 其中 GVRP 报文可选地址范围为: 01d0.f800.0006、011a.a900.0006。

当未配置透传地址时，缺省使用的地址前三字节为 01d0f8，后 3 字节为(stp: 000005，gvrp: 000006)。

16.2.7 查看 QinQ 信息

在特权模式下使用如下命令查看 QinQ 相关的配置信息：

命令	作用
show dot1q-tunnel	显示接口的 dot1q-tunnel 是否打开
show interface[*intf-id*]**dot1q-tunnel**	显示 dot1q-tunnel 口配置
show registration-table [**interface** *intf-id*]	显示基于协议的 dot1q-tunnel 端口 vid 添加策略表
show translation-table [**interface** *intf-id*]	显示基于协议 access,trunk,hybrid 端口 vid 修改策略表
show interface[*intf-id*] **vlan-mapping**	显示接口的 vlan mapping
show traffic-redirect [**interface** *intf-id*]	显示基于数据流的 vid 变更或添加策略表
show frame-tag tpid interface [*intf-id*]	显示接口 tpid 的配置
show inner-priority-trust	显示优先级复制配置
show interface intf-name remark	显示优先级映射的配置
show mac-address-mapping	显示 MAC 地址复制配置
show l2protocol-tunnel { **gvrp** | **stp** }	显示二层透传配置

16.3 QinQ典型配置用例

16.3.1 基本 QinQ 实现二层 VPN 业务

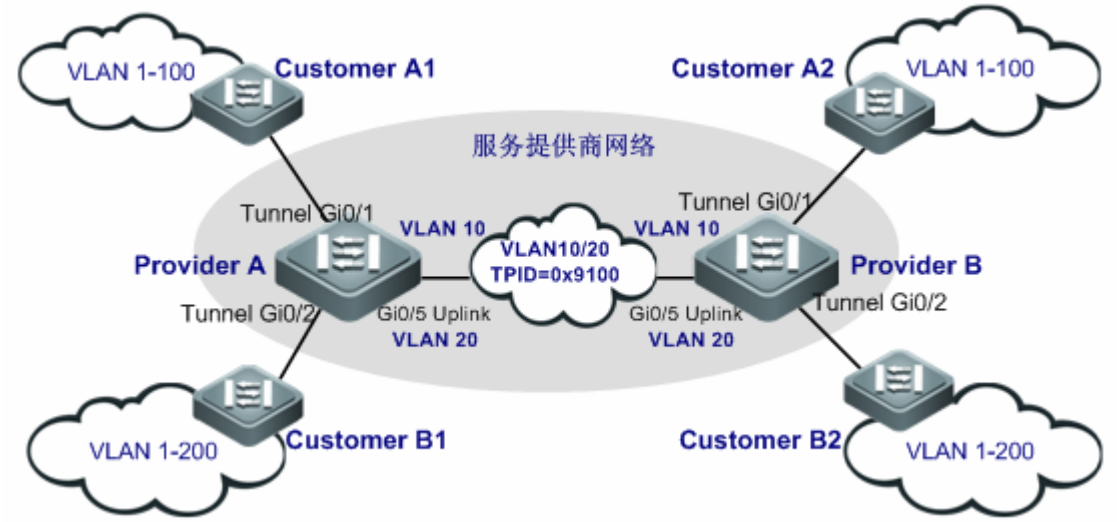
拓扑图

企业 A 和企业 B 有办公地点，每个办公地点都有自己的网络。如下图所示， Customer A1、Customer A2、Customer B1、Customer B2 分别为企业用户 A、企业用户 B 所在网络的边缘设备。Customer A1 和 Customer B1 通过服务提供商边缘设备 Provider A 接入到公网，Customer A2 和 Customer B2 通过服务提供商边缘设备 Provider B 接入到公网。

Customer A1-A2 使用的办公网络 VLAN 范围为 VLAN1-100，Customer B1-B2 使用的办公网络 VLAN 范围为 VLAN1-200。

Provider A 和 Provider B 之间为其他厂商的设备，其 TPID 值为 0x9100。

图 16-8 基本 QinQ 实现二层 VPN 业务应用拓扑



应用需求

服务提供商为企业 A 和企业 B 提供 VPN 服务，具体要求如下：

1、两个企业的数据在传送至对端时可以保留原有 VLAN 信息

2、两个企业相同 VLAN 编号的数据在服务提供商网络中传输时不会产生冲突

配置要点

1、下连用户网络的数据无需区分，在服务提供商边缘设备（本例为 Provider A 和 Provider B）上启用基本 QinQ 即能满足需求。

2、锐捷交换机的 TPID 值与其他厂商不一致，需在在服务提供商边缘设备（本例为 Provider A 和 Provider B）Uplink 接口上将 TPID 值调整为与第三方设备一样的值。

在 QinQ 配置模型中，当边缘设备连接服务商网络的上链口或服务提供商设备之间相互连接的的接口为 Trunk port、Hybrid port 的时候，请避免将 Trunk port 或 Hybrid port 的 Native vlan 设置为 tunnel 口的缺省 vlan。因为当报文从 Trunk port 或 Hybrid port 输出时，会被剥去 VID 为其 Native vlan 的 Tag。

由于开启 QinQ 功能的设备会为用户报文封装其他 VLAN 的外层 Tag，不会按报文中原始的 VLAN 进行转发，因此不需要在设备上创建用户的 VLAN。

配置步骤

1）配置 Provider A

第一步，创建服务商 VLAN 10、20 用于区别两个用户的数据

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#vlan 10
Ruijie(config-vlan)#exit
Ruijie(config)#vlan 20
Ruijie(config-vlan)#exit
```

第二步，在连接企业 A 网络的接口上启用基本 QinQ 功能，使用 VLAN10 对企业 A 网络的数据进行隧道传输。

```
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#switchport mode dot1q-tunnel
Ruijie(config-if-GigabitEthernet 0/1)#switchport dot1q-tunnel native vlan 10
Ruijie(config-if-GigabitEthernet 0/1)#switchport dot1q-tunnel allowed vlan add untagged 10
```

第三步，在连接企业 B 网络的接口上启用基本 QinQ 功能，使用 VLAN20 对企业 B 网络的数据进行隧道传输。

```
Ruijie(config)#interface gigabitEthernet 0/2
Ruijie(config-if-GigabitEthernet 0/2)#switchport mode dot1q-tunnel
Ruijie(config-if-GigabitEthernet 0/2)#switchport dot1q-tunnel native vlan 20
Ruijie(config-if-GigabitEthernet 0/2)#switchport dot1q-tunnel allowed vlan add untagged 20
```

第四步，配置 Uplink 口

```
Ruijie(config)# interface gigabitEthernet 0/5
Ruijie(config-if-GigabitEthernet 0/5)#switchport mode uplink
```

第五步，在 Uplink 口上调整输出报文的 TPID 值为第三方设备可识别的 0x9100。

```
Ruijie(config-if-GigabitEthernet 0/5)#frame-tag tpid 9100
```

2）配置 Provider B

Provider B 设备上的配置同 Provider A 配置类似，请参考上文 Provider A 的配置。此处不再重复说明。

验证结果

第一步，确认 Tunnel 口的配置是否正确，关注点：接口类型是否为 dot1q-tunnel、外层 Tag VLAN 是否为 Native VLAN 且其是否已加入接口的许可 VLAN 列表、服务商网络边缘设备上链口是否为 Uplink、Trunk 或 Hybrid Port。

```
Ruijie#show running-config
interface GigabitEthernet 0/1
 switchport mode dot1q-tunnel
 switchport dot1q-tunnel allowed vlan add untagged 10
 switchport dot1q-tunnel native vlan 10
 spanning-tree bpdufilter enable
!
interface GigabitEthernet 0/2
 switchport mode dot1q-tunnel
 switchport dot1q-tunnel allowed vlan add untagged 20
 switchport dot1q-tunnel native vlan 20
 spanning-tree bpdufilter enable
!
interface GigabitEthernet 0/5
 switchport mode uplink
 frame-tag tpid 0x9100
```

第二步，确认设备接口的 QinQ 配置，再次确认，关注点同第一步。

```
Ruijie#show interfaces dot1q-tunnel

========Interface Gi0/1========
Native vlan: 10
Allowed vlan list:1,10,
Tagged vlan list:

========Interface Gi0/2========
Native vlan: 20
Allowed vlan list:1,20,
Tagged vlan list:
```

第三步，确认 TPID 值的配置，关注点：接口为 Uplink 口、TPID 值。

```
Ruijie#show frame-tag tpid
Ports         Tpid
------- -------------
Gi0/5        0x9100
```

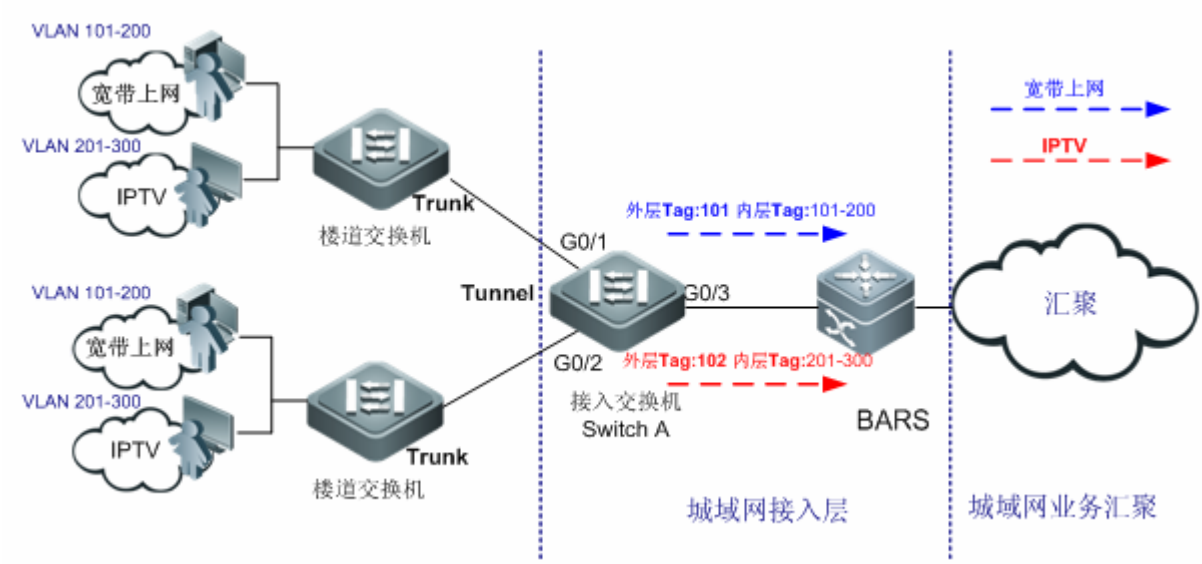
Provider B 设备上的配置验证同 Provider A 的类似，请参考上文 Provider A 的配置验证过程，此处不再重复说明。

16.3.2 基于 C-Tag 的灵活 QinQ 实现网上业务区分

拓扑图

下图是城域网基于 C-Tag 流分类的灵活 QinQ 组网示意图。宽带上网、IPTV 业务都是城域网的所承载业务的重要部分。如下图所示，用户端设备通过小区的楼道交换机汇聚，宽带上网、IPTV 业务通过分配不同的 VLAN 进行区分，其中宽带上网用户位于 VLAN 101-200 范围内，IPTV 用户位于 201-300 范围内。

图 16-9 基于 C-Tag 的灵活 QinQ 实现 Internet 接入业务



应用需求

根据 VLAN ID 对用户的宽带上网和 IPTV 数据进行区分，以便针对不同业务流实行不同的 QOS 服务策略

配置要点

在城域网接入层的接入交换机与楼层汇聚交换机连接的接口（本例为 SwitchA 的 G 0/1，G0/2）上配置基于 C-Tag 的灵活 QinQ，根据内层 VLAN Tag 进行业务数据分类即可满足需求。

基于 C-Tag 进行流分类添加 S-Tag 的灵活 QinQ VLAN 标签规划：

设备	业务	内层 VLAN Tag	外层 VLAN Tag	流分类规则
Switch A	宽带上网	101-200	101	C-Tag VLAN 区间
Switch A	IPTV	201-300	201	C-Tag VLAN 区间

由于开启 QinQ 功能的设备会为用户报文封装其他 VLAN 的外层 Tag，不会按报文中原始的 VLAN 进行转发，因此不需要在设备上创建用户的 VLAN。

配置步骤

- 配置 Switch A

第一步， 创建服务商 VLAN 101、201，用于区分不同的业务数据

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#vlan 101
```

```
Ruijie(config-vlan)#exit
Ruijie(config)#vlan 201
Ruijie(config-vlan)#exit
```

第二步， 在接入交换机的下链口上配置基于 C-Tag 添加外层 VLAN Tag 的灵活 QinQ 功能

```
Ruijie(config)#interface range gigabitEthernet 0/1-2
Ruijie(config-if-range)# switchport mode dot1q-tunnel
```

！ 配置 Gi 0/1 和 Gi 0/2 接口类型为 Tunnel port

```
Ruijie(config-if-range)# switchport dot1q-tunnel allowed vlan add untagged 101,201
```

！ 将服务商 VLAN101,201 加入到 Tunnel port 许可 VLAN 列表，并配置对端报文返回至 Tunnel port 输出时剥离服务商 Tag

```
Ruijie(config-if-range)# dot1q outer-vid 101 register inner-vid 101-200
```

！ 配置从 Tunnel port 输入的 vlan101-200 (C-tag)的数据帧在服务商网络中传输打上 vlan 101(S-tag)的标签

```
Ruijie(config-if-range)# dot1q outer-vid 201 register inner-vid 201-300
```

！ 配置从 Tunnel port 输入的 vlan201-300 (C-tag)的数据帧在服务商网络中传输打上 vlan 201(S-tag)的标签

第三步，配置 Uplink 口

```
Ruijie(config)# interface gigabitEthernet 0/3
Ruijie(config-if-GigabitEthernet 0/3)#switchport mode uplink
```

在 Tunnel port 上必须允许外层 Tag VLAN(包括 Native VLAN)通过，同时接入公网的接口也必须允许这些 VLAN 报文通过。本例中，Tunnel port 的 Native VLAN 为缺省值 VLAN1，默认允许。

验证结果

第一步，确认配置是否正确，关注点：下连接口类型是否为 dot1q-tunnel，外层 Tag VLAN 是否已加入接口的许可 VLAN 列表，接口上的映射策略是否正确，uplink 口是否设置正确。

```
Ruijie#show running-config interface gigabitEthernet 0/1
interface GigabitEthernet 0/1
 switchport mode dot1q-tunnel
 switchport dot1q-tunnel allowed vlan add untagged 101,201
 dot1q outer-vid 101 register inner-vid 101-200
 dot1q outer-vid 201 register inner-vid 201-300
 spanning-tree bpdufilter enable
!
interface GigabitEthernet 0/2
 switchport mode dot1q-tunnel
 switchport dot1q-tunnel allowed vlan add untagged 101,201
 dot1q outer-vid 101 register inner-vid 101-200
 dot1q outer-vid 201 register inner-vid 201-300
 spanning-tree bpdufilter enable
!
```

```
interface GigabitEthernet 0/3
 switchport mode uplink
```

第二步，确认设备接口的 QinQ 配置，再次确认，关注点同第一步。

```
Ruijie#show interfaces dot1q-tunnel

========Interface Gi0/1========
Native vlan: 1
Allowed vlan list:1,101,201
Tagged vlan list:

========Interface Gi0/2========
Native vlan: 1
Allowed vlan list:1, 101,201
Tagged vlan list:
```

第三步，确认基于 C-Tag 添加 TAG 的映射策略；关注点：内外层 VLAN 标签映射关系是否正确。

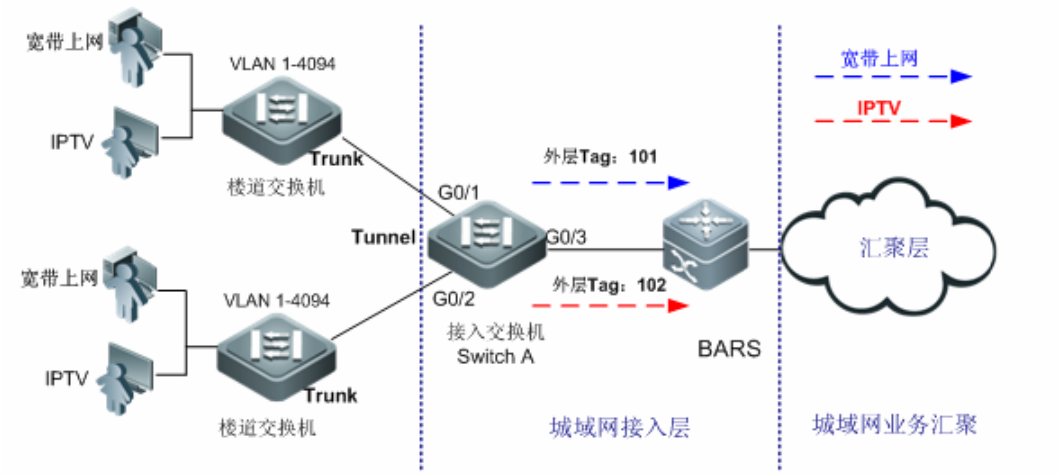
```
Ruijie#show registration-table

Ports     Type              Outer-VID    Inner-VID-list
------    ----------      ----------  --------------
Gi0/1     Add-outer       101           101-200
Gi0/1     Add-outer       201           201-300
Gi0/2     Add-outer       101           101-200
Gi0/2     Add-outer       201           201-300
```

16.3.3 基于 ACL 的灵活 QinQ 实现网上业务区分

拓扑图

下图是城域网基于 ACL 流分类的灵活 QinQ 组网示意图。服务提供商向用户提供使用宽带上网和 IPTV 两种业务。用户网络存在大量老式的低端网络接入设备，无法通过 VLAN ID 对业务流进行有效的区分，所有类型业务都在同一个 VLAN 上行。

图 16-10 基于 ACL 流分类的灵活 QinQ 实现 Internet 接入业务



应用需求

根据协议类型对下连用户的宽带上网、IPTV 种业务进行区分，以便针对不同业务流实行不同的 QOS 服务策略

配置要点

在城域网接入层的接入交换机与楼层汇聚交换机连接的接口（本例为 SwitchA 的 G 0/1，G0/2）上配置基于 ACL 流分类的灵活 QinQ 功能来对用户业务进行区分及分流即可满足用户需求。

宽带上网业务通常使用 PPPoE 拨号，其协议号一般为 0x8863/0x8864；IPTV 业务使用 IPoE，其协议号为 0x0800。

基于 ACL 进行流分类添加 S-Tag 的灵活 QinQ VLAN 标签规划：

设备	业务	内层 VLAN Tag	外层 VLAN Tag	流分类规则
Switch A	宽带上网(PPPoE)	1-4094	101	协议号 0x8863/0x8864
Switch A	IPTV(IPoE)	1-4094	201	协议号 0x0800

配置步骤

■ 配置 Switch A

第一步，创建用于区分流的 ACL

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# expert access-list extended acl1
```

！PPPOE 协议类型 0x8863/0x8864

```
Ruijie(config-exp-nacl)# permit 0x8863 any any
Ruijie(config-exp-nacl)# permit 0x8864 any any
Ruijie(config-exp-nacl)#exit
Ruijie(config)# expert access-list extended acl2
```

！匹配 IPOE 协议类型 0x0800

```
Ruijie(config-exp-nacl)#permit 0x0800 any any
```

第二步，创建服务商 VLAN 101、201,用于区分用户数据。

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#vlan 101
Ruijie(config-vlan)#exit
Ruijie(config)#vlan 201
Ruijie(config-vlan)#exit
```

由于开启 QinQ 功能的设备会为用户报文封装其他 VLAN 的外层 Tag，不会按报文中原始的 VLAN 进行转发，因此不需要在设备上创建用户的 VLAN。

第三步，在接入交换机的下链口上配置基于 ACL 添加外层 VLAN Tag 的灵活 QinQ 功能

```
Ruijie(config)#interface range gigabitEthernet 0/1-2
Ruijie(config-if-range)# switchport mode dot1q-tunnel
```

！ 配置 Gi 0/1 和 Gi 0/2 接口类型为 Tunnel port

```
Ruijie(config-if-range)#switchport dot1q-tunnel allowed vlan add untagged 101,201
```

！ 将服务商 VLAN101,201 加入到 Tunnel port 许可 VLAN 列表，并配置当对端报文返回至 Tunnel port 输出时剥离服务商 Tag

Ruijie(config-if-range)#traffic-redirect access-group acl1 nested-vlan 101 in

！ 配置从 Tunnel port 输入的匹配 ACL1 的数据帧在服务商网络中传输打上 vlan 101(S-tag)的标签

```
Ruijie(config-if-range)#traffic-redirect access-group acl2 nested-vlan 201 in
```

！ 配置从 Tunnel port 输入的匹配 ACL2 的数据帧在服务商网络中传输打上 vlan201(S-tag)的标签

第四步， 配置 GigabitEthernet 0/3 接口为 Uplink 口

```
Ruijie(config)# interface gigabitEthernet 0/3
Ruijie(config-if-GigabitEthernet 0/3)#switchport mode uplink
```

在 Tunnel port 上必须允许外层 Tag VLAN(包括 Native VLAN)通过，同时接入公网的接口也必须允许这些 VLAN 报文通过。本例中，Tunnel port 的 Native VLAN 为缺省值 VLAN1，默认允许。

验证结果

第一步，确认 Tunnel 口的配置是否正确，关注点：接口类型是否为 dot1q-tunnel，外层 Tag VLAN 是否已加入接口的许可 VLAN 列表，接口上的策略是否配置正确。

查看 GigabitEthernet 0/1 接口的配置

```
Ruijie#show running-config interface gigabitEthernet 0/1
```

```
interface GigabitEthernet 0/1
 switchport mode dot1q-tunnel
 switchport dot1q-tunnel allowed vlan add untagged 101,201
 traffic-redirect access-group acl1 nested-vlan 101 in
 traffic-redirect access-group acl2 nested-vlan 201 in
 spanning-tree bpdufilter enable
!
interface GigabitEthernet 0/2
 switchport mode dot1q-tunnel
switchport dot1q-tunnel allowed vlan add untagged 101,201
 traffic-redirect access-group acl1 nested-vlan 101 in
 traffic-redirect access-group acl2 nested-vlan 201 in
 spanning-tree bpdufilter enable
!
interface GigabitEthernet 0/3
 switchport mode uplink
```

第二步，确认设备接口的 QinQ 配置，再次确认，关注点同第一步。

```
Ruijie#show interfaces dot1q-tunnel

========Interface Gi0/1========
Native vlan: 1
Allowed vlan list:1,101,201
Tagged vlan list:

========Interface Gi0/2========
Native vlan: 1
Allowed vlan list:1,101,201
Tagged vlan list:
```

第三步，确认 ACL 的配置是否正确。关注点：ACL 表项是否正确。

```
Ruijie#show access-lists
expert access-list extended acl1
 10 permit 0x8863 any any
 20 permit 0x8864 any any
```

！ 匹配宽带业务流

```
expert access-list extended acl2
 10 permit 0x800 any any
```

！ 匹配 IPTV 业务流

第四步，确认基于流添加 TAG 的映射策略；关注点：内外层 VLAN 标签映射关系是否正确。

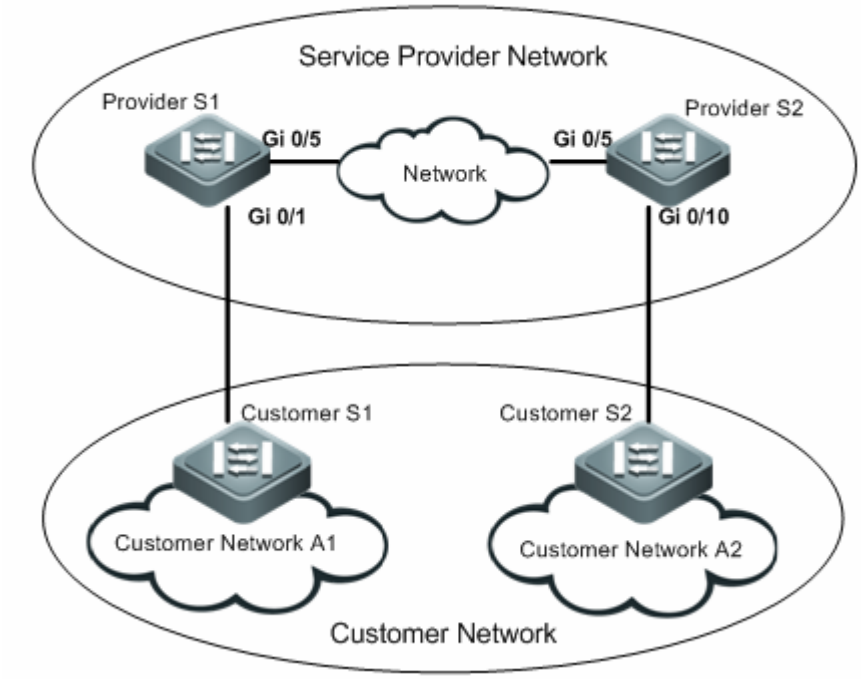
```
Ruijie#show traffic-redirect
Ports       Type           VID     Match-filter
```

```
-------    ----------    -----   ------------
Gi0/1       Nested-vid   101         acl1
Gi0/1       Nested-vid   201         acl2
Gi0/2       Nested-vid   101         acl1
Gi0/2       Nested-vid   201         acl2
```

16.3.4 BPDU Tunnel 典型配置用例

拓扑图

图 16-11 BPDU Tunnel 应用拓扑图



如上图所示，上部为服务提供商网络，下部为用户网络。其中，服务提供商网络包括边缘设备 Provider S1 和 Provider S2。Customer Network A1 和 Customer Network A2 为同一用户在不同地域的两个站点，Customer S1 和 Customer S2 为用户网络到服务商网络的接入设备，分别通过 Provider S1 和 Provider S2 接入服务提供商网络。

应用需求

1、用户网络的数据报文在服务提供商网络的 VLAN200 中传输。

2、处于不同地域的 Customer Network A1 和 Customer Network A2 可以跨越服务提供商网络进行统一生成树计算，而不影响服务商网络。

配置要点

1、在服务提供商边缘设备（本例为 Provider S1/Provider S2_上开启基本 QinQ 功能可满足第一个需求

2 在服务提供商边缘设备（本例为 Provider S1/Provider S2_上开启 STP 协议透传功能，使服务提供商网络可以通过 BPDU TUNNEL 对用户网络的 STP 报文进行隧道传输。

> 在 QinQ 配置模型中，当边缘设备连接服务商网络的上链口或服务提供商设备之间相互连接的的接口为 Trunk port、Hybrid port 的时候，请避免将 Trunk port 或 Hybrid port 的 Native vlan 设置为 tunnel 口的缺省 vlan。因为当报文从 Trunk port 或 Hybrid port 输出时，会被剥去 VID 为其 Native vlan 的 Tag。

配置步骤

- 配置 Provider S1

第一步，创建服务商 VLAN 200

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#vlan 200
Ruijie(config-vlan)#exit
```

第二步，在连接用户网络的接口上开启基本 QinQ 功能，使用 VLAN200 对用户网络的数据进行隧道传输

```
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#switchport mode dot1q-tunnel
Ruijie(config-if-GigabitEthernet 0/1)#switchport dot1q-tunnel native vlan 200
Ruijie(config-if-GigabitEthernet 0/1)#switchport dot1q-tunnel allowed vlan add untagged 200
```

第三步，在连接用户网络的接口上开启 STP 协议透传功能

```
Ruijie(config-if-GigabitEthernet 0/1)#l2protocol-tunnel stp enable
Ruijie(config-if-GigabitEthernet 0/1)#exit
```

第四步，全局开启 STP 协议透传功能

```
Ruijie(config)#l2protocol-tunnel stp
```

第五步，配置 uplink port

```
Ruijie(config)# interface gigabitEthernet 0/5
Ruijie(config-if-GigabitEthernet 0/5)#switchport mode uplink
```

- 配置 Provider S2

Provider S2 设备上的配置同 Provider S1 配置类似，请参考上文 Provider S1 的配置。此处不再重复说明。

验证结果

第一步，验证 STP 协议透传功能配置。关注点：STP 协议透传功能是否开启。

```
Ruijie#show l2protocol-tunnel stp

L2protocol-tunnel: Stp Enable
GigabitEthernet 0/1 l2protocol-tunnel stp enable
```

第二步，确认 Tunnel 口的配置是否正确，关注点：接口类型是否为 dot1q-tunnel，外层 Tag VLAN 是否为 Native VLAN 且其是否已加入接口的许可 VLAN 列表，服务商网络边缘设备上链口的类型是否为 Uplink。

```
Ruijie#show running-config
interface GigabitEthernet 0/1
 switchport mode dot1q-tunnel
 switchport dot1q-tunnel allowed vlan add untagged 200
 switchport dot1q-tunnel native vlan 200
 l2protocol-tunnel stp enable
 spanning-tree bpdufilter enable
!
interface GigabitEthernet 0/5
 switchport mode uplink
```

Provider S2 设备上的配置验证同 Provider S1 的类似，请参考上文 Provider S1 的配置验证过程，此处不再重复说明。

17 ERPS

17.1 ERPS概述

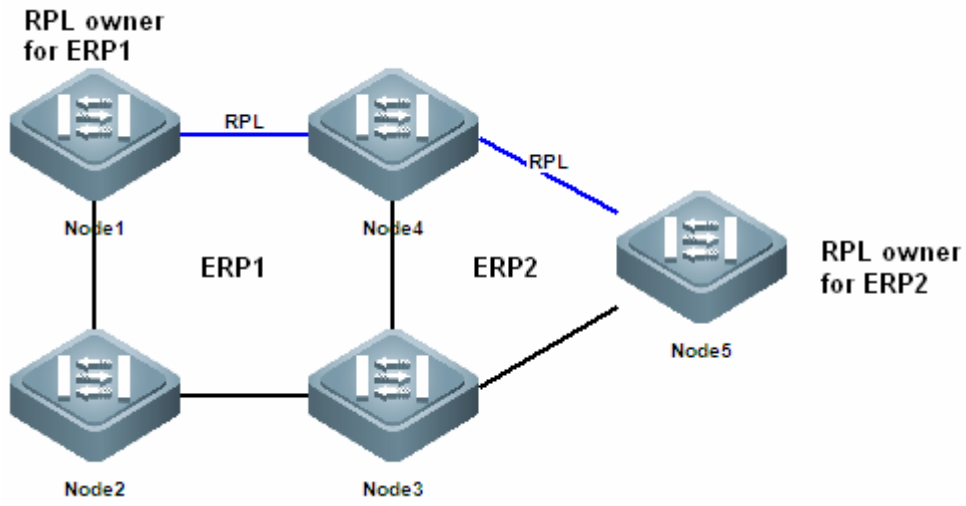
ERPS（Ethernet Ring Protection Switching，以太环保护切换协议）为 ITU 开发的一种环网保护协议，也称 G.8032。它是一个专门应用于以太环网的链路层协议。它在以太环网完整时能够防止数据环路引起的广播风暴，而当以太环网上一条链路断开时能迅速恢复环网上各个节点之间的通信。

城域网和企业网大多采用环网来构建以提供高可靠性，但环上任意一个节点发生故障都会影响业务。环网采用的技术一般是 RPR 或以太环网。RPR 需要专用硬件，因此成本较高。而以太环网技术日趋成熟且成本低廉，城域网和企业网采用以太环网的趋势越来越明显。

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

17.1.1 基本概念

图 17-1 ERPS 组网示意图



以太环

以太环分为普通以太环和以太子环：

- **普通以太环：**是一个环形连接的以太网网络拓扑。
- **以太子环：**以太子环为非闭环拓扑，它通过相交节点挂接在其它环或网络上，和相交节点间归属于其它环或网络的通道一起形成闭环拓扑。

每个以太环（不论是普通以太环还是以太子环）都有以下两种状态：

- **Idle 状态：**整个环网物理链路是连通的。

- **Protection 状态**：环网中某处物理链路断开。

根据 G.8032 标准（ITU-T G.8032/Y.1344 Amendment 1）的描述，对于相交环，相交的两个节点要求直连，不能再有其它设备。

节点

以太环上的每台设备都称为一个节点。

对于某个特定的以太环而言，节点的角色分为下列几种：

- **RPL owner 节点**：紧挨着 RPL 链路，在以太环无故障的情况下，负责阻塞 RPL 链路，防止网络出现环路的节点。每个以太环（不论是普通以太环还是以太子环）都有且仅有一个 RPL owner 节点。如图 1 所示，Node1 为以太环 ERP1 的 RPL owner 节点；Node5 为以太子环 ERP2 的 RPL owner 节点。
- **非 RPL owner 节点**：以太环上除 RPL owner 节点外的其它节点。如图 1 所示，除 Node1 和 Node5 外的其它节点，被称为各个环的非 RPL owner 节点。

对于全局（指不针对某个特定的以太环）而言，节点的角色分为下列几种：

- **相交节点**：在相交以太环中，同时属于多个环的节点被称为相交节点。如图 1 所示，Node3 与 Node4 被称为相交节点。
- **非相交节点**：在相交以太环中，只属于某个以太环的节点被称为非相交节点。如图 1 所示，除 Node3 和 Node4 外的其它节点，都被称为非相交节点。

链路与通道

- **RPL（Ring Protection Link，环保护链路）**：每个以太环（不论是普通以太环还是以太子环）都有且仅有一条 RPL。当以太环处于 Idle 状态时，RPL 链路处于阻塞状态，不转发数据报文，以避免形成环路。如图 1 所示，Node1 与 Node4 间的链路为以太环 ERP1 的 RPL 链路，Node1 阻塞 RPL 端口（RPL 链路所在的端口）；Node4 与 Node5 间的链路为以太环 ERP2 的 RPL 链路，Node5 阻塞 RPL 端口。
- **子环链路**：在相交环当中，归属于子环，由子环控制的链路。如图 1 所示，假设 ERP1 是普通以太环，ERP2 是以太子环，则 Node4 与 Node5 间的链路及 Node3 与 Node5 间的链路为子环 ERP2 的链路，其它链路归属于普通以太环 ERP1。

Node3 与 Node4 间的链路属于普通以太环 ERP1，不属于以太子环 ERP2，不受 ERP2 的控制。

- **R-APS （Ring Auto Protection Switch）virtual channel**：在相交环中，相交节点间，用于传输子环协议报文，但不属于子环的通路被称为子环的 R-APS 虚拟通道。如图 1 所示，由于 Node1 阻塞 RPL 链路，子环 ERP2 的协议报文在以太环 ERP1 中，通过 Node3 与 Node4 间的直连链路传播，则 Node3 与 Node4 间的直连通路就被称为子环 ERP2 的 R-APS 虚拟通道。

VLAN

ERPS 中有两种类型的 VLAN，一种是 R-APS VLAN，另一种是数据 VLAN。

- **R-APS VLAN**：R-APS VLAN 用来传递 ERPS 协议报文。设备上接入 ERP 环的端口都属于 R-APS VLAN，且只有接入 ERP 环的端口可加入此 VLAN。不同环的 R-APS VLAN 必须不同。R-APS VLAN 的接口上不允许配置 IP 地址。

- **数据 VLAN：**与 R-APS VLAN 相对，数据 VLAN 用来传输数据报文。数据 VLAN 中既可包含 ERP 环端口，也可包含非 ERP 环端口。

不同 ERP 环的 R-APS VLAN 必须配置成不同，否则可能导致协议工作异常。因不同 ERP 环的报文通过 R-APS VLAN 来区分。

17.1.2 ERPS协议报文

ERPS 协议报文（也称 R-APS 报文）的类型及其作用如下表所示：

报文类型	说明
SF（Signal Fail）报文	当节点的自身链路 down 时，发送该报文通知其它节点。
NR（No Request）报文	当节点的自身链路从故障中恢复时，发送该报文通知 RPL owner 节点。
（NR，RB)（No Request，RPL Blocked）报文	由 RPL owner 发送，当 ERP 环上的所有设备均无故障时，RPL owner 会周期性发送此报文。
Flush 报文	在相交环当中，由相交节点发送，用于将子环拓扑的变化通知子环所挂接的以太环上的其它设备。

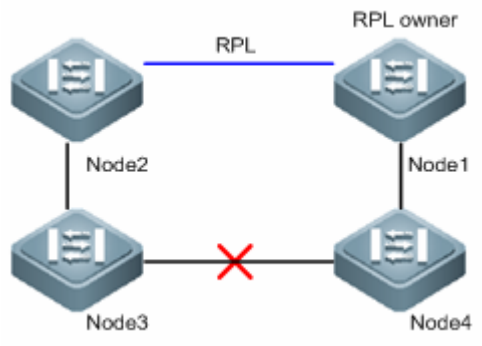
17.1.3 ERPS的定时器

ERPS 协议的定时器及其作用如下表所示：

报文类型	说明
Holdoff timer	该定时器用于防止由于链路的间歇性故障，导致 ERPS 不断进行拓扑切换。配置了此定时器之后，当检测到链路故障时，ERPS 不立即执行拓扑切换，而是等定时器超时之后，如果确认链路仍故障，才执行拓扑切换。
Guard timer	该定时器用于防止设备接收到过时的 R-APS 消息。当设备检测到链路从故障中恢复时，对外发送链路恢复的消息报文，并启动 guard 定时器。在 guard 定时器超时之前，除指示子环拓扑变化的 flush 报文外，其它的报文都将被直接丢弃，不进行处理。
WTR（Wait-to-restore） timer	此定时器只对 RPL owner 设备有效，对其它设备无效。该定时器主要用于防止 RPL owner 对环网的状态产生误判。当 RPL owner 检测到故障恢复时，不立即执行拓扑切换，而是等 WTR 定时器超时之后，如果确认以太环的确已从故障中恢复，才执行拓扑切换。如果在 WTR 定时器超时之前又再次检测到环网故障，则取消 WTR 定时器，不再执行拓扑切换。

17.1.4 工作原理

图 17-2 ERPS 单环



正常状态

- 所有的节点在物理拓扑上以环的方式连接。
- 环路保护协议通过阻塞 RPL 链路，确保不会成环(Loop)。如图 2 所示，Node1 和 Node2 间的链路为 RPL 链路。
- 对相邻节点间的每条链路进行故障检测。

链路故障

- 与故障相邻的节点检测到故障。
- 与故障链路相临的节点对故障链路进行阻塞，并使用 R-APS(SF)消息向环上的其他节点报告故障。如图 2 所示，假设 Node3，Node4 间链路故障，则 Node3 和 Node4 会在阻塞完故障链路后，分别向环网上各个节点发送 R-APS(SF)消息。
- R-APS(SF)消息触发 RPL 拥有节点打开 RPL 端口。R-APS(SF)消息还触发所有的节点更新各自 MAC 表项和 ARP/ND 表项，然后节点进入保护状态（Protection）。

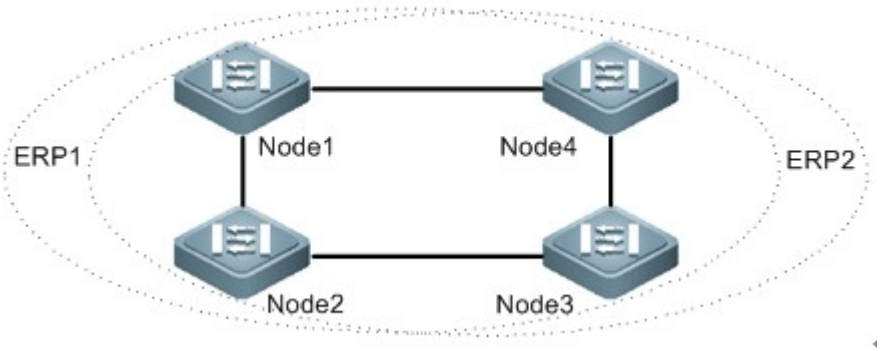
链路恢复

- 当故障恢复时，故障相邻的节点继续保持阻塞状态，并发送 R-APS(NR)消息，表示没有本地故障。
- 当 RPL 拥有节点收到第一个 R-APS(NR)消息后，开始启动 WTR 定时器。
- 当 WTR 定时器耗尽后，RPL 拥有节点阻塞 RPL，并发送 R-APS(NR，RB)消息。
- 其他节点收到这个消息后，更新各自 MAC 表项和 ARP/ND 表项，发送 R-APS(NR)消息的那个节点停止周期性发送消息，并打开原先阻塞的端口。
- 环网又恢复到了最初的正常状态。

负载均衡

在同一个环网中，可能同时存在多个 VLAN 的数据流量，ERPS 可以实现流量的负载分担，即不同 VLAN 的流量沿不同的路径进行转发。

图 17-3 单环负载分担



通过在同一个物理环网上配置多个以太环，不同以太环发送不同 VLAN（称为保护 VLAN）的流量，实现不同 VLAN 的数据流量在该环网中的拓扑不同，从而达到负载分担的目的。

如图 3 所示，一个物理环网对应了两个以太环，两个以太环保护的 VLAN 不同，Node1 为 ERP1 的 RPL owner，Node3 为 ERP2 的 RPL owner。通过配置，可以实现不同 VLAN 分别阻塞不同的链路，从而实现单环的负载分担。

由于上述普通以太环和以太子环的概念，使得上述单环的工作原理直接适用于相交环。在相交环当中，各环独立运行，各环的工作原理同单环。

17.1.5 典型组网

ERPS 的正常运行依赖于用户正确的配置。下面介绍几种典型的组网：

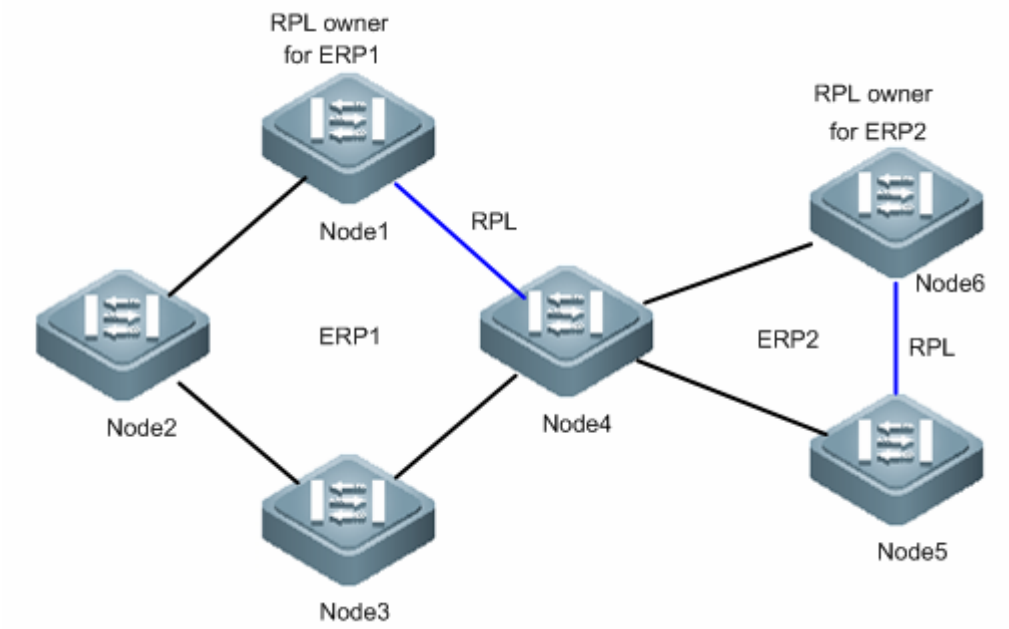
单环

如图 2 所示，网络拓扑中只有一个环；有且仅有一个 RPL owner 节点；有且仅有一条 RPL 链路；所有节点需具有相同的 R-APS VLAN。

相切环

如图 4 所示，网络拓扑中的两个环共用一台设备；每个环有且仅有一个 RPL owner 节点，每个环有且仅有一条 RPL 链路；不同环需具有不同的 R-APS VLAN。

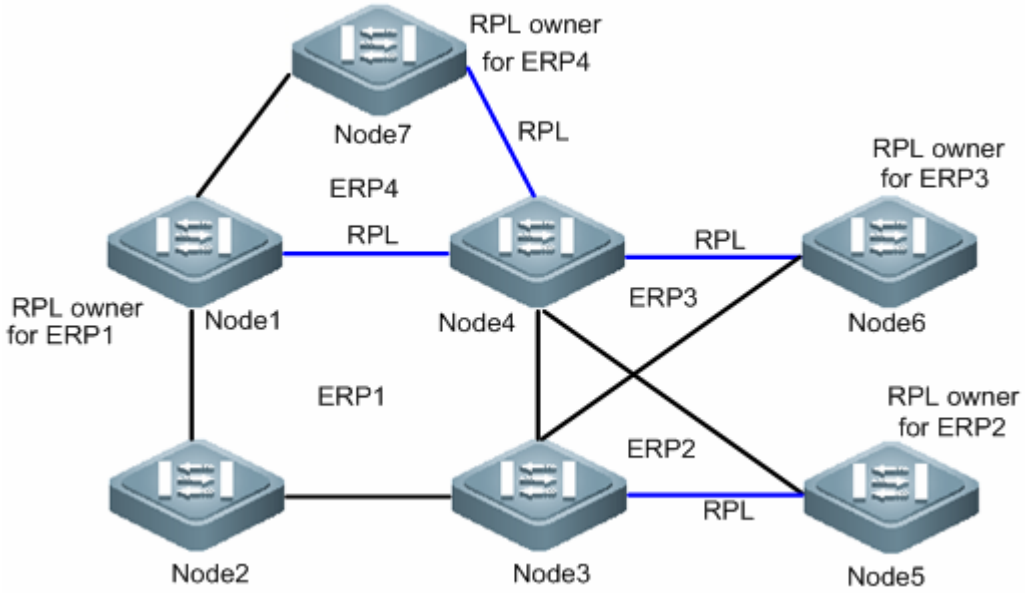
图 17-4 相切环拓扑示意图



相交环

除了支持如图 1 所示的两环相交的拓扑外，还支持如图 5 所示的多环相交的拓扑结构。网络拓扑中有两个或两个以上的环共用一条链路（相交的两个节点间必须直连，不能再有其它节点）；每个环有且仅有一个 RPL owner 节点，每个环有且仅有一条 RPL 链路；不同环需具有不同的 R-APS VLAN。

图 17-5 多环相交环拓扑示意图



协议还支持更加灵活的拓扑。比如：支持一个环与多个环相切；支持一个环的每条链路上均挂接着多个子环；支持一个环与多个环相切，同时与多个环相交等。在此，不一一进行列举。

17.1.6 协议规范

与 ERPS 相关的协议规范有：

- ITU-T G.8032/Y.1344
- ITU-T G.8032/Y.1344 Amendment 1

17.2 配置ERPS基本特性

以下章节描述如何配置 ERPS 的基本特性：

- （必选）配置 R-APS VLAN
- （必选）配置 ERP 环
- （必选）配置 RPL
- （必选）使能 ERPS
- （可选）关联子环与其它以太环
- （可选）使能子环拓扑变化通告
- （可选）配置定时器
- （可选）配置负载均衡
- （可选）配置链路状态检测方法
- 查看 ERPS 配置信息

17.2.1 缺省配置

下表用来描述 ERPS 的缺省配置。

功能特性	缺省值
R-APS VLAN	没有配置任何 R-APS VLAN
ERP 环	没有配置任何 ERP 环
RPL	没有配置 RPL
全局及指定环的 ERPS 状态	没有使能全局和指定环的 ERPS
关联子环与其它以太环	子环与其它以太环没有建立关联关系
子环拓扑变化通告	没有使能子环拓扑变化通告功能
定时器	Holdoff time 的缺省值为 0 Guard time 的缺省值为 500 milliseconds WTR time 的缺省值为 5 minutes
负载均衡	没有配置负载均衡
链路状态检测方法	采用检测链路物理状态（up or down）的方法，而非 OAM 方法。

17.2.2 配置R-APS VLAN

R-APS VLAN 用于传输 ERPS 协议报文。缺省情况下，没有配置任何 R-APS VLAN。进入特权模式，按以下步骤配置 R-APS VLAN。

命令	作用
Ruijie# **configure terminal**	进入全局配置模式
Ruijie(config)# **erps raps-vlan** *vlan-id*	创建 R-APS VLAN，同时进入 ERPS 配置模式，vlan-id 必须是设备上没有被使用的 VLAN

如果要删除 R-APS VLAN，可用 **no erps raps-vlan** *vlan-id* 全局配置命令进行设置。

配置举例：

进入全局配置模式。

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

配置全局 R-APS VLAN。

```
Ruijie(config)# erps raps-vlan 4093
```

R-APS VLAN 必须是设备上没有被使用的 VLAN，VLAN 1 不能被设置为 R-APS VLAN。

不同设备的同一个以太环需配置相同的 R-APS VLAN。

启用 ERPS 的设备需要关闭所有二层端口的风暴控制功能。

17.2.3 配置ERP环

配置 ERP 环包括配置普通以太环和以太子环，下面分别说明：

缺省情况下，没有配置任何普通以太环，进入特权模式，按以下步骤配置普通以太环。

命令	作用
Ruijie# **configure terminal**	进入全局配置模式
Ruijie(config)# **interface** *interface-name1* Ruijie(config-if)# **switchport mode trunk** Ruijie(config-if)# **exit** Ruijie(config)# **interface** *interface-name2* Ruijie(config-if)# **switchport mode trunk** Ruijie(config-if)# **exit** Ruijie(config)# **erps raps-vlan** *vlan-id* Ruijie(config-erps)# **ring-port west** *interface-name1* **east** *interface-name2*	配置普通的以太环： 配置端口的链路模式 进入 ERPS 配置模式 在 ERPS 模式下指定 ERP 环的端口

如果要删除普通以太环，可用 erps 模式下的 **no ring-port** 配置命令进行设置。

配置举例：

进入全局配置模式。

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

配置以太环端口的链路模式。

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
Ruijie(config)# interface fastEthernet 0/2
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
```

进入 erps 配置模式。

```
Ruijie(config)# erps raps-vlan 4093
```

配置加入以太环，参于 ERPS 协议计算的端口。

Ruijie(config-erps4093)# ring-port west fastEthernet 0/1 east fastEthernet 0/2

以太子环通常只需要在相交环的相交节点上配置，缺省情况下，没有配置任何以太子环，进入特权模式，按以下步骤配置以太子环。

命令	作用
Ruijie# **configure terminal**	进入全局配置模式
Ruijie(config)# **interface** *interface-name* Ruijie(config-if)# **switchport mode trunk** Ruijie(config-if)# **exit** Ruijie(config)# **erps raps-vlan** *vlan-id* Ruijie(config-erps)# **ring-port west virtual-channel east** *interface-name*	在相交环的相交节点上，配置子环的方式 1： 配置端口的链路模式 进入 ERPS 配置模式 在 ERPS 模式下指定 ERP 环的端口（其中的 **west** 端口为 **virtual-channel**）
Or：	
Ruijie(config)# **interface** *interface-name* Ruijie(config-if)# **switchport mode trunk** Ruijie(config-if)# **exit** Ruijie(config)# **erps raps-vlan** *vlan-id* Ruijie(config-erps)# **ring-port west** *interface-name* **east virtual-channel**	在相交环的相交节点上，配置子环的方式 2： 配置端口的链路模式 进入 ERPS 配置模式 在 ERPS 模式下指定 ERP 环的端口（其中的 **east** 端口为 **virtual-channel**）

如果要删除以太子环，可用 erps 模式下的 **no ring-port** 配置命令进行设置。

配置举例：

进入全局配置模式。

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

配置以太环端口的链路模式。

```
Ruijie(config)# interface fastEthernet 0/3
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
```

进入 erps 配置模式。

```
Ruijie(config)# erps raps-vlan 100
```

配置加入以太环，参于 ERPS 协议计算的端口。

```
Ruijie(config-erps100)#  ring-port west fastEthernet 0/3 east virtual-channel
```

- 加入 ERP 环的端口必须是 trunk 口；当端口加入 ERP 环之后，不再允许修改端口的 trunk 属性。
- 如果将环端口配置到 **virtual-channel** 上，则此环将被认为是个子环。
- 配置 ERP 环的端口不管 ERP 环有没有使能，都不参与 STP 计算。在配置 ERP 环过程中，需要保证环端口关闭 STP 计算情况下不存在环路。
- ERPS 和 RERP、REUP 不共用端口。

17.2.4 配置RPL

缺省情况下，没有配置 RPL。进入特权模式，按以下步骤配置 RPL。

命令	作用
Ruijie# **configure terminal**	进入全局配置模式
Ruijie(config)# **erps raps-vlan** *vlan-id*	进入 ERPS 配置模式
Ruijie(config-erps)# **rpl-port** {**west** | **east**} [**rpl-owner**]	配置 RPL

如果要删除 RPL，可用 erps 模式下的 **no rpl-port** 配置命令进行设置。

配置举例：

进入全局配置模式。

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

配置以太环端口的链路模式。

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
Ruijie(config)# interface fastEthernet 0/2
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
```

进入 erps 配置模式。

```
Ruijie(config)# erps raps-vlan 4093
```

配置加入以太环，参于 ERPS 协议计算的端口。

```
Ruijie(config-erps4093)#  ring-port west fastEthernet 0/1 east fastEthernet 0/2
```

指明 RPL 链路所在的端口和 RPL owner。

```
Ruijie(config-erps4093)#  rpl-port west rpl-owner
```

每个环需要且仅能配置一条 RPL 链路和一个 RPL owner 节点。

17.2.5 使能ERPS

缺省情况下，全局和指定环的 ERPS 功能均关闭，进入特权模式，按以下步骤开启全局和指定环的 ERPS 功能：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式
Ruijie(config)# **erps enable**	使能全局 ERPS 功能
Ruijie(config)# **erps raps-vlan** *vlan-id*	进入 ERPS 配置模式
Ruijie(config-erps)# **state enable**	使能指定环的 ERPS 功能

如果要关闭 ERPS 功能，可用全局配置模式下的 **no erps enable** 或 erps 配置模式下的 **no state enable** 配置命令进行设置。

配置举例：

进入全局配置模式。

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

配置以太环端口的链路模式。

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
Ruijie(config)# interface fastEthernet 0/2
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
```

进入 erps 配置模式。

```
Ruijie(config)# erps raps-vlan 4093
```

配置加入以太环，参于 ERPS 协议计算的端口。

```
Ruijie(config-erps4093)# ring-port west fastEthernet 0/1 east fastEthernet 0/2
```

使能指定环的 ERPS 功能。

```
Ruijie(config-erps4093)# state enable
```

使能全局 ERPS 功能。

```
Ruijie(config-erps4093)# exit
```

```
Ruijie(config)# erps enable
```

只有同时使能全局 ERPS 协议和指定环的 ERPS 协议之后，指定环的 ERPS 协议才真正开始运行。

17.2.6 关联以太环与它的子环

缺省情况下，以太环和它的子环间没有建立关联关系，进入特权模式，按以下步骤配置以太环和它的子环间的关联关系。

命令	作用
Ruijie# **configure terminal**	进入全局配置模式
Ruijie(config)# **erps raps-vlan** *vlan-id*	进入以太环的 ERPS 配置模式
Ruijie(config-erps)# **associate sub-ring raps-vlan** *vlan-list*	配置以太环与它的子环间的关联关系

如果要删除子环和其它以太环间的关联关系，可用 erps 配置模式下的 **no associate sub-ring raps-vlan** *vlan-list* 配置命令进行设置。

配置举例：

进入全局配置模式。

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

配置普通以太环。

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
Ruijie(config)# interface fastEthernet 0/2
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
Ruijie(config)# erps raps-vlan 4093
Ruijie(config-erps4093)# ring-port west fastEthernet 0/1 east fastEthernet 0/2
```

配置以太子环。

```
Ruijie(config)# erps raps-vlan 100
Ruijie(config)# interface fastEthernet 0/3
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
Ruijie(config)# erps raps-vlan 100
Ruijie(config-erps100)# ring-port west fastEthernet 0/3 east virtual-channel
```

关联子环和其它以太环。

```
Ruijie(config)# erps raps-vlan 4093
Ruijie(config-erps4093)# associate sub-ring raps-vlan 100
```

需要在以太环的所有节点上配置此命令，以使其子环的 ERPS 协议报文可以在该以太环中传播。

配置关联关系主要是为了使子环的协议报文可以在其它以太环中传播，用户也可以通过其它方式（如配置端口的许可 VLAN）达到这一目的。只是应保证只有接入 ERPS 环的那两个端口允许子环的协议报文通过，而其它端口都不允许其通过，否则，其它 VLAN 的报文可能通过透传进入子环的 R-APS VLAN，从而对 ERPS 环产生冲击。

17.2.7 使能子环拓扑变化通告

当在相交环的相交节点上使能子环的拓扑变化通告后，当子环的拓扑发生变化时，如果相交节点间的链路处于故障状态或阻塞状态，相交节点将发送报文通知子环所关联的其它以太环上的节点进行拓扑更新。

缺省情况下，没有使能子环拓扑变化通告，进入特权模式，按以下步骤使能子环拓扑变化通告。

命令	作用
Ruijie# **configure terminal**	进入全局配置模式
Ruijie(config)# **erps raps-vlan** *vlan-id*	进入子环的 ERPS 配置模式
Ruijie(config-erps)# **sub-ring tc-propagation enable**	使能子环拓扑变化通告

如果要关闭子环拓扑变化通告，可用 erps 配置模式下的 **no sub-ring tc-propagation** 配置命令进行设置。

配置举例：

进入全局配置模式。

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

配置普通以太环。

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
Ruijie(config)# interface fastEthernet 0/2
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
Ruijie(config)# erps raps-vlan 4093
Ruijie(config-erps4093)# ring-port west fastEthernet 0/1 east fastEthernet 0/2
```

配置以太子环。

```
Ruijie(config)# interface fastEthernet 0/3
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
Ruijie(config)# erps raps-vlan 100
Ruijie(config-erps100)# ring-port west fastEthernet 0/3 east virtual-channel
```

关联子环和其它以太环。

```
Ruijie(config-erps100)# sub-ring associate raps-vlan 4093
```

使能子环的拓扑变化通告。

```
Ruijie(config-erps100)# sub-ring tc-propagation enable
```

只需要在相交环的相交节点上配置此命令。

17.2.8 配置定时器

用户可在设备上设置 ERPS 的协议定时器，进入特权模式，按以下步骤配置协议定时器：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式
Ruijie(config)# **erps raps-vlan** *vlan-id*	进入 ERPS 配置模式
Ruijie(config-erps)# **timer** { **holdoff-time** *interval1* | **guard-time** *interval2* | **wtr-time** *interval3* }	配置协议定时器： **Holdoff** 定时器：单位为 100 毫秒，缺省值为 0，范围是 0-100； **Guard** 定时器：单位为 10 毫秒，缺省值为 50，范围是 1-200； **WTR** 定时器：单位为分钟，缺省值为 5，范围是 5-12。

如果恢复定时器的缺省值，可用 erps 配置模式下的 **no timer** { **holdoff-time** | **guard-time** | **wtr-time** }配置命令进行设置。

配置举例：

进入全局配置模式。

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

进入 ERPS 配置模式。

```
Ruijie(config)# erps raps-vlan 4093
```

配置 ERPS 协议定时器。

```
Ruijie(config-erps4093)# timer holdoff-time 10
Ruijie(config-erps4093)# timer guard-time 10
Ruijie(config-erps4093)# timer wtr-time 10
```

配置了 holdoff 定时器之后，当检测到链路故障时，ERPS 不立即执行拓扑切换，而是等定时器超时之后，如果确认链路仍故障，才执行拓扑切换。故，会影响链路故障时的拓扑收敛时间。

17.2.9 配置负载均衡

缺省情况下，没有配置负载均衡功能。进入特权模式，按以下步骤配置负载均衡功能：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式
Ruijie(config)# **spanning-tree mst configuration**	进入 MST 配置模式。
Ruijie(config-mst)# **instance** *instance-id* **vlan** *vlan-range*	把 vlan 组添加到一个 MST instance 中 *instance-id*，范围为 0－64

Ruijie(config-mst)# **exit**	*vlan-range*，范围为 1－4094 举例来说： instance 1 vlan 2-200 就是把 vlan 2 到 vlan 200 都添加到 instance 1 中。 instance 1 vlan 2、20、200 就是把 vlan 2、vlan 20，vlan 200 添加到 instance 1 中。 同样，您可以用 no 命令把 vlan 从 instance 中删除，删除的 vlan 自动转入 instance 0。
Ruijie(config)# **erps raps-vlan** *vlan-id*	进入 ERPS 配置模式
Ruijie(config-erps)# **protected-instance** *instance-id-list*	配置以太环的保护 VLAN（*instance-id-list* 所对应的 VLAN 即为保护 VLAN。保护 VLAN 由该以太环的 R-APS VLAN + 该以太环需要保护的数据 VLAN 组成）。

如果要关闭负载均衡功能，可用 erps 模式下的 **no protected-instance** 配置命令进行设置。

下面以图 3 中的 Node4 节点为例，简要说明负载均衡的配置方式。假设图 3 中 ERP1 的 R-APS VLAN 为 100，保护的数据 VLAN 为 1-99，101-2000；ERP2 的 R-APS VLAN 为 4093，保护的数据 VLAN 为 2001-4092，4094。则负载均衡的配置如下：

进入全局配置模式。

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

配置 ERP1 的保护 VLAN。

```
Ruijie(config)# spanning-tree mst configuration
Ruijie(config-mst)# instance 1 vlan 100, 1-99, 101-2000
Ruijie(config-mst)# exit
Ruijie(config)# erps raps-vlan 100
Ruijie(config-erps100)#  protected-instance 1
```

配置 ERP2 的保护 VLAN。

```
Ruijie(config)# spanning-tree mst configuration
Ruijie(config-mst)# instance 2 vlan 4093, 2001-4092, 4094
Ruijie(config-mst)# exit
Ruijie(config)# erps raps-vlan 4093

Ruijie(config-erps4093)#  protected-instance 2
```

17.2.10 配置链路状态检测方法

对于链路的状态检测，可直接检测链路的物理状态（up 或 down），也可通过 OAM（Operation, administration and maintenance，关于 OAM 的更多信息请参见 OAM 的配置手册）检测链路的逻辑状态（单向故障、双向故障 或 正常）。缺省情况下，采用直接监测链路物理状态的方法。进入特权模式，按以下步骤切换链路状态的监测方法：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式

Ruijie(config)# **erps monitor link-state by oam vlan** *vlan-id*	配置链路状态的检测方法

如果要恢复为缺省配置，可用 **no erps monitor link-state by oam** 全局配置命令进行设置。

配置举例：

进入全局配置模式。

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

配置链路状态的监测方法。

```
Ruijie(config)# erps monitor link-state by oam vlan 100
```

上述配置命令仅是让 ERPS 依据 OAM 的检测结果执行拓扑切换。若要让 OAM 执行链路状态检测，还需开启 OAM 等，具体请参见 OAM 的配置手册。

若采用 OAM 方式进行链路检测，由于 OAM 检测链路状态的效率较低，可能会导致拓扑变化时的收敛时间较长。

17.2.11 查看ERPS配置信息

在特权模式下使用如下命令查看设备的 ERPS 配置及状态：

命令	作用
Ruijie# **show erps**	查看设备的 ERPS 配置及状态。

以下例子使用 **show erps** 命令查看设备的 ERPS 配置及状态息：

```
Ruijie# show erps
ERPS Information
Global Status                    : Enabled
Link monitored by           : Not Oam
-------------------------------------------
R-APS VLAN                       : 4093
Ring Status                      : Enabled
West Port                        : Gi 0/5 (Blocking)
East Port                        : Gi 0/7 (Forwarding)
RPL Port                         : West Port
Protected VLANs                  : ALL
RPL Owner                        : Enabled
Holdoff Time                     : 0 milliseconds
Guard Time                       : 500 milliseconds
WTR Time                         : 5 minutes
Current Ring State               : Idle
-------------------------------------------
R-APS VLAN                       : 100
Ring Status                      : Enabled
```

```
West Port                       : Virtual Channel
East Port                       : Gi 0/10 (Forwarding)
RPL Port                        : None
Protected VLANs                 : ALL
RPL Owner                       : Disabled
Holdoff Time                    : 0 milliseconds
Guard Time                      : 500 milliseconds
WTR Time                        : 5 minutes
Current Ring State              : Idle
-----------------------------------------
R-APS VLAN                      : 200
Ring Status                     : Enabled
West Port                       : Virtual Channel
East Port                       : 12 (Forwarding)
RPL Port                        : None
Protected VLANs                 : ALL
RPL Owner                       : Disabled
Holdoff Time                    : 0 milliseconds
Guard Time                      : 500 milliseconds
WTR Time                        : 5 minutes
Current Ring State              : Idle

Ruijie# show erps raps_vlan 4093 sub-ring
R-APS VLAN: 4093
Sub-Ring R-APS VLANs    TC Propagation State
------------------      --------------------
100                        Enable
200                        Enable
```

17.3 ERPS典型配置举例

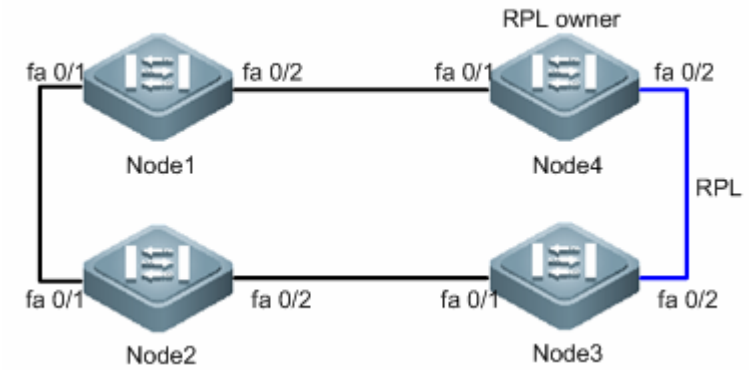
17.3.1 单环配置举例

组网需求

- Node1、Node2、Node3 和 Node4 节点构成一个单环拓扑；
- 环的 R-APS VLAN 为 4093；
- Node4 节点为 RPL owner 节点，Node3 和 Node4 间的链路为 RPL；

组网拓扑

图 17-6 单环配置举例



配置要点

必须且只能配置一个 RPL owner 节点；必须且只能配置一条 RPL；所有节点必须具有相同的 R-APS VLAN。

配置步骤

- 配置 Node1

进入全局配置模式

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

配置 R-APS VLAN

```
Ruijie(config)# erps raps-vlan 4093
Ruijie(config-erps4093)# exit
```

配置以太环端口的链路模式。

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
Ruijie(config)# interface fastEthernet 0/2
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
```

进入 erps 配置模式。

```
Ruijie(config)# erps raps-vlan 4093
```

配置加入以太环，参于 ERPS 协议计算的端口。

```
Ruijie(config-erps4093)# ring-port west fastEthernet 0/1 east fastEthernet 0/2
```

使能指定环的 ERPS 功能。

```
Ruijie(config-erps4093)# state enable
```

使能全局 ERPS 功能。

```
Ruijie(config-erps4093)# exit
Ruijie(config)# erps enable
```

- 配置 Node2

Node2 的配置同 Node1。

- 配置 Node3

Node3 需要在 Node1 配置命令的基础上（不包括使能指定环的 ERPS 功能的命令）

再配置以下命令：

进入全局配置模式

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

进入 erps 配置模式。

```
Ruijie(config)# erps raps-vlan 4093
```

指明 RPL 链路所在的端口。

```
Ruijie(config-erps4093)# rpl-port east
```

使能指定环的 ERPS 功能。

```
Ruijie(config-erps4093)# state enable
```

- 配置 Node4

Node4 需要在 Node1 配置命令的基础上（不包括使能指定环的 ERPS 功能的命令）

再配置以下命令：

进入全局配置模式

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

进入 erps 配置模式。

```
Ruijie(config)# erps raps-vlan 4093
```

指明 RPL 链路所在的端口和 RPL owner。

```
Ruijie(config-erps4093)# rpl-port east rpl-owner
```

使能指定环的 ERPS 功能。

```
Ruijie(config-erps4093)# state enable
```

显示验证

在各个节点上执行 show erps 命令，确认配置。以面以 Node4 节点为例，举例说明：

```
Ruijie# show erps
ERPS Information
Global Status                    : Enabled
Link monitored by           : Not Oam
-----------------------------------------
R-APS VLAN                       : 4093
Ring Status                      : Enabled
West Port                        : Fa 0/1 (Forwardin)
East Port                        : Fa 0/2 (Blocking)
RPL Port                         : East Port
Protected VLANs                  : ALL
RPL Owner                        : Enabled
Holdoff Time                     : 0 milliseconds
Guard Time                       : 500 milliseconds
WTR Time                         : 5 minutes
Current Ring State               : Idle
```

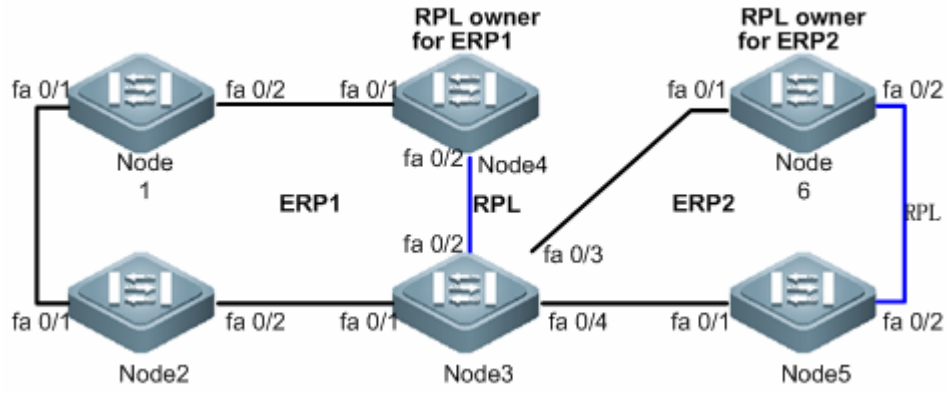
17.3.2 相切环配置举例

组网需求

- Node1、Node2、Node3 和 Node4 节点构成一个普通的以太环 ERP1；Node3、Node5、Node6 构成另一个普通以太环 ERP2。
- ERP1 的 R-APS VLAN 为 4093；ERP2 的 R-APS VLAN 为 100。
- Node4 节点为 RPL owner 节点，Node3 和 Node4 间的链路为 ERP1 的 RPL；Node6 点为 RPL owner 节点，Node5 和 Node6 的链路为 ERP2 的 RPL。

组网拓扑

图 17-7 相切环配置举例



配置要点

ERP1 和 ERP2 都必须且只能配置一个 RPL owner 节点；ERP1 和 ERP2 都必须且只能配置一条 RPL；所有节点的 ERP1 必须具有相同的 R-APS VLAN；所有节点的 ERP2 必须具有相同的 R-APS VLAN。

配置步骤

- 配置 Node1

进入全局配置模式

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

配置 R-APS VLAN

```
Ruijie(config)# erps raps-vlan 4093
Ruijie(config-erps4093)# exit
```

配置以太环端口的链路模式。

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
Ruijie(config)# interface fastEthernet 0/2
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
```

进入 erps 配置模式。

```
Ruijie(config)# erps raps-vlan 4093
```

配置加入以太环，参于 ERPS 协议计算的端口。

```
Ruijie(config-erps4093)#  ring-port west fastEthernet 0/1 east fastEthernet 0/2
```

使能指定环的 ERPS 功能。

```
Ruijie(config-erps4093)# state enable
```

使能全局 ERPS 功能。

```
Ruijie(config-erps4093)# exit
Ruijie(config)# erps enable
```

- 配置 Node2

Node2 的配置同 Node1。

- 配置 Node3

Node3 需要在 Node1 配置命令的基础上（不包括使能指定环的 ERPS 功能的命令）

再配置以下命令：

进入全局配置模式

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

进入 erps 配置模式。

```
Ruijie(config)# erps raps-vlan 4093
```

指明 RPL 链路所在的端口。

```
Ruijie(config-erps4093)# rpl-port east
```

使能指定环的 ERPS 功能。

```
Ruijie(config-erps4093)# state enable
```

配置 ERP2 的 R-APS VLAN

```
Ruijie(config-erps4093)# exit
Ruijie(config)# erps raps-vlan 100
Ruijie(config-erps100)# exit
```

配置 ERP2 环端口的链路模式。

```
Ruijie(config)# interface fastEthernet 0/3
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
Ruijie(config)# interface fastEthernet 0/4
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
```

进入 ERPS 配置模式。

```
Ruijie(config)# erps raps-vlan 100
```

配置加入以太环，参于 ERPS 协议计算的端口。

```
Ruijie(config-erps100)# ring-port west fastEthernet 0/3 east fastEthernet 0/4
```

使能 ERP2 的 ERPS 功能。

```
Ruijie(config-erps100)# state enable
```

- 配置 Node4

Node4 需要在 Node1 配置命令的基础上（不包括使能指定环的 ERPS 功能的命令）

再配置以下命令：

进入全局配置模式

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

进入 erps 配置模式。

```
Ruijie(config)# erps raps-vlan 4093
```

指明 RPL 链路所在的端口和 RPL owner。

```
Ruijie(config-erps4093)# rpl-port east rpl-owner
```

使能指定环的 ERPS 功能。

```
Ruijie(config-erps4093)# state enable
```

- 配置 Node5

进入全局配置模式

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

配置 R-APS VLAN

```
Ruijie(config)# erps raps-vlan 100
Ruijie(config-erps100)# exit
```

配置以太环端口的链路模式。

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
Ruijie(config)# interface fastEthernet 0/2
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
```

进入 erps 配置模式。

```
Ruijie(config)# erps raps-vlan 100
```

配置加入以太环，参于 ERPS 协议计算的端口。

```
Ruijie(config-erps100)# ring-port west fastEthernet 0/1 east fastEthernet 0/2
```

指明 RPL 链路所在的端口。

```
Ruijie(config-erps100)# rpl-port east
```

使能指定环的 ERPS 功能。

```
Ruijie(config-erps100)# state enable
```

使能全局 ERPS 功能。

```
Ruijie(config-erps100)# exit
Ruijie(config)# erps enable
```

- 配置 Node6

Node6 的配置基本同 Node5，只不过需将“**rpl-port east**”命令改为用“**rpl-port east rpl-owner**”。

显示验证

在各个节点上执行 **show erps** 命令，确认配置。以面以 Node3 节点为例，举例说明：

```
Ruijie# show erps
ERPS Information
Global Status                    : Enabled
Link monitored by           : Not Oam
-----------------------------------------
R-APS VLAN                       : 100
Ring Status                      : Enabled
West Port                        : Fa 0/3 (Forwarding)
East Port                        : Fa 0/4 (Forwarding)
RPL Port                         : None
Protected VLANs                  : ALL
RPL Owner                        : Disabled
Holdoff Time                     : 0 milliseconds
Guard Time                       : 500 milliseconds
WTR Time                         : 5 minutes
Current Ring State               : Idle
-----------------------------------------
R-APS VLAN                       : 4093
Ring Status                      : Enabled
West Port                        : Fa 0/1 (Forwarding)
East Port                        : Fa 0/2 (Forwarding)
RPL Port                         : East Port
Protected VLANs                  : ALL
RPL Owner                        : Disabled
Holdoff Time                     : 0 milliseconds
Guard Time                       : 500 milliseconds
WTR Time                         : 5 minutes
Current Ring State               : Idle
```

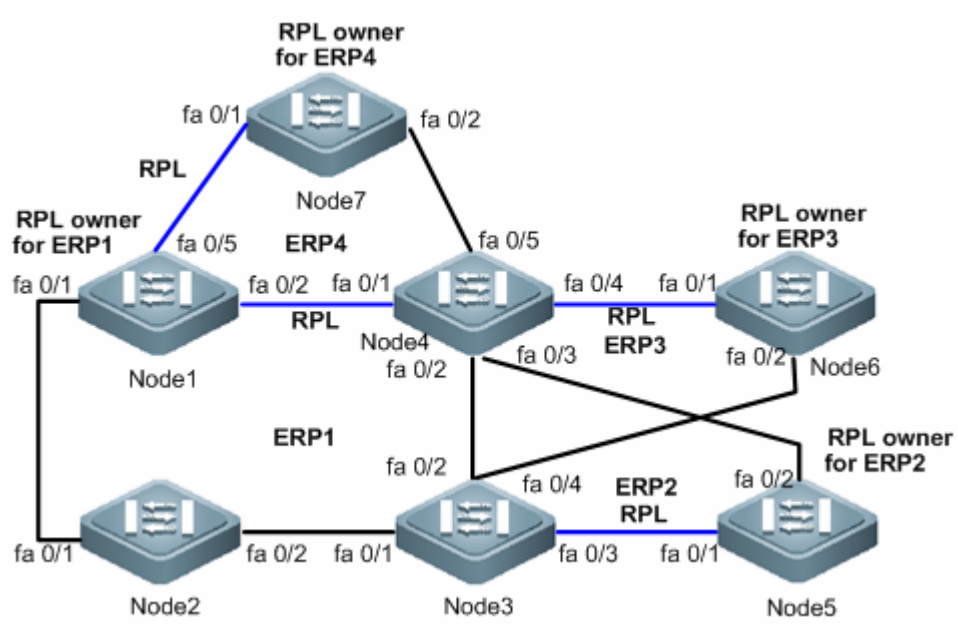
17.3.3 相交环配置举例

组网需求

- Node1、Node2、Node3 和 Node4 节点构成一个普通的以太环 ERP1；Node3、Node5 和 Node4 构成一个以太子环 ERP2；Node3、Node6 和 Node4 构成一个以太子环 ERP3；Node1、Node4 和 Node7 构成一个以太子环 ERP4。
- ERP1 的 R-APS VLAN 为 4093;ERP2 的 R-APS VLAN 为 100;ERP3 的 R-APS VLAN 为 200;ERP4 的 R-APS VLAN 为 300。
- Node4 节点为 RPL owner 节点，Node1 和 Node4 间的链路为 ERP1 的 RPL；Node5 点为 RPL owner 节点，Node3 和 Node5 的链路为 ERP2 的 RPL;Node6 节点为 RPL owner 节点,Node4 和 Node6 间的链路为 ERP1 的 RPL;Node7 节点为 RPL owner 节点，Node7 和 Node1 间的链路为 ERP1 的 RPL。

组网拓扑

图 17-8 多环相交配置举例



配置要点

每个 ERP 环都必须且只能配置一个 RPL owner 节点；每个 ERP 环都必须且只能配置一条 RPL；所有节点的 ERP1 必须具有相同的 R-APS VLAN；所有节点的 ERP2 必须具有相同的 R-APS VLAN；所有节点的 ERP3 必须具有相同的 R-APS VLAN；所有节点的 ERP4 必须具有相同的 R-APS VLAN。

配置步骤

- 配置 Node1

进入全局配置模式

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

配置 R-APS VLAN 4093

```
Ruijie(config)# erps raps-vlan 4093
Ruijie(config-erps4093)# exit
```

配置以太环端口的链路模式。

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
Ruijie(config)# interface fastEthernet 0/2
Ruijie(config-if)# switchport mode trunk
```

```
Ruijie(config-if)# exit
```

进入 erps 配置模式。

```
Ruijie(config)# erps raps-vlan 4093
```

配置加入以太环，参于 ERPS 协议计算的端口。

```
Ruijie(config-erps4093)# ring-port west fastEthernet 0/1 east fastEthernet 0/2
```

指明 RPL 链路所在的端口和 RPL owner。

```
Ruijie(config-erps4093)# rpl-port east rpl-owner
```

使能指定环的 ERPS 功能。

```
Ruijie(config-erps4093)# state enable
```

使能全局 ERPS 功能。

```
Ruijie(config-erps4093)# exit
Ruijie(config)# erps enable
```

配置子环 ERP4 的 R-APS VLAN

```
Ruijie(config)# erps raps-vlan 300
Ruijie(config-erps300)# exit
```

配置 ERP4 环端口的链路模式。

```
Ruijie(config)# interface fastEthernet 0/5
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
```

进入 ERPS 配置模式。

```
Ruijie(config)# erps raps-vlan 300
```

配置加入以太环，参于 ERPS 协议计算的端口。

```
Ruijie(config-erps300)# ring-port west fastEthernet 0/5 east virtual-channel
```

使能 ERP4 的 ERPS 功能。

```
Ruijie(config-erps300)# state enable
```

关联 ERP1 和 ERP2、ERP3、ERP4。

```
Ruijie(config-erps300)#  exit
Ruijie(config)# erps raps-vlan 4093
Ruijie(config-erps4093)# associate sub-ring raps-vlan 100,200,300
```

- 配置 Node2

进入全局配置模式

```
Ruijie# configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
```

配置 R-APS VLAN 4093

```
Ruijie(config)# erps raps-vlan 4093
Ruijie(config-erps4093)# exit
```

配置以太环端口的链路模式。

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
Ruijie(config)# interface fastEthernet 0/2
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
```

进入 erps 配置模式。

```
Ruijie(config)# erps raps-vlan 4093
```

配置加入以太环，参于 ERPS 协议计算的端口。

```
Ruijie(config-erps4093)# ring-port west fastEthernet 0/1 east fastEthernet 0/2
```

使能指定环的 ERPS 功能。

```
Ruijie(config-erps4093)# state enable
```

使能全局 ERPS 功能。

```
Ruijie(config-erps4093)# exit
Ruijie(config)# erps enable
```

#关联 ERP1 和 ERP2、ERP3、ERP4。

```
Ruijie(config-erps300)# exit
Ruijie(config)# erps raps-vlan 4093
Ruijie(config-erps4093)# associate sub-ring raps-vlan 100,200,300
```

- 配置 Node3

Node3 需要在 Node2 配置的基础上，再配置以下命令：

进入全局配置模式

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

配置子环 ERP2 的 R-APS VLAN

```
Ruijie(config)# erps raps-vlan 100
Ruijie(config-erps100)# exit
```

配置 ERP2 环端口的链路模式。

```
Ruijie(config)# interface fastEthernet 0/3
```

```
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
```

进入 ERPS 配置模式。

```
Ruijie(config)# erps raps-vlan 100
```

配置加入以太环，参于 ERPS 协议计算的端口。

```
Ruijie(config-erps100)# ring-port west virtual-channel east fastEthernet 0/3
```

使能 ERP2 的 ERPS 功能。

```
Ruijie(config-erps100)# state enable
```

配置子环 ERP3 的 R-APS VLAN

```
Ruijie(config)# erps raps-vlan 200
Ruijie(config-erps200)# exit
```

配置 ERP2 环端口的链路模式。

```
Ruijie(config)# interface fastEthernet 0/3
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
```

进入 ERPS 配置模式。

```
Ruijie(config)# erps raps-vlan 200
```

配置加入以太环，参于 ERPS 协议计算的端口。

```
Ruijie(config-erps200)# ring-port west virtual-channel east fastEthernet 0/3
```

使能 ERP2 的 ERPS 功能。

```
Ruijie(config-erps200)# state enable
```

关联普通以太环 ERP1 和子环 ERP2、ERP3 和 ERPS4。

```
Ruijie(config-erps300)# exit
Ruijie(config)# erps raps-vlan 4093
Ruijie(config-erps4093)# associate sub-ring raps-vlan 100,200,300
```

- 配置 Node4

Node4 需要在 Node2 配置的基础上（不包括使能指定环的 ERPS 功能的命令）

再配置以下命令：

进入全局配置模式

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

进入 erps 配置模式。

```
Ruijie(config)# erps raps-vlan 4093
```

指明 RPL 链路所在的端口和 RPL owner。

```
Ruijie(config-erps4093)# rpl-port west
```

使能指定环的 ERPS 功能。

```
Ruijie(config-erps4093)# state enable
```

配置子环 ERP2 的 R-APS VLAN

```
Ruijie(config)# erps raps-vlan 100
Ruijie(config-erps100)# exit
```

配置 ERP2 环端口的链路模式。

```
Ruijie(config)# interface fastEthernet 0/3
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
```

进入 ERPS 配置模式。

```
Ruijie(config)# erps raps-vlan 100
```

配置加入以太环，参于 ERPS 协议计算的端口。

```
Ruijie(config-erps100)# ring-port west virtual-channel east fastEthernet 0/3
```

使能 ERP2 的 ERPS 功能。

```
Ruijie(config-erps100)# state enable
```

配置子环 ERP3 的 R-APS VLAN

```
Ruijie(config)# erps raps-vlan 200
Ruijie(config-erps200)# exit
```

配置 ERP2 环端口的链路模式。

```
Ruijie(config)# interface fastEthernet 0/3
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
```

进入 ERPS 配置模式。

```
Ruijie(config)# erps raps-vlan 200
```

配置加入以太环，参于 ERPS 协议计算的端口。

```
Ruijie(config-erps200)# ring-port west virtual-channel east fastEthernet 0/3
```

使能 ERP2 的 ERPS 功能。

```
Ruijie(config-erps200)# state enable
```

配置子环 ERP4 的 R-APS VLAN

```
Ruijie(config)# erps raps-vlan 300
Ruijie(config-erps300)# exit
```

配置 ERP2 环端口的链路模式。

```
Ruijie(config)# interface fastEthernet 0/3
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
```

进入 ERPS 配置模式。

```
Ruijie(config)# erps raps-vlan 300
```

配置加入以太环，参于 ERPS 协议计算的端口。

```
Ruijie(config-erps300)#  ring-port west virtual-channel east fastEthernet 0/5
```

使能 ERP2 的 ERPS 功能。

```
Ruijie(config-erps300)# state enable
```

关联普通以太环 ERP1 和子环 ERP2、ERP3 和 ERPS4。

```
Ruijie(config-erps300)#  exit
Ruijie(config)# erps raps-vlan 4093
Ruijie(config-erps4093)# associate sub-ring raps-vlan 100,200,300
```

- 配置 Node5

进入全局配置模式

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

配置 R-APS VLAN

```
Ruijie(config)# erps raps-vlan 100
Ruijie(config-erps100)# end
```

配置以太环端口的链路模式。

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
Ruijie(config)# interface fastEthernet 0/2
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
```

进入 erps 配置模式。

```
Ruijie(config)# erps raps-vlan 100
```

配置加入以太环，参于 ERPS 协议计算的端口。

```
Ruijie(config-erps100)# ring-port west fastEthernet 0/1 east fastEthernet 0/2
```

指明 RPL 链路所在的端口和 RPL owner。

```
Ruijie(config-erps100)# rpl-port east rpl-owner
```

使能指定环的 ERPS 功能。

```
Ruijie(config-erps100)# state enable
```

使能全局 ERPS 功能。

```
Ruijie(config-erps100)# exit
Ruijie(config)# erps enable
```

- 配置 Node6

Node6 的配置基本同 Node5，只是需将 R-APS VLAN 改为 VLAN 200。

- 配置 Node7

Node7 的配置基本同 Node5，只是需将 R-APS VLAN 改为 VLAN 300。

显示验证

在各个节点上执行 **show erps** 命令，确认配置。以面以 Node3 节点为例，举例说明：

```
Ruijie# show erps
ERPS Information
Global Status                    : Enabled
Link monitored by           : Not Oam
------------------------------------------
R-APS VLAN                       : 100
Ring Status                      : Enabled
West Port                        : Virtual Channel
East Port                        : Fa 0/3 (Forwarding)
RPL Port                         : None
Protected VLANs                  : ALL
RPL Owner                        : Disabled
Holdoff Time                     : 0 milliseconds
Guard Time                       : 500 milliseconds
WTR Time                         : 5 minutes
Current Ring State               : Idle
------------------------------------------
R-APS VLAN                       : 200
Ring Status                      : Enabled
West Port                        : Virtual Channel
East Port                        : Fa 0/4 (Forwarding)
RPL Port                         : None
Protected VLANs                  : ALL
RPL Owner                        : Disabled
Holdoff Time                     : 0 milliseconds
```

```
Guard Time                          : 500 milliseconds
WTR Time                            : 5 minutes
Current Ring State                  : Idle
----------------------------------------------
R-APS VLAN                          : 4093
Ring Status                         : Enabled
West Port                           : Fa 0/1 (Forwarding)
East Port                           : Fa 0/2 (Blocking)
RPL Port                            : East Port
Protected VLANs                     : ALL
RPL Owner                           : Disabled
Holdoff Time                        : 0 milliseconds
Guard Time                          : 500 milliseconds
WTR Time                            : 5 minutes
Current Ring State                  : Idle
```

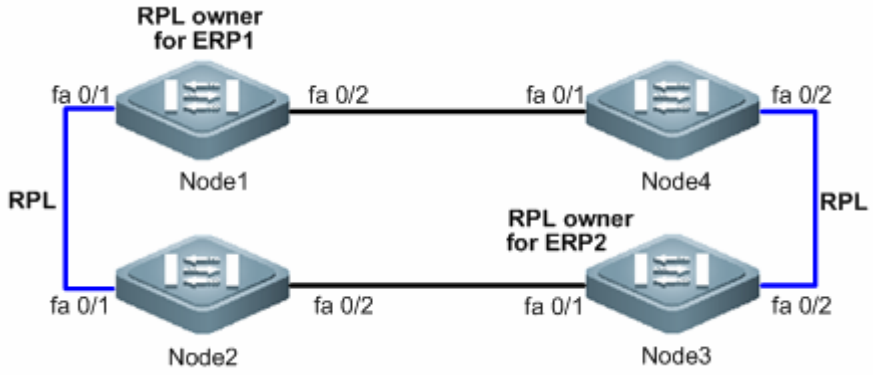
17.3.4 负载均衡配置举例

组网需求

- Node1、Node2、Node3 和 Node4 节点构成一个物理拓扑环。该物理拓扑环对应两个以太环 ERP1 和 ERP2。
- ERP1 的 RPL owner 为 Node1 节点，RPL 链路为 Node1 和 Node2 间的链路。ERP2 的 RPL owner 为 Node3 节点，RPL 链路为 Node3 和 Node4 间的链路。
- ERP1 的 R-APS VLAN 为 100，所保护 R 的数据 VLAN 为 1-99，101-2000。ERP2 的 R-APS VLAN 为 4093，所保护的数据 VLAN 为 2001-4092，4094。

组网拓扑

图 17-9 负载均衡配置举例



配置要点

以太环的保护 VLAN 由该以太环的 R-APS VLAN + 该以太环需要保护的数据 VLAN 组成。

配置步骤

- 配置 Node1

进入全局配置模式

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

配置以太环 ERP1：

配置以太环 ERP1 的端口的链路模式。

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
Ruijie(config)# interface fastEthernet 0/2
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
```

配置以太环 ERP1 的保护 VLAN、端口和 RPL。

```
Ruijie(config)# spanning-tree mst configuration
Ruijie(config-mst)# instance 1 vlan 1-2000
Ruijie(config-mst)# exit
Ruijie(config)# erps raps-vlan 100
Ruijie(config-erps100)# protected-instance 1
Ruijie(config-erps100)# ring-port west fastEthernet 0/1 east fastEthernet 0/2
Ruijie(config-erps100)# rpl-port west rpl-owner
```

配置以太环 ERP2：

配置加入以太环 ERP1，参于 ERPS 协议计算的端口。

```
Ruijie(config)# spanning-tree mst configuration
Ruijie(config-mst)# instance 2 vlan 2001-4094
Ruijie(config-mst)# exit
Ruijie(config)# erps raps-vlan 4093
Ruijie(config-erps4093)# protected-instance 2
Ruijie(config-erps4093)# ring-port west fastEthernet 0/1 east fastEthernet 0/2
```

使能指定环的 ERPS 功能和全局 ERPS 功能。

```
Ruijie(config-erps4093)# state enable
Ruijie(config-erps4093)# exit
Ruijie(config)# erps enable
```

- 配置 Node2

除配置 RPL 的命令外，Node2 上的其它配置命令同 Node1。

Node2 上配置以太环 ERP1 的 RPL 的命令为：

```
Ruijie(config)# erps raps-vlan 100
Ruijie(config-erps100)# rpl-port west
```

■ 配置 Node3

除配置 RPL 的命令外，Node3 上的其它配置命令同 Node1。

Node2 上不配置以太环 ERP1 的 RPL，则是配置以太环 ERP2 的 RPL：

```
Ruijie(config)# erps raps-vlan 4093
Ruijie(config-erps4093)# rpl-port east rpl-owner
```

■ 配置 Node4

除配置 RPL 的命令外，Node4 上的其它配置命令同 Node3。

Node2 上配置以太环 ERP2 的 RPL 的命令为：

```
Ruijie(config)# erps raps-vlan 100
Ruijie(config-erps100)# rpl-port east
```

显示验证

在各个节点上执行 **show erps** 命令，确认配置。以面以 Node1 节点为例，举例说明：

```
Ruijie# show erps
ERPS Information
Global Status                    : Enabled
Link monitored by           : Not Oam
-------------------------------------------
R-APS VLAN                       : 200
Ring Status                      : Enabled
West Port                        : Gi 0/1 (Blocking)
East Port                        : Gi 0/2 (Forwarding)
RPL Port                         : West Port
Protected VLANs                  : 1-2000
RPL Owner                        : Enabled
Holdoff Time                     : 0 milliseconds
Guard Time                       : 500 milliseconds
WTR Time                         : 5 minutes
Current Ring State               : Idle
-------------------------------------------
R-APS VLAN                       : 4093
Ring Status                      : Enabled
West Port                        : Gi 0/1 (Forwarding)
East Port                        : Gi 0/2 (Blocking)
RPL Port                         : West Port
Protected VLANs                  : 2001-4094
```

```
RPL Owner                       : Enabled
Holdoff Time                    : 0 milliseconds
Guard Time                      : 500 milliseconds
WTR Time                        : 5 minutes
Current Ring State              : Idle
```

18 BUFFER

18.1 概述

BUFFER 管理指的是对芯片缓存进行合理的分配，从而使得交换设备能更好应对各种突发流量。

网络中存在的不总是平稳的流量，也存在各式各样的突发流量。当网络流量平稳且带宽足够时，所有的数据流都得到了较好的处理；当网络存在突发流量时，即使平均的流量速率不超过带宽，也可能发生数据流丢弃。

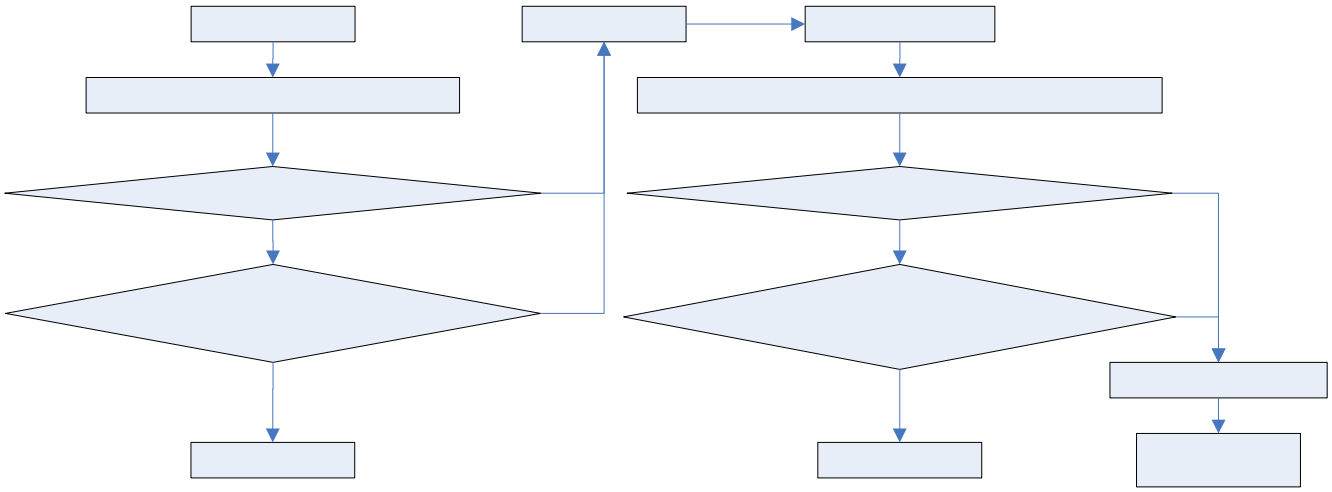
数据报文进入交换设备中，在转发之前，都会被存储在交换设备的缓存当中。正常情况下，数据报文在缓存中的驻留时间很短，在微秒级别内就被转发出去；当存在突发流量的情况下，如果突发流量的瞬时速率超过交换设备的处理能力，那么来不及处理的数据报文就在交换设备的缓存中堆积，一旦缓存不足就会发生丢包。此时 BUFFER 管理就应运而生，可以通过合理的配置缓存来为不同的业务分配不同的缓存使用量，从而达到优化网络的目的。

18.2 功能详解

工作原理

缓存在硬件的工作机制

在硬件上缓存分输入和输出两个方向进行管理，处理机制如下图所示：



由于在缓存管理时，输入方向都调成最大值从而保证输入方向不丢包，让丢包发生在输出方向。因此输入方向的缓存不开放调整，CLI 仅提供输出方向的缓存调整。缓存调整通过配置端口组缓存限制来使得各端口拥有不同的缓存使用量。

保证缓存

保证缓存也称之为独享缓存，这部分缓存是基于各个队列进行分配，某个队列的保证缓存只能由该队列使用，其他队列无法使用。每个队列默认都会分配一定量的保证缓存，这部分缓存可以让该队列在平稳流量下正常线速转发报文。目前不支持配置。

共享缓存

整机总缓存中，扣除各队列的保证缓存后，剩下的就是总共享缓存。共享缓存可供所有端口使用。每个端口可以设置一个共享缓存的门限，该门限限制该端口最多可使用的共享缓存数量。当各端口配置的共享缓存总和超过全局的总共享缓存，此时采用的是先到先得的缓存占用机制。

↘ 缓存模式

缓存模式是一个全局的概念，是基于所有面板口的所有队列调整保证缓存和共享缓存。当前支持配 3 种缓存模式：默认缓存模式，Burst 增强缓存模式（即大缓存模式），无限制共享模式。

这 3 种缓存模式对应的队列保证缓存和共享缓存具体值依产品而定，几种模式的缓存管理特征及适用场景分别如下：

普通缓存模式

该模式兼顾考虑了交换机的突发大流量缓存能力、QoS 调度支持、流控支持三方面因素。对以上三方面的支持比较均衡，没有特别的偏向，因此支持程度都是适中。

- 适用环境：
  - 对缓存无特别需求的环境。因为该模式缓存管理较为中庸，兼顾考虑了各方面因素，出问题的概率较小；
  - 存在低速口且低速口正常工作不处于休眠状态的环境。所谓的低速口是指，端口形态为万兆加千兆的设备上出现协商为百兆的端口，或者端口形态为千兆加百兆的设备上出现协商为十兆的端口；
  - 部署 QoS 的环境。可以中等程度支持，表现为 1 个端口输入情况下同时有 5 个端口拥塞才会出现入口丢包进而 QoS 失效；
  - 部署流控的环境。可以中低程度支持，表现为 4 个端口同时打 1 个端口才会出现出口丢包进而流控失效；
- 不适用环境：
  - 具有特别明显的突发大流量特征的环境不适用，因为该模式下 Burst 缓存能力适中；
  - 没有部署流控但又对丢包容忍度较低的环境不适用，因为该模式下考虑对 QoS 中等支持，而 QoS 的特征即丢包；
- 典型应用：
  - 园区网环境。主要特征有：环境开放可能随时接入低速终端，对丢包容忍度较高（根据经验值，可以忍受 1%~2% 的丢包率）；

Burst 增强缓存模式

该模式主要基于普通缓存模式考虑的三方面因素对交换机的突发大流量缓存能力做增强支持，即 Burst 增强。由于 Burst、QoS、流控支持之间存在一定的矛盾互斥关系，因此在 Burst 增强模式下，QoS 和流控支持会适当减弱。Burst 增强模式的缓存配置特征主要是将输出队列缓存限制得比较大，提高单个端口队列及整机的缓存能力，同时也能支持流控及 QoS。

- 适用环境：
  - 拓扑稳定，接入到交换机的设备类型固定，交换机上不会随便接入低速网卡终端设备；
  - 具有特别明显的突发大流量特征的环境；
  - 对丢包容忍度较低的环境，因为单个队列缓存能力配置得尽量大，即使不开流控，也可以通过缓存来减少丢包；
  - 部署 QoS 的环境。但只能弱支持，表现为一个端口输入情况下同时有 2 个端口拥塞就会出现入口丢包进而 QoS 失效；
  - 部署流控的环境。但只能弱支持，表现为 2 个端口同时打 1 个端口才会出现出口丢包进而流控失效。在该模式下，流控部署一般建议仅接入交换机的上联口开启流控，而下联口不开启流控；
- 不适用环境：
  - 存在低速口的环境（低速口的定义参照以上普通缓存模式里的介绍）。因为该模式下缓存放开共享，单个队列的缓存能力更强，如果存在低速口，则会严重影响非低速口的缓存申请造成非低速口丢包严重的问题；
  - 组播网络。原因同存在低速口的情况类似，非组播出口可能受到严重影响；
- 典型应用：
  - 广播电视台的非线性编辑网络，配合流控使用（上联口开流控即可）。主要特征有：拓扑稳定，具有特别明显的

突发大流量特征，对丢包容忍度很低，没有部署 QoS；

- 广播电视台的 IPQAM 推流网络。主要特征有：具有特别明显的突发大流量特征，对丢包容忍度较低；
- 网络同传环境。主要特征有：接入到交换机的设备类型稳定，没有部署 QoS，对带宽利用率要求较高（缓存放开共享可以提高带宽利用率）；
- 视频监控网络。主要特征有：接入到交换机的设备类型稳定，对丢包容忍度较低；

无限制共享模式

该模式主要可以最大程度利用整机缓存，但不支持 QOS 及流控。主要出于兼容考虑而保留。

- 适用环境：
  - 拓扑稳定，接入到交换机的设备类型固定，交换机上不会随便接入低速网卡终端设备；
  - 具有特别明显的突发大流量特征的环境；
- 不适用环境：
  - 同 burst 增强模式；

18.3 配置详解

18.3.1 缺省配置

功能特性	缺省值
全局 buffer 模式	Default
全局自定义缓存	无
端口自定义组绑定	千兆端口绑定千兆端口组，万兆端口绑定万兆端口组

18.3.2 配置全局buffer模式

配置全局 buffer 模式

命令	作用
Ruijie(config)# **buffer mode {default | enhanced | shared}**	配置全局 buffer 模式

恢复默认模式使用 no buffer mode 命令，下面的例子说明了如何配置 buffer 模式为 burst 增强模式及无限制共享模式：

```
Ruijie#configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Ruijie(config)#buffer mode enhanced

Ruijie(config)#buffer mode shared
```

查看配置

- 查看全局 buffer 模式配置

```
Ruijie# show buffer configuration

Buffer mode: Shared
```

```
port-group    threshold

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

18.3.3 配置全局自定义缓存

配置全局自定义缓存

命令	作用
Ruijie(config)# **buffer threshold egress-port-group {ge | xe | udf [pgid]} set [persent]**	配置全局自定义缓存水线

删除自定义缓存配置使用 no buffer threshold egress-port-group {ge | xe | udf [pgid]}命令，下面的例子说明了如何配置千兆端口组的输出缓存为整机的 50%：

```
Ruijie#configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Ruijie(config)# buffer threshold egress-port-group ge set 50
```

下面的例子说明了如何配置自定义端口组 1 的输出缓存为整机的 10%：

```
Ruijie#configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Ruijie(config)# buffer threshold egress-port-group udf 1 set 10
```

查看配置

- 查看全局 buffer 模式配置

```
Ruijie# show buffer configuration

Buffer mode: Default

port-group    threshold

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

Ge            50

Udf 1         10
```

18.3.4 配置端口自定义组绑定

配置端口自定义组绑定

命令	作用
Ruijie(config)# **buffer egress-port-group udf [pgid]**	配置端口自定义组绑定

恢复默认绑定使用 no buffer egress-port-group udf 命令，下面的例子说明了如何配置端口 1 绑定到自定义组 1：

```
Ruijie#configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Ruijie(config)# interface GigabitEthernet 0/1

Ruijie(config-if-GigabitEthernet 0/1)# buffer egress-port-group udf 1
```

查看配置

- 查看端口 buffer 配置

```
Ruijie# show buffer interface

Interface                port-group

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

GigabitEthernet 0/1      udf 1

GigabitEthernet 0/2      udf 1
```

配置指南-IP 地址及应用

本分册介绍 IP 地址及应用配置指南相关内容，包括以下章节：

1. IP 地址与服务
2. IPv6
3. DHCP
4. UDP-Helper
5. DHCPv6
6. DNS
7. FTP Server
8. FTP Client
9. IPv6 隧道
10. 网络通信检测工具
11. TCP
12. IPv4 快转

1 IP 地址与服务

1.1 配置IP地址

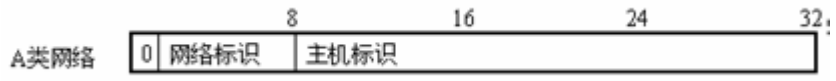
1.1.1 IP地址简介

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。

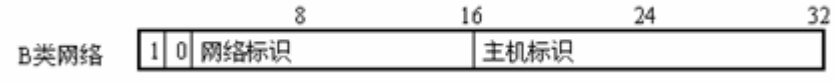
A 类地址，最高比特位为“0”，有 7 个比特位表示网络号，24 个比特位表示本地地址。这样总共有 128 个 A 类网络。

图 1-1



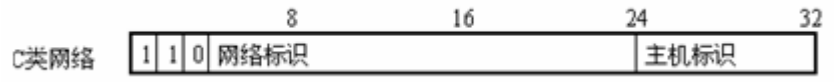
B 类地址，前两个最高比特位为“10”，有 14 个比特位表示网络号，16 个比特位表示本地地址。这样总共有 16,348 个 B 类网络。

图 1-2



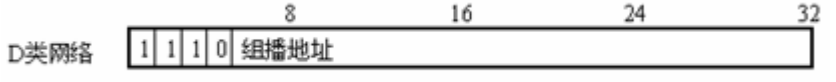
C 类地址，前三个最高比特位为“110”，有 21 个比特位表示网络号，8 个比特位表示本地地址。这样总共有 2,097,152 个 C 类网络。

图 1-3



D 类地址，前四个最高比特位为“1110”，其余比特位为组播地址。

图 1-4



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。

1.1.2 配置IP地址

IP 地址配置任务包括以下各项，但只有第一项配置是必须要做，其它任务可以根据网络的具体需要决定是否要执行。

- 配置接口 IP 地址（要求）
- 配置地址解析协议（ARP）（可选）
- 关闭 IP 路由（可选）
- 配置广播包处理（可选）

1.1.2.1 配置接口IP地址

一个设备只有配置了 IP 地址，才可以接收和发送 IP 数据包，接口配置了 IP 地址，说明该接口允许运行 IP 协议。

要分配一个接口的 IP 地址，在接口配置模式中执行以下命令：

命令	作用
Ruijie(config-if)# **ip address** *ip-address mask*	设置一个接口的 IP 地址
Ruijie(config-if)# **no ip address**	取消一个接口的 IP 地址配置

网络掩码也是一个 32 比特的数值，标识着该 IP 地址的哪几个比特为网络部分。网络掩码中，值为“1”的比特对应的 IP 地址比特位就是网络部分，值为“0”的比特对应的 IP 地址比特位就是主机地址部分。如 A 类网络对应的网络掩码为“255.0.0.0”。您可以利用网络掩码对一个网络进行子网划分，子网划分就是将主机地址部分的一些比特位也作为网络部分，缩小主机容量，增加网络的数量，这时的网络掩码就称为子网掩码。

理论上，子网掩码的比特位可以是主机地址部分中的任何一段比特位。

只支持从网络部分开始的从左到右连续的子网掩码。

接口配置多个 IP 地址

锐捷产品可以支持一个接口配置多个 IP 地址，其中一个为主 IP 地址，其余全部为次 IP 地址。次 IP 地址的配置理论上没有数目限制，但是次 IP 地址与主 IP 以及次 IP 之间地址必须属于不同网络。在网络建设中，会经常使用到次 IP 地址，通常在以下情况下应该考虑使用次 IP 地址：

一个网络没有足够多的主机地址。例如，现在一般局域网需要一个 C 类网络，可分配 254 台主机。但是当局域网主机超过 254 台时，一个 C 类网络将不够分配，有必要分配另一个 C 类网络地址。这样设备就需要连接两个网络，所以就需要配置多个 IP 地址。

许多旧的网络是基于第二层的桥接网络，没有进行子网的划分。次 IP 地址的使用可以使该网络很容易升级到基于 IP 层的路由网络。对于每个子网，设备都配置一个 IP 地址。

一个网络的两个子网被另外一个网络隔离开，您可以创建一个被隔离网络的子网，通过配置次 IP 地址的方式，将隔离的子网连接起来。一个子网不能在设备的两个或两个以上接口出现。

配置次 IP 地址之前，需要确定已经配置了主 IP 地址。如果网络上的一台设备配置了次 IP 地址，则其它设备也必须配置同一网络的次 IP 地址。当然如果其它设备原先没有分配 IP 地址，可以配置为主地址。

要配置次 IP 地址，在接口配置模式中执行以下命令：

命令	作用
Ruijie(config-if)# **ip address** *ip-address mask* secondary	设置接口次 IP 地址
Ruijie(config-if)# **no ip address** *ip-address mask* **secondary**	取消接口次 IP 地址配置

1.1.2.2 配置地址解析协议（ARP）

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

局域网上两台 IP 设备之间需要通信，必须要知道对方的 48 比特的 MAC 地址。根据 IP 地址来获知 MAC 地址的过程称为地址解析（ARP）。而根据 MAC 地址获知 IP 地址的过程称为反向地址解析（RARP）。地址解析的方式有两类：1）地址解

析协议（ARP）；2）代理地址解析协议（Proxy ARP）。关于 ARP 、Proxy ARP、RARP，分别在 RFC 826，RFC 1027，RFC 903 文档中描述。

ARP 是用来绑定 MAC 地址和 IP 地址的，以 IP 地址作为输入，ARP 能够知道其关联的 MAC 地址。一旦知道了 MAC 地址，IP 地址与 MAC 地址对应关系就会保存在设备的 ARP 缓冲中。有了 MAC 地址，IP 设备就可以封装链路层的帧，然后将数据帧发送到局域网上去。缺省配置下，以太网上 IP 和 ARP 的封装为 Ethernet II 类型，也可以封装成其它类型的以太网帧类型如 SNAP。

RARP 的工作原理与 ARP 类似，不过 RARP 是以 MAC 地址作为输入，然后得到关联的 IP 地址。RARP 通常应用在无盘工作站上。

通常情况下，不需要特别配置设备的地址解析已经可以工作了。

静态配置 ARP

ARP 协议提供了 IP 地址和 MAC 地址动态映射的功能，通常情况下不需要进行静态配置。锐捷产品通过配置静态 ARP，还可以响应不是属于自己 IP 地址的 ARP 请求。

要配置静态 ARP，在全局配置模式中执行以下命令：

命令	作用
Ruijie(config)# **arp** *ip-address mac-address arp-type*	定义静态 ARP，其中 arp-type 目前只支持 arpa 类型。
Ruijie(config)# **no arp** *ip-address*	取消静态 ARP

ARP 封装设置

目前 ARP 封装只支持 Ethernet II 类型，在锐捷产品中也表示为 ARPA 关键字。

ARP 超时设置

ARP 超时设置只对动态学习到的 IP 地址和 MAC 地址映射起作用。超时时间设置得越短，ARP 缓冲中保存的映射表就越真实，但是 ARP 消耗网络带宽也越多，所以需要权衡利弊。除非有特别的需要，否则一般不需要配置 ARP 超时时间。

要配置 ARP 超时时间，在接口配置模式中执行以下命令：

命令	作用
Ruijie(config-if)# **arp timeout** *seconds*	配置 ARP 超时时间，范围 0-2147483，其中 0 表示不老化
Ruijie(config-if)# **no arp timeout**	恢复缺省配置

缺省情况下，超时时间为 3600 秒，即 1 个小时。

配置可信任 ARP 功能

防 ARP 欺骗。锐捷网络智能三层接入/汇聚交换机能够支持可信任 ARP 功能。

可信任 ARP 作为一类特殊 ARP，添加在交换机端的 ARP 表中，用于防止 ARP 欺骗。可信任 ARP 同时具有静态 ARP 和动态 ARP 两者的特征，其优先级高于动态 ARP 表项、并且低于静态 ARP 表项。可信任 ARP 具有类似于动态 ARP 的老化

机制——在 ARP 老化时主动发送 ARP 请求报文探测主机是否存在，如果主机有应答则代表主机还是活动的那么就更新 ARP 的老化时间，否则删除 ARP 表项。可信任 ARP 具有静态 ARP 的相关特征，即不会通过学习 ARP 报文动态更新 ARP 表项的 MAC、接口等相关字段。

可信任 ARP 是 GSN 客户端用户认证上线时，认证服务端通过接入交换机获取用户真实的 IP-MAC 关联信息，并根据用户的网关信息，在网关交换机上添加的。该过程对于网络管理员来说是透明的，不会对网络管理员的原有网络管理产生任何影响。

综上所述，因为可信任 ARP 来源真实有效，且不会被 ARP 报文动态更新，所以可以有效的防止针对网关的 ARP 欺骗

要启用可信任 ARP 功能，在全局配置模式中执行 **service trustedarp** 命令。

命令	作用
Ruijie(config)# **service trustedarp**	启用可信任 ARP 功能
Ruijie(config)# **no service trustedarp**	关闭可信任 ARP 功能

如果设置可信任 ARP 时需要 VLAN 转换，可以执行 **arp trusted user-vlan** *vid1* **translated-vlan** *vid2* 命令。

命令	作用
Ruijie(config)# **arp trusted user-vlan** *vid1* **translated-vlan** *vid2*	添加可信任 ARP 时进行 VLAN 转换

要查看交换机上存在的可信任 ARP，可以执行 show arp trusted 命令。

命令	作用
Ruijie(config)# **show arp trusted** *[ip [mask]]*	查看交换机上的可信任 ARP

如果要强制删除交换机上的可信任 ARP，可以执行 clear arp trusted。

命令	作用
Ruijie(config)# **clear arp trusted** *[ip [mask]]*	删除交换机上的可信任 ARP

执行 **clear arp trusted** 会删除交换机上的所有的可信 ARP，可能导致用户不能上网。

一般情况下使用 **clear arp trusted** *ip* 删除指定的可信任 ARP 表项。

默认情况下，可信任 ARP 不会老化，如果需要允许可信任 ARP 老化，在全局配置模式执行 arp trusted aging。

命令	作用
Ruijie(config)# **arp trusted aging**	允许可信任 ARP 老化

用户根据需要调整可信任 ARP 的容量，可以通过在全局模式下执行 **arp trusted** *number* 实现。

命令	作用
Ruijie(config)# **arp trusted** *number*	调整可信任 ARP 的容量为 *number*。

配置本地 ARP 代理功能

本命令只在锐捷三层交换机上支持

在扁平化组网模型下，ARP 防欺骗变得更加重要，为了增强 ARP 功能的安全性。我们提出了本地代理 ARP 的概念。即网段内的 ARP 代理应答。命令形式是：local-proxy-arp。这个功能的主要目标是隔离 PC 之间的 ARP 报文，即 PC 发出的 ARP 报文，其他 PC 收不到。部署时要求不同的 PC 之间进行端口隔离。

本地 ARP 代理命令只有配置在 SVI 接口下才有意义，因为只有这种接口下才会存在多个 2 层的交换口作为成员口。在 route-port,、L3AP 以及各种路由器接口上不允许配置。

要启用本地 ARP 代理功能，在接口模式下执行 local-proxy-arp 命令。

命令	作用
Ruijie(config-if)# local-proxy-arp	启用本地 ARP 代理功能
Ruijie(config-if)# no local-proxy-arp	关闭本地 ARP 代理功能

关闭 IP 路由

IP 路由功能缺省情况下是启动的，除非确定不需要 IP 路由功能，否则不要执行该操作。关闭 IP 路由将使设备丢失所有的路由，而且没有路由转发的功能。

要关闭 IP 路由功能，在全局配置模式中执行以下命令：

命令	作用
Ruijie(config)# **no ip routing**	关闭 IP 路由功能
Ruijie(config)# **ip routing**	启动 IP 路由功能

1.1.2.3 配置广播包处理

广播包是指目标地址为某个物理网络上所有主机的数据包。锐捷产品支持两种类型广播包：1）定向广播，是指数据包接收者为一个指定网络的所有主机，目标地址的主机部分全为“1”；2）淹没广播，是指数据包接收者为所有网络的主机，目标地址 32 比特位全为“1”时。广播包目前被一些 IP 协议的泛滥使用，其中包括十分重要的 IP 协议。所以如何控制和使用广播包是一个网络管理人员的基本职责。

如果 IP 网络设备转发淹没广播，可能会引起网络的超负载，严重影响网络的运行，这种情况称为广播风暴。设备提供了一些办法能够将广播风暴限制在本地网络，阻止其继续扩张。但对于桥和交换机等基于二层网络设备，将转发和传播广播风暴。

解决广播风暴最好的办法就是给每个网络指定一个广播地址，这就是定向广播，这要求使用广播包的 IP 协议尽可能应用定向广播而不是淹没广播进行数据传播。

关于广播问题的详细描述，请参见 RFC 919 和 RFC 922。

创建 IP 广播地址

当前使用最多的广播包，其目标地址为全“1”，表示为 255.255.255.255。锐捷产品可以通过软件定义产生其它地址的广播包，而且可以接收所有类型的广播包。

要配置有别于 255.255.255.255 的广播地址，在接口配置模式中执行以下命令：

命令	作用

Ruijie(config-if)# **ip broadcast-address** *ip-address*	创建新的广播地址
Ruijie(config-if)# **no ip broadcast-address**	取消新的广播地址

定向广播到物理广播转换

IP 定向广播报文是指目标地址为某个 IP 子网广播地址的 IP 报文，如目标地址为 172.16.16.255 的报文就称为定向广播报文。但是产生该报文的节点又不是目标子网的成员。

没有与目标子网直连的设备接收到 IP 定向广播报文，跟转发单播报文一样处理定向广播报文。当定向广播报文到达直连该子网的设备后，设备将把定向广播报文转换为淹没广播报文（一般指目标 IP 地址为全“1”的广播报文），然后以链路层广播方式发送给目标子网上的所有主机。

您可以在指定的接口上，启动定向广播到物理广播转换的功能，这样该接口就可以转发到直连网络的定向广播了。该命令只影响到达最终目标子网的定向广播报文的最后传输，而不影响其它定向广播报文的正常转发。

在接口上，您还可以通过定义访问控制列表来控制转发某些定向广播。当定义了访问列表，只有符合访问列表中定义的数据包才进行定向广播到物理广播的转换。

要配置定向广播到物理广播的转换，在接口配置模式中执行以下命令：

命令	作用
Ruijie(config-if)# **ip directed-broadcast** [*access-list-number*]	在接口上，启动定向广播到物理广播的转换
Ruijie(config-if)# **no ip directed-broadcast**	取消转换

1.1.3 监视和维护IP地址

1.1.3.1 清除缓冲和表内容

您可以删除一些特定缓冲、表、数据库的全部内容，主要包括三个方面：

- 清除 ARP 缓冲；
- 清除主机名到 IP 地址的映射表；
- 清除路由表。

命令	作用
Ruijie# **clear arp-cache**	清除 ARP 缓冲
Ruijie# **clear ip route** {*network* [*mask*] | *}	清除 IP 路由表

1.1.3.2 显示系统和网络状态

您可以查看 IP 路由表、缓冲、数据库的所有内容，通过这些信息对网络故障的排除十分有帮助。通过测试本地设备网络的可达到性，您可以知道数据包在离开本设备后将往哪条路径发送。

要显示系统和网络统计量，在特权用户模式中执行以下命令：

命令	作用
show arp [[*ip* [*mask*] | *mac-address*] | **static** | **complete** | **incomplete**]	显示 ARP 缓冲表，其中 complete / incomplete 关键字是用来分别显示动态 ARP 中已解析 / 未解析的表项。
show ip arp	显示 IP ARP 缓冲表
show ip interface [*interface-type interface-number*]	显示接口 IP 信息
show ip route [*network* [*mask*]]	显示路由表
show ip route	显示路由表摘要
Ruijie# **ping** *ip-address* [**length** *bytes*] [**ntimes** *times*] [**timeout** *seconds*]	测试网络可达性

1.2 配置IP服务

1.2.1 IP连接管理

IP 协议栈提供了许多服务用来控制和管理 IP 连接，ICMP 就提供了许多这些服务。当网络发生任何问题，设备或接入服务器将发送 ICMP 消息给主机或其它设备。详细的 ICMP 消息定义，请参见 RFC 792。

启用 ICMP 协议不可达消息

当设备接收到目标为自己的非广播包，该数据包中采用了设备不能处理的 IP 协议，设备就向源地址发送 ICMP 协议不可达消息。另外，如果设备由于不知道路由而不能转发数据包时，也会发送 ICMP 主机不可达消息。这种特性缺省是启用的。

如果要重新启用 ICMP 协议不可达消息，在接口配置模式中执行以下命令：

命令	作用
Ruijie(config-if)# **ip unreachables**	启用 ICMP 协议不可达和主机不可达消息
Ruijie(config-if)# **no ip unreachables**	关闭 ICMP 协议不可达和主机不可达消息

启用 ICMP 重定向消息

路由有时会不够优化，使得设备从一个接口接收到的数据包，还要从该接口发送出去。如果设备将数据包从接收接口重新发送出去，设备就会给数据源发送一个 ICMP 重定向消息，告诉数据源到该目标地址的网关为同一子网上的另外一台设备。这样数据源就会将后续的数据包按照最佳的路径进行发送。该特性缺省是启用。

要配置 ICMP 重定向消息，在接口配置模式中执行以下命令：

命令	作用
Ruijie(config-if)# **ip redirects**	启用 ICMP 重定向消息，缺省启用
Ruijie(config-if)# **no ip redirects**	关闭 ICMP 重定向消息

启用 ICMP 掩码应答消息

网络设备有时需要知道互联网上某个子网的子网掩码，为了获取该信息，网络设备 可以发送 ICMP 掩码请求消息，接收到 ICMP 掩码请求消息的网络设备就会发送掩码应答消息。锐捷产品可以响应 ICMP 掩码请求消息，缺省情况下是启用该特性的。

要配置 ICMP 掩码应答消息，在接口配置模式中执行以下命令：

命令	作用
Ruijie(config-if)# **ip mask-reply**	启用掩码应答消息
Ruijie(config-if)# **no ip mask-reply**	关闭掩码应答消息

设置 IP MTU

设备所有的接口都有缺省的 MTU（最大传输单元）值，所有大于 MTU 的数据包要从该接口转发出去必须分段，否则发送失败。

锐捷产品允许调整接口的 MTU 值，而且 MTU 的变化会引起 IP MTU 的变化，IP MTU 总是会自动与接口 MTU 保持一致。但是反之不行，如果调整了 IP MTU 值，接口 MTU 不会跟着改变。

一个物理网络上的设备接口，相同协议 MTU 值必须保持一致。

要设置 IP MTU 值，在接口配置模式中执行以下命令：

命令	作用
Ruijie(config-if)# **ip mtu** *bytes*	设置 MTU 值，范围 68~1500
Ruijie(config-if)# **no ip mtu**	恢复缺省值

配置 IP 源路由

锐捷产品支持 IP 源路由。当设备接收到 IP 数据包时，会对 IP 报头的严格源路由、宽松源路由、记录路由等选项进行检查，这些选项在 RFC 791 中有详细描述。如果检测到该数据包启用了其中一个选项，就会执行响应的动作；如果检测到无效的选项，就会给数据源发送一个 ICMP 参数问题消息，然后丢弃该数据包。锐捷产品缺省情况下支持 IP 源路由特性。

要配置 IP 源路由，在全局模式中执行以下命令：

命令	作用
Ruijie(config)# **ip source-route**	启用 IP 源路由
Ruijie(config)# **no ip source-route**	关闭 IP 源路由

2 IPv6

2.1 IPv6 概述

随着 Internet 的迅速增长以及 IPv4 地址空间的逐渐耗尽，IPv4 的局限性就越来越明显。对新一代互联网络协议（Internet Protocol Next Generation - IPng）的研究和实践已经成为热点，Internet 工程任务工作小组(IETF)的 IPng 工作组确定了 IPng 的协议规范，并称之为"IP 版本 6"（IPv6），该协议的规范在 RFC2460 中有详细的描述。

IPv6 的主要特点：

更大的地址空间

地址长度由 IPv4 的 32 位扩展到 128 位，即 Ipv6 有 2^128-1 个地址，IPv6 采用分级地址模式，支持从 Internet 核心主干网到企业内部子网等多级子网地址分配方式。

简化了报头格式

新 IPv6 报文头的设计原则是力图将报文头开销降到最低，因此将一些非关键性字段和可选字段从报文头中移出，放到扩展的报文头中，虽然 IPv6 地址长度是 IPv4 的四倍，但包头仅为基本 IPv4 首部的两倍。改进的 IPv6 报文头在设备转发时拥有更高的效率，例如 IPv6 报文头中没有校验和，IPv6 设备在转发中不需要去处理分片(分片由发起者完成)。

高效的层次寻址及路由结构

IPv6 采用聚合机制，定义非常灵活的层次寻址及路由结构，同一层次上的多个网络在上层设备中表示为一个统一的网络前缀，这样可以显著减少设备必须维护的路由表项，这也大大降低了设备的选路和存储开销。

简单的管理：即插即用

通过实现一系列的自动发现和自动配置功能，简化网络节点的管理和维护。比如邻接节点发现（Neighbor Discovery）、最大传输单元发现（MTU Discovery）、路由器通告（Router Advertisement）、路由器请求（Router Solicitation）、节点自动配置（Auto-configuration）等技术就为即插即用提供了相关的服务。特别要提到的是 IPv6 支持全状态和无状态两种地址配置方式，在 IPv4 中，动态主机配置协议 DHCP 实现了主机 IP 地址及其相关配置的自动设置，IPv6 承继 IPv4 的这种自动配置服务，并将其称为全状态自动配置(Stateful Autoconfiguration)。除了全状态自动配置，IPv6 还采用了一种被称为无状态自动配置（Stateless Autoconfiguration）的自动配置服务。在无状态自动配置过程中，主机自动获得链路本地地址、本地设备的地址前缀以及其它一些相关的配置信息。

安全性

IPSec 是 IPv4 的一个可选扩展协议，但是在 IPv6 中它是 IPv6 的一个组成部分，用于提供 IPv6 的安全性。目前，IPv6 实现了认证头（Authentication Header，AH）和封装安全载荷（Encapsulated Security Payload，ESP）两种机制。前者实现数据的完整性及对 IP 包来源的认证，保证分组确实来自源地址所标记的节点；后者提供数据加密功能，实现端到端的加密。

更好的 QoS 支持

IPv6 包头的新字段定义了数据流如何识别和处理。IPv6 包头中的流标识（Flow Label）字段用于识别数据流身份，利用该字段，IPv6 允许用户对通信质量提出要求。设备可以根据该字段标识出同属于某一特定数据流的所有包，并按需对这些包提供特定的处理。

用于邻居节点交互的新协议

IPv6 的邻居发现协议（Neighbor Discovery Protocol）使用一系列 IPv6 控制信息报文（ICMPv6）来实现相邻节点（同一链路上的节点）的交互管理。邻居发现协议以及高效的组播和单播邻居发现报文替代了以往基于广播的地址解析协议 ARP、ICMPv4 路由器发现等报文。

可扩展性

IPv6 特性具有很强的可扩展性，新特性可以添加在 IPv6 包头之后的扩展包头中。不象 IPv4，包头最多只能支持 40 字节的的可选项，IPv6 扩展包头的大小仅受到整个 IPv6 包最大字节数的限制。

目前已经实现的 IPv6 支持下列特性：

- IPv6 协议
- IPv6 地址格式
- IPv6 地址类型
- ICMPv6
- IPv6 邻居发现
- 路径 MTU 发现
- ICMPv6 重定向
- 地址冲突检测
- IPv6 无状态自动配置
- IPv6 地址配置
- IPv6 路由转发，支持静态路由配置
- 配置 IPv6 协议的各种参数
- 诊断工具 Ping IPv6

2.1.1 IPv6 地址格式

IPv6 地址的基本表达方式是 X : X : X : X : X : X : X : X，其中 X 是一个 4 位十六进制整数(16 位)。每一个数字包含 4 个比特，每个整数包含 4 个十六进制数字，每个地址包括 8 个整数，一共 128 位。下面是一些合法的 IPv6 地址：

2001:ABCD:1234:5678:AAAA:BBBB:1200:2100

800 : 0 : 0 :0 : 0 : 0 : 0 : 1

1080 : 0 : 0 : 0 : 8 : 800 : 200C : 417A

这些整数是十六进制整数，其中 A 到 F 表示的是 10 到 15。地址中的每个整数都必须表示出来，但起始的 0 可以不必表示。某些 IPv6 地址中可能包含一长串的 0 (就像上面的第二和第三个例子一样)。当出现这种情况时，允许用“：：”来表示这一长串的 0。即地址 800 : 0 : 0 : 0 : 0 : 0 : 0 : 1 可以被表示为：800 :: 1

这两个冒号表示该地址可以扩展到一个完整的 128 位地址。在这种方法中，只有当 16 位组全部为 0 时才会被两个冒号取代，且两个冒号在地址中只能出现一次。

在 IPv4 和 IPv6 的混合环境中还有一种混合的表示方法。IPv6 地址中的最低 32 位可以用于表示 IPv4 地址，该地址可以按照一种混合方式表达，即 X : X : X : X : X : X : d . d . d . d，其中 X 表示一个 1 6 位整数，而 d 表示一个 8 位的十进制整数。例如，地址 0 : 0 : 0 : 0 : 0 : 0 : 192 .168 . 20 .1 就是一个合法的 IPv6 地址。使用简写的表达方式后，该地址也可以表示为：: : 192 .168 . 20 . 1。典型代表是 IPv4 兼容 IPv6 地址和 IPv4 映射 IPv6 地址，IPv4 兼容 IPv6 地址前 96 比特是 0，表示法为“**::**A.B.C.D”，例如“**::**1.1.1.1”，目前 IPv4 兼容地址已被废除；IPv4 映射 IPv6 地址表示法为“**::**FFFF:A.B.C.D”，用于把 IPv4 地址表示为 IPv6 地址，如把 IPv4 地址“1.1.1.1”映射到 IPv6 地址“**::**FFFF:1.1.1.1”。

由于 IPv6 地址被分成两个部分：子网前缀和接口标识符，因此可以按照类似 CIDR 地址的方式被表示为一个带额外数值的地址，其中该数值指出了地址中有多少位是代表网络部分(网络前缀)，即 IPv6 节点地址中指出了前缀长度，该长度与 IPv6 地址间以斜杠区分，例如：12AB::CD30:0:0:0:0/60，这个地址中用于选路的前缀长度为 60 位。

2.1.2 IPv6 地址类型

RFC4291 定义了三种 IPv6 地址类型：

单播(Unicast)：单个接口的标识符。送往一个单播地址的包将被传送至该地址标识的接口上。

泛播(Anycast)：一组接口的标识符。送往一个泛播地址的包将被传送至该地址标识的接口之一(根据选路协议选择“最近”的一个)。

组播(Multicast)：一组接口(一般属于不同节点)的标识符。送往一个组播地址的包将被传送至加入该组播地址的所有接口上。

在 IPv6 中已经没有定义广播地址。

下面逐一介绍这几类地址：

单播地址（Unicast Addresses）

单播地址分为未指定地址、环回地址、链路本地地址、站点本地地址和全球单播地址。目前，站点本地地址被废除了，除了未指定地址、环回地址和链路本地地址以外的单播地址，都是全球单播地址。

1) 未指定地址

未指定地址是 0:0:0:0:0:0:0:0，通常简写为**::**，常见的两个用途是：

若主机启动时没有单播地址，则以未指定地址作为源地址，发送路由器请求，从网关获取前缀信息，从而自动生成单播地址。

给主机配置 IPv6 地址时，检测地址是否和同网段其它主机的地址冲突，则以未指定地址作为源地址发送邻居请求（相当于免费 ARP）。

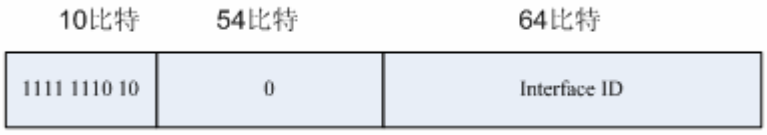
2) 环回地址

环回地址是 0:0:0:0:0:0:0:1，通常简写为**::**1，相当于 IPv4 地址 127.0.0.1，一般在节点给自身发报文时使用。

3) 链路本地地址

链路本地地址的格式如下：

图 2-1

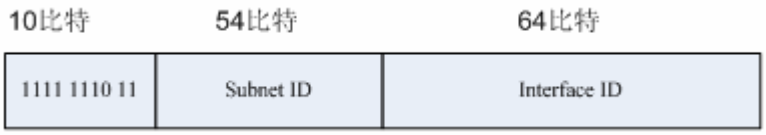


链路本地地址用于单个网络链路上给主机编号。前缀的前 10 位标识的地址即链路本地地址。设备永远不会转发源地址或者目的地址带有链路本地地址的报文。该地址的中间 54 位置成 0。后 64 位表示接口标识符，地址空间的这部分允许单个网络连接多达（2 的 64 次方减 1）个主机。

4) 站点本地地址

站点本地地址的格式如下：

图 2-2



站点本地地址可以用在站点内传送数据，设备不会将源地址或者目的地址带有站点本地地址的报文转发到 internet 上，即这样的包只能在站点内转发，而不能把包转发到站点外去。站点可以理解为一个公司的局域网，这种地址类似于 IPv4 的私有地址，如 192.168.0.0/16。RFC3879 已经废除了站点本地地址。对于新的实现，不再支持该前缀，统一视为全球单播地址；对于已经实现和部署的，可以继续用这个前缀。

5) 全球单播地址

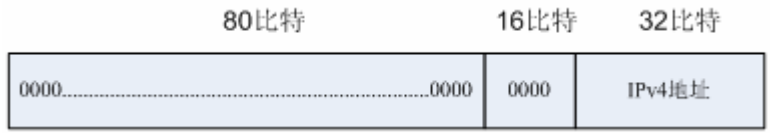
全球单播地址格式如下：

图 2-3

全球单播地址中有一类地址是嵌入 IPv4 地址的 IPv6 地址，用于 IPv4 节点和 IPv6 节点互通，分为 IPv4 兼容 IPv6 地址和 IPv4 映射 IPv6 地址两种。

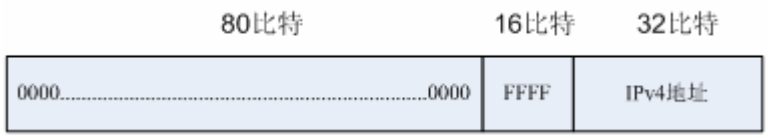
IPv4 兼容 IPv6 地址格式（IPv4-compatible IPv6 address）

图 2-4



IPv4 映射 IPv6 地址格式（IPv4-mapped IPv6 address）

图 2-5



IPv4 兼容 IPv6 地址主要是用在自动隧道上，这类节点既支持 IPv4 也支持 IPv6，IPv4 兼容 IPv6 地址通过 IPv4 设备以隧道方式传送 IPv6 报文，目前 IPv4 兼容 IPv6 地址已被废除。而 IPv4 映射 IPv6 地址则被 IP6 节点用于访问只支持 IPv4 的节点，例如当一个 IPv4/IPv6 主机的 IPv6 应用程序请求解析一个主机名字(该主机只支持 IPv4)时，那么名字服务器内部将动态生成 IPv4 映射的 IPv6 地址返回给 IPv6 应用程序。

组播地址（Multicast Addresses）

IPv6 组播的地址格式如下：

```
|    8     |  4 |  4 |                   112 bits                   |
+--------+----+----+----------------------------------------------+
|11111111|flgs|scop|                   group ID                   |
+--------+----+----+----------------------------------------------+
```

地址格式中的第 1 个字节为全“1”代表是一个组播地址。

标志字段：

由 4 个比特位组成。目前只指定了第 4 位，该位用来表示该地址是由 Internet 编号机构指定的知名的组播地址，还是特定场合使用的临时组播地址。如果该标志位为“0”，表示该地址为知名组播地址；如果该位为“1”，表示该地址为临时地址。其他 3 个标志位保留将来用。

范围字段：

由 4 个比特位组成，用来表示组播的范围。即组播组是包括本地节点、本地链路、本地站点、还是包括 IPv6 全球地址空间中任何位置的节点。

组标识符字段：

长 112 位，用于标识组播组。根据组播地址是临时的还是知名的以及地址的范围，同一个组播标识符可以表示不同的组。

IPv6 的组播地址是以 FF00::/8 为前缀的这类地址。一个 IPv6 的组播地址通常标识一系列不同节点的接口。当一个报文发送到一个组播地址上时，那么该报文将分发到标识有该组播地址的每个节点的接口上。一个节点(主机或者设备)必须加入下列的组播：

本地链路所有节点组播地址 FF02::1

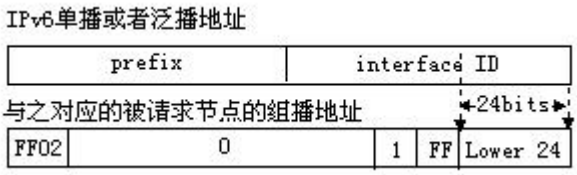
被请求节点的组播地址， 前缀为 FF02:0:0:0:0:1:FF00:0000/104

如果是设备那么还必须加入本地链路所有设备的组播地址 FF02::2。

被请求节点的组播地址是对应于 IPv6 单播(unicast)和泛播(anycast)地址的，IPv6 节点必须为配置的每个单播地址和泛播地址加入其相应的被请求节点的组播地址。被请求节点的组播地址的前缀为 FF02:0:0:0:0:1:FF00:0000/104，另外 24 位由单播地址或者泛播地址的低 24 比特组成，例如对应于单播地址 FE80::2AA:FF:FE21:1234 的被请求节点的组播地址是 FF02::1:FF21:1234 ，

被请求节点组播地址通常用于邻居请求(NS)报文中，被请求节点组播地址的格式如下：

图 2-6



泛播地址（Anycast Addresses）

泛播地址与组播地址类似，同样是多个节点共享一个泛播地址，不同的是只有一个节点期待接收给泛播地址的数据包而组播地址成员的所有节点均期待着接收发给该地址的所有包。泛播地址被分配在正常的 IPv6 单播地址空间，因此泛播地址在形式上与单播地址无法区分开，一个泛播地址的每个成员，必须显式地加以配置，以便识别是泛播地址。

泛播地址只能分配给设备，不能分配给主机，并且泛播地址不能作为报文的源地址。

在 RFC2373 中预定义了一个泛播地址，称之为子网路由器的泛播地址。下图显示了子网路由器的泛播地址格式，这类地址由子网前缀后面跟着一系列的 0(作为接口标识符)组成。

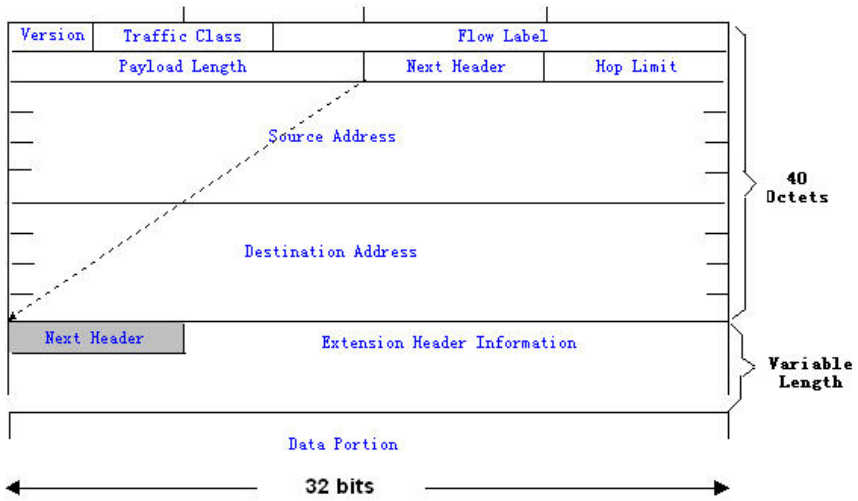
其中子网前缀标识了一个指定的链路(子网)，送给子网路由器泛播地址的报文将被分发到在该子网上的一个设备。子网路由器的泛播地址通常是被用于一个节点上的应用程序需要和远程子网的一个设备通信而使用。

图 2-7

IPv6 包头结构

IPv6 包头格式如下图：

图 2-8



在 IPv4 中，所有包头以 4 字节为单位。在 IPv6 中，包头以 8 字节为单位，包头的总长度是 40 字节。IPv6 包头定义了以下字段：

版本(Version)：

长度为 4 位，对于 IPv6 该字段必须为 6。

类别(Traffic Class)：

长度为 8 位，指明为该包提供了某种服务，相当于 IPv4 中的“TOS”。

流标签(Flow Label)：

长度为 20 位，用于标识属于同一业务流的包，一个节点可以同时作为多个业务流的发送源，流标签和源节点地址唯一标识了一个业务流。

净荷长度(Payload Length)：

长度为 16 位，其中包括包净荷的字节长度，同时也包含了各个 IPv6 扩展选项的长度(如果存在)，换句话说就是包含了除 IPv6 头本身外的 IPv6 包的长度。

下一个头(Next Header)：

这个字段指出了 IPv6 头后所跟的头字段中的协议类型。与 IPv4 协议字段类似，下一个头字段可以用来指出高层是 TCP 还是 UDP，它也可以用来指明 IPv6 扩展头的存在。

跳数(Hop Limit)：

长度为 8 位。每当设备对包进行一次转发之后，这个字段就会被减 1，如果该字段达到 0，这个包就将被丢弃。它与 IPv4 包头中的生存期字段类似。

源地址(Source Address)：

长度为 128 位，指出了 IPv6 包的发送方地址。

目的地址(Destination Address)：

长度为 128 位，指出了 IPv6 包的接收方地址。

IPv6 的扩展头，目前 IPv6 定义了下列的扩展头：

逐跳选项头(Hop-by-Hop Options)：

此扩展头必须紧随在 IPv6 头之后，它包含包所经过的路径上的每个节点都必须检查的选项数据。

选路头（Routing （Type 0））：

此扩展头指明包在到达目的地途中将经过哪些节点，它包含包沿途经过的各节点的地址列表。IPv6 头的最初目的地址是选路头的一系列地址中的第一个地址，而不是包的最终目的地址。此地址对应的节点接收到该包之后，对 IPv6 头和选路头进行处理，并把包发送到选路头列表中的第二个地址，如此继续，直到包到达其最终目的地。

分片头（Fragment）：

此扩展头用于源节点对长度超出源节点和目的节点路径 MTU 的包进行分片。

目的地选项头（Destination Options）：

此扩展头代替了 IPv4 选项字段，目前唯一定义的目的地选项是在需要时把选项填充为 6 4 位（8 字节）的整数倍，此扩展头可以用来携带由目的地节点检查的信息。

上层扩展头(Upper-layer header)：

指明了上层传输数据的协议，如 TCP(6)、UDP(17)。

此外还有身份验证头(Authentication)和封装安全性净荷(Encapsulating Security Payload)的扩展头，这将放到 IPSec 章节描述，目前我们实现的 IPv6 还未支持 IPSec。

IPv6 的路径 MTU 发现

和 IPv4 的路径 MTU 发现类似，IPv6 的路径 MTU 发现允许一台主机动态的发现并调整发送数据路径上的 MTU 的大小。另外，当主机要发送的数据包的大小如果比发送数据路径上的 MTU 大时，那么将由主机自己负责分片。这种由主机分片的行为使得设备无需处理分片从而节省了 IPv6 设备的资源，同时也提高了 IPv6 网络的效率。

- 在 IPv4 最小的链路 MTU 是 68 字节，这意味着在每条发送数据的路径上的链路必须至少支持 68 字节大小的链路 MTU。
- 在 IPv6 最小的链路 MTU 是 1280 字节，对于 IPv6 的链路强烈推荐使用 1500 的链路 MTU。

2.1.3 IPv6 邻居发现

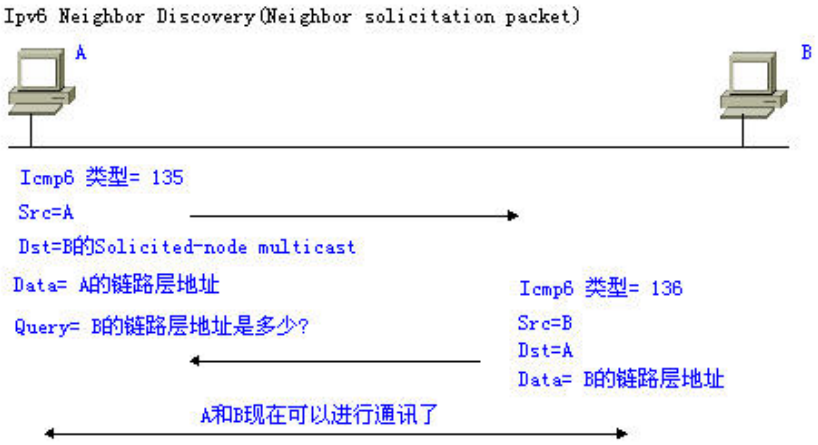
邻居发现协议是 IPv6 协议的一个基本的组成部分，它的主要功能有路由器发现、前缀发现、参数发现、地址自动配置、地址解析（相当于 ARP）、确定下一跳、邻居不可达检测、地址冲突检测和重定向。邻居发现定义了 5 种 ICMP 报文：“路由器请求， ICMP 类型为 133；路由器公告， ICMP 类型为 134；邻居请求，相当于 ARP 请求，ICMP 类型为 135；邻居公告，相当于 ARP 应答，ICMP 类型为 136；ICMP 重定向报文，ICMP 类型为 137”。

地址解析

当一个节点要与另外一个节点通信时，那么该节点必须获取对方的链路层地址，此时就要向该节点发送邻居请求(NS)报文,报文的目的地址是对应于目的节点的 IPv6 地址的被请求多播地址，发送的 NS 报文同时也包含了自身的链路层地址。当对应的节点收到该邻居请求后发回一个响应的报文称之为邻居公告报文(NA)，其目的地址是邻居请求的源地址，内容为被请求的节点的链路层的地址。当源节点收到该应答报文后就可以和目的节点进行通讯了。

下图是地址解析的过程：

图 2-9



邻居不可达检测

当一个邻居被认为可到达的时间到期以后，如果有 IPv6 单播报文需要发送给这个邻居，将执行邻居不可达检测 (Neighbor Unreachability Detection)。

邻居不可达检测和向邻居发送 IPv6 报文可以同时进行，在检测过程中，继续向该邻居转发 IPv6 报文。

地址冲突检测

当给主机配置 IPv6 地址以后，想知道这个 IPv6 地址在链路上是不是唯一的，需要执行地址冲突检测，发送源 IPv6 地址是未指定地址的邻居请求。

路由器，前缀和参数发现

路由器公告报文(RA)在设备上是定期被发往链路本地所有节点的。

路由器公告报文发送如下图：

图 2-10

路由器公告报文中通常包含如下内容：

- 一个或者多个 IPv6 地址前缀（用于 on-link 确定，或无状态地址自动配置）
- IPv6 地址前缀的有效期。
- 主机自动配置使用的方式(有状态还是无状态)。
- 作为缺省设备的信息(即决定本设备是否要作为缺省设备，如果是那么还宣布自己充当缺省设备的时间)。
- 提供给主机配置的一些其它信息如跳数限制、MTU、邻居请求重传间隔时间等。

路由器公告报文同时也用来应答主机发出的路由器请求(RS)报文，路由器请求报文允许主机一旦启动后可以立即获得自动配置的信息而无需等待设备发出的路由器公告报文(RA)。当主机刚启动时如果没有单播地址，那么主机发出的路由器请求报文将使用未指定地址(0:0:0:0:0:0:0:0)作为请求报文的源地址，否则使用已有的单播地址作为源地址，路由器请求报文使用本地链路所有设备组播地址(FF02::2)作为目的地址。作为应答路由器请求(RS)报文的路由器公告(RA)报文将使用请求报文的源地址作为目的地址(如果源地址是未指定地址那么将使用本地链路所有节点组播地址 FF02::1)。

在路由器公告报文中下列参数是可以被配置的：

Ra-interval 路由器公告报文的发送间隔。

Ra-lifetime 路由器生存期，即设备是否充当本地链路的缺省路由器以及充当该角色的时间。

Prefix 本地链路的 IPv6 地址前缀，用于 on-link 确定，或无状态地址自动配置，包括前缀的其它参数配置 。

Rs-initerval 邻居请求报文重传的时间间隔。

Reachabletime 检测到邻居可到达事件后认为邻居是可到达的所维持的时间。

以上这些参数在 IPv6 接口属性中进行配置。

缺省在该接口上不主动发送路由器公告报文，如果想允许路由器公告报文的发送可以在接口配置模式下使用命令 no ipv6 nd suppress-ra 。

为了能够使节点无状态地址自动配置能够正常工作，路由器公告报文中公告的前缀的长度必须为 64 比特。

重定向

当路由器收到 IPv6 报文以后，发现存在更优的下一跳，就发送 ICMP 重定向报文把更优的下一跳告诉主机，下一次主机直接把 IPv6 报文发给更优的下一跳。

2.2 配置IPv6

下面将分别介绍 IPv6 的各个功能模块的配置。

2.2.1 配置IPv6 的地址

本节的任务描述了如何在一个接口上配置 IPv6 地址。缺省没有配置 IPv6 地址。

一旦 IPv6 的接口创建并且该接口的链路是 UP 状态的，那么系统将为该接口自动生成链路本地地址。目前 IPv6 不支持配置

配置 IPv6 地址过程如下：

命令	作用
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**interface** *interface-id*	进入接口配置模式。 注意，如果是二层端口，必须执行“no switchport”转换成三层端口。
Ruijie(config-if)#**ipv6 enable**	打开接口的 IPv6 协议。如果没有执行这条命令，给接口配置 IPv6 地址时会自动打开 IPv6 协议。
Ruijie(config-if)#**ipv6 address** *ipv6-address/prefix-length* Ruijie(config-if)#**ipv6 address** *ipv6-prefix/prefix-length* eui-64	为该接口配置 IPv6 的单播地址。如果指定参数 eui-64，只需指定前缀，接口标识符是按 EUI-64 格式自动生成，最终生成的 IPv6 地址是把配置的前缀和接口标识符合并形成的。 注意：无论是否使用 eui-64 关键字，在删除地址时都必须输入完整的地址形式(前缀+接口标识符/前缀长度)。 如果在接口上配置 IPv6 地址，那么接口的 IPv6 协议就会自动打开，即使使用 no ipv6 enable 也不能关闭 IPv6 协议。
Ruijie(config-if)#**end**	退回到特权模式。
Ruijie#**show ipv6 interface** *interface-id*	查看 IPv6 接口的相关信息
Ruijie#**copy running-config startup-config**	保存配置。

使用 **no ipv6 address** *ipv6-prefix/prefix-length* [**eui-64**]命令删除已配置的地址，下面是配置 IPv6 地址的例子：

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# ipv6 enable
Ruijie(config-if)# ipv6 address fec0:0:0:1::1/64
Ruijie(config-if)# end
Ruijie# show ipv6 interface GigabitEthernet 0/1
Interface GigabitEthernet 0/1 is Up, ifindex: 1
address(es):
Mac Address: 00:00:00:00:00:01
INET6: fe80::200:ff:fe00:1 , subnet is fe80::/64
INET6: fec0:0:0:1::1 , subnet is fec0:0:0:1::/64
Joined group address(es):
ff01:1::1
ff02:1::1
ff02:1::2
ff02:1::1:ff00:1
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds<160-240>
ND router advertisements live for 1800 seconds
```

2.2.2 配置ICMPv6 的重定向功能

本节描述如何配置接口的 ICMPv6 的重定向功能，缺省情况下在接口上是打开 IPv6 重定向功能的。当设备在转发包的过程中遇到下列情况同时发生时必须向报文的发起者发送重定向报文：

- 报文的目的地址不是一个多播地址；
- 报文的目的地址不是设备本身；
- 设备为该报文决定的下一跳的输出接口和收到该报文的接口相同，即下一跳和发起者处在同一条链路上；
- 报文的源地址标识的节点是本地设备上的一个邻居，即在设备上的邻居表中存在该邻居。

只有设备可以产生重定向报文，主机不能产生，并且设备收到重定向报文不会为其更新路由表

下面是配置一个接口打开重定向功能的过程：

命令	作用
Ruijie#**configure terminal**	进入全局配置模式。

Ruijie(config)#**interface** *interface-id*	进入接口配置模式 注意，如果是二层端口，必须执行“no switchport”转换成三层端口。
Ruijie(config-if)#**ipv6 redirects**	打开该接口的 IPv6 重定向功能
Ruijie(config-if)#**end**	退回到特权模式。
Ruijie#**show ipv6 interface** *interface-id*	查看接口配置的相关信息。
Ruijie#**copy running-config startup-config**	保存配置。

使用 **no ipv6 redirects** 命令关闭重定向的功能，下面是配置重定向功能打开的例子：

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie (config-if)# ipv6 redirects
Ruijie (config-if)# end
Ruijie # show ipv6 interface GigabitEthernet 0/1
Interface GigabitEthernet 0/1 is Up, ifindex: 1
address(es):
Mac Address: 00:d0:f8:00:00:01
INET6: fe80::2d0:f8ff:fe00:1 , subnet is fe80::/64
INET6: fec0:0:0:1::1 , subnet is fec0:0:0:1::/64
Joined group address(es):
ff01:1::1
ff02:1::1
ff02:1::2
ff02:1::1:ff00:1
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds<160-240>
ND router advertisements live for 1800 seconds
```

2.2.3 配置静态邻居

本节描述如何配置一个静态邻居，缺省情况下没有配置静态邻居，通常邻居是通过邻居发现协议(NDP)来动态学习并且维护其状态的，同时也允许手工为其配置静态的邻居。

下面是配置一个静态邻居的过程：

命令	作用
Ruijie#**configure terminal**	进入全局配置模式。

Ruijie(config)#**ipv6 neighbor** *ipv6-address interface-id hardware-address*	使用该命令在网络接口上配置一个静态的邻居。
Ruijie(config)#**end**	退回到特权模式。
Ruijie**#show ipv6 neighbors**	查看邻居表。
Ruijie#**copy running-config startup-config**	保存配置。

使用“**no ipv6 neighbor** *ipv6-address interface-id*”命令允许删除指定的邻居，下面是在 GigabitEthernet 0/1 上配置一个静态邻居的例子：

```
Ruijie(config)# ipv6 neighbor fec0:0:0:1::100 GigabitEthernet 0/1 00d0.f811.1234
Ruijie (config)# end
Ruijie# show ipv6 neighbors verbose fec0:0:0:1::100
IPv6 Address         Linklayer Addr   Interface
fec0:0:0:1::100      00d0.f811.1234   GigabitEthernet 0/1
State: REACH/H Age: - asked: 0
```

配置的静态邻居，只有邻居前缀与接口匹配时才生效。这里所说的匹配是指，配置的静态邻居前缀属于接口上配置的某一地址的网段内，且与该接口地址不冲突。无效的静态邻居，处于 inactive 状态，送往该目的的数据包不会按静态邻居指定的 mac 地址发送，而是根据路由和动态学习方式学习 mac 地址。静态邻居的有效性状态，可以通过 show ipv6 neighbor static 命令查看

2.2.4 配置地址冲突检测

本节主要描述如何配置地址冲突检测的次数，地址冲突检测是在所有的单播地址被正式赋予接口前所要进行的工作，即用来检测地址的唯一性。无论是手工配置的、无状态自动配置的还是有状态自动配置的地址都要进行地址冲突检测。但是有下面两种情况不需要进行地址冲突检测：

- 管理上禁止地址冲突检测，即将用于地址冲突检测时发送的邻居请求报文数设置为 0
- 被明确的配置为泛播地址的是不能应用于地址冲突检测的

另外如果接口的地址冲突检测功能没有关闭的话，接口每次从 Donw 状态变为 Up 状态时都会为配置的地址重新启动地址冲突检测过程。

下面是配置用于地址冲突检测时所发送的邻居请求报文的数量的过程：

命令	作用
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)#**interface** *interface-id*	进入接口配置模式。 注意，如果是二层端口，必须执行“no switchport”转换成三层端口。
Ruijie(config-if)#**ipv6 nd dad attempts** *attempts*	用于地址冲突检测时所发送的邻居请求报文的数量。当配置为 0 时表示禁止 在该接口上启用地址冲突检测功能

Ruijie(config-if)#**end**	退到特权模式。
Ruijie#**show ipv6 interface** *interface-id*	查看网络接口上的 IPv6 信息
Ruijie#**copy running-config startup-config**	保存配置。

使用**no ipv6 nd dad attempts** 命令将恢复缺省值，下面是配置SVI1上地址冲突检测发送邻居请求(NS)报文次数的例子：

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# ipv6 nd dad attempts 3
Ruijie(config-if)# end
Ruijie# show ipv6 interface GigabitEthernet 0/1
Interface GigabitEthernet 0/1 is Up, ifindex: 1
address(es):
Mac Address: 00:d0:f8:00:00:01
INET6: fe80::2d0:f8ff:fe00:1 , subnet is fe80::/64
INET6: fec0:0:0:1::1 , subnet is fec0:0:0:1::/64
Joined group address(es):
ff01:1::1
ff02:1::1
ff02:1::2
ff02:1::1:ff00:1
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 3
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds<160-240>
ND router advertisements live for 1800 seconds
```

2.2.5 配置接口IPv6 mtu

设备所有的接口都有缺省的 MTU（最大传输单元）值，如果一个 IPv6 报文超过 IPv6 MTU 的大小，RGOS 软件就会对报文进行拆分。所有在同一物理网段上的设备，其互联接口的 IPv6 MTU 一定要一致。

一个物理网络上的设备接口，相同协议 MTU 值必须保持一致。

要设置 IPv6 MTU 值，在接口配置模式中执行以下命令：

命令	作用
Ruijie(config-if)# **ipv6 mtu** *bytes*	设置 MTU 值，范围 1280~1500
Ruijie(config-if)# **no ipv6 mtu**	恢复缺省值

2.2.6 配置路由器的其它接口参数

设备的接口中关于 IPv6 的配置参数主要分为 2 部分，一类是用来控制设备本身行为的，一类是用来控制设备发送的路由器公告报文的内容以决定收到该路由器公告报文的主机进行什么样的动作。

下面逐一介绍这些命令：

命令	作用
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**interface** *interface-id*	进入接口配置模式。 注意，如果是二层端口，必须执行“no switchport”转换成三层端口。
Ruijie(config-if)#**ipv6 enable**	启用 IPv6 功能
Ruijie(config-if)#**ipv6 nd ns-interval** *milliseconds*	（可选）定义了邻居请求报文的重传间隔，单位是毫秒，即千分之一秒。缺省值是 1000 毫秒，即 1 秒。
Ruijie(config-if)#**ipv6 nd reachable-time** *milliseconds*	（可选）定义了邻居被认为可到达的时间，单位是毫秒，即千分之一秒。缺省值是 30000 毫秒，即 30 秒。
Ruijie(config-if)# **ipv6 nd prefix {***ipv6-prefix*/*prefix-length* | **default**} [[*valid-lifetime preferred-lifetime*] | [**at** *valid-date preferred-date*] | [**infinite** {**infinite** | *preferred-lifetime*}]] [**no-advertise**] | [[**off-link**] [**no-autoconfig**]]	（可选）设置路由器公告(RA)报文中所要公告的地址前缀
Ruijie(config-if)#**ipv6 nd ra-lifetime** *seconds*	（可选）设置路由器公告(RA)报文中的路由器生存期时间，即充当缺省设备的时间，当设置为 0 表示不充当其所直连的网络的缺省设备。缺省值是 1800 秒。
Ruijie(config-if)#**ipv6 nd ra-interval** {*seconds* | **min-max** *min_value max_value*}	（可选）设置设备定期发送路由器公告(RA)报文的间隔，单位是秒。缺省值是 200 秒.。 如果指定关键字 min-max，那么实际发送报文的间隔将在最小值和最大值之间随机选择一个值；如果不指定该关键字，实际发送报文的间隔将在配置值上下浮动百分之二十。
Ruijie(config-if)#**ipv6 nd managed-config-flag**	（可选）设置路由器公告(RA)报文中的“managed address configuration”标志位，决定了收到该路由器公告的主机是否要使用全状态自动配置来获取地址。缺省配置是在路由器公告报文中该标志位没有被设置。
Ruijie(config-if)#**ipv6 nd other-config-flag**	（可选）设置路由器公告报文中的“other stateful configuration”标志位，决定了收到该路由器公告的主机是否要使用全状态的自动配置来获取除地址之外的信息。缺省配置是在路由器公告报文中该标志位没有被设置。
Ruijie(config-if)#**ipv6 nd suppress-ra**	（可选）设置是否在该接口上阻止路由器公告（RA）报文发送。缺省配置是在网络接口上不发送路由器公告。
Ruijie(config-if)#**end**	退回到特权模式。
Ruijie#show **ipv6 interface** [*interface-id*] [ra-info]	显示接口的 ipv6 信息或者该接口发送 RA 的信息。
Ruijie#**copy running-config startup-config**	（可选）保存配置。

使用以上命令的 **no** 命令可以将其恢复缺省值，具体命令的使用指南可以参考“配置 IPv6 命令”。

2.3 IPv6 的监控与维护

主要是提供相关的命令用来显示 IPv6 协议内部的一些信息，比如显示接口的 IPv6 信息、邻居表和路由表等信息。

命令	作用
show ipv6 interface [*interface-id*] [*ra-info*]	显示接口上关于 IPv6 的信息
show ipv6 neighbors [**verbose**] [*interface-id*] [*ipv6-address*]	显示邻居的信息
show ipv6 route [**static | local | connected | bgp | rip | ospf | isis]**	显示 IPv6 路由表的信息

查看一个接口上关于 IPv6 的信息

```
Ruijie# show ipv6 interface
interface GigabitEthernet 0/1 is Down, ifindex: 1
address(es):
Mac Address: 00:d0:f8:00:00:01
INET6: fe80::2d0:f8ff:fe00:1 , subnet is fe80::/64
INET6: fec0:1:1:1::1 , subnet is fec0:1:1:1::/64
Joined group address(es):
ff01:1::1
ff02:1::1
ff02:1::2
ff02:1::1:ff00:1
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds<160-240>
ND router advertisements live for 1800 seconds
```

查看一个接口上关于设备在该接口上要发送的路由器公告报文的信息

```
Ruijie# show ipv6 interface ra-info
GigabitEthernet 0/1: DOWN
RA timer is stopped
waits: 0, initcount: 3
statistics: RA(out/in/inconsistent): 4/0/0, RS(input): 0
Link-layer address: 00:00:00:00:00:01
Physical MTU: 1500
ND router advertisements live for 1800 seconds
ND router advertisements are sent every 200 seconds<160-240>
```

```
Flags: !M!O, Adv MTU: 1500
ND advertised reachable time is 0 milliseconds
ND advertised retransmit time is 0 milliseconds
ND advertised CurHopLimit is 64
Prefixes: (total: 1)
fec0:1:1:1::/64(Def, Auto, vltime: 2592000, pltime: 604800, flags: LA)
```

查看 IPv6 的邻居表信息

```
Ruijie# show ipv6 neighbors
IPv6 Address                Linklayer Addr  Interface
fe80::200:ff:fe00:1       0000.0000.0001   GigabitEthernet 0/1
State: REACH/H Age: - asked: 0
fec0:1:1:1::1              0000.0000.0001   GigabitEthernet 0/1
State: REACH/H Age: - asked: 0
```

3 DHCP

3.1 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。

3.1.1 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。

3.1.2 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。

图 3-1 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 DHCPOFFER 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 DHCPREQUEST 采用广播包，是为了让其它所有发送 DHCPOFFER 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 DHCPOFFER 信息包中包含无效的配置参数，客户端会向服务器发送 DHCPDECLINE 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 DHCPOFFER 信息包，DHCP 服务器会发送 DHCPNAK 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设备，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。

3.1.3 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。

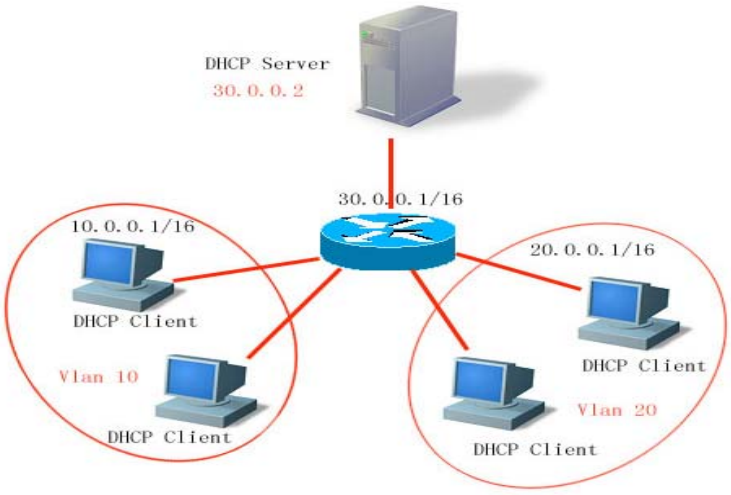
3.1.4 DHCP中继代理

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：

图 3-2



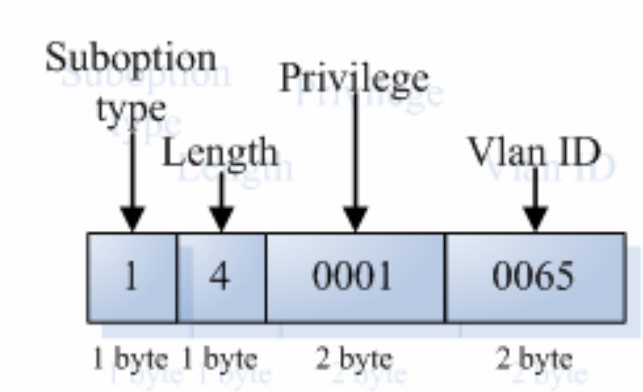
VLAN 10 和 VLAN 20 分别对应 10.0.0.1/16 和 20.0.0.1/16 的网络，而 DHCP 服务器在 30.0.0.1/16 的网络上，30.0.0.2 的 DHCP 服务器要对 10.0.0.1/16 和 20.0.0.1/16 的网络进行动态 IP 管理，只要在作为网关的设备上打开 DHCP 中继功能，并配置 30.0.0.2 为 DHCP 服务器的 IP 地址。

3.1.4.1 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。锐捷网络实现的 relay agent information 目前存在三种应用方案，下面分别对三种应用方案进行说明：

- relay agent information option dot1x：此种应用方案需要结合 802.1x 认证以及锐捷网络产品 RG-SAM。DHCP 中继根据 RG-SAM 在 802.1x 认证过程中下发的 IP 权限，以及 DHCP 客户端所属 vid，组合构成 Circuit ID 子选项。选项格式如下图所示：

图 3-3



- relay agent information option82：此种option的应用不需要结合其他协议模块的运行。DHCP中继根据接收DHCP请求报文的实体端口，以及设备自身的物理地址信息，组合构成option82 选项。选项格式如 图 3-4、图 3-5 所示：

图 3-4 Agent Circuit ID

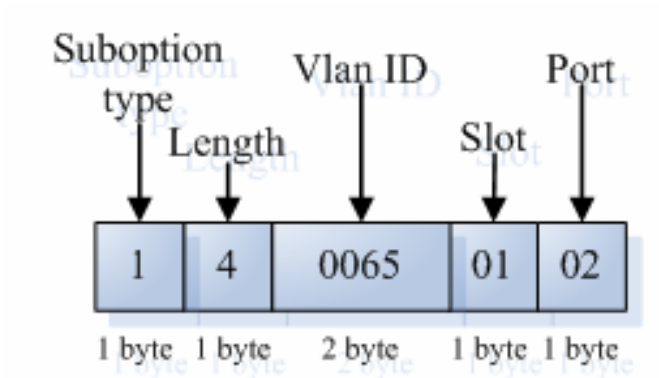
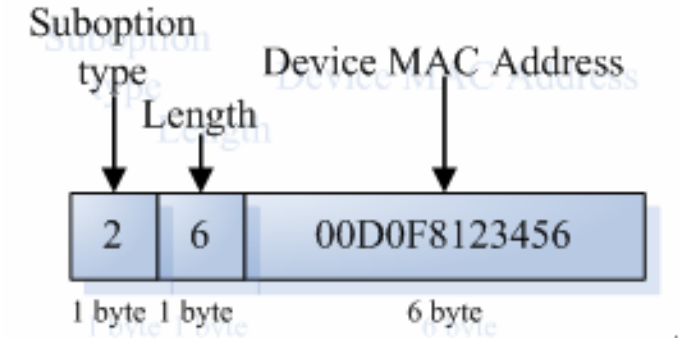


图 3-5 Agent Remote ID



3.1.4.2 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

能够使能此选项，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。

3.2 配置DHCP服务器

要配置 DHCP，请按照下面任务列表进行配置，其中前三个配置任务是必须的。

- 启用 DHCP 服务器与中继代理（要求）
- 配置 DHCP 排斥地址（要求）
- 配置 DHCP 地址池（要求）
- 配置 CLASS（可选）
- 配置绑定数据库保存（可选）
- 手工地址绑定（可选）
- 配置 Ping 包次数（可选）
- 配置 Ping 包超时时间（可选）

3.2.1 启用DHCP服务器

要启用 DHCP 服务器，全局配置模式中执行以下命令：

命令	作用
Ruijie(config)# **service dhcp**	启用 DHCP 服务器功能
Ruijie(config)# **no service dhcp**	关闭 DHCP 服务器功能

☑ 缺省情况下，DHCP 服务器和 DHCP 中继共用 **service dhcp** 这条命令，但是这两个功能是互斥的，两者之间的切换依赖于是否配置了 DHCP 地址池。

☑ DHCP 功能可能和某些功能出现冲突，也就是说和这些功能不能同时使用，请参考具体的提示信息。

3.2.2 配置DHCP排斥地址

如果没有特别配置，DHCP 服务器会试图将在地址池中定义的所有子网地址分配给 DHCP 客户端。因此，如果你想保留一些地址不想分配，比如已经分配给服务器或者设备了，你必须明确定义这些地址是不允许分配给客户端的。

要配置哪些地址不能分配给客户端，在全局配置模式中执行以下命令：

命令	作用
Ruijie(config)# **ip dhcp excluded-address** *low-ip-address* [*high-ip-address*]	定义 IP 地址范围，这些地址 DHCP 不会分配给客户端

Ruijie(config)# **no ip dhcp excluded-address** *low-ip-address* [*high-ip-address*]	取消配置地址排斥

配置 DHCP 服务器，一个好的习惯是将所有已明确分配的地址全部不允许 DHCP 分配，这样可以带来两个好处：

- 不会发生地址冲突；
- DHCP 分配地址时，减少了检测时间，从而提高 DHCP 分配效率。

3.2.3 配置DHCP地址池

DHCP 的地址分配以及给客户端传送的 DHCP 各项参数，都需要在 DHCP 地址池中进行定义。如果没有配置 DHCP 地址池，即使启用了 DHCP 服务器，也不能对客户端进行地址分配；但是如果启用了 DHCP 服务器，不管是否配置了 DHCP 地址池，DHCP 中继代理的总是起作用的。

你可以给 DHCP 地址池起个有意义、易记忆的名字，地址池的名字由字符和数字组成。锐捷产品可以定义多个地址池，根据 DHCP 请求包中的中继代理 IP 地址来决定分配哪个地址池的地址。

- 如果 DHCP 请求包中没有中继代理的 IP 地址，就分配与接收 DHCP 请求包接口的 IP 地址同一子网或网络的地址给客户端。如果没定义这个网段的地址池，地址分配就失败；
- 如果 DHCP 请求包中有中继代理的 IP 地址，就分配与该地址同一子网或网络的地址给客户端。如果没定义这个网段的地址池，地址分配就失败。

要进行 DHCP 地址池配置，请根据实际的需要执行以下任务，其中前三个任务要求执行：

- 配置地址池并进入其配置模式（要求）
- 配置地址池子网号及其掩码（要求）
- 配置客户端缺省网关（要求）
- 配置客户端启动文件（可选）
- 配置地址租期（可选）
- 配置客户端的域名（可选）
- 配置域名服务器（可选）
- 配置 NetBIOS WINS 服务器（可选）
- 配置客户端 NetBIOS 节点类型（可选）
- 配置 DHCP 地址池根据 Option82 分配地址（可选）

配置地址池名并进入其配置模式

要配置地址池名并进入地址池配置模式，地址池的配置模式显示为“Ruijie(dhcp-config)#”；在全局配置模式中执行以下命令：

命令	作用
Ruijie(config)# **ip dhcp pool** *dhcp-pool*	配置地址池名并进入地址池配置模式

配置地址池子网号及其掩码

进行动态地址绑定的配置，必须配置新建地址池的子网及其掩码，为 DHCP 服务器提供了一个可分配给客户端的地址空间。除非有地址排斥配置，否则所有地址池中的地址都有可能分配给客户端。DHCP 在分配地址池中的地址，是按顺序进行的，如果该地址已经在 DHCP 绑定表中或者检测到该地址已经在该网段中存在，就检查下一个地址，直到分配一个有效的地址。

要配置地址池子网和掩码，在地址池配置模式中执行以下命令:

命令	作用
Ruijie(dhcp-config)# **network** *network-number mask*	配置 DHCP 地址池的网络号和掩码

☑ 锐捷产品的 DHCP 动态地址池中，地址的分配是以客户端的物理地址和客户端 ID 为索引的，这就意味着 DHCP 动态地址池中不可能存在相同客户端的两份租约；如果客户端和服务器之间的网络拓扑存在路径上的冗余（客户端可以通过直连路径，同时也可以通过中继路径到达服务器），就会导致服务器分配地址出现问题，可能导致地址分配失败；因此，为了避免上述问题，要求网络管理员在构建网络的时候，通过其它的方式，如调整物理链路或者网络路径，来避免这种客户端到服务器的路径冗余。

配置客户端缺省网关

配置客户端默认网关，这个将作为服务器分配给客户端的默认网关参数。缺省网关的 IP 地址必须与 DHCP 客户端的 IP 地址在同一网络。

要配置客户端的缺省网关，在地址池配置模式中执行以下命令：

命令	作用
Ruijie(dhcp-config)# **default-router** *address* [*address2…address8*]	配置缺省网关

配置客户端启动文件

客户端启动文件是客户端启动时要用到的启动映像文件。启动映像文件通常是 DHCP 客户端需要下载的操作系统。

要配置客户端的启动文件，在地址池配置模式中执行以下命令：

命令	作用
Ruijie (dhcp-config)# **bootfile** *filename*	配置客户端启动文件名

配置地址租期

DHCP 服务器给客户端分配的地址，缺省情况下租期为 1 天。当租期快到时客户端需要请求续租，否则过期后就不能使用该地址。

要配置地址租期，在地址池配置模式中执行以下命令：

命令	作用
Ruijie(dhcp-config)# **lease** {*days* [*hours*] [*minutes*] | **infinite**}	配置地址租期

配置客户端的域名

可以指定客户端的域名，这样当客户端通过主机名访问网络资源时，不完整的主机名会自动加上域名后缀形成完整的主机名。

要配置客户端的域名，在地址池配置模式中执行以下命令：

命令	作用
Ruijie(dhcp-config)# **domain-name** *domain*	配置域名

配置域名服务器

当客户端通过主机名访问网络资源时，需要指定 DNS 服务器进行域名解析。要配置 DHCP 客户端可使用的域名服务器，在地址池配置模式中执行以下命令：

命令	作用
Ruijie(dhcp-config)# **dns-server** *address* [*address2…address8*]	配置 DNS 服务器

配置 NetBIOS WINS 服务器

WINS 是微软 TCP/IP 网络解析 NetNBIOS 名字到 IP 地址的一种域名解析服务。WINS 服务器是一个运行在 Windows NT 下的服务器。当 WINS 服务器启动后，会接收从 WINS 客户端发送的注册请求，WINS 客户端关闭时，会向 WINS 服务器发送名字释放消息，这样 WINS 数据库中与网络上可用的计算机就可以保持一致了。

要配置 DHCP 客户端可使用的 NetBIOS WINS 服务器，在地址池配置模式中执行以下命令：

命令	作用
Ruijie(dhcp-config)# **netbios-name-server** *address* [*address2…address8*]	配置 DNS 服务器

配置客户端 NetBIOS 节点类型

微软 DHCP 客户端 NetBIOS 节点类型有四种：1）Broadcast，广播型节点，通过广播方式进行 NetBIOS 名字解析；2）Peer-to-peer，对等型节点，通过直接请求 WINS 服务器进行 NetBIOS 名字解析；3）Mixed，混合型节点，先通过广播方式请求名字解析，后通过与 WINS 服务器连接进行名字解析；4）Hybrid，复合型节点，首先直接请求 WINS 服务器进行 NetBIOS 名字解析，如果没有得到应答，就通过广播方式进行 NetBIOS 名字解析。

缺省情况下，微软操作系统的节点类型为广播型或者复合型。如果没有配置 WINS 服务器，就为广播型节点；如果配置了 WINS 服务器，就为复合型节点。

要配置 DHCP 客户端 NetBIOS 节点类型，在地址池配置模式中执行以下命令：

命令	作用
Ruijie(dhcp-config)# **netbios-node-type** *type*	配置 NetBIOS 节点类型

配置 DHCP 地址池根据 Option82 分配地址

通常，DHCP 中继代理在转发报文的过程中会添加一个 Option82 选项用来记录客户端的相关信息（如客户端所处的 VLAN、设备槽号、端口号或者用户的 1X 等级等等），DHCP 服务器在收到该报文后可以通过解析 Option82 信息来根据客户端的具体信息进行地址分配。如对某个 VLAN 或者某个用户等级的客户端分配某个范围内的 IP 地址。在需要根据用户的具体网络位置信息（如 VLAN、槽号、端口号）来为用户分配特有的 IP 地址范围或者根据用户的优先级分配特有的（如受限、非受限）IP 地址时，可以采用该功能。

每个 DHCP 地址池可以根据 Option82 信息进行地址分配，我们把 Option82 信息进行匹配归类，在 DHCP 地址池中为这些归类分别指定可以分配的网段范围。这个归类称为 CLASS，一个 DHCP 地址池可以关联多个 CLASS，每个 CLASS 可以指定不同的网段范围。

在地址分配的过程中可以先根据客户端所处的网段确定可以分配的地址池，再根据其 Option82 信息进一步确定其所属的 CLASS，从 CLASS 对应的网段范围中分配 IP 地址。当一个请求报文匹配地址池中的多个 CLASS 时，按照 CLASS 在地址池中配置的先后顺序从对应的 CLASS 网段范围中分配地址，如果该 CLASS 已无可分配地址，则继续从下一个匹配的 CLASS 网段范围进行分配，依此类推。每个 CLASS 对应一个网段范围，网段范围必须从低地址到高地址，可以允许多个 CLASS 之间的网段范围重复。如果指明了地址池关联的 CLASS，但对应的网段范围没有配置，则该 CLASS 默认的网段范围和 CLASS 所处的地址池的网段范围相同。

要配置地址池关联的 CLASS 以及 CLASS 所对应的网段范围，在地址池配置模式中执行以下命令：

命令	作用
Ruijie(dhcp-config)# **class** *class-name*	配置关联的 CLASS 名称，并进入地址池的 CLASS 配置模式
Ruijie(config-dhcp-pool-class)#**address range** *low-ip-address high-ip-address*	配置对应的网段范围

当配置的 CLASS 在全局 CLASS 查找不到的情况下，会自动创建一个全局的 CLASS；在地址池中配置关联 CLASS 与静态手工绑定配置冲突，不可同时配置；每个地址池下允许配置的 CLASS 数目最大为 5 个。

3.2.4 配置CLASS

配置 CLASS 的 Option82 匹配信息

在全局模式下进入 CLASS 配置模式后，可以配置每个 CLASS 对应的具体的 Option82 匹配信息。一个 CLASS 可以匹配多个 Option82 信息，请求报文匹配时只要匹配其中一条信息即认为通过匹配，如果 CLASS 不配置任何的匹配信息，则认为该 CLASS 可以匹配任何携带 Option82 信息的请求报文。请求报文只有匹配了具体的 CLASS 后，才可从对应的地址池关联的 CLASS 网段范围中分配地址。

要配置全局的 CLASS 以及 CLASS 所对应的匹配 Option82 信息，在全局配置模式中执行以下命令：

命令	作用
Ruijie(config)# **ip dhcp class** *class-name*	配置 CLASS 名并进入全局 CLASS 配置模式
Ruijie(config-dhcp-class)# **relay agent information**	进入 Option82 匹配信息配置模式
Ruijie(config-dhcp-class-relayinfo)# **relay-information hex** *aabb.ccdd.eeff…* [*]	配置具体的 Option82 匹配信息 aabb.ccdd.eeff..为 16 进制数 *代表不完全匹配模式，只需要匹配*之前信息即通过匹配

全局 CLASS 可匹配的最大个数为 20 个。

配置 CLASS 的标识信息

要配置标识信息来描述 CLASS 代表的含义，在全局配置模式中执行以下命令：

命令	作用
Ruijie(config)# **ip dhcp class** *class-name*	配置 CLASS 名并进入 CLASS 配置模式
Ruijie(config-dhcp-class)#**remark *used* in #1 building**	配置标识信息

配置是否使用 CLASS 分配

要设置使用 CLASS 来进行地址分配，在全局配置模式中执行如下命令：

命令	作用
Ruijie(config)# **ip dhcp use class**	配置使用 CLASS 进行地址分配

3.2.5 配置绑定数据库保存

配置定时把绑定数据库保存到 FLASH

为了防止设备断电重启导致设备上的 DHCP 服务器的绑定数据库（租约信息）丢失，DHCP 提供可配置的定时把绑定数据库写入 FLASH 的命令，默认情况下，定时为 0，即不定时写 FLASH。

要配置定时把绑定数据库保存到 FLASH，在全局配置模式中执行以下命令：

命令	作用
Ruijie(config)# **[no] ip dhcp database write-delay** [*time*]	设置 DHCP 延迟写 FLASH 的时间 *time*：600s--86400s，缺省为 0

由于不停擦写 FLASH 会造成 FLASH 的使用寿命缩短，所以在设置延迟写 FLASH 时间时需要注意，设置时间较短有利于设备信息更有效的保存，设置时间较长能够减少写 FLASH 的次数，延长 FLASH 的使用寿命。

配置手动把绑定数据库保存到 FLASH

为了防止设备断电重启导致设备上的 DHCP 绑定数据库（租约信息）丢失，除了配置定时写 FLASH 外，也可以根据需要手动地把当前的绑定数据库信息立即写入 FLASH。

要配置手动把绑定数据库保存到 FLASH，在全局配置模式中执行以下命令：

命令	作用
Ruijie(config)# **ip dhcp database write-to-flash**	把 DHCP 绑定数据库信息写入 FLASH

3.2.6 手工地址绑定

地址绑定是指 IP 地址和客户端 MAC 地址的映射关系。地址绑定有两种：1）手工绑定，就是在 DHCP 服务器数据库中，通过手工定义将 IP 地址和 MAC 地址进行静态映射，手工绑定其实是一个特殊地址池；2）动态绑定，DHCP 服务器接收到 DHCP 请求时，动态地从地址池中分配 IP 地址给客户端，而形成的 IP 地址和 MAC 地址映射。

要定义手工地址绑定，首先需要为每一个手动绑定定义一个主机地址池，然后定义 DHCP 客户端的 IP 地址和硬件地址或客户端标识。硬件地址就是 MAC 地址。客户端标识，微软客户端一般定义客户端标识，而不定义 MAC 地址，客户端标识包含了网络媒介类型和 MAC 地址。关于媒介类型的编码，请参见 RFC 1700 中关于“Address Resolution Protocol Parameters”部分内容。以太网类型为“01”。

要配置手工地址绑定，在地址池配置模式中执行以下命令：

命令	作用
Ruijie(config)# **ip dhcp pool** *name*	定义地址池名，进入 DHCP 配置模式
Ruijie(dhcp-config)# **host *address*** [*netmask*]	定义客户端 IP 地址
Ruijie(dhcp-config)# **hardware-address** *hardware-address [type]* Or： Ruijie(dhcp-config)# **client-identifier** *unique-identifier*	定义客户端硬件地址，如 aabb.bbbb.bb88 type 标识客户端媒介类型 定义客户端的标识，如 01aa.bbbb.bbbb.88
Ruijie(dhcp-config)# **client-name** *name*	（可选）用标准的 ASCII 字符定义客户端的名字，名字不要包括域名。如定义 mary 主机名，不可定义成 mary.rg.com

3.2.7 配置Ping包次数

缺省情况，当 DHCP 服务器试图从地址池中分配一个 IP 地址时，会对该地址执行两次 Ping 命令(一次一个数据包)。如果 Ping 没有应答，DHCP 服务器认为该地址为空闲地址，就将该地址分配给 DHCP 客户端；如果 Ping 有应答，DHCP 服务器认为该地址已经在使用，就试图分配另外一个地址给 DHCP 客户端，直到分配成功。

要配置 Ping 包次数，在全局配置模式中执行以下命令：

命令	作用
Ruijie(config)# **ip dhcp ping packets** [*number*]	配置 DHCP 服务器在分配地址之前的 Ping 包次数，如果设为 0 则不进行 Ping 操作，缺省为 2。

3.2.8 配置Ping包超时时间

缺省情况下，DHCP 服务器 Ping 操作如果 500 毫秒没有应答，就认为没有该 IP 地址主机存在。你可以通过调整 Ping 包超时时间，改变服务器 Ping 等待应答的时间。

要配置 Ping 包超时时间，在全局配置模式中执行以下命令：

命令	作用
Ruijie(config)# **ip dhcp ping timeout** *milliseconds*	配置 DHCP 服务器 Ping 包超时时间，缺省为 500ms。

3.3 配置DHCP客户端

配置 DHCP 客户端任务列表如下：

- 配置以太网接口 DHCP 客户端（可选）
- 配置 PPP 封装链路上的 DHCP 客户端（可选）
- 配置 FR 封装链路上的 DHCP 客户端（可选）
- 配置 HDLC 封装链路上的 DHCP 客户端（可选）

3.3.1 配置以太网接口DHCP客户端

要配置以太网接口 DHCP 客户端，在接口配置模式中执行以下命令：

命令	作用
Ruijie(config-if)# **ip address dhcp**	配置通过 DHCP 得到 IP 地址

3.3.2 配置PPP封装链路上的DHCP客户端

要配置 DHCP 客户端，在接口配置模式中执行以下命令：

命令	作用
Ruijie(config-if)# **ip address dhcp**	配置通过 DHCP 得到 IP 地址

3.3.3 配置FR封装链路上的DHCP客户端

要配置 DHCP 客户端，在接口配置模式中执行以下命令：

命令	作用
Ruijie(config-if)# **ip address dhcp**	配置通过 DHCP 得到 IP 地址

3.3.4 配置HDLC封装链路上的DHCP客户端

要配置 DHCP 客户端，在接口配置模式中执行以下命令：

命令	作用
Ruijie(config-if)# **ip address dhcp**	配置通过 DHCP 得到 IP 地址

3.4 配置DHCP中继

3.4.1 启用DHCP中继代理

在全局配置模式下，请按如下步骤配置 DHCP 中继代理：

命令	作用
Ruijie (config)# **service dhcp**	启用 DHCP 代理
Ruijie(config)# **no service dhcp**	关闭 DHCP 代理。

3.4.2 配置DHCP 服务器的IP地址

在配置 DHCP 服务器的 IP 地址后，设备将收到的 DHCP 请求报文将转发给它；同时，将收到的 DHCP 服务器响应报文转发给 DHCP 客户端。

DHCP 服务器地址可以全局配置，也可以在三层接口上配置。全局或者每个三层接口上最多可以配置 20 个 DHCP 服务器地址。在接口上收到 DHCP 请求报文时，首先使用接口上的 DHCP 服务器列表；如果接口上面没有配置 DHCP 服务器列表，则使用全局配置的 DHCP 服务器列表。

DHCP 中继支持基于 vrf 的中继功能，配置方法就是在对应的服务器地址前面添加 vrf 参数。

全局配置模式下可对 dhcp relay 的 cycle-mode 参数进行配置，当不启用 cycle-mode 的时候表示 dhcp relay 允许把接收到的 dhcp client 请求报文转发到以上规则的所有 dhcp server 上；当启用 cycle-mode 的时候表示 dhcp relay 只把接收到的 dhcp client 请求报文转发到以上规则的第一个 dhcp server 上。cycle-mode 只在全局配置模式下配置，作用于全局和接口，默认为不启用。

配置 DHCP 服务器地址请按如下方式进行：

命令	作用
Ruijie(config)# **ip helper-address** [**vrf** {*vrf-name*} | **global**] *A.B.C.D*	添加一个全局的 DHCP 服务器地址。可以显示的指定服务器所属的 VPN 或者全局空间
Ruijie(config)# **ip helper-address cycle-mode**	启用 dhcp relay 的 cycle-mode 功能
Ruijie(config-if)# **ip helper-address** [**vrf** {*vrf-name*} | **global**] *A.B.C.D*	添加一个接口的 DHCP 服务器地址。此命令必须在三层接口下配置。 可以显示指定服务器所属的 VPN 或者全局空间，默认与当前接口属于同一 VPN 空间，或者全局空间；
Ruijie(config)# **no ip helper-address** [**vrf** {*vrf-name*} | **global**] *A.B.C.D*	删除一个全局的 DHCP 服务器地址
Ruijie(config)# **no ip helper-address cycle-mode**	关闭 dhcp relay 的 cycle-mode 功能
Ruijie(config-if)# **no ip helper-address** [**vrf** {*vrf-name*} | **global**] *A.B.C.D*	删除一个接口的 DHCP 服务器地址

3.4.3 配置DHCP option dot1x

通过理解 DHCP Relay Agent Information 的描述可知，在网络如果需要根据用户权限的不同而给用户分配不同权限 IP 时，我们就可以通过配置 **ip dhcp relay information option dot1x** 来配置打开 DHCP 中继设备的 option dot1x 功能。当设备做为 DHCP 中继转发 DHCP 请求报文时，结合 802.1x，在 DHCP 请求报文中添 option 选项信息。该功能和 dot1x 功能结合使用。

在全局配置模式下，请按如下步骤配置 DHCP option dot1x：

命令	作用
Ruijie(config)# **ip dhcp relay information option dot1x**	启用 DHCP option dot1x 功能
Ruijie(config)# **no ip dhcp relay information option dot1x**	关闭 DHCP option dot1x 功能。

3.4.4 配置DHCP option dot1x access-group

在 option dot1x 的应用方案中，需要设备控制未认证或低权限的 IP 只有访问特定的一些 IP 地址的权限，以及限制低权限用户之间的互相访问，此时可以通过配置命令 **ip dhcp relay information option dot1x access-group** *acl-name* 来实现。这里的 *acl-name* 所定义的 ACL 必须预先配置，用以对某些内容进行过滤，主要是用于禁止未认证用户之间的互相访问。另外，这里所关联的 ACL 被应用到设备所有端口上，并且该 ACL 没有缺省的 ACE，与其它接口所关联的 ACL 没有冲突关系，例如：

为未认证的所用用户规划一类 IP 地址，为 192.168.3.2-192.168.3.254，192.168.4.2-192.168.4.254，192.168.5.2-192.168.5.254；另外 192.168.3.1、192.168.4.1、192.168.5.1 作为网关地址，不分配给用户。则用户在未认证之前使用 192.168.3.x-5.x 的地址到达 web portal 以下载客户端软件。因此需要在设备上配置如下：

```
Ruijie# configure terminal
Ruijie(config)# ip access-list extended DenyAccessEachOtherOfUnauthrize
Ruijie(config-ext-nacl)# permit ip any host 192.168.3.1
```

//允许发往网关的报文

```
Ruijie(config-ext-nacl)# permit ip any host 192.168.4.1
Ruijie(config-ext-nacl)# permit ip any host 192.168.5.1
Ruijie(config-ext-nacl)# permit ip host 192.168.3.1 any
```

//允许源 IP 地址为网关的报文通讯

```
Ruijie(config-ext-nacl)# permit ip host 192.168.4.1 any
Ruijie(config-ext-nacl)# permit ip host 192.168.5.1 any
Ruijie(config-ext-nacl)# deny ip 192.168.3.0 0.0.0.255 192.168.3.0 0.0.0.255
```

//禁止未认证用户相互访问

```
Ruijie(config-ext-nacl)# deny ip 192.168.3.0 0.0.0.255 192.168.4.0  0.0.0.255
Ruijie(config-ext-nacl)# deny ip 192.168.3.0 0.0.0.255 192.168.5.0  0.0.0.255
Ruijie(config-ext-nacl)# deny ip 192.168.4.0 0.0.0.255 192.168.4.0  0.0.0.255
Ruijie(config-ext-nacl)# deny ip 192.168.4.0 0.0.0.255 192.168.5.0  0.0.0.255
```

```
Ruijie(config-ext-nacl)# deny ip 192.168.5.0 0.0.0.255 192.168.5.0  0.0.0.255
Ruijie(config-ext-nacl)# deny ip 192.168.5.0 0.0.0.255 192.168.3.0  0.0.0.255
Ruijie(config-ext-nacl)# deny ip 192.168.5.0 0.0.0.255 192.168.4.0  0.0.0.255
Ruijie(config-ext-nacl)# exit
```

然后再使用命令 **ip dhcp relay information option dot1x access-group DenyAccessEachOtherOfUnauthrize** 把命令应用全局接口上。在全局配置模式下，请按如下步骤配置 **DHCP option dot1x access-group**：

命令	作用
Ruijie(config)# **ip dhcp relay information option dot1x access-group** *acl-name*	应用 DHCP option dot1x acl
Ruijie(config)# **no ip dhcp relay information option dot1x access-group** *acl-name*	取消 DHCP option dot1x acl 的应用。

3.4.5 配置DHCP option 82

当配置命令 **ip dhcp relay information option82** 命令时，设备做为 DHCP 中继，在转发 DHCP 请求报文过程中，在 DHCP 请求报文中添加 option 信息。

在全局配置模式下，请按如下步骤配置 DHCP option82：

命令	作用
Ruijie(config)# **ip dhcp relay information option82**	启用 DHCP option82 功能
Ruijie(config)# **no ip dhcp relay information option82**	关闭 DHCP option82 功能。

3.4.6 配置DHCP relay check server-id

当配置命令 **ip dhcp relay check server-id** 后，DHCP Relay 仅将 DHCP 请求报文转发到 option server-id 中指定的服务器。如果没有配置该命令，则向所有配置的 DHCP 服务器转发 DHCP 请求报文。

在全局配置模式下，请按如下步骤配置 **DHCP relay check server-id** 功能：

命令	作用
Ruijie(config)# **ip dhcp relay check server-id**	启用 DHCP relay check server-di 功能
Ruijie(config)# **no ip dhcp relay check server-id**	关闭 DHCP relay check server-id 功能。

3.4.7 配置DHCP relay suppression

在指定接口上配置命令 **ip dhcp relay suppression** 后，将屏蔽该接口上收到的 DHCP 请求报文；而对于其他接口上收到的 DHCP 请求报文，则正常转发。

在接口配置模式下，请按如下步骤配置 **ip dhcp relay suppression** 功能：

命令	作用
Ruijie(config-if)# **ip dhcp relay suppresson**	启用 DHCP relay suppresson 功能
Ruijie(config-if)# **no ip dhcp relay suppresson**	关闭 DHCP relay suppresson 功能。

3.4.8 配置DHCP relay的其他注意事项

配置 DHCP option dot1x 的注意事项

- 此命令的实际生效需要在 AAA/802.1x 相关的配置正确的情况下。
- 在应用此方案时需要启用 802.1x 的 DHCP 模式的 IP 授权。
- 此命令与 dhcp option82 命令互斥，不能同时使用。
- 在启用了 802.1x 的 DHCP 模式的 IP 授权的模式下，也会设置 MAC + IP 的绑定，所以不能与 DHCP 动态绑定功能同时启用。

配置 DHCP option82 的注意事项

- DHCP option82 功能与 **dhcp option dot1x** 功能互斥，不能同时使用。

3.4.9 DHCP Relay配置实例

如下命令打开了 dhcp relay 功能、添加了两组服务器地址的例子：

```
Ruijie# configure  terminal                              //打开 DHCP 中继功能
Ruijie(config)# service dhcp                 //打开 DHCP option82 功能
Ruijie(config)# ip dhcp relay information option82
Ruijie(config)# ip helper-address 192.18.100.1 //添加全局服务器地址
Ruijie(config)# ip helper-address 192.18.100.2     //添加接口服务器地址
Ruijie(config)# interface gigabitEthernet 0/3
Ruijie(config-if-gigabitEthernet 0/3)# ip helper-address 192.18.200.1
Ruijie(config-if-gigabitEthernet 0/3)# ip helper-address 192.18.200.2
Ruijie(config-if-gigabitEthernet 0/3)# end
```

3.5 监视和维护信息

3.5.1 显示DHCP配置

请在特权模式下用 **show running-config** 命令显示 DHCP 配置。

```
Ruijie# show running-config
Building configuration...
Current configuration : 1464 bytes
version RGNOS 10.1.00(1), Release(11758)(Fri Mar 30 12:53:11 CST 2007 -nprd
hostname Ruijie
vlan 1
```

```
ip helper-address 192.18.100.1
ip helper-address 192.18.100.2
ip dhcp relay information option dot1x
interface GigabitEthernet 0/1
interface GigabitEthernet 0/2
interface GigabitEthernet 0/3
no switchport
ip helper-address 192.168.200.1
ip helper-address 192.168.200.2
interface VLAN 1
ip address 192.168.193.91 255.255.255.0
line con 0
exec-timeout 0 0
line vty 0
exec-timeout 0 0
login
password 7 0137
line vty 1 2
login
password 7 0137
line vty 3 4
login
end
```

3.5.2 监视和维护DHCP服务器

监视和维护 DHCP 服务器有三类命令：

- 清除命令，可以清除 DHCP 地址绑定、地址冲突、服务器统计状态等信息；
- 调试（debug）命令，输出必要的调试信息，主要用于故障诊断和排除；
- 显示命令，显示 DHCP 相关信息。

锐捷产品提供了四条清除命令，要进行相关清除信息操作，在命令执行模式中执行以下命令：

命令	作用
Ruijie# **clear ip dhcp binding** { *address* | *}	清除 DHCP 地址绑定信息
Ruijie# **clear ip dhcp conflict** { *address* | *}	清除 DHCP 地址冲突信息
Ruijie# **clear ip dhcp server statistics**	清除 DHCP 服务器统计状态
Ruijie# **clear ip dhcp relay statistics**	清除 DHCP 代理统计状态

要进行 DHCP 服务器的调试，在命令执行模式中执行以下命令：

命令	作用
Ruijie# **debug ip dhcp server [events | packet]**	调试 DHCP 服务器

要显示 DHCP 服务器的工作状态，在命令执行模式中执行以下命令：

命令	作用
show ip dhcp binding [*address*]	显示 DHCP 地址绑定信息
show ip dhcp conflict	显示 DHCP 地址冲突信息
show ip dhcp server statistics	显示 DHCP 服务器统计信息
show ip dhcp relay-statistics	显示 DHCP 代理统计信息

3.5.3 监视和维护DHCP客户端

监视和维护 DHCP 客户有两类命令，可以通过在客户端上进行以下操作：

1) 调试（debug）命令，输出必要的调试信息，主要用于故障诊断和排除.

2) 显示命令，显示 DHCP 相关信息。

要进行 DHCP 客户的调试，在命令执行模式中执行以下命令：

命令	作用
Ruijie# **debug ip dhcp client**	调试 DHCP 客户

要显示 DHCP 客户获得的租约信息，在命令执行模式中执行以下命令：

命令	作用
show dhcp lease	显示 DHCP 租约信息

3.6 DHCP配置用例

3.6.1 地址池支持Option82 配置范例

在以下配置中，定义了一个地址池 net82，地址池网段为 172.16.1.0/24，关联的 CLASS 有 class1、class2、class3、class4。class1 从 172.16.1.1—172.16.1.8 范围中分配地址，class2 从 172.16.1.9—172.16.1.18 范围中分配地址，class3 从 172.16.1.19—172.16.1.28 范围中分配地址，class4 不指明网段范围，默认从地址池的整个网段范围中分配地址。并设置 class1 匹配 Option82 信息 0100002120，class2 匹配 Option82 信息 0106020145，class3 匹配 Option82 信息 06020506*，class4 匹配任何信息。如下：

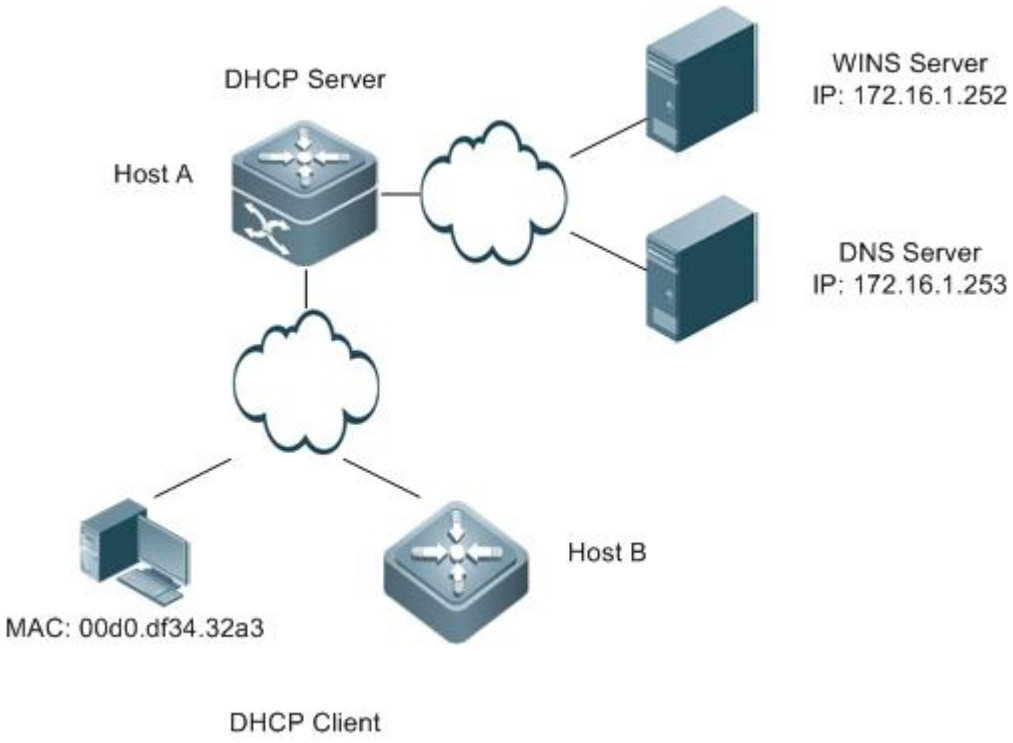
```
!
ip dhcp class class1
 relay agent information
    relay-information hex 0100002120
!
ip dhcp class class2
 relay agent information
    relay-information hex 0106020145
!
ip dhcp class class3
```

```
 relay agent information
    relay-information hex 06020506*
!
ip dhcp class class4
!
ip dhcp pool net82
network 172.16.1.0 255.255.255.0
class class1
address range 172.16.1.1 172.16.1.8
class class2
address range 172.16.1.9 172.16.1.18
class class3
address range 172.16.1.19 172.16.1.28
class class4
```

3.6.2 DHCP典型配置用例

拓扑图

图 3-6 DHCP 案例示意图



应用需求

- Host A 可以作为 DHCP Server 为一部分客户端用户分配动态 IP 地址。可分配地址的网段为 172.16.1.0/24，缺省网关为 172.16.1.254，域名为 ruijie.com，域名服务器为 172.16.1.253，WINS 服务器为 172.16.1.252，NetBIOS 节点类型为复合型，地址租期为 1 天。在地址的网段中除了 172.16.1.2~172.16.1.100 地址外，其余地址均为可分配地址。
- Host A 为一部分客户端用户分配固定 IP 地址。对 MAC 地址为 00d0.df34.32a3 的 DHCP 客户端分配的 IP 地址为 172.16.1.101，掩码为 255.255.255.0，主机名为 admin，缺省网关为 172.16.1.254，域名服务器为 172.16.1.253，WINS 服务器为 172.16.1.252，NetBIOS 节点类型为复合型。
- HOST B 为设备接口 FastEthernet 0/0 配置 DHCP 自动分配地址。

配置要点

- 在 Host A 上开启 DHCP 服务器功能，创建一个地址池，用于配置动态分配 IP 地址，另外创建一个地址池，用于手工绑定 IP 地址。并在相应的地址池指定域名服务器地址（本例为 DNS Server 和 WINS Server 的地址）以及客户端的域名。
- 在 Host B 上指定接口开启 DHCP 客户端功能，自动获取 IP 地址。

配置步骤

第一步，在 Host A 上，创建新的 DHCP 地址池，配置动态分配 IP 地址。

！配置地址池名为“dynamic”，并进入 DHCP 配置模式。

```
HostA# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
HostA(config)# ip dhcp pool dynamic
```

！在 DHCP 配置模式下，配置一个可分配给客户的 IP 地址网段，并配置该地址网段的默认网关。并设置租期为 1 天。

```
HostA(dhcp-config)# network 172.16.1.0 255.255.255.0
HostA(dhcp-config)# default-router 172.16.1.254
HostA(dhcp-config)# lease 1
```

第二步，指定“dynamic”地址池的 DNS Server，并配置客户端的域名。

！假设 DNS Server 的 IP 地址是 172.16.1.253，在地址池中配置域名服务器，并配置客户端域名为 ruijie.com。

```
HostA(dhcp-config)# dns-server 172.16.1.253
HostA(dhcp-config)# domain-name ruijie.com
```

第三步，指定“dynamic”地址池的 WINS Server，并配置客户端 NetBIOS 节点类型。

!假设 WIN Server 的 IP 地址是 172.16.1.252，在地址池中配置 NetBIOS WINS 服务器，并配置 NetBIOS 节点类型为 Hybrid。

```
HostA(dhcp-config)# netbios-name-server 172.16.1.252
HostA(dhcp-config)# netbios-node-type h-node
```

第四步，在全局模式下配置排斥地址。

！如上，IP 地址为 172.16.1.254、172.16.1.253、172.16.1.252 已经分配作为对应网段的网关、DNS 服务器、WINS 服务器的地址，并且地址范围 172.16.1.2~172.16.1.100 也不允许分配。通过排斥地址配置明确这些地址不允许分配给客户端用户。

```
HostA(dhcp-config)# exit
HostA(config)# ip dhcp excluded-address 172.16.1.252 172.16.1.254
HostA(config)# ip dhcp excluded-address 172.16.1.2 172.16.1.100
```

第五步，创建另一个地址池，配置手工绑定 IP 地址。

！配置地址池名为“static”，并进入 DHCP 配置模式。

```
HostA(config)# ip dhcp pool static
```

！ 指明 IP 地址为 172.16.1.101/24 手工绑定 MAC 地址为 00d0.df34.32a3，客户端名称为 admin。注意：定义客户端的标识需增加网络媒介类型标识（以太网类型为“01”），即手工绑定的 MAC 地址对应的客户端标识为 00d0.df34.32a3.14。

```
HostA(dhcp-config)# host 172.16.1.101 255.255.255.0
HostA(dhcp-config)# client-identifier 00d0.df34.32a3.14
HostA(dhcp-config)# client-name admin
```

第六步，指定“static”地址池对应的网关地址。

！配置网关地址为 172.16.1.254。

```
HostA(dhcp-config)# default-router 172.16.1.254
```

第七步，指定“static”地址池的 DNS Server，并配置客户端的域名。

！同上，假设 DNS Server 的 IP 地址是 172.16.1.253，在地址池中配置域名服务器，并配置客户端域名为 ruijie.com。

```
HostA(dhcp-config)# dns-server 172.16.1.253
HostA(dhcp-config)# domain-name ruijie.com
```

第八步，指定“static”地址池的 WINS Server，并配置客户端 NetBIOS 节点类型。

！同上，假设 WIN Server 的 IP 地址是 172.16.1.252，在地址池中配置 NetBIOS WINS 服务器，并配置 NetBIOS 节点类型为 Hybrid。

```
HostA(dhcp-config)# netbios-name-server 172.16.1.252
HostA(dhcp-config)# netbios-node-type h-node
HostA(dhcp-config)# exit
```

第九步，在 Host A 上启用 DHCP Server。

```
HostA(dhcp-config)# exit
HostA(config)# service dhcp
```

第十步，在 Host B 上启用 DHCP Client。

！此例默认客户端的接口为三层口，启动 DHCP client。

```
HostB(config)# interface fastEthernet 0/1
HostB(config-if-fastEthernet 0/1)# ip address dhcp
```

验证结果

第一步，查看 Host A 的配置信息

```
HostA# show running-config
!
service dhcp
!
ip dhcp excluded-address 172.16.1.252 172.16.1.254
ip dhcp excluded-address 172.16.1.2 172.16.1.100
!
!
ip dhcp pool dynamic
 netbios-node-type n-node
 netbios-name-server 172.16.1.252
 domain-name ruijie.com
 lease 1 0 0
 network 172.16.1.0 255.255.255.0
 dns-server 172.16.1.253
 default-router 172.16.1.254
!
ip dhcp pool static
 client-name admin
 client-identifier 00d0.df34.32a3.14
 host 172.16.1.101 255.255.255.0
 netbios-node-type n-node
 netbios-name-server 172.16.1.252
 domain-name ruijie.com
 dns-server 172.16.1.253
 default-router 172.16.1.254
!
```

第二步，查看 Host B 的配置信息

```
HostB# show running-config
!
interface fastEthernet 0/1 //注：如果是交换机设备，这里应该还有 no switchport 命令，将接口设置为三层口
ip address dhcp
```

第三步，接入一台 MAC 地址为 0013.2049.9014 的 PC，在 Host A 上查看 DHCP Server 分配 IP 地址信息。

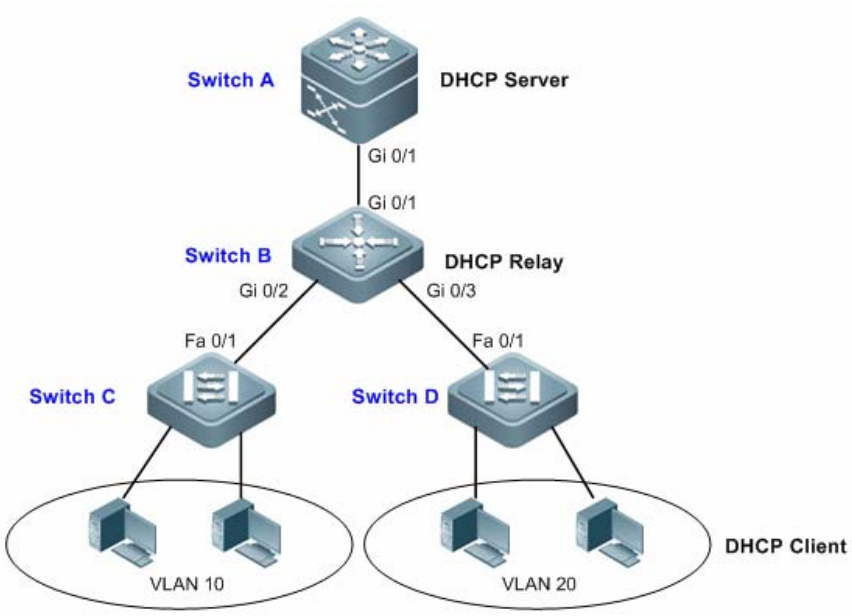
```
Ruijie#show ip dhcp binding
IP address    Client-Identifier/     Lease expiration         Type
                Hardware address
172.16.1.101  00d0.df34.32a3.14      IDLE                       Manual 172.16.1.102  0100.e04c.70b7.e2 000
days 23 hours 48 mins Automatic
```

3.7 DHCP Relay配置用例

3.7.1 DHCP Relay典型配置用例（交换机）

拓扑图

图 3-7 DHCP Relay 用例示意图



应用需求

如上图所示，Switch C 和 Switch D 作为接入设备，分布着 VLAN 10 和 VLAN 20 的 PC 用户，Switch B 作为网关设备，Switch A 作为核心路由设备。主要需求如下：

- Switch A 可以充当 DHCP Server，为不同 VLAN 用户动态分配不同网段的 IP 地址。
- Switch C 和 Switch D 下的接入用户可以跨网段动态获取 IP 地址。

配置要点

- **配置 DHCP Server**：在 Switch A 上，分别为 VLAN 10 和 VLAN 20 的用户创建 DHCP 地址池，开启 DHCP Server 功能。（DHCP Server 的相关配置可参见《DHCP 配置指南》）
- **配置 DHCP Relay**：在 Switch B 上，指定 DHCP 服务器地址（本例配置 DHCP Server 地址为 10.1.1.2/24），并开启 DHCP Server 功能。

Switch C 和 Switch D 上仅需根据具体情况配置对应端口所属 VLAN，一旦接入 PC 即可动态获取 IP 地址。此处不再详细列举。

配置步骤

第一步，配置 DHCP Server

！在全局模式下，在 Switch A 上创建一个 DHCP 地址池，命名为“vlan10”，对应的 IP 网段为 192.168.1.0/24，网关地址为 192.168.1.1。

```
SwitchA(config)#ip dhcp pool vlan10
SwitchA(dhcp-config)#network 192.168.1.0 255.255.255.0
SwitchA(dhcp-config)#default-router 192.168.1.1
SwitchA(dhcp-config)#exit
```

！同上，创建“vlan20”地址池，IP 网段为 192.168.2.0/24，网关地址为 192.168.2.1.

```
SwitchA(config)#ip dhcp pool vlan20
SwitchA(dhcp-config)#network 192.168.2.0 255.255.255.0
SwitchA(dhcp-config)#default-router 192.168.2.1
SwitchA(dhcp-config)#exit
```

！在全局模式下，配置排斥地址为 192.168.1.1 和 192.168.2.1，避免分配的 IP 地址与网关地址冲突。

```
SwitchA(config)#ip dhcp excluded-address 192.168.1.1
SwitchA(config)#ip dhcp excluded-address 192.168.2.1
```

！开启 DHCP Server。

```
SwitchA(config)#service dhcp
```

第二步，配置 Switch A 与 Switch B 之间三层通信。

！在 Switch A 上，配置端口 Gi 0/1 为 Route Port，对应的 IP 地址为 10.1.1.2/24。

```
SwitchA(config)#interface gigabitEthernet 0/1
SwitchA(config-if-GigabitEthernet 0/1)#no switchport
SwitchA(config-if-GigabitEthernet 0/1)#ip address 10.1.1.2 255.255.255.0
SwitchA(config-if-GigabitEthernet 0/1)#exit
```

！在 Switch B 上，配置端口 Gi 0/1 为 Route Port，对应的 IP 地址为 10.1.1.3/24

```
SwitchB(config)#interface gigabitEthernet 0/1
SwitchB(config-if)#no switchport
SwitchB(config-if)#ip address 10.1.1.3 255.255.255.0
SwitchB(config-if)#exit
```

！在 Switch A 上配置缺省路由

```
SwitchA(config)#ip route 0.0.0.0 0.0.0.0 10.1.1.3
```

第三步，配置接入用户的网关

！在 Switch B 上，配置 VLAN 10 的 SVI 为 192.168.1.1/24。

```
SwitchB(config)#vlan 10
SwitchB(config-vlan)#exit
SwitchB(config)#interface vlan 10
SwitchB(config-if)#ip address 192.168.1.1 255.255.255.0
SwitchB(config-if)#exit
```

！同上，配置 VLAN 20 的 SVI 为 192.168.2.1/24。

```
SwitchB(config)#vlan 20
SwitchB(config-vlan)#exit
SwitchB(config)#interface vlan 20
SwitchB(config-if)#ip address 192.168.2.1 255.255.255.0
SwitchB(config-if)#exit
```

第四步，配置 DHCP Relay

！在 Switch B 上，全局配置 DHCP 服务器的地址为 10.1.1.2，并开启 DHCP Server。

```
SwitchB(config)#ip helper-address 10.1.1.2
SwitchB(config)#service dhcp
```

第五步，配置 Switch B 和 Switch C、D 之间的二层通信

！在 Switch B 上，配置端口 Gi 0/2 和 Gi 0/3 为 Trunk Port。

```
SwitchB(config)#interface range gigabitEthernet 0/2-3
SwitchB(config-if-range)#switchport mode trunk
```

！同理，配置 Switch C、D 的端口 Fa 0/1 为 Trunk Port，此处不列举。

验证结果

第一步，查看各设备的配置信息。

！Switch A 的配置

```
SwitchA#show running-config
!
service dhcp
!
ip dhcp excluded-address 192.168.1.1
ip dhcp excluded-address 192.168.2.1
!
ip dhcp pool vlan10
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
!
ip dhcp pool vlan20
 network 192.168.2.0 255.255.255.0
 default-router 192.168.2.1
```

```
!
interface GigabitEthernet 0/1
 no switchport
 no ip proxy-arp
 ip address 10.1.1.2 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 10.1.1.3
!
```

！Switch B 的配置

```
SwitchB#show running-config
!
vlan 10
!
vlan 20
!
service dhcp
ip helper-address 10.1.1.2
!
interface GigabitEthernet 0/1
 no switchport
 no ip proxy-arp
 ip address 10.1.1.3 255.255.255.0
!
interface GigabitEthernet 0/2
 switchport mode trunk
!
interface GigabitEthernet 0/3
 switchport mode trunk
!
interface VLAN 10
 no ip proxy-arp
 ip address 192.168.1.1 255.255.255.0
!
interface VLAN 20
 no ip proxy-arp
 ip address 192.168.2.1 255.255.255.0
!
```

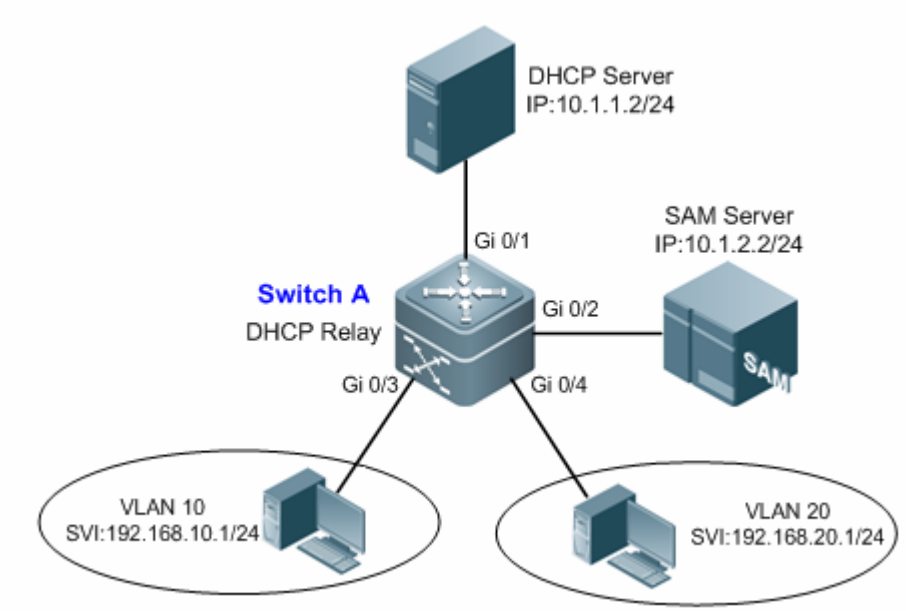
第二步，将两台 PC 分别接入 VLAN 10 和 VLAN 20 下的端口，查看 PC 动态获取 IP 地址的情况。

```
SwitchA#show ip dhcp binding
IP address Client-Identifier/ Lease expiration  Type Hardware address
192.168.1.2 0100.1320.4990.14 000 days 23 hours 59 mins  Automatic
192.168.2.2 0100.e04c.70b7.e2 000 days 23 hours 59 mins  Automatic
```

3.7.2 DHCP Option dot1x典型配置用例

拓扑图

图 3-8 DHCP Option Dot1X 用例示意图



应用需求

Switch A 作为三层设备，实现不同网段之间的路由通信。

接入用户划分属于不同 VLAN，通过 Dot1x 认证上网，SAM Server 为不同用户下发不同的访问权限。

DHCP Server 可以基于认证用户的权限为其分配 IP 地址。

配置要点

- **配置基本 DHCP Relay 功能：**在 Switch A 上，指定 DHCP 服务器地址（本例为 10.1.1.2/24），开启 DHCP Server 功能。通过以上配置，用户可以跨网段动态获取 IP 地址。
- **配置 802.1X 认证：**在 Switch A 上，设置 802.1X 认证的开关，指定用户端口为受控端口（本例为 Gi 0/3 和 Gi 0/4）。通过以上配置，用户需要通过 Dot1x 认证才能上网。
- **配置下发权限 IP：**在 Switch A 上，开启 DHCP Option dot1x 功能，配置 IP 授权模式为 DHCP Server。通过以上配置，DHCP Server 可以基于用户的权限分配 IP 地址。

对于 802.1X 的相关配置说明请参考《802.1X 配置指南》

本例的应用实现需要关联配置 SAM 和 DHCP 服务器，此处不再列举。

配置步骤

配置 Switch A

第一步，配置用户的网关地址以及服务器的接口地址。

！配置端口 Gi 0/3 和 Gi 0/4 对应的 VLAN，并配置各 VLAN 对应的 SVI。

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#interface gigabitEthernet 0/3
Ruijie(config-if-GigabitEthernet 0/3)#switchport access vlan 10
Ruijie(config-if-GigabitEthernet 0/3)#exit
Ruijie(config)#interface gigabitEthernet 0/4
Ruijie(config-if-GigabitEthernet 0/4)#switchport access vlan 20
Ruijie(config-if-GigabitEthernet 0/4)#exit
Ruijie(config)#interface vlan 10
Ruijie(config-if-VLAN 10)#ip address 192.168.10.1 255.255.255.0
Ruijie(config-if-VLAN 10)#exit
Ruijie(config)#interface vlan 20
Ruijie(config-if-VLAN 20)#ip address 192.168.20.1 255.255.255.0
Ruijie(config-if-VLAN 20)#exit
```

！配置 DHCP Server 和 SAM Server 的接口地址。

```
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#no switchport
Ruijie(config-if-GigabitEthernet 0/1)#ip address 10.1.1.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/1)#exit
Ruijie(config)#interface gigabitEthernet 0/2
Ruijie(config-if-GigabitEthernet 0/2)#no switchport
Ruijie(config-if-GigabitEthernet 0/2)#ip address 10.1.2.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/2)#exit
```

第二步，配置 DHCP Relay 相关功能。

！配置 DHCP Server 的地址为 10.1.1.2/24，并开启 DHCP 服务。

```
Ruijie(config)#ip helper-address 10.1.1.2
Ruijie(config)#service dhcp
```

！开启 DHPC Option dot1x 功能。

```
Ruijie(config)#ip dhcp relay information option dot1x
```

第三步，配置 802.1X 相关功能。

！开启 AAA，指定 Radius Server 的地址为 10.1.2.2/24，配置 Radius Key 为“ruijie”。

```
Ruijie(config)#aaa new-model
Ruijie(config)#radius-server host 10.1.2.2
```

```
Ruijie(config)#radius-server key ruijie
```

！创建 Dot1x 认证方法列表“d1x”，并配置 Dot1x 应用该认证方法列表。

```
Ruijie(config)#aaa authentication dot1x d1x group radius
Ruijie(config)#dot1x authentication d1x
```

！配置用户端口 Gi 0/3 和 Gi 0/4 为受控口。

```
Ruijie(config)#interface range gigabitEthernet 0/3-4
Ruijie(config-if-range)#dot1x port-control auto
Ruijie(config-if-range)#exit
```

！配置 IP 授权模式为 DHCP Server。

```
Ruijie(config)#aaa authorization ip-auth-mode dhcp-server
```

验证结果

第一步，查看各设备的配置信息。

！Switch A 的配置

```
Ruijie#show running-config
!
aaa new-model
!
aaa authorization ip-auth-mode dhcp-server
aaa authentication dot1x d1x group radius
!
vlan 10
!
vlan 20
!
service dhcp
ip helper-address 10.1.1.2
!
ip dhcp relay information option dot1x
!
radius-server host 10.1.2.2
radius-server key ruijie
!
dot1x authentication d1x
interface GigabitEthernet 0/1
 no switchport
 no ip proxy-arp
 ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet 0/2
```

```
 no switchport
 no ip proxy-arp
 ip address 10.1.2.1 255.255.255.0
!
interface GigabitEthernet 0/3
 switchport access vlan 10
 dot1x port-control auto
!
interface GigabitEthernet 0/4
 switchport access vlan 20
 dot1x port-control auto
!
interface VLAN 10
 no ip proxy-arp
 ip address 192.168.10.1 255.255.255.0
!
interface VLAN 20
 no ip proxy-arp
 ip address 192.168.20.1 255.255.255.0
!
```

4 UDP-Helper

UDP-Helper 简介

UDP-Helper 的主要功能是实现 UDP 广播报文的中继转发。通过配置需要转发的目的服务器，它能将 UDP 广播报文转换成单播报文后发往指定的目的服务器，起到中继的作用。

使能 UDP-Helper 功能后，将对接收到的广播报文的目的 UDP 端口号进行判断，当这个目的 UDP 端口号与需要转发的端口号相匹配时，它将修改报文的目的 IP 地址为配置的目的服务器的 IP 地址，以单播的方式发送指定的目的服务器。

使能 UDP-Helper 功能后，默认对 69、53、37、137、138、49 端口的广播报文进行中继转发。

BOOTP/DHCP 广播报文的中继由 DHCP Relay 模块使用 UDP 端口 67、68 来实现，因此端口 67、68 不能配置成 UDP-Helper 中继端口。

4.1 配置UDP-Helper

4.1.1 缺省的 UDP-Helper 配置

属性	缺省值
中继转发功能	关闭
中继转发的 UDP 端口号	打开 UDP-Helper 功能后默认对 69、53、37、137、138、49 端口的 UDP 广播报文进行中继转发。
中继转发的目的服务器	没有配置

4.1.2 启动 UDP-Helper 的中继转发功能

命令	作用
Ruijie(config)# **udp-helper enable**	udp-helper enable 命令用来启动 UDP 广播报文的中继转发功能。缺省 UDP 广播报文的中继转发处于关闭状态

使用 **no udp-helper enable** 命令用来关闭 UDP 的中继转发功能。

缺省情况下中继转发功能处于关闭状态

启动 UDP 广播报文的中继转发功能，则默认对 69、53、37、137、138、49 的 UDP 端口的广播报文进行中继转发

当关闭 UDP 广播报文的中继转发功能后，所有已配置的 UDP 端口都被取消，包括默认端口

4.1.3 配置中继转发的目的服务器

命令	作用
Ruijie(config-if)# **ip helper-address** *ip-address*	配置 UDP 广播报文中继转发的目的服务器。缺省情况下没有配置中继转发的目的服务器。

使用 **no ip helper-address** 命令删除中继转发的目的服务器。

一个接口最多对应 20 个目的服务器

如果中继转发的目的服务器是在某指定接口上配置的，在启动 UDP-Helper 功能后，从该接口接收的指定 UDP 端口的广播报文，将以单播形式发送到该接口配置的目的服务器上

4.1.4 配置需要中继转发的 UDP 端口

命令	作用
Ruijie(config)# **ip forward-protocol udp** [*port*]	配置需要中继转发的 UDP 端口。 如果只指定了 UDP 参数，则默认对缺省的端口进行中继转发，否则根据需要进行配置。 使能 UDP-Helper 功能后，缺省对 69、53、37、137、138、49 端口的广播报文将进行中继转发

使用 **no ip forward-protocol udp** [*port*]命令关闭需要中继转发的 UDP 端口。

只有打开 UDP-Helper 的中继转发功能并配置了中继转发的目的服务器后，才能配置需要中继转发的 UDP 端口。否则，将会有错误提示信息。

当启动 UDP 中继转发功能后， 69、53、37、137、138、49 默认端口的广播 UDP 报文转发功能将会立即启动，不需要用户再配置。

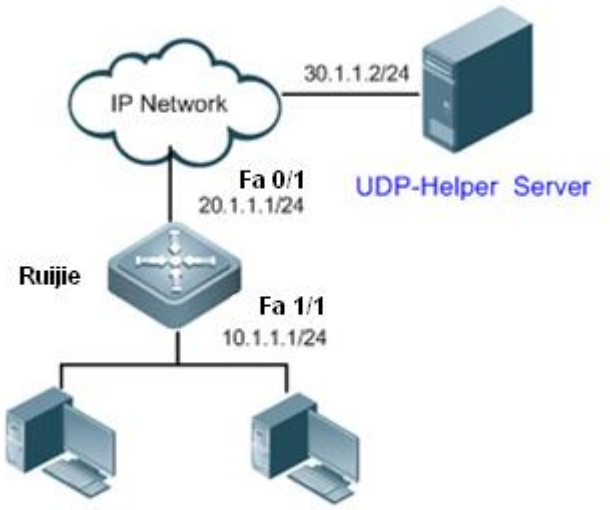
设备最多支持配置 256 个需要中继转发的 UDP 端口。

对默认端口的配置有两种方式，如 **ip forward-protocol udp domain** 和 **ip forward-protocol udp** *53* 的配置是相同的。

4.2 UDP-Helper配置举例

拓扑图

图 4-1 UDP-Helper 配置组网图



应用需求

要求网络设备能够将目的端口号为 1000 的 UDP 广播报文中继转发到指定的 UDP-Helper 服务器（服务器 IP 地址为 30.1.1.2/24）

配置要点

在设备上配置 UDP-Helper 中继转发功能步骤如下：

1) 使能 UDP-Helper 中继转发功能

2) 配置 UDP-Helper 中继转发的目的服务器

3) 配置需要中继转发的 UDP 广播报文的目的端口号（本例要求中继转发目的端口号为 1000 的 UDP 广播报文；此外，设备默认中继转发目的端口号为 69、53、37、137、138、49 的 UDP 广播报文）

只有打开 UDP-Helper 的中继转发功能并配置了中继转发的目的服务器后，才能配置需要中继转发的 UDP 端口。否则，将会有错误提示信息。

当启动 UDP 中继转发功能后， 69、53、37、137、138、49 默认端口的广播 UDP 报文转发功能将会立即启动，不需要用户再配置。

配置步骤

配置 UDP-Helper 相关功能之前，请先确保网络设备到 UDP-Helper 服务器所在网段的路由可达。接口 IP 配置如拓扑图所示。具体配置过程此处省略。下面介绍 UDP-Helper 功能相关配置。

第一步，在网络设备上开启 UDP-Helper 中继转发功能

```
Ruijie(config)#udp-helper enable
```

第二步，在 fastEthernet 1/1 上配置 UDP-Helper 中继转发的目的服务器的 IP 地址为 30.1.1.2

```
Ruijie(config)# interface fastEthernet 1/1
Ruijie(config-if-fastEthernet 1/1)# ip address 10.1.1.1 255.255.255.0
```

```
Ruijie(config-if-fastEthernet 1/1)# ip helper-address 30.1.1.2
Ruijie(config-if-fastEthernet 1/1)# exit
```

第三步，配置网络设备将目的端口号为 1000 的 UDP 广播报文进行中继转发

```
Ruijie(config)# ip forward-protocol udp 1000
```

配置验证

显示网络设备配置信息；关注点：中继转发功能开关、中继服务器 IP 地址、需要中继转发的 UDP 广播报文目的端口号。

```
Ruijie# show run
!
udp-helper enable
!
ip forward-protocol udp 1000
!
interface fastEthernet 0/1
ip address 20.1.1.1 255.255.255.0
!
interface fastEthernet 1/1
ip helper-address 30.1.1.2
 ip address 10.1.1.1 255.255.255.0
!
```

测试验证功能是否生效

第一步，发送目的端口号为 999 的 UDP 广播报文

PC1 发送 UDP 广播报文，报文格式为：

```
Src_mac:0000.0000.0001
Dst_mac:0xFFFFFFFFFFFF
Src_ip:1.0.0.3
Dst_ip:255.255.255.255
Dst_port:999
```

使用 PC2 充当 UDP-Helper 服务器，在 PC2 上未接收到该报文。

第二步，发送目的端口号为 1000 的 UDP 广播报文

PC1 发送 UDP 广播报文，报文格式为：

```
Src_mac:0000.0000.0001
Dst_mac:0xFFFFFFFFFFFF
Src_ip:1.0.0.3
Dst_ip:255.255.255.255
Dst_port:1000
```

使用 PC2 充当 UDP-Helper 服务器，在 PC2 上接收到报文。报文的目的 IP 地址为 30.1.1.2，且数据部分和发送的报文相同。

第三步，发送目的端口号为 69、53、37、137、138、49 的 UDP 广播报文

PC1 发送 UDP 广播报文，报文格式为（以目的端口号 69 为例）：

```
Src_mac:0000.0000.0001
Dst_mac:0xFFFFFFFFFFFF
Src_ip:1.0.0.3
Dst_ip:255.255.255.255
Dst_port:69
```

使用 PC2 充当 UDP-Helper，在 PC2 上接收到报文。报文的目的 IP 地址为 30.1.1.2，且数据部分和发送的报文相同。

从以上验证结果可以看出，网络设备成功将目的端口号为用户指定端口号（本例指定配置的目的端口号为 1000 和默认目的端口号 69、53、37、137、138、49）的 UDP 广播报文中继转发到指定的 UDP-Helper 服务器。

5 DHCPv6

5.1 DHCPv6 概述

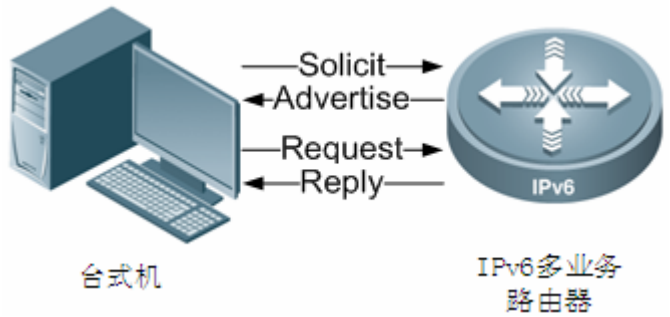
随着 IPv6 网络的发展，基于 IPv6 网络的应用范围也逐步广泛起来，作为 IPv6 在设计之初就提出的框架，网络节点的自动配置成为了 IPv6 网络的一个主要特点。在新的网络框架中，提出了无状态配置和有状态配置的概念。通过无状态自动配置，网络中新加入的节点可以通过路由通告(Router Advertisement)完成所有的配置。而在有状态自动配置中，网络节点需要通过和网络中的相关配置服务器交互完成地址以及其他参数的配置。DHCPv6 作为目前唯一提出的有状态配置模型，在 RFC3315 中进行了详细的描述。

RFC3315（Dynamic Host Configuration Protocol for IPv6，基于 IPv6 的动态主机配置协议）对 DHCPv6 的应用模型进行了比较完善的描述。类似 DHCPv4 中的框架，DHCPv6 应用模型由服务器、客户端和中继组成，客户端和服务器经过一问一答的方式，获取配置参数，中继可以将客户端和非本地链路内的服务器透明连接起来。报文的交互、参数的维护基本上维持了 DHCPv4 中的做法，但 DHCPv6 根据新的网络对报文结构和流程处理作了适当的处理。

在 IPv6 网络中，网络节点的自动配置分为两种：

- 无状态自动配置：网络节点从路由通告中获取配置参数。
- 有状态自动配置：网络节点通过 DHCPv6 服务器获取配置参数。

图 5-1 DHCPv6 有状态自动配置



在上图的描述中，新的网络节点[主机或者接口]在本地链路内发送一个到所有 DHCPv6 服务器和 DHCPv6 中继（地址：FF02::1:2 端口：547）的多播报文--Solicit，服务器收到该报文后会单播回应 Advertise 报文。客户端选择服务器之后，发送 Request 报文请求配置信息，服务器完成参数的分配后即回应 Reply 报文。

如上所述，这样一个 4 报文的交互非常类似 DHCPv4 中 4 报文交互（Discover-Offer-Request-Ack）。当然，在此基础上 DHCPv6 作了很多修改和扩展：

使用多播而不是广播，因为在 IPv6 的网络中广播已经被废除，取而代之的是多播；

通过特殊的选项（Rapid Commit，将 4 报文的交互精简为 2 报文的交互 Solicit-Reply；

新的报文结构，DHCPv6 对原有的 DHCPv4 报文作了很大的修改，去除了 DHCP 报文头中的可选参数，留下了少数的几个在所有交互中都要用到的字段，其他选填的字段一律通过选项的形式封装在报文的选项域中；在服务器/中继的交互中，客户端发送来的 DHCP 报文整个被当作一个选项封装在 Relay 的报文中发向服务器；

新的地址参数，如上描述，DHCPv6 中地址字段从 DHCP 的固定报文头中删掉，整个地址参数以及相关的时间参数被同一封装在一个叫做 IA（Identity Association）的选项中，每个 DHCPv6 客户端关联一个 IA，而每个 IA 中可以包含多个地址以及相关的时间信息；并且根据地址类型的不同生成对应的 IA，如 IA_NA（Identity association for non-temporary addresses，IA 中包含的地址是非临时地址）、IA_TA（Identity association for temporary addresses，IA 中包含的地址是临时地址）；

新的客户端服务端标识，被称之为 DUID（DHCP Unique IDentifier）；

无状态的 DHCPv6 自动配置，也就是说网络节点进行自动配置的时候，可以将地址配置和参数配置分开，对应的每一种配置都可以使用 DHCP 方式获取，也就是说网络节点可以通过 DHCPv6 服务器获取非地址的其他参数，这一点相对 DHCPv4 的分配方式是非常大的改变，相关信息在 RFC3736 中有详细描述；

基于前缀的分配，可以通过 DHCPv6 分配网络前缀，而不仅仅是 IPv6 的地址。这也归功于 DHCPv6 对 IA 的定义，只需要扩展 IA 的类型就可以将一个前缀以一个地址的形式（时间参数等）分配给客户端，这个新的 IA 类型我们称之为 IA_PD（Identity Association for Prefix Delegation），在 RFC3633 中有详细的描述。

5.1.1 DHCPv6 服务器

5.1.1.1 IPv6 地址分配方法

在 IPv6 网络中，长度为 128 位的 IPv6 地址通常使用 16 进制格式来书写，这个特性使得通过手工方式来进行地址分配变得困难，因为 IPv6 地址的格式并不符合人眼的直觉，所以 IPv6 地址的自动分配方式也成为了网络规划中的一个重要方面。为了促成在无人工干预或最小人工干预下进行地址分配，发展出许多应用于处理分配给 IPv6 主机的地址和参数配置的方法和技术。有如下几种不同的 IPv6 地址分配方法：

- 手工分配方法

通过手工分配方法静态配置 IPv6 地址，适合于配置路由接口和静态的网络参数。手工分配方法比较容易出错。

- 无状态的地址自动分配方法

无状态的地址自动分配（Stateless Address Autoconfiguration）是一种用于给 IPv6 节点分配地址的方法，不需要人工干预。如果对一个 IPv6 节点使用该方法，该节点必须通过网络与至少一台 IPv6 路由器连接。IPv6 路由器由管理员进行配置，并在链路上发送路由通告（Router Advertisement）信息。这些信息将被连接到路由器的 IPv6 节点收到，并由节点自行完成 IPv6 地址和路由参数的配置。

- 有状态的 DHCPv6 方法

RFC3315 所定义的 DHCPv6（Dynamic Host Configuration Protocol for IPv6）协议，支持 DHCP Server 发送诸如 IPv6 地址这样的配置参数给 IPv6 节点，该协议提供了灵活地添加和重复使用网络地址的功能。

- DHCPv6-PD 方法

RFC3633 所定义的 DHCPv6-PD（DHCPv6 Prefix Delegation）方法，是 DHCPv6 的一种扩展。在典型的 DHCPv6 方法中，DHCPv6 Server 分配有状态的 IPv6 地址给 DHCPv6 Client。作为一种扩展功能，DHCPv6-PD Server 可以通过分配前缀（Prefix Delegation）信息，分配一个完整的子网以及其他网络和接口参数给 DHCPv6-PD Client。

- 无状态的 DHCPv6 方法

无状态的 DHCPv6 方法结合了无状态的地址自动分配和有状态的 DHCPv6 两种方法的特点。设备可以使用无状态的地址自动分配方法获取 IPv6 地址，同时也可以利用 DHCPv6 去获取更多的参数。这些参数是无状态的地址自动分配方法无法提供的，设备可以利用这些信息来完成所有的配置。

网络规划中，上述 IPv6 地址和参数分配方法允许同时使用。

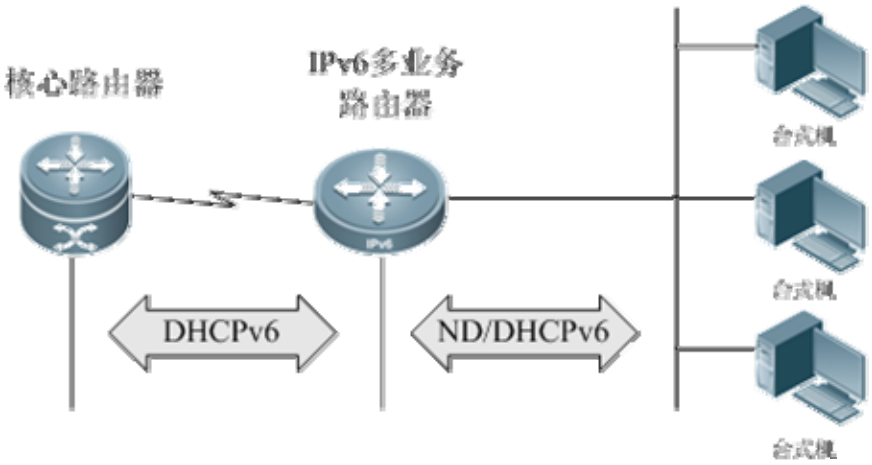
锐捷 DHCPv6 Server 支持分配 IPv6 地址和前缀，IPv6 地址的分配也就是为 DHCPv6 Client 自动分配 IPv6 地址。前缀的分配实现了灵活的站点级别的自动配置，可以灵活地控制站点地址空间。使得网络的终端设备，如 PC 可以结合无状态的自动配置或有状态的自动配置来实现地址和其他网络参数的自动配置。

锐捷 DHCPv6 Server 同时支持 DHCPv6-PD Server 扩展，以下统一称为 DHCPv6 Server。

5.1.1.2 DHCPv6 应用

DHCPv6 服务器实现了 IAPD 和 IANA 分配。IANA 的分配也就是为客户端自动分配 IPv6 地址，这与 DHCPv4 类似。IAPD 的分配则是实现了灵活的站点级自动配置，可以灵活地控制站点地址空间。而网络的终端设备，如 PC 可以通过无状态自动配置或有状态自动配置实现地址自动配置。

图 5-2 基于前缀的 DHCPv6 应用



上图描述当前基于前缀的 DHCPv6 在 IPv6 网络中的应用。

核心路由器运行基于前缀[PD]分配的 DHCPv6 server；

IPv6 多业务路由器在与核心路由器相连的接口上运行 DHCPv6 client，从核心路由器获取前缀空间，并将其保存在 IPv6 的全局前缀池中；

IPv6 多业务路由器在与台式机相连的接口上打开自动配置，运行基于接口的路由通告或者基于地址[NA]分配的 DHCPv6 server；

台式机通过 ND 的方式或者基于地址[NA]分配的 DHCPv6 client 的方式完成地址以及参数的配置。

在以上模型中，DHCPv6 完成如下功能：

客户端[主机、节点]在链路范围内发送基于前缀[PD]的多播请求[Solicit]，寻找 DHCPv6 服务器；

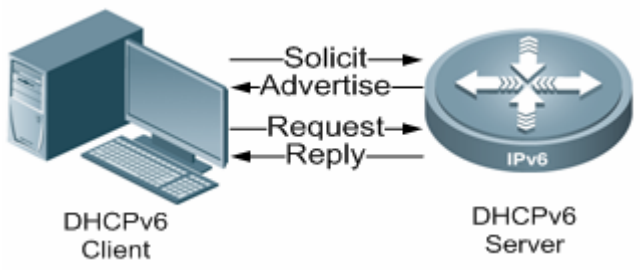
服务器收到请求之后，向主机发送单播[Advertise]报文；

客户端选择其中一台服务器，发送多播请求报文[Request]；

服务器发送单播确认报文[Reply]，完成地址分配。

在 IPv6 网络中，通过应用 DHCPv6，使用户终端能够自动获取 IPv6 地址及相关参数。

图 5-3 DHCPv6 交互过程



一次典型的 DHCPv6 交互过程：

1) DHCPv6 客户端发送一个目的地址为 FF02::1:2、目的 UDP 端口为 547 的 Solicit 报文，声明需要 DHCP 服务。本网段内所有的 DHCPv6 服务器都会接收此报文。

2) 每一个 DHCPv6 服务器在收到 Solicit 报文后，向 DHCPv6 客户端单播回复一个 Advertise 报文，声明可以为其提供 DHCP 服务。

3) DHCPv6 客户端从收到的 Advertise 报文中选择一个服务器，发送一个目的地址为 FF02::1:2、目的 UDP 端口为 547 的 Request 报文，声明自己做出的选择。本网段内所有的 DHCPv6 服务器都会接收此报文。

4) 被选中的 DHCPv6 服务器收到 Request 报文后，单播发送 Reply 报文，声明为 DHCPv6 客户端分配的 IP 地址等信息

FF02::1:2 用来标识同一网段中所有 DHCPv6 服务器和中继。

Solicit、Request 报文使用此地址作为目的地址，只在本网段内传播

5.1.1.3 DUID基本概念

DUID（DHCP Unique Identifier）即 DHCP 唯一标识。在 RFC3315 中明确定义，每一台 DHCPv6 设备（包括客户端、中继和服务器）都必须拥有一个 DHCPv6 唯一标识，并用于在设备之间交换 DHCPv6 消息时相互验证。此外，DUID 不能用在其他用途上。对于所有的 DHCPv6 设备，DUID 必须设计为不能重复的，并且对于任何设备本身都是稳定的（例如一个设备的 DUID 不会因为更换了某个部件而改变）。一个 DUID 长度不能超过 128 个字节，协议规定可以有三种类型的 DUID 定义：

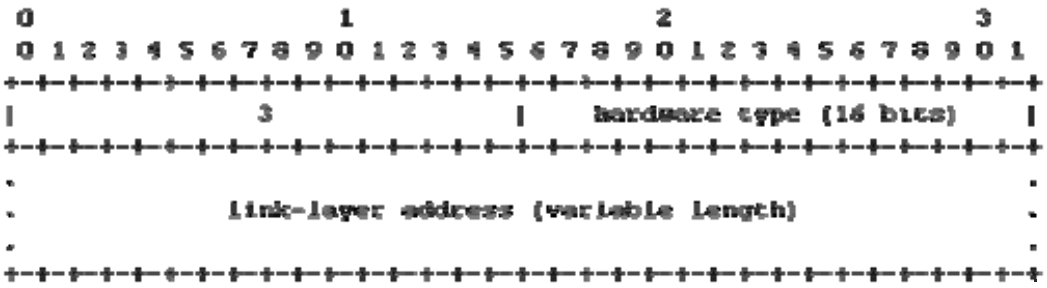
链路地址加时间（DUID Based on Link-Layer address plus Time，DUID-LLT）；

厂商的私有 ID 加企业内部编号（DUID Assigned by Vendor Based on Enterprise Number，DUID-EN）；

链路地址（Link-Layer address，DUID-LL）；

锐捷 DHCPv6 设备目前采用 DUID-LL 类型 DUID。DUID-LL 的结构如下：

图 5-4



其中，DUID type 为 DUID 类型，DUID-LL 类型取值为 0x0003；Hardware type 为硬件类型，设备支持的硬件类型为以太网，取值为 0x0001；Link layer address 为链路层地址，取值为设备的 MAC 地址。

5.1.1.4 DHCPv6 地址分配

与 DHCPv4 不同，在 DHCPv6 中 Server 分配给 Client 的不是单个的地址，而是一个地址集合（Identity association，IA），DHCPv6 Server 以 IA 为单位进行地址分配，每一个 IA 都由 IAID 唯一标识。IAID（Identity association identifier）由 DHCPv6 Client 生成。IA 与 Client 成一一对应关系，一个 IA 中可以包含多个地址，Client 可以将 IA 中的地址分配给设备上的其他接口。IA 中可以包含的地址有以下三类：

NA：Non-temporary Addresses，全球唯一地址；

TA：Temporary Addresses，临时地址（基本没有相关应用）；

PD：Prefix Delegation，前缀空间；

因此根据 IA 中包含的地址不同，IA 又分为 IA_NA、IA_TA、IA_PD 三种类型（IA-Type）。锐捷 DHCPv6 Server 支持分配 IA_NA 和 IA_PD，不支持 IA_TA。

5.1.1.5 DHCPv6 地址绑定

DHCPv6 的地址绑定（DHCPv6 Bindings）是一组可管理的地址信息结构，地址绑定基于地址集合（IA）之上，为 Server 和 Client 都可以识别。在 Server 上的地址绑定数据，记录着分配给每个 Client 的 IA 和其他配置信息。每个 Client 可以申请多个地址绑定，Server 上的地址绑定数据以地址绑定表的形式组织的，并以 DUID、IA-Type、IAID 为索引。

5.1.1.6 DHCPv6 报文类型

RFC3315 标准规定，DHCPv6 使用 UDP 546 和 547 端口进行报文交互，DHCPv6 Client 使用 546 端口上接收报文，DHCPv6 Server 和 Relay 在 547 端口上接收报文。RFC3315 定义 DHCPv6 Server/Client/Relay 之间可以收发的报文类型，如下：

Client 允许发送给 Server 的报文类型包括：Solicit、Request、Confirm、Renew、Rebind、Release、Decline、Information-request；

Server 允许发送给 Client 的报文类型包括：Advertise、Reply、Reconfigure；

Relay 允许发送给 Relay 或 Server 的报文类型包括：Relay-forward；

Server 或 Relay 允许发送给 Relay 的报文类型包括：Relay-reply；

Dhcp 交互时，有时为了简化交互流程，不是所有类型的报文都会使用，可以根据报文携带的 DHCPv6 选项灵活控制，而 Dhcp 数据也会根据选用不同的选项而变化。DHCPv6 的报文类型和作用与 DHCPv4 相似，虽然 DHCPv6 报文为新网络及流程做了改变，但是有些报文类型还是可以对应。以下为 DHCPv6 和 DHCPv4 的报文类型对照表：

DHCPv6 报文类型	DHCPv4 报文类型
Solicit (1)	DHCPDISCOVER
Advertise (2)	DHCPOFFER
Request (3), Renew (5), Rebind (6)	DHCPREQUEST
Reply (7)	DHCPACK / DHCPNAK
Release (8)	DHCPRELEASE
Information-request (11)	DHCPINFORM
Decline (9)	DHCPDECLINE
Confirm (4)	无
Reconfigure (10)	DHCPFORCERENEW
Relay-forward (12), Relay-reply (13)	无

锐捷 DHCPv6 Server 不支持 Reconfigure 报文类型。DHCPv4 相关的内容可以参见“DHCP 配置指南”章节。

5.1.1.7 DHCPv6 Server工作原理

DHCPv6 的应用模型基本延续了 DHCPv4 的框架，DHCPv6 应用模型由 Server、Client 和 Relay 组成，Client 和 Server 经过一问一答的方式，获取配置参数，Relay 可以将 Client 和非本地链路内的 Server 透明连接起来。报文的交互、参数的维护基本上维持了 DHCPv4 中的做法，但 DHCPv6 根据新的网络对报文结构和流程处理作了修改。DHCPv6 与 DHCPv4 相比：

DHCPv6 采用了新的报文结构，DHCPv6 对原有的 DHCPv4 报文作了很大的修改，去除了 DHCPv4 报文头部中的可选参数，留下了少数的几个在所有报文交互过程中都要用到的字段，其他选填的字段一律通过选项的形式封装在报文的选项域中。

DHCPv6 采用新的地址参数，如上描述，DHCPv6 中地址字段从 DHCPv4 的固定报文头部中删掉，整个地址参数以及相关的时间参数被同一封装在 IA 选项中，每个 DHCPv6 Client 关联一个 IA，而每个 IA 中可以包含多个地址以及相关的时间信息；并且根据地址类型的不同生成对应的 IA，如 IA_NA、IA_TA、IA_PD；

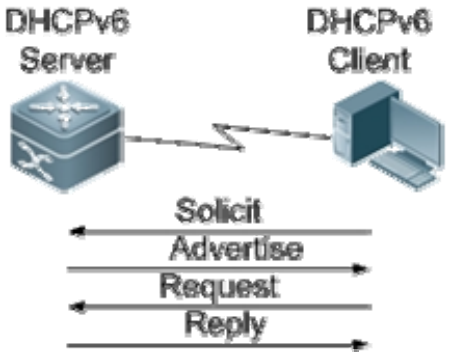
DHCPv6 引入新的客户端服务端标识，即 DUID；

DHCPv6 支持无状态的 DHCPv6 自动配置，也就是说网络节点进行自动配置的时候，可以将地址配置和参数配置分开，对应的每一种配置都可以使用 DHCP 方式获取，也就是说网络节点可以通过 DHCPv6 服务器获取非地址的其他参数，这一点相对 DHCPv4 的分配方式是非常大的改变；

DHCPv6 支持基于前缀的分配，可以通过 DHCPv6 分配网络前缀，而不仅仅是 IPv6 的地址；

DHCPv6 基本的应用模型。如下图所示：

图 5-5 典型的 DHCPv6 地址分配



上图是一次典型的 DHCPv6 地址分配过程：

1) DHCPv6 Client 在本地链路内发送一个目的地址为 FF02::1:2、目的 UDP 端口为 547 的多播 Solicit 请求报文，本地链路内所有的 DHCPv6 Server 和 DHCPv6 Relay 都会收到。

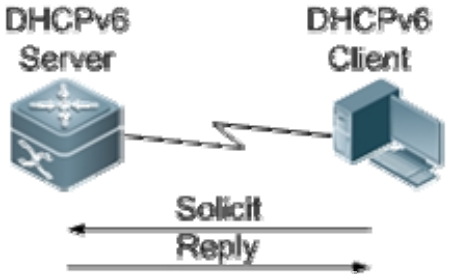
2) DHCPv6 Server 收到多播 Solicit 请求报文后，单播回应 Advertise 响应报文；

3) DHCPv6 Client 选择 Server 后，在本地链路内发送一个目的地址为 FF02::1:2、目的 UDP 端口为 547 的多播 Request 请求报文；

4) DHCPv6 Server 收到 Request 报文后，单播发送 Reply 响应报文，完成配置过程。

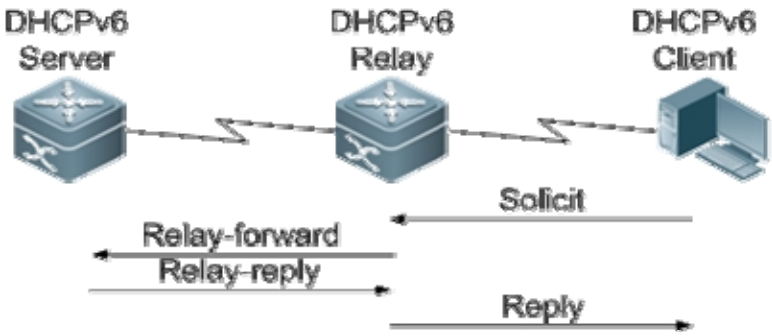
如上所述，这是一个 4 报文的 DHCPv6 交互，类似 DHCPv4 中 4 报文交互（Discover-Offer-Request-Ack）。如果通过特殊的选项（Rapid Commit），还可以将交互精简为 2 报文的交互（Solicit-Reply）。Client 在 Solicit 报文中添加该选项，服务器收到对应的报文之后，回应 Reply。如下图所示：

图 5-6 精简的 2 报文交互



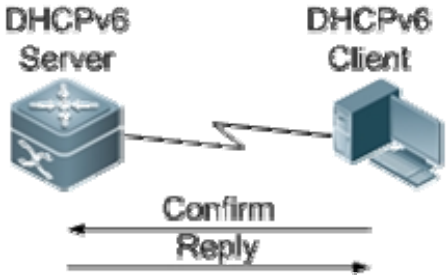
在 Server 和 Client 之间，可以引入 Relay，Relay 完成不同网段上的 Client、Server 之间的地址分配过程。Client 发送来的请求报文被整个地当作一个选项，封装在 Relay-forward 的报文中发向 Server。Server 解析出报文中请求信息，将应答消息封装在 Relay-reply 报文的 Relay 消息选项中，并将 Relay-reply 报文发送给 Relay。Relay 再解析出应答信息，并转给 Client。如下图所示：

图 5-7 Server、Relay 和 Client 之间的交互



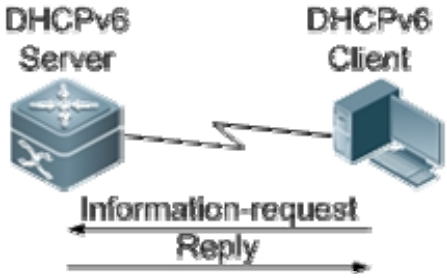
当 Client 的网络连接发生变化，Client 发送 Confirm 报文给 Server，询问 Server 之前分配的资源是否可用。Server 收到报文后，回应 Reply 报文。如下图所示：

图 5-8 Server 响应 Confirm 报文



如果 Client 使用无状态的地址配置，但是又通过 DHCP 的方式获取其它参数，此时 Client 发送 Information-request 报文给 Server。Server 收到报文后，将回应一个 Reply 报文。如下图所示：

图 5-9 Server 响应 Information-request 报文



5.1.1.8 协议规范

- DHCPv6 协议规范参见 RFC3315；
- DHCPv6-PD 协议规范参见 RFC3633。

5.1.2 DHCPv6 客户端

DHCPv6 客户端可以自动地从 DHCPv6 服务器获得前缀空间以及其它配置参数。客户端获取到前缀空间之后，将该前缀空间保存在 IPv6 的全局前缀空间内，这样这个前缀就可以通过前缀划分分配给其他接口，用来进行前缀通告等。

DHCPv6 的客户端是基于接口的，获取到的相关参数也是基于接口的，比如域名服务器，SNTP 服务器，在对应的接口网络协议不通时，相关的配置也会自动失效。

5.1.3 DHCPv6 中继代理

DHCPv6 中继代理在 DHCPv6 服务器和客户端之间转发 DHCPv6 数据包。当客户端与服务器不在同一个物理网络上，就必须有中继代理来转发 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，路由器一般不会修改 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 中继代理就象 DHCP 服务器；在 DHCP 服务器看来，DHCP 中继代理就像 DHCP 客户端。

5.1.3.1 DHCPv6 Relay Agent的作用

在 DHCPv6 Relay Agent 的帮助下，DHCPv6 服务器能够为其他网段的 DHCPv6 客户端提供服务；如果没有 DHCPv6 Relay Agent 的帮助，DHCPv6 服务器只能为属于同一网段的 DHCPv6 客户端提供服务。

图 5-10 DHCPv6 Relay Agent 的作用

DHCPv6 Relay Agent 的作用（对照图中标号）：

1）DHCPv6 中继（即：启用 DHCPv6 Relay Agent 的网关）能够接收 DHCPv6 客户端发往 DHCPv6 服务器的报文。

2）DHCPv6 中继将收到的（DHCPv6 客户端发往 DHCPv6 服务器的）报文封装在 Relay-Forward 报文中，单播发送给指定的 DHCPv6 服务器。

3）DHCPv6 服务器收到 Relay-Forward 报文后，能够将答复封装在 Relay-Reply 报文中，单播发送给 DHCPv6 中继。

4）DHCPv6 中继收到 Relay-Reply 报文后，还原出（DHCPv6 服务器发往 DHCPv6 客户端的）报文，单播发送给 DHCPv6 客户端

> 在 DHCPv6 客户端的地址续租、重新绑定、地址释放等过程中，以及服务器端的配置刷新等过程中，DHCPv6 Relay Agent 发挥了类型的作用。

5.1.3.2 协议规范

RFC3315 Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

5.2 配置DHCPv6

5.2.1 配置DHCPv6 Server

5.2.1.1 缺省配置

下表用来描述 DHCPv6 Server 的缺省配置。

功能特性	缺省值
DHCPv6 Server 功能	关闭
DHCPv6 配置信息池	未配置

5.2.1.2 配置DHCPv6 Server功能

这个任务阐述怎样创建并配置一个 DHCPv6 配置信息池，以及如何将这个池与接口上的 DHCPv6 Server 相关联。

配置步骤如下：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式
Ruijie(config)# **ipv6 dhcp pool** *poolname*	配置 DHCPv6 配置信息池并进入池配置模式
Ruijie(config-dhcp)#**domain-name** *domain*	配置一个可分配给 DHCPv6 客户端的 domain-name
Ruijie(config-dhcp)#**dns-server** *ipv6-address*	配置可提供给 DHCPv6 客户端的 DNS server
Ruijie(config-dhcp)#**prefix-delegation** *ipv6-prefix/prefix-length client-DUID* [*lifetime*]	配置可分配给某个特定的客户端 IAPD 的地址前缀
Ruijie(config-dhcp)#**prefix-delegation pool** *poolname* [**lifetime** {*valid-lifetime* | *preferred-lifetime*}]	为 DHCPv6 Server 配置一个前缀池，从该前缀池中可为客户端分配地址前缀
Ruijie(config-dhcp)#**iana-address prefix** *ipv6-prefix/prefix-length* [**lifetime** {*valid-lifetime* | *preferred-lifetime*}]	为 DHCPv6 Server 配置一个 IANA 地址前缀，从该前缀指定的地址范围中可为客户端分配 IANA 地址
Ruijie(config-dhcp)#**exit**	退出 DHCPv6 池配置模式
Ruijie(config)#**interface *type number***	进入接口配置模式
Ruijie(config-if)#**ipv6 dhcp server** *poolname* [*rapid-commit*] [**preference** *value*]	在接口上启用 DHCPv6 Server

举例：

配置一个名为 pool1 的配置信息池，并配置域名、DNS Server、IA_NA、IA_PD 等，然后在 FastEthernet 0/1 接口上打开 DHCPv6 Server 功能

```
Ruijie# configure terminal
Ruijie(config)# ipv6 local pool client-prefix-pool 2008:10::/64 78
```

```
Ruijie(config)# ipv6 dhcp pool pool1
Ruijie(config-dhcp)# domain-name example.com
Ruijie(config-dhcp)# dns-server 2008:1::1
Ruijie(config-dhcp)# prefix-delegation 2008:2::/64
0003000100d0f82233ac
Ruijie(config-dhcp)# prefix-delegation pool client-prefix-pool lifetime 2000 1000
Ruijie(config-dhcp)# iana-address prefix 2008:50::/64
Ruijie(config-dhcp)# exit
Ruijie(config)# interface fastethernet 0/1
Ruijie(config-if)# ipv6 dhcp server pool1
```

DHCPv6 Server 不支持为客户端分配网关地址，需要在设备上开启 RA 通告功能 Ruijie(config-if)# **no ipv6 nd suppress-ra**

同时需要设置路由器公告(RA)报文中的“managed address configuration”标志位，决定了收到该路由器公告的主机是否要使用有状态自动配置来获取地址。缺省配置是在路由器公告报文中该标志位没有被设置：

Ruijie(config-if)# **ipv6 nd managed-config-flag**

设置路由器公告报文中的“other stateful configuration”标志位，决定了收到该路由器公告的主机是否要使用有状态的自动配置来获取除地址之外的信息。缺省配置是在路由器公告报文中该标志位没有被设置 Ruijie(config-if)# **ipv6 nd other-config-flag**

最后关闭前缀通告功能：Ruijie(config-if)# **ipv6 nd prefix** *ipv6-prefix/prefix-length* **no-advertise**

5.2.1.3 配置无状态DHCPv6 Server功能

无状态的 DHCPv6 Server 不需要配置前缀池，Client 通过 RA 通告已经获得了地址，Server 向 Client 提供除了地址以外的配置信息。配置步骤如下：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **ipv6 dhcp pool** *poolname*	配置 DHCPv6 配置信息池，并进入池配置模式。
Ruijie(config-dhcp)# **domain-name** *domain*	配置一个可分配给 DHCPv6 Client 的 domain-name。
Ruijie(config-dhcp)# **dns-server** *ipv6-address*	配置可提供给 DHCPv6 Client 的 DNS Server。
Ruijie(config-dhcp)# **exit**	退出 DHCPv6 池配置模式。
Ruijie(config)# **interface** *interface-name*	进入接口配置模式。
Ruijie(config-if)# **ipv6 dhcp server** *poolname* [**rapid-commit**] [**preference** *value*]	在接口上启用 DHCPv6 Server。
Ruijie(config-if)# **ipv6 nd other-config-flag**	设置 IPv6 RA 中的“other stateful configuration”标志位。

配置举例：

配置一个名为 pool1 的配置信息池，并配置域名、DNS Server 等，然后在 FastEthernet 0/1 接口上打开 DHCPv6 Server 功能，并设置 IPv6 RA 中的标志位：

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# ipv6 dhcp pool pool1
Ruijie(config-dhcp)# domain-name example.com
Ruijie(config-dhcp)# dns-server 2008:1::1
Ruijie(config-dhcp)# exit
Ruijie(config)# interface fastethernet 0/1
Ruijie(config-if)# ipv6 dhcp server pool1
Ruijie(config-if)# ipv6 nd other-config-flag
```

DHCPv6 Server 不支持为客户端分配网关地址，需要在设备上开启 RA 通告功能 Ruijie(config-if)# **no ipv6 nd suppress-ra**

5.2.1.4 查看DHCPv6 Server配置

要查看 DHCPv6 Server 的配置和状态信息，可以使用以下命令：

命令	作用
show ipv6 dhcp	显示设备的 DUID 信息。
show ipv6 dhcp binding	显示 DHCPv6 服务器的地址绑定信息。
show ipv6 dhcp conflict	显示 DHCPv6 服务器的冲突地址信息。
show ipv6 dhcp interface	显示 DHCPv6 接口信息。
show ipv6 dhcp pool	显示 DHCPv6 池信息。
show ipv6 dhcp server statistics	显示 DHCPv6 统计信息

查看配置举例：

```
Ruijie# show ipv6 dhcp
This device's DHCPv6 unique identifier(DUID): 00:03:00:01:00:d0:f8:22:33:b0

Ruijie# show ipv6 dhcp binding
Client  DUID: 00:03:00:01:00:d0:f8:22:33:ac
  IAPD: iaid 0, T1 1800, T2 2880
    Prefix: 2001:20::/72
            preferred lifetime 3600, valid lifetime 3600
        expires at Jan 1 2008 2:23 (3600 seconds)

Ruijie# show ipv6 dhcp interface
VLAN 1 is in server mode
  Server pool dhcp-pool
  Rapid-Commit: disable

Ruijie# show ipv6 dhcp pool
```

```
DHCPv6 pool: dhcp-pool
  DNS server: 2011:1::1
  DNS server: 2011:1::2
  Domain name: example.com

Ruijie# show ipv6 dhcp server static
DHCPv6 server statistics:

Packet statistics:
DHCPv6 packets received:            7
Solicit received:                   7
Request received:                   0
Confirm received:                   0
Renew received:                     0
Rebind received:                    0
Release received:                   0
Decline received:                   0
Relay-forward received:             0
Information-request received:       0
Unknown message type received:      0
Error message received:             0

DHCPv6 packet sent:                 0
Advertise sent:                     0
Reply sent:                         0
Relay-reply sent:                   0
Send reply error:                   0
Send packet error:                  0

Binding statistics:
Bindings generated:                 0
IAPD assigned:                      0
IANA assigned:                      0

Configuration statistics:
DHCPv6 server interface:            1
DHCPv6 pool:                        0
DHCPv6 iapd binding:                0
```

5.2.2 配置DHCPv6 Client

这个任务阐述怎样在接口上启用 DHCPv6 客户端功能，以及启用前缀请求。

配置步骤如下：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式
Ruijie (config)# **interface** *type number*	进入接口配置模式
Ruijie(config-if)#**ipv6 dhcp client pd** *prefix-name* [*rapid-commit*]	在接口上启用 DHCPv6 Client，并在接口上启用了前缀请求。

举例：

```
Ruijie# configure terminal
Ruijie(config)# interface fastethernet 0/1
Ruijie(config-if)# ipv6 dhcp client pd pd_name
```

5.2.2.1 配置无状态DHCPv6 Client

配置步骤如下：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式
Ruijie(config)# **interface** *type number*	进入接口配置模式
Ruijie(config-if)# **ipv6 enable**	在接口上启用 IPv6 功能

举例:

```
Ruijie# configure terminal
Ruijie(config)# interface fastethernet 0/1
Ruijie(config-if)# ipv6 enable
```

5.2.2.2 在接口上重新启动DHCPv6 Client

这个任务阐述怎样在接口上重新启动 DHCPv6 Client。

配置步骤如下：

命令	作用
Ruijie#**clear ipv6 dhcp client** *interface-type interface-number*	在接口上重新启动 DHCPv6 Client

举例：

```
Ruijie# clear ipv6 dhcp client fastethernet 0/1
```

5.2.3 配置DHCPv6 Relay Agent

5.2.3.1 缺省配置

功能特性	缺省值
DHCPv6 Relay Agent 功能	关闭
DHCPv6 Relay Agent 服务器地址	未指定

5.2.3.2 配置DHCPv6 Relay功能

这个任务阐述怎样在接口上启用 DHCPv6 Relay 功能，以及配置 Relay 转发地址。

配置步骤如下：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式
Ruijie(config)# **interface** *type number*	进入接口配置模式
Ruijie(config-if)#**ipv6 dhcp relay destination** *ipv6-address* [*interface-type interface-number*]	在接口上启用 DHCPv6 Relay，并指定 Relay 的转发地址。
Ruijie(config-if)# **end**	退出接口模式。

采用如下命令查看 DHCPv6 Relay 目的地址：

```
show ipv6 dhcp relay destination { all | interface interface-type interface-number }
```

采用如下命令删除 DHCPv6 Relay 目的地址：

```
no ipv6 dhcp relay destination ipv6-address [ interface-type interface-number ]
```

举例：在接口 VLAN 1 上开启 DHCPv6 Relay Agent 功能，目的地址 3001::2。

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#interface vlan 1
Ruijie(config-if)#ipv6 dhcp relay destination 3001::2
Ruijie(config-if)#end
```

- IPv6 DHCP Relay Destination 命令只能在三层接口上启用;
- 一台设备允许同时配置多个 Relay Agent Destination（最多 20 个）;
- 当 Destination 配置的是组播地址的时候，后面必须指定出接口编号。

5.2.3.3 查看/清除DHCPv6 Relay 信息

命令	作用
show ipv6 dhcp relay destination { all | interface *interface-type interface-number* }	查看 DHCPv6 Relay 目的地址
show ipv6 dhcp relay statistics	查看 DHCPv6 Relay Agent 报文统计信息。
clear ipv6 dhcp relay statistics	清除 DHCPv6 Relay Agent 报文统计信息

举例：查看 DHCPv6 Relay 目的地址。

```
Ruijie# show ipv6 dhcp relay destination all
Interface: Vlan1
Destination address(es)           Output Interface
3001::2
```

举例：查看 DHCPv6 Relay Agent 统计信息。

```
Ruijie# show ipv6 dhcp relay statistics
Packets dropped               :  2
    Error                     :  2
    Excess of rate limit      :  0
Packets received              :  28
    SOLICIT                   :  0
    REQUEST                   :  0
    CONFIRM                   :  0
    RENEW                     :  0
    REBIND                    :  0
    RELEASE                   :  0
    DECLINE                   :  0
    INFORMATION-REQUEST       :  14
    RELAY-FORWARD             :  0
    RELAY-REPLY               :  14
Packets sent                  :  16
    ADVERTISE                 :  0
    RECONFIGURE               :  0
    REPLY                     :  8
    RELAY-FORWARD             :  8
    RELAY-REPLY               :  0
```

5.3 典型配置举例

5.3.1 DHCPv6 Server典型配置举例

组网需求

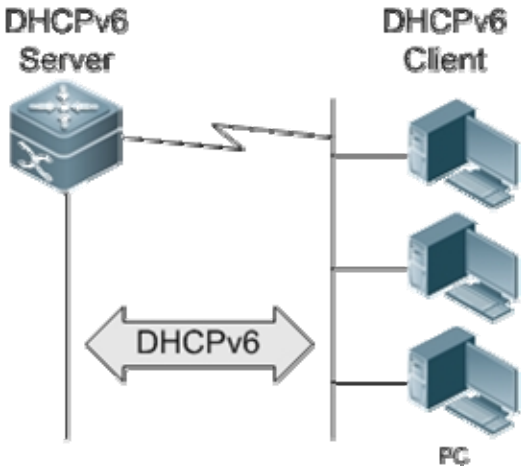
用户环境中，最常见的是在网络核心或汇聚位置部署 DHCPv6 Server，用来分配和管理整个子网的 IP 地址分配。

组网拓扑

如下图，在汇聚设备上开启 DHCPv6 Server 功能，为子网中的 PC 分配 IPv6 地址和其他网络配置信息。在 Server 上配置了可供分配的 IA_NA 地址范围，当 PC 请求地址分配时，Server 收到该请求后从 IA_NA 地址范围中计算出一个可用的地址

分配给 PC。同时，Server 也提供 DNS Server 地址以及域名等信息。另外，要保证 DHCPv6 Server 功能生效，在开启 Server 功能的三层接口上，还需要配置与 IA_NA 处于同一网段的 IP 地址：

图 5-11 DHCPv6 Server 组网拓扑图



配置要点

如果核心设备作为 DHCPv6 Server，可能会增加该设备的 CPU 和内存占用率，当 Client 数量增加时，同时也会增加对 Server 的压力。因此，DHCPv6 Server 尽量采用高性能的设备充当，或采用单独的设备作为 DHCPv6 Server。

配置步骤

汇聚网关设备上启用 DHCPv6 Server 功能：

配置一个名为 pool1 的配置信息池，并配置域名、DNS Server、IA_NA 等，然后在 vlan 1 接口上打开 DHCPv6 Server 功能：

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# ipv6 dhcp pool pool1
Ruijie(config-dhcp)# domain-name example.com
Ruijie(config-dhcp)# dns-server 2008:1::1
Ruijie(config-dhcp)# iana-address prefix 2008:50::/64
Ruijie(config-dhcp)# exit
Ruijie(config)# interface vlan 1
Ruijie(config-if)# ipv6 address 2008:50::1/64
Ruijie(config-if)# ipv6 dhcp server pool1
Ruijie(config-if)# no ipv6 nd suppress-ra
Ruijie(config-if)# ipv6 nd managed-config-flag
Ruijie(config-if)# ipv6 nd other-config-flag
Ruijie(config-if)# ipv6 nd prefix 2008:50::/64 no-advertise
```

显示验证

显示汇聚网关设备上 DHCPv6 Server 的配置状况：

```
Ruijie# show ipv6 dhcp interface
VLAN 1 is in server mode
  Server pool pool1
  Rapid-Commit: disable

Ruijie# show ipv6 dhcp pool
DHCPv6 pool: pool1
  DNS server: 2008:1::1
  Domain name: example.com

Ruijie# show ipv6 dhcp server statistics
DHCPv6 server statistics:

Packet statistics:
DHCPv6 packets received:            7
Solicit received:                   7
Request received:                   0
Confirm received:                   0
Renew received:                     0
Rebind received:                    0
Release received:                   0
Decline received:                   0
Relay-forward received:             0
Information-request received:       0
Unknown message type received:      0
Error message received:             0

DHCPv6 packet sent:                 0
Advertise sent:                     0
Reply sent:                         0
Relay-reply sent:                   0
Send reply error:                   0
Send packet error:                  0

Binding statistics:
Bindings generated:                 0
IAPD assigned:                      0
IANA assigned:                      0

Configuration statistics:
DHCPv6 server interface:            1
DHCPv6 pool:                        0
DHCPv6 iapd binding:                0
```

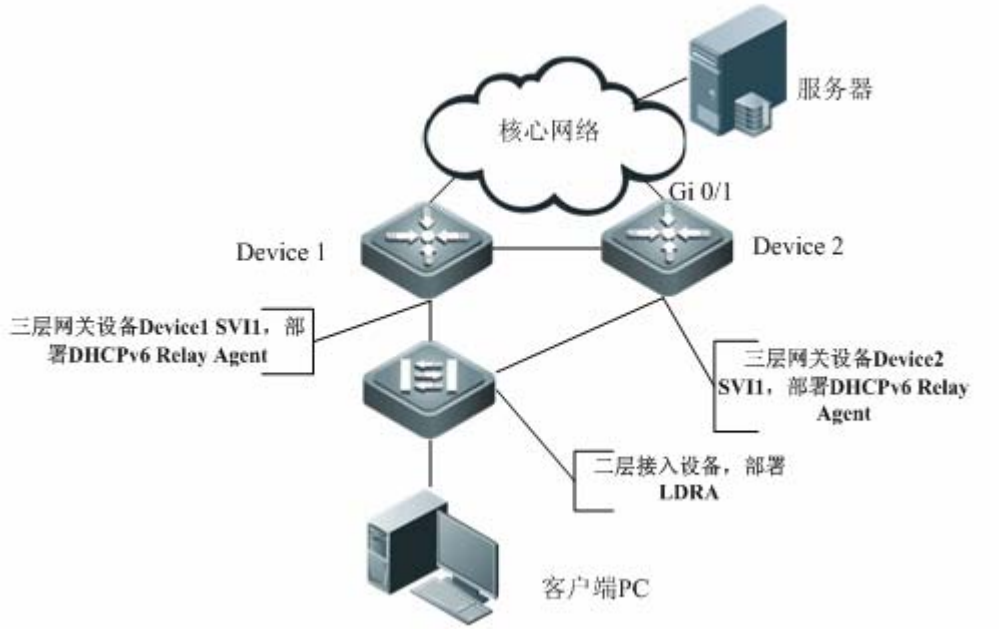
5.3.2 DHCPv6 Relay 典型配置举例

组网需求

Device1 开启 DHCPv6 Relay Agent 并且目的地址指向 3001::2；Device2 希望通过下一级 Relay 继续处理转到其他服务器，所以开启 DHCPv6 Relay Agent 并且目的地址指向 FF02::1:2（所有服务器和 Relay 组播地址），出接口指定为上联目标地址的三层接口为 gi 0/1。

组网拓扑

图 5-12DHCPv6 Relay Agent 组网拓扑图



配置要点

在网关上启用 DHCPv6 Relay Agent 功能，将 Destination 指向已知的服务器地址或者下一级 Relay 地址。

配置步骤

- 汇聚网关设备 Device1 上启用 DHCPv6 Relay Agent 功能并指定目的地址 3001::2：

```
Ruijie#config
Enter configuration commands, one per line.  End with CNTL/Z
Ruijie(config)#interface vlan 1
Ruijie(config-if)# ipv6 dhcp relay destination 3001::2
```

- 汇聚网关设备 Device2 上启用 DHCPv6 Relay Agent 功能并指定目的地址 FF02::1:2：

```
Ruijie#config
Enter configuration commands, one per line.  End with CNTL/Z
```

```
Ruijie(config)#interface vlan 1
Ruijie(config-if)#ipv6 dhcp relay destination FF02::1:2 interface gi 0/1
```

检查配置效果

- 显示汇聚 Device 1 上 DHCPv6 Relay Agent 配置状况

```
Ruijie# show ipv6 dhcp relay destination all
Interface: Interface vlan 1
Server address(es)                              Output Interface
3001：：2
```

- 显示汇聚 Device 2 上 DHCPv6 Relay Agent 配置状况

```
Ruijie# show ipv6 dhcp relay destination all
Interface: Interface vlan 1
Server address(es)                              Output Interface
FF02::1:2                                         gi0/1
```

6 DNS

6.1 DNS概述

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，每台设备上都配置主机到 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。

6.2 配置域名解析

6.2.1 缺省的 DNS 配置

DNS 的缺省配置如下表：

功能特性	缺省值
DNS 域名解析功能开关	打开
DNS 服务器 IP 地址	空
静态主机列表	空
DNS 服务器最大个数	6

6.2.2 打开 DNS 域名解析服务

本节描述如何打开 DNS 域名解析功能开关。

命令	作用
Ruijie(config)# **ip domain-lookup**	打开 DNS 域名解析功能开关

使用 **no ip domain-lookup** 命令关闭 DNS 域名解析的功能

```
Ruijie(config)# ip domain-lookup
```

6.2.3 配置 DNS Server

本节描述如何配置 DNS 服务器。只有配置了 DNS 服务器，才能进行动态域名解析。

您如果要删除 DNS 服务器，可以使用 **no ip name-server** [*ip-address* | *ipv6-address*] 命令。其中参数 **ip-address** 和 **ipv6-address** 表示删除指定的域名服务器，否则删除所有的域名服务器。

命令	作用
Ruijie(config)# **ip name-server** {*ip-address* | *ipv6-address*}	添加 DNS Server 的 IP/IPV6 地址。每次执行这条命令，设备都会添加一个 DNS Server。当无法从第一个 Server 获取到域名时，设备会尝试向后续几个 Server 发送 DNS 请求，直到正确收到回应为止。 系统最多支持 6 个域名服务器。

6.2.4 静态配置主机名和 IP/IPV6 地址的映射

本节描述如何配置主机名和 IP/IPV6 地址的映射。本地维护了一张主机名和 IP/IPV6 地址的对应表，也叫主机名到 IP/IPv6 地址的映射表。主机名到 IP/IPV6 地址的映射表内容有两个来源：手工配置和动态学习。在不能动态学习的情况下，手工配置就有必要了。

命令	作用
Ruijie(config)# **ip host *host-name*** *ip-address*	手工配置主机名和 IP 地址映射
Ruijie(config)# **ipv6 host *host-name*** *ipv6-address*	手工配置主机名和 IPV6 地址映射

使用该命令的 **no** 形式就可以删除主机名和 IP/IPV6 地址的映射。

6.2.5 清除动态主机名缓存表

本节描述如何清除动态主机名缓存表。如果输入 **clear host** 或 **clear host *** 命令将清除动态缓存表。否则只删除指定域名的表项。

命令	作用
Ruijie# **clear host** [*host-name*]	清除动态主机名缓存表。 该命令不能删除静态配置的主机名。

6.2.6 域名解析信息显示

本节描述如何显示 DNS 的相关配置信息：

命令	作用
show hosts [*host-name*]	查看 DNS 的相关参数

```
Ruijie# show hosts
```

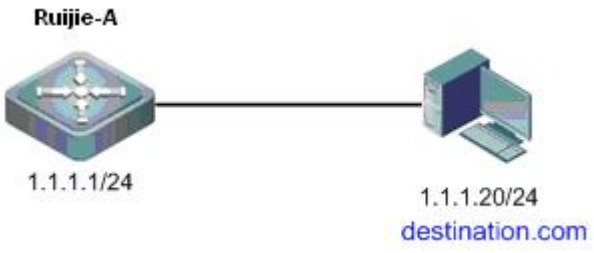
```
Name servers are:
192.168.5.134  static

Host                    type        Address            TTL(sec)
www.163.com           static     192.168.5.243     ---
```

6.3 DNS典型配置举例

6.3.1 静态域名解析配置举例

拓扑图

图 6-1 静态域名解析配置组网图



应用需求

由于网络设备 Ruijie-A 经常访问域名为 destination.com 的主机，可利用静态域名解析功能，实现通过 destination.com 主机名访问 IP 地址为 1.1.1.20 的主机，提高域名解析的效率。

配置要点

1) 确保设备和主机间路由可达

2) 主机名和 IP 地址间的映射正确

配置步骤

手工配置主机名和 IP 地址间的映射；本例中，配置主机名为 destination.com 其对应 IP 地址为 1.1.1.20

```
Ruijie-A(config)#ip host destination.com 1.1.1.20
```

配置验证

第一步，查看域名解析信息；关注点主机、IP 地址间的映射关系是否正确。

```
Ruijie-A# show host
Name servers are:
Host                  type    Address                    TTL(sec)
destination.com    static  1.1.1.20                   ---
```

第二步，使用 **ping** *destination.com* 命令，查看执行结果。

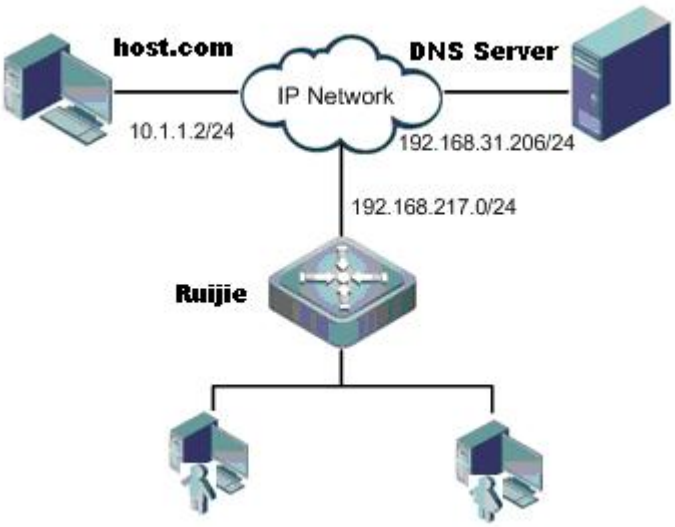
```
Ruijie-A# ping destination.com
Translating "destination.com"...[OK]
Sending 5, 100-byte ICMP Echoes to 1.1.1.20, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

从以上显示信息可以看出，Ruijie-A 通过静态域名解析，成功实现通过 destination.com 主机名访问 IP 地址为 1.1.1.20 的主机。

6.3.2 动态域名解析配置举例

拓扑图

图 6-2 动态域名解析配置组网图



应用需求

- DNS 域名服务器的 IP 地址为 192.168.31.206/24。
- 网络设备为 DNS 客户端，通过动态域名解析功能，实现通过 host.com 主机名访问 IP 地址为 10.1.1.2 的主机。

配置要点

1) DNS 客户端和 DNS 服务器端、访问主机间的路由要可达

2) DNS 域名解析开关打开。域名解析功能开关默认开启。

3) 正确配置 DNS 域名服务器的 IP 地址

配置步骤

第一步，配置 DNS 域名服务器

不同域名服务器的配置方法不同，请根据实际情况搭建 DNS 服务器。具体方法在此不做具体说明。

在 DNS 服务器上添加主机和 IP 地址的映射。本例中，设置主机名：host.com；IP 地址为 10.1.1.2/24

第二步，配置 DNS 客户端

DNS 客户端和 DNS 服务器端、访问主机间的路由要可达。接口 IP 配置如拓扑图所示。具体配置过程此处省略。

！打开 DNS 域名解析功能开关；该功能默认开启

```
Ruijie(config)#ip domain-lookup
```

！配置域名服务器的 IP 地址为 192.168.31.206

```
Ruijie(config)#ip name-server 192.168.31.206
```

配置验证

第一步，使用 **ping** *host.com* 命令，查看执行结果。

```
Ruijie# ping host.com
Translating " host.com "...[OK]
Sending 5, 100-byte ICMP Echoes to 10.1.1.2, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

从以上显示信息可以看出，客户端设备能 ping 通主机，且对应的目的 IP 地址为 10.1.1.2。设备通过动态域名解析，成功实现通过 host.com 主机名访问 IP 地址为 10.1.1.2 的主机。

第二步，查看域名解析信息；关注点主机名、主机 IP 地址。

```
Ruijie# show host
Name servers are:
192.168.31.206 static
Host                    type        Address           TTL(sec)
host.com              dynamic      10.1.1.2           3503
```

从以上显示信息可以看出，主机名同主机 IP 地址的映射表项正确。

7 FTP Server

7.1 概述

FTP Server 功能可以将一台设备配置为 FTP 服务器。这样可以通过 FTP 客户端与之连接，通过 FTP 协议往设备上传或下载文件。

用户可以利用 FTP Server 功能方便地获取设备中的文件，如 syslog 日志文件等；也可以通过 FTP 直接往设备的文件系统拷贝文件。

7.1.1 支持的 FTP 命令

当设备收到 FTP 连接请求时， FTP 服务器将要求客户端提供登录用户名和密码以进行身份认证。

如果客户端通过身份认证，即可执行 FTP 客户端命令进行操作。目前的 FTP 服务器并没有支持所有的 FTP 命令，具体支持的 FTP 客户端命令如下：

ascii	delete	mdelete	mput	quit	send
bin	dir	mdir	nlist	recv	size
bye	disconnection	mget	open	rename	system
cd	get	mkdir	passive	rhelp	type
cdup	image	mls	put	rmdir	user
close	ls	modtime	pwd	rstatus	

以上 FTP 客户端命令的用法请参考您所使用的 FTP 客户端软件的文档。另外不少 FTP 客户端工具（如 CuteFTP、FlashFXP 等）均提供了图形化的操作界面，使用此类工具可以无需再通过 FTP 命令进行操作。

7.2 配置FTP服务器

7.2.1 启用/关闭 FTP 服务器

FTP 服务器功能在缺省情况下是关闭的，故如果要使用此功能必须通过全局配置模式下的 **ftp-server enable** 启动 FTP 服务器。但是请注意：在正确配置服务器的顶层目录、登录用户名和密码之前客户端仍然无法访问 FTP 服务器。因此建议在首次启动服务之前先参考后面的章节完成服务器顶层目录、登录用户名与密码的配置。

如果需要关闭 FTP 服务功能，使用全局配置模式下的 **no ftp-server enable** 命令即可停止 FTP 服务。

命令	作用
Ruijie(config)# **ftp-server enable**	启动 FTP 服务器
Ruijie(config)# **no ftp-server enable**	关闭 FTP 服务器

在当前的实现中 FTP 服务器在同一时间仅能允许一个客户登录。在当前正在服务的客户端断开连接之前其余客户端均无法连上 FTP 服务器。

7.2.2 配置服务器顶层目录

配置 FTP 服务器顶层目录可以限制 FTP 客户端的访问范围（关于如何查看及管理当前设备上的目录请参考《文件系统配置指南》的描述）。如：可以指定服务器的顶层目录为“/syslog”目录，则 FTP 客户端登录后将仅能访问设备上“/syslog”目录下的文件和文件夹。

可以用全局配置模式下的 **ftp-server topdir** 命令配置服务器的顶层目录，该命令的 **no** 形式功能为清除顶层目录设置，这样将彻底禁止客户端访问服务器上的任何文件。

命令	作用
Ruijie(config)# **ftp-server topdir** *directory*	配置 FTP 服务器的顶层目录
Ruijie(config)# **no ftp-server topdir**	清除 FTP 服务器顶层目录配置，禁止客户端访问服务器上任何文件。

假设当前设备的日志文件均存储于设备的“/syslog”目录下。若希望通过管理 PC 上的 FTP 客户端直接从设备上下载日志文件，但又不允许 FTP 客户端访问到“/syslog”目录以外的文件，可以如下配置服务器顶层目录：

```
Ruijie(config)# ftp-server topdir /syslog
```

如上配置后 FTP 客户端登录后将仅能访问到设备上“/syslog”目录下的文件和子目录。客户端由于顶层目录的限制将无法退到“/syslog”目录的上级目录中。

7.2.3 配置会话空闲时限

当前 FTP 服务器不支持并发连接。如果用户登录到 FTP 服务器与服务器建立了连接，一旦某连接异常中断或用户非正常中断连接，FTP 服务器可能无法知道用户断开而将继续保持连接，导致与服务器的连接被长期占用使服务器无法响应其他用户的登录请求。

配置会话空闲时限（Session idle timeout）可以防止这类情况的发生。当 FTP 服务器与某用户的连接在一定时间内没有进行命令交互后，FTP 服务器即可认为连接已经失效而自动断开与该用户的连接。系统缺省的会话空闲时限为 30 分钟。

通过全局配置模式下的 **ftp-server timeout** 命令可以配置会话空闲时限。

命令	作用
Ruijie(config)# **ftp-server timeout** *time*	配置 FTP 会话的空闲时限，time 为配置的空闲时限（单位：分钟；范围：1-3600）
Ruijie(config)# **no ftp-server timeout**	恢复空闲时限为默认值（30 分钟）

可以如下配置会话空闲时限为 5 分钟：

```
Ruijie(config)# ftp-server timeout 5
```

则如果当前客户端在 5 分钟内没有进行任何操作，FTP 服务器将自动断开与其的连接。断开连接后 FTP 服务器可以开始响应新的连接请求。

会话的空闲时间是指在一个 FTP 会话中从上次 FTP 操作完成后到下次 FTP 操作开始之间的时间。服务器在一个 FTP 命令服务完成后（如一个文件全部传输完毕后）从 0 开始计算会话空闲时间；在下个命令到来的时候停止计算会话空闲时间。因此会话空闲时限的配置并不会对某些耗时的文件传输操作带来任何影响。

7.2.4 配置服务器登录用户名和密码

FTP 服务器使用登录用户名和密码对客户端进行身份认证，在缺省状态下服务器的登录用户名和密码均为空。

FTP 服务器不支持匿名用户和空密码，因此必须通过全局配置模式下的 **ftp-server username** 和 **ftp-server password** 命令配置有效的登录用户名和密码，否则客户端将无法通过服务器的身份认证。FTP 服务器仅能配置一个用户名和一个密码。

命令	作用
Ruijie(config)# **ftp-server username** *username*	设置用户名为 *username*
Ruijie(config)# **no ftp-server username**	清除用户名设置
Ruijie(config)# **ftp-server password** [*type*] *password*	指定的 FTP 用户名相关联的缺省口令。 type 定义密码的加密类型：0 或 7,缺省是 0。0 代表密码未加密（明文）；7 代表密码为加密过的密文。
Ruijie(config)# **no ftp-server password**	取消密码配置

用户名最大长度为 64 个字符，中间不允许有空格。用户名可以由英文字母、半角数字和半角符号组成。

密码必须包含字母或数字，密码前后可以有空格，但将被忽略；密码中间的空格作为密码的一部分。明文密码的最小长度为 1 个字符、最大长度为 25 个字符；密文密码的最小长度为 4 个字符、最大长度为 52 个字符。密文密码是由明文密码加密生成，其格式必须遵循加密规范，若使用密文密码进行密码设置，客户端必须采用对应的明文密码才能登录成功。

可以如下配置 FTP 服务器的用户名为“admin”，密码为“letmein”：

```
Ruijie(config)# ftp-server username admin
Ruijie(config)# ftp-server password letmein
```

7.2.5 查看服务器的状态信息和调试信息

使用特权模式下的 **show ftp-server** 命令可以显示 FTP 服务器的相关状态信息；使用特权用户模式下的 **debug ftpserver** 命令可以在 FTP 服务器运行过程中显示详细的调试信息。

命令	作用
Ruijie# **show ftp-server**	显示 FTP 服务器状态信息
Ruijie# **debug ftpserver**	打开 FTP 服务器的调试信息输出
Ruijie# **no debug ftpserver**	关闭 FTP 服务器的调试信息输出

可以如下查看 FTP 服务器的相关状态信息：

```
Ruijie# show ftp-server
ftp-server information
=====================================
enable : Y
topdir : /
```

```
timeout: 20min
username config : Y
password config : Y
type: BINARY
control connect : Y
ftp-server: ip=192.167.201.245  port=21
ftp-client: ip=192.167.201.82  port=4978
port data connect : Y
ftp-server: ip=192.167.201.245  port=22
ftp-client: ip=192.167.201.82  port=4982
passive data connect : N
```

如下打开 FTP 服务器的调试信息：

```
Ruijie# debug ftpserver
FTPSRV_DEBUG:(RECV)   SYST
FTPSRV_DEBUG:(REPLY)  215 RGOS Type: L8
FTPSRV_DEBUG:(RECV)   PORT 192,167,201,82,7,120
FTPSRV_DEBUG:(REPLY)  200 PORT Command okay.
```

要关闭服务器的调试信息输出，可以执行如下命令：

```
Ruijie# no debug ftpserver
```

7.3 FTP Server典型配置用例

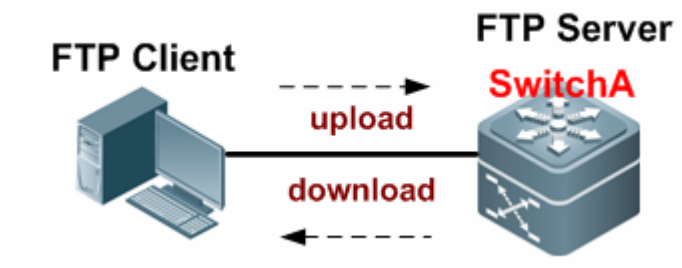
组网需求

某设备（如下图中的 SwitchA）的日志文件均存储于设备的“/syslog”目录下。要求通过配置设备为 FTP Server 并满足如下要求：

- 客户端使用用户名为 admin，密码为 ruijie 进行 FTP 服务器登陆；
- 成功登陆后，通过管理 PC 上的 FTP 客户端直接从设备上下载日志文件，但不允许 FTP 客户端访问到“/syslog”目录以外的文件；
- 当前客户端在 5 分钟内若没有进行任何操作，FTP 服务器将自动断开与其的连接，断开连接后 FTP 服务器可以开始响应新的连接请求。

组网拓扑

图 7-1AAA 典型应用图



配置要点

要满足上述需求，通过以下配置实现：

1) 配置登录服务器用户名为“admin”、密码为“ruijie”；

2) 配置会话空闲时限为 5 分钟；

3) 配置服务器顶层目录为“/syslog”；

4) 启动 FTP 服务器；

配置步骤

配置 SwitchA 为 FTP Server

第一步：配置登录服务器用户名为“admin”、密码为“ruijie”

```
Ruijie#configure
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#ftp-server username admin
Ruijie(config)#ftp-server password ruijie
```

第二步：配置会话空闲时限为 5 分钟

```
Ruijie(config)#ftp-server timeout 5
```

第三步：配置服务器顶层目录为“/syslog”

```
Ruijie(config)#ftp-server topdir /syslog
```

第四步：启动 FTP 服务器

```
Ruijie(config)#ftp-server enable
```

显示验证

第一步：查看 FTP 服务器的相关状态信息：

```
Ruijie(config)#show ftp-server
    ftp-server information
==================================
```

```
enable : Y
topdir : /syslog
timeout: 5min
username config : Y
password config : Y
transfer type: ASCII
control connection : N
port data connection : N
passive data connection : N
```

第二步，打开 FTP 服务器的调试信息：

```
Ruijie# debug ftpserver
FTPSRV_DEBUG:(RECV)   SYST
FTPSRV_DEBUG:(REPLY)  215 RGOS Type: L8
FTPSRV_DEBUG:(RECV)   PORT 192,167,201,82,7,120
FTPSRV_DEBUG:(REPLY)  200 PORT Command okay.
```

8 FTP Client

FTP Client 为用户提供在设备上通过 FTP 协议与远程 FTP 服务器进行文件传输的功能。

8.1 FTP概述

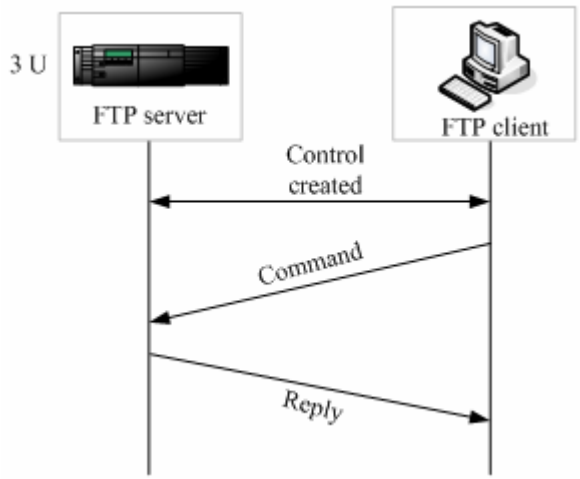
FTP 是 File Transfer Protocol（文件传输协议）的英文简称，是 TCP/IP 的一种具体应用，通过在 FTP 客户端和服务器之间建立面向连接的，可靠的 TCP 连接，用户可以访问一个运行有 FTP 服务器程序的远程计算机。用户通过客户端向服务器发出命令，服务器响应命令并把执行结果返回客户端，通过这种命令交互，用户可以察看服务器目录下的文件，并把文件从远程计算机上拷到本地，或把本地的文件传送到远程计算机去。FTP 协议在 RFC 959 中有详细的描述。

8.1.1 FTP 连接模式

FTP 协议要用到两个 TCP 连接，一个是控制链路（也称命令链路），用来在 FTP 客户端与服务器之间传递命令；另一个是数据链路，用来上传或下载数据。

- 控制连接：对于一些比较简单的连接只需要建立控制连接，客户端向服务器发送命令，服务器接收到命令则进行命令响应，其过程如下：

图 8-1 控制连接

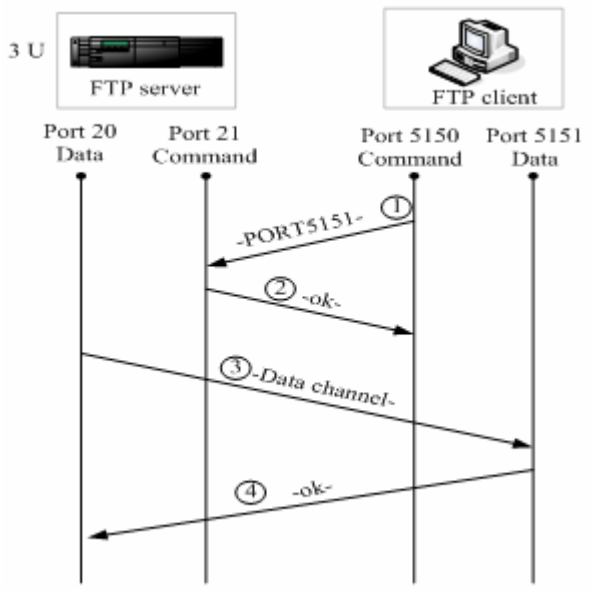


- 控制连接与数据连接：当客户端发出的命令需要上传或下载数据时，这时不仅要建立控制连接还需要建立数据连接。

FTP 协议有两种数据连接方式：主动（PORT）方式和被动（PASV）方式。这两种工作模式主要区别在于数据连接建立方式不同，控制连接基本是一样的。

8.1.1.1 主动方式

图 8-2 PORT（主动）模式



该模式下 FTP server 在数据连接时是主动去连接 FTP client，所以被称为主动连接，其主要执行如下四个步骤：

1) 客户端使用图例中的源端口 5150 与 server 端的 21 端口通信，请求建立连接，告诉服务器将用的端口是 5151

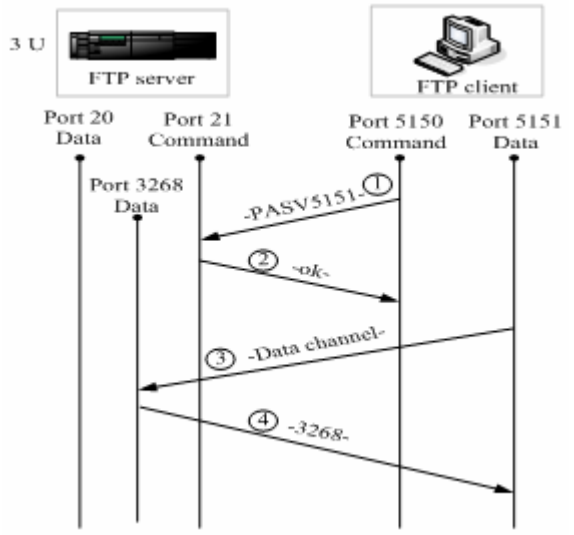
2) server 收到后，发送应答信息，OK(ACK)，client and server 通过控制端口交换控制信令

3) 服务器打开 20 端口作为数据发送的源端口，向客户端的 5151 端口发送

4) 客户端应答，传输过程结束

8.1.1.2 被动方式

图 8-3 PASV（被动）模式



该模式一般通过 passive 命令进行设置，由于 FTP server 在数据连接时是被动连接 FTP Client，所以称为被动连接，其主要执行如下四个步骤：

1) 被动模式下，客户端初始化控制信令连接，使用图例中 5150 源端口与服务器的 21 端口建立连接，并使用 passive 命令请求进入被动模式

2) 服务器同意进入 PASV 模式，并随机选择一个大于 1024 的端口号，告知客户端。

3) 客户端接收到此信息后，使用图例中的 5151 端口与刚才服务器提供的 3268 端口进行数据通信，这里 5151 是源端口，3268 是目的端口

4) 服务器收到信息，回传数据并发送应答 ACK（OK）

当客户端和服务器建立数据连接后，就可以进行 FTP 最基本的上传和下载功能，并且在客户端可以对服务器进行一些相关文件操作。

用于传输命令和反馈信息的传输的控制连接始终存在，而数据连接只在需要的时候建立；PASV 和 PORT 模式的设置选择权仅在 FTP Client，由 FTP Client 发出命令建立不同的数据连接模式，锐捷 FTP Client 默认方式为被动模式

8.1.2 FTP 传输模式

FTP 的传输有两种方式：文本（ASCII）传输模式和二进制（BINARY）数据传输模式。锐捷产品 FTP Client 目前支持 ASCII 和 BINARY 两种传输模式，默认情况下为 BINARY 传输模式。

8.1.2.1 文本模式

ASCII 模式和 BINARY 模式的区别是回车换行的处理，ASCII 模式将回车换行转换为本机的回车字符，比如 Unix 下是\n，Windows 下是\r\n，Mac 下是\r。

8.1.2.2 二进制模式

BINARY 模式可用来传送可执行文件，压缩文件和图片文件，不对数据进行任何处理。以 Unix 传送文本文件到 Windows 为例，使用 BINARY 模式时，不会对 Unix 下的换行符进行从\r 到\r\n 的转换，因此在 windows 上看这个文件是没有换行的，里面是一个个的黑方块。由于不进行回车换行的处理，因此 BINARY 模式比文本模式更快，可以传输所有 ASCII 值，保证不出错。

如果存在文本格式转换的需要，如 Unix 格式的文本和 DOS 格式的文本之间的转换，有很多工具都可以做到，因此一般将 FTP 默认设置成二进制模式。

8.1.3 FTP Client 简介

锐捷 FTP Client 并不像标准 FTP 客户端一样实现交互式命令，其控制连接相关的 open、user、pass 指令由 CLI 输入 copy 命令自动完成，在控制连接建立完成后，则进入文件传输过程，建立数据连接，实现文件的上传或下载。

原来的设备支持 TFTP，但是 TFTP 是用于小文件传输，FTP 协议支持大文件传输，在设备上实现文件传输协议 FTP，使设备可以同其它客户机或服务器进行文件传输

8.2 配置FTP Client

8.2.1 配置连接方式

FTP Client 默认连接方式为被动（PASV）模式，要配置设备使用主动模式连接，在全局配置模式中执行以下命令：

命令	作用
configure terminal	进入全局配置模式
ftp-client [vrf *vrfname***] port**	设置 FTP 为主动连接模式

要设置设备使用被动方式连接，在全局模式下执行以下命令：

命令	作用
configure terminal	进入全局配置模式
no ftp-client [vrf *vrfname***] port**	设置 FTP 为被动连接模式

8.2.2 配置传输模式

FTP Client 默认传输方式为二进制（BINARY）模式，要配置设备使用文本（ASCII）传输模式，在全局配置模式中执行以下命令：

命令	作用
configure terminal	进入全局配置模式
ftp-client [vrf *vrfname***] ascii**	设置 FTP 为文本传输模式

要配置设备使用二进制（BINARY）传输模式，在全局配置模式中执行以下命令：

命令	作用
configure terminal	进入全局配置模式
no ftp-client [vrf *vrfname***] ascii**	设置 FTP 为二进制传输模式

8.2.3 配置源 IP 地址

FTP Client 可以对与服务端进行通信的客户端源 IP 地址进行绑定，在全局配置模式中通过以下命令配置源 IP 地址：

命令	作用
configure terminal	进入全局配置模式
ftp-client [vrf *vrfname***] source-address** {*ip-address* | *ipv6-address*}	配置进行 FTP 连接的客户端源 IP 地址，支持 ipv4 和 ipv6

如果要删除客户端源 IP 地址绑定，可通过以下命令：

命令	作用
configure terminal	进入全局配置模式
no ftp-client [vrf *vrfname***] source-address**	删除客户端源 ip 地址绑定

8.2.4 恢复默认配置

要恢复 FTP Client 为默认配置，则在全局模式下执行以下命令：

命令	作用
configure terminal	进入全局配置模式
default ftp-client [vrf *vrfname***]**	恢复 FTP Client 为缺省配置，数据连接为被动方式，文件传输为二进制模式，清除源 IP 绑定

8.2.5 下载文件

在 CLI 命令模式下，按如下步骤设置来完成文件的下载：

下载前，首先在主机上打开 FTP Server 软件，而后登录到设备，在特权模式下使用以下命令下载文件

命令	作用
Ruijie#**copy ftp**://*username*:*password@dest-address[/remote-directory]/remote-file* **flash**:[*local-directory/*]*local-file* [**vrf** *vrfname*]	下载主机端的 URL 指定的文件 filename 到设备，可重设文件名

FTP URL 中关键字 username 指定访问 FTP Server 的用户名，最长不超过三十二个字节，不可包含“:”、“@”、“/”和空格等字符，不可省略；关键字 password 指定访问 FTP Server 的密码，约束条件同 username；关键字 dest-address 指定 FTP Server 的 IP 地址，可选关键字 local-directory 指定 Server 端的目录路径，关键字 remote-file 指定要操作的 Server 端文件名；Flash URL 中的可选关键字 local-directory 指定设备目录，如果未指定，则表示当前工作目录，关键字 local-file 表示要操作的本地文件名，可选关键字 VRF 表示对 vrf 的支持。

Flash URL 如果包含 directory 字段，则必须保证设备中已创建了该目录，此下载命令不支持目录的自动创建。

8.2.5.1 下载文件示例

从用户名为 user，密码为 pass，IP 地址为 192.168.23.69 的 FTP Server 的 root 目录下载文件名为 remote-file 的文件到设备上的 home 目录中，存储的文件名为 local-file

```
Ruijie# copy ftp://user:pass@192.168.23.69/root/remote-file flash: home/local-file
```

8.2.6 上传文件

在 CLI 命令模式下，按如下步骤设置来完成文件的上传：

上传文件前，首先在主机端打开 FTP Server 软件，而后登录到设备，在特权模式下使用以下命令上传文件，其中关键字 dest-address 指定 FTP Server 的 IP 地址

命令	作用
Ruijie# **copy flash**:[*local-directory/*]*local-file* **ftp:**//*username*:*password@dest-address[/remote-directory]/remote-file* [**vrf** *vrfname*]	上传 Flash URL 指定的设备文件 filename 到主机端，可重设文件名

关键字及参数说明同上一条命令。

8.2.6.1 上传文件示例

把设备 home 目录中的 local-file 文件上传到用户名为 user，密码为 pass，IP 地址为 192.168.23.69 的 FTP Server 的 root 目录下，文件命名为 remote-file

```
Ruijie# copy flash: home/local-file ftp://user:pass@192.168.23.69/root/remote-file
```

9 IPv6 隧道

9.1 概述

IPv6 的根本目的是继承和取代 IPv4，但从 IPv4 到 IPv6 的演进是一个逐渐的过程。因此在 IPv6 完全取代 IPv4 之前，不可避免地，这两种协议要有一个共存时期。在这个过渡阶段的初期，IPv4 网络仍然是主要的网络，IPv6 网络类似孤立于 IPv4 网络中的小岛。过渡的问题可以分成两大类：

- 被孤立的 IPv6 网络之间透过 IPv4 网络互相通信的问题；
- IPv6 的网络与 IPv4 网络之间通信的问题；

本文讨论的隧道（Tunnel）技术，就是解决问题 1 的，解决问题 2 的方案是 NAT-PT（网络地址转换-协议转换），不在本文讨论范围内。

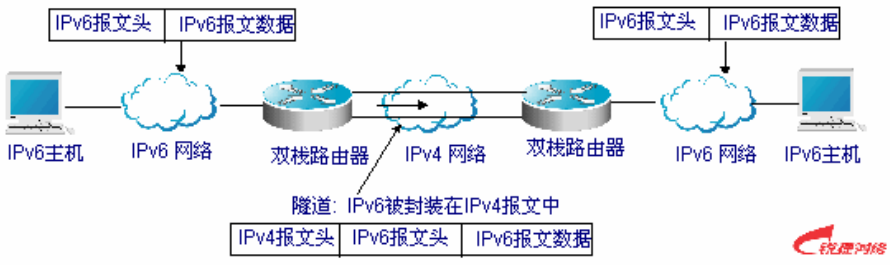
IPv6 隧道是将 IPv6 报文封装在 IPv4 报文中，这样 IPv6 协议包就可以穿越 IPv4 网络进行通信。因此被孤立的 IPv6 网络之间可以通过 IPv6 的隧道技术利用现有的 IPv4 网络互相通信而无需对现有的 IPv4 网络做任何修改和升级。IPv6 隧道可以配置在边界路由器之间也可以配置在边界路由器和主机之间，但是隧道两端的节点都必须既支持 IPv4 协议栈又支持 IPv6 协议栈。目前，我公司支持下列几种隧道技术:

隧道类型	参考标准
Manually Config Tunnel	RFC2893
automatic 6to4 Tunnel	RFC3056
Intra-Site Automatic Tunnel Addressing Protocol(ISATAP)	draft-ietf-ngtrans-isatap-22

通过 IPv6 隧道技术将被孤立的 IPv6 网络互联起来并不是最终的 IPv6 的网络架构，而只是一种过渡的技术。

使用隧道技术的模型如下图：

图 9-1



下面分别介绍各隧道的特点：

9.1.1 6ver4 手工隧道(IPv6 Manually Configured Tunnel)

一个 6ver4 手工隧道类似于在两个 IPv6 域之间通过 IPv4 的主干网络建立了一条永久链路。适合用在两台边界路由器或者边界路由器和主机之间对安全性要求较高并且比较固定的连接上。

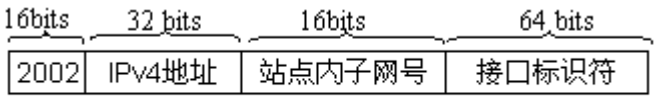
在隧道接口上，IPv6 地址需要手工配置，并且隧道的源 IPv4 地址(Tunnel Source)和目的 IPv4 地址(Tunnel Destination)必须手工配置。隧道两端的节点必须支持 IPv6 和 IPv4 协议栈。6ver4 手工隧道在实际应用中总是成对配置的，即在两台边缘设备上同时配置，可以将其看作是一种点对点的隧道。

9.1.2 6to4 自动隧道(Automatic 6to4 Tunnel)

6to4 自动隧道技术允许将被孤立的 IPv6 网络透过 IPv4 网络互联。它和 6ver4 手工隧道的主要区别是 6ver4 手工隧道是点对点的隧道，而 6to4 隧道是点对多点的隧道。

6to4 隧道将 IPv4 网络视为 Nonbroadcast Multi-access（NBMA，非广播多路访问）链路，因此 6to4 的设备不需要成对的配置，嵌入在 IPv6 地址的 IPv4 地址将用来寻找自动隧道的另一端。6to4 隧道可以看做是点到多点的隧道。6to4 自动隧道可以被配置在一个被孤立的 IPv6 网络的边界路由器上，对于每个报文它将自动建立隧道到达另一个 IPv6 网络的边界路由器。隧道的目的地址就是另一端的 IPv6 网络的边界路由器的 IPv4 地址，该 IPv4 地址将从该报文的目的 IPv6 地址中提取，其 IPv6 地址是以前缀 2002::/16 开头的，形式如下:

图 9-2



IPv6 6to4 地址格式

6to4 地址是用于 6to4 自动构造隧道技术的地址，其内嵌的 IPv4 地址通常是站点边界路由器出口的全局 IPv4 地址，在自动隧道建立时将使用该地址作为隧道报文封装的 IPv4 目的地址。6ot4 隧道两端的设备同样必须都支持 IPv6 和 IPv4 协议栈。6to4 隧道通常是配置在边界路由器之间。

例如：6to4 站点边界路由器出口的全局 IPv4 地址是 211.1.1.1（用十六进制数表达为 D301:0101），站点内的某子网号为 1，接口标识符为 2e0:ddff:fee0:e0e1，那么其对应的 6to4 地址可以表示为：

2002: D301:0101:1: 2e0:ddff:fee0:e0e1

> 6to4 地址内嵌的 IPv4 地址不能为私有的 IPv4 地址（即 10.0.0.0/8，172.16.0.0/12，192.168.0.0/16 网段的地址）而必须是全局的 IPv4 地址。

6to4 隧道常用的应用模型：

- 简单应用模型

6to4 隧道最简单、最常用的应用是用来多个 IPv6 站点之间的互联，每个站点至少必须有一个连接通向一个它们共享的 IPv4 网络。这个 IPv4 网络可以是 Internet 网络也可以是某个组织团体内部的主干网。关键是每个站点必须要一个全局唯一的 IPv4 地址，6to4 隧道将使用该地址构照一个 6to4/48 的 IPv6 前缀：2002:IPV4 地址/48。

- 混合应用模型

在上面所描述的应用的基础上，通过在纯 IPv6 网络的边缘提供 6to4 中继设备，实现其它 6to4 网络接入纯 IPv6 网络中，实现该功能的设备我们称之为 6to4 中继路由器(6to4 Relay Router)。

9.1.3 ISATAP自动隧道(ISATAP Tunnel)

站内自动隧道寻址协议(ISATAP)是一种站点内部的 IPv6 体系架构将 IPv4 网络视为一个非广播型多路访问（NBMA）链路层的 IPv6 隧道技术，即将 IPv4 网络当作 IPv6 的虚拟链路层。

ISATAP 主要是用在当一个站点内部的纯 IPv6 网络还不能用，但是又要在站点内部传输 IPv6 报文的情况，例如站点内部有少数测试用的 IPv6 主机要互相通讯。使用 ISATAP 隧道允许站点内部同一虚拟链路上的 IPv4/IPv6 双栈主机互相通讯。

在ISATAP站点上，ISATAP设备提供标准的路由器公告报文，从而允许站点内部的ISATAP主机进行自动配置；同时ISATAP设备也执行站点内的 ISATAP 主机和站点外的 IPv6 主机转发报文的功能。

ISATAP 使用的 IPv6 地址前缀可以是任何合法的 IPv6 单点传播的 64 位前缀，包括全球地址前缀、链路本地前缀和站点本地前缀等，IPv4 地址被置于 IPv6 地址最后的 32 比特上，从而允许自动建立隧道。

ISATAP 很容易与其他过渡技术结合起来使用，尤其是在和 6to4 隧道技术相结合使用时，可以使内部网的双栈主机非常容易地接入 IPv6 主干网。

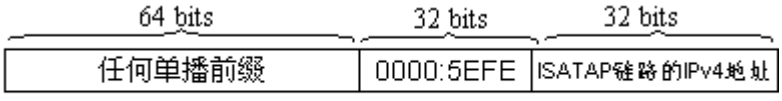
- ISATAP 接口标识符

ISATAP 使用的单播地址的形式是 64 比特的 IPv6 前缀加上 64 比特的接口标识符。64 比特的接口标识符是由修正的 EUI-64 地址格式生成的，其中接口标识符的前 32 比特的值为 0000:5EFE，这就意味着这是一个 ISATAP 的接口标识符。

- ISATAP 的地址结构

ISATAP 地址是指接口标识符中包含 ISATAP 接口标识符的单播地址，下图显示了 ISATAP 的地址结构：

图 9-3



IPv6 ISATAP 地址格式

从上图中可以看到接口标识符中包含了 IPv4 的地址，该地址就是双栈主机的 IPv4 地址，在自动建立自动隧道时将被使用。

例如：IPv6 的前缀是 2001::/64，嵌入的 IPv4 的地址是 192.168.1.1，在 ISATAP 地址中，IPv4 地址用十六进制数表达为 C0A8:0101，因此其对应的 ISATAP 地址为：

2001::0000:5EFE:C0A8:0101

9.1.4 Tunnel接口概述

Tunnel 接口用于实现隧道功能，是系统虚拟的接口。Tunnel 接口并不特别指定传输协议或者负载协议，它提供的是一个用来实现标准的点对点的传输链路。每一个单独的链路都必须设置一个 Tunnel 接口。

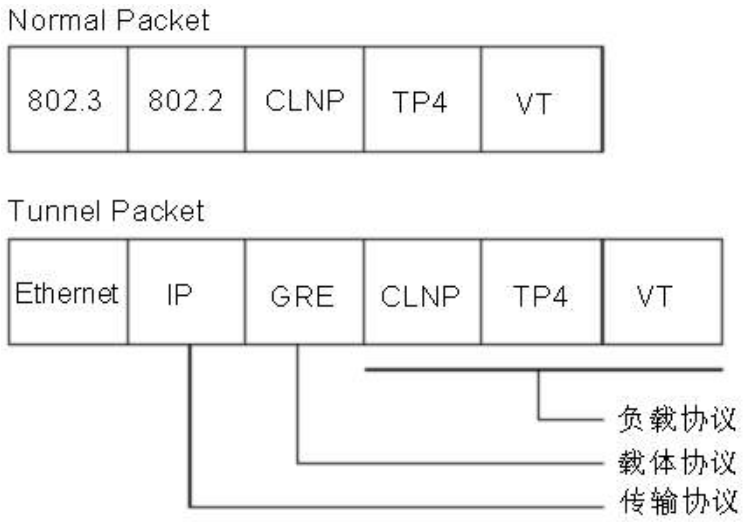
Tunnel 功能实现包括下面三个主要组成部分：

1) 负载协议：通过 Tunnel 传输的负载(网络数据)的封装协议。目前我司产品软件在 Tunnel 接口上只支持 IP 协议作为负载协议；

2) 载体协议：用来二次封装并辨识待传输负载的协议。

3) 传输协议：实际传输经过载体协议二次封装后的负载的网络协议。我司产品使用最广泛应用的 IP 协议作为传输协议。

图 9-4 使用 Tunnel 传输网络时数据包在传输前后的构成对比示意图



图中通过以太网封装 GRE 实现了 IP Tunnel 传输功能。实际上，如果两个私有同种协议网络需要通过异种公有网络实现互通讯，就可以采用 Tunnel 模式实现。

Tunnel 传输适用于以下情况：

- 允许运行非 IP 协议的本地网络之间通过一个单一网络 (IP 网络) 通讯，因为 Tunnel 支持多种不同的负载协议；允许那些对路由跳数有限制的协议可以在更广泛的范围内工作，因为 Tunnel 使用的是传输协议 (IP) 的路由工作；
- 允许通过单一的网络 (IP 网络) 连接间断子网；
- 允许在广域网上提供 VPN (virtual private network) 功能。

由于 Tunnel 将负载封装后传输，这会带来处理上的复杂性，在某些情况下需要注意以下的变化。

- 由于 Tunnel 是点对点的链路，在路由的时候看起来只有一跳（hop），可实际上可能其路由花费不止一跳。在使用 Tunnel 的时候必须注意到 Tunnel 链路的路由与实际路由并不一致。
- 由于 Tunnel 传输将负载封装在传输协议中，在设置防火墙特别是访问控制链表(ACL)的时候，这一点需要考虑；同时必须注意到此时负载协议的传输带宽等(如 MTU)也比理论值更小。

下面将只介绍配置 Tunnel 接口的特有属性，其它属性的配置(包括 IP 地址以及其它参数、防火墙和备份中心参数等)将在请参见相关章节。

9.2 通用的Tunnel接口配置

9.2.1 Tunnel接口的配置任务列表

Tunnel 接口的配置任务包括：

- 进入指定 Tunnel 接口的配置模式；
- 设置 Tunnel 接口的源地址；

- 设置 Tunnel 接口目的地址（自动隧道不必配置）；
- 设置 Tunnel 封装格式；
- 设置 Tunnel 的 TOS（可选）；
- 设置 Tunnel 的 TTL（可选）；
- 设置 Tunnel 的保活功能（可选）；
- 设置 Tunnel 外层协议的 VRF（可选）；

9.2.2 进入指定Tunnel接口的配置模式

要创建 Tunnel 接口并进入该接口的配置模式，在全局配置模式中执行以下命令：

命令	作用
Ruijie(config)# **interface tunnel** *tunnel-number*	进入指定 Tunnel 接口配置模式
Ruijie(config)# **no interface tunnel** *tunnel-number*	删除已创建的 Tunnel 接口

同其它逻辑接口一样，第一次进入指定的 Tunnel 接口的时候就创建了一个 Tunnel 接口。

Tunnel 接口不支持 MTU 配置命令。

9.2.3 设置Tunnel接口的源地址

一个 Tunnel 接口需要明确配置隧道的源地址和目的地址，为了保证隧道接口的稳定性，一般将 Loopback 地址作为隧道的源地址和目的地址。在 tunnel 接口正常工作之前，需要确认源地址和目的地址的连通性。

要配置 Tunnel 接口的源地址，在 tunnel 接口配置模式中执行以下命令：

命令	作用
Ruijie(config-if)# **tunnel source** {*ip-address* | *interface-name interface-number*}	设置 Tunnel 接口的源地址
Ruijie(config-if)# **no tunnel source**	取消 Tunnel 接口源地址设置

命令 **tunnel source** 设置的是 Tunnel 接口用来进行实际通讯的源地址，它也是 Tunnel 位于本地的端点。

9.2.4 设置Tunnel接口目的地址

要设置 tunnel 接口的目的地址，在 tunnel 接口配置模式中执行以下命令：

命令	作用
Ruijie(config-if)# **tunnel destination** { *ip-address* }	设置 Tunnel 接口目的地址
Ruijie(config-if)# **no tunnel destination**	取消 Tunnel 接口目的地址设置

命令 **tunnel destination** 设置的 Tunnel 接口用来进行实际通讯的目的地址，它也是 Tunnel 位于远程对端的端点。

在同一台设备上，禁止使用相同的源地址或目的地址，创建两个或多个相同封装模式的 Tunnel 接口。

9.2.5 设置Tunnel封装格式

Tunnel 的封装格式就是 Tunnel 的载体协议。Tunnel 接口的默认封装格式是 IPv6IP 手工隧道。当然，用户也可以根据实际使用情况来决定 Tunnel 接口的封装格式。

命令	作用
Ruijie(config-if)# **tunnel mode** { **ipv6** | **ipv6ip** [6to4 | isatap]}	设置 Tunnel 封装格式
Ruijie(config-if)# **no tunnel mode**	取消 Tunnel 接口封装格式设置，恢复默认值

tunnel mode 命令支持的情况与设备的型号有关，请以设备的实际情况为准。

9.2.6 设置Tunnel的TTL

由于 Tunnel 是点对点的链路，所以对于负载协议来说，在路由的时候看起来只有一跳（hop），但实际上传输协议的路由花费可能不止一跳。我司产品允许设置 Tunnel 的 TTL，也即设置 tunnel 所发送的封装报文中传输协议报头 TTL 值。隧道中间节点会递减传输协议报头中的 TTL 值，丢弃 TTL 为 0 的报文。

命令	作用
Ruijie(config-if)# **tunnel ttl** *hop-count*	设置 Tunnel 的 TTL 值
Ruijie(config-if)# **no tunnel ttl**	取消 Tunnel 的 TTL 设置，恢复为缺省值 255

缺省情况下，tunnel 传输协议的 TTL 值为 255。

9.2.7 设置Tunnel的TOS

在 tunnel 接口模式下配置外层传送协议 IPv4 的 TOS 字节，或者 IPv6 的 traffic class 的 8 个比特。

命令	作用
Ruijie(config-if)# **tunnel tos** *num*	设置 Tunnel 的 TOS 值
Ruijie(config-if)#**no tunnel tos**	取消 Tunnel 的 TOS 设置

缺省情况下，如果隧道内层承载与外层封装都是 IPv4 协议，则缺省将内层 IPv4 头的 tos 字节拷贝到外层 IPv4 头。如果隧道内层承载与外层封装都是 IPv6 协议，则缺省将内层 IPv6 头的 traffic class8 比特拷贝到外层 IPv6 头。其他情况，外层 IPv4 tos / IPv6 traffic class,为 0。

9.2.8 Tunnel接口的故障诊断与排除

如果 Tunnel 两端不能正常通讯，可以从以下几方面考察：

4) 首先必须确保 Tunnel 的两端存在可连通的物理通道，即在不使用 Tunnel 的时候这两端也具有网络连通性，也就是 Tunnel 的源通讯地址(本地地址)必须能与 Tunnel 的目的通讯地址(对端的网络地址)进行正常通讯；

5) 其次必须确保 Tunnel 两端的源地址与目的地址具备对应性，也就是 Tunnel 一端的源通讯地址必须与 Tunnel 的另一端的目的通讯地址一致；

6) 然后还必须确保 Tunnel 使用了正确的封装格式，系统默认使用 IPv6IP 手工隧道，并且 Tunnel 两端必须使用相同的封装格式；

9.3 配置IPv6 隧道

IPv6 隧道接口数目相关配置，参见《硬件表项容量》文档“配置 IPv6 隧道接口最大数目”章节。

9.3.1 配置 6ver4 手工隧道

本节解释如何配置手工隧道。

要配置手工隧道，在隧道接口上要配置一个 IPv6 地址并且要 6ver4 手工隧道的源端和目的端的 IPv4 地址。在配置隧道两端的主机或者设备必须支持双栈(IPv6 协议栈和 IPv4 协议栈)。

不能在设备上配置隧道的源（Tunnel Source）和目的（Tunnel Destination）地址相同的手工隧道。

简要步骤

```
config terminal
interface tunnel tunnel-num
tunnel mode ipv6ip
ipv6 enable
tunnel source {ip-address | type num}
tunnel destination ip-address
end
```

详细步骤

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **interface tunnel** *tunnel-num*	指定隧道接口号创建隧道接口，并进入接口配置模式。
Ruijie(config-if-Tunnel id)# **tunnel mode ipv6ip**	指定隧道的类型为 6ver4 手工隧道。
Ruijie(config-if-Tunnel id)# **ipv6 enable**	使能该接口的 IPv6 功能，您也可以通过配置 IPv6 地址直接启动该接口的 IPv6 功能。
Ruijie(config-if-Tunnel id)# **tunnel source** {*ip-address* | *type num*}	指定隧道的 IPv4 源地址或者引用的源接口号。注意如果指定了接口，那么接口上必须已经配置了 IPv4 的地址。
Ruijie(config-if-Tunnel id)# **tunnel destination** *ip-address*	指定隧道的目的地址。
Ruijie(config-if-Tunnel id)# **end**	退到特权模式。
Ruijie# **copy running-config startup-config**	保存配置。

参考 “验证 IPv6 隧道的配置和监控”一节来检查隧道的工作情况。

9.3.2 配置 6to4 隧道

本节介绍如何配置 6to4 隧道。

6to4 隧道的目的地址是由从 6to4 IPv6 地址中提取的 IPv4 地址决定的，6to4 隧道两端的设备必须支持双栈，即支持 IPv4 和 IPv6 协议栈。

> 在一台设备上只支持配置一个 6to4 隧道。6to4 隧道使用的封装源地址（IPv4 地址）必须是全局可路由的地址，否则 6to4 隧道将不能正常工作。

简要步骤

```
config terminal
interface tunnel tunnel-num
tunnel mode ipv6ip 6to4
ipv6 enable
tunnel source {ip-address | type num}
exit
ipv6 route 2002::/16 tunnel tunnel-number
end
```

详细步骤

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **interface tunnel** *tunnel-num*	指定隧道接口号创建隧道接口，并进入接口配置模式。
Ruijie(config-if-Tunnel id)# **tunnel mode ipv6ip 6to4**	指定隧道的类型为 6to4 隧道。
Ruijie(config-if-Tunnel id)# **ipv6 enable**	使能该接口的 IPv6 功能，您也可以通过配置 IPv6 地址直接启动该接口的 IPv6 功能。
Ruijie(config-if-Tunnel id)# **tunnel source** {*ip-address* | *type num*}	指定隧道的封装源地址或者引用的源接口号。 注意： 被引用的接口上必须已经配置了 IPv4 的地址。 使用的 IPv4 地址必须是全局可路由的地址。
Ruijie(config-if-Tunnel id)# **exit**	退回全局配置模式。
Ruijie(config)# **ipv6 route** *2002::/16* **tunnel** *tunnel-number*	为 IPv6 6to4 前缀 2002::/16 配置一条静态的路由并关联输出接口到该隧道接口上(即前面步骤 2 中指定的隧道接口)。
Ruijie(config)# **end**	退回特权模式。
Ruijie# **copy running-config startup-config**	保存配置。

参考“验证 IPv6 隧道的配置和监控”一节来检查隧道的工作情况。

9.3.3 配置ISATAP隧道

本节介绍如何配置 ISATAP 设备。

在 ISATAP 隧道接口上，ISATAP IPv6 地址的配置以及前缀的公告配置和普通 IPv6 接口的配置是一样的，但是为 ISATAP 隧道接口配置的地址必须使用修正的 EUI-64 地址，因为 IPv6 地址中的接口标识符的最后 32 位是由隧道源地址(Tunnel Source)引用的接口的 IPv4 地址)构成的。ISATAP 地址格式参见上面的内容。

> 设备上允许同时配置多个 ISATAP 隧道，但是每个 ISATAP 隧道的 tunnel source 必须是不同的，否则收到 ISATAP 隧道报文时无法区分是属于哪个 ISATAP 隧道。

简要步骤

```
config terminal
interface tunnel tunnel-num
tunnel mode ipv6ip isatap
ipv6 address ipv6-prefix/prefix-length eui-64
tunnel source interface-type num
no ipv6 nd suppress-ra
end
```

详细步骤

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **interface tunnel** *tunnel-num*	指定隧道接口号创建隧道接口，并进入接口配置模式。
Ruijie(config-if-Tunnel id)# **tunnel mode ipv6ip isatap**	指定隧道的类型为 ISATAP 隧道。
Ruijie(config-if-Tunnel id)# **ipv6 address** *ipv6-prefix*/*prefix-length* [**eui-64**]	配置 IPv6 ISATAP 地址,注意指定使用 eui-64 关键字，这样将自动生成 ISATAP 的地址，在 ISATAP 接口上配置的地址必须为 ISATAP 的地址。
Ruijie(config-if-Tunnel id)# **tunnel source type** *num*	指定隧道引用的源接口号,被引用的接口上必须已经配置了 IPv4 的地址。
Ruijie(config-if-Tunnel id)# **no ipv6 nd suppress-ra**	缺省情况下是禁止在接口上发送路由器公告报文的,使用该命令打开该功能从而允许 ISATAP 主机进行自动配置。
Ruijie(config)# **end**	退回特权模式。
Ruijie# **copy running-config startup-config**	保存配置。

参考 “验证 IPv6 隧道的配置和监控”一节来检查隧道的工作情况。

9.3.4 配置隧道支持IPv6 组播

目前在 IPV6 网络中，不仅 IPV6 单播业务需要能够使用隧道方式穿越 IPv4 网络，而且 IPv6 组播业务也需要能使用隧道方式穿越 IPv4 网络。

IPv6 隧道组播的配置非常简单，在 TUNNEL 接口上的同其它普通接口（如 SVI 口）上一样配置就可以了。

- 仅在 6ver4 手工隧道能支持组播，对于其它类型的隧道，虽然也能够进行配置，但是不会对组播数据报文进行接收和转发。
- 对于 6ver4 手工隧道，如果隧道是建立在一个任何类型的 IPv6 隧道上，虽然也能够进行组播相关的配置，但是不会对组播数据报文进行接收和转发。
- IPv6 组播数据穿越 IPv4 网络时，有关 MTU 方面的限制同 IPv6 单播数据是一样的。

9.3.5 验证IPv6 隧道的配置和监控

本节介绍如何验证 IPv6 隧道的配置以及实际运行情况：

简要步骤

```
enable
show interface tunnel number
show ipv6 interface tunnel mumber
ping protocol destination
show ip route
show ipv6 route
```

详细步骤

命令	作用
show interface tunnel *tunnel-num*	查看指定 tunnel 接口的信息.
show ipv6 interface tunnel *tunnel-num*	查看 tunnel 接口的 IPv6 信息
ping *protocol destination*	检查网络的基本连通性
show ip route	查看 IPv4 路由器表
show ipv6 route	查看 IPv6 路由表

- 查看 Tunnel 接口的信息

```
Ruijie# show interface tunnel 1
Tunnel 1 is UP  , line protocol is UP
Hardware is  Tunnel
Interface address is: no ip address
  MTU 1480 bytes, BW 9 Kbit
  Encapsulation protocol is Tunnel, loopback not set
  Keepalive interval is no set
  Carrier delay is 2 sec
  Rxload is 1/255, Txload is 1/255
  Tunnel source 192.168.5.215, destination 192.168.5.204
  Tunnel TOS/Traffic Class not set, Tunnel TTL 255
  Tunnel protocol/transport ipv6/ip
```

- 查看 Tunnel 接口的 IPv6 信息

```
Ruijie# show ipv6 interface tunnel 1
interface Tunnel 1 is Up, ifindex: 6354
address(es):
Mac Address: N/A
INET6: fe80::3d9a:1601 , subnet is fe80::/64
Joined group address(es):
ff02::2
ff01::1
ff02::1
ff02::1:ff9a:1601
INET6: 3ffe:4:0:1::1 , subnet is 3ffe:4:0:1::/64
Joined group address(es):
ff02::2
```

```
ff01::1
ff02::1
ff02::1:ff00:1
MTU is 1480 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds<240--160>
ND router advertisements live for 1800 seconds
```

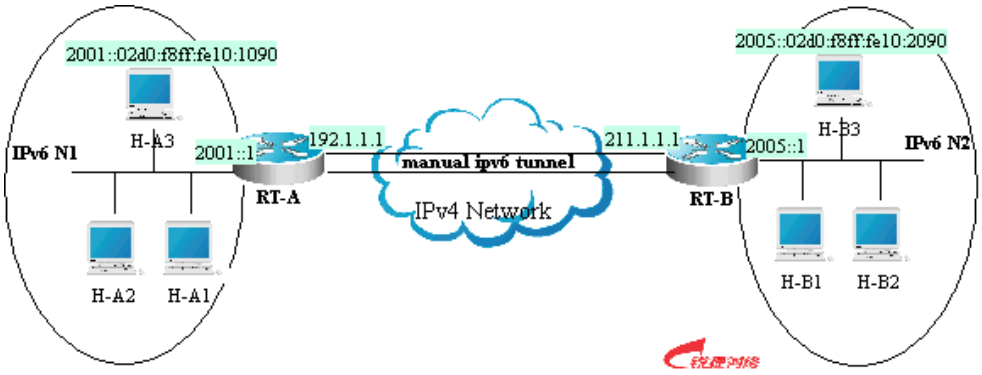
9.4 IPv6 隧道配置实例

下面章节介绍 IPv6 隧道配置实例

- 配置手工隧道例子
- 配置 6to4 隧道例子
- 配置 ISATAP 隧道例子
- 配置 ISATAP 和 6to4 隧道的例子

9.4.1 配置 6ver4 手工隧道实例

图 9-5



如上图，IPv6 网络 N1 和 N2 被 IPv4 网络隔离开了，现在通过配置手工隧道将这两个网络互联起来，如可以使 N1 中的 H-A3 主机可以访问 N2 中的 H-B3 主机。

图中 RT-A 和 RT-B 是支持 IPv4 和 IPv6 协议栈的设备，隧道的配置在 N1 和 N2 的边界路由器上(RT-A 和 RT-B)进行，注意手工隧道必须对称配置，既在 RT-A 和 RT-B 上都要配置。

和隧道相关的具体配置分别如下：

前提：假设 IPv4 的路由是连通的，下面不再列出关于 IPv4 的路由配置情况。

- RT-A 的配置

连接 IPv4 网络的接口

```
interface FastEthernet 2/1
no switchport
ip address 192.1.1.1 255.255.255.0
```

连接 IPv6 网络的接口

```
interface FastEthernet 2/2
no switchport
ipv6 address 2001::1/64
no ipv6 nd suppress-ra （可选）
```

配置手工隧道接口

```
interface Tunnel 1
tunnel mode ipv6ip
ipv6 enable
tunnel source FastEthernet 2/1
tunnel destination 211.1.1.1
```

配置进隧道的路由

```
ipv6 route 2005::/64 tunnel 1
```

- RT-B 的配置

连接 IPv4 网络的接口

```
interface FastEthernet 2/1
no switchport
ip address 211.1.1.1 255.255.255.0
```

连接 IPv6 网络的接口

```
interface FastEthernet 2/2
no switchport
ipv6 address 2005::1/64
no ipv6 nd suppress-ra （可选）
```

配置手工隧道接口

```
interface Tunnel 1
tunnel mode ipv6ip
ipv6 enable
tunnel source FastEthernet 2/1
tunnel destination 192.1.1.1
```

配置进隧道的路由

```
ipv6 route 2001::/64 tunnel 1
```

9.4.2 配置 6ver4 手工隧道支持组播实例

假设网络模型如上个实例，在上个实例的基础上，要增加对 PIM SMv6 组播的支持。

和组播相关的具体配置分别如下：

- RT-A 的配置

#全局下启用组播

```
ipv6 multicast-routing
```

在接口上启用 PIM SMv6

```
interface Tunnel 1
IPv6 pim sparse-mode
```

- RT-B 的配置

全局下启用组播

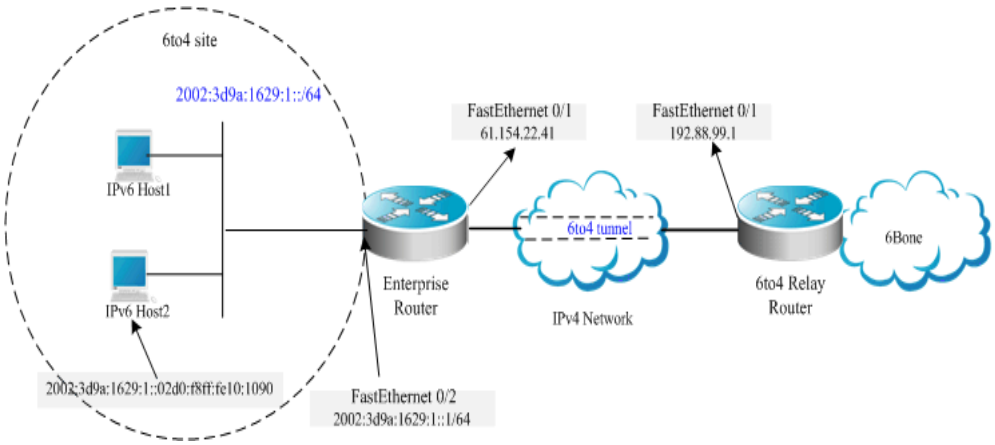
```
ipv6 multicast-routing
```

在接口上启用 PIM SMv6

```
interface Tunnel 1
IPv6 pim sparse-mode
```

9.4.3 配置 6to4 隧道实例

图 9-6



如上图是一个 IPv6 网络(6to4 站点)使用 6to4 隧道通过 6to4 中继路由器接入 IPv6 主干网(6bone)的一个例子。

在前面已经介绍了 6to4 隧道技术主要用在将孤立的 IPv6 网络互联起来，并且可以通过 6to4 中继路由器方便的接入 IPv6 主干网络。6to4 隧道是自动隧道，嵌入在 IPv6 地址的 IPv4 地址将用来寻找自动隧道的另一端，因此 6to4 隧道无须配置隧道的目的端，同时 6to4 隧道的配置不像手工隧道要对称配置。

61.154.22.41 的十六进制格式为：3d9a:1629

192.88.99.1 的十六进制格式为：c058:6301

在边界路由器上配置 6to4 隧道时，必须使用全局可路由的 IPv4 地址。否则 6to4 隧道将不能正常工作

下面是图中 2 个设备的配置（假设 IPv4 的路由是连通的，不考虑 IPv4 路由配置）：

Enterprise Router 的配置

连接 IPv4 网络的接口

```
interface FastEthernet 0/1
no switchport
ip address 61.154.22.41 255.255.255.128
```

连接 IPv6 网络的接口

```
interface FastEthernet 0/2
no switchport
ipv6 address 2002:3d9a:1629:1::1/64
no ipv6 nd suppress-ra
```

配置 6to4 隧道接口

```
interface Tunnel 1
tunnel mode ipv6ip 6to4
ipv6 enable
tunnel source FastEthernet 0/1
```

配置进隧道的路由

```
ipv6 route 2002::/16 Tunnel 1
```

配置到 6to4 中继路由器的路由,以便可以访问 6bone

```
ipv6 route ::/0 2002:c058:6301::1
```

ISP 6to4 Relay Router 的配置

连接 IPv4 网络的接口

```
interface FastEthernet 0/1
no switchport
ip address 192.88.99.1 255.255.255.0
```

配置 6to4 隧道接口

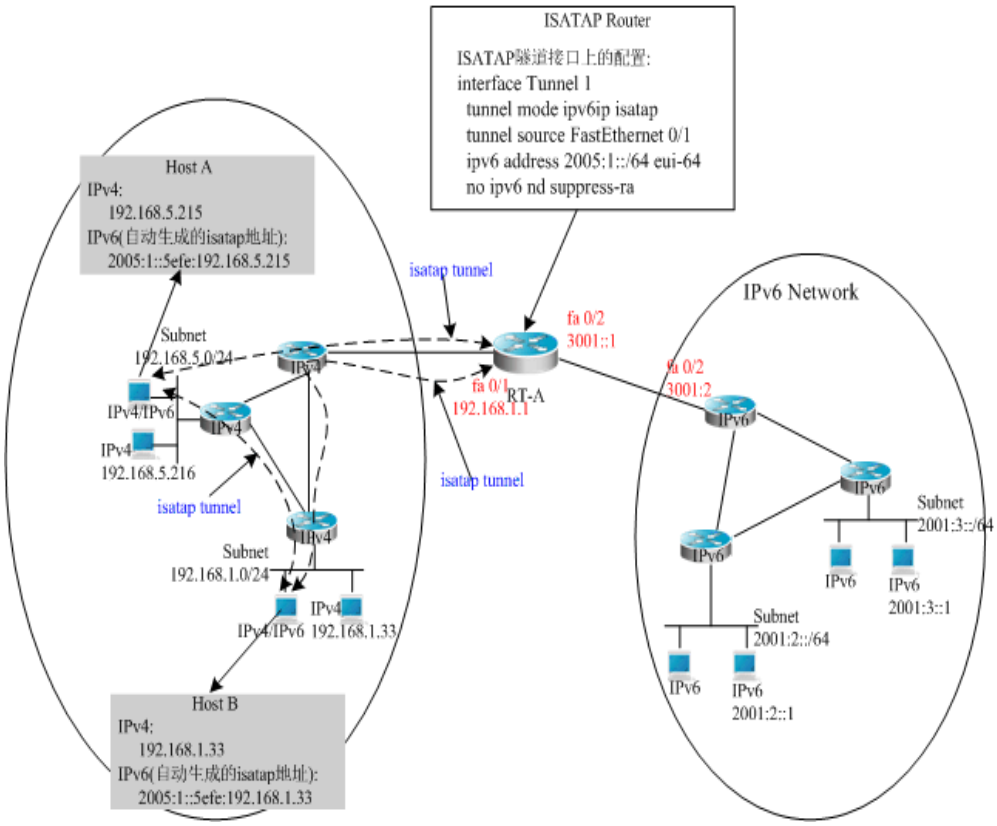
```
interface Tunnel 1
tunnel mode ipv6ip 6to4
ipv6 enable
tunnel source FastEthernet 0/1
```

配置进隧道的路由

```
ipv6 route 2002::/16 Tunnel 1
```

9.4.4 配置ISATAP隧道实例

图 9-7



如上图，是一个使用 ISATAP 隧道的典型拓扑，ISATAP 隧道主要用于 IPv4 站点内部被隔离的 IPv4/IPv6 双栈主机之间进行通信，而 ISATAP 设备在 ISATAP 站点中的主要功能有 2 个：

接收站内 ISATAP 主机发来的路由器请求报文后应答路由器公告报文用来提供给站点内的 ISATAP 主机进行自动配置。

负责站点内的 ISATAP 主机和站点外的 IPv6 主机转发报文的功能

上图中当 Host A 和 Host B 发送路由器请求给 ISATAP Router，ISATAP Router 将应答路由器公告报文，主机收到该报文后进行自动配置同时也会生成各自的 ISATAP 地址。之后 Host A 和 Host B 的 IPv6 通信将通过 ISATAP 隧道进行。当 Host A 或者 Host B 要与站点外的 IPv6 主机通信时，那么 Host A 先将该报文通过 ISATAP 隧道发送到 ISATAP 路由器 RT-A 上，然后由 RT-A 转发到 IPv6 网络上。

上图中 ISATAP Router（RT-A）的配置如下：

连接 IPv4 网络的接口

```
interface FastEthernet 0/1
no switchport
ip address 192.168.1.1 255.255.255.0
```

配置 ISATAP 隧道接口

```
interface Tunnel 1
tunnel mode ipv6ip isatap
tunnel source FastEthernet 0/1
ipv6 address 2005:1::/64 eui-64
no ipv6 nd suppress-ra
```

连接 IPv6 网络的接口

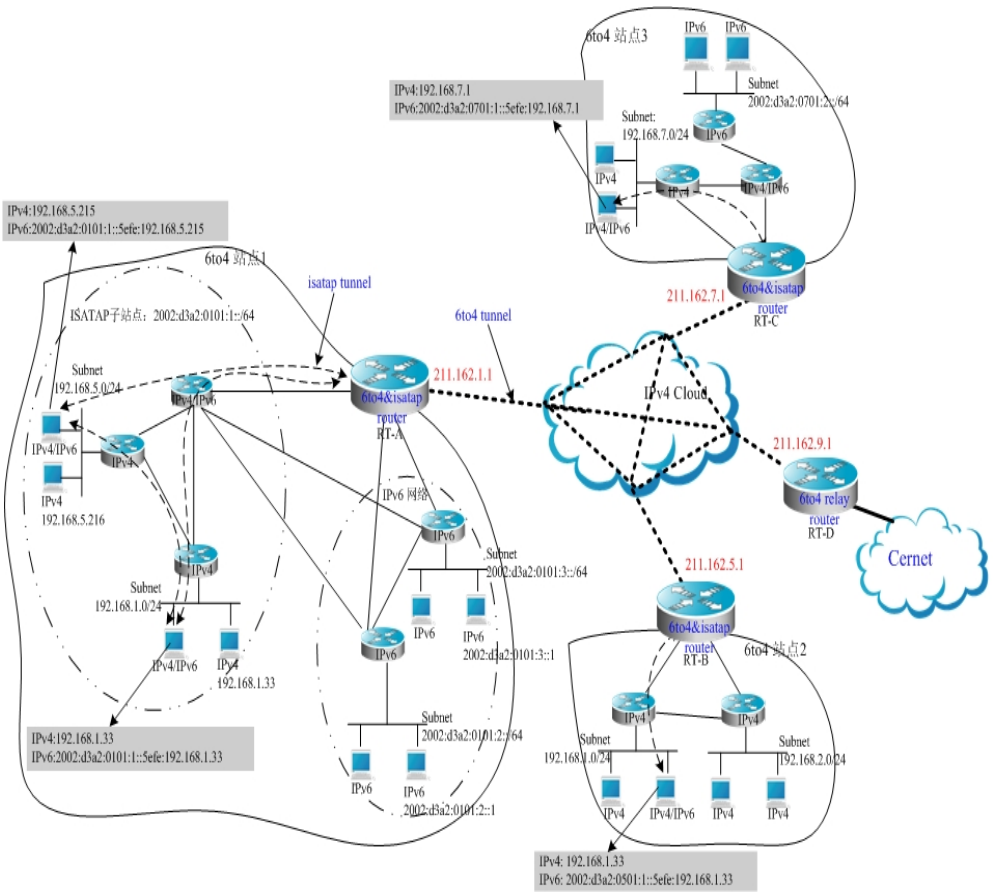
```
interface FastEthernet  0/2
no switchport
ipv6 address 3001::1/64
```

配置到 IPv6 网络的路由

```
ipv6 route 2001::/64 3001::2
```

9.4.5 配置ISATAP和 6to4 隧道综合应用实例

图 9-8



上图是一个6to4隧道和ISATAP隧道混合使用的例子。通过6to4隧道技术将各个6to4站点互联起来，并通过**6to4 relay router**将6to4站点接入Cernet网络，同时在6to4站点内部使用了ISATAP隧道技术，在站内被IPv4隔离的IPv6主机通过ISATAP隧道进行IPv6通信.

上图中所使用的全局 IP 地址包括 6to4 Relay 路由器的地址仅仅是为了举例方便，实际规划拓扑时应该使用真正的全局 IP 地址以及 6to4 Relay 的地址，目前有不少组织提供了免费公开的 6to4 Relay 路由器的地址.

下面分别介绍上图中 6to4 站点的边界路由器的配置，注意这里只列出相关的主要配置。

RT-A 的配置：

连接 Internet 网络的接口

```
interface GigabitEthernet 0/1
no switchport
ip address 211.162.1.1 255.255.255.0
```

连接站点内部的 IPv4 网络的接口

```
interface FastEthernet  0/1
no switchport
ip address 192.168.0.1 255.255.255.0
```

配置 ISATAP 隧道接口

```
interface Tunnel 1
tunnel mode ipv6ip isatap
tunnel source FastEthernet 0/1
ipv6 address 2002:d3a2:0101:1::/64 eui-64
no ipv6 nd suppress-ra
```

连接 IPv6 网络的接口 1

```
interface FastEthernet 0/2
no switchport
2002:d3a2:0101:10::1/64
```

连接 IPv6 网络的接口 2

```
interface FastEthernet  0/2
no switchport
2002:d3a2:0101:20::1/64
```

配置 6to4 隧道接口

```
interface Tunnel 2
tunnel mode ipv6ip 6to4
ipv6 enable
tunnel source GigabitEthernet 0/1
```

配置进 6to4 隧道的路由

```
ipv6 route 2002::/16 Tunnel 2
```

配置到 6to4 中继路由器 RT-D 的路由,以便可以访问 Cernet 网络

```
ipv6 route ::/0 2002:d3a2::0901::1
```

RT-B 的配置：

连接 Internet 网络的接口

```
interface GigabitEthernet 0/1
no switchport
ip address 211.162.5.1 255.255.255.0
```

连接站点内部的 IPv4 网络的接口 1

```
interface FastEthernet  0/1
no switchport
ip address 192.168.10.1 255.255.255.0
```

连接站点内部的 IPv4 网络的接口 2

```
interface FastEthernet  0/2
no switchport
ip address 192.168.20.1 255.255.255.0
```

配置 ISATAP 隧道接口

```
interface Tunnel 1
tunnel mode ipv6ip isatap
tunnel source FastEthernet 0/1
ipv6 address 2002:d3a2:0501:1::/64 eui-64
no ipv6 nd suppress-ra
```

配置 6to4 隧道接口

```
interface Tunnel 2
tunnel mode ipv6ip 6to4
ipv6 enable
tunnel source GigabitEthernet 0/1
```

配置进 6to4 隧道的路由

```
ipv6 route 2002::/16 Tunnel 2
```

配置到 6to4 中继路由器 RT-D 的路由,以便可以访问 Cernet 网络

```
ipv6 route ::/0 2002:d3a2::0901::1
```

RT-C 的配置：

连接 Internet 网络的接口

```
interface GigabitEthernet 0/1
no switchport
ip address 211.162.7.1 255.255.255.0
```

连接站点内部的 IPv4 网络的接口

```
interface FastEthernet 0/1
```

```
no switchport
ip address 192.168.0.1 255.255.255.0
```

配置 ISATAP 隧道接口

```
interface Tunnel 1
tunnel mode ipv6ip isatap
tunnel source FastEthernet 0/1
ipv6 address 2002:d3a2:0701:1::/64 eui-64
no ipv6 nd suppress-ra
```

连接 IPv6 网络的接口

```
interface FastEthernet 0/2
no switchport
2002:d3a2:0701:10::1/64
```

配置 6to4 隧道接口

```
interface Tunnel 2
tunnel mode ipv6ip 6to4
ipv6 enable
tunnel source GigabitEthernet 0/1
```

配置进 6to4 隧道的路由

```
ipv6 route 2002::/16 Tunnel 2
```

配置到 6to4 中继路由器 RT-D 的路由,以便可以访问 Cernet 网络

```
ipv6 route ::/0 2002:d3a2::0901::1
```

RT-D(6to4 Relay)的配置：

连接 Internet 网络的接口

```
interface GigabitEthernet 0/1
no switchport
ip address 211.162.9.1 255.255.255.0
```

连接 IPv6 网络的接口

```
interface FastEthernet 0/1
no switchport
2001::1/64
no ipv6 nd suppress-ra
```

配置 6to4 隧道接口

```
interface Tunnel 1
tunnel mode ipv6ip 6to4
ipv6 address 2002:d3a2::0901::1/64
tunnel source GigabitEthernet 0/1
```

配置进 6to4 隧道的路由

```
ipv6 route 2002::/16 Tunnel 1
```

10 网络通信检测工具

10.1 Ping连通性测试

为了测试网络的连通性，很多的网络设备都支持 Echo 协议，该协议包括发送一个特殊的数据包给指定的网络地址，然后等待该地址应答回来的数据包，通过 Echo 协议，可以评估网络的连通性、延时和网络的可靠性，利用 RGOS 提供的 Ping 工具，可以有效的帮助用户诊断、定位网络中的连通性问题。

Ping 命令运行在普通用户模式和特权用户模式下，在普通用户模式下，只能运行基本的 **Ping** 功能，而在特权用户模式下，还可以运行 Ping 的扩展功能。

命令	作用
Ruijie# **ping** [**ip**] [*address* [**length** *length*] [**ntimes** *times*] [**data** *data*][**source** *source*] [**timeout** *seconds*] [**df-bit**] [**validate**]]	**Ping**：网络连通性测试工具

普通的 Ping 功能，可以在普通用户模式和特权用户模式下执行，缺省将 5 个长度为 100Byte 的数据包发送到指定的 IP 地址，在指定的时间（缺省为 2 秒）内，如果有应答，则显示‘!’符号；如果没有应答，则显示‘.’符号。最后输出一个统计信息。以下为普通 ping 的实例：

```
Ruijie# ping 192.168.5.1
Sending 5, 100-byte ICMP Echoes to 192.168.5.1, timeout is 2 seconds:
< press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

扩展的 Ping 功能，只能在特权用户模式下执行。在扩展 Ping 中，可以指定发送数据包的个数、长度、超时的时间等等。和普通的 Ping 功能一样，最后也输出一个统计信息， 以下为一个扩展 Ping 的实例：

```
Ruijie# ping 192.168.5.197 length 1500 ntimes 100 data ffff source 192.168.4.190 timeout 3
Sending 100, 1500-byte ICMP Echoes to 192.168.5.197, timeout is 3 seconds:
  < press Ctrl+C to break >
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 2/2/3 ms
```

10.2 Ping IPv6 连通性测试

为了测试网络的连通性，很多的网络设备都支持 Echo 协议，该协议包括发送一个特殊的数据包给指定的网络地址，然后等待该地址应答回来的数据包，通过 Echo 协议，可以评估网络的连通性、延时和网络的可靠性，利用 RGOS 提供的 Ping 工具，可以有效的帮助用户诊断、定位网络中的连通性问题。

Ping ipv6 命令运行在普通用户模式和特权用户模式下，在普通用户模式下，只能运行基本的 **Ping ipv6** 功能，而在特权用户模式下，还可以运行 **Ping ipv6** 的扩展功能。

命令	作用

Ruijie# **ping ipv6** [*address* [**length** *length*] [**ntimes** *times*] [**data** *data*][**source** *source*] [**timeout** *seconds*]]	**Ping**：网络连通性测试工具

普通的 Ping 功能，可以在普通用户模式和特权用户模式下执行，缺省将 5 个长度为 100Byte 的数据包发送到指定的 IP 地址，在指定的时间（缺省为 2 秒）内，如果有应答，则显示‘!’符号；如果没有应答，则显示‘.’符号，如果应答的数据内容与请求的数据内容不匹配，则显示一个‘C’。最后输出一个统计信息。以下为普通 ping 的实例：

```
Ruijie# ping ipv6 2000::1
Sending 5, 100-byte ICMP Echoes to 2000::1, timeout is 2 seconds:
< press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

扩展的 Ping 功能，只能在特权用户模式下执行。在扩展 Ping 中，可以指定发送数据包的个数、长度、超时的时间等等。和普通的 Ping 功能一样，最后也输出一个统计信息， 以下为一个扩展 Ping 的实例：

```
Ruijie# ping ipv6 2000::1  length 1500 ntimes 100 data ffff source 2000::2 timeout 3
Sending 100, 1500-byte ICMP Echoes to 2000::1, timeout is 3 seconds:
  < press Ctrl+C to break >
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 2/2/3 ms
```

10.3 Traceroute连通性测试

执行 **Traceroute** 命令，可以显示数据包从源地址到目的地址，所经过的所有网关。**Traceroute** 命令主要用于检查网络的连通性，并在网络故障发生时，准确地定位故障发生的位置。

网络传输的规则是，一个数据包每经过一个网关，数据包中的 TTL 域的数据执行减 1 操作。当 TTL 域的数据为 0 时，该网关便丢弃这个数据包，并送回一个地址不可达的错误数据包给源地址。根据这个规则，**Traceroute** 命令的执行过程是：首先给目的地址发送一个 TTL 为 1 的数据包，第一个网关便送回一个 ICMP 错误消息，以指明此数据包不能被发送，因为 TTL 超时，之后将数据包的 TTL 域加 1 后重新发送，同样第二个网关返回 TTL 超时错误，这个过程一直继续下去，直到到达目的地址，记录每一个回送 ICMP TTL 超时信息的源地址，便记录下了数据从源地址到达目的地址，IP 数据包所经历的整个完整的路径。

Traceroute 命令可以在普通用户模式和特权用户模式下执行，具体的命令格式如下：

命令	作用
Ruijie# **traceroute** [**ip**] [*address* [**probe** *probe*] [**ttl** *minimum maximum*] [**source** *source*] [**timeout** *seconds*]]	跟踪数据包发送网络路径

以下为应用 Traceroute 的两个例子，一个为网络连接畅通，一个为网络连接存在某些网关不通的情况。

- 网络畅通的 Traceroute 例子：

```
Ruijie# traceroute 61.154.22.36
  < press Ctrl+C to break >
Tracing the route to 61.154.22.36
1       192.168.12.1        0 msec   0 msec   0 msec
2       192.168.9.2         4 msec   4 msec 4 msec
```

```
3       192.168.9.1          8 msec  8 msec  4 msec
4       192.168.0.10         4 msec  28 msec  12 msec
5       202.101.143.130     4 msec  16 msec  8 msec
6       202.101.143.154    12 msec  8 msec  24 msec
7       61.154.22.36        12 msec  8 msec  22 msec
```

从上面的结果可以清楚地看到，从源地址要访问 IP 地址为 61.154.22.36 的主机，网络数据包都经过了哪些网关（1－6），同时给出了到达该网关所花费的时间，这对于网络分析，是非常有用的。

■ 网络中某些网关不通的 Traceroute 例子：

```
Ruijie# traceroute 202.108.37.42
< press Ctrl+C to break >
Tracing the route to 202.108.37.42
1       192.168.12.1        0 msec  0 msec  0 msec
2       192.168.9.2         0 msec  4 msec 4 msec
3       192.168.110.1      16 msec  12 msec  16 msec
4       *  *  *
5       61.154.8.129        12 msec  28 msec  12 msec
6       61.154.8.17          8 msec  12 msec  16 msec
7       61.154.8.250        12 msec  12 msec  12 msec
8       218.85.157.222      12 msec  12 msec  12 msec
9       218.85.157.130      16 msec  16 msec  16 msec
10      218.85.157.77       16 msec  48 msec  16 msec
11      202.97.40.65        76 msec  24 msec  24 msec
12      202.97.37.65        32 msec  24 msec  24 msec
13      202.97.38.162       52 msec  52 msec  224 msec
14      202.96.12.38        84 msec  52 msec  52 msec
15      202.106.192.226     88 msec  52 msec  52 msec
16      202.106.192.174     52 msec  52 msec  88 msec
17      210.74.176.158     100 msec  52 msec  84 msec
18      202.108.37.42        48 msec  48 msec  52 msec
```

从上面的结果可以清楚地看到，从源地址要访问 IP 地址为 202.108.37.42 的主机，网络数据包都经过了哪些网关（1－17），并且网关 4 出现了故障。

10.4 Traceroute IPv6 连通性测试

执行 **Traceroute ipv6** 命令，可以显示数据包从源地址到目的地址，所经过的所有网关。**Traceroute ipv6** 命令主要用于检查网络的连通性，并在网络故障发生时，准确地定位故障发生的位置。

网络传输的规则请参考 **Traceroute** 小节。

Traceroute IPv6 命令可以在普通用户模式和特权用户模式下执行，具体的命令格式如下：

命令	作用

Ruijie# **traceroute ipv6** [*address* [**probe** *probe*] [**ttl** *minimum maximum*] [**source** *source*] [**timeout** *seconds*]]	跟踪数据包发送网络路径

以下为应用 Traceroute ipv6 的两个例子，一个为网络连接畅通，一个为网络连接存在某些网关不通的情况。

网络畅通的 Traceroute ipv6 例子：

```
Ruijie# traceroute ipv6 3004::1
  < press Ctrl+C to break >
Tracing the route to 3004::1
1       3000::1          0 msec  0 msec  0 msec
2       3001::1          4 msec  4 msec 4 msec
3       3002::1          8 msec  8 msec  4 msec
4       3004::1          4 msec  28 msec  12 msec
```

从上面的结果可以清楚地看到，从源地址要访问 IP 地址为 *3004::1* 的主机，网络数据包都经过了哪些网关（1—4），同时给出了到达该网关所花费的时间，这对于网络分析，是非常有用的。

■ 网络中某些网关不通的 Traceroute ipv6 例子：

```
Ruijie# traceroute ipv6 3004::1
  < press Ctrl+C to break >
Tracing the route to 3004::1
1       3000::1          0 msec  0 msec  0 msec
2       3001::1          4 msec  4 msec 4 msec
3       3002::1          8 msec  8 msec  4 msec
4       * * *
5       3004::1          4 msec  28 msec  12 msec
```

从上面的结果可以清楚地看到，从源地址要访问 IP 地址为 *3004::1* 的主机，网络数据包都经过了哪些网关（1—5），并且网关 4 出现了故障。

11 TCP

11.1 概述

TCP 模块为应用层提供了一个可靠的、有连接的基于 IP 的传输层协议。

应用层向 TCP 层发送用于网间传输的、用 8 位字节表示的数据流，然后 TCP 把数据流分割成适当长度的报文段，最大传输段大小（MSS）通常受该计算机连接的网络的数据链路层的最大传送单元（MTU）限制。之后 TCP 把结果包传给 IP 层，由它来通过网络将包传送给接收端实体的 TCP 层。

TCP 为了保证不发生丢包，就给每个字节一个序号，同时序号也保证了传送到接收端实体的包的按序接收。然后接收端实体对已成功收到的字节发回一个相应的确认(ACK)；如果发送端实体在合理的往返时延(RTT)内未收到确认，那么对应的数据（假设丢失了）将会被重传。

- 在数据正确性与合法性上，TCP 用一个校验和函数来检验数据是否有错误，在发送和接收时都要计算校验和；同时可以使用 md5 认证对数据进行加密。
- 在保证可靠性上，采用超时重传和捎带确认机制。
- 在流量控制上，采用滑动窗口协议，协议中规定，对于窗口内未经确认的分组需要重传。
- 在拥塞控制上，采用广受好评的 TCP 拥塞控制算法（也称 AIMD 算法）。该算法主要包括三个主要部分：1）加性增、乘性减；2）慢启动；3）对超时事件做出反应。

11.2 配置TCP

11.2.1 修改建立TCP连接的超时时间

建立 TCP 连接需要经过三次握手：主动端先发送 SYN 报文，被动放回应 SYN+ACK 报文，然后主动端再回应 ACK。

- 在主动端发送 SYN 后，如果被动端一直不回应 SYN+ACK 报文，主动端会不断的重传 SYN 报文直到超过一定的重传次数或超时时间。
- 在主动端发送 SYN 后，被动端回应 SYN+ACK 报文，但主动端不再回复 ACK，被动端也会一直重传直到超过一定的重传次数或超时时间。（SYN 报文攻击会出现这种情况）

可以通过以下命令配置 SYN 报文的超时时间（发送 SYN 报文到三次握手成功的最大时间），也就是建立 TCP 连接的超时时间。

命令	作用
Ruijie(config)# **ip tcp syntime-out** *seconds*	修改建立 TCP 连接的超时时间。 单位秒，取值范围 5-300，缺省值 20

使用 **no ip tcp syntime-out** 命令恢复参数缺省值。

☑ 本命令仅对 IPv4 TCP 生效。

11.2.2 修改缓冲区大小

TCP 的接收缓冲区是用来缓存从对端接收到的数据，这些数据后续会被应用程序读取。一般情况下，TCP 报文的窗口值反映接收缓冲区的空闲空间的大小。对于带宽比较大、有大批量数据的连接，增大接收缓冲区的大小可以显著提供 TCP 传输性能。TCP 的发送缓冲区是用来缓存应用程序的数据，发送缓冲区的每个字节都有序列号，被应答确认的序列号对应的数据会从发送缓冲区删除掉。增大发送缓冲区可以提高 TCP 跟应用程序的交互能力，也因此会提高性能。但是增大接收和发送缓冲区会导致 TCP 占用比较多的内存。

命令	作用
Ruijie(config)# **ip tcp window-size** *size*	修改 TCP 连接的接收和发送缓冲区大小。 单位字节，取值范围 0-65535，缺省值 4096。

使用 **no ip tcp window-size** 命令恢复接收和发送缓冲区大小为缺省值。

☑ 本命令只支持 IPv4 TCP。

🕮 本命令对于已经存在的 TCP 连接不生效，只对新建立的 TCP 连接生效。

🕮 本命令对接收缓冲区和发送缓冲区同时生效。

11.2.3 禁止端口不可达时的重置报文

TCP 模块在分发 TCP 报文时，如果找不到该报文所属的 TCP 连接会主动回复一个 reset 报文以终止对端的 TCP 连接。攻击者可能利用大量的端口不可达的 TCP 报文对设备进行攻击。

可以使用以下命令禁止/恢复在收到端口不可达的 TCP 报文时发送 reset 报文。

命令	作用
Ruijie(config)# **ip tcp not-send-rst**	禁止在接收到端口不可达的 TCP 报文时发送 reset 报文。

使用 **no ip tcp not-send-rst** 命令恢复发送 reset 报文。

☑ 本命令仅对 IPv4 TCP 生效。

11.2.4 限制TCP连接的MSS的最大值

MSS 是最大传输段大小的缩写，指一个 TCP 报文的数据载荷的最大长度，不包括 TCP 选项。

在 TCP 建立连接的三次握手中，有一种很重要的工作那就是进行 MSS 协商。连接的双方都在 SYN 报文中增加 MSS 选项，其选项值表示本端最大能接收的段大小，即对端最大能发送的段大小。连接的双方取本端发送的 MSS 值和接收对端的 MSS 值的较小者作为本连接最大传输段大小。

发送 SYN 报文时的 MSS 选项值的计算方法如下。

- 非直连网络中：mss = 默认值 536。
- 直连网络中：mss = 对端 ip 地址对应的出口的 MTU - 20 字节 ip 头 - 20 字节 tcp 头。
  一般来说如果出口配置的某些应用影响了接口的 mtu，那么该应用会相应的设置 mtu，如隧道口，vpn 口等。

10.4(3)的直连网络中被动连接方回复的syn+ack报文的mss选项值并不是通过mtu计算出来，而是采用默认值536。

计算出来的 mss 不能超过接收缓冲区的大小并且不能超过用户配置的 **ip tcp mss** 大小，如果超过取最小者。

如果该连接支持某些选项，那么 mss 还要减去选项 4 字节对齐后的长度值。如 md5 选项要减去 20 字节，md5 选项长度 18 字节，对齐后 20 字节。

到这里得到的 rmss 值就是要发送的 syn 报文 mss 选项的值。举例：一般情况下在直连网络中建立 bgp 邻居，那么该连接的发送的 mss 为 1500 – 20 – 20 – 20 = 1440。

ip tcp mss 命令的作用是限制即将建立的 TCP 连接的 MSS 的最大值。任何新建立的连接协商的 MSS 值不能超过配置的值。

命令	作用
Ruijie(config)# **ip tcp mss** *max-segment-size*	限制 TCP 连接的 MSS 的最大值。 单位为字节，取值范围 68-10000。

使用 **no ip tcp mss** 命令取消此限制。

本命令仅对 IPv4 TCP 生效。

11.2.4.1 启用PMTU发现功能

TCP 的路径最大传输单元（PMTU）发现功能是按 RFC1191 实现的，这个功能可以提高网络带宽的利用率。当用户使用 TCP 来批量传输大块数据时，该功能可以使传输性能得到明显提升。

命令	作用
Ruijie(config)# **ip tcp path-mtu-discovery** [**age-timer** *minutes* **| age-timer infinite**]	启用 PMTU 发现功能。 **age-timer** *minutes*：TCP 在发现 PMTU 后，重新进行探测的时间间隔。单位分钟，取值范围 10-30。缺省值 10。 **age-timer infinite**：TCP 在发现 PMTU 后，不重新探测。

按 RFC1191 的描述，TCP 在发现 PMTU 后，隔一段时间可以使用更大的 MSS 来探测新的 PMTU。这个时间间隔就是使用参数 **age-timer** 来指定。当设备发现的 PMTU 比 TCP 连接两端协商出来的 MSS 小时，设备就会按上述配置时间间隔，去尝试发现更大的 PMTU。直到 PMTU 达到 MSS 的值，或者用户停止这个定时器，这个探测过程才会停止。停止这个定时器，使用 **age-timer infinite** 参数。

使用 **no ip tcp path-mtu-discovery** 命令关闭 PMTU 发现功能。

本命令针对 IPv4 和 IPv6 的 TCP 同时生效。

此功能的启用与关闭，对于已经存在的 TCP 连接不生效，只对新建立的 TCP 连接生效。

11.3 监视与维护

命令	作用
Ruijie# **show tcp connect**	显示系统当前 TCP 连接的基本信息
Ruijie# **show tcp pmtu**	显示 TCP PMTU 的信息

Ruijie# **show tcp port**	显示系统当前 TCP 端口使用情况

12 IPv4 快转

12.1 概述

为了适应更高端设备的需要，目前我们使用了(Prefix Tree+Adjacency) 的 Express Forwarding 模型来实现快转。如果设备只缓存核心路由表的部分信息，当出现 Cache 失效时，需要中央 CPU 再次添加 Cache。Express Forwarding 构造了整个核心路由表的镜像，减少了对 CPU 的冲击，也保证了路由性能的稳定性。

Express Forwarding 用以下两个部件来构造路由表的镜像：

- Prefix Tree

前缀树。这是一棵根据最长匹配原则组织的 IP 前缀树，用于检索邻接节点。在实现中，用于构造 Prefix Tree 的数据结构一般与核心路由表的 Radix Tree 不同，而是使用了一种称为 M-Tries Tree 的数据结构来实现更快的多步查找。用 M-Tries Tree 构造 Prefix Tree 会比用 Radix Tree 消耗更多的内存空间，更新 Prefix 和节点信息也会相对耗时，但却能获得很高的检索性能。

- Adjacency

邻接节点。包含了被路由报文的输出接口信息，例如下一跳列表、下一处理部件、链路层输出封装等信息。当报文与该邻接节点匹配时，直接对报文进行封装，而后调用该节点的发送函数即可实现转发。为了便于检索和更新，邻接节点构成的表一般组织成哈希表的形式；为了支持路由负载均衡，邻接节点的下一条列表信息被组织为负载均衡表的形式；邻接节点中也可以不包含下一跳信息，也可以包含下一处理部件的索引号（例如其它线卡，多业务卡）。

Express Forwarding 路由分为三个步骤：

7) Express Forwarding 对报文解封装；

8) 用 Prefix Tree 来检索其报文路由所要输出的邻接节点；

9) 匹配到输出邻接节点后，再根据领接节点的信息确定报文的最终输出接口，然后在根据输出接口类型进行封装。

☑ 在目前的三层交换机上，IP 报文的转发主要通过交换芯片实现，因此需要将这种转发信息下载到交换芯片，实现硬件快转。IP 快转模块负责维护路由转发信息，并向向交换芯片写入转发信息，但不负责数据转发。

12.1.1 使能快转报文检验功能

使能快转报文检验功能。用于检验 IP 报文目的地址是否包含非法地址，非法地址包括 3 类地址：1、全 0 的地址；2、第 1 个字节是 127 的地址；3、E 类地址（排除 255.255.255.255）。

为了提高性能，默认关闭了快转报文检验功能。

在全局配置模式中执行以下命令：

命令	作用
Ruijie(config)# **ip ref check**	使能快转报文检验功能。
Ruijie(config)#**no ip ref check**	关闭快转报文检验功能。

12.2 快转表维护与监控

快转模块只是被动地接收并维护外部路由信息，本身不会主动添加或删除某些任何路由信息，所以快转内部更多的是提供当前的路由统计信息。

12.2.1 全局统计信息

全局统计信息就是指当前快转表中几种数据结构相关信息，包括当前路由条数、邻接节点个数、负载均衡表个数、权重节点个数。

命令	作用
show ip ref	显示当前快转中的统计信息

12.2.2 错误报文信息

对于目的地址包含非法地址的 IP 报文，存储在缓存区中。非法地址包括 3 类地址：1、全 0 的地址；2、第 1 个字节是 127 的地址；3、E 类地址（排除 255.255.255.255）。该命令可以显示记录在缓存中的目的地址包含非法地址的 IP 报文。

命令	作用
show ip logging [clear]	显示存储在缓存区中的目的地址包含非法地址的 IP 报文；使用 clear 命令清除缓存区内容。

12.2.3 邻接表信息

快转表中，一类重要的数据结就是邻接表。我们可以通过以下命令来查看当前的邻接信息：

命令	作用
show ip ref adjacency [**glean** | **local** | **ip** | {**interface** *interface_type interface_number)*]	可以指定显示集合邻接、本地邻接、指定 IP 对应邻接、指定接口关联邻接及所有邻接节点相关信息。

当以下情况出现时，报文转发的依据是邻接表。

- 直连路由，如：1.1.0.0/16　vlan1
- 比以上直连路由掩码更长的路由，如 1.1.1.0/24 vlan2 2.2.2.2
- 存在以上直连路由的邻居，如：1.1.1.1

目标 ip 地址为 1.1.1.1 的报文按邻接 1.1.1.1 的信息转发。因为 1.1.1.1/32 是最长匹配。

12.2.4 快转表路由信息

快转接收外部路由通告，维护自己的快转表，该快转表是核心路由表的一个镜象，其中的路由信息是相同的。通过下面的命令来显示快转表相关路由信息：

命令	作用

show ip ref route [**default** | {*ip mask*}]	显示当前快转表中的默认路由信息；如未指定默认路由，则显示快转表中所有路由信息，包括 0 路由、默认路由与普通的网关路由。

12.2.5 把快转表同步到硬件转发表

三层交换机常常因为软件转发表中路由总数超过硬件转发表容量或者硬件哈希桶冲突，出现硬件转发表和软件转发表不一致的问题。如果软件转发表中路由总数超过硬件转发表容量，用户应该想方设法减少路由数量，然后执行特权模式命令**“ip ref synchronize all** “把软件转发表同步到硬件转发表。

命令	作用
Ruijie# **ip ref synchronize all**	当软件转发表和硬件转发表不一致的时候，可以执行这条命令进行同步。

交换机在硬件转发表容量不足或者其他原因添加失败时，会以日志的形式打印该事件，其格式为：EFHW-4-(TBL_NO_RESOURCE): DESCRIPTION.

☑ 三层交换机主要使用硬件转发单播报文。

12.3 配置交换机快转ECMP/WCMP策略

在交换机中硬件转存在 ECMP/WCMP 路由时，同样也存在负载均衡策略。当该路由存在多个下一跳时，硬件能够依据我们设定的策略来选择其中一个下一跳。

该策略可以表达为：HASH(KEY(SIP,[DIP] [TCP/UDP Port] [UDF]))

该表达式解释为：通过对一个关键字进行 Hash 运算，采用运算出来的值来选择下一跳。其中能够设定的策略包括两个方面：一方面是：HASH 算法的选择，硬件能提供 2 种选择：CRC32_Upper 和 CRC32_Lower。另外一个方面是：KEY。可以通过选择报文的某些字段来组成 KEY，默认情况下仅选择源 IP 地址(SIP)。同时也能够增加选择 TCP/UDP 报文的对应端口的值、报文的目的 IP(DIP)、用户自定义值来参与 KEY 的组成。

命令	作用
Ruijie(config)# **ip ref ecmp load-balance** {[**crc32_lower** |**crc32_upper**] [**dip**] [**port**] [**udf** *number*]}	采用 DIP，Port，UDF 的任意组合参与 Key 的生成。并且选择 CRC32_Lower 或者 CRC32_Upper 其中一种作为 Hash 算法。
Ruijie(config)# **no ip ref ecmp load-balance** {[**crc32_lower** | **crc32 upper**] [**dip**] [**port**] [**udf** *number*]}	no 命令将在系统保存设置的基础上除去 no 命令中所带的关键字作为 Key 的组成部分。 比如系统保存设置为 SIP + DIP + Port。 **no ip ref ecmp route dip port** 命令执行后，参与 Key 组成的成员就只有 SIP 一个了。如果 no 命令后接的成员并不在系统保存设置中，执行该命令不会出现错误。

配置指南-IP 路由

本分册介绍 IP 路由配置指南相关内容，包括以下章节：

1. 协议无关
2. RIP
3. RIPng
4. 策略路由
5. VRF

1 协议无关

1.1 开启IP路由功能

缺省情况下，IP/IPv6 路由功能开启。

命令	作用
Ruijie(config)# **ip routing**	开启 IPv4 路由功能
Ruijie(config)# **ipv6 unicast-routing**	开启 IPv6 路由功能

配置对应的 **no** 命令，可以关闭 IP/IPv6 路由功能。

1.2 配置静态路由

静态路由就是手工配置的路由，使报文沿手工指定的路径传送到目标地。可以同时配置多条静态路由。如果配置的静态路由条目达到了指定的上限，则不能再添加新的静态路由。

命令	作用
Ruijie(config)# **ip route** [**vrf** *vrf_name*] *network net-mask* { *ip-address* | *interface* [*ip-address*] } [*distance*] [**tag** *tag*] [**permanent**] [**weight** *number*] [**description** *description-text*] [**disable** | **enable**]	配置 IPv4 静态路由。
Ruijie(config)# **ipv6 route** *ipv6-prefix / prefix-length* { *ipv6-address* | *interface* [*ipv6-address*] } [*distance*] [**weight** *number*]	配置 IPv6 静态路由。
Ruijie(config)# **ip static route-limit** *number*	配置 IPv4 静态路由条目数的上限。
Ruijie(config)# **ipv6 static route-limit** *number*	配置 IPv6 静态路由条目数的上限。

配置对应的 **no** 命令，可以删除已配置的静态路由，或取消静态路由条目数的上限。

如果没有执行删除动作，锐捷产品将永久保留静态路由。但是用户可以用动态路由协议学到的更好路由来替代静态路由，更好的路由是指管理距离更小的距离，包括静态路由在内所有的路由都携带管理距离的参数。以下为锐捷产品各种来源路由的管理距离表：

路由来源	缺省管理距离值
直连网络	0
静态路由	1
RIP 路由	120
不可达路由	255

当一个接口属于“down”状态时，所有指向该接口的路由将全部从路由表中消失。另外，当锐捷产品找不到静态路由下一跳地址的转发路由时，该静态路由也会从路由表中消失。

指定 VRF 的静态路由添加到对应的 VRF 中，如果同时指定了出口，但是出口所属的 VRF 和指定 VRF 不符合，将不会添加成功，如果没有指定 VRF，则默认添加到全局路由表中。

静态路由的默认权重为 1，可以使用 **show ip route weight** 命令查看非默认权重的静态路由。权重参数 weight 用于实现 WCMP 功能，当存在负载均衡路由可到达某地址时，交换机会根据各条路由的权重值分配数据流量，weight 较大的路由会分担较多的数据报文，较小者会分担较少的数据报文。路由器的 WCMP 限制一般为 32，而交换机则由于各款芯片所能支持的权重不同，所以其 WCMP 限制数量与型号有关；具体型号的路由权重值，请参考产品规格书。

当负载均衡路由的权重之和大于 WCMP 限制时，超出限制的路由不会生效。例如，如果某设备上 WCMP 限制为 8，那么下面两条静态路由配置中，只有一条会生效：

```
Ruijie(config)#ip route 10.0.0.0 255.0.0.0 172.0.1.2 weight 6
Ruijie(config)#ip route 10.0.0.0 255.0.0.0 172.0.1.4 weight 6
Ruijie(config)#show ip route 10.0.0.0

Routing entry for 10.0.0.0/8
  Distance 1, metric 0
  Routing Descriptor Blocks:
  *172.0.1.2, generated by "static"
Ruijie(config)#show ip route weight

------------[distance/metric/weight]-----------
S    10.0.0.0/8 [1/0/6] via 172.0.1.2
```

静态路由数默认最大值 1024，如果配置的静态路由数已经超过了指定的上限，则不会自动删除，但是添加不进来。

若要查看 IP 路由配置情况，可以使用 **show ip route** 命令查看 IP 路由表。

在配置 IPv4 静态路由时，可以对该路由进行描述，比如：这条路由是去上海的，等等。

1.3 配置缺省路由

不是所有的设备都有一张完整的全网路由表，为了使每台设备能够处理所有包的路由转发，通常的做法是功能强大的网络核心设备具有完整的路由表，其余的设备将缺省路由指向核心设备。缺省路由可以通过动态路由协议进行传播，也可以在每台设备上进行手工配置。

手工配置缺省路由的方法：

- 缺省静态路由
- 缺省网络
- 将缺省路由引入路由协议

1.3.1 配置静态缺省路由

配置命令参见前文“配置静态路由”。

- 在 IPv4 网络中配置缺省路由，目的地址与掩码为全零。
- 在 IPv4 网络中配置缺省路由，指定目的地址为::/0（前缀长度为 0）。

1.3.2 配置缺省网络

配置缺省网络，在全局命令配置模式中执行以下命令：

命令	作用
Ruijie(config)# **ip default-network network**	配置缺省网络
Ruijie(config)# **no ip default-network network**	删除缺省网络

通过 **default-network** 产生缺省路由只要满足以下条件即可，即该缺省网络不是直连接口网络，但在路由表中可到达。

当设备有缺省路由时，不管是动态路由协议学习到的还是手工配置产生的，当执行 **show ip route** 命令时，路由表中的“gateway of last resort”会显示最后网关的信息。一个路由表可能会有多条网络路由为候选缺省路由，但只有最好的缺省路由才能成为“gateway of last resort”。

1.3.3 将缺省路由引入路由协议

在一台路由器上配置“将缺省路由引入路由协议”后，该路由器会将缺省路由通告给其它路由器，其它路由器在自己的路由表里生成指向这台路由器的缺省路由。

要将缺省路由引入路由协议，在路由进程配置模式中执行以下命令：

命令	作用
Ruijie(config-router)# **default-information originate** [**always**] [**metric** *metric*] [**route-map** *map-name*]	将缺省路由引入路由协议进程并进行通告。 always：无论本地路由表是否存在缺省路由，都引入一条缺省路由。 metric：对引入的缺省路由的 metric 值进行设置 route-map：对引入缺省路由进行过滤和设置

使用对应的 **no** 命令，可以取消将缺省路由引入路由协议进程。

1.4 配置ECMP/WCMP策略

在存在冗余链路的网络环境中，到达同一目的地址的路由可能存在多个下一跳。按照传统的路由技术，发往目的地址的报文只能利用其中的一条链路，其它链路都处于备份状态或无效状态。一旦当前链路故障，链路切换也需要一定时间。锐捷产品支持 ECMP 和 WCMP 技术，可以充分利用冗余链路、部署流量策略。

- ECMP（Equal-Cost Multipath Routing，等价多路径）使设备能够同时使用该路由的每条链路，平均分配流量，且无时延无丢包地完成链路切换。
- WCMP（Weighted Cost Multipath，加权多路径）使设备能够同时使用该路由的每条链路，按权重分配流量，且无时延无丢包地完成链路切换。用户可以根据链路出口带宽或其他因素设置路由权重。

通过配置 ECMP/WCMP 策略，可以改变 ECMP 和 WCMP 在多条链路上分配流量的办法。ECMP/WCMP 策略的实现方法：以报文的某些字段作为关键字，通过 hash 算法选择下一跳。

hash 关键字

- SIP [21:16] [5:0] ：源 IP 地址，第 0 位到第 5 位，第 16 位到第 21 位。
- DIP [21:16] [5:0] ：目的 IP 地址，第 0 位到第 5 位，第 16 位到第 21 位。
- MAC SA [5:0] ：源 MAC 地址，第 0 位到第 5 位。
- MAC DA [5:0] ：目的 MAC 地址，第 0 位到第 5 位。
- L4 sport [13:8] [5:0] ：四层源端口号，第 0 位到第 5 位，第 8 位到第 13 位。
- L4 dport [13:8] [5:0] ：四层目的端口号，第 0 位到第 5 位，第 8 位到第 13 位。
- src port [5:0] ：报文进入的源端口号，第 0 位到第 5 位。若入口为 AP 口，则为 AP 的硬件 ID 号；否则，为物理端口的硬件 ID 号。

hash 算法

支持如下 8 种算法，缺省选用 src-dst-mac 算法。

- src-ip：根据报文的源 IP 进行流量分配。源 IP 不同的流量通过不同的下一跳，源 IP 相同的流量通过相同的下一跳。
- dst-ip：根据报文的源 IP 进行流量分配。目的 IP 不同的流量通过不同的下一跳，目的 IP 相同的流量通过相同的下一跳。
- src-dst-ip：根据报文的源 IP 与目的 IP 进行流量分配。（源 IP，目的 IP）不同的流量通过不同的下一跳，（源 IP，目的 IP）相同的流量通过相同的下一跳。
- src-mac：根据报文的源 MAC 进行流量分配。源 MAC 不同的流量通过不同的下一跳，源 MAC 相同的流量通过相同的下一跳。
- dst-mac：根据报文的源 MAC 进行流量分配。目的 MAC 不同的流量通过不同的下一跳，目的 MAC 相同的流量通过相同的下一跳。
- src-dst-mac：根据报文的源 MAC 与目的 MAC 进行流量分配。（源 MAC，目的 MAC）不同的流量通过不同的下一跳，（源 MAC，目的 MAC）相同的流量通过相同的下一跳。
- src-port：根据报文的输入端口进行流量分配。（源端口）不同的流量通过不同的下一跳，（源端口）相同的流量通过相同的下一跳。
- src-dst-ip-l4port：根据报文的源 IP，目的 IP，四层源端口以及四层目的端口进行流量分配。（源 IP,目的 IP，四层源端口号，四层目的端口）不同的流量通过不同的下一跳，（源 IP,目的 IP，四层源端口号，四层目的端口）相同的流量通过相同的下一跳。

配置 ECMP/WCMP 策略

命令	作用

Ruijie(config)# **aggregateport load-balance** { **src-mac** | **dst-mac** | **src-dst-mac** | **src-ip** | **dst-ip** | **src-dst-ip** | **src-port** | **src-dst-ip-l4port** }	配置 ECMP/WCMP 策略。 src-ip：根据报文的源 IP 来分配流量。 dst-ip：根据报文的目的 IP 来分配流量。 src-dst-ip：根据报文的源 IP 与目的 IP 来分配流量。 src-mac：根据报文的源 MAC 来分配流量。 dst-mac：根据报文的目的 MAC 来分配流量。 src-dst-mac：根据报文的源 MAC 与目的 MAC 来分配流量。 src-port：根据报文的输入端口进行流量分配。 src-dst-ip-l4port：根据报文的源 IP，目的 IP，四层源端口以及四层目的端口进行流量分配。

以上配置同时适用于 IPv4 和 IPv6。

使用相同的命令来配置 ECMP/WCMP 策略和 AP 流量平衡模式。如果设备上未配置 AP，此命令仅对 ECMP/WCMP 策略生效。

由于 ECMP 和 AP 的流量平衡模式是统一控制的，当 ECMP 的下一跳出口是 AP 口的时候，会进行两次完全相同算法的计算，如果 ECMP 的下一跳出口数目和对应出口 AP 的成员口数目存在 1 以外的其他公约数（比如 ECMP 的下一跳出口数目为 2，AP 的下一跳出口数目为 4，则存在公约数 2；特别地，如果两者相等，会均衡最差），则会影响到两级的流量平衡（第一级 ECMP，第二级 AP）。要使得两级流量平衡效果较好，在部署时，要注意 ECMP 的下一跳出口数目和对应出口 AP 的成员口数目不能存在 1 以外的其他公约苏。

例：配置 ECMP/WCMP 策略，根据报文源 IP 与目的 IP 来分配流量。

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

1.5 限制等价路由中的路径数

一条等价路由中存在多条路径到达同一目标地址，路径之间可以冗余备份或负载均衡。

命令	作用
Ruijie(config)# **maximum-paths** *number*	设置等价路由中的最大路径数。缺省值 8

如果限制路径数为 1，则到达同一目标地址只存在一条路径，相当于取消了等价路由。

使用对应的 **no** 命令，恢复缺省值。

以上配置同时适用于 IPv4 和 IPv6。

1.6 多路由共享下一跳

如果两条路由的下一跳完全一样（所有下一跳都一致，包括 weight），则两个路由共享下一跳。这样可以节约硬件资源，但在删除路由或者更新路由的时候，可能由于硬件资源不足导致删除路由失败或者更新路由失败，从而删除掉整条路由。

当此情况发生时，会输出如下提示信息：

```
*Aug 24 11:20:39: %7: Warning: Because hardware resource is not enough, route:
*Aug 24 11:20:39: %7: 191.168.200.120/32 191.168.200.120
*Aug 24 11:20:39: %7: were deleted
```

1.7 配置路由图

路由图(**route-map**)是与具体路由协议无关的一种过滤策略集，提供给路由协议和策略路由使用。在路由协议中，用于路由信息的过滤和修改；在策略路由中，用于控制报文转发。

定义路由图

定义路由图，在全局配置模式中执行以下命令：

命令	作用
Ruijie(config)# **route-map** *route-map-name* [[**permit** | **deny**] *sequence*]	定义路由图，进入路由图配置模式
Ruijie(config)# **no route-map** *route-map-name* [{ **permit** | **deny** } *sequence*]	删除路由图

在路由图配置模式下，定义匹配规则和匹配后的操作。此时可以执行一个或多个的 **match** 命令和一个或多个的 **set** 命令。如果没有 **match** 命令，则匹配所有；如果没有 **set** 命令，则不做任何操作。

针对路由图的不同应用，支持的 **match** 命令与 **set** 命令可能不同。如下情况下会给予用户提示信息：

- 配置关联 **route-map** 的命令时，检查 **route-map** 所配置的 **match** 命令与 **set** 命令在当前所关联应用的适用情况，存在不适用情况时给予用户提示信息。
- 配置 **route-map**、**match** 命令或者 **set** 命令时，检查该 **route-map** 关联的所有应用对于 **route-map** 配置的所有 **match** 命令与 **set** 命令的适用情况，存在不适用情况时给予用户提示信息。

策略路由关联路由图的应用不支持上述信息提示功能。

定义匹配条件

要定义规则的匹配条件，在路由图配置模式中执行以下命令：

命令	作用
Ruijie(config-route-map)# **match interface** [*interface-type interface-number*]	匹配路由的下一跳接口
Ruijie(config-route-map)# **match ip address** *access-list-number* [*access-list-number*]	匹配访问列表中的地址
Ruijie(config-route-map)# **match ip next-hop** *access-list-number* [*access-list-number*]	匹配访问列表中的下一跳地址
Ruijie(config-route-map)# **match ip route-source** *access-list-number* [*access-list-number*]	匹配访问列表中的路由源地址
Ruijie(config-route-map)# **match ipv6 address** { *access-list-name* | **prefix-list** *prefix-list-name* }	匹配 IPv6 访问列表或前缀列表
Ruijie(config-route-map)# **match ipv6 next-hop** { *access-list-name* | **prefix-list** *prefix-list-name* }	匹配访问列表或前缀列表的下一跳地址

Ruijie(config-route-map)# **match ipv6 route-source** { *access-list-name* | **prefix-list** *prefix-list-name* }	匹配访问列表或前缀列表的路由源地址
Ruijie(config-route-map)# **match metric** *metric*	匹配路由的量度值 *Metric* ：0-4294967295
Ruijie(config-route-map)# **match route-type** { **local** | **internal** | { { **external** | **nssa-external** } [**type-1**] [**type-2**] } | [**level-1** | **level-2**] }	匹配路由的类型
Ruijie(config-route-map)# **match tag** *tag*	匹配路由的标记值 *tag* ：0-4294967295

定义匹配后的操作

要定义匹配后的操作，在路由图配置模式中执行以下命令：

命令	作用
Ruijie(config-route-map)# **set dampening** *half-life reuse suppress max-suppress-time*	设置路由的路由振荡参数
Ruijie(config-route-map)# **set ip next-hop** *ip-address* [*weight*] [*ip-address* [*weight*]]	设置下一跳 IP 地址
Ruijie(config-route-map)# **set ipv6 next-hop** *global-ipv6-address* [*weight*] [*global-ipv6-address* [*weight*]]	设置下一跳 IPv6 地址。
Ruijie(config-route-map)# **set metric** *metric*	设置重分布路由的量度值
Ruijie(config-route-map)# **set metric** [+ *metric-value* | - *metric-value* | *metric-value*]	设置重分布路由的类型
Ruijie(config-route-map)# **set next-hop** *next-hop*	设置重分布路由的下一跳 *next-hop*：下一跳的 IP 地址
Ruijie(config-route-map)# **set tag** *tag*	设置重分布路由的标记值

1.8 配置路由重分布

为了支持本设备能够运行多个路由协议进程，锐捷产品提供了路由信息从一个路由进程重分布到另外一个路由进程的功能。比如将静态路由重新分布后通告到 RIP 路由域中。

在路由重分布中，经常通过路由图（route maps）的应用，对两个路由域之间的路由相互分布进行有条件的控制。

在路由进程配置模式中执行以下命令：

命令	作用
Ruijie(config-router)# **redistribute** { **connected** | **static** } [**metric** *metric-value*] [**route-map** *route-map-name*]	进行重分布路由
Ruijie(config-router)# **default-metric** *metric*	给所有重分布路由设置缺省量度值

路由重分布很容易造成路由环路，在使用时应该谨慎。

1.9 配置路由过滤

路由过滤就是对进出站路由进行控制，使得设备只学到必要、可预知的路由，对外只向可信任的设备通告必要的、可预知的路由。路由的泄漏和混乱，是会影响网络运行的，因此特别是电信运营商和金融业务网络，是十分有必要配置路由过滤的。

控制路由更新通告

为了防止本地网络上的其它路由设备学到不必要的路由信息，可以通过控制路由更新通告来遏制指定路由的更新。

要遏制路由更新通告，在路由进程配置模式中执行以下命令:

命令	作用
Ruijie(config-router)# **distribute-list** { [*access-list-number* | *access-list-name*] **prefix** *prefix-list-name* } **out** [*interface-type interface-number* | *protocol*]	根据访问列表规则，允许或拒绝某些路由被分发出去。 **prefix**：前缀列表
Ruijie(config-router)# **no distribute-list** { [*access-list-number* | *access-list-name*] | **prefix** *prefix-list-name* } **out** [*interface-type interface-number* | *protocol*]	取消遏制路由更新通告

控制路由更新处理

为了避免处理进站路由更新报文的某些指定路由，可以配置该特性。

要控制路由更新处理，在路由进程配置模式中执行以下命令：

命令	作用
Ruijie(config-router)# **distribute-list** { [*access-list-number* | *access-list-name*] | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*] | **gateway** *prefix-list-name* } **in** [*interface-type interface-number*]	根据访问列表规则，允许或拒绝接收分发进来的指定的路由。 prefix：前缀列表 gateway：使用前缀列表根据路由的源进行对分发进来的路由进行过滤。
Ruijie(config-router)# **no distribute-list** { [*access-list-number* | *name*] | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*] | **gateway** *prefix-list-name* } **in** [*interface-type interface-number*]	取消控制路由更新处理

1.10 配置密钥链

通过密钥链管理认证密钥，为这些密钥指定 ID，认证串和发送接收方向上的生存期，每个密钥通过唯一的 ID 标识和保存。

要管理认证密钥，在全局配置模式中执行以下命令：

命令	作用
Ruijie(config)# **key chain** *key-chain-name*	配置密钥链
Ruijie(config-keychain)# **key** *key-id*	配置密钥

Ruijie(config-keychain-key)# **key-string** [**0 | 7**] *text*	配置认证串 0 指定密钥以明文显示 7 指定密钥以密文显示
Ruijie(config-keychain-key)# **accept-lifetime** *start-time* { **infinite** | *end-time* | **duration** *seconds* }	配置接收方向生存期
Ruijie(config-keychain-key)# **send-lifetime** *start-time* { **infinite** | *end-time* | **duration** *seconds* }	配置发送方向生存期
Ruijie(config-keychain-key)# **end**	退出密钥链密钥配置模式
Ruijie# **show key chain**	显示密钥链配置信息

1.11 配置举例

配置要求

一台设备，通过 RIP 与其它设备交换路由信息，另外还有 3 条静态路由，要求 RIP 重新分布静态路由，并且只允许通告 172.16.1.0/24、192.168.1.0/24 两条路由。

路由设备具体配置

这也是在实际应用中比较常见的路由过滤配置例子，通过配置分布列表来实现。另外注意以下配置中没有指定重分布路由的量度值，因为此处重分布的路由为静态路由，RIP 会自动分配量度值。RIP 配置中的版本指定与关闭自动汇总是必须的，因为访问列表中允许的路由是 172.16.1.0/24 的路由，RIP 要对外通告该路由，首先得支持无类路由的存在，而且在通告时不能被汇总成 172.16.0.0/16 网络。

配置静态路由

```
Ruijie(config)# ip route 172.16.1.0 255.255.255.0 172.200.1.2
Ruijie(config)# ip route 192.168.1.0 255.255.255.0 172.200.1.2
Ruijie(config)# ip route 192.168.2.0 255.255.255.0 172.200.1.4
```

配置 RIP

```
Ruijie(config)# router rip
Ruijie(config-router)# version 2
Ruijie(config-router)# redistribute static
Ruijie(config-router)# network 192.168.34.0
Ruijie(config-router)# distribute-list EXT_ACL out static
Ruijie(config-router)# no auto-summary
```

配置扩展 ACL

```
Ruijie(config)# ip access-list extended EXT_ACL
Ruijie(config-ext-nacl)#10 permit ip 192.168.1.0 0.0.0.255 any
Ruijie(config-ext-nacl)#10 permit ip 172.16.1.0 0.0.0.255 any
```

2 RIP

2.1 概述

RIP (Routing Information Protocol) 路由协议是一种相对古老，在小型以及同介质网络中得到了广泛应用的路由协议。RIP 采用距离向量算法，是一种距离向量协议。RIPv1 在 RFC 1058 文档中定义，RIPv2 在 RFC 2453 文档中定义，锐捷 RGOS 软件同时支持这两个版本。

RIP 使用 UDP 报文交换路由信息，UDP 端口号为 520。通常情况下 RIPv1 报文为广播报文；而 RIPv2 报文为组播报文，组播地址为 224.0.0.9。RIP 每隔 30 秒向外发送一次更新报文。如果设备经过 180 秒没有收到来自对端的路由更新报文则将所有来自此设备的路由信息标志为不可达，路由进入不可达状态后，120 秒内仍未收到更新报文就将这些路由从路由表中删除。

RIP 使用跳数来衡量到达目的地的距离，称为路由量度。在 RIP 中，设备到与它直接相连网络的跳数为 0；通过一个设备可达的网络的跳数为 1 ，其余依此类推；不可达网络的跳数为 16。

运行 RIP 路由协议的设备，可以从邻居学到缺省路由，也可以自己产生缺省路由。当满足以下条件之一，锐捷产品就可以通过 **default-information originate** 命令引入缺省路由，并通告给邻居设备：

- 配置了 **ip default-network**
- 其它路由协议学到缺省路由或配置了静态缺省路由

RIP 将向指定的网络接口发送更新报文，如果接口的网络没有与 RIP 路由进程关联，该接口就不会通告任何更新报文。RIP 有 RIPv1 和 RIPv2 两个版本，RIPv2 支持明文认证、MD5 密文认证和支持可变长子网掩码。

锐捷的 RIP 采用水平分割（Split Horizon）等手段防止形成环路路由。

2.2 配置RIP

RIP 配置任务列表如下：

- 创建 RIP 路由进程（必须）
- RIP 报文单播配置（可选）
- 水平分割配置（可选）
- 定义 RIP 版本（可选）
- 配置路由汇聚功能（可选）
- RIP 认证配置
- RIP 时钟调整（可选）
- RIP 路由源地址验证配置（可选）
- RIP 接口状态控制（可选）

- RIP 接口通告缺省路由（可选）
- RIP 接口通告超网路由（可选）
- RIP VRF 配置(可选)
- RIP BFD 配置(可选)
- RIP 触发扩展配置(可选)

关于以下主题的配置，请参见《协议无关配置》章节。

- 路由信息过滤
- 路由重分布
- 缺省路由分发配置

以下为 RIP 的缺省配置：

功能特性	缺省值
网络接口	接口加入 RIP 运行的情况下，缺省接收 RIPv1 和 RIPv2 报文，通告 RIPv1 报文。 在接口通告 RIPv1 报文的情况下： 缺省以广播方式发送报文； 缺省不通告超网路由； 在接口通告 RIPv2 报文的情况下： 缺省以多播方式发送报文； 缺省将路由自动汇聚成有类路由； 缺省通告超网路由。 缺省开启水平分割。
RIP 邻居	未定义 RIP 邻居
报文源地址验证	打开
定时器	缺省情况下： 更新时间为 30 秒； 无效时间为 180 秒； 清除时间为 120 秒。
偏移量列表	未定义偏移量列表
自动汇聚	打开
重分布	缺省不启用路由重分布 如果启用： 重分布 OSPF，则重分布该实例的所有子类型的路由； 重分布 ISIS，则重分布该实例的 level-2 子类型的路由； 其他情况下，重分布该类型的所有路由； 分发路由的 metric 值为缺省 metric 值。
缺省路由分发	缺省不启用分发缺省路由。 如果启用：分发路由的 metric 值为缺省 metric 值。
缺省 metric(default metric)	重分发其他协议的路由所使用的 metric 值，缺省值为 1。
管理距离	120

RIP 触发扩展	缺省不启用 RIP 触发扩展 如果启用： Update Request、Update Response 报文的重传时间间隔，缺省为 5 秒 Update Request、Update Response 报文的最大重传次数，缺省为 36 次
RIP GR	启用 Helper 功能

2.2.1 创建RIP路由进程

设备要运行 RIP 路由协议，首先需要创建 RIP 路由进程，并定义与 RIP 路由进程关联的网络。

要创建 RIP 路由进程，在全局配置模式中执行以下命令：

命令	作用
Ruijie(config)# **router rip**	创建 RIP 路由进程
Ruijie(config-router)#**network** *network-number wildcard*	定义关联网络

用户可以同时配置 *network-number* 和 *wildcard* 参数，使得在该地址范围内的接口地址网段参与 RIP 的运行。

如果未配置 *wildcard* 参数，RGOS 将默认按照有类地址范围来处理，使得在该有类地址范围内的接口地址网段参与 RIP 运行。

Network 命令定义的关联网络有两层意思：RIP 对外通告关联网络的路由信息；RIP 只通过关联网络的接口通告和接收路由更新信息。

2.2.2 配置RIP报文更新单播通告

RIP 通常为广播或组播协议，如果 RIP 路由信息需要通过非广播网传输，则需要配置设备，以便支持 RIP 利用单播通告路由信息更新报文。

要配置 RIP 报文更新单播通告，在 RIP 路由进程配置模式中执行以下命令：

命令	作用
Ruijie(conf-router)# **neighbor** *ip-address*	配置 RIP 报文单播通告

配合该命令的使用，用户还可以控制接口是否允许通告 RIP 路由更新报文，限制一个接口通告广播式的路由更新报文，需要在路由进程配置模式中配置 **passive-interface** 命令。关于路由信息通告限制的相关描述，请参见《协议无关配置》中的“路由过滤”章节。

在配置 FR、X.25 时，如果地址映射时指定了 Broadcast 关键字，则无需配置 **neighbor**。**Neighbor** 命令的作用更多体现在减少广播报文和路由过滤上。

2.2.3 配置水平分割

多台设备连接在 IP 广播类型网络上，又运行距离向量路由协议时，就有必要采用水平分割的机制以避免路由环路的形成。水平分割可以防止设备将某些路由信息从学习到这些路由信息的接口通告出去，这种行为优化了多个设备之间的路由信息交换。

然而对于非广播多路访问网络（如帧中继、X.25 网络），水平分割可能造成部分设备学习不到全部的路由信息。在这种情况下，可能需要关闭水平分割。如果一个接口配置了次 IP 地址，也需要注意水平分割的问题。

如果配置了 **poisoned-reverse** 参数，将启用带毒性逆转的水平分割，设备仍然会将路由信息从学习到这些路由信息的接口通告出去，但是将路由信息的度量值设置为不可达。

要配置关闭或打开水平分割，在接口配置模式中执行以下命令：

命令	作用
Ruijie(config-if)# **no ip rip split-horizon**	关闭水平分割
Ruijie(config-if)# **ip rip split-horizon**	打开水平分割

要配置关闭或打开带毒性逆转的水平分割，在接口配置模式中执行以下命令：

命令	作用
Ruijie(config-if)# **no ip rip split-horizon poisoned-reverse**	关闭带毒性逆转的水平分割
Ruijie(config-if)# **ip rip split-horizon poisoned-reverse**	打开带毒性逆转的水平分割

所有接口的默认行为设置为开启不带毒性逆转的水平分割。

2.2.4 定义RIP版本

锐捷产品支持 RIP 版本 1 和版本 2，RIPv2 可以支持认证、密钥管理、路由汇聚、CIDR 和 VLSMs。其中密钥管理、VLSMs 描述请参见《协议无关配置》。

缺省情况下，锐捷产品可以接收 RIPv1 和 RIPv2 的数据包，但是只发送 RIPv1 的数据包。用户可以通过配置，只接收和发送 RIPv1 的数据包，也可以只接收和发送 RIPv2 的数据包。

要配置软件只接收和发送指定版本的数据包，在路由进程配置模式中执行以下命令：

命令	作用
Ruijie(config-router)# **version** {**1** | **2**}	定义 RIP 版本

以上命令使软件缺省情况下只接收和发送指定版本的数据包，如果需要可以更改每个接口的缺省行为。

要配置接口只发送哪个版本的数据包，在接口配置模式中执行以下命令：

命令	作用
Ruijie(config-if)# **ip rip send version 1**	指定只发送 RIPv1 数据包
Ruijie(config-if)# **ip rip send version 2**	指定只发送 RIPv2 数据包
Ruijie(config-if)# **ip rip send version 1 2**	指定只发送 RIPv1 和 RIPv2 数据包

要配置接口只接收哪个版本的数据包，在接口配置模式中执行以下命令：

命令	作用
Ruijie(config-if)# **ip rip receive version 1**	指定只接收 RIPv1 数据包
Ruijie(config-if)# **ip rip receive version 2**	指定只接收 RIPv2 数据包
Ruijie(config-if)# **ip rip receive version 1 2**	指定只接收 RIPv1 和 RIPv2 数据包

2.2.5 配置路由汇聚功能

RIP 路由自动汇聚，就是当子网路由穿越有类网络边界时，将自动汇聚成有类网络路由。RIPv2 缺省情况下将进行路由自动汇聚，RIPv1 不支持该功能。

RIPv2 路由自动汇聚的功能，提高了网络的伸缩性和有效性。如果有汇聚路由存在，在路由表中将看不到包含在汇聚路由内的子路由，这样可以大大缩小路由表的规模。

通告汇聚路由会比通告单独的每条路由更有效率，主要有以下因素：

- 当查找 RIP 数据库时，汇聚路由会得到优先处理；
- 当查找 RIP 数据库时，任何子路由将被忽略，减少了处理时间。

有时可能希望学到具体的子网路由，而不愿意只看到汇聚后的网络路由，这时需要关闭路由自动汇聚功能。

要配置路由自动汇聚，在 RIP 路由进程模式中执行以下命令：

命令	作用
Ruijie(config-router)# **no auto-summary**	关闭路由自动汇聚
Ruijie(config-router)# **auto-summary**	打开路由自动汇聚

还可以配置接口级汇聚，在某个接口下配置路由汇聚到指定的有类子网范围，在接口模式下执行以下命令：

命令	作用
Ruijie(config-if)# **ip rip summary-address** *ip-address ip-network-mask*	配置接口级路由汇聚
Ruijie(config-if)# **no ip rip summary-address** *ip-address ip-network-mask*	取消接口级路由汇聚

2.2.6 配置RIP认证

RIPv1 不支持认证，如果设备配置 RIPv2 路由协议，可以在相应的接口配置认证。

锐捷产品的 RIPv2 支持两种认证方式：明文认证和 MD5 认证。缺省的认证方式为明文认证。

如果要使用明文认证，用户可以直接使用 **ip rip authentication text-password** 方式配置明文认证字符串，也可以通过关联密钥串获取明文认证字符串，后者优先级高于前者。

如果要使用 MD5 认证，必须通过关联密钥串进行 MD5 认证。

如果采用明文认证，但未配置明文认证字符串，或者未配置关联密钥串，此时并不会有认证行为发生。同样，如果采用 MD5 认证，但未配置关联密钥串，也不会有认证行为发生。

如果密钥串在接口配置中指定了，请使用 **key chain** 全局配置命令进行该密钥串的定义，否则将可能导致 RIP 数据包认证失败。

要配置 RIP 认证，在接口配置模式中执行以下命令：

命令	作用

Ruijie(config-if)# **ip rip authentication mode** {**text** | **md5**}	应用密钥串，启用 RIP 认证配置接口 RIP 认证。 text：明文认证。 md5：MD5 认证。
Ruijie(config-if)# **ip rip authentication text-password [0|7]** *password-string*	配置明文认证字符串，长度为 1～16 字节。 0 指定密钥以明文显示 7 指定密钥以密文显示
Ruijie(config-if)# **ip rip authentication key-chain** *key-chain-name*	配置使用密钥串进行认证。

2.2.7 调整RIP时钟

RIP 提供了时钟调整的功能，用户可以根据网络的具体情况进行时钟调整，使 RIP 路由协议能够运行得更好。可以对以下时钟进行调整：

- 路由更新时间：以秒计，定义了设备发送路由更新报文的周期；
- 路由无效时间：以秒计，定义了路由表中路由因没有更新而变为无效的时间；
- 路由清除时间：以秒计，该时间过后，该路由将被清除出路由表；

通过调整以上时钟，可能会加快路由协议的收敛时间以及故障恢复时间。要调整 RIP 时钟，在 RIP 路由进程配置模式中执行以下命令：

命令	作用
Ruijie(config-router)# **timers basic** *update invalid flush*	调整 RIP 时钟

缺省情况下，更新时间为 30 秒，无效时间为 180 秒，清除时间为 120 秒。

连接在同一网络上的设备，RIP 时钟值一定要一致。

2.2.8 配置RIP路由源地址验证

缺省情况下，RIP 会对接收的路由更新报文源地址进行验证，如果源地址无效，RIP 就会丢弃该报文。判断源地址是否有效，就是判断源 IP 地址是否与接口 IP 地址在相同的网络内。如果是无编号 IP 地址接口，将不会进行有效性验证。

要配置路由源地址验证，在 RIP 路由进程配置模式中执行以下命令：

命令	作用
Ruijie(config-router)# **no validate-update-source**	关闭源地址验证
Ruijie(config-router)# **validate-update-source**	启动源地址验证

2.2.9 控制RIP接口状态

在某些情况下，需要对 RIP 工作进行灵活配置，如仅希望设备学习 RIP 路由，并不进行 RIP 路由通告，此时可以配置被动接口；或希望单独配置某个接口的状态，则可以使用命令对指定接口的 RIP 报文的发送或接收进行控制。

要配置某接口为被动模式，在 RIP 路由进程配置模式中执行以下命令：

命令	作用
Ruijie(config-router)# **passive-interface** {**default** | *interface-type interface-num*}	配置被动接口
Ruijie(config-router)#**no passive-interface** {**default** | *interface-type interface-num*}	取消被动接口

被动接口接收到 RIP 请求后，不进行响应；但在收到非 RIP（如路由诊断程序等）请求后，会进行响应，因为这些请求程序希望了解所有设备的路由情况。

要禁止或允许某接口接收 RIP 报文，在接口配置模式中执行以下命令。

命令	作用
Ruijie(config-if)# **no ip rip receive enable**	禁止接口接收 RIP 报文
Ruijie(config-if)# **ip rip receive enable**	允许接口接收 RIP 报文

要禁止或允许某接口发送 RIP 报文，在接口配置模式中执行以下命令

命令	作用
Ruijie(config-if)# **no ip rip send enable**	禁止接口发送 RIP 报文
Ruijie(config-if)# **ip rip send enable**	允许接口发送 RIP 报文

2.2.10 配置RIP接口通告缺省路由

如果需要在某个指定接口的更新报文中产生一条默认路由（0.0.0.0/0）,可以在接口配置模式下执行以下命令：

命令	作用
Ruijie(config-if)# **ip rip default-information originate** [**metric** *metric-value*]	通告默认路由，也通告其它路由
Ruijie(config-if)# **no ip rip default-information**	取消接口通告默认路由

如果需要在某个指定接口的更新报文中产生一条默认路由（0.0.0.0/0），并且该接口只通告这条默认路由，不通告其它 RIP 路由，可以在接口配置模式下执行以下命令：

命令	作用
Ruijie(config-if)# **ip rip default-information only** [**metric** *metric-value*]	通告默认路由，不通告其它路由
Ruijie(config-if)# **no ip rip default-information**	取消接口通告默认路由

如果同时配置了接口下的 **ip rip default-information** 和 RIP 进程的 default-information originate，则只通告接口配置的缺省路由。

2.2.11 配置RIP接口通告超网路由

当路由的掩码长度小于其自然掩码长度时，这条路由称为超网路由。如 80.0.0.0/6，根据 IP 地址分类，80.0.0.0 属于 A 类网络，其自然掩码长度为 8，所以 80.0.0.0/6 是超网路由。

当 RIPv1 路由设备监听 RIPv2 路由响应报文时，如果监听到超网路由信息，由于 RIPv1 会将报文中路由信息的子网掩码忽略，从而学习到错误的路由。所以，这种情况下，RIPv2 路由设备需要在相应的接口配置禁止向 RIPv1 路由设备通告超网路由。

要配置某接口是否允许超网路由的通告，在接口配置模式中执行以下命令：

命令	作用
Ruijie(config-if)# **no ip rip send supernet-routes**	禁止接口通告超网路由
Ruijie(config-if)# **ip rip send supernet-routes**	允许接口通告超网路由

- 接口上只接收 RIPv1 报文时，不接收 RIPv2 报文，也就不会接收超网路由；
- 接口上能够接收 RIPv2 报文时，支持接收超网路由；
- 接口上发送 RIPv1 报文时，不发送超网路由；
- 接口上发送 RIPv2 报文时，缺省支持发送超网路由。
- 通过接口模式命令“no ip rip send supernet-routes”控制不发送超网路由。
- 自动汇聚(auto-summary)：对超网路由无效，即超网路由不会被汇聚。
- 接口配置汇聚路由(ip rip summary)：不支持配置超网路由。

2.2.12 配置RIP VRF

RIP 支持 VRF，在 RIP 进程中可创建多个 RIP 实例，分别管理对应的 VRF。缺省情况下 RIP 进程只有一个实例，用来管理全局路由表。当 VRF 创建后，如需使用 RIP 管理 VRF 路由表，可以通过创建新的 RIP 实例管理该 VRF 路由表。

使用 **address-family** 命令使路由设备进入地址族配置子模式（提示为：(config-router-af)#）。当第一次指定子模式关联的 VRF 时，RIP 会创建对应该 VRF 的 RIP 实例。在该子模式下，可以配置相应的 VRF 的 RIP 实例。该模式下的 RIP 配置方法与全局路由中的 RIP 配置方法完全相同。

要离开地址族配置子模式并返回路由配置模式，使用 **exit-address-family** 命令。

要配置管理 VRF 的 RIP 实例，在 RIP 路由进程配置模式中执行以下命令：

命令	作用
Ruijie(config-router)# **address-family ipv4 vrf** *vrf-name*	创建管理与名为 *vrf-name* 的 VRF 对应的 RIP 实例
Ruijie(config-router)# **no address-family ipv4 vrf** *vrf-name*	删除与名为 *vrf-name* 的 VRF 对应的 RIP 实例

2.2.13 配置RIP BFD

RIP BFD 的配置请参见《BFD 配置》相关章节。

2.2.14 配置RIP触发扩展

RIP 触发扩展功能（TRIP，Triggered RIP）是 RIP 协议在广域网（WAN，Wide Area Network）上的扩展，主要应用于按需链路。

当启用了 RIP 触发扩展功能，RIP 协议不再定时发送路由更新，只在以下事件发生的时候 RIP 才会向广域网接口发送路由更新：

- 当接收到路由请求报文。
- RIP 路由信息发生变化。
- 当接口状态变化。
- 当路由设备启动。

由于取消了 RIP 定时更新，因此需要采用确认和重发机制来保证更新报文在广域网上的成功发送和接收。RIP 为此扩展了 3 种新的报文类型，并通过 RIP 报文头部的 Command 字段来区分：

- Update Request（更新请求）：类型值为 9，请求对端发送所需要的路由表信息。
- Update Response（更新应答）：类型值为 10，包含对端所需要的路由更新信息。
- Update Acknowledge（更新确认）：类型值为 11，对收到的 Update Response 报文进行确认，表示已收到对端发送的路由更新信息。

在以下两种情况下允许启用该功能：A.接口仅存在一个邻居；B.存在多个邻居但是以单播方式交互。建议在 PPP、帧中继、X.25 等链路层协议上启用该功能；

建议在配置该功能的接口上启用带毒性逆转的水平分割功能，否则可能会出现无效路由信息残留等现象；

必须要保证同一链路的所有路由设备都启用了该功能，否则将导致该功能失效，无法正确交互路由信息；

不支持该功能与 BFD 联动 RIP 功能同时启用；

启用该功能时，请保证链路两端的 RIP 配置一致，如：RIP 认证，接口支持的 RIP 协议版本等；

如果接口启用了该功能，则无论是否启用源地址校验功能（**validate-update-source**），对该接口的报文都进行源地址校验。

要配置启用或禁用该功能，在接口配置模式中执行以下命令：

命令	作用
Ruijie(config-if)# **ip rip triggered**	启用 RIP 触发扩展
Ruijie(config-if)# **no ip rip triggered**	禁用 RIP 触发扩展

2.2.15 配置RIP GR

单机仅支持 GR Helper 能力。在 VSU 系统中，支持 GR Restarter 和 GR Helper 能力。

RIP 优雅重启（Graceful Restart，GR）功能，是为了实现在协议的重新启动过程中数据转发不间断。当路由设备启用了 RIP 优雅重启，当 RIP 协议重启过程中，会继续维持重启前的转发表，并向邻居发送请求报文重新学习路由，在优雅重启周期内完成路由的重新收敛，优雅重启周期到期后，将退出 GR，更新转发表项，并将路由表向邻居进行通告。

优雅重启周期为执行 RIP 重启到 RIP 完成优雅重启的最长时间，在这段时间内转发表维持为重启前的转发表，并执行 RIP 路由恢复工作，使 RIP 恢复到协议重启前的状态。当重启周期到期后，RIP 将退出 GR 状态，执行普通的 RIP 操作。

graceful-restart grace-period 允许用户显式修改重启周期。注意，要能够保证在 RIP 路由无效时间之内完成 GR 重启，并经过一次 RIP 路由更新周期。如果该值设置不当，可能无法保证优雅重启过程中数据转发的不间断，典型的情况如：如重启周期大于邻居的路由无效时间，在路由无效时间到期时还没有完成 GR，没有重新向邻居通告路由，邻居的路由在无效时间到期后就停止转发，导致网络的数据转发中断。所以除非有明确的需求，否则不建议调整优雅重启周期。如果需要调整，请结合 **timers basic** 命令的配置，确定重启周期的值大于路由更新时间，且小于路由无效时间。

要配置启用或禁用该功能，在 RIP 路由进程配置模式中执行以下命令：

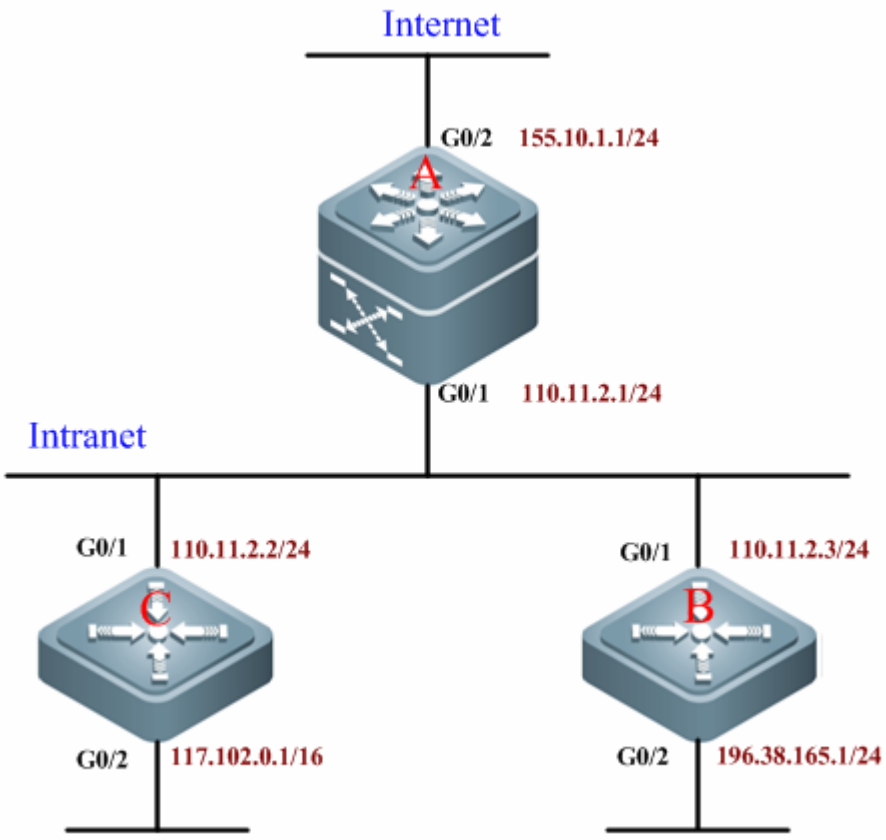
命令	作用
Ruijie(config-router)# **graceful-restart** [**grace-period** *grace-period*]	启用 RIP 优雅重启
Ruijie(config-router)# **no graceful-restart** [**grace-period**]	禁用 RIP 优雅重启

2.3 配置举例

2.3.1 RIP路由配置及定义版本

组网拓扑

图 2-1 RIP 路由配置及定义版本应用



组网需求

某小型公司办公网络规模比较小，需要任意两个节点之间能够网络层互通。网络需求如下：

- 需要设备自动适应网络拓扑变化，降低人工维护工作量；
- 需要路由信息更新时可以携带子网掩码；
- A 只接收从外部网络发来的路由信息，但不对外发布内部网络的路由信息；
- A、B、C 之间能够交互 RIP 信息，以便于内部主机能够访问 Internet。

配置要点

- 根据用户需求及用户网络环境，选择 RIPv2 路由协议实现用户网络之间互通；
- 要使 A 只接收从外部网络发来的路由信息，但不对外发布内部网络的路由信息，则需在 A 的 G0/2 端口设置为被动接口。

配置步骤

配置 A

！ 配置 A 相应端口的 IP 地址

```
Ruijie>enable
Ruijie#configure terminal
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if)#ip address 110.11.2.1 255.255.255.0
Ruijie(config-if)#exit
Ruijie(config)#interface gigabitEthernet 0/2
Ruijie(config-if)#ip address 155.10.1.1 255.255.255.0
```

！ 创建 RIP 的路由进程

```
Ruijie(config)#router rip
```

！ 定义 RIP 的版本为 2

```
Ruijie(config-router)#version 2
```

！ 配置 G0/2 为被动接口

```
Ruijie(config-router)#passive-interface gigabitEthernet 0/2
```

！ 关闭路由自动汇聚

```
Ruijie(config-router)#no auto-summary
```

！ 定义关联网络

```
Ruijie(config-router)#network 110.11.2.0 255.255.255.0
Ruijie(config-router)#network 155.10.1.0
```

配置 B

！ 配置 B 相应端口的 IP 地址

```
Ruijie>enable
Ruijie#configure terminal
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if)#ip address 110.11.2.2 255.255.255.0
Ruijie(config-if)#exit
Ruijie(config)#interface gigabitEthernet 0/2
Ruijie(config-if)#ip address 196.38.165.1 255.255.255.0
Ruijie(config-if)#exit
```

！ 创建 RIP 的路由进程

```
Ruijie(config)#router rip
```

！ 定义 RIP 的版本为 2

```
Ruijie(config-router)#version 2
```

！ 关闭路由自动汇聚

```
Ruijie(config-router)#no auto-summary
```

！ 定义关联网络

```
Ruijie(config-router)#network 110.11.2.0
Ruijie(config-router)#network 196.38.165.0
```

配置 C

！ 配置 C 相应端口的 IP 地址

```
Ruijie>enable
Ruijie#configure terminal
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if)#ip address 110.11.2.3 255.255.255.0
Ruijie(config-if)#exit
Ruijie(config)#interface gigabitEthernet 0/2
Ruijie(config-if)#ip address 117.102.0.1 255.255.0.0
Ruijie(config-if)#exit
```

！ 创建 RIP 的路由进程

```
Ruijie(config)#router rip
```

！ 定义 RIP 的版本为 2

```
Ruijie(config-router)#version 2
```

！ 关闭路由自动汇聚

```
Ruijie(config-router)#no auto-summary
```

！ 定义关联网络

```
Ruijie(config-router)#network 110.11.2.0
Ruijie(config-router)#network 117.102.0.0
```

显示验证

查看各个设备的路由表：

1、在 A 上查看路由表，如下所示（黑体字部分为通过 RIP 学习到的路由信息）：

```
Ruijie#show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    110.11.2.0/24 is directly connected, GigabitEthernet 0/1
C    110.11.2.1/32 is local host.
R 117.102.0.0/16 [120/1] via 110.11.2.2, 00:00:47, GigabitEthernet 0/1
C    155.10.1.0/24 is directly connected, GigabitEthernet 0/2
C    155.10.1.1/32 is local host.
C    192.168.217.0/24 is directly connected, VLAN 1
C    192.168.217.233/32 is local host.
R  196.38.165.0/24 [120/1] via 110.11.2.3, 00:19:18, GigabitEthernet 0/1
```

2、在 B 上查看路由表，如下所示（黑体字部分为通过 RIP 学习到的路由信息）：

```
Ruijie#show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    110.11.2.0/24 is directly connected, GigabitEthernet 0/1
C    110.11.2.2/32 is local host.
R 155.10.1.0/24 [120/1] via 110.11.2.1, 00:15:21, GigabitEthernet 0/1
C    196.38.165.0/24 is directly connected, GigabitEthernet 0/2
C    196.38.165.1/32 is local host.
```

```
R 117.102.0.0/16 [120/1] via 110.11.2.2, 00:00:47, GigabitEthernet 0/1
```

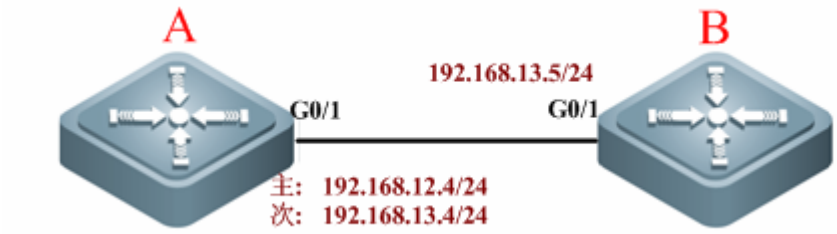
3、在 C 上查看路由表，如下所示（黑体字部分为通过 RIP 学习到的路由信息）：

```
Ruijie#show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    110.11.2.0/24 is directly connected, GigabitEthernet 0/1
C    110.11.2.3/32 is local host.
C    117.102.0.0/16 is directly connected, GigabitEthernet 0/2
C    117.102.0.1/32 is local host.
R  155.10.1.0/24 [120/1] via 110.11.2.1, 00:20:55, GigabitEthernet 0/1
R  196.38.165.0/24 [120/1] via 110.11.2.3, 00:19:18, GigabitEthernet 0/1
```

2.3.2 RIP水平分割

组网拓扑

图 2-2 RIP 水平分割应用拓扑图



组网需求

网络中运行有两台设备如下所示，其中 A 配置了次地址。

通过配置设备要求达到以下要求：

- 两台设备都运行 RIP 路由协议；
- B 能够学到 192.168.12.0/24 的网段路由。

配置要点

为了达到配置要求，需要做如下配置：

- 设备运行 RIPv2 路由协议；
- A 一定要关闭水平分割功能（默认情况下所有接口都开启水平分割功能），否则 A 不会将 192.168.12.0 网段通告给 B。

配置步骤

配置 A

！配置以太网端口

```
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#ip address 192.168.12.4 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/1)#ip address 192.168.13.4 255.255.255.0 secondary
```

！关闭端口的水平分割

```
Ruijie(config-if-GigabitEthernet 0/1)#no ip rip split-horizon
```

！配置 RIP 路由协议

```
Ruijie(config)#route rip
Ruijie(config-router)#version 2
Ruijie(config-router)#network 192.168.12.0
Ruijie(config-router)#network 192.168.13.0
```

！ 关闭路由自动汇聚功能

```
Ruijie(config-router)#no auto-summary
```

配置 B

！配置以太网端口

```
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#ip address 192.168.13.5 255.255.255.0
```

！配置 RIP 路由协议

```
Ruijie(config)#route rip
Ruijie(config-router)#version 2
Ruijie(config-router)#network 192.168.13.0
```

显示验证

查看关闭水平分割前后 B 的路由表

1、未关闭水平分割前，在 B 上查看路由表，如下所示：

```
Ruijie#show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
```

```
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default
Gateway of last resort is no set
C    192.168.13.0/24 is directly connected, GigabitEthernet 0/1
C    192.168.13.5/32 is local host.
```

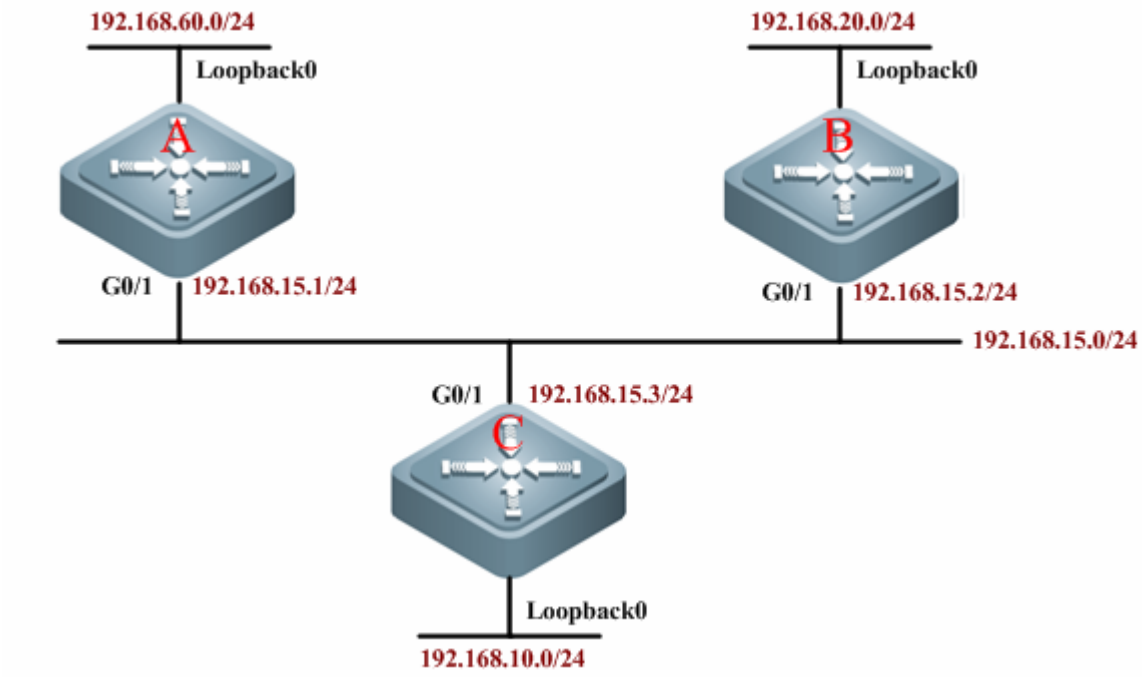
2、关闭水平分割后，在 B 上查看路由表，如下所示（黑体字部分为通过 RIP 学习到的路由信息）：

```
Ruijie#show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
R    192.168.12.0/24 [120/1] via 192.168.13.4, 00:00:10, GigabitEthernet 0/1
C    192.168.13.0/24 is directly connected, GigabitEthernet 0/1
C    192.168.13.5/32 is local host.
```

2.3.3 RIP单播更新

组网拓扑

图 2-3 RIP 单播更新应用拓扑图



组网需求

如下图所示，三台设备全部连接在局域网上，并且全部运行 RIP 路由协议。

- A 可以学习到 B、C 通告的路由；
- C 可以学到 A、B 通告的路由；
- B 不能学习到 C 通告的路由。

配置要点

为了实现以上配置要求，需要在 C 上配置 RIP 报文单播。在 C 的 RIP 处理中增加一条命令 **neighbor**，使 RIP 协议能够以单播的方式向 A 的接口发送通告。设置 C 的 G0/1 上的 **passive-interface** 命令防止在该链路上广播更新。

配置步骤

配置 A

！ 配置相应接口的 IP 地址

```
Ruijie>enable
Ruijie#configure terminal
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if)#ip address 192.168.15.1 255.255.255.0
Ruijie(config-if)#exit
Ruijie(config)#interface Loopback 0
Ruijie(config-if)#ip address 192.168.60.1 255.255.255.0
```

```
Ruijie(config-if)#exit
```

！ 创建 RIP 的路由进程

```
Ruijie(config)#router rip
```

！ 定义关联网络

```
Ruijie(config-router)#network 192.168.60.0
Ruijie(config-router)#network 192.168.15.0
```

配置 B

！ 配置相应接口的 IP 地址

```
Ruijie>enable
Ruijie#configure terminal
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if)#ip address 192.168.15.2 255.255.255.0
Ruijie(config-if)#exit
Ruijie(config)#interface Loopback 0
Ruijie(config-if)#ip address 192.168.20.1 255.255.255.0
Ruijie(config-if)#exit
```

！ 创建 RIP 的路由进程

```
Ruijie(config)#router rip
```

！ 定义关联网络

```
Ruijie(config-router)#network 192.168.20.0
Ruijie(config-router)#network 192.168.15.0
```

配置 C

！ 配置相应接口的 IP 地址

```
Ruijie>enable
Ruijie#configure terminal
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if)#ip address 192.168.15.3 255.255.255.0
Ruijie(config-if)#exit
Ruijie(config)#interface Loopback 0
Ruijie(config-if)#ip address 192.168.10.1 255.255.255.0
Ruijie(config-if)#exit
```

！ 创建 RIP 的路由进程

```
Ruijie(config)#router rip
```

！ 定义关联网络

```
Ruijie(config-router)#network 192.168.15.0
Ruijie(config-router)#network 192.168.10.0
```

！ 配置 G0/1 为被动接口

```
Ruijie(config-router)#passive-interface gigabitEthernet 0/1
```

！ 启动单播更新

```
Ruijie(config-router)#neighbor 192.168.15.1
```

显示验证

查看各个设备的路由表（此处主要查看 B 和 C 上的路由信息）：

1、在 B 上查看路由表，如下所示：

```
Ruijie#show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    192.168.20.0/24 is directly connected, Loopback 0
C    192.168.20.1/32 is local host.
C    192.168.15.0/24 is directly connected, GigabitEthernet 0/1
C    192.168.15.2/32 is local host.
R 192.168.60.0/24 [120/1] via 192.168.15.1, 00:15:21, GigabitEthernet 0/1
```

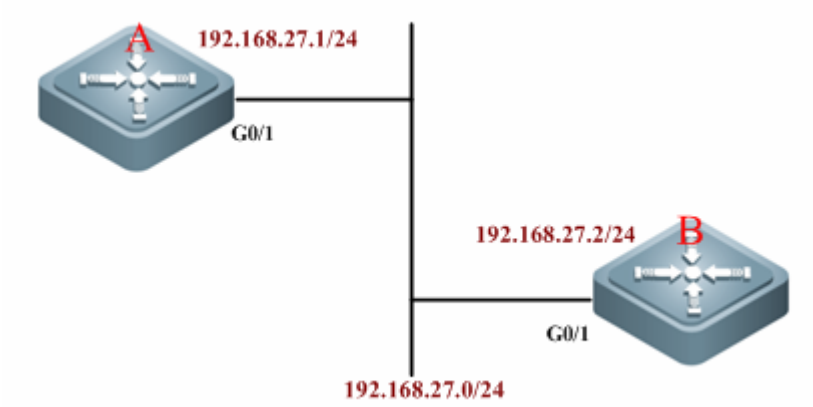
2、在 C 上查看路由表，如下所示（黑体字部分为通过 RIP 学习到的路由信息）：

```
Ruijie#show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    192.168.10.0 is directly connected, Loopback 0
C    192.168.10.1/32 is local host.
R 192.168.60.0/24 [120/1] via 192.168.15.1, 00:15:21, GigabitEthernet 0/1
C    192.168.15.0/24 is directly connected, GigabitEthernet 0/1
C    192.168.15.3/32 is local host.
R 192.168.20.0 [120/1] via 192.168.15.2, 00:00:47, GigabitEthernet 0/1
```

2.3.4 RIP认证

组网拓扑

图 2-4 RIP 认证应用拓扑图



组网需求

两台设备通过以太网互连，运行 RIP 路由协议，采用 MD5 认证方式。要求如下：

- A 发送 RIP 包的认证密钥为 Hello，可接收认证密钥为 Hello、World 的 RIP 包；
- B 发送 RIP 包的认证密钥为 World，可接收认证密钥为 Hello、World 的 RIP 包。
- 第一个密钥从 2010 年 10 月 1 日下午 4：30 开始使用，使用的时长是 12H（43200s）
- 第二个密钥从 2010 年 10 月 2 日凌晨 4：00 开始生效，并在这个时间以后永久有效。

配置要点

RIPv1 不支持认证，如果设备配置 RIPv2 路由协议，可以在相应的接口配置认证。

密钥串定义了该接口可使用的密钥集合，如果密钥串没有配置，即使接口应用了密钥串，也不会有认证行为发生。所以在配置应用认证前应该先配置密钥链以及密钥链上的密钥串。

RGOS 支持两种 RIP 认证方式：明文认证和 MD5 认证。缺省的认证方式为明文认证。

- 配置发送 RIP 包的认证密钥需要配置 keychain 的第一个 key；
- 配置可接收的认证密钥只需要配置在 keychain 里面任意一个 key

配置步骤

A 的配置：

！ 配置以太网接口的 IP 地址

```
Ruijie>enable
Ruijie#configure terminal
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if)#ip address 192.168.27.1 255.255.255.0
Ruijie(config-if)#exit
```

！ 配置密钥链，密钥链名称为 ripchain

```
Ruijie(config)#key chain ripchain
```

！ 配置第一个密钥“Key 1”,它含有一个口令“Hello”,并根据相应的需求配置时效

```
Ruijie(config-keychain)#key 1
Ruijie(config-keychain-key)#key-string Hello
Ruijie(config-keychain-key)#accept-lifetime 16:30:00 Oct 1 2010 duration 43200
Ruijie(config-keychain-key)#send-lifetime 16:30:00 Oct 1 2010 duration 43200
Ruijie(config-keychain-key)#exit
```

！ 配置第二个密钥“Key 2”,它含有一个口令“World”,并根据相应的需求配置时效

```
Ruijie(config-keychain)#key 2
Ruijie(config-keychain-key)#key-string World
Ruijie(config-keychain-key)#accept-lifetime 04:00:00 Oct 2 2010 infinite    //密钥生效时间
Ruijie(config-keychain-key)#send-lifetime 04:00:00 Oct 2 2010 infinite          //密钥生效时间
Ruijie(config-keychain-key)#end
```

！ 配置 G0/1 将使用 MD5 认证的这个密钥去验证来自 B 的更新消息

```
Ruijie#configure terminal
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if)#ip rip authentication key-chain ripchain
Ruijie(config-if)#ip rip authentication mode md5
Ruijie(config-if)#exit
```

！ 配置 RIP 路由协议

```
Ruijie(config)#router rip
Ruijie(config-router)#version 2
Ruijie(config-router)#network 192.168.27.0
```

B 的配置:

！ 配置以太网接口的 IP 地址

```
Ruijie>enable
Ruijie#configure terminal
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if)#ip address 192.168.27.2 255.255.255.0
Ruijie(config-if)#exit
```

！ 配置密钥链

```
Ruijie(config)#key chain ripchain //密钥链名只在本地有效，此处也可使用别的密钥链名。
```

！ 配置第一个密钥“Key 1”,它含有一个口令“Hello”,并根据相应的需求配置时效

```
Ruijie(config-keychain)#key 1
Ruijie(config-keychain-key)#key-string Hello
Ruijie(config-keychain-key)#accept-lifetime 16:30:00 Oct 1 2010 duration 43200
Ruijie(config-keychain-key)#send-lifetime 16:30:00 Oct 1 2010 duration 43200
Ruijie(config-keychain-key)#exit
```

！ 配置第二个密钥“Key 2”,它含有一个口令“World”,并根据相应的需求配置时效

```
Ruijie(config-keychain)#key 2
Ruijie(config-keychain-key)#key-string World
Ruijie(config-keychain-key)#accept-lifetime 04:00:00 Oct 2 010 infinite
Ruijie(config-keychain-key)#send-lifetime 04:00:00 Oct 2 2010 infinite
Ruijie(config-keychain-key)#end
```

！ 配置 G0/1 将使用 MD5 认证的这个密钥去验证来自 A 的更新消息

```
Ruijie#configure terminal
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if)#ip rip authentication key-chain ripchain
Ruijie(config-if)#ip rip authentication mode md5
Ruijie(config-if)#exit
```

！ 配置 RIP 路由协议

```
Ruijie(config)#router rip
Ruijie(config-router)#version 2
Ruijie(config-router)#network 192.168.27.0
```

显示验证

通过 show run 查看设备配置的正确性（本例查看 A 的配置信息）：

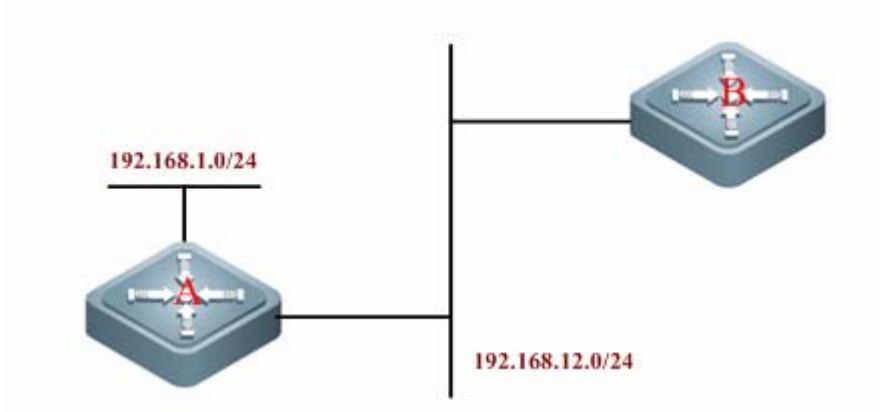
```
Ruijie#show run

Building configuration...
Current configuration : 1561 bytes

!
vlan 1
!
!
key chain ripchain
 key 1
  key-string Hello
  accept-lifetime 16:30:00 Oct 01 2010 duration 43200
```

```
  send-lifetime 16:30:00 Oct 01 2010 duration 43200
 key 2
  key-string World
  accept-lifetime 04:00:00 Oct 02 2010 infinite
  send-lifetime 04:00:00 Oct 02 2010 infinite
!
no service password-encryption
!
interface GigabitEthernet 0/1
ip rip authentication mode md5
 ip rip authentication key-chain ripchain
 no ip proxy-arp
 ip address 192.168.27.1 255.255.255.0
!
interface GigabitEthernet 0/2
!
interface GigabitEthernet 0/3
!
interface GigabitEthernet 0/4
。。。。。。
!
!
!
router rip
 version 2
 network 192.168.27.0
!
!
!
line con 0
line vty 0 4
 login
!
!
end
```

2.3.5 RIP超网路由

组网拓扑

图 2-5 RIP 超网路由用用拓扑图



组网需求

两台设备通过以太网互连，A 运行 RIPv2，B 为只支持 RIPv1 协议的路由设备，无法支持超网路由的学习。

要求：

- 在 A 配置一条超网路由 80.0.0.0/6，下一跳指向回环接口 loopback 1（192.168.1.0）；
- 将上述静态路由重分发到 RIP；
- 在 A 禁止通告超网路由。

配置要点

B 仅支持 RIPv1 协议，根据 RFC 1058 文档规定，该设备应能够接收更高版本 RIP 协议的更新报文，但需要将报文中的子网掩码和下一跳等字段忽略处理，所以，B 接收到路由 80.0.0.0/6 后，会将其当作 80.0.0.0/8 进行处理。为了避免 B 学习到错误的路由，需要在 A 上禁止通告超网路由。

配置步骤

配置 A：

！ 配置以太网端口

```
Ruijie(config)#interface FastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)#ip address 192.168.12.1 255.255.255.0
Ruijie(config-if-FastEthernet 0/1)#no ip rip send supernet-routes
//禁止通告超网路由
```

！ 配置回环端口

```
Ruijie(config)#interface loopback 1
Ruijie(config-if-Loopback 1)#ip address 192.168.1.1 255.255.255.0
```

！ 配置静态路由

```
Ruijie(config)#ip route 80.0.0.0 252.0.0.0 loopback 1
```

！ 配置 RIP 路由协议

```
Ruijie(config)#router rip
Ruijie(config-router)#version 2
Ruijie(config-router)#network 192.168.12.0
Ruijie(config-router)#network 192.168.1.0
Ruijie(config-router)#redistribute static
//静态路由重分发
```

配置 B(只支持 RIPv1)：

！ 配置以太网端口

```
Ruijie(config)#interface FastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)#ip address 192.168.12.3 255.255.255.0
```

！ 配置 RIP 路由协议

```
Ruijie(config)#router rip
Ruijie(config-router)#network 192.168.12.0
```

显示验证

查看各个设备的路由表：

1、在 A 上查看路由表，如下所示：

```
Ruijie#show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
S    80.0.0.0/6 is directly connected, Loopback 1
C    192.168.1.0/24 is directly connected, Loopback 1
C    192.168.1.1/32 is local host.
C    192.168.12.0/24 is directly connected, FastEthernet 0/1
C    192.168.12.1/32 is local host.
```

2、在 B 上查看路由表，如下所示（黑体字部分为通过 RIP 学习到的路由信息）：

```
Ruijie#show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
```

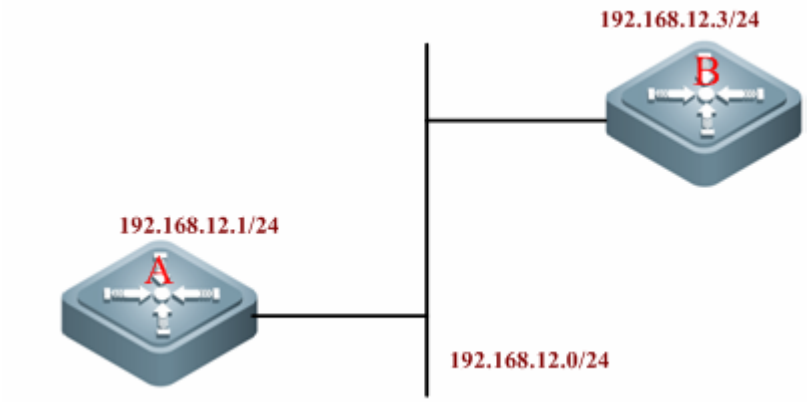
```
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
R    80.0.0.0/6 [120/1] via 192.168.12.1, 00:00:46, GigabitEthernet 0/1
R    192.168.1.0/24 [120/1] via 192.168.12.1, 00:38:17, FastEthernet 0/1
C    192.168.12.0/24 is directly connected, FastEthernet 0/1
C    192.168.12.2/32 is local host.
```

2.3.6 RIP VRF

配置要求

两台路由设备通过以太网互连，运行 RIP 路由协议。设备之间连接图以及 IP 地址分配如下图。

图 2-6 RIP VRF 配置例子



通过 RIP，在 A 的名为 redvpn 的 VRF 和 B 的名为 bluevpn 的 VRF 之间交互路由信息。

设备具体配置

设备 A 的配置：

创建 VRF

```
ip vrf redvpn
```

接口绑定 VRF，并配置端口地址。

```
interface fastEthernet 0/1
ip vrf forwarding redvpn
ip address 192.168.12.1 255.255.255.0
```

配置 RIP 路由协议，创建 RIP 实例

```
router rip
address-family ipv4 vrf redvpn
```

```
network 192.168.12.0
exit-address-family
```

设备 B 的配置：

创建 VRF

```
ip vrf  bluevpn
```

接口绑定 VRF，并配置端口地址。

```
interface fastEthernet 0/1
ip vrf forwarding bluevpn
ip address 192.168.12.3 255.255.255.0
```

配置 RIP 路由协议，创建 RIP 实例

```
router rip
address-family ipv4 vrf bluevpn
exit-address-family
```

2.3.7 RIP 触发扩展

配置要求

两台路由设备通过 PPP 链路互连，运行 RIP 路由协议。设备之间连接图以及 IP 地址分配如下图。

图 2-7 RIP 触发扩展配置例子

通过配置 RIP 触发扩展，在 A 和 B 间的广域网链路上交互路由信息，并启用带毒性逆转的水平分割。

设备具体配置

设备 A 的配置：

接口封装 PPP 链路协议，配置端口地址，启用 TRIP，并启用带毒性逆转的水平分割。

```
interface Serial 0/0
encapsulation ppp
ip address 192.168.12.1 255.255.255.0
ip rip triggered
ip rip split-horizon poisoned-reverse
```

配置 RIP 路由协议

```
router rip
network 192.168.12.0
```

设备 B 的配置：

#接口封装 PPP 链路协议，配置端口地址，启用 TRIP，并启用带毒性逆转的水平分割。

```
interface Serial 0/0
encapsulation ppp
ip address 192.168.12.2 255.255.255.0
ip rip triggered
ip rip split-horizon poisoned-reverse
```

配置 RIP 路由协议

```
router rip
network 192.168.12.0
```

3 RIPng

3.1 概述

RIPng 与 RIP 一样，是一个距离向量路由协议，它使用跳数作为路由度量值。RIPng 是一个内部网关协议，适用于中小型的网络。RIPng 是对 RIP 进行必要的改造以使其适应 IPv6 下的选路要求，因此 RIPng 的基本工作原理同 RIP 是一样的，其主要的变化在地址和报文格式方面。由于是基于 IPv6 的，加入了对 IPv6 的地址与前缀的支持，更新报文的作用地址统一采用多播组地址 FF02::9，取消了 RIP 中的安全验证，它的安全机制主要是通过 IPv6 的安全机制实现；端口采用的是 521；分组格式、掩码、最大报文长度都有所不同。具体请参考 RFC2080、RFC2081。由于与 RIP 的不同，相应的 CLI 的命令也有所增减。

3.2 配置RIPng

RIPng 配置列表包括：

- 创建 RIPng 路由进程（必须）
- 配置接口运行 RIPng（必须）
- 调整 RIPng 时钟（可选）
- 配置水平分割（可选）
- 配置重分发缺省度量值（可选）
- 调整接口量度值（可选）
- 配置接口通告缺省路由（可选）
- 配置消极接口（可选）
- 配置 RIPng 路由过滤（可选）

关于以下主题的配置，请参见《协议无关配置》章节。

- 路由重分布

以下为 RIPng 的缺省配置：

功能特性	缺省值
网络接口	接口偏移量 metric 缺省值为 1；
重分布	缺省不启用路由重分布 如果启用： 重分布指定路由进程的所有子类型路由 分发路由的 metric 值为缺省 metric 值
水平分割	开启
毒性逆转	关闭

定时器	缺省情况下： 更新时间为 30 秒 无效时间为 180 秒 清除时间为 120 秒
缺省 metric (default metric)	重分发其他协议的路由所使用的 metric 值，缺省值为 1
管理距离	120

3.2.1 创建RIPng路由进程

路由设备要运行 RIPng 路由协议，首先需要创建 RIPng 路由进程，并定义与 RIPng 路由进程关联的网络或接口地址。

要创建 RIPng 路由进程，在全局配置模式中执行以下命令：

命令	作用
Ruijie(config)# **ipv6 router rip**	创建 RIPng 路由进程。

3.2.2 配置接口运行RIPng

要使接口加入 RIPng 运行，可以接口配置模式下执行：

命令	作用
Ruijie(config-if)# **ipv6 rip enable**	使接口运行 RIPng

以下例子中，将接口 **ethernet** 0/0 加入 RIPng 运行，2001:db8:6::/64 范围内的路由被汇聚为 2001:db8:6::/64 通告。

```
Ruijie(config)# interface ethernet 0/0
Ruijie(config-if)# ipv6 address 2001:db8:6::1/64
Ruijie(config-if)# ipv6 rip enable
```

📖 与 RIP 不同的是，该命令将接口直接加入 RIPng 运行，而不必配置 **Network** 命令。

3.2.3 调整RIPng时钟

RIPng 提供了时钟调整的功能，可以根据网络的具体情况对时钟进行调整，使 RIPng 路由协议能够运行得更好。可以对以下时钟进行调整：

- 路由更新时间：以秒计，定义了路由设备发送路由更新报文的周期；
- 路由无效时间： 以秒计，定义了路由表中路由因没有更新而变为无效的时间；
- 路由清除时间：以秒计，该时间过后，该路由将被清除出路由表；

通过调整以上时钟，可能会加快路由协议的收敛时间以及故障恢复时间。要调整 RIPng 时钟，在 RIPng 路由进程配置模式中执行以下命令：

命令	作用
Ruijie(config-router)# **times** *update invalid garbage-collection*	调整 RIPng 时钟

以下的例子配置调整了 RIPng 的三个定时器的值：

```
Ruijie(config-router)# timers 10 30 90
```

连接在同一网络上的路由设备，RIPng 时钟值一定要一致。

3.2.4 配置水平分割

当多台路由设备连接在 IP 广播类型网络上，又运行距离向量路由协议时，就有必要采用水平分割的机制来避免路由环路的形成。水平分割可以防止路由设备将某些路由信息从学习到这些路由信息的接口通告出去，这种行为优化了多个路由设备之间的路由信息交换。

然而对于非广播多路访问网络（如帧中继、X.25 网络），水平分割可能造成部分路由设备学习不到全部的路由信息。在这种情况下，可能需要关闭水平分割。

要配置关闭或打开水平分割，在路由进程配置模式中执行以下命令：

命令	作用
Ruijie(config-router)# **no split-horizon**	关闭水平分割
Ruijie(config-router)# **split-horizon**	打开水平分割

缺省情况下，加入 RIPng 的所有接口打开水平分割。

目前版本的实现只支持在 RIPng 路由进程配置水平分割，即该命令作用于所有启用了 RIPng 的接口，后续 RGOS 软件会实现基于接口的水平分割配置，可以为指定接口设定水平分割状态。

与水平分割不同的是，启用毒性逆转时，路由设备将某些路由信息从学习到这些路由信息的接口通告出去，只是将相应的 metric 的值设置为 infinity(16)。

要配置打开或关闭毒性逆转功能，在路由进程配置模式中执行以下命令：

命令	作用
Ruijie(config-router)#**split-horizon poisoned-reverse**	开启带毒性逆转的水平分割
Ruijie(config-router)#**no split-horizon poisoned-reverse**	关闭带毒性逆转的水平分割

启用毒性逆转将占用相当一部分带宽。

3.2.5 配置重分发缺省度量值

当一个协议重分布其它协议的路由时，由于各个协议的度量值不一样，需要设置重分布别的协议的度量值，RIPng 缺省度量值为 1。

要定义重分布其它路由协议时 RIPng 缺省的量度值，请使用路由进程配置命令 **default-metric**。要恢复缺省值 1 请使用 **no default-metric**。

命令	作用
Ruijie(config-router)# **default-metric** *metric*	RIPng 的量度值被设置为 *metric*
Ruijie(config-router)# **no default-metric**	恢复缺省值 1

3.2.6 调整接口量度值

在学习到的路由加入路由表前，路由的 metric 要加上接口上设置的量度值。所以可以通过设置接口的量度值影响路由的使用。

要设置接口上的量度值，可以在接口配置模式下执行以下命令：

命令	作用
Ruijie(config-if)# **ipv6 rip metric-offset** *value*	配置接口度量值，度量范围：1-16

以下例子将接口 ethernet 0/0 上的接口量度值设置为 6：

```
Ruijie(config)# interface ethernet 0/0
Ruijie(config-if)# ipv6 rip metric-offset 6
```

3.2.7 配置接口通告缺省路由

要在本 RIPng 进程更新报文中产生一条 IPv6 默认路由（::/0），可在接口配置模式下执行：

命令	作用
Ruijie(config-if)# **ipv6 rip default-informaton originate**	在接口上产生一条默认路由到 RIPng，并和其它路由一起通告

要在本 RIPng 进程更新报文中产生一条 IPv6 默认路由（::/0），并且该接口只通告这条默认路由，可在接口配置模式下执行：

命令	作用
Ruijie(config-if)# **ipv6 rip default-informaton only**	在接口上产生一条默认路由到 RIPng，并且只通告该默认路由

3.2.8 配置消极接口

为了防止本地网络上的其它路由设备学到本设备发出的路由信息，可以通过配置消极接口来遏制路由更新报文从该网络接口发送出去。

要取消在一个接口上发送更新报文的功能，请在路由进程配置命令模式下执行：

命令	作用
Ruijie(config-router)# **passive-interface** { **default** | *interface-type interface-num* }	抑制接口发送更新报文

当配置 **default** 选项时，所有接口被设置为 passive 模式；当配置接口时，相应的接口被设置为 passive 模式。

3.2.9 配置RIPng路由过滤

控制路由更新通告

为了防止本地网络上的其它路由设备学到不必要的路由信息，可以通过控制 RIPng 路由更新通告来遏制指定路由的更新。

要遏制路由更新通告，在路由进程配置模式中执行以下命令:

命令	作用
Ruijie(config-router)# **distribute-list prefix-list** *prefix-list-name* **out** [*interface-type interface-name*]	根据前缀列表规则，允许或拒绝某些路由被通告出去。
Ruijie(config-router)# **no distribute-list prefix-list** *prefix-list-name* **out** [*interface-type interface-name*]	取消抑制路由更新通告。

以下的配置例子，只在接口 eth0 上对要发送的更新报文使用过滤，只有在 **prefix-list** *outlist* 前缀表范围内的更新路由才被发送。

```
Ruijie(config)# ipv6 router rip
Ruijie(config-router)# distribute-list prefix-list outlist out eth0
```

控制路由更新处理

为了避免接收路由更新报文的某些指定路由，可以配置该特性。

要控制路由更新处理，请在路由进程配置模式中执行以下命令：

命令	作用
Ruijie(config-router)# **distribute-list prefix-list** *prefix-list-name* **in** [*interface-type interface-name*]	根据访问列表规则，允许或拒绝接收路由更新指定的路由。
Ruijie(config-router)# **no distribute-list prefix-list** *prefix-list-name* **in** [*interface-type interface-name*]	取消控制路由更新处理。

以下的配置例子，只在接口 eth0 上对接收到的更新报文使用过滤，只有在 **prefix-list** *inlist* 前缀表范围内的更新路由才被接收。

```
Ruijie(config)# ipv6 router rip
Ruijie(config-router)# distribute-list prefix-list inlist in eth0
```

3.3 监视与维护

RIPng 调试开关

要查看 RIPng 的调试信息，观察 RIPng 路由处理的行为，请在特权配置模式下执行以下命令：

命令	作用
Ruijie# **debug ipv6 rip** [*interface-type interface-num* | nsm]	打开 RIPng 调试开关
Ruijie# **no debug ipv6 rip** [*interface-type interface-num* | nsm]	关闭 RIPng 调试开关

使用相应命令 **no** 形式关闭相应的 RIPng 调试开关。

显示 RIPng 路由表

要显示 RIPng 路由表的各项目信息，请在用户模式或特权模式下执行以下命令：

命令	作用
show ipv6 rip database	显示 RIPng 路由表信息

显示 RIPng 路由进程信息

要显示 RIPng 路由协议协进程的参数和各个统计数据，请在用户模式或特权模式下执行以下命令：

命令	作用
show ipv6 rip	显示 RIPng 路由进程信息

显示 RIPng 调试信息

要显示 RIPng 路由进程调试状态信息，请在特权模式或全局配置模式执行以下命令：

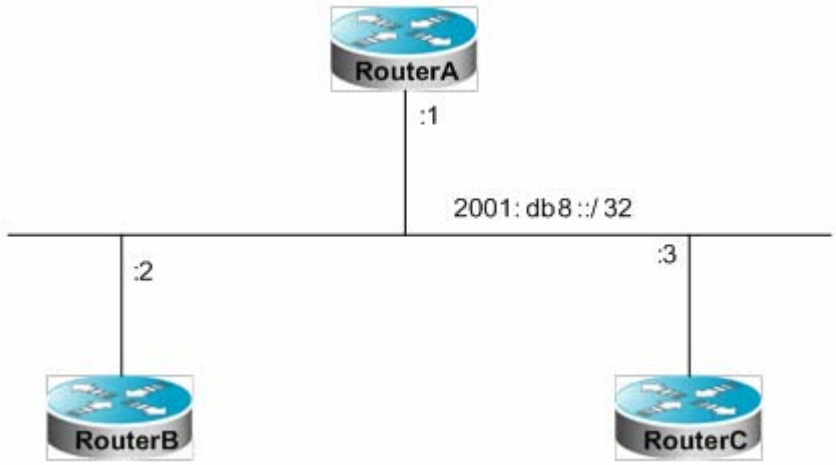
命令	作用
show debugging	显示 RIPng 路由进程调试状态信息

3.4 配置举例

配置要求

有三台设备，设备连接图见图 1。三台设备全部运行 RIPng，其中 Router A 作为网关设备，向 Router B 和 Router C 通告缺省路由，度量值为 3；Router B 和 Router C 的所有 RIPng 接口设置为 passive 模式，不向外通告 RIPng 更新报文。

图 3-1 缺省路由通告配置



- 路由设备具体配置

路由设备 A 的配置：

配置网络接口

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# ipv6 enable
Ruijie(config-if)# ipv6 address 2001:db8::1/32
Ruijie(config-if)# ipv6 rip enable
Ruijie(config-if)# ipv6 rip default-information originate metric 3
```

配置 RIPng

```
Ruijie(config)# ipv6 router rip
Ruijie(config-router)# exit
```

路由设备 B 的配置：

配置网络接口

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# ipv6 enable
Ruijie(config-if)# ipv6 address 2001:db8::2/32
Ruijie(config-if)# ipv6 rip enable
```

配置 RIPng

```
Ruijie(config)# ipv6 router rip
Ruijie(config-router)# passive-interface default
Ruijie(config-router)# exit
```

路由设备 C 的配置：

配置网络接口

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# ipv6 enable
Ruijie(config-if)# ipv6 address 2001:db8::3/32
Ruijie(config-if)# ipv6 rip enable
```

配置 RIPng

```
Ruijie(config)# ipv6 router rip
Ruijie(config-router)# passive-interface default
Ruijie(config-router)# exit
```

4 策略路由

4.1 概述

策略路由（Policy-Based Routing）就是基于策略的路由（在路由图中设置策略）。与静态路由相似，策略路由也是手工配置的路由，不能随网络变化自动更新，仅在本地有效。与静态路由、动态路由相比，策略路由更加灵活。静态路由、动态路由只能依据目的地址转发报文。策略路由可以依据源地址、目的地址、报文长度、入端口等转发报文。

现有用户网络，常常会出现使用到多个 ISP（Internet Server Provider，Internet 服务提供商）资源的情形。由于不同 ISP 申请到的带宽不一，或为了保护某些重点用户的网络资源，需要使用策略路由。通过有选择的控制数据报文的转发，不仅能够充分对利用 ISP 资源，又能满足灵活、多样的应用。

4.1.1 策略

配置策略路由，需要首先在路由图中配置策略。

- 通过 route-map 命令，创建路由图中的策略。
- 通过 match 命令，定义 IP/IPv6 报文的匹配条件。
- 通过 set 命令，定义对符合匹配条件的 IP 报文的处理动作。

创建策略

一个路由图中可以包含多条策略。每条策略都有对应的序号（Sequence），序号越小优先级越高。策略路由生效时，报文会按序号依次匹配策略，一旦匹配某条策略，就执行该策略对应的处理动作，然后退出策略路由的执行。如果不能匹配任何一条策略，则执行普通的路由转发。

创建策略时，可以指定策略的匹配模式为 permit 或者 deny：

- permit：允许模式。当报文满足该策略的 match 规则时，会对该 IP/IPv6 报文应用相应的 set 规则；如报文不满足策略的任一 match 规则，报文将会使用该路由图的下一条策略进行匹配。
- deny：拒绝模式。当报文满足该节点的所有 match 规则时，不对该 IP/IPv6 报文执行策略转发而是执行普通的路由转发。

设置 Match（匹配条件）

一条策略可以包含 0 条、1 条或多条 match 规则。如果包含 0 条 match 规则，则无条件执行 set 规则。如果包含多条 match 规则，必须同时匹配所有 match 规则，才能执行 set 规则。

策略路由支持以下 match 规则：

	命令	说明

IPv4 策略路由	**match ip address**	以源 IPv4 地址（和目的 IPv4 地址）作为匹配条件。一条策略中可以包含多条 **match ip address** 规则。
IPv6 策略路由	**match ipv6 address**	以源 IPv6 地址（和目的 IPv6 地址）作为匹配条件。一条策略中最多只能包含一条 **match ipv6 address** 规则。

IPv4 策略路由使用 IP 标准或者扩展 ACL 定义报文的源 IP 地址（和目的 IP 地址）范围。IPv6 策略路由使用 IPv6 扩展 ACL 定义报文的源 IPv6 地址（和目的 IPv6 地址）范围。

策略路由如果引用了 ACL，但是该 ACL 不存在，等价所有报文都匹配；如果引用了 ACL，但是其中没有任何 ACE，则跳过该策略，从下一个策略的 ACL 开始匹配。建议不做空 ACL 的配置和应用。

ACE 的 deny 选项行为执行普通转发。**deny any any** 行为是跳到下个 IPV6 ACL 开始匹配。

配置 PBR 功能后，会对发往本机的报文同时生效。如果用户希望发往本机的 IP/IPv6 报文不使用策略路由，则用户需要在 PBR 规则中在 IP/IPV6 ACL 前面手工添加“deny 设备 IP/IPv6 地址”的 ACE。

设置 Set（处理动作）

一条策略中可以包含 0 条或 1 条或多条 set 规则。如果包含 0 条 set 规则，则退出策略路由的执行。如果包含多条 set 规则，则执行所有 set 规则（如有优先级关系，则优先级最高者生效）。

策略路由支持以下 set 命令：

	命令	说明
IPv4 策略路由	**set ip tos**	修改 IP 报文的 tos 字段，供 QoS 使用。 此命令不能与 set ip dscp 同时配置。
	set ip dscp	修改 IP 报文的 dscp 字段，供 QoS 使用。 此命令不能与 **set ip tos** 同时配置。
	set ip nexthop	配置下一跳。该命令的优先级比普通路由高。匹配 match 规则的报文将优先转发到 **set ip nexthop** 所指定的下一跳，而不管该报文在路由表中的实际选路结果是否和策略路由指定的下一跳一致。 下一跳必须是直连的，否则此命令无效。
IPv6 策略路由	**set ipv6 next-hop**	配置下一跳。该命令的优先级比普通路由高。匹配 match 规则的 IPv6 报文将优先转发到 **set ipv6 nexthop** 所指定的下一跳，而不管该 IPv6 报文在路由表中的实际选路结果和策略路由指定的下一跳是否一致。 下一跳必须是直连的，否则此命令无效。

优先级顺序：**set ip nexthop >** 普通路由 **>** 缺省路由。以上 set 命令允许同时配置，但只有优先级最高的生效。

优先级顺序：**set ipv6 next-hop >** 普通路由 **>** 缺省路由。以上 set 命令允许同时配置，但只有优先级最高的生效。

在多个下一跳之间冗余备份或负载均衡

通过多次配置 set 规则，可以在一条策略中设置多个下一跳。多个下一跳之间可以是冗余备份，也可以是负载均衡。缺省为冗余备份。

- 冗余备份
  按配置顺序，第一个可达的下一跳生效。当前生效的下一跳（R1）发生故障后，流量会自动切换到下一个可达的下一跳（R2）。当 R1 恢复可达时，流量会自动切回 R1。
  新添加的下一跳排序在最后。假设多个下一跳的原有顺序为 R2/R3/R1，删除 R1 后再添加 R1，顺序变为 R2/R3/R1。
  如果所有的下一跳都不可达，则丢弃报文。

- 负载均衡
  多个下一跳之间基于流进行负载分担，可以设定负载分担的比重。某一个的生效下一跳失效后，将流量在其它生效下一跳上负载分担。

配置下一跳时，WCMP(Weighted Cost Multiple Path)最多支持 4 个下一跳， ECMP(Equal Cost Multiple Path)最多支持 32 个下一跳。

WCMP 下一跳的权重缺省值为 1。

4.1.2 策略路由

将包含策略的路由图应用在接口和设备上，即可实现策略路由。

- 将路由图应用在接口上，则接口收到的 IP 报文遵循策略进行路由。
  可控制该接口上收到的 IP 报文，对于从该接口发出的 IP 报文则不受策略控制。

一个接口最多只能配置一个路由图，在同一个接口上多次配置路由图会相互覆盖，后配置的生效。

- 将路由图应用在设备上，则设备发出的 IP 报文遵循策略进行路由。
  可控制本机发往其他设备的 IP 报文，对于其他设备发送给本机的 IP 报文则不受策略控制。

4.1.3 策略路由优先级

一般情况下，策略路由的优先级高于普通路由。即报文优先选用策略路由进行转发，如果没有匹配任意一个的策略路由条件，那么再按照普通路由进行转发。用户也可以配置策略路由的优先级比普通路由低，接口上收到的 IP/IPv6 报文则先进行普通路由的转发，如果无法匹配普通路由，再进行策略路由转发。

4.1.4 策略路由使用track功能

通过在 **set ip nexthop** 命令中增加参数设置，可以指定下一跳为 track 的跟踪对象。策略路由使用 track 功能，可以极大的增强策略路由对于网络环境变化的感知能力。

当 track 功能感知到当前用于转发的下一跳不可达，会立即通知策略路由将流量切换到下一个可达的下一跳（冗余备份）或者其余所有可达的下一跳（负载均衡）。

IPv6 PBR 不支持与 track 联动。

4.1.5 策略路由使用BFD功能

通过在 **set ip nexthop** 命令中增加参数设置，可以在本地与下一跳之间建立 BFD 会话。策略路由与 BFD 联动，可以极大的增强策略路由对于网络环境变化的感知能力。

当 BFD 功能感知到当前用于转发的下一跳不可达，会立即通知策略路由切换到下一个可达的下一跳（冗余备份）或者其余所有可达的下一跳（负载均衡）。

PBR 与 BFD 联动功能请参见“BFD”章节。

4.2 配置IPv4 策略路由

4.2.1 配置路由图

关于配置 route-map 的更多内容，请参见“IP 路由（协议无关）”章节。

PBR 容量相关配置，参见《硬件表项容量》文档“配置策略路由最大条目数”章节。

创建策略

命令	作用
Ruijie(config)# **route-map** *route-map-name* [{ **permit** | **deny** } *sequence*]	创建路由图中的策略。

设置 Match（匹配条件）

命令	作用
Ruijie(config-route-map)# **match ip address** {*access-list-number* | *access-list-name*}	设置匹配条件：IP 报文的源地址和目的地址属于 ACL 中定义的地址范围。

使用 Ruijie(config)# **ip access-list** {**extended** | **standard**} {*id* | *name*} 命令配置 ACL，定义 IP 报文的源地址/目的地址范围等。

设置 Set（处理动作）

命令	作用
Ruijie(config-route-map)# **set ip tos** <*0-15*>	修改 IP 报文的 TOS 域的值
Ruijie(config-route-map)# **set ip dscp** <*0-63*>	修改 IP 报文 DSCP 域的值
Ruijie(config-route-map)# **set ip next-hop** *ip-address* [*weight*] [*ip-address* [*weight*]]	设置下一跳

4.2.2 应用路由图

命令	作用
Ruijie(config-if)# **ip policy route-map** *name*	在接口上应用路由图，则接口收到的报文遵照策略转发。
Ruijie(config)# **ip local policy route-map** *route-map-name*	在设备上应用路由图，则本地发送的报文遵照策略转发。

例：配置策略路由，将 Fastethernet 0/0 收到的所有报文转发到 192.168.5.5。

```
Ruijie(config)# access-list 1 permit any
Ruijie(config)# route-map name
Ruijie(config-route-map)# match ip address 1
Ruijie(config-route-map)# set ip next-hop 192.168.5.5
Ruijie(config-route-map)# int fastethernet 0/0
Ruijie(config-if)# ip policy route-map name
```

4.2.3 设置多个下一跳之间是冗余备份或负载分担

命令	作用
Ruijie(config)# **ip policy** { **load-balance** | **redundance** }	设置多个下一跳之间为负载均衡或冗余备份。缺省为冗余备份。

4.3 配置IPV6 策略路由

PBR 容量相关配置，参见《硬件表项容量》文档“配置策略路由最大条目数”章节。

4.3.1 配置路由图

创建策略

命令	作用
Ruijie(config)# **route-map** *route-map-name* [**permit** | **deny**] *sequence*	创建路由图中的一条策略

设置 Match（匹配条件）

命令	作用
Ruijie(config-route-map)# **match ipv6 address** *access-list-name*	设置匹配条件：IP 报文的源地址和目的地址属于 ACL 中定义的地址范围。

使用 Ruijie(config)# **ipv6 access-list** *access-list-name* 命令配置 IPv6 ACL，定义 IPv6 报文的源地址/目的地址范围。

设置 Set（处理动作）

命令	作用
Ruijie (config-route-map)# **set ipv6 next-hop** *global-ipv6-address* [*weight*] [*global-ipv6-address* [*weight*]] [*global-ipv6-address*]	设置下一跳的 IPv6 地址。

4.3.2 应用路由图

命令	作用
Ruijie(config-if)# **ipv6 policy route-map** *route-map-name*	在接口应用策略路由

例：在 Fastethernet 0/0 口上配置策略路由，使所有进入的报文都转发到下一跳为 2001::1234 的设备。

```
Ruijie(config)# ipv6 access-list acl_pbr_1
Ruijie(config-ipv6-acl)#permit ipv6 any any
Ruijie(config)# route-map rm_fa_0_0
Ruijie(config-route-map)# match ipv6 address acl_pbr_1
Ruijie(config-route-map)# set ipv6 next-hop 2001::1234
Ruijie(config-route-map)# int fastethernet 0/0
Ruijie(config-if)# ipv6 policy route-map rm_fa_0_0
```

4.3.3 设置多个下一跳之间是冗余备份或负载分担

命令	作用
Ruijie(config)# **ipv6 policy** { **load-balance** | **redundance** }	设置多个下一跳之间为负载均衡或冗余备份。缺省为冗余备份。

4.4 监视与维护

命令	作用
Ruijie# **show access-list**	显示当前配置的 ACL。
Ruijie# **show route-map** [*name*]	显示当前配置的路由图。
Ruijie# **show ip policy** [*route-map-name*]	查看配置的 IPv4 策略路由。
Ruijie# **show ipv6 policy** [*route-map-name*]	显示配置的 IPv6 策略路由。

以下显示当前系统配置的 ACL：

```
Ruijie# show access-list
ipv6 access-list alc_pbr
 10 permit ipv6 any any
```

以下例子显示了当前系统配置的路由图：

```
Ruijie# show route-map
route-map RM_for_Vlan_1, permit, sequence 10
```

```
  Match clauses:
    ipv6 address acl_for_pbr_1
  Set clauses:
    ipv6 next-hop 2001::1234
route-map RM_for_Vlan_2, permit, sequence 10
  Match clauses:
    ipv6 address acl_for_pbr_2
  Set clauses:
ipv6 next-hop 2001::5678
```

以下例子显示了当前系统上应用的 IPv6 策略路由

```
Ruijie(config-if)#show ipv6 policy
Interface          Route map
VLAN 1             RM_for_Vlan_1
VLAN 2             RM_for_Vlan_2
```

4.5 配置举例

4.5.1 IPv4 策略路由

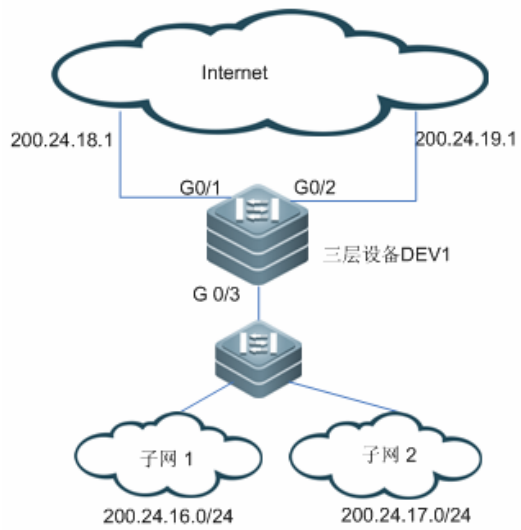
组网需求

某局域网有两个出口连接到因特网。通常情况下，希望这两个出接口能够实现负载分担并互为备份。具体要求是：子网 1 的所有访问因特网的数据流走出接口 GigabitEthernet 0/1；子网 2 的所有访问因特网的数据流走出接口 GigabitEthernet 0/2。如果出接口 GigabitEthernet 0/1 链路断开，那么能够将该接口上的数据流切换到 GigabitEthernet 0/2 上，反之亦然。

网络拓扑

三层设备 DEV1 通过 G0/3 口连接子网 1 和子网 2；通过 G0/1 和 G0/2 口连接因特网，其下一跳为 200.24.18.1、200.24.19.1。子网 1 的网段为 200.24.16.0/24，子网 2 的网段为 200.24.17.0/24。

图 4-1



配置步骤

配置两个不同的 ACL，分别用来匹配子网 1 和子网 2

```
Ruijie(config)#access-list 1 permit 200.24.16.0 0.0.0.255
Ruijie(config)#access-list 2 permit 200.24.17.0 0.0.0.255
```

配置用于控制子网 1 数据流的路由图，注意出接口 G0/1 的下一跳优先

```
Ruijie(config)#route-map RM_FOR_PBR 10
Ruijie(config-route-map)#match ip address 1
Ruijie(config-route-map)#set ip nexthop 200.24.18.1
Ruijie(config-route-map)#set ip nexthop 200.24.19.1
```

配置用于控制子网 2 数据流路由图，注意出接口 G0/2 的下一跳优先

```
Ruijie(config)#route-map RM_FOR_PBR 20
Ruijie(config-route-map)#match ip address 2
Ruijie(config-route-map)#set ip nexthop 200.24.19.1
Ruijie(config-route-map)#set ip nexthop 200.24.18.1
```

配置策略路由的负载分担模式为冗余备份

```
Ruijie(config)#ip policy redundance
```

在接口 GigabitEthernet 0/3 上应用策略路由

```
Ruijie(config)#interface GigabitEthernet 0/3
Ruijie(config-if)#ip policy route-map RM_FOR_PBR
```

4.5.2 IPv6 策略路由

组网需求

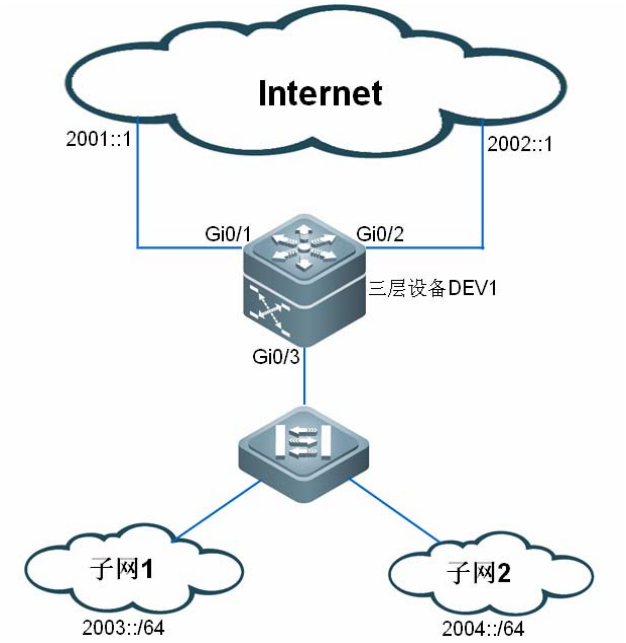
某局域网有两个出口连接到因特网。希望这两个出接口能够实现负载分担并互为备份。要求：

- 子网 1 的所有访问因特网的数据流走出接口 GigabitEthernet 0/1。
- 子网 2 的所有访问因特网的数据流走出接口 GigabitEthernet 0/2。
- 如果出接口 GigabitEthernet 0/1 链路断开，那么能够将该接口上的数据流切换到 GigabitEthernet 0/2 上，反之亦然。

组网拓扑

三层设备 DEV1 通过接口 G0/3（routed port 接口）连接子网 1 和子网 2；通过 G0/1 和 G0/2 口连接因特网，其下一跳为 2001::1/64、2002::1/64。子网 1 的网段为 2003::/64,子网 2 的网段为 2004::/64。

图 4-2



配置步骤

配置两个不同的 ACL，分别用来匹配子网 1 和子网 2

```
Ruijie(config)#ipv6 access-list net1
Ruijie(config-ipv6-acl)#permit ipv6 2003::/64 any
Ruijie(config)#ipv6 access-list net2
Ruijie(config-ipv6-acl)#permit ipv6 2004::/64 any
```

配置用于控制子网 1 数据流的路由图，注意出接口 G0/1 的下一跳优先

```
Ruijie(config)#route-map RM_FOR_PBR 10
Ruijie(config-route-map)#match ipv6 address net1
Ruijie(config-route-map)#set ipv6 next-hop 2001::1
Ruijie(config-route-map)#set ipv6 next-hop 2002::1
```

配置用于控制子网 2 数据流路由图，注意出接口 G0/2 的下一跳优先

```
Ruijie(config)#route-map RM_FOR_PBR 20
Ruijie(config-route-map)#match ipv6 address net2
Ruijie(config-route-map)#set ipv6 next-hop 2002::1
Ruijie(config-route-map)#set ipv6 next-hop 2001::1
```

配置策略路由的负载分担模式为冗余备份

```
Ruijie(config)#ipv6 policy redundance
```

在接口 GigabitEthernet 0/3 上应用策略路由

```
Ruijie(config)#interface GigabitEthernet 0/3
Ruijie(config-if-GigabitEthernet 0/3)#ipv6 policy route-map RM_FOR_PBR
```

显示验证

查看配置的路由图信息

```
Ruijie#show route-map
route-map RM_FOR_PBR, permit, sequence 10
  Match clauses:
    ipv6 address net1
  Set clauses:
    ipv6 next-hop 2001::1 2002::1
route-map RM_FOR_PBR, permit, sequence 20
  Match clauses:
    ipv6 address net2
  Set clauses:
ipv6 next-hop 2002::1 2001::1
```

查看 IPv6 策略路由应用信息

```
Ruijie#show ipv6 policy
Interface                    Route map
GigabitEthernet 0/3          RM_FOR_PBR
```

查看配置的 ACL 信息

```
Ruijie#show access-lists
ipv6 access-list net1
 10 permit ipv6 2003::/64 any
 (0 packets matched)
ipv6 access-list net2
 10 permit ipv6 2004::/64 any
 (0 packets matched)
```

4.5.3 使用track功能的IPv4 策略路由

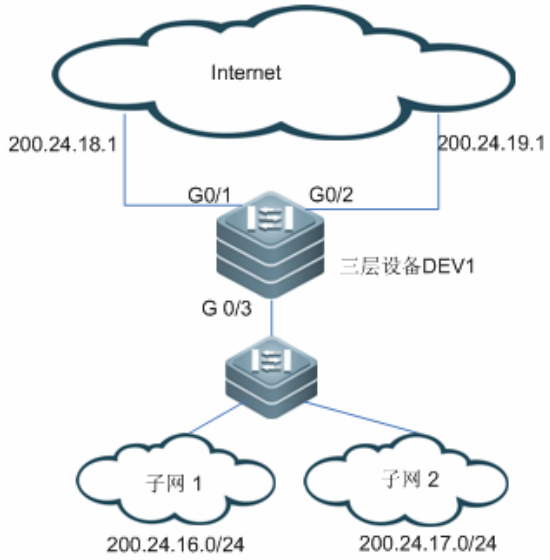
组网需求

某局域网有两个出口连接到因特网。通常情况下，希望这两个出接口能够实现负载分担并互为备份。具体要求是：子网 1 的所有访问因特网的数据流走出接口 GigabitEthernet 0/1；子网 2 的所有访问因特网的数据流走出接口 GigabitEthernet 0/2。如果下一跳 200.24.18.1 出现故障不能转发数据，那么在指定的时间内，能够将该接口上的数据流切换到 GigabitEthernet 0/2 上，反之亦然。

网络拓扑

三层设备 DEV1 通过 G0/3 口连接子网 1 和子网 2；通过 G0/1 和 G0/2 口连接因特网，其下一跳为 200.24.18.1、200.24.19.1。子网 1 的网段为 200.24.16.0/24，，子网 2 的网段为 200.24.17.0/24。

图 4-3



配置步骤

配置跟踪出接口 GigabitEthernet 0/1 下一跳 200.24.18.1

```
Ruijie(config)#ip rns 1
Ruijie(config-ip-rns)#icmp-echo 200.24.18.1
Ruijie(config)#track 1 rns 1
```

配置跟踪出接口 GigabitEthernet 0/2 下一跳 200.24.19.1

```
Ruijie(config)#ip rns 2
Ruijie(config-ip-rns)#icmp-echo 200.24.19.1
Ruijie(config)#track 2 rns 2
```

配置路由图使用该 track 对象

```
Ruijie(config)#route-map RM_FOR_PBR 10
Ruijie(config-route-map)#match ip address 1
Ruijie(config-route-map)#set ip nexthop verify-availability 200.24.18.1 track 1
Ruijie(config-route-map)#set ip nexthop verify-availability 200.24.19.1 track 2
```

配置用于控制子网 2 数据流路由图，注意出接口 G0/2 的下一跳优先

```
Ruijie(config)#route-map RM_FOR_PBR 20
Ruijie(config-route-map)#match ip address 1
Ruijie(config-route-map)#set ip nexthop verify-availability 200.24.19.1 track 2
Ruijie(config-route-map)#set ip nexthop verify-availability 200.24.18.1 track 1
```

配置策略路由的负载分担模式为冗余备份

```
Ruijie(config)#ip policy redundance
```

在接口 GigabitEthernet 0/3 上应用策略路由

```
Ruijie(config)#interface GigabitEthernet 0/3
Ruijie(config-if)#ip policy route-map RM_FOR_PBR
```

5 VRF

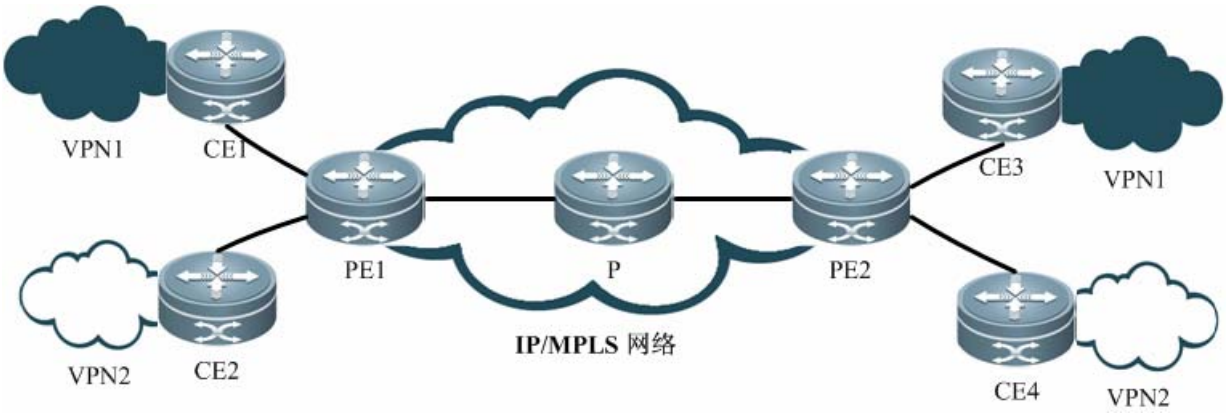
5.1 概述

VPN 为用户提供了一种安全的方式在 ISP 骨干网上共享带宽。一个 VPN 即是共享路由的站点集。用户站点通过一到多个接口链接到服务提供商网络，服务提供商为每一个接口关联一个 VPN 路由表。VPN 路由表也叫 VRF。

5.1.1 VRF的典型应用

传统 VPN 架构

图 5-1 传统的 BGP/MPLS VPN 架构



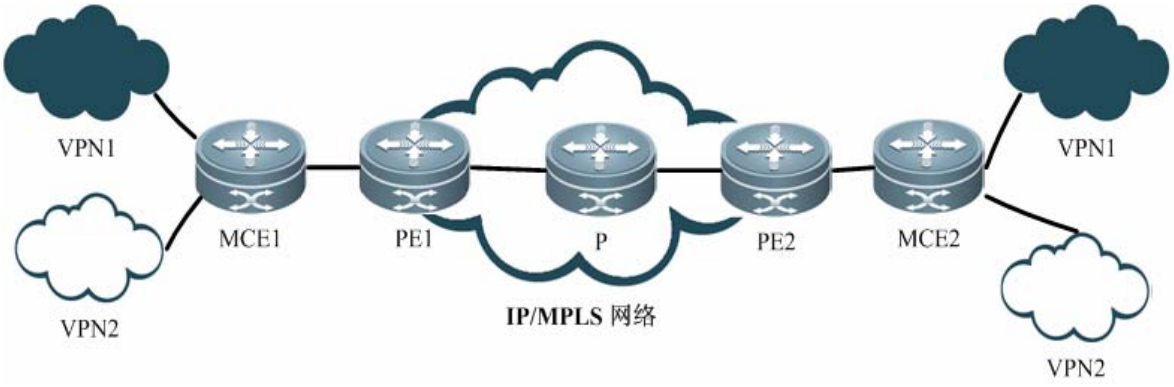
在传统的 BGP/MPLS VPN 中，每个 VPN 站点配备一台 CE。CE 仅供这一个 VPN 站点使用，不支持 VRF。

MCE 应用

MCE 即 multi-VRF CE，或 multi-VRF Customer Edge Device。

如果多个 VPN 站点共用一台 CE，则此 CE 被称为 MCE。与每个 VPN 站点一台 CE 相比，MCE 可以降低设备开支和维护成本，同时保持 VPN 之间的路由隔离。

图 5-2 MCE 应用环境



在 MCE 应用中，一个 MCE 连接多个 VPN 站点，为每个 VPN 维护一个 VRF，不同的 VRF 之间路由隔离。

MCE 和 PE 之间的物理线路被多个 VPN 公用，需要为每个 VPN 建立自己的逻辑线路。可以通过多种方式实现，如子接口、VLAN 接口。因此，MCE 和 PE 使用子接口、VLAN 接口绑定 VPN。

MCE 与 VPN 站点之间、MCE 与 PE 之间可以利用静态路由，动态路由协议（RIP、OSPF、ISIS、BGP）交互路由信息。PE 和 MCE 之间建议使用 EBGP。当然使用 OSPF、RIP、静态路由等也可以实现，其复杂度增加。如果使用 OSPF 进行路由交互，需要小心配置，建议在 OSPF 协议使用 capability vrf-lite 功能。

5.1.2 在VRF下配置路由

在 VRF 下配置的路由，仅用于指导此 VRF 的报文转发。

静态路由、动态路由协议（RIP、OSPF、BGP）均支持 VRF。

关于静态路由 VRF 的配置方法，请参见“IP 路由（协议无关）”章节。

关于 RIP VRF 的配置方法，请参见“RIP”章节。

关于 OSPF VRF 的配置方法，请参见“OSPF”章节。

关于 BGP VRF 的配置方法，请参见“BGP”章节。

5.1.3 缩略语

缩略语	说明
CE	Customer Edge Device，用户边界设备
PE	Provider Edge Device，运营商边界设备
MCE	Multi-CE，多角色 CE 设备
VPN	Virtual Private Network，虚拟专用网
VRF	VPN Routing and Forwarding Table，VPN 路由转发表

5.2 配置VRF

VRF 支持 IPV4，不支持 IPV6。

创建 VRF

命令	作用
Ruijie(config)# **ip vrf** *vrf-name*	创建 VRF，进入 VRF 模式。*vrf-name* 不要超过 31 个字符。
Ruijie(config)# **no ip vrf** *vrf-name*	删除名为 *vrf-name* 的 VRF。
Ruijie(config-vrf)# **description** *string*	配置 VRF 描述符，最大长度是 244 字符。

例：创建 VRF vrf1

```
Ruijie(config)#ip vrf vrf1
Ruijie(config-vrf)#description vpn-a
```

接口绑定 VRF

命令	作用
Ruijie(config-if)# **ip vrf forwarding** *vrf-name*	把接口绑定到 VRF。缺省情况下，接口属于不属于任何 VRF。
Ruijie(config-if)# **no ip vrf forwarding**	接口去除同 VRF 的绑定，这个时候接口属于全局。

必须先绑定 VRF，再配置 IPv4 地址。
如果将接口绑定到 VRF 之前，接口上已经配置了 IPv4 地址，则此配置将失效（保留 IPv6 配置）。

如果把接口绑定到 VRF，同时开启该接口的 IPv6 协议，则设备无法转发该接口上收到的 IPv6 报文。

5.3 监视与维护

命令	作用
Ruijie# **show ip route vrf** *vrf-name*	显示指定 VRF 中的路由
Ruijie# **show ip vrf** [*vrf-name*]	显示 VRF 的简要信息
Ruijie # **show ip vrf detail** [*vrf-name*]	显示 VRF 的详细信息
Ruijie # **show ip vrf interfaces** [*vrf-name*]	显示 VRF 的接口绑定信息

配置指南-组播

本分册介绍组播配置指南相关内容，包括以下章节：

1. IGMP Snooping
2. MLD Snooping

1 IGMP Snooping

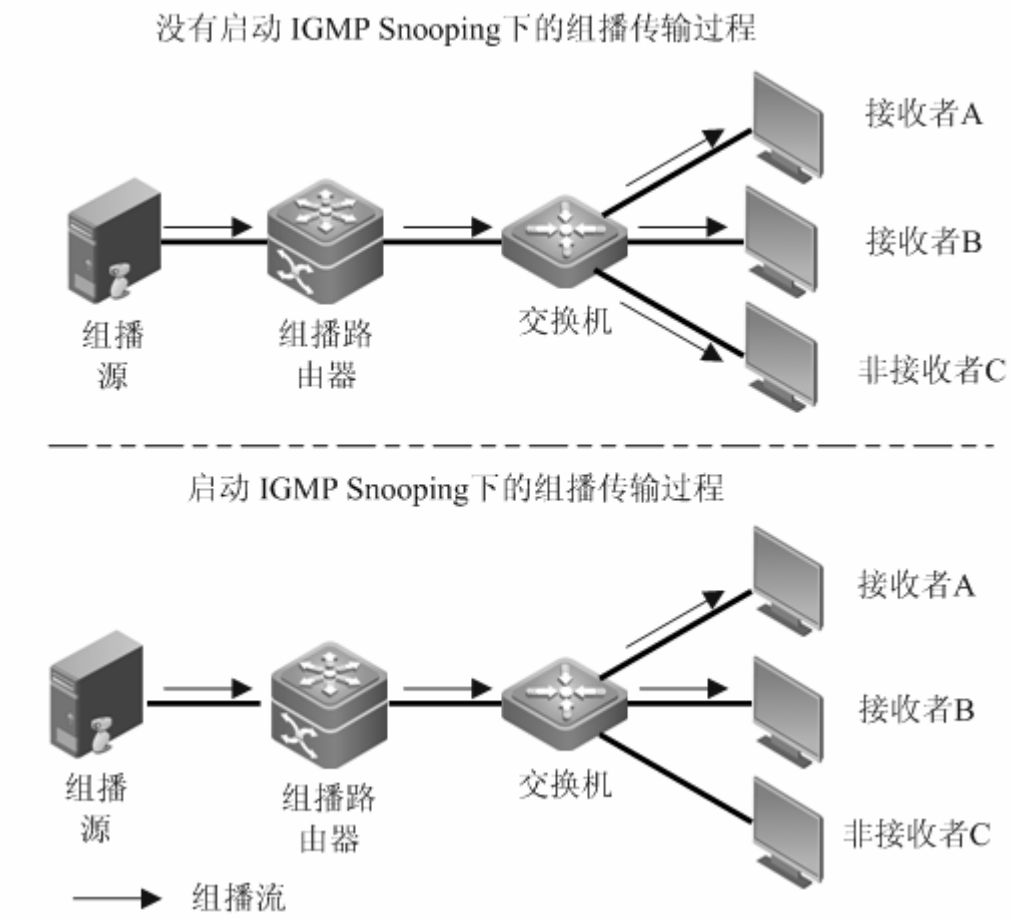
1.1 概述

1.1.1 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，都是指在 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。

图 1-1 VLAN 上运行 IGMP Snooping 前后的对比

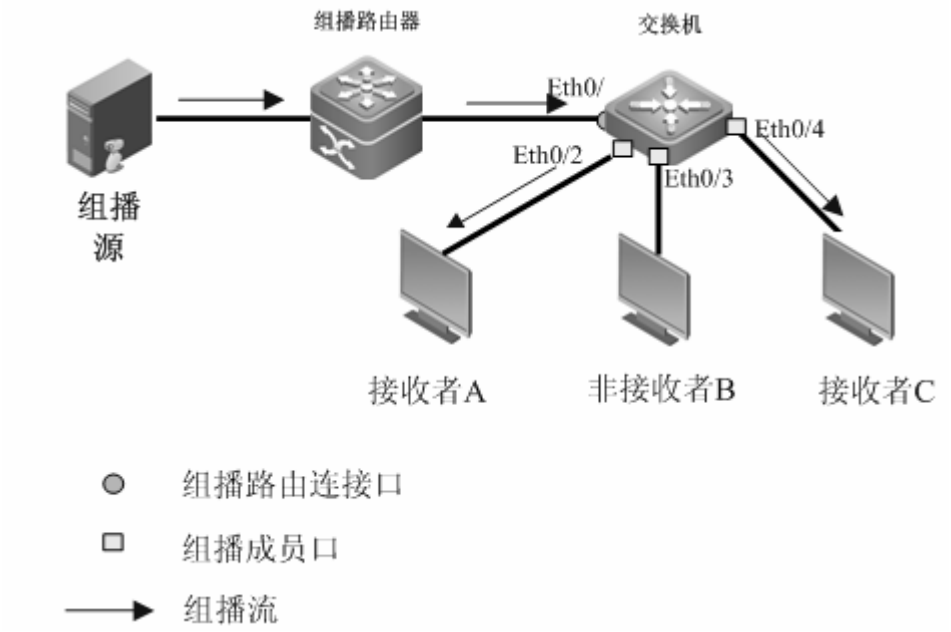


组播设备支持二层组播(IGMP Snooping)与三层组播(Multicast-routing)共同使用。即在一台设备上，既支持三层组播的路由转发，又支持在 VLAN 内的窥探，以实现更为精确的报文转发功能。

1.1.2 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）。

图 1-2 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，又称侦听者端口（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、Eth0/3 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。

1.1.3 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 普遍组查询报文或 PIM Hello 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 的查询报文	将该端口从 IGMP Snooping 组播组的转发表中删除

1.1.4 IGMP Snooping的工作机制

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）发送普通组查询报文，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 查询报文的最长响应时间，当定时器超时时，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。对于 IGMP 的特定组源查询报文，不做定时器的更新处理。

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，交换机将其通过给 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。

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。

1.1.5 IGMP Snooping的各种工作模式

- DISABLE 模式。在 DISABLE 模式下，IGMP Snooping 不起作用，即二层组播不起作用，VLAN 内不“窥探”主机与路由设备之间的 IGMP 报文，组播帧在 VLAN 内被广播。
- IVGL 模式(Independent VLAN Group Learning)。在 IVGL 模式下，各 VLAN 间的组播流是相互独立的。主机只能朝与自己处于同一个 VLAN 的路由连接口请求接收组播流；交换机在接收到任何一个 VLAN 的组播流时，只能往相同 VLAN 内的成员口转发。
- SVGL 模式(Shared VLAN Group Learning)。在 SVGL 模式下，各 VLAN 的主机共享同一组播流，主机可以跨 VLAN 申请组播流。必须指定一个 shared VLAN（缺省为 VLAN1），仅 shared VLAN 的组播流，可以被转发给该组地址对应的所有成员口，这些成员口可能属于各个 VLAN。必须用 profile 划分一个组地址范围给 SVGL，仅此范围内的组播流可以跨 VLAN 转发，此范围外的所有组播流将被丢弃。
- IVGL-SVGL 模式：也称为混杂模式。在 IVGL-SVGL 模式下，IVGL、SVGL 两种模式并存。必须用 Profile 划分一个组地址范围给 SVGL，在此范围内的组播流适用 SVGL 模式，此范围外的组播流适用 IVGL 模式。

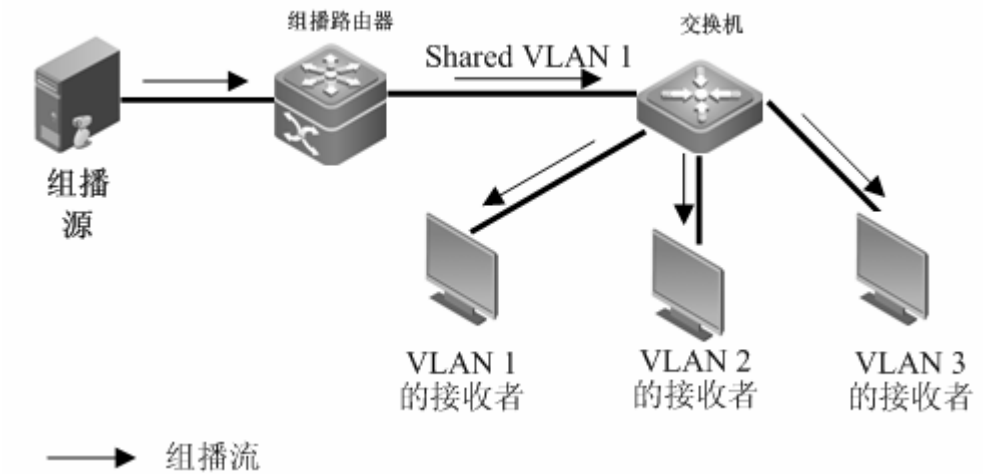
SVGL 模式、IVGL-SVGL 模式与 IP 组播功能相冲突。

PIM Snooping 必须依赖于 IGMP Snooping 的 IVGL 或 IVGL-SVGL 模式。

IGMP Profiles 用于定义组地址范围，供其他功能引用。

组播 VLAN

图 1-3 组播 VLAN



当 IGMP Snooping 运行在 SVGL 模式（或 IVGL-SVGL 模式）时，可以实现一种典型应用：组播 VLAN。如上图所示，交换机上运行 IGMP Snooping 的 SVGL 模式（或 IVGL-SVGL 模式），将用户主机所在的 VLAN 设置为子 VLAN，则当用户主机同时进行组播点播时，组播路由器只需把组播报文向 shared VLAN 复制一份，报文即可被交换机投送到各个子 VLAN。

而如果交换机上运行 IGMP Snooping 的 IVGL 模式，则组播路由器需要把组播数据在每个 VLAN 内都复制一份。这样既造成了带宽的浪费，也给三层设备增加了额外的负担。

1.1.6 IGMP Snooping和QinQ的关系

当在设备开启 IGMP Snooping 和配置了 dot1q-tunnel 端口之后，对于从 dot1q-tunnel 端口收到的 IGMP 报文，IGMP Snooping 可以有以下的两种处理方式。缺省情况下，工作于方式二。

- 方式一：将组播表项建立在 IGMP 报文所在的 VLAN 上。在 IGMP 报文所在的 VLAN 上转发 IGMP 报文。比如：假设设备开启 IGMP Snooping，设备的端口 A 为 dot1q-tunnel 端口，端口 A 的缺省 VLAN 为 VLAN 1，且端口 A 允许 VLAN 1 和 VLAN 10 的报文通过。当向端口 A 发送 VLAN 10 的组播请求报文时，IGMP Snooping 将建立 VLAN 10 的组播表项，并将组播请求报文转发到 VLAN 10 的路由连接口上。
- 方式二：将组播表项建立在 dot1q-tunnel 端口的缺省 VLAN 上。为组播报文添加一层 dot1q-tunnel 端口缺省 VLAN 的 VLAN Tag 之后，再将其在 dot1q-tunnel 端口的缺省 VLAN 内转发。比如：假设设备开启 IGMP Snooping，设备的端口 A 为 dot1q-tunnel 端口，端口 A 的缺省 VLAN 为 VLAN 1，且端口 A 允许 VLAN 1 和 VLAN 10 的报文通过。当向端口 A 发送 VLAN 10 的组播请求报文时，IGMP Snooping 将建立 VLAN 1 的组播表项，并为组播请求报文添加一层 VLAN 1 的 VLAN Tag 之后，再将其转发到 VLAN 1 的路由连接口上。

1.1.7 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。

1.1.8 组播安全控制

组播权限控制

IGMP 本身没有对用户是否能加入某个组播组进行控制的办法，而由于组播数据流是在接入节点进行复制的，因此在接入节点对用户是否允许获得某个组播视频流的控制，对视频数据的安全性、保障运营商利益、防止非法用户等方面显得尤为重要。目前，可以通过设备管理功能在用户端口预先设定个性化的 Profile，对于特定的一个或一组组播节目设置访问权限，允许或禁止用户的加入、控制组播业务，防止非法用户占用网络资源。通过类似的功能，还可以在接入节点上对用户访问组播节目进行更精细的控制，如组播预览等功能，对于特定用户，限制其可以观看的节目和数量等，从而有效保护网络带宽资源。

组播设备支持对用户进行多样化的控制：

- 基于端口控制用户点播组播流的权限
  在某些情况下，可能需要在端口上，对用户点播组播流的权限进行控制，此时可以采用基于端口的组播过滤器进行配置。详细配置见“配置端口过滤器”章节描述。
- 基于 VLAN 控制用户点播组播流的权限
  在某些情况下，可能需要在对不同 VLAN，允许点播不同范围的组播流，此时可以采用基于 VLAN 的组播过滤器进行配置。详细配置见“配置 VLAN 过滤器”章节描述。

- 基于端口控制用户所能点播的组播流数量
  如果用户在同一个端口点播多条组播流，对网络带宽会产生较大的压力，此时通过配置端口允许的组播流数量，可以有效地控制用户点播的组播流。详细配置见“配置 IGMP Filtering”章节描述。

- 组播预览
  对于一些组播视频流，如果用户没有开通点播此视频流的权限，而服务提供商又想能够让用户进行预览，达到预览时间后，再停止组播流。要实现这种功能，需要设备能够提供基于用户的组播预览功能。

源 IP 检查

IGMP SNOOPING 源 IP 检查功能，提高了网络的安全性。

IGMP SNOOPING 源 IP 检查指严格限定 IGMP 组播流的源 IP 地址。当 IGMP SNOOPING 源 IP 检查关闭时，进入的视频流均是合法的，二层组播设备会按照 IGMP Sooping 的转发表把它们转发到已注册的成员端口上。当 IGMP SNOOPING 源 IP 检查打开时，只有和设置的源 IP 地址相同的组播数据流才是合法的，组播设备把它们转发向已注册的端口；其它源 IP 地址的组播数据流被视为非法的，将被丢弃。

1.2 配置IGMP Snooping

- 当在 Private VLAN 或者 Super VLAN 上开启二层组播后，当子 VLAN 内存在组播源时，由于组播转发时需要进行入口合法性检查，此时需要多复制一条表项，入口为组播流进入的子 VLAN。造成的影响是多占用了一条组播硬件表项，表现出来的组播容量减少 1。部署网络时，建议组播流从 Private VLAN 或者 Super VLAN 的主 VLAN 进入，其它子 VLAN 作为出口 VLAN 连接主机接受组播流。

- 当在 Private VLAN 或者 Super VLAN 上开启二层组播，作为组播流转发出口的端口建议为 Access 口。如果组播流转发出口为 Trunk 口，可能会导致该 Trunk 口转发出多份重复组播流的情况发生。

- 当设备启动 IGMP Snooping 功能后，VLAN 内部的组播协议报文将不能在 VLAN 内进行硬件广播，此时这些组播协议报文将由软件进行广播，由于软件广播比硬件广播的转发性能低，因此 VLAN 内如果存在大量组播协议报文转发需求的情况下，建议关闭 IGMP Snooping 功能，以保证组播协议报文的转发性能。

1.2.1 启动IGMP Snooping（IVGL模式）

命令	作用
Ruijie(config)# **ip igmp snooping ivgl**	启动并设置 IGMP Snooping 为 IVGL 模式。

启动 IGMP Snooping 的时候，必须指定 IGMP Sooping 的工作模式。缺省情况下，IGMP Snooping 处于关闭状态。

例：打开并设置 IGMP Snooping 为 IVGL 模式

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping ivgl
Ruijie(config)# show ip igmp snooping
IGMP Snooping running mode: IVGL
SVGL vlan: 1
SVGL profile number: 0
Source port check: Disable
```

```
Source ip check: Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable
```

1.2.2 启动IGMP Snooping（SVGL或IVGL-SVGL模式）

IGMP Snooping 的 SVGL 模式或 IVGL-SVGL 模式，可以实现组播 VLAN。

在 SVGL 模式、IVGL-SVGL 模式下，组播数据报文跨 VLAN 转发后，报文的源 MAC 地址将被替换成交换机的 MAC 地址。

启动 SVGL 或 IVGL-SVGL 模式

命令	作用
Ruijie(config)# **ip igmp snooping svgl**	启动 IGMP Snooping 的 SVGL 模式
Ruijie(config)# **ip igmp snooping ivgl-svgl**	启动 IGMP Snooping 的 IVGL-SVGL 模式

例：打开并设置 IGMP Snooping 为 SVGL 模式

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping svgl
Ruijie(config)# show ip igmp snooping
IGMP Snooping running mode: SVGL
SVGL vlan: 1
SVGL profile number: 0
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable
```

例：打开并设置 IGMP Snooping 为 IVGL-SVGL 模式

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping ivgl-svgl
Ruijie(config)# show ip igmp snooping
IGMP Snooping running mode: IVGL_SVGL
SVGL vlan: 1
SVGL profile number: 0
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable
```

使用 profile 定义应用 SVGL 模式的组

命令	作用

Ruijie(config)# **ip igmp snooping svgl profile** *profile_num*	配置 SVGL 关联一条 profile
Ruijie(config)# **no ip igmp snooping svgl profile**	删除 SVGL 关联的 profile。

IGMP Snooping 的 SVGL 模式或 IVGL-SVGL 模式，必须为 SVGL 关联一个 profile，用于定义应用 SVGL 模式的组地址范围。只有此范围内的组播报文可以跨 VLAN 转发。如果未关联 profile，则没有一个组播组可以应用 SVGL 模式。

Profile 的配置方法参见后文“配置 IGMP Profile”。

例：配置 SVGL 模式应用的组地址范围

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping ivgl-svgl
Ruijie(config)# ip igmp snooping svgl profile 1
Ruijie(config)# end
Ruijie# show ip igmp snooping
IGMP Snooping running mode: IVGL_SVGL
SVGL vlan: 1
SVGL profile number: 1
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable
IGMP Globle Querier: Disable
IGMP Preview: Disable
IGMP Preveiw group aging time : 60(Seconds)
Dynamic Mroute Aging Time : 300(Seconds)
Tunnel IGMP Packet:  Disable
vlan 1
-------------
IGMP Snooping state: Enabled
Multicast router learning mode: pim-dvmrp
IGMPv2 immediate leave: Disabled
IGMP VLAN querier: Disable
```

指定 Shared VLAN

命令	作用
Ruijie(config)# **ip igmp snooping svgl vlan** *num*	指定 Shared VLAN。缺省为 VLAN 1。
Ruijie(config)# **no ip igmp snooping svgl vlan**	恢复 Shared VLAN 为缺省值。

IGMP Snooping 的 SVGL 模式或 IVGL-SVGL 模式，必须存在一个 Shared VLAN。只有发往 Shared VLAN 的组播报文才能被跨 VLAN 转发。

例：指定 Shared VLAN 为 VLAN 2

```
Ruijie# configure terminal
```

```
Ruijie(config)# ip igmp snooping svgl vlan 2
```

指定 Sub VLAN

命令	作用
Ruijie(config)# **ip igmp snooping svgl subvlan** *num*	指定子 VLAN。缺省所有 VLAN（非 Shared VLAN）都是子 VLAN。
Ruijie(config)# **no ip igmp snooping svgl subvlan**	取消子 VLAN。

如果不指定子 VLAN，则所有 VLAN 都可以收到 Shared VLAN 的组播报文。如果指定子 VLAN，则只有子 VLAN 能够收到 Shared VLAN 的组播报文。设备最多支持 127 个子 VLAN。

例：将 VLAN 3 和 VLAN 6 设置为子 VLAN

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping svgl subvlan 3,6
IGMP Snooping running mode: IVGL-SVGL
SVGL vlan: 1
SVGL profile number: 1
IGMP Snooping SVGL subvlan 3,6
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable
IGMP Globle Querier: Disable
Dynamic Mroute Aging Time : 300(Seconds)

vlan 1
-------------
IGMP Snooping state: Enabled
Multicast router learning mode: pim-dvmrp
IGMPv2 immediate leave: Disabled
IGMP VLAN querier: Disable

vlan 3
-------------
IGMP Snooping state: Enabled
Multicast router learning mode: pim-dvmrp
IGMPv2 immediate leave: Disabled
IGMP VLAN querier: Disable

vlan 4
-------------
IGMP Snooping state: Enabled
Multicast router learning mode: pim-dvmrp
IGMPv2 immediate leave: Disabled
IGMP VLAN querier: Disable
```

```
vlan 6
-------------
IGMP Snooping state: Enabled
Multicast router learning mode: pim-dvmrp
IGMPv2 immediate leave: Disabled
IGMP VLAN querier: Disable
```

1.2.3 关闭IGMP Snooping

命令	作用
Ruijie(config)# **no ip igmp snooping**	关闭所有 VLAN 的 IGMP Snooping。
Ruijie(config)# **no ip igmp snooping vlan** *num*	关闭指定 VLAN 的 IGMP Snooping。
Ruijie(config)# **ip igmp snooping vlan** *num*	打开指定 VLAN 的 IGMP Snooping。

当全局打开 IGMP Snooping，所有 VLAN 也将自动打开 IGMP Snooping 功能。使用 **no ip igmp snooping vlan** 命令可以仅在特定 VLAN 上关闭 IGMP Snooping 功能。

例：关闭 IGMP Snooping

```
Ruijie# configure terminal
Ruijie(config)# no ip igmp snooping
Ruijie(config)# show ip igmp snooping
IGMP Snooping running mode: DISABLE
SVGL vlan: 1
SVGL profile number: 0
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable
```

例：关闭 vlan 3 的 IGMP Snooping

```
Ruijie# configure terminal
Ruijie(config)# no ip igmp snooping vlan 3
Ruijie(config)# show ip igmp snooping
IGMP Snooping running mode: IVGL
SVGL vlan: 1
SVGL profile number: 0
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable

vlan 1
-------------
IGMP Snooping                   :Enabled
```

```
Multicast router learning mode  :pim-dvmrp
IGMPv2 immediate leave          :Disabled

vlan 2
-------------
IGMP Snooping                   :Enabled
Multicast router learning mode  :pim-dvmrp
IGMPv2 immediate leave          :Disabled

vlan 3
-------------
IGMP Snooping                   :Disabled
Multicast router learning mode  :pim-dvmrp
IGMPv2 immediate leave          :Disabled

vlan 4
-------------
IGMP Snooping                   :Enabled
Multicast router learning mode  :pim-dvmrp
IGMPv2 immediate leave          :Disabled
```

用户在 VLAN 内启用 IGMP Snooping 后，如果用户在该 VLAN 内存在 IPv6 组播应用，建议在该 VLAN 上也启用 MLD Snooping。

1.2.4 配置路由连接口

静态路由连接口

命令	作用
Ruijie(config)# **ip igmp snooping vlan** *vlan-id* **mrouter interface** *interface-id*	设置接口为静态路由连接口。
Ruijie(config)# **no ip igmp snooping vlan** *vlan-id* **mrouter interface** *interface-id*	取消接口为静态路由连接口。

在 IVGL 模式下，所有 VLAN 的静态路由连接口的配置均可生效。

在 SVGL 模式下，如果未配置 Sub VLAN，则只有属于 Share VLAN 的静态路由连接口的配置可生效，其它情况可配置但不生效；如果配置了 Sub VLAN，则属于 Share VLAN 或者非 Sub VLAN 的静态路由连接口的配置可生效，其它情况可配置但不生效。

在 IVGL-SVGL 模式下，如果未配置 Sub VLAN，所有 VLAN 的静态路由连接口的配置均可生效；如果配置了 Sub VLAN，则属于 Share VLAN 或者非 Sub VLAN 的静态路由连接口的配置可生效，其它情况可配置但不生效。

动态路由连接口

命令	作用
Ruijie(config)# **ip igmp snooping vlan** *vlan-id* **mrouter learn pim-dvmrp**	在 VLAN 上启动动态学习路由连接口的功能。缺省启动。
Ruijie(config)# **no ip igmp snooping vlan** *vlan-id* **mrouter learn pim-dvmrp**	关闭动态学习路由连接口的功能，并清空所有动态学习到的路由连接口。
Ruijie(config)# **ip igmp snooping dyn-mr-aging-time** *time*	配置动态路由连接口老化时间，取值范围 1-3600，默认值为 300s。
Ruijie(config)# **no ip igmp snooping dyn-mr-aging-time**	恢复动态路由连接口的老化时间为默认值。

对于动态路由连接口，如果在其老化时间超时前没有收到 IGMP 普遍组查询报文或者 PIM Hello 报文，交换机将把该端口从路由器端口列表中删除。

动态路由连接口的老化时间值应该根据实际网络拓扑及配置决定，即配置取值应该大于相关组播设备 Hello 消息发送间隔。建议配置成组播设备 Hello 消息发送间隔的 3.5 倍。

动态路由连接口老化时间并非即配即用。在下一次定时器更新时，才会启用该配置值。

例：设置以太网接口 1/1 为 VLAN1 的静态路由连接口，并启动 VLAN1 动态学习路由连接口功能

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping vlan 1 mrouter interface gigabitEthernet 1/1
Ruijie(config)# ip igmp snooping vlan 1 mrouter learn pim-dvmrp
Ruijie(config)# end
Ruijie# show ip igmp snooping mrouter
Vlan   Interface             State
----   --------------------   ------
1      GigabitEthernet 1/1   static
1      GigabitEthernet 0/2   dynamic
Ruijie# show ip igmp snooping mrouter learn
Vlan   learn method
----   ------------------
1      pim-dvmrp
```

例：配置动态路由连接口老化时间为 100s

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping dyn-mr-aging-time 100
```

1.2.5 配置成员口

静态成员口

命令	作用

Ruijie(config)# **ip igmp snooping vlan** *vlan-id* **static** *ip-addr* **interface** *interface-id*	配置一个静态成员口。 • *vlan-id*：组播流的 vid • *ip-addr*：组播地址 • *interface-id*： 端口号
Ruijie(config)# **no ip igmp snooping vlan** *vlan-id* **static** *ip-addr* **interface** *interface-id*	删除一个静态成员口。 • *vlan-id*：组播流的 vid • *ip-addr*：组播地址 • *interface-id*： 端口号

如果某端口所连接的主机需要固定接收发往某 IP 组播组的 IP 组播数据，可以配置该端口静态加入该 IP 组播组，成为静态成员端口。

可以用 **no ip igmp snooping vlan** *vlan-id* **static** *ip-addr* **interface** *interface-id* 删除组播成员的静态配置。

例：配置 IGMP snooping 静态成员端口

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping vlan 1 static 233.3.3.4 interface GigabitEthernet 0/7
Ruijie(config)# end
Ruijie# show ip igmp snooping gda
Abbr: M - mrouter
      D - dynamic
      S - static
VLAN  Address      Member ports
----  -----------  ----------------------
1     233.3.3.4    GigabitEthernet 0/7(S)
```

在 IVGL 模式下，所有 VLAN 的静态成员口的配置均可生效。

在 SVGL 模式下，如果未配置 Sub VLAN，则只有属于 Share VLAN 的静态成员口的配置可生效，其它情况可配置但不生效；如果配置了 Sub VLAN，则属于 Share VLAN 或者非 Sub VLAN 的静态成员口的配置可生效，其它情况可配置但不生效。

在 IVGL-SVGL 模式下，如果未配置 Sub VLAN，所有 VLAN 的静态成员口的配置均可生效；如果配置了 Sub VLAN，则属于 Share VLAN 或者非 Sub VLAN 的静态成员口的配置可生效，其它情况可配置但不生效。

动态成员口老化时间

命令	作用
Ruijie(config)# **ip igmp snooping host-aging-time** *time*	配置 IGMP 动态成员口存活时间，范围为 1-65535，缺省值为 260s。
Ruijie(config)# **no ip igmp snooping host-aging-time**	恢复 IGMP 查询报文的最长响应时间为缺省值。

动态成员端口老化时间是指当交换机的某端口收到主机发送的加入某 IP 组播组的 IGMP 加入报文时，为这个动态成员端口设置的老化时间。

在收到 IGMP 加入报文后，会重置这个动态成员端口的老化定时器，定时器时间为 host-aging-time。如果定时器超时，则认为该端口下不存在接收组播报文的用户主机，组播设备就会把该端口从 IGMP Snooping 的成员口中删除。配置完该命令，

后面收到的 IGMP 加入报文时设置的动态成员端口老化定时器的值为 host-aging-time。该配置在下一次收到加入报文时生效，当前已启动的成员口的定时器不会被更新。

例：配置 IGMP 动态端口老化时间为 30s

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping host-aging-time 30
```

IGMP 查询报文的最大响应时间

命令	作用
Ruijie(config)# **ip igmp snooping query-max-response-time** *time*	配置 IGMP 查询报文的最长响应时间，范围为 1-65535，缺省值为 10s。
Ruijie(config)# **no ip igmp snooping query-max-response-time**	恢复 IGMP 查询报文的最长响应时间为缺省值，缺省值为 10s。

在收到 IGMP 普通查询报文后，组播设备会重置所有动态成员口的老化定时器，定时器时间为 query-max-response-time。如果定时器超时，则认为该端口下不存在接收组播报文的用户主机，组播设备就会把该端口从 IGMP Snooping 的成员口中删除。

在收到 IGMP 特定组查询报文后，组播设备会重置该特定组的所有动态成员口的老化定时器，定时器时间为 query-max-response-time。如果定时器超时，则认为该端口下不存在接收组播报文的用户主机，组播设备就会把该端口从 IGMP Snooping 的成员口中删除。

对于 IGMPv3 的特定组源查询报文，不做定时器的更新处理。该配置在下一次收到查询报文时生效，当前已启动的定时器不会被更新。

例：配置 IGMP 查询报文的最长响应时间为 15s

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping query-max-response-time 15
```

成员口快速离开

命令	作用
Ruijie(config)# **ip igmp snooping fast-leave enable**	打开成员口快速离开功能。缺省关闭。
Ruijie(config)# **no ip igmp snooping fast-leave enable**	关闭端口快速离开功能。

端口快速离开是指当交换机从某端口收到主机发送的离开某 IP 组播组的 IGMP 离开组报文时，直接把该端口从对应转发表项的成员口中删除。在交换机上，如果端口下只连接有一个接收者，则可以通过使能端口快速离开功能以节约带宽和资源。该功能运用在相关端口下只存在一个点播者的情况。

例：打开成员口快速离开功能

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping fast-leave enalbe
```

1.2.6 配置IGMP report报文抑制

命令	作用
Ruijie(config)# **ip igmp snooping suppression enable**	打开 IGMP Report 报文抑制功能，缺省关闭。
Ruijie(config)# **no ip igmp snooping suppression enable**	关闭 IGMP Report 报文抑制功能。

每当成员口收到一个 IGMP Report 报文，都会将该报文转发给路由连接口。如果在一个查询间隔内，某 VLAN 的成员口上收到了多份相同的 Report 报文，路由连接口上就会收到多份相同的 Report 报文。如果打开 Report 报文抑制功能，则在一个查询间隔内，路由连接口只会将收到的某 IP 组播组的第一个 IGMP report 报文发送出去。否则路由连接口会将所有收到的 IGMP report 报文发送出去。打开 IGMP Report 报文抑制功能，有利于减少网络中的报文数量。

例：打开 IGMP Report 报文抑制功能

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping suppression enable
```

1.2.7 配置源IP检查

命令	作用
Ruijie(config)# **ip igmp snooping source-check default-server** *address*	打开源 IP 检查功能并指定默认源 IP。缺省关闭。
Ruijie(config)# **no ip igmp snooping source-check default-server**	关闭源 IP 检查功能。
Ruijie(config)# **ip igmp snooping limit-ipmc vlan** *vid* **address** *address* **server** *address*	（可选）为特定的 VLAN/组地址指定源 IP。缺省选用默认源 IP。
Ruijie(config)# **no ip igmp snooping limit-ipmc vlan** *vid* **address** *address*	取消为特定的 VLAN/组地址指定的源 IP。

必须先开启源 IP 检查，指定所有组的默认源 IP，才能对特定 VLAN 特定组指定源 IP 地址。

例：打开源 IP 检查，设置默认源 IP 为 1.1.1.1，VLAN1 组 233.3.3.3 的源 IP 为 1.1.1.2。

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping source-check default-server 1.1.1.1
Ruijie(config)# ip igmp snooping limit-ipmc vlan 1 address 233.3.3.3 server 1.1.1.2
```

IGMP Snooping 的源 IP 检查功能，不能同三层组播共用。即打开了三层组播的情况下，启动源 IP 检查功能，将对三层组播的转发会有影响。

1.2.8 配置IGMP Profiles

命令	作用
Ruijie(config)# **ip igmp profile** *profile-number*	进入 Profile 模式，分配一个数字以供标识，该数字范围为 1－1024，缺省情况下没有配置任何一条 profile。

Ruijie(config-profile)# **range** *low-address high_address*	设定组地址范围，该值即可以是一个单个的 IP 组地址也可以是一个组地址的区间（前面的为低 IP 组地址，后面为高 IP 组地址），同时可以配置多个 range 范围。
Ruijie (config-profile)# **permit** | **deny**	(可选）配置是要 permit 还是 deny 这一批组播地址范围，缺省值是 deny。这个行为表示：允许/禁止 range 内的这些组地址，并禁止/允许其它的组地址。

profile 是一种针对组的“过滤器”，供其它功能引用。配置步骤：

1，使用 ip igmp profile 命令创建一个 profile，并进入 profile 模式

2，使用 range 命令定义一个组范围

3，使用 permit 命令允许此范围内的组通过过滤器、使用 deny 命令将此范围内的组过滤掉。

如果要删除其中一个 profile，可以用 **no ip igmp profile** *profile number* 来执行。如果要删除 profile 里的一个 range，可以用 **no range** *ip multicast address* 来执行。

profile 缺省执行 deny。即所有未被 permit 的组，都被 deny。

例：配置 profile 1，允许组 224.2.2.2～224.2.2.244（不包括 224.2.2.117）

```
Ruijie(config)# ip igmp profile 1
Ruijie(config-profile)# range 224.2.2.2 224.2.2.244
Ruijie(config-profile)# permit
Ruijie(config-profile)# range 224.2.2.117
Ruijie(config-profile)# deny
```

1.2.9 配置端口过滤器

命令	作用
Ruijie(config-if)# **ip igmp snooping filter** *profile-number*	应用 Profile 于该端口，*profile number* 范围为 1- 1024。缺省情况下，一个端口不关联任何的 profile。
Ruijie(config-if)# **no ip igmp snooping filter**	删除接口上关联的 profile，接口上将允许所有组通过。
Ruijie(config-if)# **ip igmp snooping max-groups** *number*	限制端口能够动态加入的组数，参数范围为 0 – 1024。缺省情况下，无限制。

在某些情况下，可能需要控制某个端口只能接收一批特定的组播数据流、控制该端口下最多允许动态加入多少组。IGMP Filtering 满足了这种需求。

可以把某一个 IGMP Profile 应用在一个端口下，如果该端口收到 IGMP Report 报文，则二层组播设备就会查找这个端口所要加入的组播地址是否在 IGMP Profile 允许范围之内。若是，则允许加入，之后才进行后续处理。

也可以在一个端口下配置最多允许加入的组的个数，超过范围，二层组播设备也不再接收、处理 IGMP Report 报文。

例：配置端口过滤器

```
Ruijie# configure terminal
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# ip igmp snooping filter 1
```

```
Ruijie(config-if)# ip igmp snooping max-groups 1000
Ruijie(config-if)# end
Ruijie# show ip igmp snooping interface fastEthernet 0/1
Interface          Filter profile number  max-group
-----------------  ---------------------  ---------
FastEthernet 0/1   1                      1000
```

1.2.10 配置VLAN过滤器

命令	作用
Ruijie(config)# **ip igmp snooping vlan** *num* **filter** *profile-number*	应用 Profile 于该 VLAN，*profile number* 范围为 1- 1024。缺省情况下，一个 VLAN 不关联任何的 profile。
Ruijie(config-if)# **no ip igmp snooping vlan** *num* **filter**	删除 VLAN 上关联的 profile，VLAN 上将允许所有组通过。

在某些情况下，可能需要控制特定 VLAN 出口的组播数据流接收权限。基于 VLAN 的过滤器满足了这种需求。

可以把某一个 IGMP Profile 应用在一个 VLAN 下，如果该 VLAN 下的端口收到 IGMP Report 报文，则二层组播设备就会查找这个端口所要加入的组播地址是否在 IGMP Profile 允许范围之内。若是，则允许加入，之后才进行后续处理。

例：配置 VLAN 过滤器

```
Ruijie# configure terminal
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# ip igmp snooping vlan 2 filter 1
```

1.2.11 配置组播预览

命令	作用
Ruijie(config)# **ip igmp snooping preview** *profile-number*	应用 Profile 于该预览信息，*profile number* 范围为 1- 1024。缺省情况下，不允许任何组播流进行预览。
Ruijie(config)# **ip igmp snooping preview interval** *num*	配置预览时间，*num* 范围为<1- 300>,缺省情况为 60sec。
Ruijie(config)# **no ip igmp snooping preview**	不允许预览。

例：允许对不满足 profiles1 但满足 profiles2 的组播流进行组播预览

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping preview 2
Ruijie(config)# int fa 0/1
Ruijie(config-if)# ip igmp snooping filter 1
```

1.2.12 配置IGMP Snooping和QinQ的关系

命令	作用
Ruijie(config)# **ip igmp snooping tunnel**	打开透传 IGMP 报文的功能。缺省关闭。
Ruijie(config)# **no ip igmp snooping tunnel**	关闭透传 IGMP 报文的功能。

- 如果打开透传 IGMP 报文的功能，则连接在 dot1q-tunnel 端口的用户将需要点播从 IGMP 报文 VLAN 过来的组播流，将组播表项建立在 IGMP 报文所在的 VLAN 上，并在该 VLAN 内转发 IGMP 报文。例如：设备开启 IGMP Snooping，端口 A 为 dot1q-tunnel 端口，端口 A 的缺省 VLAN 为 VLAN 1，且端口 A 允许 VLAN 1 和 VLAN 10 的报文通过。当向端口 A 发送 VLAN 10 的组播请求报文时，IGMP Snooping 将建立 VLAN 10 的组播表项，并将组播请求报文转发到 VLAN 10 的路由连接口上。
- 如果关闭透传 IGMP 报文的功能，则连接在 dot1q-tunnel 端口的用户将需要点播从 dot1q-tunnel 端口的缺省 VLAN 上过来的组播流，将组播表项建立在 dot1q-tunnel 端口的缺省 VLAN 上，并为组播报文添加一层 dot1q-tunnel 端口缺省 VLAN 的 VLAN Tag 之后，再将其在 dot1q-tunnel 端口的缺省 VLAN 内转发。例如：设备开启 IGMP Snooping，端口 A 为 dot1q-tunnel 端口，端口 A 的缺省 VLAN 为 VLAN 1，且端口 A 允许 VLAN 1 和 VLAN 10 的报文通过。当向端口 A 发送 VLAN 10 的组播请求报文时，IGMP Snooping 将建立 VLAN 1 的组播表项，并为组播请求报文添加一层 VLAN 1 的 VLAN Tag 之后，再将其转发到 VLAN 1 的路由连接口上。

1.2.13 配置IGMP Snooping查询器

启动 IGMP Snooping 查询器

命令	作用
Ruijie(config)# **ip igmp snooping querier**	全局启动 IGMP Snooping 查询器功能。
Ruijie(config)# **no ip igmp snooping querier**	全局关闭 IGMP Snooping 查询器功能。
Ruijie(config)# **ip igmp snooping vlan** *num* **querier**	启动某 VLAN 的 IGMP Snooping 查询器功能。
Ruijie(config)# **no ip igmp snooping vlan** *num* **querier**	关闭某 VLAN 的 IGMP Snooping 查询器功能。

配置 IGMP Snooping 查询器的源 IP

命令	作用
Ruijie(config)# **ip igmp snooping querier address** a.b.c.d	全局配置查询器的源 IP 地址。
Ruijie(config)# **no ip igmp snooping querier address**	取消全局配置查询器的源 IP 地址。
Ruijie(config)# **ip igmp snooping vlan** *num* **querier address** a.b.c.d	配置某 VLAN 的查询器的源 IP 地址。
Ruijie(config)# **no ip igmp snooping vlan** *num* **querier address**	取消某 VLAN 的查询器的源 IP 地址。

例：全局配置查询器源 IP 地址

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping querier address 192.168.2.2
```

例：配置某 VLAN 的查询器源 IP 地址

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping vlan 2 querier address 192.168.2.2
```

配置查询报文最大响应时间

命令	作用
Ruijie(config)# **ip igmp snooping querier max-response-time** *num*	全局设置发送查询报文的最大响应时间。缺省值为 10sec。
Ruijie(config)# **no ip igmp snooping querier max-response-time**	全局恢复发送查询报文的最大响应时间为缺省值。
Ruijie(config)# **ip igmp snooping vlan** *num* **querier max-response-time** *num*	设置某 VLAN 的发送查询报文的最大响应时间。缺省值为 10sec。
Ruijie(config)# **no ip igmp snooping vlan** *num* **querier max-response-time**	恢复某 VLAN 的发送查询报文的最大响应时间为缺省值。

例：全局配置查询报文最大响应时间

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping querier 20
```

例：配置某 VLAN 的查询报文最大响应时间

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping vlan 2 querier 20
```

配置查询报文查询间隔

命令	作用
Ruijie(config)# **ip igmp snooping querier query-interval** *num*	全局设置 IGMP 定时发送查询报文的时间间隔。缺省值为 60sec。
Ruijie(config)# **no ip igmp snooping querier query-interval**	全局恢复 IGMP 定时发送查询报文的时间间隔为缺省值。
Ruijie(config)# **ip igmp snooping vlan** *num* **querier query-interval** *num*	设置某 VLAN 的 IGMP 定时发送查询报文的时间间隔。缺省值为 60sec。
Ruijie(config)# **no ip igmp snooping vlan** *num* **querier query-interval**	恢复某 VLAN 的 IGMP 定时发送查询报文的时间间隔为缺省值。

例：全局配置查询报文查询间隔

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping querier query-interval 300
```

例：配置某 VLAN 的查询报文查询间隔

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping vlan 2 querier query-interval 300
```

配置非查询者超时时间

命令	作用
Ruijie(config)# **ip igmp snooping querier timer expiry** *num*	全局配置非查询者超时时间。

Ruijie(config)# **no ip igmp snooping querier timer expiry**	全局配置非查询者超时时间为缺省值。
Ruijie(config)# **ip igmp snooping vlan** *num* **querier timer expiry** *num*	配置某 VLAN 的非查询者超时时间。
Ruijie(config)# **no ip igmp snooping vlan** *num* **querier timer expiry**	配置某 VLAN 的非查询者超时时间为缺省值。

例：全局配置非查询者超时时间

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping querier timer expiry 70
```

例：配置某 VLAN 的非查询者超时时间

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping vlan 2 querier timer expiry 70
```

配置 IGMP Snooping 查询器运行的 IGMP 版本

命令	作用
Ruijie(config)# **ip igmp snooping querier version** *num*	全局配置查询器运行的 IGMP 版本。取值范围为<1-2>,缺省值为 2。
Ruijie(config)# **no ip igmp snooping querier version**	全局恢复 IGMP 版本的缺省值。
Ruijie(config)# **ip igmp snooping vlan** *num* **querier version** *num*	VLAN 上配置查询器运行的 IGMP 版本。取值范围为<1-2>,缺省值为 2。
Ruijie(config)# **no ip igmp snooping vlan** *num* **querier version**	VLAN 上恢复 IGMP 版本的缺省值。

例：全局配置查询器运行的 IGMP 版本

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping querier version 1
```

例：VLAN 上配置查询器运行的 IGMP 版本

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping vlan 2 querier version 1
```

1.3 监视与维护

1.3.1 查看IGMP Snooping配置信息

命令	作用
Ruijie# **show ip igmp snooping**	查看 IGMP Snooping 当前的工作模式及全局配置。

例：查看 IGMP Snooping 配置信息

```
Ruijie# show ip igmp snooping
```

```
IGMP Snooping running mode: IVGL
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable
IGMP Globle Querier: Disable
IGMP Preview: Disable
IGMP Preveiw group aging time : 60(Seconds)
Dynamic Mroute Aging Time : 300(Seconds)
Tunnel IGMP Packet:  Disable

vlan 1
-------------
IGMP Snooping state: Enabled
Multicast router learning mode: pim-dvmrp
IGMPv2 fast leave: Disabled
IGMP VLAN querier: Disable
```

1.3.2 查看和清除IGMP Snooping的统计值

命令	作用
Ruijie# **show ip igmp snooping statistics** [**vlan** *vlan-id*]	查看 IGMP Snooping 的统计信息。
Ruijie# **clear ip igmp snooping statistics**	清除 IGMP Snooping 的统计信息

例：查看 IGMP Snooping 的统计信息

```
Ruijie# show ip igmp snooping statistics
Current number of Gda-table entries: 1
Configured Statistics database limit: 1024
Current number of IGMP Query packet received : 1957
Current number of IGMPv1/v2 Report packet received: 5
Current number of IGMPv3 Report packet received: 4
Current number of IGMP Leave packet received: 1

 GROUP     Interface  Last         Last       Report  Leave
                      report time  reporter   pkts    pkts
---------  ---------  -----------  ---------  ------  --------
233.3.3.3   gi1/1    00:02:40      1.1.1.1    3       1
```

1.3.3 查看路由连接口

命令	作用
Ruijie# **show ip igmp snooping mrouter**	查看 IGMP Snooping 的路由连接口信息。

例：查看 IGMP Snooping 的路由连接口

```
Ruijie# show ip igmp snooping mrouter
Multicast Switching Mroute Port
  D: DYNAMIC
  S: STATIC
(*, *, 1):
  VLAN(1)  1 MROUTES:
GigabitEthernet 0/2(S)
```

1.3.4 查看和清除IGMP Snooping的转发表

命令	作用
Ruijie# **show ip igmp snooping gda-table**	查看 IGMP Snooping 的转发表。 转发表即 GDA（Group Destination Address）表。
Ruijie# **clear ip igmp snooping gda-table**	清除动态成员口。 此命令不能删除静态成员口。

例：查看 GDA 表

```
Ruijie# show ip igmp snooping gda-table
Multicast Switching Cache Table
  D: DYNAMIC
  S: STATIC
  M: MROUTE
(*, 233.3.6.29, 1):
  VLAN(1) 3 OPORTS:
    GigabitEthernet 0/3(S)
    GigabitEthernet 0/2(M)
    GigabitEthernet 0/1(D)

(*, 233.3.6.30, 1):
  VLAN(1) 2 OPORTS:
    GigabitEthernet 0/2(M)
    GigabitEthernet 0/1(D)
```

如果在 Private-vlan 或者 Super-vlan 上启动了 IGMP Snooping，那么此时建立的 gda 转发表项都是基于 Private-vlan 或者 Super-vlan 的主 VLAN 创建的。该转发表项表明，所有转发出口都可以接收来自主 VLAN 过来的组播流信息；对于从子 VLAN 转发过来的组播流信息，其转发规则还需要遵循 Private-vlan 或者 Super-vlan 的转发规则进行。在这种情况下，每个 gda 的转发表项可能会对应多个硬件转发表项，所以会有可能表现出转发表项容量低于指标值的情况。

1.3.5 查看Profile

命令	作用
Ruijie# **show ip igmp profile** *profile-number*	查看 Profile 的信息。

例：查看 Profile 的信息

```
Ruijie# show ip igmp profile 1
Profile     1
        Permit
        range 224.0.1.0,    239.255.255.255
```

1.3.6 查看端口过滤器

命令	作用
Ruijie# **show ip igmp snooping interface** *interface*	查看端口过滤器的信息

例：查看 IGMP Filtering 的信息

```
Ruijie# show ip igmp snooping interface GigabitEthernet 0/7
Interface            Filter Profile number  max-groups
-------------------  ---------------------  -----------
GigabitEthernet 0/7  1                      4294967294
```

1.3.7 查看IGMP Snooping查询器

命令	作用
Ruijie# **show ip igmp snooping querier**	查看 IGMP Snooping 查询器的信息。
Ruijie# **show ip igmp snooping querier detail**	查看 IGMP Snooping 查询器的详细信息。

例：查看 IGMP Snooping 查询器的信息

```
Ruijie# show ip igmp snooping querier detail
Vlan      IP Address           IGMP Version           Port
-----------------------------------------------------------


Global IGMP switch querier status
---------------------------------------------------
admin state                    : Enable
admin version                  : 2
source IP address              : 1.1.1.1
query-interval (sec)           : 125
max-response-time (sec)        : 10
querier-timeout (sec)          : 60

Vlan 1:   IGMP switch querier status
---------------------------------------------------
admin state                    : Enable
admin version                  : 2
source IP address              : 1.1.2.2
query-interval (sec)           : 125
```

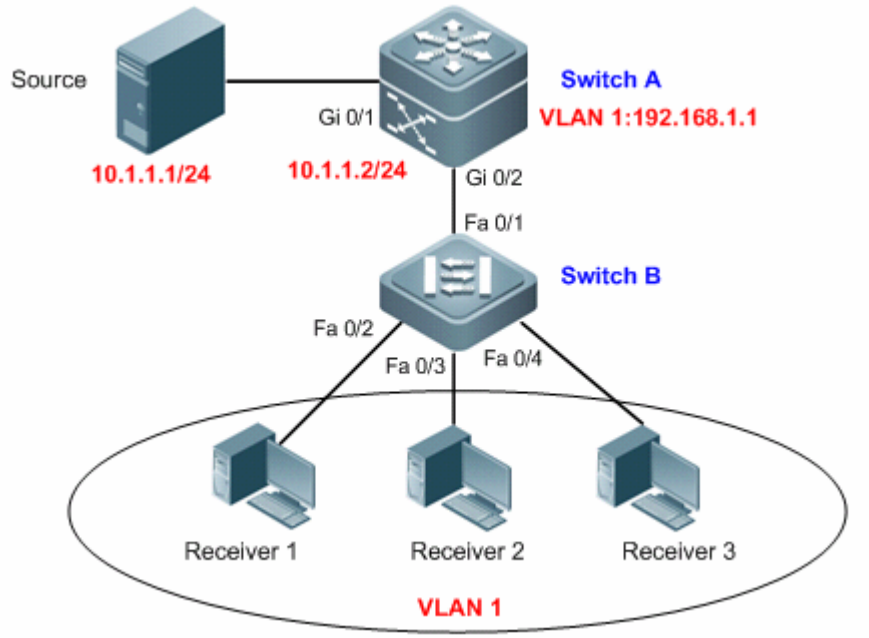
```
max-response-time (sec)         : 10
querier-timeout (sec)           : 60
operational state               : Disable
operational version             : 2

Vlan 2:   IGMP switch querier status
-------------------------------------------------------
admin state                     : Disable
admin version                   : 2
source IP address               : 1.1.1.1
query-interval (sec)            : 125
max-response-time (sec)         : 10
querier-timeout (sec)           : 60
operational state               : Disable
operational version             : 2
```

1.4 配置举例

1.4.1 IVGL模式典型应用

拓扑图

图 1-4



应用需求

如上图所示，Switch A 作为组播路由设备直连组播源，Switch B 作为二层接入设备下联多个组播接收者，属于同一个 VLAN。主要需求如下：

- 在 Switch A 上，实现三层组播路由；在 Switch B 上，组播数据流不会在 VLAN 内广播，能够发给指定的接收者。
- Receiver 1 能够固定接收组地址为 224.1.1.1 的 IP 组播数据流；Receiver 2 仅允许接收组地址为 225.1.1.1~226.1.1.1 的 IP 组播数据流；Receiver 3 仅允许加入 100 个 IP 组播组。
- 在 Switch B 上，所有接入端口能够快速离开某 IP 组播组。
- 在 Switch B 上，抑制 IGMP 成员转发给 Switch A 的响应报文，减轻 Switch A 的负担。

配置要点

- 在组播路由设备上（本例为 Switch A）开启相应的组播路由转发功能并在相应三层接口上配置组播路由协议（本例为 Gi 0/1 和 VLAN 1）；在二层组播设备上（本例为 Switch B）配置 IGMP Snooping 为 IVGL 模式，路由连接口可通过动态生成，也可以静态配置（本例配置端口 Fa 0/1 为静态路由连接口）。
- 将 Receiver 1 直连的端口（本例为 Fa 0/2）配置为对应组的静态成员端口；将 Receiver 2 直连的端口（本例为 Fa 0/3）配置 IGMP Filtering 功能；将 Receiver 3 直连的端口（本例为 Fa 0/4）配置允许最多动态加入的组播组数。
- 在运行 IGMP Snooping 的设备上（本例为 Switch B）配置端口快速离开功能。
- 在运行 IGMP Snooping 的设备上（本例为 Switch B）配置 IGMP Snooping 成员关系报告报文的响应抑制功能。

配置步骤

第一步，在组播路由设备上配置组播路由功能。

！在 Switch A 上全局开启组播路由转发功能。

```
SwitchA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)#ip multicast-routing
```

！将 Switch A 的端口 Gi 0/1 配置为 Route Port，用于连接组播源，并配置组播路由协议

```
SwitchA(config)#interface gigabitEthernet 0/1
SwitchA(config-if-GigabitEthernet 0/1)#no switchport
SwitchA(config-if-GigabitEthernet 0/1)#ip address 10.1.1.2 255.255.255.0
SwitchA(config-if-GigabitEthernet 0/1)#ip pim dense-mode
SwitchA(config-if-GigabitEthernet 0/1)#exit
```

！配置 VLAN 1 的 SVI，并在 SVI 上配置组播路由协议。

```
SwitchA(config)#interface vlan 1
SwitchA(config-if-VLAN 1)#ip address 192.168.1.1 255.255.255.0
SwitchA(config-if-VLAN 1)#ip pim dense-mode
SwitchA(config-if-VLAN 1)#exit
```

！将端口 Gi 0/2 配置为 Trunk Port，用于连接二层组播设备。

```
SwitchA(config)#interface gigabitEthernet 0/2
SwitchA(config-if-GigabitEthernet 0/2)#switchport mode trunk
SwitchA(config-if-GigabitEthernet 0/2)#exit
```

第二步，在二层组播设备上使能 IGMP Snooping，并设置路由连接口。

！在 Switch B 上，全局配置 IGMP Snooping 为 IVGL 模式，并配置 Fa 0/1 为 VLAN 1 的路由连接口。

```
SwitchB(config)#ip igmp snooping ivgl
SwitchB(config)#ip igmp snooping vlan 1 mrouter interface fastEthernet 0/1
```

第三步，配置 Receiver 1、2、3 相应要求。

！将端口 Fa 0/2 配置为 VLAN 1、组地址为 224.1.1.1 的静态成员端口。

```
SwitchB(config)#ip igmp snooping vlan 1 static 224.1.1.1 interface fastEthernet 0/2
```

！定义 IGMP Profile1 仅允许接收组地址为 225.1.1.1~226.1.1.1 的 IP 组播数据流，并应用在端口 Fa 0/3 上。

```
SwitchB(config)#ip igmp profile 1
SwitchB<config-profile>#permit
SwitchB<config-profile>#range 225.1.1.1 226.1.1.1
SwitchB<config-profile>#exit
SwitchB(config)#interface fastEthernet 0/3
SwitchB(config-if-FastEthernet 0/3)#ip igmp snooping filter 1
SwitchB(config-if-FastEthernet 0/3)#exit
```

！配置端口 Fa 0/4 仅允许最多动态加入 100 个组播组。

```
SwitchB(config)#interface fastEthernet 0/4
SwitchB(config-if-FastEthernet 0/4)#ip igmp snooping max-groups 100
SwitchB(config-if-FastEthernet 0/4)#exit
```

第四步，在二层组播设备上配置所有接入端口能够快速离开某 IP 组播组，并配置 IGMP 成员响应报文的抑制功能。

！在 Switch B 上，使能端口快速离开功能。

```
SwitchB(config)#ip igmp snooping fast-leave enable
```

！在 Switch B 上，使能 IGMP Snooping 成员关系报告报文的响应抑制功能。

```
SwitchB(config)#ip igmp snooping suppression enable
```

验证结果

第一步，查看设备的配置信息

！Switch A 的配置

```
SwitchA#show running-config
!
ip multicast-routing
!
```

```
interface GigabitEthernet 0/1
 no switchport
 ip pim dense-mode
 no ip proxy-arp
 ip address 10.1.1.2 255.255.255.0
!
interface GigabitEthernet 0/2
 switchport mode trunk
!
interface VLAN 1
 ip pim dense-mode
 no ip proxy-arp
 ip address 192.168.1.1 255.255.255.0
```

！Switch B 的配置

```
SwitchB#show running-config
!
interface FastEthernet 0/3
 ip igmp snooping filter 1
!
interface FastEthernet 0/4
 ip igmp snooping max-group 100
!
ip igmp profile 1
permit
range 225.1.1.1 226.1.1.1
ip igmp snooping ivgl
ip igmp snooping vlan 1 static 224.1.1.1 interface FastEthernet 0/2
ip igmp snooping vlan 1 mrouter interface FastEthernet 0/1
ip igmp snooping fast-leave enable
ip igmp snooping suppression enable
```

第二步，查看 Switch B 的 IGMP Snooping 基本信息

```
SwitchB#show ip igmp snooping
IGMP Snooping running mode: IVGL
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Enable
IGMP Report suppress: Enable
IGMP Globle Querier: Disable
IGMP Preview: Disable
IGMP Preveiw group aging time : 60(Seconds)
Dynamic Mroute Aging Time : 300(Seconds)
Tunnel IGMP Packet:  Disable
```

```
vlan 1
-------------
IGMP Snooping state: Enabled
Multicast router learning mode: pim-dvmrp
IGMPv2 fast leave: Disabled
IGMP VLAN querier: Disable
```

第三步，查看 Switch B 的路由连接口信息

```
SwitchB#show ip igmp snooping mrouter
Multicast Switching Mroute Port
  D: DYNAMIC
  S: STATIC
(*, *, 1):
  VLAN(1)  1 MROUTES:
    FastEthernet 0/1 (S)
```

第四步，查看 IGMP Snooping 的接口配置情况

```
SwitchB#show ip igmp snooping interfaces
Interface         Filter profile number  max-group
----------------  ---------------------  ---------
FastEthernet 0/3  1                      4294967294
FastEthernet 0/4  0                      100
```

第五步，通过 Source 发送组地址为 224.2.2.2 的 IP 组播数据流，在 Switch B 的端口 Fa 0/2 上点播组播，查看 Switch A 的组成员状况以及 Switch B 的 GDA 表如下：

！查看 Switch A

```
SwitchA#show ip igmp groups
IGMP Connected Group Membership
Group Address  Interface  Uptime    Expires   Last Reporter
224.2.2.2      VLAN 1     00:00:51  00:03:55  0.0.0.0
```

！查看 Switch B

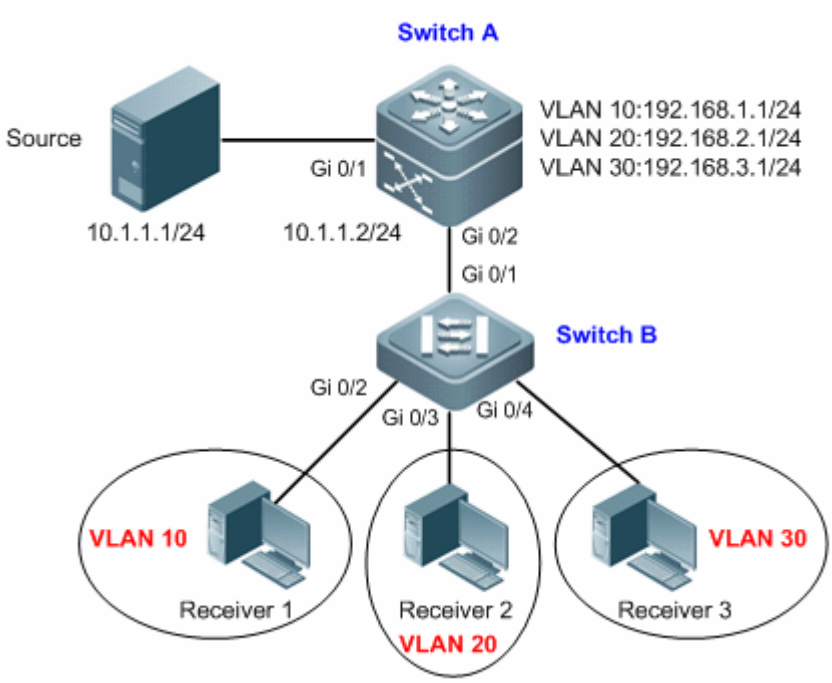
```
SwitchB#show ip igmp snooping gda-table
Multicast Switching Cache Table
  D: DYNAMIC
  S: STATIC
  M: MROUTE
(*,224.1.1.1, 1):
  VLAN(1) 2 OPORTS:
    FastEthernet 0/1(M)
    FastEthernet 0/2(S)
(*,224.2.2.2, 1):
  VLAN(1) 2 OPORTS:
```

```
FastEthernet 0/1(M)
FastEthernet 0/2(D)
```

1.4.2 IVGL-SVGL模式典型应用

拓扑图

图 1-5



应用需求

如上图所示，Switch A 作为组播路由设备直连组播源，Switch B 作为二层接入设备下联多个组播接收者，分别属于不同的 VLAN。主要需求如下：

- 在 Switch A 上，实现三层组播路由；在 Switch B 上，组播数据流不会在 VLAN 内广播，能够发给指定的接收者。
- 在 Switch B 上指定组播地址为 224.1.1.1~226.1.1.1 的 IP 组播数据流可以跨 VLAN 间转发，其它 IP 组播数据流只能往相同 VLAN 内的成员端口转发。

配置要点

- 在组播路由设备上（本例为 Switch A）开启相应的组播路由转发功能并在相应三层接口上配置组播路由协议（本例为 Gi 0/1 以及 VLAN 10、20、30）；在二层组播设备上（本例为 Switch B）配置 IGMP Snooping 为 IVGL-SVGL 模式，路由连接口可通过动态生成，也可以静态配置（本例配置端口 Gi 0/1 为静态路由连接口）。
- 在运行 IGMP Snooping 的二层组播设备（本例为 Switch B）上指定一个 VLAN 为 Share VLAN（本例为 VLAN 10），配置 Share VLAN 的组播地址范围(本例为 224.1.1.1~226.1.1.1)，则该组播地址范围内的 IP 组播数据流可以跨 VLAN 转发，并默认其它地址范围的 IP 组播数据流只能在相同的 VLAN 内转发。

配置步骤

第一步，在组播路由设备上配置组播路由功能。

！在 Switch A 上，全局开启组播路由转发功能。

```
SwitchA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)#ip multicast-routing
```

！将 Switch A 的端口 Gi 0/1 配置为 Route Port，用于连接组播源，并配置组播路由协议

```
SwitchA(config)#interface gigabitEthernet 0/1
SwitchA(config-if-GigabitEthernet 0/1)#no switchport
SwitchA(config-if-GigabitEthernet 0/1)#ip address 10.1.1.2 255.255.255.0
SwitchA(config-if-GigabitEthernet 0/1)#ip pim dense-mode
SwitchA(config-if-GigabitEthernet 0/1)#exit
```

！在 Switch A 上，配置 VLAN 10、20、30 的 SVI，并在 SVI 上配置组播路由协议。

```
SwitchA(config)#vlan 10
SwitchA(config-vlan)#exit
SwitchA(config)#interface vlan 10
SwitchA(config-if-VLAN 10)#ip address 192.168.1.1 255.255.255.0
SwitchA(config-if-VLAN 10)#ip pim dense-mode
SwitchA(config-if-VLAN 10)#exit
SwitchA(config)#vlan 20
SwitchA(config-vlan)#exit
SwitchA(config)#interface vlan 20
SwitchA(config-if-VLAN 20)#ip address 192.168.2.1 255.255.255.0
SwitchA(config-if-VLAN 20)#ip pim dense-mode
SwitchA(config-if-VLAN 20)#exit
SwitchA(config)#vlan 30
SwitchA(config-vlan)#exit
SwitchA(config)#interface vlan 30
SwitchA(config-if-VLAN 30)#ip address 192.168.3.1 255.255.255.0
SwitchA(config-if-VLAN 30)#ip pim dense-mode
SwitchA(config-if-VLAN 30)#exit
```

！在 Switch A 上，将端口 Gi 0/2 配置为 Trunk Port，用于连接二层组播设备。

```
SwitchA(config)#interface gigabitEthernet 0/2
SwitchA(config-if-GigabitEthernet 0/2)#switchport mode trunk
SwitchA(config-if-GigabitEthernet 0/2)#exit
```

第二步，在二层组播设备上创建 VLAN，并配置对应 VLAN 用户端口

！在 Switch B 上，创建 VLAN 10、20、30，配置端口 Gi 0/2 属于 VLAN 10、Gi 0/3 属于 VLAN 20，Gi 0/4 属于 VLAN 30。

```
SwitchB#configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchB(config)#interface gigabitEthernet 0/2
SwitchB(config-if-GigabitEthernet 0/2)#switchport access vlan 10
SwitchB(config-if-GigabitEthernet 0/2)#exit
SwitchB(config)#interface gigabitEthernet 0/3
SwitchB(config-if-GigabitEthernet 0/3)#switchport access vlan 20
SwitchB(config-if-GigabitEthernet 0/3)#exit
SwitchB(config)#interface gigabitEthernet 0/4
SwitchB(config-if-GigabitEthernet 0/4)#switchport access vlan 30
SwitchB(config-if-GigabitEthernet 0/4)#exit
```

！配置端口 Gi 0/1 为 Trunk Port。

```
SwitchB(config)#interface gigabitEthernet 0/1
SwitchB(config-if-GigabitEthernet 0/1)#switchport mode trunk
SwitchB(config-if-GigabitEthernet 0/1)#exit
```

第三步，在二层组播设备上使能 IGMP Snooping，并设置路由连接口。

！在 Switch B 上，全局配置 IGMP Snooping 为 IVGL-SVGL 模式，并配置 Gi 0/1 为 VLAN 10、20、30 的路由连接口。

```
SwitchB(config)#ip igmp snooping ivgl-svgl
SwitchB(config)#ip igmp snooping vlan 10 mrouter interface gigabitEthernet 0/1
SwitchB(config)#ip igmp snooping vlan 20 mrouter interface gigabitEthernet 0/1
SwitchB(config)#ip igmp snooping vlan 30 mrouter interface gigabitEthernet 0/1
```

第四步，在二层组播设备上配置 Share VLAN，并指定组播地址范围。

！在 Switch B 上，指定 VLAN 10 为 Share VLAN。

```
SwitchB(config)#ip igmp snooping svgl vlan 10
```

！在 Switch B 上，配置 IGMP Profile 1 允许 IP 组播地址为 224.1.1.1~226.1.1.1，并关联 SVGL 模式。

```
SwitchB(config)#ip igmp profile 1
SwitchB<config-profile>#permit
SwitchB<config-profile>#range 224.1.1.1 226.1.1.1
SwitchB<config-profile>#exit
SwitchB(config)#ip igmp snooping svgl profile 1
```

验证结果

第一步，查看设备的配置信息

！Switch A 的配置

```
SwitchA#show running-config
!
vlan 10
!
vlan 20
```

```
!
vlan 30
!
ip multicast-routing
!
interface GigabitEthernet 0/1
 no switchport
 ip pim dense-mode
 no ip proxy-arp
 ip address 10.1.1.2 255.255.255.0
!
interface GigabitEthernet 0/2
 switchport mode trunk
!
interface VLAN 10
 ip pim dense-mode
 no ip proxy-arp
 ip address 192.168.1.1 255.255.255.0
!
interface VLAN 20
 ip pim dense-mode
 no ip proxy-arp
 ip address 192.168.2.1 255.255.255.0
!
interface VLAN 30
 ip pim dense-mode
 no ip proxy-arp
 ip address 192.168.3.1 255.255.255.0
```

！Switch B 的配置

```
SwitchB#show running-config
!
vlan 10
!
vlan 20
!
vlan 30
!
interface GigabitEthernet 0/1
 switchport mode trunk
!
interface GigabitEthernet 0/2
 switchport access vlan 10
!
interface GigabitEthernet 0/3
```

```
 switchport access vlan 20
!
interface GigabitEthernet 0/4
 switchport access vlan 30
!
ip igmp profile 1
permit
range 224.1.1.1 226.1.1.1
ip igmp snooping ivgl-svgl
ip igmp snooping svgl vlan 10
ip igmp snooping svgl profile 1
ip igmp snooping vlan 10 mrouter interface GigabitEthernet 0/1
ip igmp snooping vlan 20 mrouter interface GigabitEthernet 0/1
ip igmp snooping vlan 30 mrouter interface GigabitEthernet 0/1
```

第二步，查看 Switch B 的 IGMP Snooping 基本信息

```
SwitchB#show ip igmp snooping
IGMP Snooping running mode: IVGL_SVGL
SVGL vlan: 10
SVGL profile number: 1
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable
IGMP Globle Querier: Disable
IGMP Preview: Disable
IGMP Preveiw group aging time : 60(Seconds)
Dynamic Mroute Aging Time : 300(Seconds)
Tunnel IGMP Packet:  Disable
vlan 1
-------------
IGMP Snooping state: Enabled
Multicast router learning mode: pim-dvmrp
IGMPv2 immediate leave: Disabled
IGMP VLAN querier: Disable

vlan 10
-------------
IGMP Snooping state: Enabled
Multicast router learning mode: pim-dvmrp
IGMPv2 immediate leave: Disabled
IGMP VLAN querier: Disable

vlan 20
-------------
```

```
IGMP Snooping state: Enabled
Multicast router learning mode: pim-dvmrp
IGMPv2 immediate leave: Disabled
IGMP VLAN querier: Disable

vlan 30
-------------
IGMP Snooping state: Enabled
Multicast router learning mode: pim-dvmrp
IGMPv2 immediate leave: Disabled
IGMP VLAN querier: Disable
```

第三步，查看 Switch B 的路由连接口信息

```
SwitchB#show ip igmp snooping mrouter
Multicast Switching Mroute Port
  D: DYNAMIC
  S: STATIC
(*, *, 10):
  VLAN(10)  1 MROUTES:
    GigabitEthernet 0/1(S)

(*, *, 20):
  VLAN(20)  1 MROUTES:
    GigabitEthernet 0/1(S)

(*, *, 30):
  VLAN(30)  1 MROUTES:
    GigabitEthernet 0/1(S)
```

第四步，通过 Source 发送组地址为 224.1.1.1 的 IP 组播数据流，在 Switch B 的端口 Gi 0/3（属于 VLAN 20，IP 地址 192.168.2.3）上点播组播，查看 Switch A 的组成员状况以及 Switch B 的 GDA 表如下：

！查看 Switch A

```
SwitchA#show ip igmp groups
IGMP Connected Group Membership
Group Address  Interface  Uptime    Expires   Last Reporter
224.1.1.1      VLAN 10    00:00:16  00:04:04  192.168.2.3
```

！查看 Switch B

```
SwitchB#show ip igmp snooping gda-table
Multicast Switching Cache Table
  D: DYNAMIC
  S: STATIC
  M: MROUTE
(*,224.1.1.1, 20):
```

```
  VLAN(1) 2 OPORTS:
    GigabitEthernet 0/3(D)
    GigabitEthernet 0/1(M)
```

！通过以上信息可以看出，端口 Gi 0/3 点播组地址为 224.1.1.1~226.1.1.1 的 IP 组播流，则按照 Share VLAN 10 转发。

第五步，通过 Source 发送组地址为 228.1.1.1 的 IP 组播数据流，在 Switch B 的端口 Gi 0/3（属于 VLAN 20，IP 地址 192.168.2.3）上点播组播，查看 Switch A 的组成员状况以及 Switch B 的 GDA 表如下：

！查看 Switch A

```
SwitchA#show ip igmp groups
IGMP Connected Group Membership
Group Address  Interface  Uptime    Expires   Last Reporter
228.1.1.1      VLAN 20    00:00:14  00:04:06  192.168.2.3
```

！查看 Switch B

```
SwitchB#show ip igmp snooping gda-table
Multicast Switching Cache Table
  D: DYNAMIC
  S: STATIC
  M: MROUTE
(*,228.1.1.1, 20):
  VLAN(1) 2 OPORTS:
    GigabitEthernet 0/3(D)
    GigabitEthernet 0/1(M)
```

！通过以上信息可以看出现，端口 Gi 0/3 点播组地址在 224.1.1.1~226.1.1.1 以外的 IP 组播数据流，则按照所属 VLAN 20 转发。

2 MLD Snooping

2.1 概述

MLD Snooping 是 Multicast Listener Discovery Snooping（组播侦听者发现协议窥探）的简称。它用于管理和控制 IPv6 组播流在二层上的转发行为。

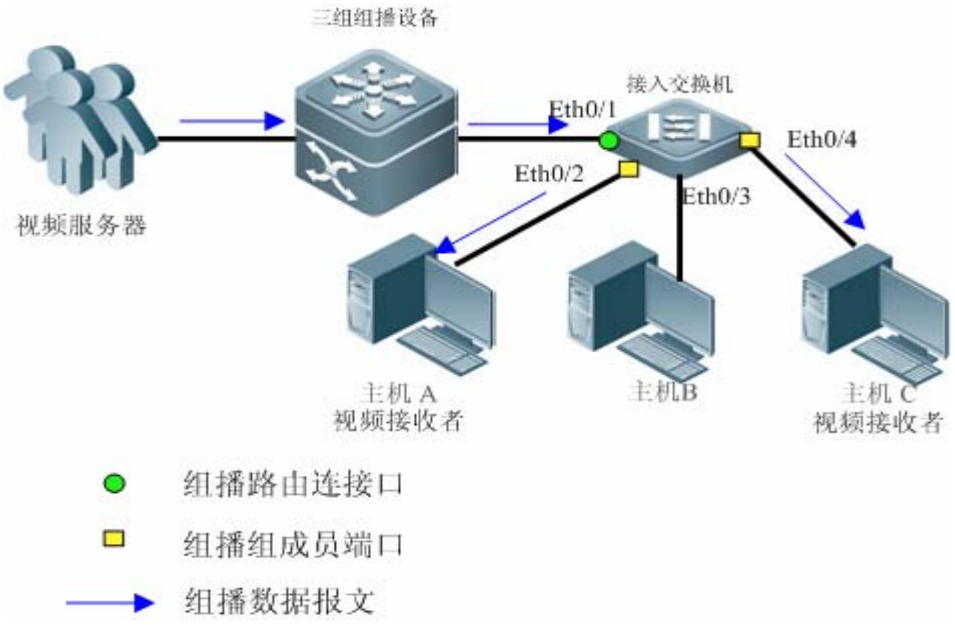
运行 MLD Snooping 的设备通过对收到的 MLD 报文进行分析，为端口和 MAC 组播地址建立起映射关系，并根据这样的映射关系在二层上转发 IPv6 组播数据。没有运行 MLD Snooping 时，IPv6 组播数据报文在二层被广播；当交换机运行了 MLD Snooping 后，已知 IPv6 组播组的组播数据报文不会在二层被广播，而是在二层交换到指定的接收者。

MLD Snooping 相关的协议规范：RFC4541

2.1.1 MLD Snooping的两类端口

如图所示，Router 连接组播源，在接入交换机运行 MLD Snooping，主机 A 和主机 C 为接收者主机（即 IPv6 组播组成员）。

图 2-1 MLD Snooping 的两类端口



- 路由连接口（Multicast Router Port）：交换机上连接三层组播设备，如接入交换的 Eth0/1 端口。
- 成员端口（Member Port）：IPv6 组播组成员端口的简称，又称侦听者端口（Listener Port），表示交换机上连接 IPv6 组播组成员侧的端口，如接入交换机 A 的 Eth0/2、Eth0/3 和 Eth0/4 端口。

2.1.2 MLD Snooping的工作模式

- DISABLE 模式：在该模式下，MLD Snooping 不起作用，即二层组播设备不“窥探”主机与路由设备之间的 MLD 报文，组播帧在 VLAN 内被广播。

- IVGL 工作模式(Independent VLAN Group Learn)：在该模式下，各 VLAN 间的组播流是相互独立的。主机只能朝与自己处于同一个 VLAN 的路由连接口请求接收组播流；交换机在接收到任何一个 VLAN 的组播数据流时，只能往相同 VLAN 内的成员端口转发。
- SVGL 工作模式(Shared VLAN Group Learn)：在该模式下，各 VLAN 的主机共享一组播流，主机可以跨 VLAN 申请组播流。指定一个 Shared VLAN，只有该 VLAN 的组播数据流才可以向跨 VLAN 的其他主机转发。只要组播数据流是属于 Shared VLAN 的，可以被转发给该组播地址的成员端口，即使有些成员端口不属于 Shared VLAN。SVGL 模式下，必须用 MLD Profile 划分一批组播地址范围给 SVGL，在这批组播地址范围内，组播转发表项的成员端口可以是跨 VLAN 转发；默认情况下所有的组范围都不在 SVGL 的应用范围，所有的组播流将被丢弃。
- IVGL-SVGL 模式：在该模式下，IVGL-SVGL 可以同时存在，可以用 MLD Profile 划分一批组播地址范围给 SVGL，在这批组播地址范围内，组播转发表项的成员端口可以是跨 VLAN 转发的，而其它的组播地址范围内对应的组播转发表项的成员端口必须是属于同一个 VLAN 的。

MLD Profiles 用于定义一个组地址范围，供其他功能引用。

2.1.3 MLD Snooping的工作原理

运行了 MLD Snooping 的交换机对不同 MLD 报文的的具体处理方式如下：

MLD QUERY

三层组播设备定期向本地网段内的所有主机与路由器（地址为 FF02::1）发送 MLD 一般组查询报文，以查询该网段有哪些 IPv6 组播组的成员。在收到 MLD 普遍组查询报文时，交换机将其通过给 VLAN 内除接收端口以外的其它所有端口转发出去，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。
- 每收到 MLD 的普遍组查询报文时，二层组播设备会对所有的成员端口启动各自的老化定时器进行更新，把其定时器时间降为配置的对 MLD 查询报文的最长响应时间。当该定时器的值减为 0 时，则认为该端口不再有成员接收组播流，二层组播设备就会把该端口从 MLD Snooping 的转发表中删除。
- 每收到 MLD 的特定组查询报文时，二层组播设备会对该特定组的所有成员端口启动老化定时器进行更新，把其定时器时间降为配置的对 MLD 查询报文的最长响应时间。当该定时器的值减为 0 时，则认为该端口不再有成员接收组播流，二层组播设备就会把该端口从 MLD Snooping 的转发表中删除。
- 当收到 MLD 的特定组源查询报文，不会对上述的两种定时器进行更新处理。

MLD REPORT

以下情况，主机会向 MLD 查询者发送 MLD 成员关系报告报文：

- 当 IPv6 组播组的成员主机收到 MLD 查询(普遍组查询或特定组查询)报文后，会应答 MLD 成员关系报告报文。
- 如果主机要加入某个 IPv6 组播组，它会主动向 MLD 查询者发送 MLD 成员关系报告报文以声明加入该 IPv6 组播组。

在收到 MLD 成员关系报告报文时，交换机将其通过给 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 IPv6 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 IPv6 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 IPv6 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 IPv6 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。

MLD LEAVE

当主机离开 IPv6 组播组时，会通过发送 MLD 离开组报文，以通知组播路由器自己离开了某个 IPv6 组播组。当交换机从某动态成员端口上收到 MLD 离开组报文时，将直接向路由连接口转发。如果启动了快速离开功能，设备将直接将相应的端口从相应组记录的转发端口列表中移出。

2.2 配置MLD Snooping

当在 Private VLAN 或者 Super VLAN 上开启二层组播后，当子 VLAN 内存在组播源时，由于组播转发时需要进行入口合法性检查，此时需要多复制一条表项，入口为组播流进入的子 VLAN。造成的影响是多占用了一条组播硬件表项，表现出来的组播容量减少 1。部署网络时，建议组播流从 Private VLAN 或者 Super VLAN 的主 VLAN 进入，其它子 VLAN 连接主机接受组播流。

当在 Private VLAN 或者 Super VLAN 上开启二层组播，作为组播流转发出口的端口建议为 Access 口。如果组播流转发出口为 Trunk 口，可能会导致该 Trunk 口转发出多份重复组播流的情况发生。

当设备启动 MLD Snooping 功能后，VLAN 内部的组播协议报文将不能在 VLAN 内进行硬件广播，此时这些组播协议报文将由软件进行广播，由于软件广播比硬件广播的转发性能低，因此 VLAN 内如果存在大量组播协议报文转发需求的情况下，建议关闭 MLD Snooping 功能，以保证组播协议报文的转发性能。

功能特性	缺省值
全局的 MLD Snooping 开关	关闭
基于 VLAN 的 MLD Snooping 开关	全局启动 MLD Snooping 后，基于 VLAN 的开关自动打开
路由连接口的老化间隔	300s
MLD 查询报文的最长响应时间	10s
动态学习路由连接口功能	关闭
组播组成员端口快速离开功能	关闭
MLD REPORT 抑制功能	关闭
基于端口对特定组播点播组过滤功能	关闭
基于端口限制最大组播组个数	1024

2.2.1 开启MLD Snooping（IVGL模式）

命令	作用
Ruijie(config)# **ipv6 mld snooping ivgl**	打开并设置 MLD Snooping 为 IVGL 模式。

以下例子是打开并设置 MLD Snooping 为 IVGL 模式：

```
Ruijie# configure terminal
```

```
Ruijie(config)# ipv6 mld snooping ivgl
Ruijie(config)# exit
Ruijie# show ipv6 mld snooping
MLD-snooping mode         :IVGL
SVGL vlan-id              :1
SVGL profile number       :0
Source check port         :Disable
Query Max Respone Time    :10 (Seconds)
```

2.2.2 开启MLD Snooping（SVGL或IVGL-SVGL模式）

启动 SVGL 或 IVGL-SVGL 模式

命令	作用
Ruijie(config)# **ipv6 mld snooping svgl**	打开并设置 MLD Snooping 为 SVGL 模式。
Ruijie(config)# **ipv6 mld nooping ivgl-svgl**	打开并设置 MLD Snooping 为 IVGL-SVGL 模式。

当配置模式为 SVGL 或 IVGL-SVGL 模式时，必须关联一个 porfile 用于指定 SVGL 模式应用的组播地址范围。

MLD SNOPING SVGL 模式和 ipv4/v6 三层组播不能共存。

在 SVGL 模式、IVGL-SVGL 模式下，组播数据报文跨 VLAN 转发后，报文的源 MAC 地址将被替换成交换机的 MAC 地址。

以下例子是打开并设置 MLD Snooping 为 SVGL 模式：

```
Ruijie# configure terminal
Ruijie(config)# ipv6 mld snooping svgl
Ruijie(config)# exit
Ruijie# show ipv6 mld snooping
MLD-snooping mode         :SVGL
SVGL vlan-id              :1
SVGL profile number       :0
Source check port         :Disable
Query Max Respone Time    :10 (Seconds)
```

以下例子是打开并设置 MLD Snooping 为 IVGL-SVGL 模式：

```
Ruijie# configure terminal
Ruijie(config)# ipv6 mld snooping ivgl-svgl
Ruijie(config)# exit
Ruijie# show ipv6 mld snooping
MLD-snooping mode         :IVGL-SVGL
SVGL vlan-id              :1
SVGL profile number       :0
Source check port         :Disable
Query Max Respone Time    :10 (Seconds)
```

配置 SVGL 模式应用的组播地址范围

命令	作用
Ruijie(config)# **ipv6 mld snooping svgl profile** 1	svgl 关联 profile1。

当配置了 MLD Snooping 的工作模式为纯 SVGL 模式或是混杂的 IVGL-SVGL 并存模式，此时都需要为 SVGL 关联一个 profile，用于指明哪些组地址范围内可以应用 SVGL 模式，即组播转发表项的成员端口可以是跨 VLAN 转发的，而其它的组播地址范围内对应的组播转发表项的成员端口必须是属于同一个 VLAN 的。缺省的情况下，没有关联任何一个 profile，则认为没有一个组播组可以应用 SVGL 模式。

以下是配置 SVGL 模式应用的组播地址范围的实例：

```
Ruijie# configure terminal
Ruijie(config)# ipv6 mld snooping ivgl-svgl
Ruijie(config)# ipv6 mld snooping svgl profile 1
Ruijie(config)# end
Ruijie# show ipv6 mld snooping
MLD-snooping mode         :IVGL
SVGL vlan-id              :1
SVGL profile number       :1
Source check port         :Disable
Query Max Respone Time    :10 (Seconds)
```

指定 Shared VLAN

命令	作用
Ruijie(config)# **ipv6 mld snooping svgl vlan** *num*	指定 Shared VLAN。缺省为 VLAN 1。
Ruijie(config)# **no ipv6 mld snooping svgl vlan**	恢复 Shared VLAN 为缺省值。

MLD Snooping 的 SVGL 模式或 IVGL-SVGL 模式，必须存在一个 Shared VLAN。只有发往 Shared VLAN 的组播报文才能被跨 VLAN 转发。

例：指定 Shared VLAN 为 VLAN 2

```
Ruijie# configure terminal
Ruijie(config)# ipv6 mld snooping svgl vlan 2
```

2.2.3 关闭MLD Snooping

命令	作用
Ruijie(config)# **no ipv6 mld snooping**	关闭 MLD Snooping。
Ruijie(config)# **no ipv6 mld snooping vlan** *vlan_id*	关闭特定 vlan 的 MLD Snooping。
Ruijie(config)# **ipv6 mld snooping vlan** *vlan_id*	打开特定 vlan 的 MLD Snooping。

以下例子是关闭 MLD Snooping：

```
Ruijie# configure terminal
```

```
Ruijie(config)# no ipv6 mld snooping
Ruijie(config)# exit
Ruijie# show ipv6 mld snooping
MLD-snooping mode         :DISABLE
SVGL vlan-id              :1
SVGL profile number       :0
Source check port         :Disable
Query Max Respone Time    :10 (Seconds)
```

以下例子是关闭 vlan 2 的 MLD Snooping：

```
Ruijie# configure terminal
Ruijie(config)# no ipv6 mld snooping vlan 2
Ruijie(config)# end
Ruijie# show ipv6 mld snooping
MLD-snooping mode         :IVGL
SVGL vlan-id              :1
SVGL profile number       :0
Source check port         :Disable
Query Max Respone Time    :10 (Seconds)
DISABLE VLAN              :2
```

用户在 VLAN 内启用 MLD Snooping 后，如果用户在该 VLAN 内存在 IPv4 组播应用，建议在该 VLAN 上也启用 IGMP Snooping。

2.2.4 配置动态路由连接口的老化定时器

命令	作用
Ruijie(config)# **ipv6 mld snooping dyn-mr-aging-time** *time*	配置动态路由连接口老化时间。默认值为 300s。 *time* ：<1-3600>
Ruijie(config)# **no ipv6 mld snooping dyn-mr-aging-time**	恢复动态路由连接口的老化时间为默认值。

对于动态路由连接口，如果在其老化时间超时前没有收到 MLD 普遍组查询报文或者 IPv6 PIM Hello 报文，交换机将把该端口从路由器端口列表中删除。

以下例子是配置动态路由连接口老化时间为 100s：

```
Ruijie# configure terminal
Ruijie(config)# ipv6 mld snooping dyn-mr-aging-time 100
```

2.2.5 配置路由连接口

命令	作用
Ruijie(config)# **ipv6 mld snooping vlan** *vlan-id* **mrouter interface** *interface-id*	设置接口为静态路由连接口。

Ruijie(config)# **no ipv6 mld snooping vlan** *vlan-id* **mrouter interface** *interface-id*	取消接口为静态路由连接口。
Ruijie(config)# **ipv6 mld snooping vlan** *vlan-id* **mrouter learn**	允许动态学习路由连接口。缺省允许。
Ruijie(config)# **no ipv6 mld snooping vlan** *vlan-id* **mrouter learn**	关闭动态学习，并清空该 vlan 的所有动态学习到的路由连接口。

以下例子是设置以太网接口 0/1 为路由连接口，并配置自动学习路由连接口：

```
Ruijie# configure terminal
Ruijie(config)# ipv6 mld snooping vlan 1 mrouter interface gigabitEthernet 0/1
Ruijie(config)# ipv6 mld snooping vlan 1 mrouter learn
Ruijie(config)# end
Ruijie# show ipv6 mld snooping mrouter
Vlan   Interface             State    MLD profile
----   --------------------   ------   -------------
1      GigabitEthernet 0/1   static   0
1      GigabitEthernet 0/2   dynamic  0
Ruijie# show ipv6 mld snooping mrouter learn
Vlan   learn method
----   ------------
1      pim
```

2.2.6 配置静态成员端口

命令	作用
Ruijie(config)# **ipv6 mld snooping vlan** *vlan-id* **static** *ip-addr* **interface** *interface-id*	静态配置一个端口接收某个组播流。 • *vlan-id*：组播流的 vid • *ip-addr*：组播地址 • *interface-id*： 端口号
Ruijie(config)# **no ipv6 mld snooping vlan** *vlan-id* **static** *ip-addr* **interface** *interface-id*	删除组播成员的静态配置。

如果某端口所连接的主机需要固定接收发往某 IPv6 组播组的 IPv6 组播数据，可以配置该端口静态加入该 IPv6 组播组，成为静态成员端口。

以下例子是配置 MLD Snooping 静态成员端口：

```
Ruijie# configure terminal
Ruijie(config)# ipv6 mld snooping vlan 1 static FF88::1234 interface GigabitEthernet 0/7
Ruijie(config)# end
Ruijie# show ipv6 mld snooping gda
Abbr: M - mrouter
      D - dynamic
      S - static
VLAN   Address      Member ports
----   ----------   ----------------------
```

```
1       FF88::1234    GigabitEthernet 0/7(S)
```

2.2.7 配置端口快速离开

命令	作用
Ruijie(config)# **ipv6 mld snooping fast-leave enable**	打开二层组播设备的快速离开功能。缺省关闭。
Ruijie(config)# **no ipv6 mld snooping fast–leave enalbe**	关闭端口快速离开功能。

端口快速离开是指当交换机从某端口收到主机发送的离开某 IPv6 组播组的 MLD 离开组报文时，直接把该端口从对应转发表项的出端口列表中删除。在交换机上，如果端口下只连接有一个接收者，则可以通过使能端口快速离开功能以节约带宽和资源。

以下例子是打开端口快速离开功能：

```
Ruijie# configure terminal
Ruijie(config)# ipv6 mld snooping fast–leave enalbe
```

2.2.8 配置report报文抑制功能

命令	作用
Ruijie(config)# **ipv6 mld snooping suppression enable**	打开 suppression 功能。缺省关闭。
Ruijie(config)# **no ipv6 mld snooping suppression enalbe**	关闭 Suppression 功能

当二层设备收到来自某 IPv6 组播组成员的 MLD 成员关系报告报文时，会将该报文转发给与其直连的三层设备。这样，当二层设备上存在属于某 IPv6 组播组的多个成员时，与其直连的三层设备会收到这些成员发送的相同 MLD 成员关系报告报文。

当使能了 MLD 成员关系报告报文抑制功能后，在一个查询间隔内二层设备只会把收到的某 IPv6 组播组内的第一个 MLD 成员关系报告报文转发给三层设备，而不继续向三层设备转发来自同一组播组的其它 MLD 成员关系报告报文，这样可以减少网络中的报文数量。

以下例子是打开 Suppression 功能：

```
Ruijie# configure terminal
Ruijie(config)# ipv6 mld snooping suppression enable
```

2.2.9 配置MLD Profiles

命令	作用
Ruijie(config)# **ipv6 mld profile** *profile-number*	进入 MLD Profile 模式，分配一个数字以供标识，该数字范围为 1－1024。
Ruijie (config-profile)# **permit** | **deny**	(可选）配置是要 permit 还是 deny 这一批组播地址范围，缺省值是 deny。这个行为表示：允许/禁止以下 range 内的这些组播地址，并禁止/允许其它的组播地址。

Ruijie(config-profile)# **range** *low-address high_address*	添加组播地址范围，该值即可以是一个单个的 ipv6 组地址也可以是一个组地址的区间（前面的为低 ipv6 组地址，后面为高 ipv6 组地址），同时还可以配置多个 range 范围。

如果要删除其中一个 MLD profile，可以用 **no ipv6 mld profile** *profile_number* 来执行。如果要删除 profile 里的一个 range，可以用 **no range** *low-address high_address* 来执行。

以下例子是配置 MLD Profile，要求 permit ff77::1 到 ff77::100 的组播地址，以及 ff88::123 这个组播地址，其他的组播地址都被 deny：

```
Ruijie(config)# ipv6 mld profile 1
Ruijie(config-profile)# permit
Ruijie(config-profile)# range ff77::1 ff77::100
Ruijie(config-profile)# range ff88::123
Ruijie(config-profile)# end
Ruijie# show ipv6 mld profile 1
MLD Profile 1
permit
range ff77::1 ff77::100
range ff88::123
```

2.2.10 配置MLD Filtering

命令	作用
Ruijie(config-if)# **ipv6 mld snooping filter** *profile-number*	应用 Profile 于该端口。 *profile number* 范围为 1- 1024。
Ruijie(config-if)# **ipv6 mld snooping max-groups** *number*	允许最多几个组动态加入该端口。缺省值 1024。 *number* 范围为 0 – 1024。

在某些情况下，可能需要控制某个端口只能转发一批特定范围内的组播数据流、控制该端口下最多允许动态加入多少组。MLD Filtering 满足了这种需求。可以把某一个 MLD Profile 应用在一个端口下，如果该端口收到 MLD Report 报文，则二层组播设备就会查找这个端口所要加入的组播地址是否在 MLD Profile 允许范围之内。若是，则允许加入，之后才进行后续处理。也可以在一个端口下配置最多允许加入的组的个数，超过范围，二层组播设备也不再接收、处理 MLD Report 报文。

以下例子是配置 MLD Filtering：

```
Ruijie# configure terminal
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# ipv6 mld snooping filter 1
Ruijie(config-if)# ipv6 mld snooping max-groups 1000
Ruijie (config-if)#end
Ruijie #show ipv6 mld snooping interface fastEthernet 0/1
Interface          Filter profile number   max-group
-----------------   ---------------------   ---------
FastEthernet 0/1    1                       1000
```

2.3 监视与维护

2.3.1 查看MLD Snooping当前模式

命令	作用
Ruijie# **show ipv6 mld snooping**	查看 MLD Snooping 工作模式及全局配置。

以下例子是查看 MLD Snooping 配置信息：

```
Ruijie# show ipv6 mld snooping
MLD-snooping mode       :IVGL
SVGL vlan-id            :1
SVGL profile number     :0
Source check port       :Disabled
Query max respone time  :10(Seconds)
```

2.3.2 查看和清除MLD Snooping的统计值

命令	作用
Ruijie# **show ipv6 mld snooping statistics** [**vlan** *vlan-id*]	查看 MLD Snooping 的统计信息。
Ruijie# **clear ipv6 mld snooping statistics**	清除 MLD Snooping 的统计信息

以下例子是查看 MLD Snooping 的路由连接口信息：

```
Ruijie# show ipv6 mld snooping statistics
GROUP    Interface    Last report   Last leave   Last
                      time          time         reporter
-------   ---------   -----------   ----------   ----------
FF88::1   VL1:Gi4/2   0d:0h:0m:7s   ----         2003::1111
                      Report pkts: 1          Leave pkts: 0
```

2.3.3 查看和清除MLD Snooping的转发表

命令	作用
Ruijie# **show ipv6 mld snooping gda-table**	查看 MLD Snooping 的转发表，即 GDA（Group Destination Address）。
Ruijie# **clear ipv6 mld snooping gda-table**	清除 mld snooping 转发表中的动态组信息。

以下例子是查看 GDA 表的各组播组信息以及一个组播组的所有成员端口的信息：

```
Ruijie# show ipv6 mld snooping gda-table
Abbr: M - mrouter
      D - dynamic
      S - static
VLAN   Address   Member ports
```

```
-------------------------------------
1       FF88::1    GigabitEthernet 0/7(S)
```

如果在 Private-vlan 或者 Super-vlan 上启动了 MLD Snooping，那么此时建立的 gda-table 转发表项都是基于 Private-vlan 或者 Super-vlan 的主 VLAN 创建的。该转发表项表明，所有转发出口都可以接收来自主 VLAN 过来的组播流信息；对于从子 VLAN 转发过来的组播流信息，其转发规则还需要遵循 Private-vlan 或者 Super-vlan 的转发规则进行。在这种情况下，每个 gda-table 的转发表项可能会对应多个硬件转发表项，所以会有可能表现出转发表项容量低于指标值的情况。

2.3.4 查看路由连接口信息

命令	作用
Ruijie# **show ipv6 mld snooping mrouter**	查看 MLD Snooping 的路由连接口信息。

以下例子是查看 MLD Snooping 的路由连接口信息：

```
Ruijie# show ipv6 mld snooping mrouter
Vlan    Interface              State     MLD profile number
----    ---------------------  -------   ------------------
1       GigabitEthernet 0/7    static    1
1       GigabitEthernet 0/12   dynamic   0
```

2.3.5 查看MLD Profile

命令	作用
Ruijie# **show ipv6 mld profile** *profile-number*	查看 MLD Profile 信息。

以下为查看 MLD Profile 的信息：

```
Ruijie# show ipv6 mld profile 1
MLD Profile 1
permit
range FF77::1 FF77::100
range FF88::123
```

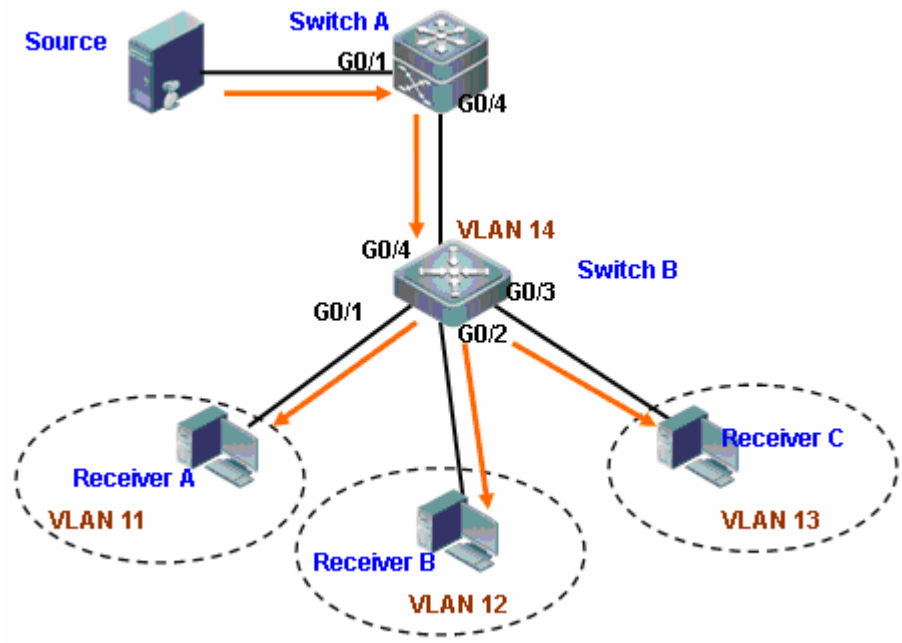
2.4 配置举例

组网需求

一台组播源服务器，一台三层组播设备，一台接入交换机，三台组播点播者。三层组播设备支持 pimsmv6 功能，接入交换机支持 MLD Snooping 功能。

组网拓扑

图 2-2



配置步骤

■ 三层交换机 Switch A 上的配置

启动三层组播

```
Ruijie# configure terminal
Ruijie(config)# ipv6 multicast-routing
Ruijie(config)# int vlan 14
Ruijie(config-if)# ipv6 pim sparse-mode
Ruijie(config-if)# ipv6 add 1111:1111::1111/64
Ruijie(config)# int gigabitEthernet 0/1
Ruijie(config-if)# no switch
Ruijie(config-if)# ipv6 pim sparse -mode
Ruijie(config-if)# ipv6 add 1111:2222::1111/64
```

配置 G0/4 口为 trunk 口，而且它的 native vlan 为 SVGL vlan

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# interface gigabitEthernet 0/4
Ruijie(config-if)# sw trunk native vlan 14
```

■ 二层交换机 Switch B 上的配置

配置 VLAN

```
Ruijie# configure terminal
Ruijie(config)# VLAN 11
```

```
Ruijie(config-vlan)# exit
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport access vlan 11
Ruijie(config-if)# exit
Ruijie(config)# VLAN 12
Ruijie(config-vlan)# exit
Ruijie(config)# interface gigabitEthernet 0/2
Ruijie(config-if)# switchport access vlan 12
Ruijie(config-if)# exit
Ruijie(config)# VLAN 13
Ruijie(config-vlan)# exit
Ruijie(config)# interface gigabitEthernet 0/3
Ruijie(config-if)# switchport access vlan 13
Ruijie(config-if)# exit
Ruijie(config)# VLAN 14
Ruijie(config-vlan)# exit
Ruijie(config)# interface gigabitEthernet 0/4
Ruijie(config-if)# switchport access vlan 14
```

配置 MLD profile

```
Ruijie# configure terminal
Ruijie(config)# ipv6 mld profile 1
Ruijie(config-profile)# permit
Ruijie(config-profile)# range ff13::  ff13:1111::
Ruijie(config-profile)# end
Ruijie# show ipv6 mld profile 1
Profile     1
        Permit
        range ff13::,   ff13:1111::
```

配置路由连接口

```
Ruijie(config)# ipv6 mld snooping vlan 14 mrouter interface gigabitEthernet 0/4
```

配置 SVGL 工作模式

```
Ruijie# configure terminal
Ruijie(config)# ipv6 mld snooping svgl
Ruijie(config)# ipv6 mld snooping svgl vlan 14
Ruijie(config)# ipv6 mld snooping svgl profile 1
```

查看 MLD Snooping 配置

```
Ruijie# show ipv6 mld snooping
mld-snooping mode        :SVGL
SVGL vlan-id             :14
SVGL profile number      :1
Source check port        :Disable
```

```
Query Max Respone Time   :10 (Seconds)
Ruijie#show run
…
ipv6 mld profile 1
permit
range ff13:: ff13:1111::
ipv6 mld snooping svgl vlan 14
ipv6 mld snooping svgl profile 1
ipv6 mld snooping svgl
ipv6 mld snooping vlan 14 mrouter interface GigabitEthernet 0/4
!
```

配置指南-安全

本分册介绍安全配置指南相关内容，包括以下章节：

1. AAA
2. RADIUS
3. TACACS+
4. 802.1x
5. Web 认证
6. SSH 终端服务
7. URPF
8. GSN
9. 基于端口的流控制
10. CPU 保护
11. DoS 保护
12. DHCP Snooping
13. 动态 ARP 检测
14. IP Source Guard
15. ND Snooping
16. DHCPv6 Snooping
17. 防网关 ARP 欺骗
18. NFPP
19. 锐捷交换机安全功能兼容模式

1 AAA

访问控制是用来控制哪些人可以访问网络服务器以及用户在网络上可以访问哪些服务的。身份认证、授权和记账（AAA）是进行访问控制的一种主要的安全机制。

1.1 AAA基本原理

AAA 是 Authentication Authorization and Accounting（认证、授权和记账）的简称，它提供了对认证、授权和记账功能进行配置的一致性框架，锐捷网络设备产品支持使用 AAA。

AAA 以模块方式提供以下服务：

认证：验证用户是否可获得访问权，可选择使用 RADIUS 协议、TACACS+协议或 Local（本地）等。身份认证是在允许用户访问网络和网络服务之前对其身份进行识别的一种方法。

授权：授权用户可使用哪些服务。AAA 授权通过定义一系列的属性对来实现，这些属性对描述了用户被授权执行的操作。这些属性对可以存放在网络设备上，也可以远程存放在安全服务器上。

记账：记录用户使用网络资源的情况。当 AAA 记账被启用时，网络设备便开始以统计记录的方式向安全服务器发送用户使用网络资源的情况。每个记账记录都是以属性对的方式组成，并存放在安全服务器上，这些记录可以通过专门软件进行读取分析，从而实现对用户使用网络资源的情况进行记账、统计、跟踪。

尽管 AAA 是最主要的访问控制方法，锐捷产品同时也提供了在 AAA 范围之外的简单控制访问，如本地用户名身份认证、线路密码身份认证等。不同之处在于它们提供对网络保护程度不一样，AAA 提供更高级别的安全保护。

使用 AAA 有以下优点：

- 灵活性和可控制性强
- 可扩充性
- 标准化认证
- 多个备用系统

1.1.1 AAA基本原理

AAA 可以对单个用户（线路）或单个服务器动态配置身份认证、授权以及记账类型。通过创建方法列表来定义身份认证、记账、授权类型，然后将这些方法列表应用于特定的服务或接口。

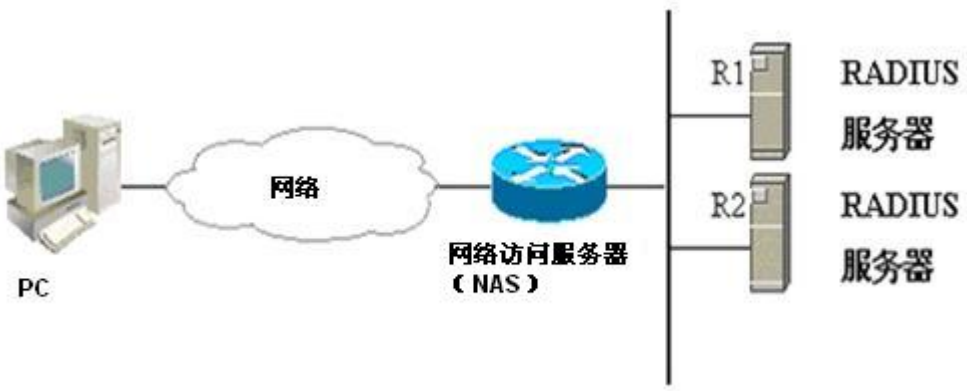
1.1.2 方法列表

由于对用户进行认证、授权和记账可以使用不同的安全方法，您需要使用方法列表定义一个使用不同方法对用户进行认证、授权和记账的前后顺序。方法列表可以定义一个或多个安全协议，这样可以确保在第一个方法失败时，有备用系统可用。锐捷产品使用方法列表中列出的第一个方法时，如果该方法无应答，则选择方法列表中的下一个方法。这个过程一直持续下去，

直到与列出的某种安全方法成功地实现通信或用完方法列表。如果用完方法列表而还没有成功实现通信，则该安全功能宣告失败。

只有在前一种方法没有应答的情况下，锐捷产品才会尝试下一种方法。例如在身份认证过程中，某种方法拒绝了用户访问，则身份认证过程结束，不再尝试其他的身份认证方法。

图 1-1



上图说明了一个典型的 AAA 网络配置，包含两台安全服务器：R1 和 R2 是 RADIUS 服务器。以及一台网络访问服务器（NAS），可以作为 RADIUS 客户端。

假设系统管理员已定义了一个方法列表，在这个列表中，R1 首先被用来获取身份信息，然后是 R2，最后是访问服务器上的本地用户名数据库。如果一个远程 PC 用户试图拨号进入网络，网络访问服务器首先向 R1 查询身份认证信息，假如用户通过了 R1 的身份认证，R1 将向网络访问服务器发出一个 ACCEPT 应答，这样用户即获准访问网络。如果 R1 返回的是 REJECT 应答，则拒绝用户访问网络，断开连接。如果 R1 无应答，网络访问服务器就将它看作 TIMEOUT，并向 R2 查询身份认证信息。这个过程会一直在余下的指定方法中持续下去，直到用户通过身份认证、被拒绝或对话被中止。如果所有的方法返回 TIMEOUT，则认证失败，连接将被断开。

REJECT 应答不同于 TIMEOUT 应答。REJECT 意味着用户不符合可用身份认证数据库中包含的标准，从而未能通过身份认证，访问请求被拒绝。TIMEOUT 则意味着安全服务器对身份认证查询未作应答，当检测到一个 TIMEOUT 时，AAA 选择身份认证方法列表中定义的下一个身份认证方法将继续进行身份认证过程。

在本文中，与 AAA 安全服务器相关的认证、授权和记账配置，均以 RADIUS 为例，而与 TACACS+有关的内容请另外参考“配置 TACACS+”。

1.2 配置AAA基本步骤

首先您必须决定要采用哪种安全解决方案，而且需要评估特定网络中的潜在安全风险，并选择适当的手段来阻止未经授权的访问。我们建议，在可能的情况下，尽量使用 AAA 确保网络安全。

1.2.1 AAA配置过程概述

如果理解了 AAA 运作的基本过程，配置 AAA 就相对简单了。在锐捷网络设备上配置 AAA 地步骤如下：

- 启用 AAA，使用全局配置模式命令 **aaa new-model**。

- 如果决定使用安全服务器，请配置安全协议的参数，如 RADIUS。
- 定义身份认证方法列表，使用 **aaa authentication** 命令。
- 如有需要，可将该方法列表应用于特定的接口或线路。

在应用特定方法列表时，如果没有明确指定使用命名的方法列表，则使用默认的身份认证方法列表进行身份认证。因此，如果不准备使用默认的身份认证方法列表，则需要指定特定的方法列表。

对于本章中使用的命令的完整描述，请参见命令手册“AAA 命令”。

1.2.2 启用AAA

要使用 AAA 安全特性，必须首先启用 AAA。

要启用 AAA，在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)**#aaa new-model**	启用 AAA。

1.2.3 停用AAA

要停用 AAA，在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)**#no aaa new-model**	停用 AAA。

1.2.4 后续的配置过程

启用 AAA 以后，便可以配置与安全方案相关的其他部分，下表说明了可能要完成的配置任务以及相关内容所在的章节。

AAA 访问控制安全解决方案方法。

配置任务	步骤	所在章节
配置 RADIUS 安全协议参数	2	配置 RADIUS
配置本地登录(Login)身份认证	3	配置认证
定义认证方法列表	4	配置认证
将方法列表应用于特定的接口或线路	5	配置认证
启用 RADIUS 授权	6	配置授权
启用 RADIUS 记账	7	配置记账

如果使用 AAA 实现身份认证，请参考“配置认证”中的相关部分。

1.3 配置认证

身份认证是在允许用户使用网络资源以前对其进行识别，在大多数情况下，身份认证是通过 AAA 安全特性来实现的。我们建议，在可能的情况下，最好使用 AAA 来实现身份认证。

1.3.1 定义AAA认证方法列表

要配置 AAA 身份认证，首先得定义一个身份认证方法的命名列表，然后各个应用使用已定义列表进行认证。方法列表定义了身份认证的类型和执行顺序。对于已定义的身份认证方法，必须有特定的应用才会被执行。默认方法列表是唯一的例外。所有应用在未进行配置时使用默认方法列表。

方法列表仅是定义将要被依次查询的、并用于认证用户身份的一系列安全方法。方法列表使您能够指定一个或多个用于身份认证的安全协议，这样确保在第一种方法失败的情况下，可以使用身份认证备份系统。我司产品使用第一种方法认证用户的身份，如果该方法无应答，将选择方法列表中的下一种方法。 这个过程一直持续下去，直到与列出的某种身份认证方法成功地实现通信或用完方法列表。如果用完方法列表而还没有成功实现通信，则身份认证宣告失败。

只有在前一种方法没有应答的情况下，锐捷产品才会尝试下一种方法。如果在身份认证过程中，某种方法拒绝了用户访问，则身份认证过程结束，不再尝试其他的身份认证方法。

1.3.2 方法列表举例

在典型 AAA 网络配置图中，它包含 2 个服务器：R1 和 R2 是 RADIUS 服务器。假设系统管理员已选定一个安全解决方案，NAS 认证采用一个身份认证方法对 Telnet 连接进行身份认证：首先使用 R1 对用户进行认证，如果无应答，则使用 R2 进行认证；如果 R1、R2 都没有应答，则身份认证由访问服务器的本地数据库完成，要配置以上身份认证列表，执行以下命令：

命令	作用
Ruijie(config)**#aaa authentication login default group radius local**	配置一个默认身份认证方法列表，其中“default”是方法列表的名称。这个方法列表中包含的协议，按照它们将被查询的顺序排列在名称之后。为所有应用的默认方法列表。

如果系统管理员希望该方法列表仅应用于一个特定的 Login 连接，必须创建一个命名方法列表，然后将它应用于特定的连接。下面的例子说明了如何将身份认证方法列表仅应用于线路 2：

命令	作用
Ruijie(config)**#aaa new-model**	打开 AAA 开关。
Ruijie(config)**#aaa authentication login** *test* **group radius local**	在全局配置模式下，定义了一个名为“test”的方法列表。
Ruijie(config-line)**#line vty** *2*	进入 VTY 线路 2 配置模式。
Ruijie(config-line)**#login authentication** *test*	在 line 配置模式下，将名为“test”方法列表应用于线路。

当远程 PC 用户试图 Telnet 访问网络设备(NAS)，NAS 首先向 R1 查询身份认证信息，假如用户通过了 R1 的身份认证，R1 将向 NAS 发出一个 ACCEPT 应答，这样用户即获准访问网络。如果 R1 返回的是 REJECT 应答，则拒绝用户访问网络，断开连接。如果 R1 无应答，NAS 就将它看作 TIMEOUT，并向 R2 查询身份认证信息。这个过程会一直在余下的指定方法中持续下去，直到用户通过身份认证、被拒绝或对话被中止。如果所有的服务器(R1、R2)返回 TIMEOUT，则认证由 NAS 本地数据库完成。

REJECT 应答不同于 TIMEOUT 应答。REJECT 意味着用户不符合可用的身份认证数据库中包含的标准，从而未能通过身份认证，访问请求被拒绝。TIMEOUT 则意味着安全服务器对身份认证查询未作应答，当验证 TIMEOUT 时，AAA 选择认证方法列表中定义的下一个认证方法继续进行认证过程。

1.3.3 认证类型

我司产品目前支持以下认证类型：

- Login（登录）认证
- Enable 认证
- PPP 认证
- DOT1X（IEEE802.1x）认证

其中 Login 认证针对的是用户终端登录到 NAS 上的命令行界面（CLI），在登录时进行身份认证；Enable 认证针对的是用户终端登录到 NAS 上的 CLI 界面以后，提升 CLI 执行权限时进行认证；PPP 认证针对 PPP 拨号用户进行身份认证；DOT1X 认证针对 IEEE802.1x 接入用户进行身份认证。

1.3.4 配置AAA身份认证的通用步骤

要配置 AAA 身份认证，都必须执行以下任务：

- 使用 **aaa new-model** 全局配置命令启用 AAA。
- 如果要使用安全服务器，必须配置安全协议参数，如 RADIUS 和 TACACS+。具体的配置请参见“配置 RADIUS”和“配置 TACACS+”。
- 使用 **aaa authentication** 命令定义身份认证方法列表。
- 如果可能，将方法列表应用于某个特定的接口或线路。

我司产品 DOT1X 认证目前不支持 TACACS+。

1.3.5 配置AAA Login认证

本节将具体介绍如何配置锐捷产品所支持的 AAA Login（登录）身份认证方法：

只有在全局配置模式下执行 **aaa new-model** 命令启用 AAA，AAA 安全特性才能进行配置使用（下同）。关于更详细的内容，请参见“AAA 概述”。

在很多情况下，用户需要通过 Telnet 访问网络访问服务器(NAS)，一旦建立了这种连接，就可以远程配置 NAS，为了防止网络未经授权的访问，要对用户进行身份认证。

AAA 安全服务使网络设备对各种基于线路的 Login（登录）身份认证变得容易。不论您要决定使用哪种 Login 认证方法，只要使用 **aaa authentication login** 命令定义一个或多个身份认证方法列表，并应用于您需要进行 Login 认证的特定线路就可以了。

要配置 AAA Login 认证，在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)**#aaa new-model**	启用 AAA。

Ruijie(config)**#aaa authentication login** {**default** | *list-name*} *method1* [*method2*...]	定义一个认证方法列表，如果需要定义多个方法列表，重复执行该命令。
Ruijie(config)**# line vty** *line-num*	进入您需要应用 AAA 身份认证的线路。
Ruijie(config-line)**#login authentication** {**default** | *list-name*}	将方法列表应用线路。

关键字 *list-name* 用来命名创建身份认证方法列表，可以是任何字符串；关键字 *method* 指的是认证实际算法。仅当前面的方法返回 ERROR（无应答），才使用后面的其他认证方法；如果前面的方法返回 FAIL(失败)，则不使用其他认证方法。为了使认证最后能成功返回，即使所有指定方法都没有应答，可以在命令行中将 **none** 指定为最后一个认证方法。

例如，在下例中，即使 RADIUS 服务器超时(TIMEOUT)，仍然能够通过身份认证：**aaa authentication login default group radius none**。

> 由于关键字 **none** 使得拨号的任何用户在安全服务器没有应答情况下都能通过身份认证，所以仅将它作为备用的身份认证方法。我们建议：一般情况下，不要使用 **none** 身份认证，在特殊情况下，如所有可能的拨号用户都是可信任的，而且用户的工作不允许有由于系统故障造成的耽搁，可以在安全服务器无应答的情况下，将 **none** 作为最后一种可选的身份认证方法，建议在 **none** 认证方法前加上本地身份认证方法。

关键字	描述
local	使用本地用户名数据库进行身份认证。
none	不进行身份认证。
group radius	使用 RADIUS 服务器组进行身份认证。
group tacacs+	使用 TACACS+服务器组进行身份认证。

上表列出了锐捷产品支持的 AAA Login 认证方法。

使用本地数据库进行 Login 认证

要配置使用本地数据库进行 Login 认证时，首先需要配置本地数据库，锐捷产品支持基于本地数据库的身份认证，建立用户名身份认证，请在全局配置模式下，根据具体需求执行以下命令：

命令	作用
Ruijie(config)**#username name [password** *password*]	建立本地用户，设置口令。

定义本地 Login 认证方法列表并应用认证方法列表，可使用以下命令：

命令	作用
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#aaa new-model**	打开 AAA 开关。
Ruijie(config)**#aaa authentication login** {**default** | *list-name*} **local**	定义使用本地认证方法。
Ruijie(config)**#end**	退出到特权模式。
Ruijie**#show aaa method-list**	确认配置的方法列表。
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#line** vty *line-num*	进入线路配置模式。
Ruijie(config-line)**#login authentication** {**default** | *list-name*}	应用方法列表。
Ruijie(config-line)**#end**	退出到特权模式。
Ruijie**#show running-config**	确认配置。

使用 RADIUS 进行 Login 认证

要配置用 RADIUS 服务器进行 Login 认证，首先要配置 RADIUS 服务器。配置 RADIUS 服务器，请在全局配置模式下，根据具体需求执行以下命令：

命令	作用
Ruijie(config)**#aaa new-model**	打开 AAA 开关。
Ruijie(config)**#radius-server host** *ip-address* [**auth-port** *port*] [**acct-port** *port*]	配置 RADIUS 服务器。
Ruijie**#show radius server**	显示 RADIUS 服务器。

配置好 RADIUS 服务器后，在配置 RADIUS 进行身份认证以前，请确保与 RADIUS 安全服务器之间已经成功进行了通信，有关 RADIUS 服务器配置的信息，请参见“配置 RADIUS”。

现在就可以配置基于 RADIUS 服务器的方法列表了，在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)**#aaa new-model**	打开 AAA 开关。
Ruijie(config)**#aaa authentication login** {**default** | *list-name*} **group radius**	定义使用 RADIUS 认证方法。
Ruijie(config)**#end**	退出到特权模式。
Ruijie**#show aaa method-list**	确认配置的方法列表。
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#line vty** *line-num*	进入线路配置模式。
Ruijie(config-line)**#login authentication** {**default** | *list-name*}	应用方法列表。
Ruijie(config-line)**#end**	退出到特权模式。
Ruijie**#show running-config**	确认配置。

1.3.6 配置AAA Enable认证

本节将具体介绍如何配置锐捷产品所支持的 AAA Enable 认证方法：

在很多情况下，用户需要通过 Telnet 等方法访问网络访问服务器(NAS)，在进行了身份认证以后，就可以进入命令行界面（CLI），此时会被赋予一个初始的执行 CLI 命令的权限（0~15 级）。不同的级别，可以执行的命令是不同的，可以使用 **show privilege** 命令查看当前的级别。关于更详细的内容，请参见“使用命令行界面”。

如果登录到命令行界面后，由于初始权限过低，不能执行某些命令，则可以使用 enable 命令来提升权限。为了防止网络未经授权的访问，在提升权限的时候，需要进行身份认证，即 Enable 认证。

要配置 AAA Enable 认证，在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)**#aaa new-model**	启用 AAA。
Ruijie(config)**#aaa authentication enable default** *method1* [*method2*...]	定义一个 Enable 认证方法列表，可以指定采用的认证方法，例如 RADIUS。

Enable 认证方法列表全局只能定义一个，因此不需要定义方法列表的名称；关键字 *method* 指的是认证实际方法。仅当前面的方法返回 ERROR（无应答），才使用后面的其他身份方法；如果前面的方法返回 FAIL(失败)，则不使用其他认证方法。为了使认证最后能成功返回，即使所有指定方法都没有应答，可以在命令行中将 **none** 指定为最后一个认证方法。

Enable 认证方法配置以后立即自动生效。此后，在特权模式下执行 **enable** 命令的时候，如果要切换的级别比当前级别要高，则会提示进行认证。如果要切换的级别小于或等于当前级别，则直接切换，不需要进行认证。

> 如果进入 CLI 界面的时候经过了 Login 身份认证（**none** 方法除外），将记录当前使用的用户名。此时，进行 Enable 认证的时候，将不再提示输入用户名，直接使用与 Login 认证相同的用户名进行认证，注意输入的口令要与之匹配。
>
> 如果进入 CLI 界面的时候没有进行 Login 认证，或在 Login 认证的时候使用了 **none** 方法，将不会记录用户名信息。此时，如果进行 Enable 认证，将会要求重新输入用户名。这个用户名信息不会被记录，每次进行 Enable 认证都要重新输入。

一些认证方法，在认证时可以绑定安全级别。这样，在认证过程中，除了根据安全协议返回的成功或失败的应答外，还需要检查绑定的安全级别。如果服务协议能绑定安全级别，则需要在认证时校验绑定的级别。如果绑定的级别大于或等于要切换的目的级别，则 Enable 认证成功，并切换到目的级别；而如果绑定的级别小于要切换的目的级别，则 Enable 认证失败，提示失败信息，维持当前的级别不变。如果服务协议不能绑定安全级别，则不校验绑定的级别，就可以切换到目的级别。

目前能够绑定安全级别的认证方法只有 RADIUS 和本地认证，因此只对这两种方法进行检查，如果采用其他认证方法则不进行检查。

使用本地数据库进行 Enable 认证

使用本地数据库进行 Enable 认证时，可以在设置本地用户时，为用户设置权限级别。如果没有设置，则默认的用户级别为 1 级。要配置使用本地数据库进行 Enable 身份认证时，首先需要配置本地数据库，并为用户设置权限级别，请在全局配置模式下，根据具体需求执行以下命令：

命令	作用
Ruijie(config)**#username** *name* [**password** *password*]	建立本地用户，设置口令。
Ruijie(config)**#username** *name* [**privilege** *level*]	为用户设置权限级别（可选）。

定义本地 Enable 认证方法列表，可使用以下命令：

命令	作用
Ruijie(config)**#aaa new-model**	打开 AAA 开关。
Ruijie(config)**#aaa authentication enable default local**	定义使用本地认证方法。
Ruijie**#show aaa method-list**	确认配置的方法列表。

使用 RADIUS 进行 Enable 认证

标准的 RADIUS 服务器可以通过 Service-Type 属性（标准属性号为 6）绑定权限，可以指定 1 级或 15 级权限；锐捷扩展的 RADIUS 服务器（例如 SAM）可以设置设备管理员的级别（私有属性号为 42），可以指定 0~15 级权限。有关 RADIUS 服务器配置的信息，请参见“配置 RADIUS”中的“指定 RADIUS 私有属性类型”章节。

要配置用 RADIUS 认证服务器进行 Enable 认证，首先要配置 RADIUS 服务器，然后再配置基于 RADIUS 服务器的 Enable 方法列表。在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)**#aaa new-model**	打开 AAA 开关。
Ruijie(config)**#aaa authentication enable default group radius**	定义使用 RADIUS 认证方法。
Ruijie**#show aaa method-list**	确认配置的方法列表。

1.3.7 配置PPP用户使用AAA认证

PPP 协议是提供在点到点链路上承载网络层数据包的一种链路层协议。在很多情况下，用户需要通过异步或 ISDN 拨号访问 NAS（网络访问服务器），一旦建立了这种连接，将启动 PPP 协商，为了防止网络未经授权的访问，PPP 在协商过程中要对拨号用户进行身份认证。

本节将具体介绍如何配置我司产品所支持的 AAA PPP 认证方法，要配置 AAA PPP 认证，在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)#**aaa new-model**	启用 AAA。
Ruijie(config)#**aaa authentication ppp** {**default** | *list-name*} *method1* [*method2*...]	定义一个 PPP 认证方法列表，可以指定采用的认证方法，目前支持 RADIUS 和 TACACS+远程认证，以及使用本地数据库进行认证。
Ruijie(config)#**interface** *interface-type interface-number*	进入需要应用 AAA 身份认证的异步或 ISDN 接口。
Ruijie(config-if-*type ID*)#**ppp authentication** {**chap** | **pap**} {**default** | *list-name*}	将身份认证方法列表应用于异步或 ISDN 接口。

PPP 协议更具体的配置方式参见“PPP、MP 协议配置”中相关章节。

1.3.8 配置 802.1x用户使用AAA认证

IEEE802.1x（Port-Based Network Access Control）是一个基于端口的网络存取控制标准，为 LAN 提供点对点式的安全接入，提供一种对连接到局域网设备的用户进行认证的手段。

本节将具体介绍如何配置我司产品所支持的 802.1x 认证方法，要配置 802.1x 认证，在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)#**aaa new-model**	启用 AAA。
Ruijie(config)#**aaa authentication dot1x** {**default** | *list-name*} *method1* [*method2*...]	定义一个 IEEE802.1x 认证方法列表，可以指定采用的认证方法，目前支持 RADIUS 远程认证，以及使用本地数据库进行认证。
Ruijie(config)#**dot1x authentication** *list-name*	802.1x 应用认证方法列表。

IEEE802.1x 协议更具体的配置方式参见“配置 802.1x”。

1.3.9 配置认证示例

下面示例演示如何配置网络设备，使用“RADIUS+本地身份”进行认证。

```
Ruijie(config)# aaa new-model
Ruijie(config)# username Ruijie password starnet
Ruijie(config)# radius-server host 192.168.217.64
Ruijie(config)# radius-server key test
Ruijie(config)# aaa authentication login test group radius local
Ruijie(config)# line vty 0
Ruijie(config-line)# login authentication test
```

```
Ruijie(config-line)# end
Ruijie# show running-config
!
aaa new-model
!
!
aaa authentication login test group radius local
username Ruijie password 0 starnet
!
radius-server host 192.168.217.64
radius-server key 7 093b100133
!
line con 0
line vty 0
login authentication test
line vty 1 4
!
!
```

上面例子中，访问服务器使用 RADIUS 服务器（IP 为 192.168.217.64）对登录的用户进行认证，如果 RADIUS 服务器没有应答，则使用本地数据库进行身份认证。

1.3.10 终端服务应用下认证示例

在终端服务的应用环境下，终端接到设备的异步串口上，再通过 IP 网络连接到网络中心服务器进行业务作业。但是，如果打开了 AAA 功能，则所有的线路都需要进行登录（Login）认证，那么终端需要先通过了设备的登录认证，才能连接到服务器，这样对终端服务的业务产生了影响。我们可以通过配置将两种线路分开，既让使用终端服务的线路不进行登录认证，直接连接服务器；同时连接到本设备的线路又可以使用登录认证来保证设备的安全。即：设置一个终端服务专用的登录认证列表，但认证方法为 none；然后将这个登录认证列表应用在打开终端服务的线路上（其他可以连接到本地的线路不变）；这样该终端就不需要进行本地的登录认证了。配置步骤如下：

```
Ruijie(config)# aaa new-model
Ruijie(config)# username Ruijie password starnet
Ruijie(config)# radius-server host 192.168.217.64
Ruijie(config)# radius-server key test
Ruijie(config)# aaa authentication login test group radius local
Ruijie(config)# aaa authentication login terms none
Ruijie(config)# line tty 1 4
Ruijie(config-line)# login authentication terms
Ruijie(config-line)# exit
Ruijie(config)# line tty 5 16
Ruijie(config-line)# login authentication test
Ruijie(config-line)# exit
Ruijie(config)# line vty 0 4
Ruijie(config-line)# login authentication test
```

```
Ruijie(config-line)# end
Ruijie# show running-config
!
aaa new-model
!
!
aaa authentication login test group radius local
aaa authentication login terms none
username Ruijie password 0 starnet
!
radius-server host 192.168.217.64
radius-server key 7 093b100133
!
line con 0
line aux 0
line tty 1 4
login authentication terms
line tty 5 16
login authentication test
line vty 0 4
login authentication test
!
!
```

上面例子中，访问服务器使用 RADIUS 服务器（IP 为 192.168.217.64）对登录的用户进行认证，如果 RADIUS 服务器没有应答，则使用本地数据库进行身份认证。我们使用 tty 1-4 作为终端服务使用的线路，不需要登录认证，而其他 tty 和 vty 线路需要进行登录认证。

1.4 配置授权

AAA 授权使管理员能够对用户可使用的服务或权限进行控制。启用 AAA 授权服务以后，网络设备通过本地或服务器中的用户配置文件信息对用户的会话进行配置。完成授权以后，该用户只能使用配置文件中允许的服务或只具备许可的权限。

1.4.1 授权类型

锐捷产品目前支持以下 AAA 授权类型：

- Exec 授权
- Command（命令）授权
- Network（网络）授权

其中 Exec 授权针对的是用户终端登录到 NAS 上的 CLI 界面时，授予用户终端的权限级别（分为 0~15 级）；命令授权针对的是用户终端登录到 NAS 上的 CLI 界面以后，针对具体命令的执行授权；而网络授权针对的是授予网络连接上的用户会话可使用的服务。

命令授权功能目前仅 TACACS+协议支持，具体内容请参考“配置 TACACS+”。

1.4.2 授权的准备工作

在配置 AAA 授权以前，必须完成下述任务：

- 启用 AAA 服务。关于如何启用 AAA 服务，请参见“AAA 概述”。
- （可选）配置 AAA 认证。授权一般是在用户通过认证之后进行，但在某些情况下，没有经过认证也可以单独授权。关于 AAA 认证的信息，请参见“配置认证”。
- （可选）配置安全协议参数。如果需要使用安全协议进行授权，需要配置安全协议参数。锐捷产品 Network 授权支持 RADIUS 和 TACACS+协议，Exec 授权支持 RADIUS 和 TACACS+协议，关于 RADIUS 协议的信息，请参见“配置 RADIUS”，关于 TACACS+协议的信息，请参见“配置 TACACS+”。
- （可选）如果需要使用本地授权，则需要使用 **username** 命令定义用户权限。

1.4.3 配置授权列表

要启用 AAA 授权，请在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)**#aaa new-model**	打开 AAA 开关。
Ruijie(config)**#aaa authorization exec** {**default** | *list-name*} *method1* [*method2*|…]	定义 AAA Exec 授权方法。
Ruijie(config)**#aaa authorization network**{default | *list-name*} *method1* [*method2*|…]	定义 AAA Network 授权方法。

1.4.4 配置AAA Exec授权

锐捷产品支持针对登录到网络访问服务器（NAS）的用户终端，授予其执行命令的权限，即 Exec 授权。体现为用户登录到 NAS 的 CLI 界面时（例如通过 Telnet），具备的级别（成功登录后，可以使用 **show privilege** 命令查看）。

不论您要决定使用哪种 Exec 授权方法，只要使用 **aaa authorization exec** 命令定义一个或多个 Exec 授权方法列表，并应用于您需要进行 Exec 授权的特定线路就可以了。

要配置 AAA Exec 授权，在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)**#aaa new-model**	启用 AAA。
Ruijie(config)**#aaa authorization exec** {**default** | *list-name*} *method1* [*method2*...]	定义一个授权方法列表，如果需要定义多个方法列表，重复执行该命令。
Ruijie(config)**#line vty** *line-num*	进入您需要应用 AAA Exec 授权的线路。
Ruijie(config-line)**#authorization exec** {**default** | *list-name*}	将方法列表应用线路。

关键字 *list-name* 用来命名创建授权方法列表，可以是任何字符串；关键字 *method* 指的是授权实际算法。仅当前面的方法返回 ERROR（无应答），才使用后面的其他方法；如果前面的方法返回 FAIL(失败)，则不使用其他授权方法。为了使授权最后能成功返回，即使所有指定方法都没有应答，可以在命令行中将 **none** 指定为最后一个授权方法。

例如，在下例中，即使 RADIUS 服务器超时(TIMEOUT)，仍然能够通过 Exec 授权：aaa authorization exec default group radius none

命令	作用
local	使用本地用户名数据库进行 Exec 授权。
none	不进行 Exec 授权。
group radius	使用 RADIUS 服务器组进行 Exec 授权。
group tacacs+	使用 TACACS+服务器组进行 Exec 授权。

上表列出了锐捷产品支持的 AAA Exec 授权方法。

Exec 授权通常结合 Login 认证一起使用，并可以在同一个线路上同时使用 Login 认证和 Exec 授权。但是要注意，由于授权和认证可以采用不同的方法和不同的服务器，因此对于相同的用户，认证和授权可能有不同的结果。用户登录时，如果 Exec 授权失败，即使已经通过了 Login 认证，也不能进入到 CLI 界面。

使用本地数据库进行 Exec 授权

要配置使用本地数据库进行 Exec 授权时，首先需要配置本地数据库。可以在设置本地用户时，为用户设置权限级别。如果没有设置，则默认的用户级别为 1 级。请在全局配置模式下，根据具体需求执行以下命令：

命令	作用
Ruijie(config)**#username** *name* [**password** *password*]	建立本地用户，设置口令。
Ruijie(config)**#username** *name* [**privilege** *level*]	为用户设置权限级别（可选）。

定义本地 Exec 授权方法列表并应用授权方法列表，可使用以下命令：

命令	作用
Ruijie(config)**#aaa new-model**	打开 AAA 开关。
Ruijie(config)**#aaa authorization exec** {**default** | *list-name*} **local**	定义使用本地认证方法。
Ruijie**#Show aaa method-list**	确认配置的方法列表。
Ruijie(config)**#line vty** *line-num*	进入线路配置模式。
Ruijie(config-line)**#authorization exec** {**default** | *list-name*}	应用方法列表。

使用 RADIUS 进行 Exec 授权

要配置用 RADIUS 服务器进行 Exec 授权，首先要配置 RADIUS 服务器，有关 RADIUS 服务器配置的信息，请参见“RADIUS 配置指导”。

配置好 RADIUS 服务器后，就可以配置基于 RADIUS 服务器的方法列表了，在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)**#aaa new-model**	打开 AAA 开关。
Ruijie(config)**#aaa authorization exec** {**default** | *list-name*} **group radius**	定义使用 RADIUS 认证方法。
Ruijie**#show aaa method-list**	确认配置的方法列表。

Ruijie(config)**#line vty** *line-num*	进入线路配置模式。
Ruijie(config-line)**#authorization exec** {**default** | *list-name*}	应用方法列表。

配置 Exec 授权示例

下例演示如何进行 Exec 授权。我们设置 VTY 线路 0~4 上的用户登录时采用 Login 认证，并且进行 Exec 授权。其中 Login 认证采用本地认证，Exec 授权先采用 RADIUS、如果没有响应可以采用本地授权。远程 RADIUS 服务器地址为 192.168.217.64，共享密钥为 test；本地用户名为 ruijie，口令为 ruijie，绑定级别是 6 级。如下：

```
Ruijie# configure terminal
Ruijie(config)# aaa new-model
Ruijie(config)# radius-server host 192.168.217.64
Ruijie(config)# radius-server key test
Ruijie(config)# username ruijie password ruijie
Ruijie(config)# username ruijie privilege 6
Ruijie(config)# aaa authentication login mlist1 local
Ruijie(config)# aaa authorization exec mlist2 group radius local
Ruijie(config)# line vty 0 4
Ruijie(config-line)# login authentication mlist1
Ruijie(config-line)# authorization exec mlist2
Ruijie(config)# end
Ruijie# show running-config
aaa new-model
!
aaa authorization exec mlist2 group radius local
aaa authentication login mlist1 local
!
username ruijie password ruijie
username ruijie privilege 6
!
radius-server host 192.168.217.64
radius-server key 7 093b100133
!
line con 0
line vty 0 4
 authorization exec mlist2
 login authentication mlist1
!
End
```

1.4.5 配置AAA Network授权

我司产品支持对包括 PPP、SLIP 等网络连接进行 Network（网络）授权，这些网络连接通过 Network 授权，可以获得诸如流量、带宽、超时等服务配置。Network 授权支持通过 RADIUS 和 TACACS+协议进行，服务器下发的授权信息封装在 RADIUS 或 TACACS+属性里，针对不同的网络连接应用，服务器下发的授权信息可能不相同。

目前该配置不支持 802.1X 的 AAA 授权，802.1X 通过另外的命令完成，具体参见“802.1X 配置”。

要配置 AAA Network 授权，在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)**#aaa new-model**	启用 AAA。
Ruijie(config)**#aaa authorization network** {**default** | *list-name*} *method1* [*method2*...]	定义一个授权方法列表，如果需要定义多个方法列表，重复执行该命令。

关键字 *list-name* 用来命名创建授权方法列表，可以是任何字符串；关键字 *method* 指的是授权实际算法。仅当前面的方法返回 ERROR（无应答），才使用后面的其他授权方法；如果前面的方法返回 FAIL(失败)，则不使用其他授权方法。为了使授权最后能成功返回，即使所有指定方法都没有应答，可以在命令行中将 **none** 指定为最后一个授权方法。

使用 RADIUS 进行 Network 授权

要配置用 RADIUS 服务器进行 Network 授权，首先要配置 RADIUS 服务器，有关 RADIUS 服务器配置的信息，请参见“配置 RADIUS”。

配置好 RADIUS 服务器后，就可以配置基于 RADIUS 服务器的方法列表了，在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)**#aaa new-model**	打开 AAA 开关。
Ruijie(config)**#aaa authorization network** {**default** | *list-name*} **group radius**	定义使用 RADIUS 授权方法。

配置 Network 授权示例

下例演示如何进行网络授权。

```
Ruijie# configure terminal
Ruijie(config)# aaa new-model
Ruijie(config)# radius-server host 192.168.217.64
Ruijie(config)# radius-server key test
Ruijie(config)# aaa authorization network test group radius none
Ruijie(config)# end
Ruijie# show running-config
aaa new-model
!
aaa authorization network test group radius none
!
radius-server host 192.168.217.64
```

```
radius-server key 7 093b100133
!
```

1.5 配置记账

AAA 记账功能够跟踪用户使用的服务和网络资源。启用记账功能以后，网络访问服务器或设备实时地以属性对的方式将用户访问网络的情况发送给安全服务器。您可以使用一些分析软件对这些数据进行分析，实现对用户的活动进行计费、审计以及跟踪等功能。

1.5.1 记账类型

锐捷产品目前支持以下记账类型：

- Exec 记账
- Command（命令）记账
- Network（网络）记账

其中 Exec 记账针对的是用户终端登录到 NAS 上的命令行界面（CLI），在登入和登出时分别进行记账；命令记账针对的是用户终端登录到 NAS 上的 CLI 界面以后，记录其具体执行的命令；而网络记账针对的与网络连接上的用户会话有关的信息。

命令记账功能目前仅 TACACS+协议支持，具体内容请参考“配置 TACACS+”。

1.5.2 记账的准备工作

在配置 AAA 记账以前，必须完成以下任务：

- 启用 AAA 安全服务。关于如何启用 AAA 的信息，请参见“AAA 概述”。
- 定义安全协议参数。进行记账，需要配置安全协议参数。锐捷产品 Network 记账支持 RADIUS 和 TACACS+安全协议；Exec 记账支持 RADIUS 和 TACACS+协议；Command 记账仅支持 TACACS+协议。关于 RADIUS 协议的信息，请参见“配置 RADIUS”， 关于 TACACS+协议的信息，请参见“配置 TACACS+”。
- （可选）配置 AAA 认证。某些记账需要在用户通过认证之后才进行（例如 Exec 记账），其他情况下，没有经过认证也可以进行记账。关于 AAA 认证的信息，请参见“配置认证”。

1.5.3 配置AAA Exec记账

Exec 记账对于已登录到 NAS 的用户终端，可以记录其进入和退出 CLI 界面的信息。在用户终端登录并进入到 NAS 的 CLI 界面时，会向安全服务器发送一个记账开始（Start）信息，在退出 CLI 界面时，会向服务器发送一个记账结束（Stop）信息。

只有登录到 NAS 的用户终端通过了 Login 认证，才会进行 Exec 记账。如果没有设置 Login 认证，或者认证时候采用了 none 方法，则不会进行 Exec 记账。针对同一个用户终端的登录，登入时如果没有进行过 Start 记账，登出时也就不会进行 Stop 记账。

要配置 AAA Exec 记账，在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)**#aaa new-model**	启用 AAA。
Ruijie(config)**#aaa accounting exec** {**default** | *list-name*} **start-stop** *method1* [*method2*...]	定义一个记账方法列表，如果需要定义多个方法列表，重复执行该命令。
Ruijie(config)**#line vty** *line-num*	进入您需要应用 AAA Exec 记账的线路。
Ruijie(config-line)**#accounting exec** {**default** | *list-name*}	将方法列表应用线路。

关键字 *list-name* 用来命名创建记账方法列表，可以是任何字符串；关键字 *method* 指的是记账实际算法。仅当前面的方法返回 ERROR（无应答），才使用后面的其他记账方法；如果前面的方法返回 FAIL(失败)，则不使用其他记账方法。为了使记账最后能成功返回，即使所有指定方法都没有应答，可以在命令行中将 **none** 指定为最后一个记账方法。

使用关键字 **start-stop**，网络访问服务器在用户开始和结束访问网络服务时都给安全服务器发送记账信息。

使用 RADIUS 进行 Exec 记账

要配置用 RADIUS 服务器进行 Exec 记账，首先要配置 RADIUS 服务器，有关 RADIUS 服务器配置的信息，请参见“配置 RADIUS”。

命令	作用
Ruijie(config)**#aaa new-model**	打开 AAA 开关。
Ruijie(config)**#aaa accounting exec** {**default** | *list-name*} **start-stop group radius**	定义使用 RADIUS 记账方法。
Ruijie(config)**#show aaa method-list**	确认配置的方法列表。
Ruijie(config)**#line vty** *line-num*	进入线路配置模式。
Ruijie(config-line)**#accounting exec** {**default** | *list-name*}	应用方法列表。

配置 Exec 记账示例

下例演示如何进行 Exec 记账。我们设置 VTY 线路 0~4 上的用户登录时采用 Login 认证，并且进行 Exec 记账。其中 Login 认证采用本地认证，Exec 记账采用 RADIUS。远程 RADIUS 服务器地址为 192.168.217.64，共享密钥为 test。本地用户名为 ruijie，口令为 ruijie。如下：

```
Ruijie# config
Ruijie(config)# aaa new-model
Ruijie(config)# radius-server host 192.168.217.64
Ruijie(config)# radius-server key test
Ruijie(config)# username ruijie password ruijie
Ruijie(config)# aaa authentication login auth local
Ruijie(config)# aaa accounting exec acct start-stop group radius
Ruijie(config)# line vty 0 4
Ruijie(config-line)# login authentication auth
Ruijie(config-line)# accounting exec acct
Ruijie(config)# end
Ruijie# show running-config
```

```
!
aaa new-model
!
aaa accounting exec acct start-stop group radius
aaa authentication login auth local
!
username ruijie password ruijie
!
radius-server host 192.168.217.64
radius-server key 7 093b100133
!
line con 0
line vty 0 4
 accounting exec acct
 login authentication auth
!
end
```

1.5.4 配置AAA Network记账

Network（网络）记账提供了关于用户会话的记账信息，包括报文的个数及字节数、IP 地址、用户名等。Network 记账目前只支持 RADIUS 协议。

> RADIUS 记账信息的格式随不同的 RADIUS 安全服务器而变化。记账记录中的内容可能会由于锐捷产品版本的不同而有些变化。

要配置 AAA Network 记账，在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)**#aaa new-model**	启用 AAA。
Ruijie(config)**#aaa accounting network** {**default** | *list-name*} **start-stop** *method1* [*method2*...]	定义一个记账方法列表，如果需要定义多个方法列表，重复执行该命令。

关键字 *list-name* 用来命名创建记账方法列表，可以是任何字符串；关键字 *method* 指的是记账实际算法。仅当前面的方法返回 ERROR（无应答），才使用后面的其他记账方法；如果前面的方法返回 FAIL(失败)，则不使用其他记账方法。为了使记账最后能成功返回，即使所有指定方法都没有应答，可以在命令行中将 **none** 指定为最后一个记账方法。

使用 RADIUS 进行 Network 记账

要配置用 RADIUS 服务器进行 Network 记账，首先要配置 RADIUS 服务器，有关 RADIUS 服务器配置的信息，请参见“配置 RADIUS”。

配置好 RADIUS 服务器后，就可以配置基于 RADIUS 服务器的方法列表了，在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)**#aaa new-model**	打开 AAA 开关。

Ruijie(config)**#aaa accounting network** {**default** | *list-name*} **start-stop group radius**	定义使用 RADIUS 记账方法。

配置 Network 记账示例

以下是使用 RADIUS 进行 Network 记账的一个例子：

```
Ruijie# config
Ruijie(config)# aaa new-model
Ruijie(config)# radius-server host 192.168.217.64
Ruijie(config)# radius-server key test
Ruijie(config)# aaa accounting network acct start-stop group radius
Ruijie(config)# end
Ruijie# show running-config
!
aaa new-model
!
aaa accounting network acct start-stop group radius
!
username Ruijie password 0 starnet
username Ruijie privilege 6
!
radius-server host 192.168.217.64
radius-server key 7 093b100133
```

1.6 监视AAA用户

命令	作用
show aaa user { *id* | **all** }	查看当前 AAA 用户信息。

1.7 配置支持VRF的AAA组

Virtual Private Networks (VPNs)为用户提供了一种安全的方式在 ISP 骨干网上共享带宽。一个 VPN 即是共享路由的站点集。用户站点通过一到多个接口链接到服务提供商网络，VPN 路由表也叫 VPN routing/forwarding (VRF) table，AAA 可以为每个自定义服务器组指定 VRF。

要配置 AAA 组的 VRF，请在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)**#aaa new-model**	打开 AAA 开关。
Ruijie(config)**#aaa group server radius** *gs_name*	配置 RADIUS 服务器组，进入服务器组配置模式。
Ruijie(config-gs-radius)**#ip vrf forwarding** *vrf_name*	为组选择 vrf。

需要产品支持 vrf 功能。

1.8 配置Login的用户认证失败锁定

Login 登录锐捷设备，为了防止 Login 用户破解密码，提供配置命令用于限制用户尝试密码的失败次数；超过尝试失败次数，用户被锁定多长时间不能登录。

要配置 Login 登录参量，请在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)**#aaa new-model**	打开 AAA 开关。
Ruijie(config)**#aaa local authentication attempts** *<1-2147483647>*	配置 login 登录，用户尝试失败次数。
Ruijie(config)**#aaa local authentication lockout-time** *<1-2147483647>*	配置 login 登录，用户尝试超过配置的失败次数，被锁定的时间长度（小时）。
Ruijie**#show aaa user lockout**	显示当前被锁定的用户列表。
Ruijie**#clear aaa local user lockout {all | user-name** *<word>***}**	清除被锁定的用户列表。

默认情况下，Login 尝试失败次数为 3 次，被锁定的时间限制为 15 小时。

1.9 配置基于域名的AAA服务

目前基于域名的 AAA 服务，仅被应用于 IEEE802.1x 认证服务，IEEE802.1x 协议更具体的配置方式参见“配置 802.1x”中相关章节。

1.9.1 概述

在多域环境下，同一台网络访问服务器（NAS）设备可为不同域中的用户提供 AAA 服务，各域中用户的属性（例如用户名及密码、服务类型、权限等）有可能各不相同，因此有必要通过设置域的方法把它们区分开，并为每个域单独配置包括 AAA 服务方法列表（例如使用的 RADIUS）在内的属性集。

本产品支持以下几种的形式的用户名

1) userid@domain-name

2) domain-name\userid

3) userid.domain-name

4) userid

对于第 4 种不带 domain-name 的形式的用户名（即以上第 4 种：userid），认为其域名称为 default，即为默认的域名。

设备基于域名的 AAA 服务基本原理如下：

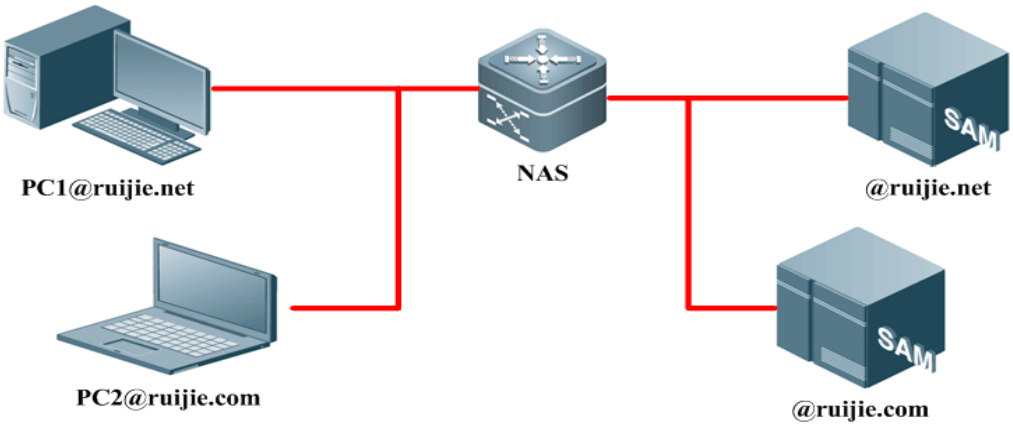
- 解析用户携带的域名称
- 根据域名称查找用户所配置的域
- 根据设备上域配置信息查找相应的 AAA 服务的方法列表名
- 根据方法列表名在系统中查找对应的方法列表

- 使用该方法列表提供 AAA 服务

上述任何一个步骤失败，用户将无法使用申请的 AAA 服务。

以下是典型的多个域环境拓扑图：

图 1-2 典型多个域网络图



1.9.2 基于域名的AAA服务配置

按如下顺序配置基于域名的 AAA 服务：

1) 启用 AAA 服务

2) 定义 AAA 服务的方法列表

3) 启用基于域名的 AAA 服务

4) 创建域

5) 配置域属性集

6) 查看域配置

系统最多支持配置 32 个域。

启用 AAA

命令	作用
Ruijie(config)#**aaa new-model**	打开 AAA 开关。

具体命令说明请参见“启用 AAA” 章节。

定义 AAA 服务的方法列表

命令	作用
Ruijie(config)**#aaa authentication dot1x {default | *list-name*} *method1* [*method2*...]**	定义一个 IEEE802.1x 认证方法列表。
Ruijie(config)**#aaa accounting network {default | *list-name*}** start-stop *method1* [*method2*...]	定义一个 Network 记账方法列表。
Ruijie(config)**#aaa authorization network {default | *list-name*}** *method1* [*method2*...]	定义一个 Network 授权方法列表。

具体说明请参见“配置认证”，“配置记账”和“配置授权”相关章节。

打开基于域名的 AAA 服务开关

命令	作用
Ruijie(config)**#aaa domain enable**	打开基于域名的 AAA 服务开关。

创建域

基于用户名查找匹配的域名时，遵循如下规则：

1) 支持使用单个‘. ‘ 、‘\’ 、‘@ ‘字符区分用户名与域名。

2) 单个 ‘@’字符后跟随的字符串为“域名”。用户名中存在多个‘@’字符时，取最后 1 个‘@’字符后跟随的字符串为域名。如用户名为 a@b@c@d 时，取 a@b@c 为用户名，d 为域。

3) 单个 ‘ \’字符之前的字符串为“域名”。用户名中存在多个‘\’字符时，取第一个‘\’字符之前的字符串为域名。如用户名为 a\b\c\d 时，取 b\c\d 为用户名，a 为域名。

4) 单个 ‘.’ 字符后跟随的字符串为“域名”，用户名中存在多个‘.’字符时，根据预先的配置，取最后 1 个‘.’字符后跟随的字符串为域名。如用户名为 a.b.c.d 时，取 a.b.c 为用户名，d 为域名。

5) 若用户名中同时存在‘. ‘ ‘\’ ‘@ ‘三种字符，匹配域名时，将先进行‘@’字符规则判断，再进行‘\’字符规则判断，最后采用‘.’的判断规则。

命令	作用
Ruijie(config)**#aaa domain** *domain-name*	创建域名为 *domain-name* 的域，并进入域配置模式。

基于域名的 AAA 服务支持最长 64 个字符的域名，不区分大小写。

配置域属性集

在域配置模式下，为已存在的域，选择关联 AAA 服务的方法列表：

命令	作用
Ruijie(config-aaa-domain)**#authentication dot1x {default | *list-name*}**	在域配置模式下，选择认证方法列表。
Ruijie(config-aaa-domain)**#accounting network {default | *list-name*}**	在域配置模式下，选择记账方法列表。
Ruijie(config-aaa-domain)**#authorization network {default | *list-name*}**	在域配置模式下，选择授权方法列表。

配置域状态：

命令	作用
Ruijie(config-aaa-domain)**#state {block | active}**	在域配置模式下，配置域的状态。

配置是否在用户名中携带域名信息：

命令	作用
Ruijie(config-aaa-domain)**#username-format {without-domain | with-domain}**	在域配置模式下，配置 NAS 与服务器交互时域中用户名是否携带域名信息。

配置域支持的最大用户数目：

命令	作用
Ruijie(config-aaa-domain)**#access-limit** *num*	在域配置模式下，配置该域能够容纳的最大用户数目，默认情况不限制用户的数目（只对 802.1x 用户生效）。

在域配置模式下，选择 AAA 服务方法列表时，这些方法列表是在进入域配置模式前已经定义；否则在域配置模式下，允许选择 AAA 方法列表名，但提示配置不存在；

缺省域（default）：在基于域名的 AAA 服务开关打开情况下，如果用户没有携带域信息，则使用缺省域。如果用户携带的域在系统中没有配置，则判定为非法用户，不提供 AAA 服务；

域配置模式下，没有选择方法列表的情况下，系统默认分配缺省方法列表；

查看域配置

配置完成基于域名的 AAA 服务后，通过以下命令可以查看相应的配置：

命令	作用
show aaa domain [*domain-name*]	显示当前基于域名的 AAA 服务域信息。

1.9.3 配置基于域名的AAA服务配置注意事项

配置基于域名的 AAA 服务需要注意以下几个方面：

1) 基于域名的 AAA 服务开关打开的情况下，使用域中选择的方法列表。开关关闭的情况下，按照接入协议（例如 802.1X 等）选定的方法列表进行 AAA 服务。例如开关关闭情况下，802.1X 中以命令 **dot1x authentication** *authen-list-name*，**dot1x accounting** *acct-list-name* 中的 *authen-list-name* 及 *acct-list-name* 为认证和记账方法列表名提供 AAA 服务。

2) 基于域名的 AAA 服务开关打开时，默认情况下没有配置缺省域，需要手动配置完成。缺省域的名称为“default”，若配置缺省域后，用户不携带域信息时，使用缺省域进行提供 AAA 服务。若缺省域没有配置，则不携带域信息的用户不能使用 AAA 服务。

3) 如果认证用户携带有域信息，而域没有在设备上配置，不能为该用户提供 AAA 服务。

4) 域选择的 AAA 服务方法列表名称必须和 AAA 服务所定义的方法列表名称必须一致。若不一致，不能够为该域中的用户提供合适的 AAA 服务。

5) 用户所携带的域名称与设备上所配置的域名的匹配采用最准确匹配。例如：设备上配置了 domain.com 和 domain.com.cn 两个域，一个用户的请求信息携带为 aaa@domain.com。则设备认为会判定该用户所属于的域为 domain.com 而不是域 domain.com.cn。

1.9.4 配置基于域名的AAA服务示例

基于域名的 AAA 服务配置示例：

```
Ruijie(config)# aaa new-model
Ruijie(config)# radius-server host 192.168.197.154
Ruijie(config)# radius-server key test
Ruijie(config)# aaa authentication dot1x default group radius
Ruijie(config)# aaa domain domain.com
Ruijie(config-aaa-domain)# authentication dot1x default
Ruijie(config-aaa-domain)# username-format without-domain
```

上面配置后，如果 radius 服务器上有用户 a1，这时使用 802.1x 客户端进行登录认证，使用用户名为 a1@domain.com，再输入正确的密码进行认证就可认证成功。相关域名信息显示如下：

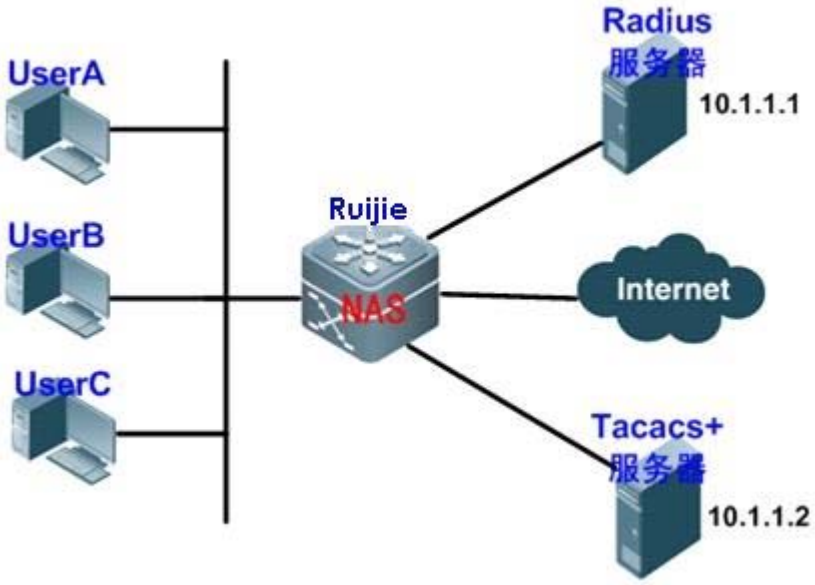
```
Ruijie#show aaa domain domain.com

=============Domain domain.com=============
State: Active
Username format: Without-domain
Access limit: No limit
802.1X Access statistic: 0

Selected method list:
 authentication dot1x default
```

1.10 AAA配置举例

1.10.1 AAA典型应用举例

组网图

图 1-3 AAA 典型应用图



应用需求

在上图的网络应用中，为了更好地对网络访问控制器设备（NAS，以下简称网络设备）进行安全管理，需要满足如下应用要求：

1) 不同的管理人员有各自的用户账号，其用户名和口令不能共享，便于帐号管理和防止泄漏；

2) 对网络设备的访问需经过认证，用户认证的实现方式可以分为本地认证和集中认证，应采用集中认证和本地认证相结合的方式，集中认证为主用、本地认证为备用。在集中认证过程中，要求先通过 Radius 服务器认证，若无响应再转本地认证。

3) 在认证时，不同的用户可以被限制只能访问特定的网络设备；

4) 对用户进行分权限管理：把网络管理用户分为超级用户和普通用户。其中，超级用户对网络设备拥有查看和配置的权限，普通用户对网络设备只拥有特定的查看权限；

5) 服务器端可将用户的认证信息、授权信息和网络行为记录在服务器中，以供日后查看和审计（本例采用 TACACS+进行记账）；

配置要点

通过“应用需求”部分的分析，部署 AAA 可以很好地满足上述需求，其对用户（线路）或服务器动态配置身份认证、授权以及记账类型。通过创建方法列表来定义身份认证、记账、授权类型，然后将这些方法列表应用于特定的服务或接口。具体详见下述“配置步骤”中各个配置点前的说明。

配置步骤

第一步：启用 AAA

！设备启用 AAA 功能

```
Ruijie# configure terminal
```

```
Ruijie(config)# aaa new-model
```

第二步：配置安全服务器

网络中的安全服务器负责认证、授权和记账。服务器上存储管理员的用户信息，服务器上的软件具备事后审计功能（服务器上的软件通过日志可以记录、统计和分析各种信息）。

！ 配置 Radius 服务器信息(设备和 RADIUS 服务器进行通讯的共享密码为 ruijie)

```
Ruijie(config)# radius-server host 10.1.1.1
Ruijie(config)# radius-server key ruijie
```

！ 配置 Tacacs+服务器信息（设备和 TACACS+服务器进行通讯的共享密钥为 redgiant）

```
Ruijie(config)# tacacs-server host 10.1.1.2
Ruijie(config)# tacacs-server key redgiant
```

第三步：配置本地用户

！ 配置口令加密以防止泄漏（配置后本地的口令以及安全服务器的密钥信息等均以简单加密形式保存和显示）

```
Ruijie(config)# service password-encryption
```

！ 配置本地用户数据库（配置用户名和口令信息并绑定用户级别）

```
Ruijie(config)# username bank privilege 10 password yinhang
Ruijie(config)# username super privilege 15 password star
Ruijie(config)# username normal privilege 2 password normal
Ruijie(config)# username test privilege 1 password test
```

！ 配置本地 enable 口令，用于本地 enable 认证

```
Ruijie(config)# enable secret w
```

！ 配置线路登陆口令（在 AAA 模式打开的情况下，终端线路上的登陆口令不起作用。配置这个口令的一般目的，是为了防止关闭 AAA 模式的情况下，终端因没有配置口令而无法登陆成功）

```
Ruijie(config)# line vty 0 15
Ruijie(config-line)# password w
```

！ 配置线路用户级别（如果未打开 Exec 授权，或者该线路未应用任何 Exec 授权方法列表并且不存在默认的 Exec 授权方法列表，该级别将被使用）

```
Ruijie(config)# line vty 0 15
Ruijie(config-line)# privilege level 10
```

第四步：配置认证

■ Login 认证

网络设备上配置 Login 认证，Login 认证可以控制用户是否能访问。定义认证方法列表，首先是 Radius 认证方法，然后是 Local 方法，在远程认证没有响应的情况下转本地认证。

！ 配置 login 认证方法列表（按 Radius、Local 的次序），然后应用到相应线路。

```
Ruijie(config)# aaa authentication login hello group radius local
```

```
Ruijie(config)# line vty 0 15
Ruijie(config-line)# login authentication hello
```

为了防止用户在 Login 认证的时候，使用穷举法破解密码，AAA 可以限制用户 Login 尝试次数，在 Login 失败达到一定次数时，用户将被锁定一段时间不能登录（默认情况下，login 尝试失败次数为 3 次，被锁定的时间限制为 15 小时）。

！ 配置失败次数为 2 次，锁定时间 10 小时

```
Ruijie(config)# aaa local authentication attempts 2
Ruijie(config)# aaa local authentication lockout-time 10
```

■ Enable 认证

网络设备上配置 Enable 认证，用户切换权限级别需要进行认证。这样，如果普通用户想通过 enable 命令切换到超级用户的权限，还需要进行一次认证过程。配置时，首先是 Radius 认证方法，远程认证没有响应的情况下转本地 Enable 认证方法。Enable 认证只能配置默认的方法列表，配置以后，会自动被应用。

！配置 enable 认证方法列表（按 Radius、Tacacs+、Local 的次序）

```
Ruijie(config)# aaa authentication enable default group radius local
```

配置授权

■ Exec 授权

网络设备上配置 Exec 授权，通过授予不同的用户级别控制其执行命令的权限。例如 15 级是超级用户，14 级是配置用户，2 级是普通用户。配置时，首先配置远程 Exec 授权，远程授权没有响应转本地授权。

！ 配置 exec 授权方法列表（按 Tacacs+、Local 的次序），然后应用到线路

```
Ruijie(config)# aaa authorization exec shouquan group tacacs+ local
Ruijie(config)# line vty 0 15
Ruijie(config-line)# authorization exec shouquan
```

！ 控制台线路若要配置进行 Exec 授权（控制台线路默认不进行 Exec 授权），配置如下：

```
Ruijie(config)# aaa authorization console
```

■ Command 授权

网络设备上配置 Command 授权，对于关键命令的执行权限只授予部分管理人员。命令授权是根据命令本身的级别，而不是用户当前的级别。例如 configure terminal 命令是 2 级的，即用户级别如果小于 2 级的，在设备 CLI 界面上将无法看见这条命令，自然也无法执行。如果将 2 级命令配置了 Command 授权，则即使当前是执行命令的是超级用户，也要通过了 Command 授权过程才能执行该命令。该授权不支持 Radius 协议。

！配置 command 授权方法列表（按 Tacacs+、Local 的次序），然后应用到线路

```
Ruijie(config)# aaa authorization commands 2 abc group tacacs+ local
Ruijie(config)# line vty 0 15
Ruijie(config-line)# authorization commands 2 abc
```

配置记账

- Exec 记账

网络设备上配置 Exec 记账，这样设备将用户的登陆和退出信息发送到服务器，以备查看和统计，以及事后审计。

！ 配置 exec 记账方法列表（使用 TACACS+服务器记账），默认应用到所有线路

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

- Command 记账

网络设备可以配置 Command 记账，设备将用户执行过的某一级别的命令发送到服务器，以备查看和统计，以及事后审计。

！配置 command 记账方法列表（只支持 tacacs+），默认应用到所有线路。

```
Ruijie(config)# aaa accounting commands 2 default start-stop group tacacs+
```

配置验证

第一步，可通过 show running-config 命令来查看当前配置信息的正确性：

```
Ruijie# show running-config
......
!
aaa new-model
aaa local authentication attempts 2
aaa local authentication lockout-time 10
aaa authorization exec shouquan group tacacs+ local
aaa authorization commands 2 abc group tacacs+
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 2 default start-stop group tacacs+
aaa authentication login hello group radius local
aaa authentication enable default group radius local
!
username bank password 7 09361c1c2f041c4d
username bank privilege 10
username super password 7 093c011335
username super privilege 15
username normal password 7 09211a002a041e
username normal privilege 2
username test password 7 093b100133
service password-encryption
!
tacacs-server key 7 072c062b121b260b06
tacacs-server host 10.1.1.2
radius-server host 10.1.1.1
radius-server key 7 072c16261f1b22
enable secret 5 $1$2MjW$xr1t0s1Euvt76xs2
!
line con 0
```

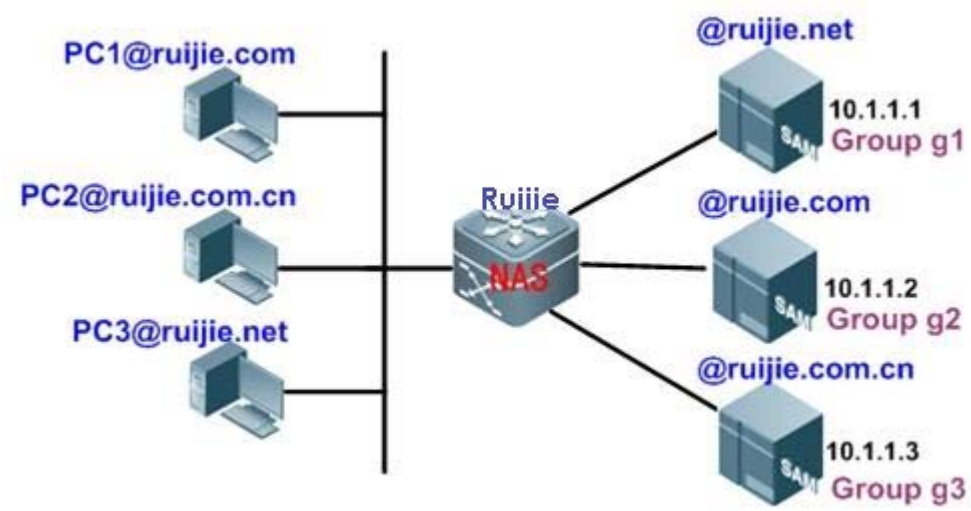
```
line vty 0 4
 authorization exec shouquan
 authorization commands 2 abc
 privilege level 10
 login authentication hello
 password 7 0938
line vty 5 15
 authorization exec shouquan
 authorization commands 2 abc
 privilege level 10
 login authentication hello
 password 7 005d
!
end
```

第二步，在实际应用中，可通过 **show aaa user** { *id* | **all** }命令来查看当前登录的 AAA 用户信息（此处显示省略说明）。

1.10.2 AAA多域认证应用举例

组网图

图 1-4 AAA 多域认证应用图



应用需求

通过配置网络访问控制器设备（NAS，以下简称网络设备）实现基于域名的 AAA 服务，包括认证、授权、记账功能：

- 使用 802.1x 客户端进行登录认证，使用用户名为 PC1@ruijie.com 或 PC2@ruijie.com.cn 或 PC3@ruijie,.net，再输入正确的密码进行认证就可认证成功。
- 对用户进行分权限管理：把网络管理用户分为超级用户和普通用户。其中，超级用户对网络设备拥有查看和配置的权限，普通用户对网络设备只拥有特定的查看权限；

■ 认证服务器端可将用户的认证信息、授权信息和网络行为记录在服务器中，以供日后查看和审计；

配置要点

通过配置基于域名的 AAA 服务，可以满足上述需求，具体说明见下述每项配置步骤前的说明。

本用例以 802.1x 客户端为例，因此网络设备必须支持 802.1x 客户端接入，若不支持则本用例不适用。

配置步骤

启用 AAA

```
Ruijie# configure terminal
Ruijie(config)# aaa new-model
```

配置安全服务器

网络中的安全服务器负责认证、授权和记账。服务器上存储管理员的用户信息，服务器上的软件具备事后审计功能（服务器上的软件通过日志可以记录、统计和分析各种信息）。

！ 配置 Radius 服务器组信息,并配置设备和 Radius 服务器进行通讯的共享密码为 ruijie

```
Ruijie(config)# aaa group server radius g1
Ruijie(config-gs-radius)# server 10.1.1.1
Ruijie(config-gs-radius)# exit
Ruijie(config)# aaa group server radius g2
Ruijie(config-gs-radius)# server 10.1.1.2
Ruijie(config-gs-radius)# exit
Ruijie(config)# aaa group server radius g3
Ruijie(config-gs-radius)# server 10.1.1.3
Ruijie(config-gs-radius)# exit
Ruijie(config)# radius-server key ruijie
```

配置本地用户

！ 配置口令加密以防止泄漏（配置后本地的口令以及安全服务器的密钥信息等均以简单加密形式保存和显示）

```
Ruijie(config)# service password-encryption
```

！ 配置本地用户数据库（配置用户名和口令信息并绑定用户级别）

```
Ruijie(config)# username bank privilege 10 password yinhang
Ruijie(config)# username super privilege 15 password star
Ruijie(config)# username normal privilege 2 password normal
Ruijie(config)# username test privilege 1 password test
```

！ 配置本地 enable 口令，用于本地 enable 认证

```
Ruijie(config)# enable secret w
```

定义 AAA 服务的方法列表

！ 配置 dot1x 认证

```
Ruijie(config)# aaa authentication dot1x renzheng group radius local
```

！ 配置 network 授权

```
Ruijie(config)# aaa authorization network shouquan group radius
```

！ 配置 network 记账

```
Ruijie(config)# aaa accounting network jizhang start-stop group radius
```

打开基于域名的 AAA 服务开关

```
Ruijie(config)# aaa domain enable
```

创建域并配置域属性集

！ 创建域

```
Ruijie(config)# aaa domain ruijie.com
```

！ 关联 AAA 服务的方法列表

```
Ruijie(config-aaa-domain)# authentication dot1x renzheng
Ruijie(config-aaa-domain)# authorization network shouquan
Ruijie(config-aaa-domain)# accounting network jizhang
```

！配置域状态

```
Ruijie(config-aaa-domain)# state active
```

！配置在用户名中不携带域名信息

```
Ruijie(config-aaa-domain)# username-format without-domain
!
Ruijie(config)# aaa authentication dot1x renzheng group g2
Ruijie(config)# aaa authorization network shouquan group g2
!
Ruijie(config)# aaa accounting network jizhang start-stop group g2
!
```

同理，域名为 ruijie.com.cn 和 ruijie.net 的配置方法与上述相同（此处不再赘述）。

配置验证

第一步，可通过 show running-config 命令来查看当前配置信息的正确性（以域名为 `ruijie.com` 为例）：

```
Ruijie# show running-config
......
!
aaa new-model
aaa domain enable
!
aaa domain ruijie.com
 authentication dot1x renzheng
 accounting network jizhang
 authorization network shouquan
 username-format without-domain
!
!
aaa group server radius g1
 server 10.1.1.1
!
aaa group server radius g2
 server 10.1.1.2
!
aaa group server radius g3
 server 10.1.1.3
!
!
aaa accounting network jizhang start-stop group g2
aaa authorization network shouquan group g2
aaa authentication dot1x renzheng group g2
!
no service password-encryption
!
radius-server key ruijie
!
```

第二步，显示当前基于域名的 AAA 服务域信息：

```
Ruijie#show aaa domain

=============Domain ruijie.com=============
State: Active
Username format: Without-domain
Access limit: No limit
802.1X Access statistic: 0

Selected method list:
 authentication dot1x renzheng
 authorization network shouquan
 accounting network jizhang
```

2 RADIUS

2.1 RADIUS概述

RADIUS 是远程认证拨号用户服务(Remote Authentication Dial-In User Service) 的简称，它是一种分布式的客户机/服务器系统，与 AAA 配合对试图连接的用户进行身份认证，防止未经授权的访问。在 RGOS 的实现中，RADIUS 客户端运行在设备或网络访问服务器（NAS）上，并向中央 RADIUS 服务器发出身份认证请求，中央服务器包含了所有的用户身份认证和网络服务信息。

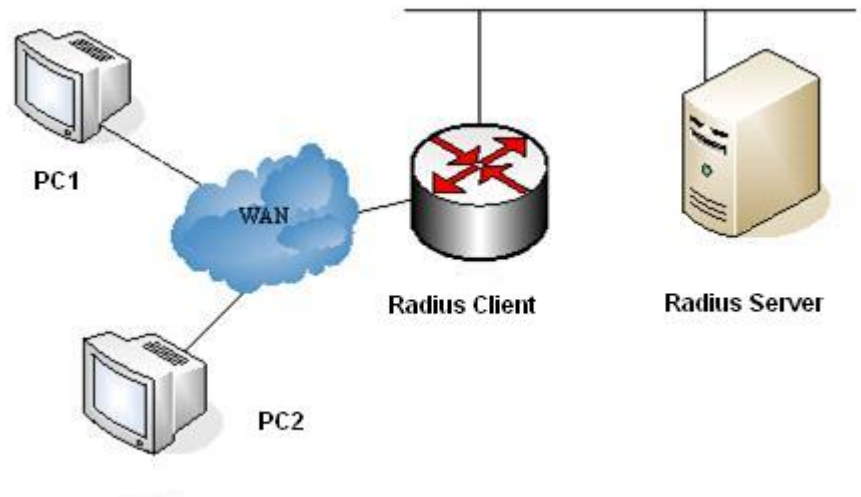
由于 RADIUS 是一种完全开放的协议，很多系统如 UNIX、WINDOWS 2000、WINDOWS 2008 等均将 RADIUS 服务器作为一个组件安装，因此 RADIUS 是目前应用最广泛的安全服务器。

RADIUS 的运行过程如下：

- 提示用户输入用户名和密码。
- 用户名和加密的密码通过网络发送到 RADIUS 服务器。
- RADIUS 返回下述响应之一：
- ACCEPT：通过用户身份认证。
- REJECT：身份认证失败，提示重新输入用户名和密码。
- CHALLENGE：RADIUS 服务器发出询问请求，从用户那里收集更多认证信息。
- 在 ACCEPT 的响应中包含用户的授权信息。

下图是一个典型的 RADIUS 拓扑图：

图 2-1 典型 RADIUS 网络配置



除了提供认证服务之外，RADIUS 服务器还提供接入用户的授权和记账的服务。

RADIUS 安全协议，也称 RADIUS 方法，是以 RADIUS 服务器组为单位进行配置的。每一个 RADIUS 方法对应一个 RADIUS 服务器组，每一个 RADIUS 服务器组可配置一至多台 RADIUS 服务器（关于使用 RADIUS 方法的细节信息，请参见“AAA 配置”章节）。如果您在一个 RADIUS 服务器组中配置了多台 RADIUS 服务器，那么当设备同第一台 RADIUS 服务器通讯失败，或者第一台 RADIUS 服务器变成不可达的状态时，设备将自动尝试同第二台 RADIUS 服务器通讯，以此类推，直到成功或者全部失败为止。

2.2 RADIUS配置任务

要在网络设备上配置 RADIUS，必须先执行以下任务：

- 启用 AAA。关于如何启用 AAA 的信息，请参见“AAA 概述”。
- 使用 **aaa authentication** 命令定义 RADIUS 身份认证方法列表。关于使用 **aaa authentication** 命令定义身份认证列表的信息，请参见“配置认证”。
- 在特定线路上应用定义的认证列表，否则使用默认身份认证列表进行认证。关于更详细信息，请参见“配置认证”。

完成以上任务后，就可进行配置 RADIUS。配置 RADIUS 包括以下几个部分：

- 配置 RADIUS 协议参数
- 指定 RADIUS 身份认证
- 指定 RADIUS 标准属性类型
- 指定 RADIUS 私有属性类型
- 配置 RADIUS 服务器可达性检测功能

2.2.1 配置RADIUS协议参数

在网络设备上配置 RADIUS 之前，应确保 RADIUS 服务器的网络通讯良好。要配置 RADIUS 协议参数，请执行以下命令：

命令	作用
Ruijie**# configure terminal**	进入全局配置模式
Ruijie(config)**# radius-server host** *ip-address* [**auth-port** *port*] [**acct-port** *port*]	配置远程 RADIUS 安全服务器的 IP 地址，指定认证端口和记帐端口。
Ruijie(config)**# radius-server key** *string*	配置设备和 RADIUS 服务器进行通讯的共享密码。
Ruijie(config)**# radius-server retransmit** *retries*	指定设备在确认 RADIUS 无效以前发送请求的次数（默认值为 3）。
Ruijie(config)**# radius-server timeout** *seconds*	指定设备重传请求以前等待的时间（默认值为 5 秒）。

配置 RADIUS，必须要配置 RADIUS Key。网络设备上的共享密码和 RADIUS 服务器上的共享密码必须一致。

在使用 RADIUS 安全协议的 802.1x 认证环境中，如果网络设备作为 802.1x 认证者，并且采用锐捷 SU 作为 802.1x 客户端软件时，建议在网络设备上设置 **radius-server timeout** 值为 3 秒(默认为 5 秒),设置 **radius-server retransmit** 值为 2 次（默认为 3 次）。

2.2.2 指定RADIUS身份认证

指定 RADIUS 服务器并定义了 RADIUS 身份认证共享密码后，需要为 RADIUS 定义身份认证方法列表。由于 RADIUS 身份认证是通过 AAA 来进行的，所以需要执行 **aaa authentication** 命令来定义身份认证方法列表，并指定身份认证方法为 RADIUS。关于更详细的信息，可以参考 AAA 配置。

2.2.3 指定RADIUS标准属性类型

通过该节可以配置标准属性的类型，目前支持设置 RADIUS Calling-Station-ID 属性（属性值为 31）。

配置 Calling-Station-ID 格式

RADIUS Calling-Station-ID 属性用于网络设备向 RADIUS Server 发送请求报文时候，标识认证用户的身份。Calling-Station-ID 属性内容是字符串，可以有多种组成格式，由于要求必须能唯一标识一个用户，因此常选择使用用户的 MAC 地址作为其内容。例如在使用 IEEE 802.1X 认证时，选择使用安装 IEEE 802.1X 客户端所在设备的 MAC 地址。关于这 MAC 地址的格式，有以下几种：

格式	说明
ietf	IETF（RFC3580）规定的标准格式，使用‘-’作为分隔符。例如： 00-D0-F8-33-22-AC
normal	常用的表示 MAC 地址的格式（点分十六进制格式），使用‘.’作为分隔符。例如： 00d0.f833.22ac
unformatted	无格式，没有任何分隔符，默认使用这个格式。例如： 00d0f83322ac

要配置 RADIUS Calling-Station-ID 属性（基于 MAC）的格式，请执行以下命令：

命令	作用
Ruijie**# configure terminal**	进入全局配置模式
Ruijie(config)# **radius-server attribute 31 mac format {ietf | normal | unformatted}**	配置 RADIUS Calling-Station-ID 属性（基于 MAC）的格式，默认使用 unformatted 格式。

2.2.4 指定RADIUS私有属性类型

通过该节可以自由配置私有属性的类型。默认配置分为锐捷产品私有属性类型的默认配置，以及扩展厂商类型的默认配置。如下：

ID	功能	TYPE	扩展 TYPE
1	max-down-rate	1	76
2	port-priority	2	77
3	user-ip	3	3
4	vlan-id	4	4

5	last-supplicant-version	5	5
6	net-ip	6	6
7	user-name	7	7
8	password	8	8
9	file-directory	9	9
10	file-count	10	10
11	file-name-0	11	11
12	file-name-1	12	12
13	file-name-2	13	13
14	file-name-3	14	14
15	file-name-4	15	15
16	max-up-rate	16	16
17	current-supplicant-version	17	17
18	flux-max-high32	18	18
19	flux-max-low32	19	19
20	proxy-avoid	20	20
21	dailup-avoid	21	21
22	ip-privilege	22	22
23	login-privilege	42	42
26	ipv6-multicast-address	79	79
27	ipv4-multicast-address	87	87
62	sdg-type	62	62
85	sdg-zone-name	85	85
103	sdg-group-name	103	103

部分私有属性功能仅在特定产品上支持，具体产品所支持的私有属性列表可以通过 **show radius vendor-specific** 命令查看；

两个属性功能不能配置为一个类型号；

以下是网络设备配置私有类型的具体实例：

```
Ruijie# show radius vendor-specific
id     vendor-specific       type-value
----- -------------------- ----------
1     max-down-rate          76
2     port-priority          77
3     user-ip                 3
4     vlan-id                 4
......

Ruijie# configure
Ruijie(config)# radius attribute 4 vendor-type 67
Ruijie(config)# show radius vendor-specific
id     vendor-specific       type-value
```

```
----- -------------------- ----------
1     max-down-rate          76
2     port-priority          77
3     user-ip                 3
4     vlan-id                 67
......
```

2.2.5 配置RADIUS服务器可达性检测功能

设备维护所配置的每台 RADIUS 服务器的可达性状态：可达或者不可达。设备不会向处于不可达状态的 RADIUS 服务器发送接入用户的认证、授权和记账请求，除非，该 RADIUS 服务器所在的 RADIUS 服务器组的所有服务器均为不可达状态。

设备支持对指定的 RADIUS 服务器进行主动探测，默认关闭。如果您为指定的 RADIUS 服务器开启主动探测功能，那么设备将会根据配置，定期向该 RADIUS 服务器发送探测请求（认证请求或者记账请求）。其时间间隔周期为：

- 处于可达状态的 RADIUS 服务器：该 RADIUS 服务器的可达状态的主动探测间隔时间（默认值为 60 分钟）。
- 处于不可达状态的 RADIUS 服务器：固定为 1 分钟。

为指定的 RADIUS 服务器开启主动探测功能，需要满足如下所有条件：

- 在设备上配置了该 RADIUS 服务器的测试用户名。
- 在设备上至少配置了一个该 RADIUS 服务器的被测端口（认证端口或者记账端口）。

对于一台处于可达状态的 RADIUS 服务器，当以下两个条件均满足时，设备认为该 RADIUS 服务器进入不可达状态：

- 距离上次收到该 RADIUS 服务器的正确响应超过 radius-server dead-criteria time seconds 设定的时间。
- 在上次收到该 RADIUS 服务器的正确响应之后，设备发往该 RADIUS 服务器的请求而未收到正确响应的次数（包括重传），达到 radius-server dead-criteria tries number 设定的次数。

对于一台处于不可达状态的 RADIUS 服务器，当以下任一条件满足时，设备认为该 RADIUS 服务器进入可达状态：

- 设备收到来自该 RADIUS 服务器的正确响应。
- 该 RADIUS 服务器处于不可达状态超过 **radius-server deadtime** 设定的时间，并且该 RADIUS 服务器没有启用主动探测功能。
- 在设备上更新该 RADIUS 服务器的认证端口或者记账端口。

RADIUS 服务器可达性检测功能允许用户对 RADIUS 服务器不可达状态的判定标准和主动探测功能进行配置。

要配置 RADIUS 服务器可达性检测功能，请在全局配置模式下执行以下命令：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式

Ruijie(config)# **radius-server dead-criteria time** *seconds* **tries** *number*	配置全局的 RADIUS 安全服务器不可达的判定标准。*seconds* 的默认值为 60 秒，*number* 的默认值为 10 次。
Ruijie(config)# **radius-server deadtime** *minutes*	配置设备停止向不可达状态的 RADIUS 服务器发送请求报文的时长（默认值为 0 分钟）。
Ruijie(config)# **radius-server host** *ip-address* [**auth-port** *port*] [**acct-port** *port*] [**test username** *name* [**idle-time** *time*] [**ignore-auth-port**] [**ignore-acct-port**]]	配置远程 RADIUS 安全服务器的 IP 地址，指定认证端口和记帐端口，指定主动探测的相关参数（测试用户名，可达状态的 RADIUS 服务器的主动探测间隔时间，是否忽略认证端口或者忽略记账端口）。

推荐使用专用的测试用户名，不被其他合法的接入用户所使用，以免对其他合法的接入用户的认证、授权或记账产生影响。

2.3 监控RADIUS

要监控 RADIUS，请在特权用户模式执行以下命令：

命令	作用
Ruijie#**debug radius** { **event** | **detail** }	打开 RADIUS 调试开关，查看 RADIUS 调试信息。

2.4 RADIUS 配置示例

典型 RADIUS 网络配置图中，RADIUS 服务器对访问用户进行身份认证，并为访问用户启用记帐功能，记录用户使用网络服务情况。

RADIUS 服务器可以是 Windows 2000/2003 Server（IAS）、UNIX 系统所带组件,也可以是一些厂商通过的专用服务器软件。

以下是网络设备配置 RADIUS 的具体实例：

```
Ruijie# configure terminal
Ruijie(config)# aaa new-model
Ruijie(config)# radius-server host 192.168.12.219 auth-port 1645 acct-port 1646
Ruijie(config)# radius-server key aaa
Ruijie(config)# aaa authentication login test group radius
Ruijie(config)# end
Ruijie# show radius server
Server IP:         192.168.12.219
Accounting Port: 1646
Authen  Port:      1645
Test Username:     <Not Configured>
Test Idle Time:    60 Minutes
Test Ports:        Authen and Accounting
Server State:      Active
     Current duration 765s, previous duration 0s
    Dead: total time 0s, count 0
```

```
    Statistics:
        Authen: request 15, timeouts 1
        Author: request 0, timeouts 0
        Account: request 0, timeouts 0
```

```
Ruijie# configure terminal
Ruijie(config)# line vty 0
Ruijie(config-line)# login authentication test
Ruijie(config-line)# end
Ruijie# show running-config
!
aaa new-model
!
aaa authentication login test group radius
!
radius-server host 192.168.12.219 auth-port 1645 acct-port 1646
radius-server key aaa
!
line con 0
line vty 0
login authentication test
line vty 1 4
!
```

2.5 RADIUS IPv6 配置示例

典型 RADIUS 网络配置图中，RADIUS 服务器对访问用户进行身份认证，并为访问用户启用记帐功能，记录用户使用网络服务情况。

RADIUS 服务器为 Windows 2008 Server，也可以是一些厂商通过的专用支持 IPv6 的服务器软件。

以下是网络设备配置 RADIUS 的具体实例：

```
Ruijie# configure terminal
Ruijie(config)# aaa new-model
Ruijie(config)# radius-server host 3000::100 auth-port 1645 acct-port 1646
Ruijie(config)# radius-server key aaa
Ruijie(config)# aaa authentication login test group radius
Ruijie(config)# end
Ruijie# show radius server
Server IP:        3000::100
Accounting Port: 1646
Authen  Port:     1645
Test Username:    <Not Configured>
Test Idle Time:   60 Minutes
```

```
Test Ports:       Authen and Accounting
Server State:     Active
     Current duration 765s, previous duration 0s
    Dead: total time 0s, count 0
    Statistics:
        Authen: request 15, timeouts 1
        Author: request 0, timeouts 0
        Account: request 0, timeouts 0
```

```
Ruijie# configure terminal
Ruijie(config)# line vty 0
Ruijie(config-line)# login authentication test
Ruijie(config-line)# end
Ruijie# show running-config
!
aaa new-model
!
aaa authentication login test group radius
!
radius-server host 3000::100 auth-port 1645 acct-port 1646
radius-server key aaa
!
line con 0
line vty 0
login authentication test
line vty 1 4
!
```

3 TACACS+

3.1 TACACS+概述

TACACS+（是在 TACACS（RFC 1492 Terminal Access Controller Access Control System））基础上进行了功能增强的安全协议。主要是通过 Client-Server 模式与 TACACS 服务器通信来实现多种用户的 AAA 功能，可用于终端用户的认证、授权和计费，在配置使用 TACACS+服务器前，需要先配置好 TACACS+服务器的相关内容。

TACACS+支持用户认证、授权和计费分析，即我们可以使用一台服务器进行认证，然后使用另外一台服务器进行授权，同时可以使用第三台服务器进行计费，每台服务器可以拥有自己的用户数据信息，可以独立进行用户的认证、授权和计费。

TACACS+的报文格式如下：

图 3-1

4	8	16	24	32 bit
Major	Minor	Packet type	Sequence no.	Flags
Session ID				
Length				

Major Version — 主要 TACACS+ 版本号。

Minor Version — 次要 TACACS+ 版本号。

Packet Type — 可能值包括：
TAC_PLUS_AUTHEN： = 0x01 （认证）；
TAC_PLUS_AUTHOR：= 0x02 （授权）；
TAC_PLUS_ACCT：= 0x03 （计费）

Sequence Number — 当前会话中的数据包序列号。会话中的第一个 TACACS+ 数据包序列号必须为 1，其后的每个数据包序列号逐次加 1。因此客户机只发送奇序列号数据包，而 TACACS+ Daemon 只发送偶序列号数据包。

Flags — 该字段包括各种位图格式的标志（flag）。Flag 值表明数据包是否进行加密。

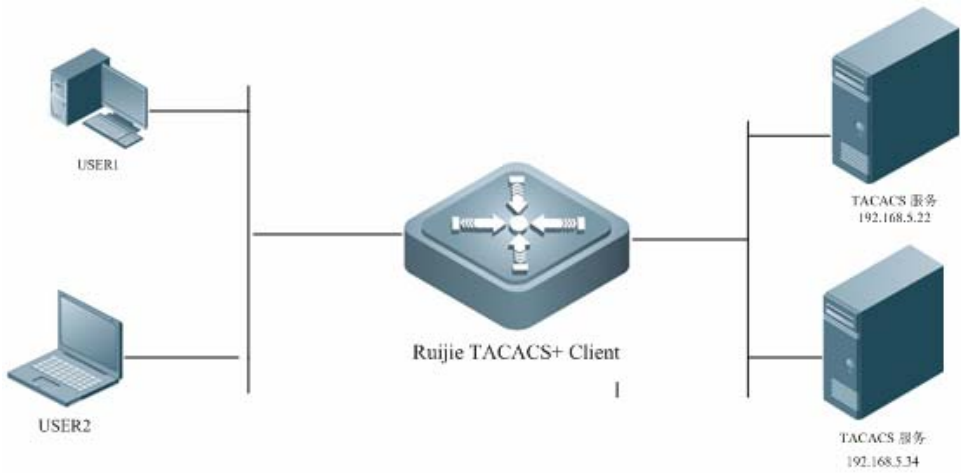
Session ID — 该 TACACS+ 会话的 ID。

Length — TACACS+ 数据包主体长度（不包括头部），报文全部以加密形式在网络上传输。

3.2 TACACS+应用

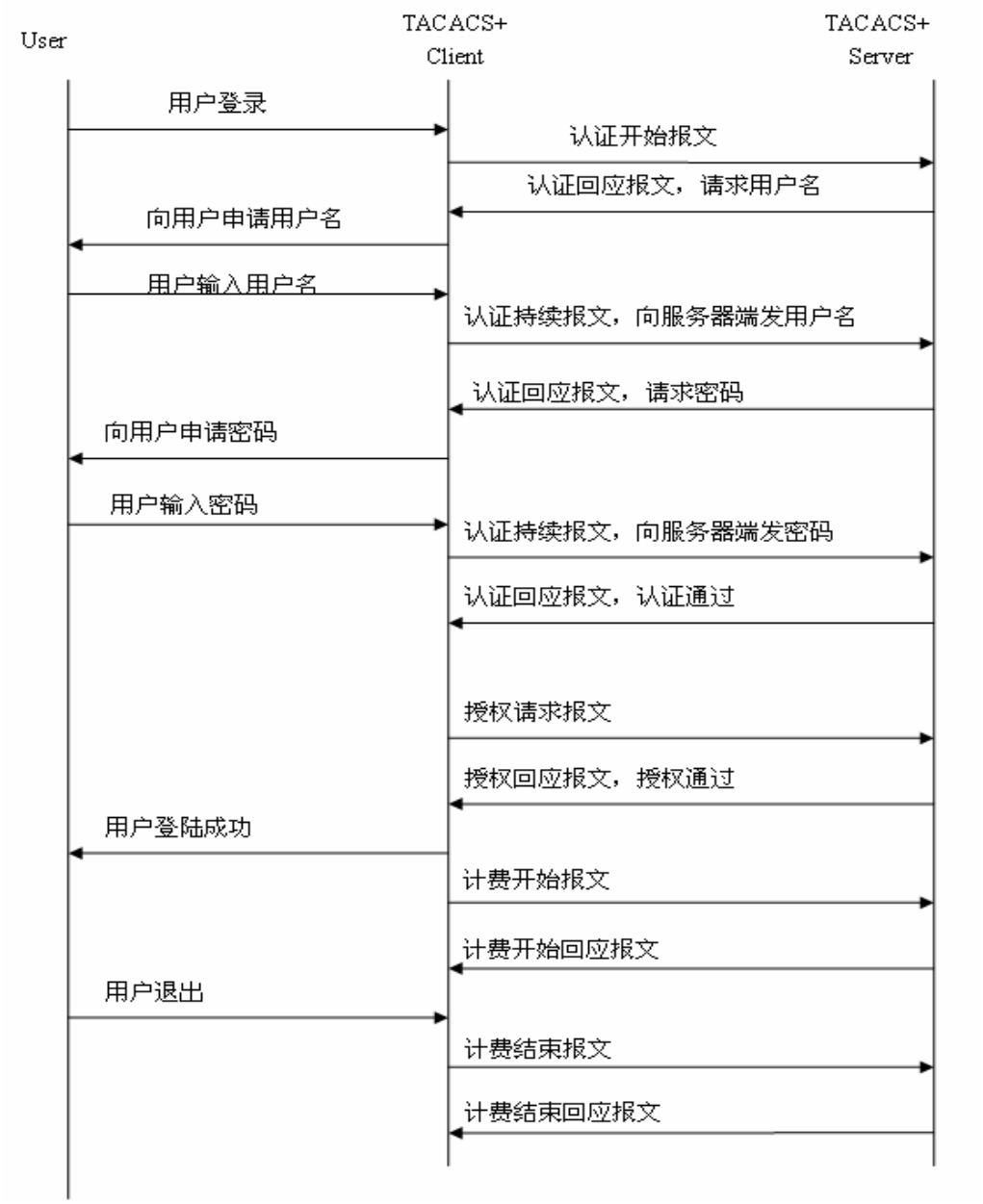
TACACS+的典型应用为终端用户的登陆管理控制，网络设备作为 TACACS+的客户端，将用户名和密码发给 TACACS+服务器进行验证，验证通过并得到授权之后可以登录到网络设备上进行操作。如下图所示：

图 3-2



下边以 login 登陆的基本认证、授权和计费说明 TACACS+运行中的数据报文的交互：

图 3-3



在整个过程中的基本消息交互流程可以分为三个部分：

1) 认证过程包含：

- 用户请求登录网络设备。
- TACACS+客户端收到请求之后，向 TACACS+服务器发送认证开始报文。
- TACACS+服务器发送认证回应报文，请求用户名；
- TACACS+客户端向用户询问用户名。
- 用户输入登陆的用户名信息。
- TACACS+客户端收到用户名后，向 TACACS+服务器发送认证持续报文，其中包括了用户名。
- TACACS+服务器发送认证回应报文，请求登录密码；
- TACACS+客户端收到向用户询问登录密码。

- 用户输入登陆的密码信息。
- TACACS+客户端收到登录密码后，向 TACACS+服务器发送认证持续报文，其中包括了登录密码。
- TACACS+服务器发送认证回应报文，指示用户通过认证。

1) 认证通过后对用户进行授权：

- TACACS+客户端向 TACACS+服务器发送授权请求报文。
- TACACS+服务器发送授权回应报文，指示用户通过授权。
- TACACS+客户端收到授权回应成功报文，向用户输出网络设备的配置界面。

2) 授权通过后，需要对登陆的用户进行计费，审计。

- TACACS+客户端向 TACACS+服务器发送计费开始报文。
- TACACS+服务器发送计费回应报文，指示计费开始报文已经收到。
- 用户退出。
- TACACS+客户端向 TACACS+服务器发送计费结束报文。
- ACACS+服务器发送计费回应报文，指示计费结束报文已经收到。

3.3 TACACS+配置任务

要在网络设备上配置 TACACS+，必须先执行以下任务：

- 使用 **aaa new-model** 命令启用 AAA。在使用 TACACS+前必须先启用 AAA，关于如何启用 **aaa new-model** 的信息，请参见“AAA 概述”。
- 使用 **tacacs-server host** 命令配置一个或多个 tacacs+服务器。
- 使用 **tacacs-server key** 命令指定服务器和网络设备共享的 key。
- 使用 **tacacs-server timeout** 命令指定等待服务器响应的超时时间。
- 如果需要认证，使用 **aaa authentication** 命令定义使用 TACACS+的身份认证方法列表。关于使用 **aaa authentication** 命令定义身份认证列表的信息，请参见“配置认证”。
- 如果需要授权，使用 **aaa authorization** 命令定义使用 TACACS+的授权方法列表。关于使用 **aaa authorization** 命令定义授权方法列表的信息，请参见“配置授权”。
- 如果需要记帐，使用 **aaa accounting** 命令定义使用 TACACS+的记帐方法列表。关于使用 **aaa accounting** 命令定义记帐方法列表的信息，请参见“配置记帐”。
- 在特定线路上应用定义的认证列表，否则使用默认列表。

3.3.1 配置TACACS+协议参数

在网络设备上配置 TACACS+之前，应确保 TACACS+服务器的网络通讯良好。要配置 TACACS+协议参数，请执行以下命令：

命令	作用
Ruijie# configure terminal	进入全局配置模式
Ruijie(config)# **tacacs-server host** {*ip-address* | *ipv6-address*} [**port** *integer*] [**timeout** *integer*] [**key** *string*]	配置远程 TACACS+安全服务器的 IP 地址，通过不同的参数组合份配置该服务器的不同的参数： *ip-address* ：配置服务器的地址。 *ipv6-address：配置服务器的 IPV6 地址。* **port** *intege* [可选] ：确定服务器使用的端口，默认使用 49，可配置范围 1 到 65535。 timeout *integer* [可选] ：用于配置本服务器的超时响应的时间，默认 5s，可配置范围 1 到 1000s key *string* [可选]：用于配置和对应 ip 的服务器的共享的密钥。
Ruijie(config)# **tacacs-server key** *string*	配置设备和 TACACS+服务器进行通讯的共享密钥，当对应的主机没有单独配置 key 时，则使用全局的配置。
Ruijie(config)# **tacacs-server timeout** *seconds*	指定设备重传请求以前等待的时间（默认值为 5 秒），当特定主机没有配置特定的超时时间时，则使用全局的配置时间。
Ruijie(config)# **ip tacacs source-interface** *interface*	指定发送 tacacs+请求到服务器使用的源 IP，默认为不指定
Ruijie(config)# **aaa group server tacacs+** *group-name*	配置 TACACS+服务器组，将不同的 TACACS+服务器划分到不同的组。
Ruijie(config-gs-tacacs)# **server** {*ip-address* | *ipv6-address*}	配置 TACACS+服务器组中的服务器地址
Ruijie(config-gs-tacacs)# **ip vrf forwarding** *vrf-name*	配置 TACACS+服务器组使用的 vrf 名字(支持 VRF 的设备存在此命令)

配置 TACACS+，必须要配置 TACACS+ Key。网络设备上的共享密码和 TACACS+服务器上的共享密码必须一致。

3.4 使用TACACS+ 进行认证、授权、记帐配置示例

典型 TACACS+网络配置图中，TACACS+服务器对访问用户进行身份认证、授权和记帐，下边分别通过 login 认证、授权和记帐，演示如何配置使用 TACACS+进行认证、授权和记帐。

3.4.1 Login 认证使用TACACS+的配置示例：

1) 首先配置启用 aaa：

```
Ruijie# configure terminal
Ruijie(config)# aaa new-model
```

2) 然后配置 tacacs+ server 信息：

```
Ruijie(config)# tacacs-server host 192.168.12.219
```

```
Ruijie(config)# tacacs-server key aaa
```

3) 然后配置使用 tacacs+的认证方法：

```
Ruijie(config)# aaa authentication login test group tacacs+
```

4) 在接口上应用配置认证方法:

```
Ruijie(config)# line vty 0 4
Ruijie (config-line)# login authentication test
```

5) 通过以上配置就实现了配置 login 的 tacacs+认证，配置显示如下。

```
Ruijie#show running-config
!
aaa new-model
!
aaa authentication login test group tacacs+
!
tacacs-server host 192.168.12.219
tacacs-server key aaa
!
line con 0
line vty 0 4
login authentication test
!
```

3.4.2 Enable认证使用TACACS+的配置示例：

1) 首先配置启用 aaa：

```
Ruijie# configure terminal
Ruijie(config)# aaa new-model
```

2) 然后配置 tacacs+ server 信息：

```
Ruijie(config)# tacacs-server host 192.168.12.219
Ruijie(config)# tacacs-server host 192.168.12.218
Ruijie(config)# tacacs-server host 192.168.12.217
Ruijie(config)# tacacs-server key aaa
```

3) 配置 tacacs+ server group 使用服务器列表中一部分服务器：

```
Ruijie(config)#aaa group server tacacs+ tacgroup1
Ruijie(config-gs-tacacs)#server 192.168.12.219
Ruijie(config-gs-tacacs)#server 192.168.12.218
```

4) 然后配置使用 tacgroup1 的认证方法：

```
Ruijie(config)# aaa authentication enable default group tacgroup1
```

5) 通过以上配置就实现了配置 enable 的部分 tacacs+服务器认证，配置显示如下。

```
Ruijie#show running-config
!
aaa new-model
!
!
aaa group server tacacs+ tacgroup1
server 192.168.12.219
server 192.168.12.218
!
aaa authentication enable default group tacgroup1
!
!
tacacs-server host 192.168.12.219
tacacs-server host 192.168.12.218
tacacs-server host 192.168.12.217
tacacs-server key aaa
!
line con 0
line vty 0 4
!
```

3.4.3 登陆授权使用TACACS+的配置示例：

1) 首先配置启用 aaa：

```
Ruijie# configure terminal
Ruijie(config)# aaa new-model
```

2) 然后配置 tacacs+ server 信息：

```
Ruijie(config)# tacacs-server host 192.168.12.219
Ruijie(config)# tacacs-server key aaa
```

3) 然后配置使用 tacacs+的授权方法：

```
Ruijie(config)# aaa authorization exec test group tacacs+
```

4) 在接口上应用配置授权:

```
Ruijie(config)# line vty 0 4
Ruijie (config-line)#authorization exec test
```

5) 通过以上配置就实现了配置登陆授权使用 tacacs+，配置显示如下。

```
Ruijie#show running-config
!
```

```
aaa new-model
!
!
aaa authorization exec test group tacacs+
!
tacacs-server host 192.168.12.219
tacacs-server key aaa
!
line con 0
line vty 0 4
authorization exec test
!
```

3.4.4 15 级Commands审计使用TACACS+的配置示例：

1) 首先配置启用 aaa：

```
Ruijie# configure terminal
Ruijie(config)# aaa new-model
```

2) 然后配置 tacacs+ server 信息：

```
Ruijie(config)# tacacs-server host 192.168.12.219
Ruijie(config)# tacacs-server key aaa
```

3) 然后配置使用 tacacs+的命令审计方法：

```
Ruijie(config)# aaa accounting commands 15 test start-stop group tacacs+
```

4) 在接口上应用配置授权:

```
Ruijie(config)# line vty 0 4
Ruijie(config-line)# accounting commands 15 test
```

5) 通过以上配置就实现了配置 enable 的部分 tacacs+服务器认证，配置显示如下。

```
Ruijie#show running-config
!
aaa new-model
!
!
aaa accounting commands 15 test start-stop group tacacs+
!
!
tacacs-server host 192.168.12.219
tacacs-server key aaa
!
line con 0
line vty 0 4
```

```
accounting commands 15 test
!
```

4 802.1x

4.1 概述

IEEE 802 LAN 中，用户只要能接到网络设备上，不需要经过认证和授权即可直接使用。这样，一个未经授权的用户，他可以没有任何阻碍地通过连接到局域网的设备进入网络。随着局域网技术的广泛应用，特别是在运营网络的出现，对网络的安全认证的需求已经提到了议事日程上。如何在以太网技术简单、廉价的基础上，提供用户对网络或设备访问合法性认证，已经成为业界关注的焦点。IEEE 802.1x 协议正是在这样的背景下提出的。

IEEE802.1x（Port-Based Network Access Control）是一个基于端口的网络存取控制标准，为 LAN 提供点对点式的安全接入。这是 IEEE 标准委员会针对以太网的安全缺陷而专门制定的标准，能够在利用 IEEE 802 LAN 优势的基础上，提供一种对连接到局域网设备的用户进行认证的手段。

IEEE 802.1x 标准定义了一种基于“客户端——服务器”（Client-Server）模式实现了限制未认证用户对网络的访问。客户端要访问网络必须先通过服务器的认证。

在客户端通过认证之前，只有 EAPOL 报文（Extensible Authentication Protocol over LAN）可以在网络上通行。在认证成功之后，正常的数据流便可在网络上通行。

应用 802.1x 我司的设备提供了 Authentication，Authorization，and Accounting 三种安全功能，简称 AAA。

- Authentication： 认证，用于判定用户是否可以获得访问权，限制非法用户；
- Authorization： 授权，授权用户可以使用哪些服务，控制合法用户的权限；
- Accounting： 计账，记录用户使用网络资源的情况，为收费提供依据。

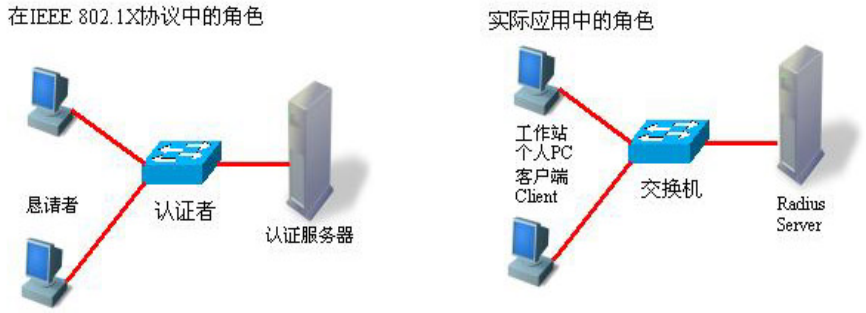
我们将从以下几个方面阐述 802.1x：

- 设备的角色
- 认证的发起及认证过程中的报文交互
- 已认证用户及未认证用户的状态
- 典型应用的拓扑结构

4.1.1 设备的角色

IEEE802.1x 标准认证体系由恳请者、认证者、认证服务器三个角色构成，在实际应用中，三者分别对应为：工作站（Client）、设备(network access server，NAS)、Radius-Server。

图 4-1



■ 恳请者

恳请者是最终用户所扮演的角色，一般是个人 PC。它请求对网络服务的访问，并对认证者的请求报文进行应答。恳请者必须运行符合 IEEE 802.1x 客户端标准的软件，目前最典型的就是 WindowsXP 操作系统自带的 IEEE802.1x 客户端支持，另外，我司也已推出符合该客户端标准的 STAR Supplicant 软件。

■ 认证者

认证者一般为交换机等接入设备。该设备的职责是根据客户端当前的认证状态控制其与网络的连接状态。在客户端与服务器之间，该设备扮演着中介者的角色：从客户端要求用户名，核实从服务器端的认证信息，并且转发给客户端。因此，设备除了扮演 IEEE802.1x 的认证者的角色，还扮演 RADIUS Client 角色，因此我们把设备称作 network access server(NAS)，它要负责把从客户端收到的回应封装到 RADIUS 格式的报文并转发给 RADIUS Server，同时它要把从 RADIUS Server 收到的信息解释出来并转发给客户端。

扮演认证者角色的设备有两种类型的端口：受控端口（controlled Port）和非受控端口（uncontrolled Port）。连接在受控端口的用户只有通过认证才能访问网络资源；而连接在非受控端口的用户无须经过认证便可以直接访问网络资源。我们把用户连接在受控端口上，便可以实现对用户的控制；非受控端口主要是用来连接认证服务器，以便保证服务器与设备的正常通讯。

■ 认证服务器

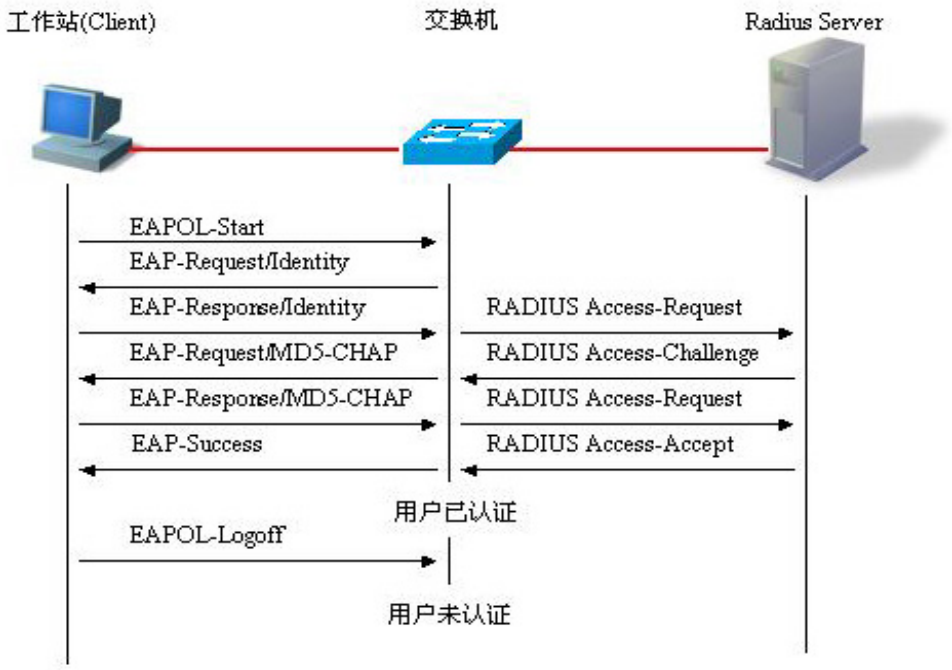
认证服务器通常为 RADIUS 服务器，认证过程中与认证者配合，为用户提供认证服务。认证服务器保存了用户名及密码，以及相应的授权信息，一台服务器可以对多台认证者提供认证服务，这样就可以实现对用户的集中管理。认证服务器还负责管理从认证者发来的记帐数据。锐捷网络科技公司实现 802.1x 的设备完全兼容标准的 Radius Server，如 MicroSoft win2000 Server 自带的 Radius Server 及 Linux 下的 Free Radius Server。

4.1.2 认证的发起及认证过程中的报文交互

恳请者和认证者之间通过 EAPOL 协议交换信息，而认证者和认证服务器通过 RADIUS 协议交换信息，通过这种转换完成认证过程。EAPOL 协议封装于 MAC 层之上，类型号为 0x888E。同时，标准为该协议申请了一个组播 MAC 地址 01-80-C2-00-00-03，用于初始认证过程中的报文传递。

下图是一次典型的认证过程中，三个角色设备的报文交互过程：

图 4-2



该过程是一个典型的由用户发起的认证过程（在一些特殊的情形下，设备也可能主动发出认证请求，过程与该图一致，只是少了用户主动发出请求这一步）。

4.1.3 已认证用户及未认证用户的状态

802.1x 中根据端口的认证状态来决定该端口上的用户是否允许访问网络，由于我们对 802.1X 进行扩展，是基于用户的，所以，我们是根据一个端口下的用户的认证状态来决定该用户是否允许访问网络资源。一个非受控端口下的所有用户均可使用网络资源，而一个受控端口下的用户只有处于已认证状态（Authorized）才能访问网络资源。一个用户刚发起认证时，状态处于未认证状态（unauthorized），这时它不能访问网络，在认证通过后，该用户的状态会变为已认证状态（authorized），此时该用户便可以使用网络资源。

如果工作站不支持 802.1x，而该机器连接在受控端口下，当设备请求该用户的用户名时，由于工作站不支持导致没对该请求做出响应。这就意味着该用户仍然处于未认证状态（unauthorized），不能访问网络资源。

相反地，如果工作站支持 802.1x，而所连的设备不支持 802.1x。用户发出的 EAPOL-START 帧无人响应，用户在发送一定数目的 EAPOL-START 帧仍未收到回应的情形下，将认为自己所连的端口是非受控端口，而直接使用网络资源。

在支持 802.1x 的设备下，所有端口的默认设置是非受控端口，我们可以把一个端口设置成受控端口，从而要求这个端口下的所有用户都要进行认证。

当用户通过了认证（设备收到了从 RADIUS Server 服务器发来的成功报文），该用户便转变成已认证状态(authorized)，该用户可以自由使用网络资源。如果用户认证失败以至仍然处于未认证状态，可以重新发起认证。如果设备与 RADIUS server 之间的通讯有故障，那么该用户仍然处于未认证状态（unauthorized），网络对该用户来说仍然是不可使用的。

当用户发出 EAPOL-LOGOFF 报文后，该用户的状态由已认证(authorized)转向未认证状态(unauthorized)。

当设备的某个端口变为 LINK-DOWN 状态，该端口上的所有用户均变为未认证(unauthorized)状态。

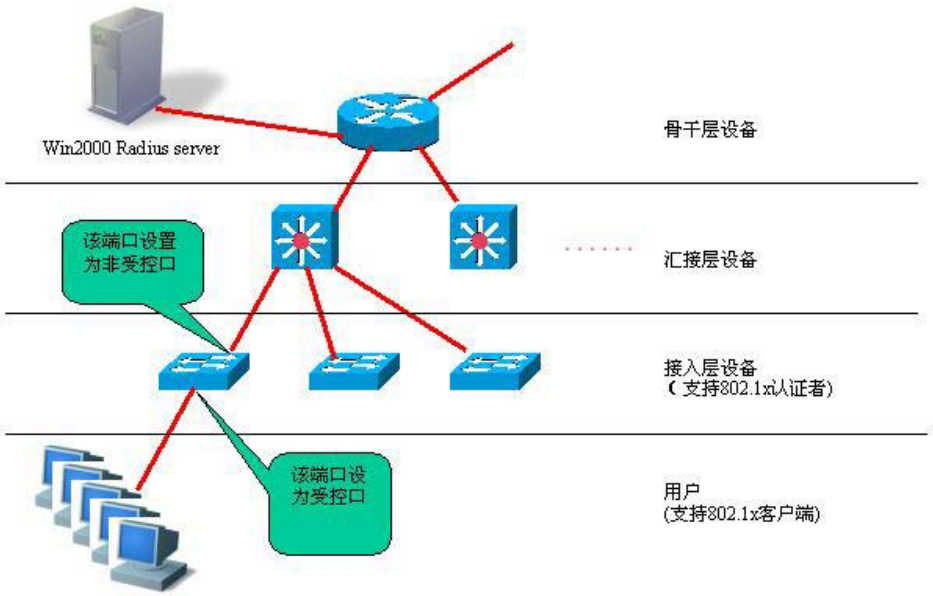
当设备重新启动，该设备上的所有用户均变为未认证状态(unauthorized)。

如果您要强制一个用户通过认证，可以通过添加静态 MAC 地址来实现。

4.1.4 典型应用的拓扑结构

方案一：带 802.1x 的设备作为接入层设备

图 4-3



该方案的说明

该方案的要求：

- 用户支持 802.1x，即要装有 802.1x 的客户端软件（windowXp 自带，Star-supplicant 或其他符合 IEEE802.1x 标准的客户端软件）；
- 接入层设备支持 IEEE 802.1x；
- 有一台（或多台）支持标准 RADIUS 的服务器作为认证服务器。

该方案的配置要点：

- 与 Radius Server 相连的口及上联口，配置成非受控口，以便设备能正常地与服务器进行通讯，以及使已认证用户能通过上联口访问网络资源；
- 与用户连接的端口要设置为受控口，以实现对接入用户的控制，用户必须通过认证才能访问网络资源。

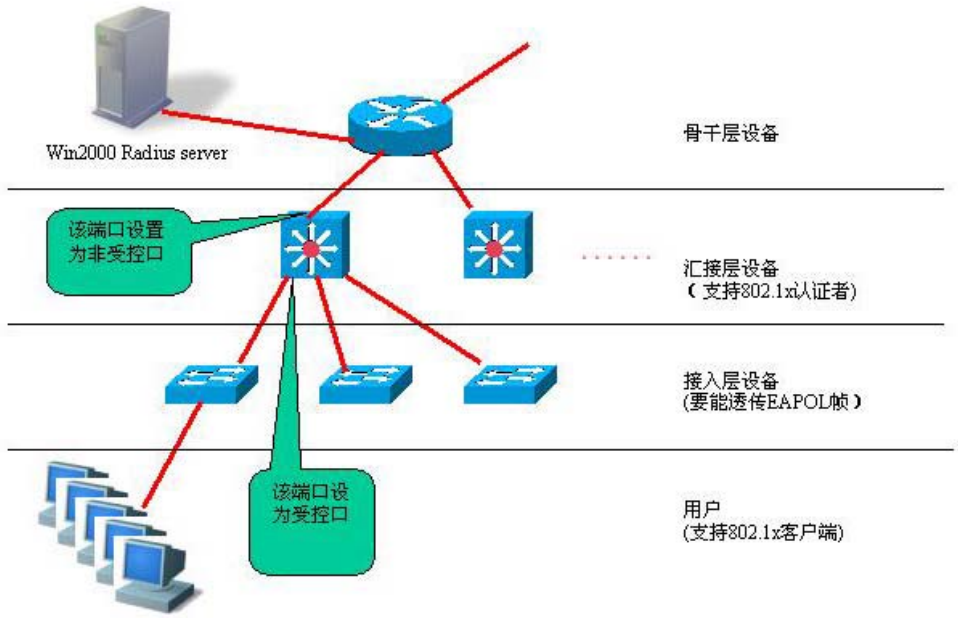
该方案的特点：

- 每台支持 802.1x 的设备所负责的客户端少，认证速度快。各台设备之间相互独立，设备的重启等操作不会影响到其它设备所连接的用户；

- 用户的管理集中于 Radius Server 上，管理员不必考虑用户连接在哪台设备上，便于管理员的管理；
- 管理员可以通过网络管理接入层的设备。

方案二：带 802.1x 的设备作为汇接层设备

图 4-4



该方案的说明

该方案的要求：

- 用户支持 802.1x，即要装有 802.1x 的客户端软件（windowXp 自带，Star-supplicant 或其他符合 IEEE802.1x 标准的客户端软件）；
- 接入层设备支持要能透传 IEEE 802.1x 帧(EAPOL)；
- 汇接层设备支持 802.1x（扮演认证者角色）；
- 有一台（或多台）支持标准 RADIUS 的服务器作为认证服务器。

该方案的配置要点：

- 与 Radius Server 相连的口及上联口，配置成非受控口，以便设备能正常地与服务器进行通讯，以及使已认证用户能通过上联口访问网络资源；
- 与接入层设备连接的端口要设置为受控口，以实现对接入用户的控制，用户必须通过认证才能访问网络资源。

该方案的特点：

- 由于是汇接层设备，网络规模大，下接用户数多，对设备的要求高，若该层设备发生故障，将导致大量用户不能正常访问网络；
- 用户的管理集中于 Radius Server 上，管理员无需考虑用户连接在哪台设备上，便于管理员的管理；

- 接入层设备可以使用较廉价的非网管型设备（只要支持 EAPOL 帧透传）；
- 管理员不能通过网络直接管理接入层设备。

4.2 配置 802.1X

4.2.1 802.1x 的默认配置

下表列出 802.1x 的一些缺省值

功能特性	缺省值
认证 Authentication	关闭 DISABLE
记帐 Accounting	关闭 DISABLE
认证服务器(Radius Server) *服务器 IP 地址(ServerIp) *认证 UDP 端口 *密码(Key)	*无缺省值 *1812 *无缺省值
记帐服务器(Accounting Server) *记帐服务器 IP 地址 *记帐 UDP 端口	*无缺省值 *1813
所有端口的类型	非受控端口（所有端口均无须认证便可直接通讯）
定时重认证 re-authentication	关闭
定时重认证周期 reauth_period	3600 秒
认证失败后允许再次认证的间隔 quiet-period	10 秒
重传时间间隔 tx-period	3 秒
最大重传次数 max-req	3 次
客户端超时时间 supp-timeout	3 秒，在该段时间内没有收到客户端的响应便认为这次通讯失败
服务器超时时间 server-timeout	5 秒，在该段时间内没有收到服务器的回应，便认为这次通讯失败
某端口下可认证主机列表	无缺省值

4.2.2 802.1X 的配置注意事项

- 只有支持 802.1x 的产品，才能进行以下设置。
- 802.1x 既可以在二层下又可以在三层下的设备运行。
- 要先设置认证服务器 IP 地址，radius－server 认证方式才可以正常工作。
- 交换机只要有一个端口打开了 1x 功能，所有的端口都会将 1x 协议报文送到 cpu。
- 如果端口 DOT1X 开启并且认证的用户数大于端口安全的最大用户数，此时无法开启端口安全。
- 端口安全和 DOT1X 同时开启时，如果安全地址老化，则 DOT1X 对应的用户必须重新认证才可以继续通信。

- 静态端口安全地址不需要认证即可上网，如果存在授权，则必须同时符合授权绑定才可以上网。
- 基于端口可迁移认证模式和端口安全共用时，已经学习到的地址同时成为安全地址，不能再迁移。
- 基于端口可迁移认证模式和端口安全共用时，如果认证地址被端口安全老化则端口必须重新认证才可以通信。
- 基于端口可迁移认证模式认证通过后，开启端口安全，则端口必须重新认证才可以通信。
- 存在 IP+MAC 绑定时，不能进行基于端口和基于用户认证模式的切换。

4.2.3 配置设备与RADIUS SERVER 之间的通讯

Radius Server 维护了所有用户的信息:用户名、密码、该用户的授权信息以及该用户的记帐信息。所有的用户集中于 Radius Server 管理，而不必分散于每台设备，便于管理员对用户的集中管理。

设备要能正常地与 RADIUS SERVER 通讯，必须进行如下设置：

Radius Server 端：要注册一个 Radius Client。注册时要告知 Radius Server 设备的 IP、认证的 UDP 端口（若记帐还要添记帐的 UDP 端口）、设备与 Radius Server 通讯的约定密码，还要选上对该 Client 支持 EAP 扩展认证方式）。对于如何在 Radius Server 上注册一个 Radius Client，不同软件的设置方式不同，请查阅相关的文档。

设备端：为了让设备能与 Server 进行通讯，设备端要做如下的设置：设置 Radius Server 的 IP 地址，认证（记帐）的 UDP 端口，与服务器通讯的约定密码。

在特权模式下，按如下步骤设置设备与 Radius Server 之间的通讯：

命令	作用
Ruijie(config)**#aaa new-model**	打开 AAA 开关
Ruijie(config)**#radius-server host** *ip-address* [**auth-port** *port*] [**acct-port** *port*]	配置 RADIUS 服务器
Ruijie(config)**#radius-server key** *string*	配置 RADIUS Key
Ruijie**#show radius server**	显示 RADIUS 服务器

使用 **no radius-server host** *ip-address* **auth-port** 命令将 Radius Server 认证 UDP 端口恢复为缺省值。使用 **no radius-server key** 命令删除 Radius Server 认证密码。以下例子是设置 server ip 为 192.168.4.12、认证 Udp 端口为 600、以明文方式设置约定密码：

```
Ruijie# configure terminal
Ruijie(config)# radius-server host 192.168.4.12
Ruijie(config)# radius-server host 192.168.4.12 auth-port 600
Ruijie(config)# radius-server key MsdadShaAdasdj878dajL6g6ga
Ruijie(config)# end
```

- 官方约定的认证的 UDP 端口为 1812
- 官方约定的记帐的 UDP 端口为 1813
- 设备与 Radius Server 约定的密码的长度建议不少于 16 个字符
- 设备与 Radius Server 连接的端口要设置成非受控口

4.2.4 设置 802.1X 认证的开关

当打开 802.1x 认证时，设备会主动要求受控端口上的主机进行认证，未通过认证的主机不允许访问网络。

在特权模式下，按如下步骤打开 1x 认证：

命令	作用
Ruijie(config)**#aaa new-model**	打开 AAA 开关
Ruijie(config)**#radius-server host** *ip-address* [**auth-port** *port*] [**acct-port** *port*]	配置 RADIUS 服务器
Ruijie(config)**#radius-server key** *string*	配置 RADIUS Key
Ruijie(config)**#aaa authentication dot1x** *auth* **group radius**	配置 dot1x 认证方法列表
Ruijie(config)**#dot1x authentication** *auth*	dot1x 应用认证方法列表
Ruijie**#show running-config**	显示配置

在基于域名的 AAA 服务开关打开情况下，也即配置命令 **aaa domain enable** 时，**dot1x authentication** 命令选择的认证方法列表将不会被使用，而使用用户所在的域配置的认证方法列表。具体配置参考“配置基于域名的 AAA 服务”。

以下例子是打开 802.1x 认证：

```
Ruijie# configure terminal
Ruijie(config)# aaa new-model
Ruijie(config)# radius-server host 192.168.217.64
Ruijie(config)# radius-server key starnet
Ruijie(config)# aaa authentication dot1x authen group radius
Ruijie(config)# dot1x authentication authen
Ruijie(config)# end
Ruijie# show running-config
!
aaa new-model
!
aaa authentication dot1x authen group radius
!
username ruijie password 0 starnet
!
radius-server host 192.168.217.64
radius-server key 7 072d172e071c2211
!
!
!
dot1x authentication authen
!
interface VLAN 1
 ip address 192.168.217.222 255.255.255.0
```

```
 no shutdown
!
!
line con 0
line vty 0 4
!
end
```

802.1x 在应用 RADIUS 认证方法时，先配置 Radius Server 的 IP 地址，并确保设备与 Radius Server 之间的通讯正常。若没有 Radius Server 的配合，设备无法完成认证功能。如何设置 Radius Server 与设备之间的通讯请见上一章节。

4.2.5 打开/关闭一个端口的认证

在 802.1x 打开的情形下，打开一个端口的认证，则该端口成为受控口，连接在该端口下的用户要通过认证才能访问网络，然而，在非受控端口下的用户可以直接访问网络。

在特权模式下，按如下步骤设置一个端口的认证状态。

命令	作用
Ruijie(config)**#interface** *interface*	进入接口设置模式,指定要配置的接口
Ruijie(config-if-*type ID*)**#dot1x port-control auto**	设置该接口为受控接口（打开接口认证功能）。使用该命令的 no 选项关闭该接口的认证功能
Ruijie**#show dot1x port-control**	查看 802.1x 接口认证配置

使用该命令的 **no dot1x port-control** 命令关闭接口的认证功能。以下例子是设置以太网接口 1/1 为受倥接口：

```
Ruijie# configure terminal
Ruijie(config)# interface f 1/1
Ruijie(config-if)# dot1x port-control auto
Ruijie(config)# end
```

当接口被设置为受控口的时候，只允许 EAP 报文过，往 CPU 的报文也在受控范围内。

4.2.6 打开定时重认证

802.1x 能定时主动要求用户重新认证，这样可以防止已通过认证的用户不会被其他用户冒用，还可以检测用户是否断线，使记费更准确。除了可以设定重认证的开关，我们还可以定义重认证的间隔。默认的重认证间隔是 3600 秒。在根据时常进行记费的场合下，要根据具体的网络规模确定重认证间隔，使之既有足够时间完成一次认证又尽可能精确。

在特权模式下，按如下步骤打开/关闭重认证状态，并且设置重认证时间间隔。

命令	作用
Ruijie(config)**#dot1x re-authentication**	打开定时重认证功能
Ruijie(config)**#dot1x timeout re-authperiod** *seconds*	设置重认证时间间隔
Ruijie**#show dot1x**	显示 dot1x 配置

使用 **no dot1x re-authentication** 命令关闭定时重认证功能，使用 **no dot1x timeout re-authperiod** 命令将重认证时间间隔恢复为缺省值。

以下例子是打开定时重认证功能，并设置重认证时间间隔为 1000 秒：

```
Ruijie# configure terminal
Ruijie(config)# dot1x re-authentication
Ruijie(config)# dot1x timeout re-authperiod 1000
Ruijie(config)# end
Ruijie# show dot1x
802.1X Status:        Disabled
Authentication Mode:  EAP-MD5
Authed User Number:   0
Re-authen Enabled:    Enabled
Re-authen Period:     1000 sec
Quiet Timer Period:   10 sec
Tx Timer Period:      3 sec
Supplicant Timeout:   3 sec
Server Timeout:       5 sec
Re-authen Max:        3 times
Maximum Request:      3 times
Filter Non-RG Supp:   Disabled
Client Oline Probe:   Disabled
Eapol Tag Enable:     Disabled
Authorization Mode:   Disabled
```

若打开重认证，请注意重认证间隔的合理性。要根据具体的网络规模而设置。

4.2.7 改变QUIET 时间

当用户认证失败时，设备将等待一段时间后，才允许用户再次认证。Quiet Period 的时间长度便是允许再认证的时间间隔。该值的作用是避免设备受恶意攻击。Quiet Period 的默认间隔为 10 秒，我们可以通过设定较短的 Quiet Period 使用户可以更快地进行再认证。

在特权模式下，按如下步骤设置 Quiet Period 的值。

命令	作用
Ruijie(config)**#dot1x timeout quiet-period** *seconds*	设置 Quiet Period 值
Ruijie**#show dot1x**	显示 dot1x 配置

使用 **no dot1x timeout quiet-period** 命令将 Quiet Period 恢复为缺省值。以下例子是设置 QuietPeriod 值 500 秒：

```
Ruijie# configure terminal
Ruijie (config)# dot1x timeout quiet-period 500
Ruijie(config)# end
```

4.2.8 设置报文重传间隔

设备发 EAP-request/identity 之后，若在一定的时间内没有收到用户的回应，设备将重传这个报文。该值的默认值为 3 秒，要根据具体的网络规模进行调整。

在特权模式下，按如下步骤设置报文重传间隔。

命令	作用
Ruijie(config)**#dot1x timeout tx-period** *seconds*	设置报文重传间隔
Ruijie**#show dot1x**	显示 dot1x 配置

使用 **no dot1x timeout tx-period** 命令将报文重传间隔恢复为缺省值。以下例子是设置报文重传间隔为 100 秒：

```
Ruijie# configure terminal
Ruijie(config)# dot1x timeout tx-period 100
Ruijie(config)# end
```

4.2.9 设置最大请求次数

设备在转发 Radius Server 发出的认证请求给客户端后，若在 **supp-timeout** 时间内没收到客户端的回应，将重传该报文。最大请求次数指的是设备重传请求的最大数，超过该次数设备将认为本次认证失败。默认的重传次数为 3 次，我们要根据具体的网络环境进行调整。

在特权模式下，按如下步骤设置报文重传次数。

命令	作用
Ruijie(config)**#dot1x max-req** *count*	设置报文重传次数
Ruijie**#show dot1x**	显示 dot1x 配置

使用 no dot1x max-req 命令将报文重传次数恢复为缺省值。以下例子是设置报文重传次数为 5 次：

```
Ruijie# configure terminal
Ruijie(config)# dot1x max-req 5
Ruijie(config)# end
```

4.2.10 设置最大重认证次数

当用户认证失败后，设备会尝试再次与用户进行认证。在认证次数超过最大重认证次数之后，设备就认为这个用户已经断线，结束认证过程。系统默认的次数是 3 次，我们可以重新设置这个值。

在特权模式下，按如下步骤设置最大重认证次数：

命令	作用
Ruijie(config)**#dot1x reauth-max** *count*	设置最大重认证次数
Ruijie**#show dot1x**	显示 dot1x 配置

使用 **no dot1x reauth-max** 命令将最大重认证次数恢复为缺省值。以下例子是设置最大重认证次数为 3 次：

```
Ruijie# configure terminal
```

```
Ruijie(config)# dot1x reauth-max 3
Ruijie(config)# end
```

4.2.11 设置Server-timeout

该值指的是 Radius Server 的最大响应时间，若在该时间内，设备没有收到 Radius Server 的响应，将认为本次认证失败。

在特权模式下，按如下步骤设置 Server-timeout、恢复为默认值。

命令	作用
Ruijie(config)**#dot1x timeout server-timeout** *seconds*	设置服务器最大响应时间，使用该命令的 no 选项将其恢复为缺省值
Ruijie**#show dot1x**	显示 dot1x 配置

4.2.12 配置设备主动发起 802.1x 认证

802.1x 是基于端口的安全访问认证，用户要访问网络，就必须先进行认证，绝大多数情况下，认证是由用户端通过发出 EAPOL-START 报文来发起的。关于认证过程中报文的交互，请参考“认证的发起及认证过程中的报文交互”。

但是在某些特殊情况下，认证却需要由设备来发起。比如设备复位、认证端口状态由 linkdown 变为 linkup，这时候为了保证已认证的用户能够继续使用网络，就需要设备主动发起认证。另外，如果用户使用了一些不会主动发起认证请求的 802.1x 客户端软件来进行认证（比如使用 WindowsXP 自带的 802.1x 客户端软件），这时候就需要设备能够主动发起认证，设备通过发出 EAP-request/identity 组播报文来强制要求认证端口下的所有用户进行认证。

以下将介绍如何配置设备主动发起 802.1x 认证，以及在不同的应用环境下用户应该如何合理地进行配置。

打开/关闭设备主动发起认证的开关

当该功能关闭时，设备只在复位和认证端口状态改变的时候发起一次认证请求，这是为了保证在线用户能够继续认证使用网络，其它任何时候设备都不会主动发起认证请求。当该功能打开后， 用户可以配置主动发起认证请求的次数、发送认证请求的间隔、用户认证通过后是否要停止发送请求等附属功能。

进入特权模式，按以下步骤打开主动认证功能：

命令	作用
Ruijie(config)**#dot1x auto-req**	打开主动认证功能，缺省情况下开启
Ruijie**#show dot1x**	显示 dot1x 配置

使用该命令的 **no** 选项可以关闭该功能，只有该功能打开的情况下，后面的设置才能起作用，设置设备主动发送认证请求的次数，用户可以设置设备主动发起认证请求的次数，这个值可根据实际的网络环境设定。

进入特权模式，按以下步骤设置发送报文的次数：

命令	作用
Ruijie(config)**#dot1x auto-req packet-num** *num*	设备主动发送 num 个 802.1x 认证请求报文,如果 num 为 0，则设备将持续地发送该报文。缺省值是 0（无限个）
Ruijie**#show dot1x auto-req**	显示配置

使用该命令的 **no** 选项恢复为默认值，下面配置报文发送间隔

进入特权模式，按以下步骤设置主动发送报文的间隔：

命令	作用
Ruijie(config)**#dot1x auto-req req-interval** *interval*	设置报文发送间隔
Ruijie**#show dot1x auto-req**	显示配置

使用该命令的 **no** 选项恢复为默认值，由于发出认证请求组播报文会导致认证口下的所有用户进行重认证，所以发送间隔不要太小，否则会影响认证效率。

设置在发现用户认证通过后是否停止发送请求报文，在某些应用需求下(比如一个端口下面只接一个用户)，我们可以指定设备在发现用户认证通过后，停止向对应端口发送认证请求，如果用户下线，则继续发送。

进入特权模式，按以下步骤设置：

命令	作用
Ruijie(config)**#dot1x auto-req user-detect**	端口有认证用户停止发送报文。该功能缺省打开
Ruijie**#show dot1x auto-req**	显示配置

使用该命令的 **no** 选项关闭该功能，用户在设置该功能时要仔细考虑当前的网络应用环境。

应用示例以上三个命令为用户提供了灵活的应用策略，用户可以根据具体的网络应用环境来选择合适的配置命令。为了方便用户进行配置，我们建立了如下的应用配置表，用户可参考该表来进行配置：

	方案 1	方案 2	方案 3
用户环境	一端口对任意用户	一端口对单用户	一端口对多用户
是否要求使用我司的 supplicant 作为认证客户端	是	否	否
建议采用的配置命令	不必打开 **dot1x auto-req** 功能	**dot1x auto-req** **dot1x auto-req packet-num** *num* **dot1x auto-req req-interval** *interval* **dot1x auto-req user-detect**	**dot1x auto-req** **dot1x auto-req packet-num** *0* **dot1x auto-req req-interval** *interval* **no dot1x auto-req user-detect**

4.2.13 配置 802.1x 记帐

锐捷网络公司的 802.1x 实现了记帐功能。该记帐是基于时长的，也就是说 802.1x 记录了用户第一次认证通过到用户主动退出或设备检测到用户中断的时间长度。

在用户第一次认证通过之后，设备会向服务器发一个记帐开始请求，当用户主动离线或设备检测到用户已离线或用户的物理连接已中断，设备将向服务器发一个记帐结束请求。服务器组将会把这些信息记录在服务器组的数据库上。网管便可以根据这些信息提供记帐的依据。

锐捷网络公司的 802.1x 十分重视记帐的可靠性，为了避免记帐服务器的意外情况，特别支持记帐备份服务器。当一个服务器由于各种原因而不能提供记帐服务，设备将自动把记帐信息转发给另一台备份服务器，这大大提高了记帐可靠性。

在用户主动退出的情形下，记帐的时长是精确的；在用户意外中断的情形下，用户记帐的精度以重认证的间隔为准（设备通过重认证检测一个用户是否意外中断）。

要打开设备的记帐工作需对设备做如下的设置：

- 在 Radius Server 注册这台设备为 Radius Client，如认证时的操作
- 设置记帐服务器的 IP 地址
- 设置记帐的 UDP 端口
- 在 802.1x 打开的前提下，打开记帐服务

在特权模式下，按如下步骤设置记帐服务：

命令	作用
Ruijie(config)**#aaa new-model**	打开 AAA 功能
Ruijie(config)**#aaa group server radius** *gs*	配置记帐服务器组
Ruijie(config-gs-radius)**#server** *address* **acct-port** *port-id*	向服务器组添加服务器
Ruijie(config-gs-radius)**# aaa accounting network** *acct* **start-stop group** *gs*	配置记账方法列表
Ruijie(config-gs-radius)**# dot1x accounting** *acct*	为 802.1X 应用记账方法列表
Ruijie**#show running-config**	显示配置

使用 **no aaa accounting network** 命令的将删除记账方法列表。使用 **no dot1x accounting** 命令使用默认的 dot1x 记帐方法。以下例子是设置记帐服务器的 IP 地址为 192.168.4.12、设置备份记帐服务器的 IP 地址为 192.168.4.13、设置记帐服务器的 UDP 端口为 1200、应用 802.1x 记帐功能：

```
Ruijie# configure terminal
Ruijie(config)# aaa new-model
Ruijie(config)# aaa group server radius acct-use
Ruijie(config-gs-radius)# server 192.168.4.12 acct-port 1200
Ruijie(config-gs-radius)# server 192.168.4.13 acct-port 1200
Ruijie(config-gs-radius)# exit
Ruijie(config)# aaa accounting network acct-list start-stop group acct-use
Ruijie(config)# dot1x accounting acct-list
Ruijie(config)# end
Ruijie# write memory
Ruijie# show running-config
```

- 与 Radius Server 的约定记帐密码与认证相同；
- 必须在 AAA 打开的前提下才能打开记帐；
- 802.1X 认证通过后才能进行记账；
- 802.1x 的记帐功能在默认的情形下是关闭的；
- 记帐的数据库格式请见相关的 Radius Server 文档；

在基于域名的 AAA 服务开关打开情况下，也即配置命令 aaa domain enable 时，dot1x accounting 命令选择的记帐方法列表将不会被使用，而使用用户所在的域配置记账方法列表。具体配置参考“配置基于域名的 AAA 服务”。

同时我们支持计费更新功能 ，在 NAS 设备上设定了计费更新包的周期后，NAS 设备即定时定期的向 Radius Server 发送计费更新包，Radius Server 上可以定义，如果多少次（几个周期）没有收到 NAS 设备发过来的某用户的计费更新包时，即认为该 NAS 或该用户不在线，Radius Server 即可停止相关用户的计费，从在线用户表中将其删除等等操作。

在特权模式下，按如下步骤设置记帐更新功能服务：

命令	作用
Ruijie(config)**#aaa new-model**	打开 AAA 功能
Ruijie(config)**#aaa accounting update**	设置记帐计费更新功能
Ruijie**#show running-config**	显示配置

用 **no aaa accounting update** 可以关闭记账更新功能服务

```
Ruijie# configure terminal
Ruijie(config)# aaa accounting update
Ruijie(config)# end
Ruijie# write memory
Ruijie# show running-config
```

以下章节为锐捷网络产品特有的功能：

为了方便宽带运营商及其他特殊场合的用途，锐捷对 802.1x 的功能在标准的基础上进行了扩展（该扩展是完全基于标准之上，没有任何的与 IEEE 802.1x 不兼容）。

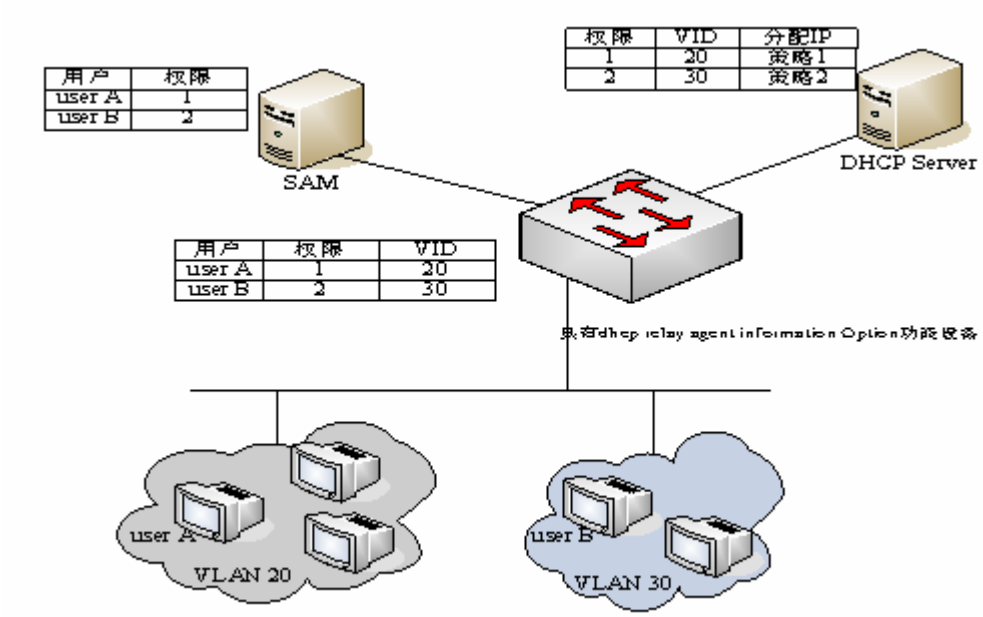
4.2.14 配置IP 授权模式

锐捷网络实现的 802.1x，可以强制要求已认证的用户使用固定的 IP。管理员通过配置 IP 授权模式来限定用户获得 IP 地址的方式。IP 授权模式有四种：DISABLE 模式、DHCP SERVER 模式、RADIUS SERVER 模式 、SUPPLICANT 模式。下面分别介绍这四种工作模式的特性：

DISABLE 模式（默认）：在该模式下，设备不对用户的 IP 做限制，用户只需认证通过便可以使用网络。

DHCP SERVER 模式：用户的 IP 通过指定的 DHCP SERVER 获得，只有指定的 DHCP SERVER 分配的 IP 才是合法的 IP，对于 DHCP 模式可以使用 DHCP relay option82 实现 802.1X 的更为灵活的 IP 分配策略。典型的方案图如下：

图 4-5



各用户通过 DHCP Client 发起 IP 请求，具有 dhcp relay option82 的网络设备融合 SAM 服务器上的用户权限，构造 option82 字段封装于 DHCP 请求报文，该 option82 字段由“vid + 权限”组成。DHCP Server 由 option82 字段选择不同的分配策略。

此种模式下需要对 DHCP Relay 及相应的 option82 进行配置，如打开 DHCP relay 功能，并选择 option82 策略，相应的配置见 DHCP Relay 配置指南和命令参考。

RADIUS SERVER 模式：用户的 IP 通过 RADIUS SERVER 指定。用户只能用 RADIUS SERVER 指定的 IP 访问网络。

SUPPLICANT 模式 ：所绑定用户的 IP 为 SUPPLICANT 认证时 PC 的 IP。认证后，用户只能用该 IP 访问网络，不可随意更改 IP。

四种模式下的应用模型：

- DISABLE 模式：适合不对用户限定 IP 的场合。用户只需通过认证便可以访问网络。
- DHCP SERVER 模式：用户 PC 通过 DHCP 获得 IP 地址，管理员通过配置设备的 DHCP RELAY 来限定用户访问的 DHCP SERVER，这样，只有指定的 DHCP SERVER 分配的 IP 才是合法的。
- RADIUS SERVER 模式：用户 PC 使用固定的 IP，RADIUS SERVER 配置了<用户—IP>的对应关系，并通过 RADIUS 的 Framed-IP-Address 属性告知设备，用户只能用该 IP 才能访问网络。
- SUPPLICANT 模式：用户 PC 使用固定的 IP，SUPPLICANT 将该信息告知设备，用户只能用认证时的 IP 才能访问网络。

用户切换模式时会导致已经认证的用户全部下线，所以建议在用户使用前就配置好认证模式。.

在特权模式下，如下配置 IP 授权模式：

命令	作用
Ruijie(config)**#aaa new-model**	打开 AAA 功能
Ruijie(config)**#aaa authorization ip-auth-mode {disabled | dhcp-server | radius-server | supplicant }**	配置 IP 授权模式
Ruijie**#show running-config**	显示配置

以下例子是把配置 IP 授权模式为 RADIUS-SERVER 模式：

```
Ruijie# configure terminal
Ruijie(config)# aaa authorization ip-auth-mode radius-server
Ruijie(config)# end
Ruijie# show running-config
!
aaa new-model
!
aaa authorization ip-auth-mode radius-server
!
Ruijie# write memory
```

4.2.15 发布广告信息

锐捷网络实现的 802.1x，可以在 Radius Server 端配置 Reply-Message 字段，当认证成功后，该字段的信息可以在锐捷网络推出的 802.1x 客户端 Star-Supplicant 上显示出来，便于运营商发布一些信息。

该消息只有在用户第一次认证时显示，重认证时不会显示，这样就避免了对用户的频繁打扰。

广告信息的显示窗口支持 HTML，会自动把消息中的 http://XXX.XXX.XX 转换成可直接跳转的连接，便于用户查看详细的信息。

广告信息的发布：

- 运行商在 Radius Server 端，配置 Reply Message 属性的内容；
- 只有锐捷的客户端 r-supplicant 才支持（对本公司设备的用户免费），其它的客户端看不到信息但不影响使用；
- 在设备端无需设置。

4.2.16 某端口下的可认证主机列表

为了增强 802.1x 的安全性，我们在不影响 IEEE 802.1x 的基础上进行了扩展，网管可以限定某个端口的认证的主机列表。如果一个端口下的可认证主机列表为空，则任何用户均可认证；若可认证主机列表不为空，那么只有列表中的主机允许认证。允许认证的主机用 MAC 标识。

添加某一端口下的可认证主机、删除某一端口下的可认证主机

命令	作用
Ruijie(config)**#dot1x auth-address-table address** *mac-addr* **interface** *interface*	设置可认证主机列表
Ruijie**#show running-config**	显示配置

若主机列表为空，该端口允许任何主机认证。

4.2.17 授权

为了方便运营商，我司的产品可以对不同类型的用户提供不同质量的服务，如：提供给用户的最大带宽不同。而这些信息集中于 Radius Server 上，管理员不必对每台设备进行配置。

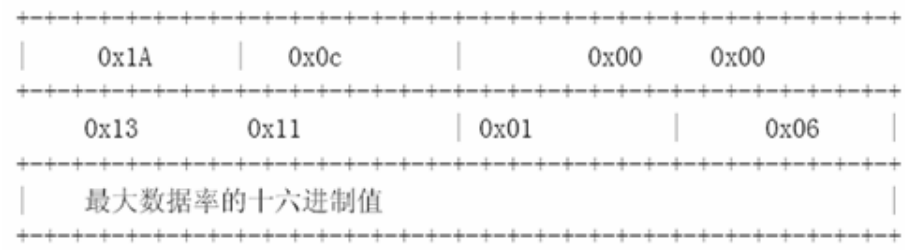
由于 Radius 没有标准的属性来表示最大数据率。我们只能通过厂商自定义属性来传递授权信息。

定义的通用格式如下：

图 4-6

对于最大数据率应填的值如下：

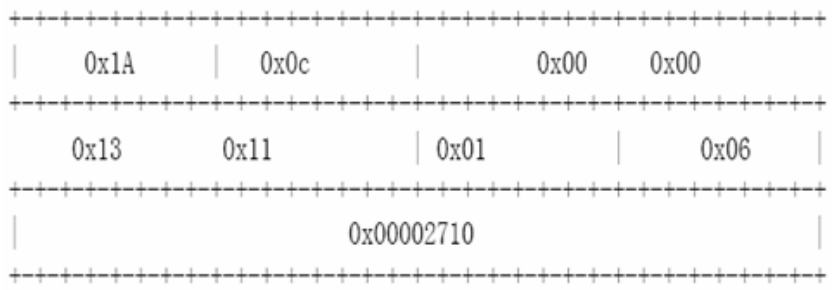
图 4-7



最大数据率的单位：kbps

对于最大数据率为 10M 的用户应填如下：

图 4-8



自定义的头按照以上格式填，最大数据率为 10M，即 10000kbsp，转换成 16 进制则 0x00002710，填在相应的字段上即可。

该功能无须设置设备端。只要设备端支持授权便可。

☑ S5750-S 系列交换机不支持 dscp 属性的下传。

4.2.18 配置认证方式

在标准中，802.1x 是通过 EAP-MD5 进行认证。锐捷网络科技公司实现的 802.1X，不但可以通过 EAP-MD5 方式认证（默认），还可以采用 CHAP 和 PAP 方式认证。采用 CHAP 的好处是可以减少一次设备与 RADIUS SERVER 的通讯，减轻 RADIUS SERVER 的压力。和 CHAP 方式一样，PAP 和 RADIUS SERVER 间的通讯也只有一次，虽然 PAP 认证方式由于其在安全方面存在很大缺陷，所以不建议使用，但是在某些情况下还是可以满足用户的特殊需求，比如当用户使用的安全服务器只支持 PAP 认证模式时，选择 PAP 认证模式就能够充分地利用现有的资源，保护用户的投资。

在特权模式下，按如下步骤设置 802.1x 的认证方式：

命令	作用
Ruijie(config)#**dot1x auth-mode** *mode*	配置认证模式
Ruijie#**show dot1x**	显示配置

以下例子是配置成 CHAP 模式的例子：

```
Ruijie# configure terminal
Ruijie (config)# dot1x auth-mode CHAP
Ruijie(config)# end
Ruijie# show dot1x
802.1X Status:        Disabled
Authentication Mode:  CHAP
Authed User Number:   0
Re-authen Enabled:    Disabled
Re-authen Period:     3600 sec
Quiet Timer Period:   10 sec
Tx Timer Period:      3 sec
Supplicant Timeout:   3 sec
Server Timeout:       5 sec
Re-authen Max:        3 times
Maximum Request:      3 times
Filter Non-RG Supp:   Disabled
Client Oline Probe:   Disabled
Eapol Tag Enable:     Disabled
Authorization Mode:   Group Server
```

4.2.19 配置备份认证服务器

我司基于 802.1x 的认证系统，可以支持备份服务器。当主服务器因各种原因当机之后，设备将自动向方法列表服务器组下一个服务器提交认证请求。

在特权模式下，按如下方式设置备份认证服务器。

命令	作用
Ruijie(config)#**aaa new-model**	打开 aaa 开关
Ruijie(config)#**aaa group server radius** *gs-name*	配置服务器组

Ruijie(config-gs-radius)#**server** *sever*	配置服务器
Ruijie(config-gs-radius)#**server** *server-backup*	配置备份服务器
Ruijie#**show dot1x**	显示配置

以下例子是配置 192.168.4.12 为备份服务器的例子：

```
Ruijie# configure terminal
Ruijie# aaa new-model
Ruijie(config)# aaa group server radius auth-ll
Ruijie(config-gs-radius)# server 192.168.4.1
Ruijie(config-gs-radius)# server 192.168.4.12
Ruijie(config-gs-radius)# end
```

4.2.20 对在线用户的配置及管理

锐捷设备提供了通过 SNMP 对已认证用户进行管理的功能。管理员可以通过 SNMP 查看已认证用户的信息，还可以强制使一个用户下线。被强制下线的用户必须再次认证才能使用网络资源。

该功能无需配置设备。

4.2.21 实现用户与IP 的捆绑

用锐捷网络公司提供的客户端，以及对 Radius Server 的正确配置，可以实现用户与 IP 的唯一绑定。某个用户必须以管理员分配的 IP 进行认证，否则将不能认证成功。

该功能无需配置设备，用户需用锐捷网络公司提供的客户端软件，管理员需配置 Radius Server。

4.2.22 基于端口的流量记费

锐捷网络设备除了提供针对时长的记费外，在设备的每个端口只接入一个用户的情形下，设备还可以提供针对流量的记费功能。

该功能无需配置设备，但需 Radius server 支持。

4.2.23 配置 802.1X端口动态VLAN自动跳转

动态 VLAN 自动跳转功能需要在远端 RADIUS 服务器上设置针对用户的下传 VLAN，RADIUS 服务器通过相应定义的 RADIUS 属性封装下传 VLAN 信息，接入设备收到该信息并在用户认证后就会自动把该用户所在端口加入到 RADIUS 服务器下传 VLAN 中。这个过程无需管理员再手工配置设备。

在接入设备端您可以通过 **show dot1x summary** 这条命令看出该用户所处的真实 VLAN，通过 **show dot1x user id** 命令可以看到 RADIUS 服务器下传 VLAN。

接入设备可以通过扩展 RADIUS 属性及 RADIUS 标准属性两种方式接收 RADIUS 服务器的下传 VLAN。

RADIUS 服务器使用基于标准扩展的属性下传 VLAN 给接入设备时，服务器将扩展属性封装在 26 号 RADIUS 标准属性中，扩展厂商 ID 为十六进制数 0x00001311，默认情况下该扩展属性类型号为 4，您可以在接入设备上通过配置命令 **radius attribute 4 vendor-type** *type* 来接收扩展属性类型号设置为 *type* 的下传 VLAN，配置命令可参见“配置 RADIUS”。

接入设备也能支持 RADIUS 服务器使用 RADIUS 标准属性下传 VLAN，包括以下属性组合：

- 64 号属性 Tunnel-Type
- 65 号属性 Tunnel-Medium-Type
- 81 号属性 Tunnel-Private-Group-ID
- 并且在应用动态 VLAN 自动跳转功能时，取值范围如下
- Tunnel-Type=VLAN (13)
- Tunnel-Medium-Type=802（6）
- Tunnel-Private-Group-ID=VLAN ID 或 VLAN Name
- 具体可参见 RFC2868 和 RFC3580。

对于接入设备接收到下传 VLAN 后处理步骤如下：先将下传 VLAN 属性作为 VLAN 名称，查看接入设备上是否配置有相同名称的 VLAN，若存在相同名称的 VLAN，则用户所在端口自动跳转至该 VLAN；若不存在相同名称的 VLAN，则将下传 VLAN 属性作为 VLAN ID，若该字符串表达的 VLAN ID 合法（系统支持的 VLAN ID 范围），则用户所在端口自动跳转至该 VLAN；若该字符串表达的 VLAN ID 为 0，则认为没有下传 VLAN 信息；其他情况用户将认证失败。

接入设备支持在端口模式为 ACCESS、TRUNK、HYBRID 模式下进行 802.1X 认证，其他端口模式下启用动态 VLAN 自动跳转功能将认证失败，在 ACCESS、TRUNK、HYBRID 端口模式下，VLAN 自动跳转支持情况如下：

1、认证端口模式为 ACCESS 端口

下发 VLAN 在设备上没有配置时，若下发 VLAN 被设备识别为 VLAN ID 时，设备创建相应的 VLAN，并使认证端口跳转到新创建的 VLAN 中，用户认证成功；若下发 VLAN 被设备识别为 VLAN 名称，无法找到对应的 VLAN ID，用户认证失败。

下发 VLAN 在设备上已经有配置存在时，若下发 VLAN 在设备上被配置为 ACCESS 口不支持跳转的 VLAN（见下面描述）时，则认证端口下用户将认证失败；若下发 VLAN 在设备上被配置为 ACCESS 口支持跳转的 VLAN，端口离开配置的 VLAN 并加入授权下发的 VLAN 中，用户认证成功。

ACCESS 口不支持跳转的 VLAN 有如下：

- 私有 VLAN；
- Remote VLAN；
- Super VLAN（包含 Sub VLAN）。

2、认证端口模式为 TRUNK 端口

TRUNK 口开启认证，修改端口的 Native VLAN 为下发 VLAN。

下发 VLAN 在设备上没有配置时，若下发 VLAN 被识别为 VLAN ID，设备创建相应的 VLAN，并且修改端口的 Native VLAN 为下发 VLAN，用户认证成功；若下发 VLAN 被识别为 VLAN 名称，无法找到对应的 VLAN ID，用户认证失败。

下发 VLAN 在设备上已经有配置存在时，若下发 VLAN 在设备上被配置为 TRUNK 口不支持跳转的 VLAN(见下面描述)时，则认证失败；若下发 VLAN 在设备上被配置为 TRUNK 口支持跳转的 VLAN，修改端口的 Native VLAN 为下发 VLAN，用户认证成功。

TRUNK 口不支持跳转 VLAN 有如下：

- 私有 VLAN；
- Remote VLAN；
- Super VLAN（包含 Sub VLAN）。

3、认证端口模式为 HYBRID 端口

如果当前 HYBRID 端口未开启 MAC VLAN 功能，下发 VLAN 处理方式如下：

下发 VLAN 在设备上没有配置时，若下发 VLAN 被识别为 VLAN ID，设备自动创建相应的 VLAN，允许下发 VLAN 以不携带 TAG 的方式通过当前 HYBRID 端口，并且修改端口的 Native VLAN 为下发 VLAN，用户认证成功；若下发 VLAN 被识别为 VLAN 名称，无法找到对应的 VLAN ID，用户认证失败。

下发 VLAN 在设备上已经配置存在时，若下发 VLAN 在设备上被配置为 HYBRID 口不支持跳转的 VLAN(见下面描述)，或者指定 VLAN 已经存在于 HYBRID 端口携带 TAG VLAN 列表中，用户认证失败；否则，允许下发 VLAN 以不携带 TAG 的方式通过当前 HYBRID 端口，并且修改端口的 Native VLAN 为下发 VLAN，用户认证成功。

如果当前 HYBRID 端口开启了 MAC VLAN 功能，下发 VLAN 处理方式如下：

如果认证服务器下发的 VLAN 在设备上不存在（MAC VLAN 要求相应 VLAN 必须静态配置存在），或者下发 VLAN 已经以携 TAG 方式加入到 HYBRID 端口中，或者 MAC VLAN 功能不支持的 VLAN 类型(见《MAC-VLAN-SCG.doc》描述)，则用户认证失败；否则，设备根据认证服务器下发的 VLAN 和用户 MAC 地址，动态地创建 MAC VLAN 表项，用户认证成功。

用户下线时，MAC VLAN 表项被动态删除。

HYBRID 端口不支持跳转的 VLAN 有如下：

- 私有 VLAN；
- Remote VLAN；
- Super VLAN（包含 Sub VLAN）；

端口上未开启 MAC VLAN 时，VLAN 下发修改了端口的 Native VLAN，但是并不改变端口的 Native VLAN 命令配置。下发 VLAN 的优先级高于命令配置 VLAN，即通过认证后起作用的 Native VLAN 是下发 VLAN，命令配置的 Native VLAN 在用户下线后生效。

端口上开启 MAC VLAN 功能并且认证模式是基于 MAC 的用户认证时，VLAN 下发通过动态生成 MAC VLAN 表项实现，不会修改端口的 Native VLAN。

对于 HYBRID 端口，无论是否开启 MAC VLAN 功能，如果授权下发的 VLAN 已经配置为携带 TAG 的方式加入端口，则 VLAN 下发失败。

端口上开启 MAC VLAN 功能时，VLAN 下发将会创建掩码为全 F 的 MAC VLAN 表项，如果 802.1x 用户的 MAC 地址被静态配置的掩码不为全 F 的 MAC VLAN 表项的 MAC 地址覆盖， 则下发的 VLAN 和该静态配置的掩码不为全 F 的

MAC VLAN 表项指定的 VLAN 必须相同；否则，将导致 VLAN 下发的 802.1x 用户出现异常，具体异常表现如下（但不限于以下）：

802.1x 用户可以认证成功，但认证成功后的合法数据报文被丢弃，无法访问网络；

用户发送 EAPOL-LOGOFF 报文下线时，设备上 802.1x 认证表项残留，认证服务器上显示该用户仍然在线；

在设备上设置某个端口进行动态 VLAN 自动跳转功能，您可以通过以下步骤配置：

- 打开 AAA 开关

命令	作用
Ruijie(config)**#aaa new-model**	打开 AAA 开关

具体参见“配置 AAA”章节。

- 配置 RADIUS 服务器

命令	作用
Ruijie(config)**#radius-server host** *host-ip*	配置 RADIUS 服务器
Ruijie(config)**#radius-server key** *text*	配置 RADIUS 服务器共享密钥

具体参见“配置 RADIUS”章节。

- 配置方法列表

命令	作用
Ruijie(config)**#aaa authentication dot1x** *list1* **group radius**	配置认证方法列表 list1
Ruijie(config)**#aaa accounting network** *list2* **start-stop group radius**	配置记账方法列表 list2

具体参见“配置 AAA”

- 802.1X 选择方法列表

命令	作用
Ruijie(config)**#dot1x authentication** *list1*	选择认证方法列表为 list1，list1 为步骤 3 中配置
Ruijie(config)**#dot1x accounting** *list2*	选择记账方法列表为 list2，list2 为步骤 3 中配置

- 接口使能 802.1X 认证

命令	作用
Ruijie(config)**#interface** *interface_id*	进入需要配置的接口模式下，*interface_id* 为所要进入接口
Ruijie(config-if-*type ID*)**#dot1x port-control auto**	接口使能 802.1X 认证

- 接口使能 VLAN 自动跳转功能

命令	作用
Ruijie(config)**#interface** *interface_id*	进入需要配置的接口模式下，*interface_id* 为所要进入接口
Ruijie(config-if-*type ID*)**#dot1x dynamic-vlan enable**	接口使能 VLAN 自动跳转功能

- VLAN 自动跳转功能必须要在接口下打开动态跳转开关，即需要相应的接口下配置命令 **dot1x dynamic-vlan enable**。否则会忽略封装下传 VLAN 的 RADIUS 属性。
- **dot1x dynamic-vlan enable** 必须在接口配置命令 **dot1x port-control auto** 后才能打开，在使用 **no dot1x port-control auto** 命令之后接口 VLAN 自动跳转功能的使能开关将自动关闭。

■ 查看动态 VLAN 自动跳转信息

完成以上配置并且在认证成功后，可以通过下列步骤查看动态 VLAN 自动跳转相关信息.

命令	作用
show dot1x user id *session_id*	查看会话号为 *session_id* 的用户信息，包括动态 VLAN 自动跳转信息。
show dot1x summary	该命令可以看出用户真实所在 VLAN

至此，接入设备上的 VLAN 自动跳转功能配置完成，有关的注意事项请参见“配置 802.1X 其他注意事项”章节。

4.2.24 实现端口的GUEST VLAN功能

端口上开启 **GUEST VLAN** 功能后，以下任一条件满足时，将该端口添加到 guest vlan 中：

■ 该端口会连续发送 3 次主动认证报文，如果在 auto-req req-interval * 3 时间内，没有收到任何 EAPOL 响应报文；

■ 90 秒内没有收到任何 EAPOL 响应报文；

■ MAB 模式下的 MAC 地址认证失败后；

您可以通过 **show running-config** 这条命令看出这条命令的配置，以及通过 **show vlan** 查看到端口是否已经跳转到 guest vlan。

设备上可以设置某个端口是否允许跳转到 guest vlan，您可以通过以下步骤配置：

命令	作用
Ruijie(config-if-*type ID*)**#interface** *interface*	进入接口配置模式
Ruijie(config-if-*type ID*)**#dot1x dynamic-vlan enable**	接口允许 Vlan 跳转
Ruijie(config-if-*type ID*)**# [no] dot1x guest-vlan** *vid*	配置是否开启 guest vlan 功能，缺省关闭
Ruijie**# show running-config**	显示配置

- 必须配置 dot1x dynamic-vlan enable，guest vlan 才能生效。
- 配置 guest vlan 期间最好不要配置二层属性，尤其是不要再手动设置端口 vlan。
- 端口加入 guest vlan 后，如果在该端口上接收到 eapol 报文或者端口从 linkup 切换为 linkdown 时，端口会从 guest vlan 中退出。
- 如果端口上配置了 GUEST VLAN 功能，端口从 linkdown 切换为 linkup 时，会重新检查是否将端口加入到 guest vlan 中。

4.2.25 代理服务器屏蔽和拨号屏蔽

用户自行架设代理服务器以及用户认证后再自行拨号上网，这是网络安全最大的两个隐患。锐捷网络设备提供代理服务器屏蔽和拨号屏蔽功能。

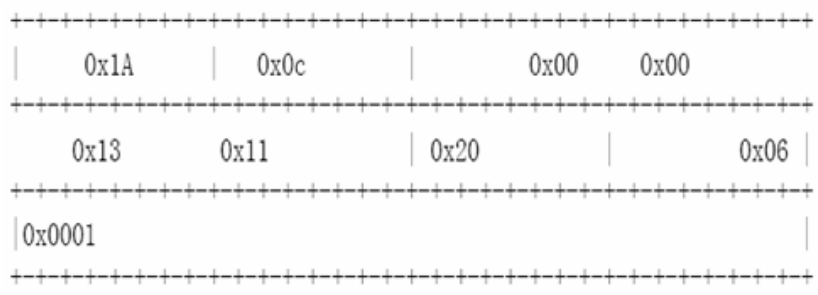
实现该功能设备端不需任何设置，只需在 RADIUS 服务器端配置相应的属性。由于 Radius 没有标准的属性来表示最大数据率，我们只能通过厂商自定义属性来传递授权信息。我们定义的通用格式见授权一节的说明。

代理服务器屏蔽功能定义的 Vendor Type 为 0x20，拨号屏蔽功能定义的 Vendor Type 为 0x21。

Attribute-Specific 字段为四个字节的厂商自定义属性，定义了对使用代理服务器上网和拨号上网行为所采取的动作. 0x0000 表示正常连接，不进行检测屏蔽, 0x0001 表示进行检测屏蔽。

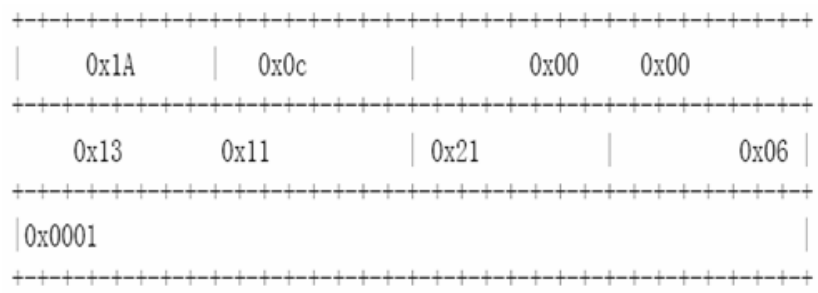
若要屏蔽通过代理服务器上网，用户应填如下信息：

图 4-9



若要屏蔽通过拨号上网，用户应填如下信息：

图 4-10



4.2.26 配置客户端在线探测

为了保证计费的准确性，需要一种在线探测机制能够在短时间内获知用户是否在线。在标准实现中的重认证机制能够满足这种需求，但是标准实现中需要 RADIUS 服务器的参与，要实现准确的探测用户是否在线将会占用设备和 RADIUS 服务器的大量资源。为了满足在占用少量资源的基础上实现计费的准确性，我们采用了一种新的客户端在线探测机制。这种机制只需要在设备和客户端之间交互，并且对网络流量的占用极小，能够实现分钟级的计费精度(用户可以通过配置来确定计费的精度)。

实现客户端在线监测需要客户端软件支持这一功能。

以下两个定时器影响到在线探测的性能和精度：

- Hello Interval: 客户端定时发送通告的间隔。
- Alive Interval：客户端在线间隔。设备在此间隔期间没有收到客户端的通告，将主动断开同客户端连接，并通知计费服务器。该值必须大于 Hello Interval。

在特权模式下，我们可以按以下方式配置客户端在线探测功能：

命令	作用
Ruijie(config)**#dot1x client-probe enable**	打开客户端在线探测功能
Ruijie(config)**#dot1x probe-timer interval** *interval*	配置 Hello Interval
Ruijie(config)**#dot1x probe-timer alive** *interval*	配置设备的 Alive Interval
Ruijie**#show dot1x**	显示配置

4.2.27 配置EAPOL 帧带TAG 的选项开关

IEEE 802.1x 约定 EAPOL 报文不能加 VLAN TAG，但基于可能的应用需求，我们提供了相应的选项开关，在打开相应开关时，能根据 Trunk Port 的相应输出规则输出 TAG。

典型的应用环境就是在汇聚层打开 802.1x 认证，参见“典型应用的拓扑结构”。

在特权模式下，我们可以按以下方式配置 EAPOL 帧带 TAG 的选项开关。

命令	作用
Ruijie(config)**#dot1x eapol-tag**	打开 EAPOL 帧带 TAG 的功能。缺省该功能是关闭的
Ruijie**#show dot1x**	显示配置

您可以用 **no dot1x eapol-tag** 命令来关闭该功能。

4.2.28 配置基于端口的用户认证

802.1x 对用户的控制默认情况下是基于用户 MAC 进行控制的，只有通过认证的用户才能使用网络，而对于其他接在同一端口的用户无法使用网络，而基于端口的控制模式及表示当某一端口有一个用户认证通过时，此端口就变成已认证端口，所有接在此端口下的用户都能够正常的使用网络。

要配置端口的控制模式为基于端口的控制模式，从特权模式开始，按步骤进行以下设置。

命令	作用
Ruijie(config)**#interface** *interface-id*	进入接口模式
Ruijie(config-if-*type ID*)**#dot1x port-control auto**	打开受控功能
Ruijie(config-if-*type ID*)**#dot1x port-control-mode { mac-based | port-based }**	选择受控的模式
Ruijie**#show dot1x port-control**	显示端口 802.1X 配置

您可以用 **no dot1x port-control-mode** 命令来恢复默认受控方式。

下面的例子显示了如何配置端口的认证模式

```
Ruijie#configure terminal
Ruijie(config)# interface interface-id
Ruijie(config-if)# dot1x port-control-mode port-base
```

基于端口的认证模式下，每个端口只能接一个认证用户。

对于基于端口的认证方式下，可以允许或禁止动态用户在多个认证端口之间迁移，默认情况是允许动态用户在不同端口之间迁移，如要禁止动态用户的迁移，从特权模式开始，按步骤进行以下设置。

命令	作用
Ruijie(config)**#dot1x stationarity enable**	禁止端口间的迁移

4.2.29 配置基于端口单用户认证

802.1x 对用户的控制默认情况下是基于用户 MAC 进行控制的，只有通过认证的用户才能使用网络，而对于其他接在同一端口的用户无法使用网络，基于端口的控制模式及表示当某一端口有一个用户认证通过时，此端口就变成已认证端口，所有接在此端口下的用户都能够正常的使用网络。

而基于端口单用户的认证是在基于端口的控制模式下，对认证用户的数量控制为单一用户。该端口下只允许单一用户认证通过，此端口就变成已认证端口，能够正常的使用网络，这时，如果发现端口有其它的用户存在，则把端口下的所有用户清除，重新认证。

要配置端口单用户的控制模式为基于端口的控制模式，从特权模式开始，按步骤进行以下设置。

命令	作用
Ruijie(config)**#interface** *interface-id*	进入接口模式
Ruijie(config-if-*type ID*)**#dot1x port-control auto**	打开受控功能
Ruijie(config-if-*type ID*)**#dot1x port-control-mode port-based single-host**	基于端口单用户的控制模式
Ruijie**#show dot1x port-control**	显示端口 802.1X 配置

您可以用 no dot1x port-control-mode 命令来恢复默认受控方式。

下面的例子显示了如何配置端口的认证模式

```
Ruijie#configure terminal
Ruijie(config)#interface interface-id
Ruijie(config-if)#dot1x port-control-mode port-base single-host
```

基于端口的认证模式下，每个端口只能接一个认证用户

single-host 是基于端口单用户的 802.1x 访问控制，在 **show dot1x port-control** 上会显示端口为 port-based，在 **show running-config** 会显示为 **dot1x port-control-mode port-based single-host**。

single-host 由于只支持单一用户形式，手动配置端口 **default-user-limit**，在 **single-host** 模式无效。如果在配置 **single-host** 后，端口下配置 **default-user-limit**，这个数量对 **single-host** 没有约束，该端口还是只允许单一用户上网。

对于基于端口的认证方式下，可以允许或禁止动态用户在多个认证端口之间迁移，默认情况是允许动态用户在不同端口之间迁移，如要禁止动态用户的迁移，从特权模式开始，按步骤进行以下设置。

命令	作用
Ruijie(config)**#dot1x stationarity enable**	禁止端口间的迁移

4.2.30 配置动态acl下发

802.1x 支持从服务器下发 acl，动态安装下发的 acl。我司产品默认支持安装 acl，只要服务器上配置为许可 acl，并能在用户认证成功后下发 acl，我司产品都会动态安装下去。

实现动态 acl 下发，需要把端口配置成为 mac-based 认证模式，或者配置成基于端口单用户认证模式，这些模式的配置请参考相关命令配置说明。

在 single-host 认证模式下，在重认证的时候支持更新 acl。即用户已经认证后，在服务器上配置了 acl，用户重新认证的时候这些 acl 生效。

支持的 acl 类型：在锐捷交换机上 acl 功能能够解析的扩展类型。

认证服务器动态 acl 下发功能需要配置如下命令:

Ruijie**# configure terminal**

Ruijie(config)**# radius vendor-specific extend**

4.2.31 配置MAC旁路认证

GUEST VLAN 提供了一种支持无 802.1X 认证客户端设备接入网络的方法，但是该技术无法判断接入设备是否安全，存在安全隐患。在某些情况下，出于网络管理和安全考虑，即便无 802.1X 认证客户端，网络管理员仍然需要控制这些接入设备的合法性。MAC 旁路认证(MAC Authentication Bypass,简称 MAB)为这种应用提供了一种解决方案。

在 802.1X 认证端口部署了 MAB 功能后，802.1x 会向该端口持续发送认证请求报文并期望得到客户端响应。如果在 tx-period*reauth-max 时间内并无客户端响应，则 802.1x 会监听该认证口下学习到的 MAC 地址，并且以该 MAC 地址为用户名和密码向认证服务器发起认证，通过服务器返回的认证结果判断该 MAC 地址是否允许访问网络。

通过如下的步骤配置 MAB 功能：

命令	作用
Ruijie(config)**#interface** *interface-id*	进入接口模式
Ruijie(config-if-*type ID*)**#dot1x mac-auth-bypass**	配置
Ruijie**#show running-config**	显示所有配置

下面的例子显示了如何配置 MAB 功能：

```
Ruijie# configure terminal
Ruijie(config)# interface fa 0/1
Ruijie(config-if)# dot1x port-control auto
Ruijie(config-if)# dot1x mac-auth-bypass
```

服务器配置 MAC 账号的用户名和密码时，均需要使用 XXXXXXXXXXXX 的格式。

端口进入 MAB 模式后，只能有一个 MAC 地址做认证，其它 MAC 地址将不会进行认证，这要取决于设备先发现哪个 MAC 地址。

端口模式和 MAC 模式均只能支持一个端口一个 MAC 地址认证。

任何时刻端口下有客户端响应 802.1x 认证，端口的 MAB 将失效，除非端口经历 down/up 的 link 变化或者重新开关端口的 1x 功能。

客户端在线探测功能对 MAB 模式下的认证 MAC 不生效。

配置了 MAB 的端口，每隔 tx-period 发出一个认证请求报文，发送 reauth-max 次之后，如果没有客户端响应，则该端口进入 MAB 模式。进入 MAB 模式的端口可以学习 mac 地址,并使用这些 MAC 地址为账号进行认证。

MAB 支持 PAP、CHAP、EAP-MD5 三种认证方法。如何配置认证方法请参考"配置认证方式"章节。

MAB 模式下的 mac 地址认证失败后，如果有配置 guest vlan，则该认证口将进入 guest vlan。如果没有配置 guest vlan，则端口维持在原有 vlan。MAB 不支持失败 VLAN，也就是说，即便 MAB 认证失败，且用户配置了失败 vlan，端口也不会进入失败 vlan。

MAB 支持动态 vlan 下发、ACL 下发等服务器部署功能。

如果某个 MAC 地址在一个端口通过 MAB 认证后，又在其它端口出现，则后出现的那个端口将被设置为违例。

静态地址、过滤地址无法进行 MAB 认证。用户如果在配置了 MAB 的端口也配置了静态地址，则当端口开始 MAB 认证且未认证通过时，该静态地址将无法通信。

MAB 认证是为无认证客户端软件的设备提供接入认证服务的，这些设备通常都无法识别 802.1Q 的 TAG 标签，因此 MAB 认证功能最好部署在 ACCESS 口上，否则即便认证通过，设备同样有可能无法通信。

端口上开启 GSN 地址绑定功能时，通过 MAB 方式认证的用户，将无法访问网络

4.2.32 配置MAC旁路认证超时时间

MAB 模式下的 MAC 地址认证上线后，除非重认证失败、端口 down 或者因为管理策略原因下线，比如管理员强制下线等，否则交换机将认为该 MAC 地址一直是可以在线的。

用户可以配置许可这些认证地址的在线时间，默认是 0，表示允许一直在线。

通过如下的步骤配置 MAB 的超时时间：

命令	作用
Ruijie(config)**#interface** *interface-id*	进入接口模式
Ruijie(config-if-*type ID*)**#dot1x mac-auth-bypass timeout-activity** *value*	配置 MAB 超时时间，单位秒，无默认值，参数的配置范围 1-65535
Ruijie**#show running-config**	显示所有配置

下面的例子显示了如何配置 MAB 超时功能：

```
Ruijie# configure terminal
Ruijie(config)# interface fa 0/1
Ruijie(config)# dot1x mac-auth-bypass timeout-activity   3600
```

如果服务器也下发了认证 mac 地址的在线时间，则这个时间和 timeout-activity 是独立生效的，也就是说，哪个时间先到，就哪个先生效。

超时时间到达后，如果端口有配置 guest vlan，则端口将切换到 guest vlan。但是认证过程中的服务器响应超时不会导致 MAB 端口进入 guest vlan。

4.2.33 配置MAC旁路认证违例

默认情况下，有一个 MAC 地址通过 MAB 认证后，该端口下的所有设备的数据都允许被转发。但是在某些安全应用下，管理员会要求一个 MAB 端口下只能有一个 MAC 地址存在，此时可以在该端口上配置 MAB 违例。配置了 MAB 违例后，一旦端口进入了 MAB 模式，如果发现该端口下有超过 1 个 MAC 地址，该端口将产生违例。

通过如下的步骤配置端口的 MAB 违例：

命令	作用
Ruijie(config)**#interface** *interface-id*	进入接口模式
Ruijie(config-if-*type ID*)**#dot1x mac-auth-bypass violation**	配置 MAB 违例
Ruijie**#show running-config**	显示所有配置

下面的例子显示了如何配置 MAB 违例：

```
Ruijie# configure terminal
Ruijie(config)# interface fa 0/1
Ruijie(config)# dot1x mac-auth-bypass violation
```

MAB 违例端口可以通过 **errdisable recover** 恢复。

由于 private vlan 的端口上同个 MAC 地址会同时出现在主从 VLAN 里面,因此不要在 private vlan 端口上配置 MAB 认证违例，否则会导致 MAB 违例判断错误，影响正常的使用。

4.2.34 配置失败VLAN

如果在交换机上，配置了失败 vlan，当该端口的用户认证失败后，该端口将进入预先配置好的失败 vlan。

失败 vlan 基于接口，您可以通过以下步骤配置：

命令	作用
Ruijie(config)**#interface** *interface-id*	进入接口模式
Ruijie(config-if-*type ID*)**#dot1x auth-fail vlan** *vid*	配置该端口的失败 vlan
Ruijie**#show run**	显示配置

下面的例子显示了如何配置失败 vlan：

```
Ruijie# configure terminal
Ruijie(config)# interface fa  0/1
Ruijie(config-if)# dot1x auth-fail vlan 2
```

如果配置的 vlan 不存在，则在端口进入失败 vlan 时会被动态创建，端口退出失败 vlan 时自动删除。

如果端口 down，则端口自动退出失败 vlan。

允许失败 vlan 和 guest vlan 配置为相同的 vlan。

端口模式下，进入 FAIL-VLAN 后，只允许之前认证失败的用户重新进行认证，其它用户的认证请求被丢弃,MAC 模式则无此限制。

失败 vlan 不支持 private vlan，也就是说不能将 private vlan 配置为 dot1x 的失败 vlan。

端口上开启 GSN 地址绑定功能时，认证失败进入 FAIL-VLAN 的用户，将无法访问网络;

4.2.35 配置失败VLAN尝试次数

失败 VLAN 是在客户端尝试认证连续失败一定次数后才会进入的。您可以通过以下步骤配置这个次数：

命令	作用
Ruijie(config)**#dot1x auth-fail max-attempt** *value*	配置进入失败 vlan 的尝试次数，默认为 3 次,参数范围 1-3
Ruijie**#show running-config**	显示所有配置

下面的例子显示了如何配置失败 VLAN 尝试次数：

```
Ruijie# configure terminal
Ruijie(config)# dot1x auth-fail max-attempt 2
```

4.2.36 配置允许MAC地址迁移

默认情况下，802.1x 用户在某一端口上认证通过后，该用户的 MAC 地址绑定在该端口上，不允许出现在其它端口上。

但是，某些情况下，用户认证通过后，可能需要迁移到其它的端口。如：开启 802.1x 认证的交换机和用户 PC 之间，使用另外一台交换机连接起来。当用户直接拔掉网线，从端口 1 迁移到端口 2 后，端口 1 因为没有接收到端口 down 事件，并不知道用户已经下线。导致 PC 连接到端口 2 后，也无法认证上网。

为了使用户切换到端口 2 后可以访问网络，可以在全局模式下，配置允许 MAC 地址迁移功能。当用户出现在端口 2 时，端口 1 上的用户被强制下线，同时在端口 1 上重新发起认证交互过程。用户可以在同一设备不同端口下迁移，也可以跨设备进行迁移；可以在受控端口之间迁移，也可以从受控端口迁移到非受控端口。

按照如下步骤配置允许 MAC 地址迁移：

命令	作用
Ruijie**# configure terminal**	进入全局配置模式
Ruijie(config)**# dot1x mac-move permit**	开启允许 MAC 地址迁移功能
Ruijie(config)**# end**	退到特权模式
Ruijie**# show dot1x**	显示 802.1x 全局配置

举例如下：

```
Ruijie# configure terminal
Ruijie(config)# dot1x mac-move permit
```

如果网络中存在 MAC 地址欺骗，开启允许 MAC 地址迁移功能后，可能造成已认证用户被虚假用户抢占，被强制下线;

- 用户未迁移端口，在原端口修改 IP 地址或者插拔网线，会触发重认证过程；
- 如果该用户 MAC 地址被配置为静态 MAC 地址，用户不能迁移；

4.2.37 配置服务器失效旁路认证

当交换机上所有配置的 RADIUS 服务器不可达时，用户认证请求将无法得到响应。对于管理员来说，无法对用户身份合法性进行检验。对于用户来说，如果交换机上没有配置其它的认证方法，可能造成无法访问网络。为了保证新认证用户可以访问网络，可以在端口上配置服务器失效旁路认证功能（Inaccessible Authentication Bypass，简称 IAB 功能）。

按照如下步骤开启 IAB 功能：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式
Ruijie(config)# **interface** *interface-id*	进入端口配置模式
Ruijie(config-if)# **dot1x critical**	配置服务器失效旁路认证功能
Ruijie(config-if)# **end**	退出到特权模式
Ruijie# **show running-config**	显示所有配置

下面的例子显示了如何配置服务器失效旁路认证功能：

```
Ruijie# configure terminal
Ruijie(config)# interface fa 0/1
Ruijie(config-if)# dot1x port-control auto
Ruijie(config-if)# dot1x critical
```

端口上开启 IAB 功能且所有服务器失效后：

1）只有 802.1x 全局配置的认证方法列表中仅存在 RADIUS 认证方法且该方法列表中的 RADIUS 服务器全部失效时，IAB 功能才生效；如果方法列表中还存在其它认证方法(如：local、none)，IAB 功能不生效；

2）全局开启 AAA 多域认证功能后，802.1x 用户认证时，不再使用全局配置的方法列表。由于 IAB 功能判断 802.1x 全局配置方法列表中的 RADIUS 服务器全部失效后，直接向用户返回认证成功，不需要输入用户名，因此 AAA 多域认证功能在该端口上失效；

3）通过 IAB 方式认证的用户，不再向计帐服务器发起计帐请求；

4）已正常认证通过的用户，不受服务器失效的影响，可以正常访问网络；

5）全局开启 802.1x IP 授权功能时，如果端口上已经存在认证成功的用户，该端口上的其它用户不能通过 IAB 方式进行认证；

6）端口上开启 GSN 地址绑定功能时，通过 IAB 方式认证的用户，将无法访问网络；

4.2.38 配置服务器失效旁路认证跳转VLAN

当 802.1x 受控端口进入服务器失效旁路认证状态时，由于暂时无法对用户身份合法性进行验证，可以配置将该端口加入到指定的 VLAN 中，仅允许用户访问指定 VLAN 内的网络资源。

按照如下步骤配置 IAB 功能跳转 VLAN：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式
Ruijie(config)# **interface** *interface-id*	进入端口配置模式
Ruijie(config-if)# **dot1x critical vlan** *vlan-id*	配置服务器失效旁路认证跳转 VLAN
Ruijie(config-if)# **end**	退出到特权模式
Ruijie# **show running-config**	显示所有配置

下面的例子显示了如何配置服务器失效旁路认证功能：

```
Ruijie# configure terminal
Ruijie(config)# interface fa 0/1
Ruijie(config-if)# dot1x port-control auto
Ruijie(config-if)# dot1x critical
Ruijie(config-if)# dot1x critical vlan 100
```

- 所有 RADIUS 服务器失效前，如果端口上已经存在认证通过的用户，服务器失效后，如果端口上未配置服务器失效跳转 VLAN，允许对新用户进行网络访问授权；如果端口上已经配置服务器失效跳转 VLAN，则不能对新用户进行网络访问授权，优先保证原有用户使用网络；
- 所有服务器失效前，如果端口上已经存在正常认证通过的用户，用户发起重认证过程中发现服务器失效，端口保持原有状态，不再跳转到失效 VLAN；
- 端口下所有用户下线后，端口自动退出失效 VLAN；
- 如果配置的失效 vlan 不存在，则在端口进入失效 vlan 时会被动态创建，端口退出失效 vlan 时会被自动删除；
- 失效 VLAN 不支持跳转到以下 VLAN：私有 VLAN、REMOTE VLAN、SUPER VLAN（包含 SUB VLAN）；

4.2.39 配置服务器失效旁路认证恢复处理

RADIUS 服务器处于失效状态时间内，有些用户没有通过认证，交换机即对用户完成网络访问的授权。当 RADIUS 服务器从失效状态恢复正常后，可以配置该功能对端口下的 IAB 用户发起主动认证，以验证用户身份的合法性。

按照如下步骤配置 IAB 恢复处理功能：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式
Ruijie(config)# **interface** *interface-id*	进入端口配置模式
Ruijie(config-if)# **dot1x critical recovery action reinitialize**	配置服务器恢复后，对端口下的 IAB 用户发起认证交互
Ruijie(config-if)# **end**	退出到特权模式
Ruijie# **show running-config**	显示所有配置

下面的例子显示了如何配置服务器失效旁路认证功能：

```
Ruijie# configure terminal
Ruijie(config)# interface fa 0/1
```

```
Ruijie(config-if)# dot1x port-control auto
Ruijie(config-if)# dot1x critical
Ruijie(config-if)# dot1x critical recovery action reinitialize
```

服务器恢复后，端口下正常认证通过的用户，可以继续访问网络，不需要重新认证；只有在服务器失效期间，通过 IAB 方式认证的用户，交换机会发起主动认证交互；

4.2.40 配置多帐号切换

在一些应用环境中，比如微软的 AD 域认证环境中，有时会出现这样的使用要求，用户先用一个用户名认证上线，然后又切换到另外一个用户名重认证，一般这种应用都是部署了一些授权应用，比如不同帐号捆绑不通的授权 vlan 等。默认情况下，设备遇到这种在线情况下切换用户名的认证请求，是不会响应的。如果要支持这种应用，需要开启多帐号切换功能。

在特权模式下，按如下步骤设置多帐号切换功能。

命令	作用
Ruijie# **configure terminal**	进入全局配置模式
Ruijie(config)# **dot1x multi-account enable**	设置多帐号切换功能
Ruijie# **show dot1x**	显示 dot1x 配置

使用 **no dot1x multi-account enable** 命令恢复默认值，以下是配置多帐号切换功能的例子。

```
Ruijie# configure terminal
Ruijie(config)# dot1x multi-account enable
Ruijie(config)# end
```

4.2.41 配置使用虚拟mac作为设备认证报文的源mac

在设备 MAC 地址的前三个字节不是 00d0.f8 或者 00.1aa9，设备会使用 001a.a917.ffff 作为 802.1X 报文的源 mac 地址。该功能默认开启。

按照如下步骤关闭使用虚拟 mac 作为设备 802.1X 报文的源 MAC 地址：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式
Ruijie(config)# **no dot1x pseudo source-mac**	关闭使用虚拟 mac 功能
Ruijie(config-if)# **end**	退出到特权模式

下面的例子显示了如何关闭使用虚拟 mac 功能：

```
Ruijie# configure terminal
Ruijie(config)# no dot1x pseudo source-mac
Ruijie(config)# end
```

4.2.42 配置多MAB认证功能

当一个端口下有多个无认证客户端的设备需要进行 802.1x 认证接入时，单用户的 MAC 旁路认证已无法满足要求，而多 MAB 认证功能就是为解决这个场景实现的。开启多 MAB 认证功能后，设备会把该端口下学习到的 mac 地址作为用户名和密码发送到服务器进行认证，如果认证通过，该设备将可以正常访问网络，否则该设备无法访问网络。

通过如下的步骤配置多 MAB 认证功能：

命令	作用
Ruijie(config)#**interface** *interface-id*	进入接口模式
Ruijie(config-if)#**dot1x mac-auth-bypass multi-user**	配置开启多 MAB 认证功能
Ruijie#**show running-config**	显示所有配置

下面的例子显示了如何配置多 MAB 认证功能：

```
Ruijie# configure terminal
Ruijie(config)# interface fa 0/1
Ruijie(config-if)# dot1x port-control auto
Ruijie(config-if)# dot1x mac-auth-bypass multi-user
```

多 MAB 用户支持 MAB 用户的在线时间，即 dot1x mac-auth-bypass timeout-activity <value>配置的时间，如果配置的值为 0，则表示用户可以一直在线；另外，多 MAB 用户支持服务器下发 session_timeout，用户实际下线时间要看这两个时长哪个先用完。

多 MAB 认证只支持 mac based 认证方式，如果端口认证模式为 port based 模式，多 MAB 认证模式无法配置生效；反之，如果开启了多 MAB 认证功能，不能更改端口认证方式，必须先关闭多 MAB 用户认证功能才能更改。

多 MAB 认证功能与单 MAB 功能互斥，在同一时刻，只能配置其中一种方式。

多 MAB 认证能与普通的 dot1x 认证共存，如果一个 mac 地址进行了 dot1x 认证，这个地址将不会进行多 MAB 认证；如果一个 mac 地址先进行多 MAB 认证，后用客户端进行认证，则多 MAB 认证用户会先下线，再进行普通 dot1x 认证。

如果配置了 Fail vlan，多 MAB 用户认证失败次数达到失败尝试次数，则会进行 Fail vlan 授权；授权时，端口是 hybrid 口，且配置了 mac vlan 功能，则进行 mac vlan 授权，否则进行 port vlan 授权。

开启多 MAB 认证功能时，guest vlan 功能失效，如果端口已经进入了 guest vlan，会先退出 guest vlan。

多 MAB 不支持 ip 授权和 gsn 地址绑定，即 ip 授权和 gsn 地址绑定功能对多 MAB 认证用户不生效。

4.2.43 配置多MAB非法用户静默时间

开启多 MAB 认证功能时，为了防止接口下的非法用户对设备进行攻击，需要禁止非法用户频繁认证，以减少服务器的压力。在全局下配置多 MAB 用户的静默时间，默认为 30s，也就是说，如果学习到一个 mac 地址并认证失败后，这个 mac 地址需要等待 30s 才会重新发起认证，这个静默时间可以根据环境进行配置，如果配置为 0，表示一个用户认证失败后可以马上进行再认证。

通过如下的步骤配置多 MAB 非法用户静默时间：

命令	作用

Ruijie# configure terminal	进入全局配置模式
Ruijie(config)#**dot1x multi-mab quiet-period** *value*	配置多 MAB 用户的静默时间
Ruijie(config)#**show running-config**	显示所有配置

下面的例子显示了如何配置多 MAB 用户的静默时间功能：

```
Ruijie# configure terminal
Ruijie(config)# dot1x multi-mab quiet-period 100
Ruijie(config)# interface fa 0/1
Ruijie(config-if)# dot1x port-control auto
Ruijie(config-if)# dot1x mac-auth-bypass multi-user
```

4.2.44 配置多MAB直通

开启多 MAB 认证功能且结合自动获取客户端功能一起使用时，如果需要放过一些免认证就可以访问的地址，如 http 重定向地址，免认证的网络资源等等，此时需要配置多 MAB 直通。

通过如下的步骤配置多 MAB 直通：

命令	作用
Ruijie# configure terminal	进入全局配置模式。
Ruijie(config)# **mac-auth-bypass direct-site** *ip-address* [*ip-mask*][dport port-num] [arp]	配置多 MAB 直通。 如果不配置 ip 地址的掩码，则默认为 255.255.255.255。 如果直通地址需要限制四层目的端口号，可以使用配置四层目的端口号，这时能够匹配的报文仅限于 TCP/UDP 报文，不配置则默认不限制四层目的端口号，这时能够匹配的报文为 IPv4 报文。 如果接入/汇聚设备启用了 ARP CHECK 功能或者使用了自动获取客户端功能，那么需要对免认证的网络资源范围进行 ARP 绑定，需要配置 arp 关键字。默认不进行 arp 绑定。
Ruijie(config)#**show running-config**	显示所有配置。

如果要取消设置免认证的网络资源，在全局配置模式下，使用 **no mac-auth-bypass direct-site** {*ip-address* [*ip-mask*][dport port-num] }。

下面的例子显示了如何配置多 MAB 直通功能：

```
Ruijie# configure terminal
Ruijie(config)# mac-auth-bypass direct-site 172.18.1.0 255.255.255.0
Ruijie(config)# mac-auth-bypass direct-site 172.18.1.1
Ruijie(config)# mac-auth-bypass direct-site 172.18.1.2 dport 80
Ruijie(config)# mac-auth-bypass direct-site 172.18.1.3 arp
Ruijie(config)# end
```

☑ S5750S 交换机产品支持多 MAB 直通，其他产品可以使用 http 免认证资源配置来实现功能；

🕮 如果需要放行 http 重定向地址，则需要将该地址显式地配置为多 MAB 直通；

命中多 MAB 直通表项的报文将绕过接入控制（DOT1X 认证、WEB 认证、全局 IP_MAC 绑定、IP SOURCE GUARD）、基于 ACL 的应用（安全 ACL、DOT1X 下发 ACL、PBR 策略路由、基于流的 QoS 限速、灵活 QinQ）；

4.2.45 配置DOT1X和多MAB优先级管理功能

端口同时开启 DOT1X 认证和多 MAB 认证时，默认优先级时 DOT1X 高于 MAB，也就是说 MAB 认证过程中，如果收到 EAPOL 报文，会停止 MAB 认证过程，然后进行 DOT1X，如果已经通过 MAB 认证在线了，收到 EAPOL 报文，MAB 用户也会下线，然后进行 DOT1X 认证。但在一些情况下，某些软件会触发系统发出 EAPOL 报文，导致已经 MAB 在线的用户掉线，而 DOT1X 又没法认证成功，影响用户使用网络。因此，为了处理这种情况，增加一个 DOT1X 和多 MAB 共用时的认证顺序和优先级管理机制，开启该功能时，用户先进行 DOT1X 认证，如果 DOT1X 认证失败，则进行 MAB 认证，同时 MAB 的优先级比 DOT1X 高，即 MAB 认证过程中和在线过程中，收到 EAPOL 报文会直接丢弃，保证 MAB 用户稳定在线。

通过如下的步骤配置启用 DOT1X 和多 MAB 优先级管理功能：

命令	作用
Ruijie(config)**#interface** *interface-id*	进入接口模式
Ruijie(config-if)**#dot1x auth-with-order**	配置开启 DOT1X 与 MAB 优先级管理功能
Ruijie**#show running-config**	显示所有配置

下面的例子显示了如何配置 DOT1X 和多 MAB 优先级管理功能：

```
Ruijie# configure terminal
Ruijie(config)# interface fa 0/1
Ruijie(config-if)# dot1x port-control auto
Ruijie(config-if)# dot1x mac-auth-bypass multi-user
Ruijie(config-if)# dot1x auth-with-order
```

DOT1X 与多 MAB 优先级管理只支持基于 MAC 认证模式，而且是在开启多 MAB 时才允许配置，如果开启后直接关闭多 MAB，DOT1X 与多 MAB 优先级管理功能同时关闭。

如果已经有用户在线，然后再开启 DOT1X 与多 MAB 优先级管理功能，该端口下原来在线用户会被踢下线。

DOT1X 与多 MAB 优先级管理功能与 FAIL VLAN 功能共用时，原有尝试服务器 Reject 一定次数才进行 FAIL VLAN 授权将失效，DOT1X 与 MAB 认证都是失败时即会尝试 FAIL VLAN 授权。

4.2.46 配置SYSLOG限速功能

DOT1X/MAB 用户成功、失败等情况下会输出相关 SYSLOG，为了避免因为 SYSLOG 太多消耗设备资源，从而影响到其他正常业务的运行，默认对 SYSLOG 的输出数量做了限制，默认每秒最多打印 5 条，超过的不输出，具体条数可以配置，如果配置为 0，表示不限制数量，要谨慎配置。

通过如下的步骤配置 SYSLOG 限速功能：

命令	作用
Ruijie(config)**#dot1x logging rate-limit** *[num]*	全局模式配置每秒打印 syslog 的最大条数
Ruijie**#show running-config**	显示所有配置

下面的例子显示了配置每秒最多输出一条 SYSLOG：

```
Ruijie# configure terminal
Ruijie(config)# dot1x loggin rate-limit 1
```

4.3 查看 802.1x 的配置及当前的统计值

本公司实现的 802.1X 可以查看丰富的状态机信息，为网管提供了强有力的管理依据，便于管理员对用户状态的时时监控，且方便解决故障。

- 查看 Radius 认证及记帐相关配置
- 查看当前的用户数
- 查看可认证地址列表
- 查看用户认证状态信息
- 查看 1x 客户端探测定时器设置
- 802.1X 端口动态 VLAN 自动跳转配置实例

4.3.1 查看Radius 认证及记帐相关配置

用 **show radius server** 命令查看 Radius Server 的相关配置，用 **show aaa user** 查看用户相关信息

```
Ruijie# show radius server
Server IP:         192.168.5.11
Accounting Port:   1813
Authen  Port:      1812
Server State:      Ready
```

4.3.2 查看当前的用户数

本公司实现的 802.1X 可以查看两类当前的用户数，一是当前用户数，二是已认证用户数。当前用户数指的是当前认证用户总数（无论是否认证成功）；已认证用户数，指的是已认证通过的用户的总数。

在特权模式下，查看当前用户数及已认证用户数，查看 1x 配置，包括当前用户数和已认证用户数使用 **show dot1x**。

以下例子是查看 802.1x 配置：

```
Ruijie# show dot1x
802.1X Status:         Disabled
Authentication Mode:   EAP-MD5
Authed User Number:    0
Re-authen Enabled:     Disabled
Re-authen Period:      3600 sec
Quiet Timer Period:    10 sec
Tx Timer Period:       3 sec
Supplicant Timeout:    3 sec
```

```
Server Timeout:       5 sec
Re-authen Max:        3 times
Maximum Request:      3 times
Filter Non-RG Supp:   Disabled
Client Oline Probe:   Disabled
Eapol Tag Enable:     Disabled
Authorization Mode:   Disabled
MAC Move Permit:       Enabled
```

4.3.3 查看可认证地址列表

本公司实现的 802.1x，对功能进行了扩展，可以设置在某些端口上只有哪些主机可以认证。查看可认证主机列表功能，可以让管理员查看目前已有的设置。

在特权模式下，按如下操作查看可认证主机列表

命令	作用
Ruijie(config)**#dot1x auth-address-table address** *mac-addr* **interface** *interface*	配置可认证主机列表
Ruijie**#show dot1x auth-address-table**	查看可认证主机列表

使用 no dot1x auth-address-table address 命令删除指定的可认证主机列表。以下例子是查看可认证主机列表：

```
Ruijie# show dot1x auth-address-table
interface:g3/1
-----------------------------------
mac addr: 00D0.F800.0001
```

4.3.4 查看用户认证状态信息

管理员可以查看本设备的当前用户的认证状态，便于排解故障。

在特权模式下，按如下操作查看用户认证状态信息。

命令	作用
show dot1x summary	查看用户认证状态信息

以下例子是查看用户认证状态信息：

```
Ruijie# show dot1x summary
ID   MAC  Interface  VLAN  Auth-State  Backend-State Port-Status
---------- --------- ----------  ------------ -----------
1   00d0f8000001 Gi3/1     1   Authenticated  IDLE       Authed
```

4.3.5 查看 1x 客户端探测定时器设置

在特权模式下，按如下操作查看 1x 定时器设置。

命令	作用
show dot1x probe-timer	查看 1x 定时器设置

以下例子是查看 1x 定时器设置:

```
Ruijie# show dot1x probe-timer
Hello Interval: 20 Seconds
Hello Alive: 250 Seconds
```

4.3.6 查看多MAB直通信息

在特权模式下，按如下操作查看多 MAB 直通信息。

命令	作用
show mac-auth-bypass direct-site	查看多 MAB 直通信息。

以下例子是查看多 MAB 直通信息:

```
Ruijie# show mac-auth-bypass direct-site
Mac-auth-bypass direct-site:
  Address          MASK             DPORT ARP Binding
  ---------------- ---------------- ----- -----------
  172.18.1.0       255.255.255.0          Off
  172.18.1.1       255.255.255.255        Off
  172.18.1.2       255.255.255.255  80    Off
  172.18.1.3       255.255.255.255        On
```

4.3.7 802.1X端口动态VLAN自动跳转配置实例

在某个学校中有三个类型的用户组，如下：

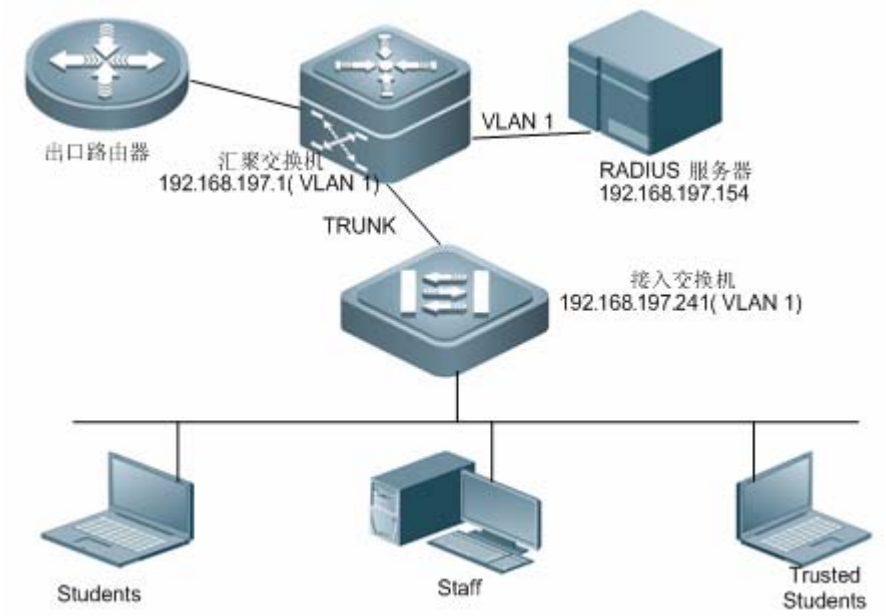
- 学生；
- 可信任的学生（如学生干部）；
- 教职工。

基本需求如下：

- 以上三个用户组中每个成员能够连接到接入设备的任意端口，并及时转入与所在用户组相应的 VLAN 中。
- 在三个用户组所在 VLAN 之间实现完全的数据隔离，即一个组的成员不能和另一个组的成员数据交换。

网络拓扑如下：

图 4-11 典型动态 VLAN 自动跳转拓扑



以下为配置实例

1) 配置 RADIUS 服务器

添加可管理接入设备 192.168.197.241，该设备使用默认认证记账端口 1812 和 1813，共享密码为 shared。

配置用户组 students 相关用户下发的 vlan

- Tunnel-Type = "VLAN",
- Tunnel-Medium-Type = "IEEE-802",
- Tunnel-Private-Group-ID = "students"

配置用户组 trusted_students 相关用户下发的 vlan

- Tunnel-Type = "VLAN",
- Tunnel-Medium-Type = "IEEE-802",
- Tunnel-Private-Group-ID = "trusted_students"

配置用户组 staff 相关用户下发的 vlan

- Tunnel-Type = "VLAN",
- Tunnel-Medium-Type = "IEEE-802",
- Tunnel-Private-Group-ID = "staff"

2) 配置接入交换机

- 打开 AAA 开关

```
configure terminal
aaa new-model
```

- 配置 RADIUS 服务器

```
configure terminal
radius-server host 192.168.197.154
radius-server key shared
```

- 配置方法列表

```
configure terminal
aaa authentication dot1x default group radius
aaa accounting network default start-stop group radius
```

- 802.1X 选择方法列表

```
configure terminal
dot1x authentication default
dot1x accounting default
```

- 接口使能 802.1X 认证

```
configure terminal
interface range fastEthernet 0/1-48
dot1x port-control auto
```

- 接口使能 VLAN 自动跳转功能

```
configure terminal
interface interface_id
dot1x dynamic-vlan enable
```

- 创建用户认证后 VLAN

```
configure terminal
vlan 2
name students
vlan 3
name trusted_students
vlan 4
name staff
```

- 创建接入设备管理 IP

```
configure terminal
interface vlan 1
ip address 192.168.197.241 255.255.255.0
```

至此完成方案配置，能够满足用户需求。

4.4 配置 802.1x其它注意事项

- 1X 和 ACL 同时应用

在非 IP 授权模式下，如果您打开某一个端口的 802.1x 认证功能，又将某一个 ACL 关联到某一个接口。则 ACL 在 MAC 地址的基础上生效。也就是说，只有源 MAC 为认证通过的用户 MAC 的报文才会经过 ACL 过滤，其它源 MAC 地址报文被丢弃，ACL 只能在该 MAC 地址的基础上进行限制。

比如，认证通过的 MAC 地址为 00d0.f800.0001，则所有源 MAC 为 00d0.f800.0001 的报文可以交换。如果该端口再关联 ACL，则 ACL 在这些能够交换的报文基础上将进一步过滤。如拒绝源 MAC 为该地址的 ICMP 报文。

- 对认证端口的限制说明：

端口模式不能修改，例如使用命令 **switchport mode trunk**；

端口在 ACCESS 模式下不能修改端口 Access VLAN；

端口在 TRUNK 模式下不能修改端口 Allowed VLAN 及 Native VLAN；

端口不能从 AP 口退出或者加入 AP 口；

- 在 VLAN 中有用户正在进行认证或有已经认证成功用户情况下的限制说明：

VLAN 不能删除；

VLAN 的类型不能修改，例如使用命令 **private-vlan primary**。

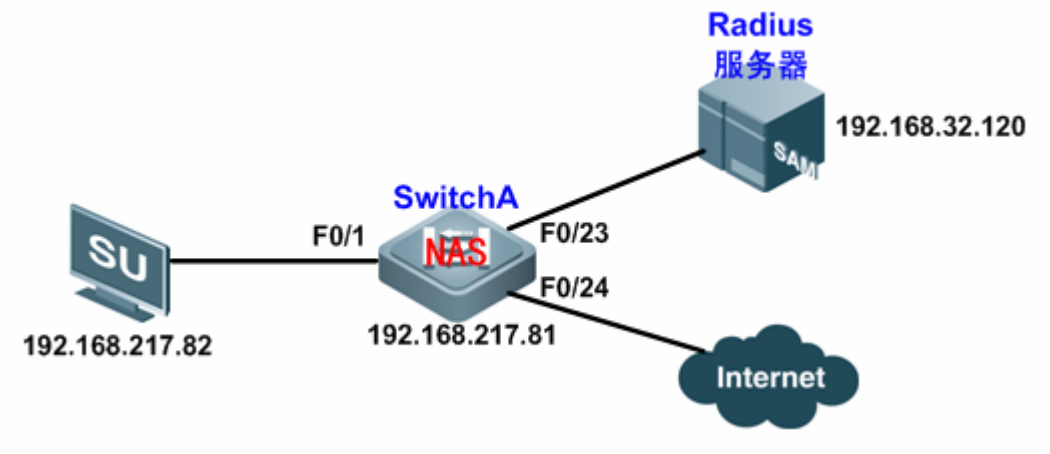
- GVRP 不能和动态 VLAN 自动跳转功能同时使用。
- 802.1x 可以和其他接入控制功能比如端口安全，IP+MAC 绑定等共用。当这些接入控制功能共用时，报文必须同时满足所有的接入控制才可以进入交换机。
- Trunk 口、Hybrid 口上由于 VLAN 跳转功能生效（如：GUEST VLAN、FAIL VLAN、VLAN 下发、服务器失效旁路认证跳转 VLAN），修改了端口的 Native VLAN 后，会导致该端口上其它 VLAN 的用户未经授权也能访问网络。因此，建议上述的 VLAN 跳转功能仅在 Access 口上开启。
- 在 Aggregate Port 口上开启受控功能之后，建议不要开启 dot1x redirect 命令，否则会导致该 Aggregate Port 口受控失败。

4.5 802.1X典型配置用例

4.5.1 基于 802.1X的AAA服务

拓扑图

图 4-12 基于 802.1X 的 AAA 服务拓扑图



应用需求

为了保证设备访问网络的合法性，需要满足如下要求：

- 要求在各端口上对接入用户进行 1X 认证，控制其访问 Internet（未认证通过的用户无法访问网络）；
- 只允许使用我司的客户端（supplicant 产品）做为 802.1x 认证的客户端；
- 要求基于时长记账，定时向 Radius Server 发送计费更新包（设备每 15 分钟向 RADIUS 服务器发送一次实时计费报文）；
- 设备在向 RADIUS 服务器发出认证请求后若 5 秒种内没有得到响应就向其重新发送报文，发送报文的次数总共为 6 次；
- 实现用户在线监测，即防止已通过认证的用户不会被其他用户冒用，检测用户是否断线；
- 为避免服务器收到恶意攻击，要求用户认证失败后，500 秒内才允许再次认证。同时在认证次数超过 5 次之后，将认定该用户已经断线，结束认证过程。

配置要点

- 开启 AAA 开关，配置设备与 RADIUS SERVER 之间的通讯；配置 802.1X 认证，同时设置接入客户端的设备端口为受控口（本例以 F0/1 口为例）；（对应“应用需求”的第 1 点）
- 打开过滤非我司 supplicant 功能的开关；（对应“应用需求”的第 2 点）
- 配置 802.1x 记帐，同时配置记帐计费更新功能，并配置计费更新包的周期；（对应“应用需求”的第 3 点）
- 配置 Radius Server 的最大响应时间为 5s，同时配置报文重传次数为 6 次；（对应“应用需求”的第 4 点）
- 配置设备的定时重认证功能；（对应“应用需求”的第 5 点）
- 配置用户认证失败时的 Quiet Period 值为 500s（设备等待时间），同时配置设备的最大重认证次数为 5 次。（对应“应用需求”的第 6 点）

配置步骤

第一步，配置 Radius Server 的相关属性：

1) 登陆 SAM 安全计费管理系统，点击“系统管理”—>“设备管理”，添加 NAS 设备的信息。几个必选项配置例如“设备 IP”为 192.168.217.81，“设备组”为 haha，“设备类型”为交换机，“具体型号”为 S21XX 及以后，“设备 key“为 ruijie,.“读写 Community”为 weilin，“ 设备超时时间(秒)”为 3s。如下所示：

图 4-13

设备			
* 设备IP	192.168.217.81	* 设备组	haha
* 设备类型	交换机	* 具体型号	S21XX及以后
* 设备Key	ruijie	* 读写Community	weilin
设备名称	S3760	设备位置	
* 设备超时时间(秒)	3	设备静默时间(秒)	
设备功能	□ 重认证 □ 记账更新 □ 客户端检测 □ Web认证		
地区	(根据设备IP范围划分)	地区	(根据Web认证接入设备IP范围划分)
联动端口		描述	

2) 点击“用户管理”—>“用户管理”，添加一个用户信息。几个必选项配置如“用户名”为 qq，“密码”为 1234567，“用户组”为 ceshi。如下所示：

图 4-14

基本信息			
* 用户名	qq	用户姓名	
* 密码	******	* 密码确认	******
* 用户组	ceshi	账户	qq
用户模板	自定义模板 模板: ceshi 计费策略: 1元1s		
用户自助权限	所有自助权限	免服务校验	需要校验
自动预销户时间		BACL	
账户余额	0.00		
用户状态	正常	暂停时间	
上次自助暂停时间		下次可自助暂停时间	无限制

第二步，配置接入交换机 SwitchA：

！ 开启 AAA 开关

```
Ruijie(config)#aaa new-model
```

！ 配置 RADIUS 服务器

```
Ruijie(config)#radius-server host 192.168.32.120
```

！ 配置 RADIUS Key

```
Ruijie(config)#radius-server key ruijie
```

！ 配置 dot1x 认证方法列表

```
Ruijie(config)#aaa  authentication dot1x hello group radius
```

！ 应用 dot1x 认证方法列表

```
Ruijie(config)#dot1x authentication hello
```

！ 配置 F0/1 为受控口（打开接口认证功能）

```
Ruijie(config)#interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)#dot1x port-control auto
Ruijie(config-if-FastEthernet 0/1)#exit
```

！ 打开过滤非我司 supplicant 功能的开关

```
Ruijie(config)#dot1x private-supplicant-only
```

！ 配置 802.1X 记账方法列表

```
Ruijie(config)#aaa accounting network jizhang start-stop group radius
```

！ 为 802.1X 应用记账方法列表

```
Ruijie(config)#dot1x accounting jizhang
```

！ 配置记帐计费更新功能

```
Ruijie(config)#aaa accounting update
```

！ 配置记账计费更新周期为 15 分钟

```
Ruijie(config)#aaa accounting update periodic 15
```

！ 配置 RADIUS 服务器的最大响应时间为 5s

```
Ruijie(config)#dot1x timeout server-timeout 5
```

！ 配置报文重传次数为 6 次

```
Ruijie(config)#dot1x max-req 6
```

！ 打开定时重认证功能

```
Ruijie(config)#dot1x re-authentication
```

！ 设置重认证时间间隔为 1000s

```
Ruijie(config)#dot1x timeout re-authperiod 1000
```

！ 设置设备的 Quiet Period 值为 500s

```
Ruijie(config)#dot1x timeout quiet-period 500
```

！配置设备的最大重认证次数为 5 次。

```
Ruijie(config)#dot1x reauth-max 5
```

！ 配置设备的缺省路由

```
Ruijie(config)#ip route 0.0.0.0 0.0.0.0 192.168.217.1
```

！ 配置设备的 ip 地址

```
Ruijie(config)#interface vlan 1
Ruijie(config-if-VLAN 1)#ip address 192.168.217.81 255.255.255.0
```

第三步，使用认证客户端（如 supplicant）进行认证，输入正确的用户名和密码，选择好网卡，经过几秒钟后，客户端认证成功。

配置验证

第一步，查看设备当前用户的认证状态信息，便于排解故障。

```
Ruijie#show dot1x summary
ID        MAC       Interface VLAN   Auth-State    Backend-State Port-Status User-Type
-------- --------------  --------- ---- --------------- ------------- ----------- ---------
1        00d0.f864.6909  Fa0/1     1    Authenticated   Idle          Authed      static
```

第二步，查看已认证用户的认证详细信息：

```
Ruijie#show dot1x user id 1

User name: qq
User id: 1
Type: static
Mac address is 00d0.f864.6909
Vlan id is 1
Access from port Fa0/1
Time online: 0days 0h 2m24s
User ip address is 192.168.217.82
Max user number on this port is 6000
Authorization session time is 20736000 seconds
Supplicant is private
Start accounting
Permit proxy user
Permit dial user
IP privilege is 0
 user acl-name qq_1_0_0 :
```

第三步，查看当前的用户数及已认证用户数的 1X 配置：

```
Ruijie#show dot1x

802.1X Status:        enable
Authentication Mode:  eap-md5
Total User Number:    1(exclude dynamic user)
Authed User Number:   1(exclude dynamic user)
Dynamic User Number:  0
Re-authen Enabled:    enable
Re-authen Period:     1000 sec
Quiet Timer Period:   500 sec
Tx Timer Period:      3 sec
Supplicant Timeout:   3 sec
Server Timeout:       5 sec
```

```
Re-authen Max:          5 times
Maximum Request:        6 times
Private supplicant only:    enable
Client Online Probe:    disable
Eapol Tag Enable:       disable
Authorization Mode:     disable
```

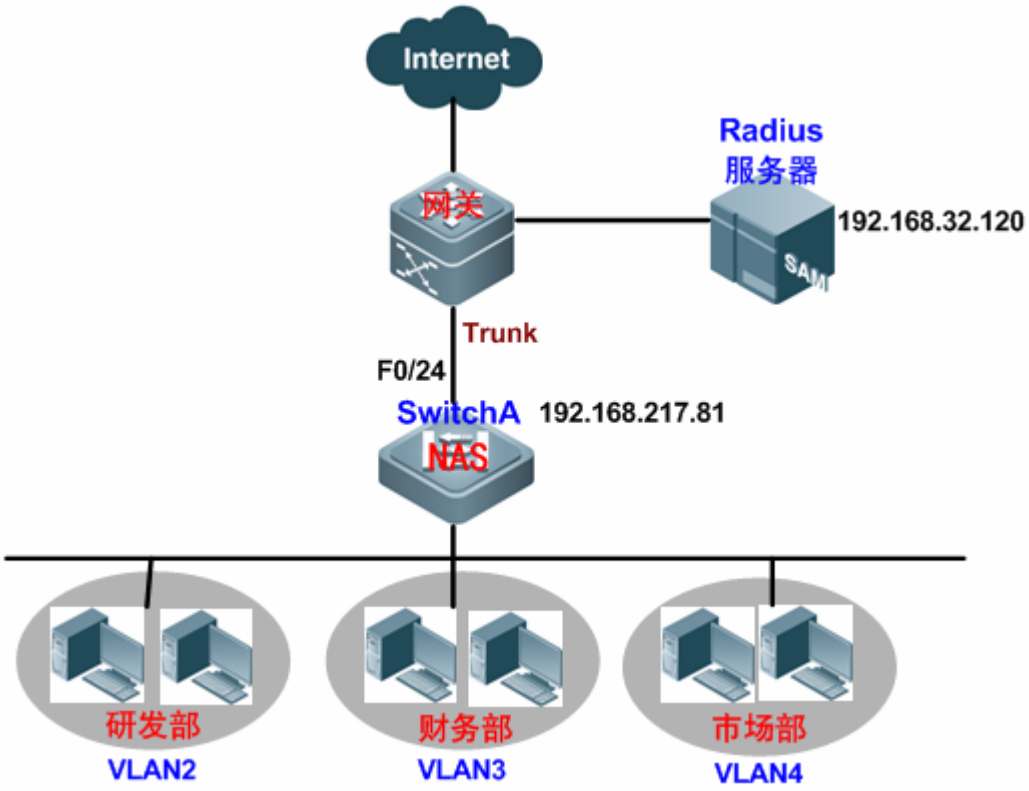
第四步，查看 Radius 认证及记帐相关配置：

```
Ruijie#show radius server

Server IP:     192.168.32.120
Accounting Port:   1813
Authen  Port:      1812
Server State:      ready
```

4.5.2 802.1X端口动态VLAN自动跳转应用

拓扑图

图 4-15 802.1X 端口动态 VLAN 自动跳转应用拓扑图



应用需求

在某个企业有三个类型的用户组，他们分别为研发部（development），财务部（finance），市场部（market）。要求满足下述需求：

1) 三个用户组中每个成员能够连接到接入设备的任意端口，并在认证通过后及时转入与所在用户组相应的 VLAN 中（研发部转入 VLAN2，财务部转入 VLAN3，市场部转入 VLAN4）

2) 在三个用户组所在 VLAN 之间实现完全的数据隔离，即一个组的成员不能和另一个组的成员进行数据交换。

配置要点

- 开启 AAA 开关，配置设备与 RADIUS SERVER 之间的通讯；
- 配置 802.1X 认证，同时设置接入客户端的设备端口为受控口
- 在相应接口使能 VLAN 自动跳转功能
- 创建用户认证后 VLAN 及 VLAN 名

配置步骤

第一步，配置 Radius Server 的相关属性（下述描述本例重点需要配置的点，其他的不再赘述）：

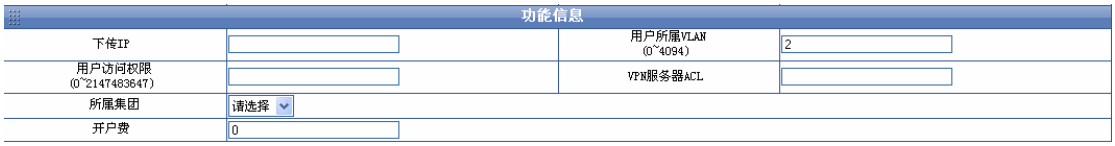
1) 点击“用户管理”—>“用户组管理”，添加相应的用户组（以 development 用户组为例）,如下所示：

图 4-16

2) 点击“用户管理”—>“用户管理”，添加相应用户的基本信息及下传 VLAN 信息（以 development 用户组为例，用户所属 VLAN 设置为 2），如下所示：

图 4-17

图 4-18



第二步，配置接入交换机 SwitchA：

！ 开启 AAA 开关

```
Ruijie(config)#aaa new-model
```

！ 配置 RADIUS 服务器

```
Ruijie(config)#radius-server host 192.168.32.120
```

！ 配置 RADIUS Key

```
Ruijie(config)#radius-server key ruijie
```

！ 配置 dot1x 认证方法列表

```
Ruijie(config)#aaa  authentication dot1x hello group radius
```

！ 应用 dot1x 认证方法列表

```
Ruijie(config)#dot1x authentication hello
```

！ 配置 802.1X 记账方法列表

```
Ruijie(config)#aaa accounting network jizhang start-stop group radius
```

！ 为 802.1X 应用记账方法列表

```
Ruijie(config)#dot1x accounting jizhang
```

！ 配置端口为受控口（打开接口认证功能）

```
Ruijie(config)#interface range fastEthernet 0/1-23
Ruijie(config-if-range)#dot1x port-control auto
```

！ 在接口使能 VLAN 自动跳转功能

```
Ruijie(config-if-range)# dot1x dynamic-vlan enable
```

！ 创建用户认证后 VLAN 和 VLAN 名

```
Ruijie(config)#vlan 2
Ruijie(config-vlan)#name development
Ruijie(config-vlan)#exit
Ruijie(config)#vlan 3
Ruijie(config-vlan)#name finance
Ruijie(config-vlan)#exit
Ruijie(config)#vlan 4
Ruijie(config-vlan)#name market
Ruijie(config-vlan)#exit
```

！ 配置上联口 F0/24 为 trunk 口。

```
Ruijie(config)#interface fastEthernet 0/24
Ruijie(config-if-FastEthernet 0/24)#switchport mode trunk
```

！ 配置设备的缺省路由

```
Ruijie(config)#ip route 0.0.0.0 0.0.0.0 192.168.217.1
```

！ 配置设备的 ip 地址

```
Ruijie(config)#interface vlan 1
Ruijie(config-if-VLAN 1)#ip address 192.168.217.81 255.255.255.0
```

第三步，使用客户端进行认证上线。认证成功后可以看到 CLI 界面显示“%DOT1X-4-TRANS_AUTHOR: Setting interface FastEthernet 0/1 author-vlan 2 succeeded.”

此时可以看到用户认证自动跳转到 VLAN2 中。

配置验证

第一步，查看设备当前用户的认证状态信息，可以从中看出用户真实所在 VLAN。

```
Ruijie#show dot1x summary
    ID         MAC       Interface VLAN   Auth-State    Backend-State Port-Status User-Type
-------- --------------  --------- ---- --------------- ------------- ----------- ---------
5        00d0.f864.6909  Fa0/1     2    Authenticated   Idle          Authed      static
```

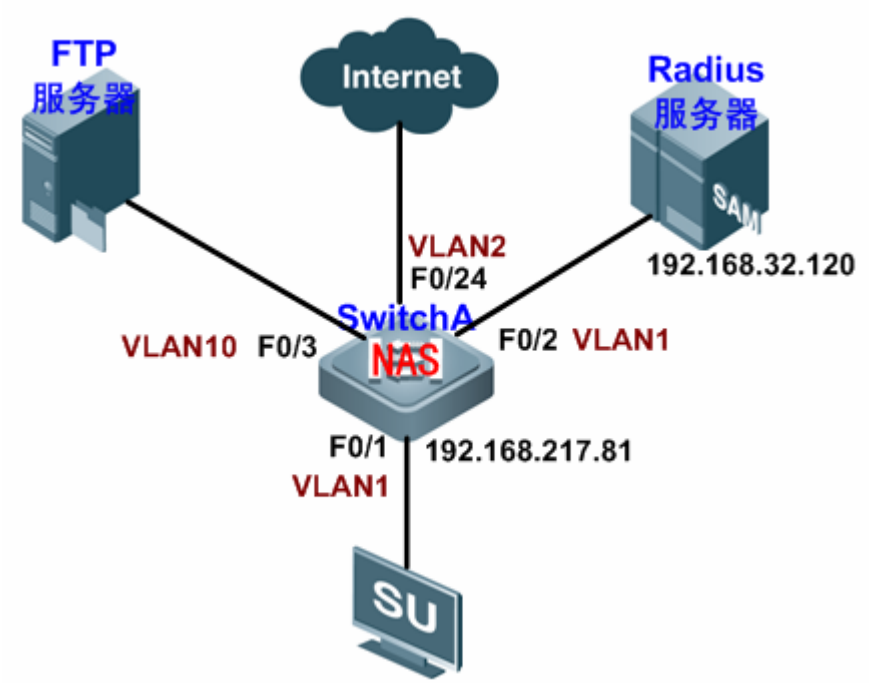
第二步，查看已认证用户的认证详细信息：

```
Ruijie#show dot1x user id 5

User name: st
User id: 5
Type: static
Mac address is 00d0.f864.6909
Vlan id is 2
Access from port Fa0/1
Time online: 0days 0h 4m35s
User ip address is 192.168.217.82
Max user number on this port is 6000
Authorization vlan is 2
Authorization session time is 20731685 seconds
Supplicant is private
Start accounting
Permit proxy user
Permit dial user
IP privilege is 0
 user acl-name st_1_0_0 :
```

4.5.3 802.1X端口Guest VLAN及VLAN下发应用

拓扑图

图 4-19 802.1X 端口 Guest VLAN 及 VLAN 下发应用拓扑图



应用需求

客户端通过 802.1x 认证接入网络，认证服务器为 RADIUS 服务器，FTP Server 是用于客户端进行相关软件下载和补丁升级的服务器，其在 VLAN10 内。Radius Server 用于认证授权记账及动态 VLAN 下发，其在 VLAN1 中，交换机连接 Internet 网络的端口（F0/24）在 VLAN2 中。要求满足如下需求：

1) 当交换机从端口发送触发认证报文（EAP-Request/Identity）超过设定的最大次数而没有收到任何回应报文后，F0/1 被加入 Guest VLAN（VLAN10）中，此时 Supplicant 和 FTP Server 都在 VLAN10 内，Supplicant 可以访问 FTP Server 并下载 802.1x 客户端。

2) 当用户认证成功上线，RADIUS 服务器下发 VLAN2。此时 Supplicant 和 F0/24 都在 VLAN2 内，Supplicant 可以访问 Internet 上网。

配置要点

- 开启 AAA 开关，配置设备与 RADIUS SERVER 之间的通讯；
- 配置 802.1X 认证，同时设置接入客户端的设备端口为受控口
- 在相应接口使能 VLAN 自动跳转功能
- 在相应接口上配置是否允许 guest vlan 功能

配置步骤

配置接入交换机 SwitchA：

！ 配置端口所属的 VLAN 信息：

```
Ruijie(config)#interface fastEthernet 0/3
Ruijie(config-if-FastEthernet 0/3)#switchport access vlan 10
Ruijie(config-if-FastEthernet 0/3)#exit
Ruijie(config)#interface fastEthernet 0/24
Ruijie(config-if-FastEthernet 0/24)#switchport access vlan 2
Ruijie(config-if-FastEthernet 0/24)#exit
```

！ 开启 AAA 开关

```
Ruijie(config)#aaa new-model
```

！ 配置 RADIUS 服务器

```
Ruijie(config)#radius-server host 192.168.32.120
```

！ 配置 RADIUS Key

```
Ruijie(config)#radius-server key ruijie
```

！ 配置 dot1x 认证方法列表

```
Ruijie(config)#aaa  authentication dot1x hello group radius
```

！ 应用 dot1x 认证方法列表

```
Ruijie(config)#dot1x authentication hello
```

！ 配置 802.1X 记账方法列表

```
Ruijie(config)#aaa accounting network jizhang start-stop group radius
```

！ 为 802.1X 应用记账方法列表

```
Ruijie(config)#dot1x accounting jizhang
```

！ 配置端口为受控口（打开接口认证功能）

```
Ruijie(config)#interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)#dot1x port-control auto
```

！ 在接口使能 VLAN 自动跳转功能

```
Ruijie(config-if-FastEthernet 0/1)# dot1x dynamic-vlan enable
```

！ 在接口配置允许 GUEST VLAN 跳转

```
Ruijie(config-if-FastEthernet 0/1)#dot1x guest-vlan 10
```

！ 配置设备的缺省路由

```
Ruijie(config)#ip route 0.0.0.0 0.0.0.0 192.168.217.1
```

！ 配置设备的 ip 地址

```
Ruijie(config)#interface vlan 1
```

```
Ruijie(config-if-VLAN 1)#ip address 192.168.217.81 255.255.255.0
```

配置验证

第一步，发送一定数量的认证报文（EAP-Request/Identity），超过设定的最大次数而没有收到任何回应报文后，端口下用户自动跳转到 VLAN10，从 CLI 界面上可以看到如下提示：

```
%DOT1X-5-TRANS_DEFAULT_TO_GUEST: Transformed interface FastEthernet 0/1 from default-vlan 1 to guest-vlan 10 ok.
```

第二步，用户下载 802.1x 客户端，认证通过后，从 CLI 界面上看到打印如下信息提示：

```
%DOT1X-4-TRANS_AUTHOR: Setting interface FastEthernet 0/1 author-vlan 2 succeeded.
```

1、查看设备当前用户的认证状态信息：

```
Ruijie#show dot1x summary
    ID         MAC       Interface VLAN   Auth-State    Backend-State Port-Status User-Type
-------- --------------  --------- ---- --------------- ------------- ----------- ---------
8        00d0.f864.6909  Fa0/1     2    Authenticated   Idle          Authed      static
```

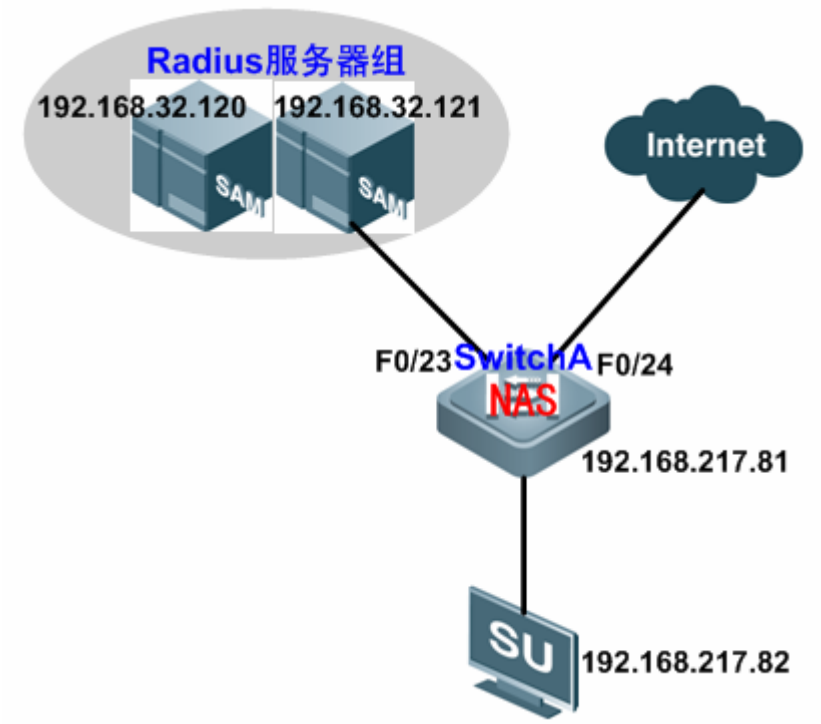
2、查看已认证用户的认证详细信息：

```
Ruijie#show dot1x user id 8

User name: st
User id: 8
Type: static
Mac address is 00d0.f864.6909
Vlan id is 2
Access from port Fa0/1
Time online: 0days 0h 4m25s
User ip address is 192.168.201.56
Max user number on this port is 6000
Authorization vlan is 2
Authorization session time is 20736000 seconds
Supplicant is private
Start accounting
Permit proxy user
Permit dial user
IP privilege is 0
 user acl-name st_1_0_0 :
```

4.5.4 基于端口的用户 1X认证及IP授权应用

拓扑图

图 4-20 基于端口的用户 1X 认证及 IP 授权应用拓扑图



应用需求

客户端通过 802.1x 认证接入网络，认证服务器为 RADIUS 服务器，要求满足如下应用需求：

1) 当主服务器因某种原因当机之后，设备可以将自动向方法列表服务器组下一个服务器提交认证请求。

2) 当设备商某一端口有一个用户认证通过时，所有接在此端口下的用户都能够正常的使用网络。

3) 禁止动态用户在多个认证端口之间迁移。

4) 认证用户的 IP 需要 通过 RADIUS Server 指定，即认证用户只能用 RADIUS Server 指定的 IP 访问网络。

配置要点

- 开启 AAA 开关，配置设备与 RADIUS SERVER 之间的通讯；
- 配置 802.1X 认证，同时设置接入客户端的设备端口为受控口；
- 配置主/备份服务器组
- 配置相应端口下用户认证的受控模式为基于端口认证；
- 配置禁止动态用户在端口间迁移；
- 配置 IP 授权模式为 RADIUS Server 模式；

配置步骤

配置接入交换机 SwitchA：

！ 开启 AAA 开关

```
Ruijie(config)#aaa new-model
```

！ 配置 RADIUS 服务器

```
Ruijie(config)#radius-server host 192.168.32.120
Ruijie(config)#radius-server host 192.168.32.121
```

！ 配置 RADIUS Key

```
Ruijie(config)#radius-server key ruijie
```

！ 配置服务器组（选择主服务器和备份服务器）

```
Ruijie(config)#aaa group server radius rj
Ruijie(config-gs-radius)#server 192.168.32.120
Ruijie(config-gs-radius)#server 192.168.32.121
```

！ 配置 dot1x 认证方法列表

```
Ruijie(config)#aaa  authentication dot1x hello group radius
```

！ 应用 dot1x 认证方法列表

```
Ruijie(config)#dot1x authentication hello
```

！ 配置 802.1X 记账方法列表

```
Ruijie(config)#aaa accounting network jizhang start-stop group radius
```

！ 为 802.1X 应用记账方法列表

```
Ruijie(config)#dot1x accounting jizhang
```

！ 配置端口为受控口（打开接口认证功能）

```
Ruijie(config)#interface range fastEthernet 0/1-22
Ruijie(config-if-range)#dot1x port-control auto
```

！配置相端口下用户认证的受控模式为基于端口认证

```
Ruijie(config-if-range)# dot1x port-control-mode port-based
Ruijie(config-if-range)#exit
```

！配置禁止动态用户在端口间迁移

```
Ruijie(config)#dot1x stationarity enable
```

！配置设备的 IP 授权模式为 RADIUS Server 模式

```
Ruijie(config)#aaa authorization ip-auth-mode radius-server
```

！ 配置设备的缺省路由

```
Ruijie(config)#ip route 0.0.0.0 0.0.0.0 192.168.217.1
```

！ 配置设备的 ip 地址

```
Ruijie(config)#interface vlan 1
Ruijie(config-if-VLAN 1)#ip address 192.168.217.81 255.255.255.0
```

配置验证

第一步，查看设备当前用户的认证状态信息：

```
Ruijie#show dot1x summary
    ID         MAC        Interface VLAN   Auth-State    Backend-State Port-Status User-Type
-------- --------------  --------- ---- --------------- ------------- ----------- ---------
none     00d0.f864.6909  Fa0/1     1    Authenticated   Idle          Authed      Dynamic
```

第二步，将该用户迁移到其他已认证端口，可以发现用户无法上网。

5 Web 认证

5.1 理解Web认证

5.1.1 Web认证概述

Web 认证是一种对用户访问网络的权限进行控制的身份认证方法，这种认证方法不需要用户安装专用的客户端认证软件，使用普通的浏览器软件就可以进行身份认证。

未认证用户使用浏览器上网时，接入设备会强制浏览器访问特定站点，也就是 Web 认证服务器，通常称为 Portal 服务器。用户无需认证即可享受 Portal 服务器上的服务，比如下载安全补丁、阅读公告信息等。。当用户需要访问认证服务器以外的其它网络资源时，就必须通过浏览器在 Portal 服务器上进行身份认证，只有认证通过后才可以使用网络资源。

除了认证上的便利性之外，由于 Portal 服务器和用户的浏览器有页面交互，可以利用这个特性在 Portal 服务器页面放置一些广告、通知、业务链接等个性化的服务，因此具有很好的应用前景。

5.1.2 锐捷Web认证概述

锐捷 Portal 服务器有 2 个版本，不同版本的 Web 认证流程不同，我们将其分别称为锐捷一代 Web 认证和锐捷二代 Web 认证。以下分别介绍这几个版本的技术原理。

- 由于一代 Web 认证和二代 Web 认证存在较大差异，配置参数也差别很大，因此在配置 Web 认证相关功能前必须仔细阅读本章节内容，避免配置错误。
- 锐捷二代 web 认证支持中国移动无线 portal 规范 2.2 版本，符合该标准的 portal 服务器均可以和锐捷设备对接。

5.1.2.1 锐捷一代Web认证

5.1.2.1.1 HTTP拦截

HTTP 拦截指接入设备将原本需要转发的 HTTP 报文拦截下来，不进行转发。这些 HTTP 报文是连接在接入设备下的用户的浏览器所发出的，但目的并不是接入设备本身。例如，某用户通过 IE 浏览器访问 www.google.com，接入设备本应该将这些 HTTP 请求报文转发到网关的，但如果启动 HTTP 拦截，这些报文将不被转发。

HTTP 拦截之后，接入设备需要将用户的 HTTP 连接请求转向自己，于是接入设备和用户之间将建立起连接会话。接入设备将利用 HTTP 重定向功能，将重定向页面推送给用户，用户的浏览器上将弹出一个页面，这个页面可以是认证页面，也可以是下载软件的链接等等。

在 Web 认证功能中，哪些用户所发出的到哪个目的端口的 HTTP 报文需要进行拦截，哪些不需要，都是可以设置的。一般地，未经过认证的用户发出的 HTTP 请求报文会被拦截，已通过认证的用户将不被拦截。HTTP 拦截是 Web 认证功能的基础，一旦浏览器发出的 HTTP 报文被拦截，就会自动触发 Web 认证的过程。

5.1.2.1.2 HTTP重定向

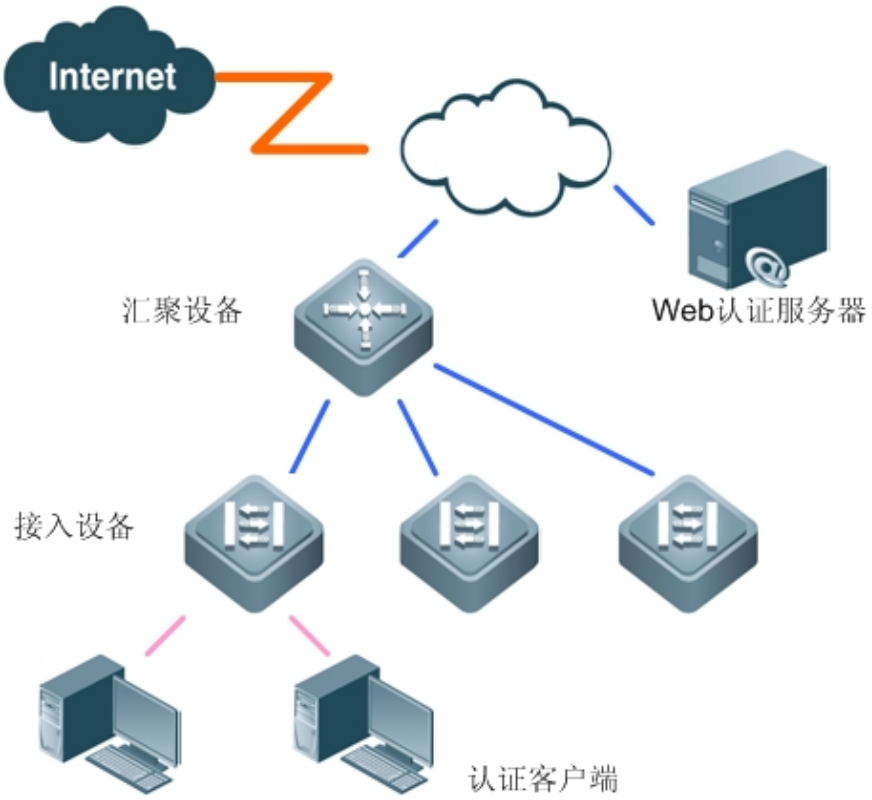
根据 HTTP 协议规定，正常情况下，用户的浏览器发出 HTTP GET 或 HEAD 请求报文后，如果接收一方能够提供资源，则以 200 报文响应，如果本地不能提供资源，则可以使用 302 报文响应。在 302 响应报文中，提供了一个新的站点路径，用户收到响应后，可以向这个新的站点重新发出 HTTP GET 或 HEAD 报文请求资源，这就是重定向。

HTTP 重定向是 Web 认证的重要环节，是发生在 HTTP 拦截之后的，利用的就是 HTTP 协议中的 302 报文的特性。HTTP 拦截过程将使得接入设备和用户之间建立起连接会话，随后用户将（本应发给其他站点的）HTTP GET 或 HEAD 报文发给接入设备，接入设备收到后，回应以 302 报文，并且在 302 报文中加入重定向页面的站点路径，这样用户将向这个站点路径重新发出请求，就会获取到重定向的页面。

5.1.3 工作原理

Web 认证的典型组网方式如下图所示，它由三个基本角色组成：认证客户端、接入设备、Portal 服务器。

图 5-1 Web 认证组网拓扑图



Web 认证的角色：

1. 认证客户端：通常是一个浏览器，运行 HTTP 协议，用户通过的浏览器上网时浏览器将发出 HTTP 请求。
2. 接入设备：在网络拓扑中一般是接入层设备与用户终端设备直接相连接，在接入设备上需要启动 Web 认证功能。

1. Portal Server：提供 Web 认证的认证界面和相关操作。Portal Server 接受认证客户端发出的基于 HTTP 的认证请求，提取其中的账号信息，将此信息发送到认证服务器进行认证，然后通告用户和接入设备认证结果。

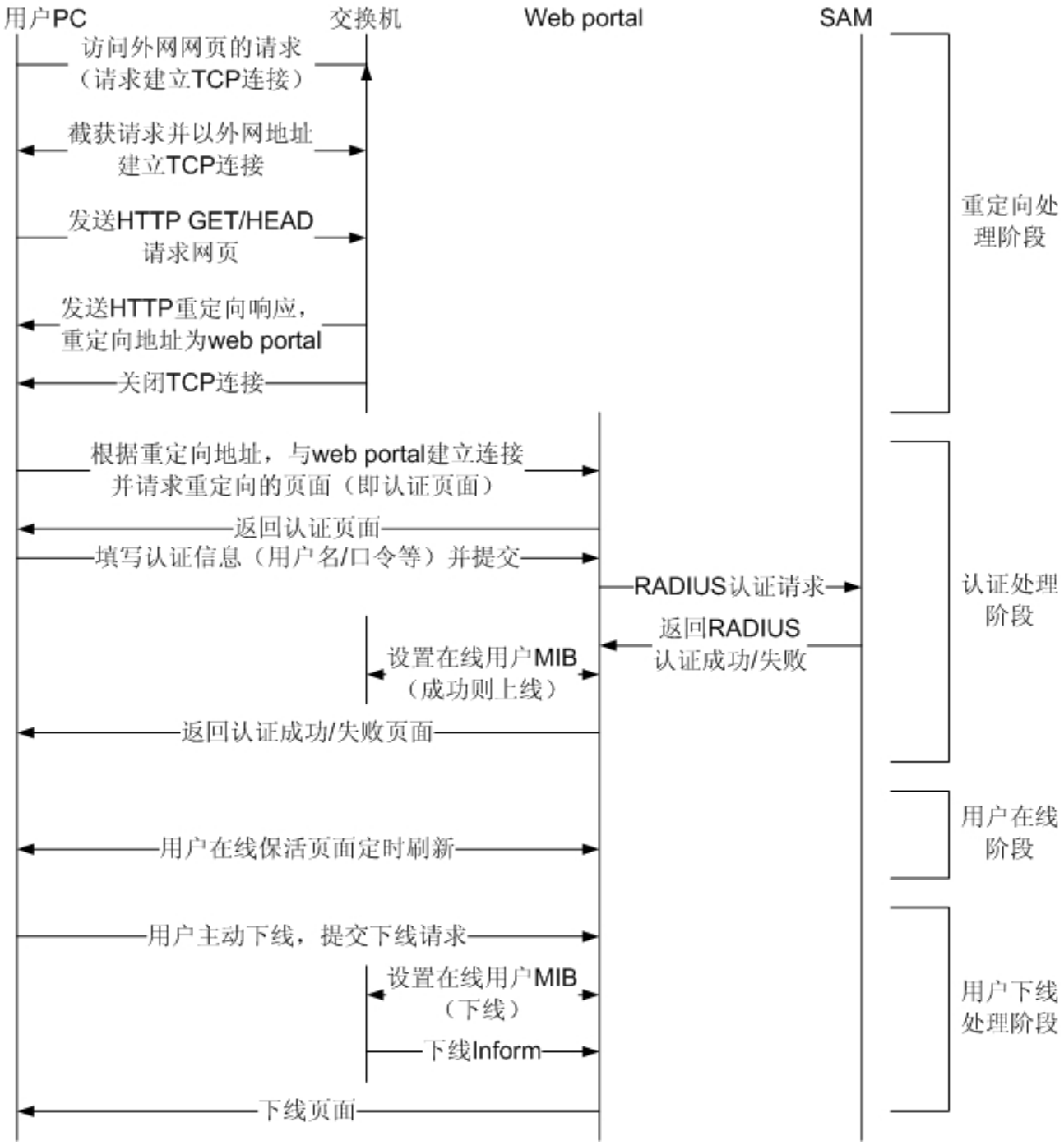
2. Radius Server：提供基于 radius 协议的远程用户认证，Portal Server 从 HTTP 中获取用户的认证账号信息，然后通过 radius 协议向 RADIUS Server 请求认证。Radius Server 通过 radius 协议向 Portal Server 反馈认证结果。

Web 认证的流程：

1. 在认证之前，接入设备将未认证用户发出的所有 HTTP 请求都拦截下来，并重定向到 Portal 服务器去，这样在用户的浏览器上将弹出一个认证页面。
2. 在认证过程中，用户在认证页面上输入认证信息（用户名、口令、校验码等等）与 Portal 服务器交互。
3. Portal 服务器和认证服务器（SAM）完成身份认证的功能。
4. 在认证通过后，Portal 服务器将通知接入设备该用户已通过认证，接入设备将允许用户访问互联网资源。

详细的原理图如下图所示：

图 5-1 锐捷一代 Web 认证流程图



用户下线流程：

用户下线分两种类型,一种是设备端检测到用户下线,比如用户时长到达,流量用完,链路断开等;一种是 Portal 服务器端发现用户下线,比如用户通过下线页面触发了下线申请,保活页面失效等。

1. 第一种情况，接入设备发现用户下线时,通告 Portal Server 用户下线，服务器设置设备删除用户信息（通过 SNMP 协议）。Portal 服务器向用户返回下线页面。

2. 第二种情况， Portal Server 发现用户下线后,通告接入设备用户下线（通过 SNMP 协议）。Portal 服务器向用户返回下线页面。

3. 2 种情况下，Portal Server 都会向 Radius Server 发起计费结束请求，通告 Radius Server 用户下线。

5.1.3.1.1 协议规范

与 HTTP 重定向相关的功能参照 HTTP 1.1 协议（RFC1945）。

与上线通告相关的通信协议参照 SNMP 协议(RFC 1157,RFC 2578)

5.1.3.2 锐捷二代Web认证

5.1.3.2.1 HTTP拦截

同锐捷一代 Web 认证的 HTTP 拦截技术。

5.1.3.2.2 HTTP重定向

同锐捷一代 Web 认证的 HTTP 重定向技术。

5.1.3.2.3 工作原理

组网拓扑图同锐捷一代 Web 认证组网拓扑图(图 1)。

Web 认证的角色：

1. 认证客户端：通常是一个浏览器，运行 HTTP 协议，用户通过浏览器上网时浏览器将发出 HTTP 请求。

2. 接入设备：在网络拓扑中一般是接入层设备，与用户终端设备直接相连接，在接入设备上需要启动 Web 认证功能。接入设备接收 Portal Server 发过来的用户认证信息，并向 Radius Server 发起认证请求，根据认证结果设置用户是否可以上网，同时向 Portal Server 反馈认证结果。

3. Portal Server：提供 Web 认证的认证界面和相关操作。Portal Server 接受认证客户端发出的基于 HTTP 的认证请求，提取其中的账号信息，将此信息发送到接入设备，同时根据接入设备反馈的认证结果，通过页面反馈给用户。

4. Radius Server：提供基于 radius 协议的远程用户认证。

Web 认证主要流程：

1. 在认证之前，接入设备将未认证用户发出的所有 HTTP 请求都拦截下来，并重定向到 Portal 服务器去，这样在用户的浏览器上将弹出一个认证页面。

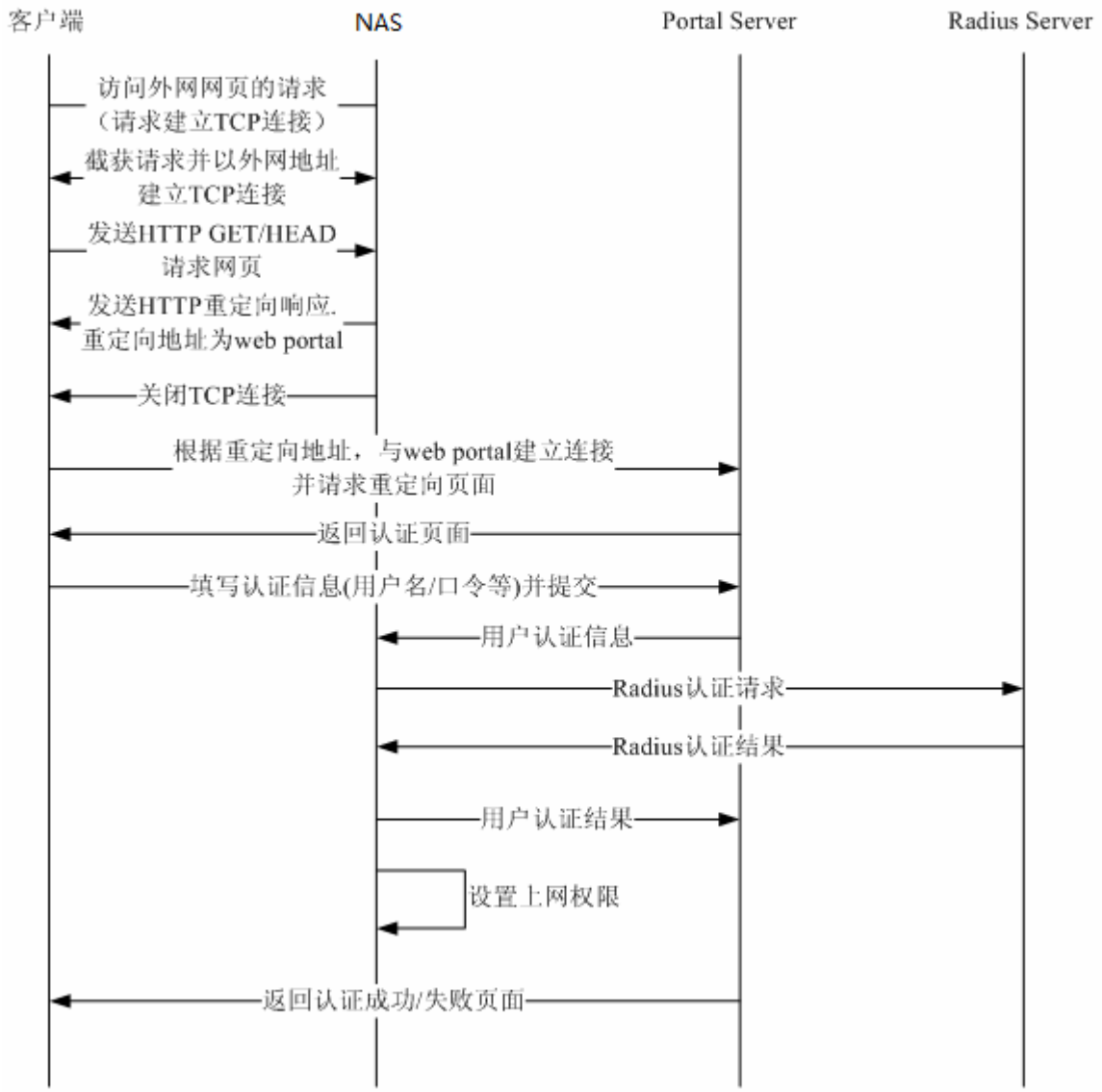
2. 在认证过程中，用户在认证页面上输入认证信息（用户名、口令、校验码等等）与 Portal 服务器交互。

3. Portal 服务器将用户的认证信息发给接入设备

4. 接入设备向 Radius Server 发起认证，并将认证结果反馈给 Portal 服务器。

5. Portal 服务器向用户返回页面，提示认证结果（成功或失败）。

锐捷二代 Web 认证流程



用户下线流程：

1. 用户下线分两种类型,一种是设备端检测到用户下线,比如用户时长到达,流量用完,链路断开等;一种是 portal 服务器端发现用户下线,比如用户通过下线页面触发了下线申请等。

2. 第一种情况，接入设备发现用户下线时,通告 Portal Server 用户下线(通过 portal 协议)，然后删除用户信息。Portal 服务器向用户返回下线页面。

3. 第二种情况， Portal Server 发现用户下线后,通告接入设备用户下线（通过 portal 协议）。Portal 服务器向用户返回下线页面。

2 种情况下，设备都会向 Radius Server 发起计费结束请求，通告 Radius Server 用户下线。

5.1.3.2.4 协议规范

与 HTTP 重定向相关的功能参照 HTTP 1.1 协议（RFC1945）。

与 radius 认证相关的功能参照 RFC2865、RFC2866。

设备和 Portal Server 间的通信协议为私有协议。

5.1.4 锐捷各类Web认证的对比

认证角色：

- 客户端：功能一样。
- 接入设备：锐捷一代 Web 认证里面，接入设备只做重定向，以及接收 Portal Server 下发的用户是否可上网的通知。锐捷二代 Web 认证里面，接入设备需要负责重定向、用户的认证、通告 Portal Server 认证是否成功。锐捷内置 portal 认证中，接入设备同时负责重定向、认证页面及其他页面的推送、用户的认证 RADIUS 客户端功能。
- Portal Server：锐捷一代 Web 认证里面，PortalServer 负责和客户端的页面交互、用户的认证、通告接入设备用户认证是否可上网。锐捷二代 Web 认证里面，Portal Server 负责和客户端的页面交互、通告接入设备用户的认证信息、接收接入设备通告的用户是否认证成功。
- Radius Server：功能一样。

认证流程：

1. 锐捷二代 Web 认证将认证从 Portal Server 迁移到接入设备，这样就降低了 Portal 服务器的压力，整体的认证性能有显著提升。
2. 锐捷二代 Web 认证由于认证在接入设备上，因此就无需等待来自 Portal Server 发送的用户是否可上网的通告。

下线流程

3. 锐捷一代 Web 认证中，计费结束报文是 Portal Server 发起的。锐捷二代 Web 认证中，计费结束报文是接入设备发起的。

实际网络中是部署一代 Web 认证，还是部署二代 Web 认证，取决于所使用的 Portal 服务器的类型。

各类 web 认证中有部分参数是可以共用，有些是不能共用的，本文档用章节分离的形式给出了区分，请仔细阅读，避免参数配置不当导致 Web 认证使用不正常。

Web 认证方案使用限制：

1）Web 认证功能只能在 FastEthernet 或 GigabitEthernet 类型接口上开启，其他类型的接口上无法开启。

2）如果一个接口是聚合口（AggregatePort）的成员，那么也不允许设置 Web 认证功能。如果一个已经开启了 Web 认证功能的接口，加入了聚合口的成员，则该接口上的 Web 认证功能将被自动关闭，该接口上已认证的用户将被清除。同时该接口的 Web 认证配置也被清除，退出聚合口后也不会自动恢复，必须重新配置。

3）如果在汇聚设备上开启 Web 认证，并且设置支持基于 VLAN 的认证，则汇聚设备与下联的接入设备连接的接口，必须是 TRUNK 模式;

4）如果在汇聚设备上开启 Web 认证，而下联的设备是三层设备（例如路由器），则汇聚设备上将不支持 IP+用户 MAC 的绑定方式，只能支持仅 IP 的绑定方式;

5）受接入设备硬件容量影响，打开 ARP CHECK 或安全通道功能，将导致可用认证用户数量减少（尤其是安全通道功能），如果以上两个功能都打开，在极端情况下可能耗尽硬件资源，Web 认证将无法进行。同时，在已开启 Web 认证的情况下，再打开上述功能时可能失败。因此不建议 Web 认证与安全通道功能共用;

6）二代 web 认证目前不支持热备，在设备主从切换的时候用户需要重新认证。

接入设备 Web 认证和 802.1x 认证共用时，需要注意:

1）在接入设备的同一个端口上，基于端口的 802.1x 认证和 Web 认证同时打开，则该端口下如果某个用户 802.1x 认证过后，其他用户的 Web 认证将不再进行，一个端口基于 MAC 的 802.1x 认证和 Web 认证同时开启，不同用户的认证方式不受影响;

2）在接入设备的同一个端口上，802.1x 认证和 Web 认证同时打开，如果先进行了 802.1x 认证，则不会再触发该 IP 用户的 Web 认证;

3）在接入设备的同一个端口上，802.1x 认证和 Web 认证同时打开，如果先进行了 Web 认证，也禁止相同 MAC 地址的用户再使用 802.1x 认证;

4）在接入设备的同一个端口上，802.1x 认证的端口动态 VLAN 跳转功能不能和 Web 认证共用;

5.2 缺省配置

下表用来描述 Web 认证的缺省配置。

功能特性	缺省值
配置 Web 认证版本	缺省使用锐捷一代 Web 认证。
配置 Portal 服务器 IP 和 URL（二代 Web 认证）	缺省无，部署二代 Web 认证时需要配置。
在端口上开启 Web 认证功能	缺省情况下关闭。
配置 Web 认证的重定向服务器 IP 地址(一代 Web 认证)	缺省情况下，设备没有配置服务器的 IP 地址。
配置 Web 认证重定向的 URL(一代 Web 认证)	缺省情况下，设备没有配置服务器的认证页面 URL。但如果有配置 IP 地址，没配置 URL，则默认使用 URL(比如：http://192.168.2.3)。
配置设备同 Portal 服务器之间的通信密钥(一代、二代 Web 认证）	缺省情况下，没有配置设备与认证服务器进行通信的密钥。
配置设备与 Portal 服务器之间的 SNMP 网管参数（一代、二代 Web 认证）	缺省情况下，设备没有配置与服务器之间的 SNMP 网管参数。
在 AAA 中配置 Web 认证的认证方法列表和几张方法列表（二代 Web 认证）	缺省情况下，AAA 中没有二代 Web 认证的认证方法列表和记账方法列表。

配置 Web 认证使用的认证方法列表（二代 Web 认证）	缺省情况使用 default 方法列表。
配置 Web 认证使用的记账方法列表（二代 Web 认证）	缺省情况使用 default 方法列表。
配置 Web 认证的在线用户记账更新时间（二代 Web 认证）	缺省情况下为 0 分钟，也即缺省不做记账更新。
配置重定向的 HTTP 端口（一代、二代 Web 认证）	缺省情况下，设备拦截用户发出的目的端口号为 80 的 HTTP 报文。
配置每个未认证用户的最大 HTTP 会话数（一代、二代 Web 认证）	缺省情况下，未认证用户的最大 HTTP 会话数为 255。
配置维持重定向连接的超时时间（一代、二代 Web 认证）	缺省情况下，维持重定向连接的超时时间为 3 秒。
配置无需认证即可直接访问的 IP（一代、二代 Web 认证）	缺省情况下，除了 Portal 服务器 IP，其它 IP 都必须认证通过才可访问。
配置已认证用户信息的更新时间间隔（一代、二代 Web 认证）	缺省情况下，设备每 180 秒更新一次在线用户的信息。
配置免认证的 IP 范围（一代、二代 Web 认证）	缺省情况下，没有设置免认证 IP，所有 IP 都必须先通过 Web 认证，才能访问网络资源。
配置流量检测功能（一代、二代 Web 认证）	缺省情况下，基于流量检测功能关闭，如果打开，则默认的检测周期 minutes 为 15 分钟，默认的检测阀值 bytes 为 0 字节。
功能特性	缺省值
配置 Web 认证版本	缺省使用锐捷一代 Web 认证。
配置 Portal 服务器 IP 和 URL（二代 Web 认证）	缺省无，部署二代 Web 认证时需要配置。
在端口上开启 Web 认证功能	缺省情况下关闭。
配置 Web 认证的重定向服务器 IP 地址(一代 Web 认证)	缺省情况下，设备没有配置服务器的 IP 地址。
配置 Web 认证重定向的 URL(一代 Web 认证)	缺省情况下，设备没有配置服务器的认证页面 URL。但如果有配置 IP 地址，没配置 URL，则默认使用 URL(比如：http://192.168.2.3)。
配置设备同 Portal 服务器之间的通信密钥(一代、二代 Web 认证）	缺省情况下，没有配置设备与认证服务器进行通信的密钥。
配置设备与 Portal 服务器之间的 SNMP 网管参数（一代、二代 Web 认证）	缺省情况下，设备没有配置与服务器之间的 SNMP 网管参数。
在 AAA 中配置 Web 认证的认证方法列表和几张方法列表（二代 Web 认证）	缺省情况下，AAA 中没有二代 Web 认证的认证方法列表和记账方法列表。
配置 Web 认证使用的认证方法列表（二代 Web 认证）	缺省情况使用 default 方法列表。
配置 Web 认证使用的记账方法列表（二代 Web 认证）	缺省情况使用 default 方法列表。
配置 Web 认证的在线用户记账更新时间（二代 Web 认证）	缺省情况下为 0 分钟，也即缺省不做记账更新。
配置重定向的 HTTP 端口（一代、二代 Web 认证）	缺省情况下，设备拦截用户发出的目的端口号为 80 的 HTTP 报文。
配置每个未认证用户的最大 HTTP 会话数（一代、二代 Web 认证）	缺省情况下，未认证用户的最大 HTTP 会话数为 255。
配置维持重定向连接的超时时间（一代、二代 Web 认证）	缺省情况下，维持重定向连接的超时时间为 3 秒。
配置无需认证即可直接访问的 IP（一代、二代 Web 认证）	缺省情况下，除了 Portal 服务器 IP，其它 IP 都必须认证通过才可访问。
配置已认证用户信息的更新时间间隔（一代、二代 Web 认证）	缺省情况下，设备每 180 秒更新一次在线用户的信息。

配置免认证的 IP 范围（一代、二代 Web 认证）	缺省情况下，没有设置免认证 IP，所有 IP 都必须先通过 Web 认证，才能访问网络资源。
配置流量检测功能（一代、二代 Web 认证）	缺省情况下，基于流量检测功能关闭，如果打开，则默认的检测周期 minutes 为 15 分钟，默认的检测阀值 bytes 为 0 字节。

5.3 配置Web认证功能开关

当前软件版本支持两种 Web 认证：

- 锐捷一代 Web 认证（缺省）。
- 锐捷二代 Web 认证。

用户可基于全局指定具体的 Web 认证版本。

如何选择版本取决于网络中使用的 Portal 服务器支持哪种版本。

要成功应用 Web 认证功能，必须按照如下顺序进行配置：

1. 配置 Web 认证所需要的必要信息，如 Portal 服务器的 IP 地址、URL 等。

1) 如果使用锐捷二代或内置 Web 认证，必须配置相应的 AAA 方法列表、RADIUS 服务器信息等。

2) 如果开启了 arpcheck 功能，必须要将网关的 arp 放行。

2. 基于端口开启 Web 认证功能。

详细配置请参见如下配置章节：

3) 配置锐捷一代 Web 认证相关参数

4) 配置锐捷二代 Web 认证相关参数

以下章节描述：

- 配置全局 Web 认证版本
- 配置启用 Web 认证功能

5.3.1 配置Web认证版本

配置 Web 认证版本。

缺省情况下，使用锐捷一代 Web 认证。若要配置全局 Web 认证版本，请按如下步骤：

命令	作用
Ruijie**# configure terminal**	进入全局配置模式。
Ruijie(config)**# web-auth portal {eportalv1 | eportalv2 }**	设置 Web 认证的版本。
Ruijie(config)**# show running-config**	查看设备的当前运行配置。

如果要恢复全局默认的 Web 认证版本，在全局配置模式下，执行 **no web-auth portal**。

配置举例：

配置使用二代 web 认证。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# web-auth portal eportalv2
Ruijie(config)# exit
```

配置何种版本取决于实际网络中部署的 Portal 服务器的支持情况。

5.3.2 配置启用Web认证功能

交换设备上 Web 认证是基于端口的，默认情况下，端口未开启 Web 认证功能，此时这个端口下所连接的用户不进行 Web 认证。

在端口上启动 Web 认证功能，将该端口设置为 Web 认证受控口，请按照如下步骤：

	命令	作用
Step 1	Ruijie**# configure terminal**	进入全局配置模式。
Step 2	Ruijie(config)**# interface** *interface-name*	进入端口的配置模式。
Step 3	Ruijie(config-if)**# web-auth port-control [ip-only-mode]**	在端口上启动 Web 认证功能。 **ip-only-mode**：（可选）默认情况下，Web 认证通过以后，需要将用户的 IP、MAC 和端口进行绑定。而当物理接口下联三层设备时，为了应对不同 IP 具有相同的 MAC 地址的情况，需要设置使用这个参数，使认证通过以后，仅将用户的 IP 和端口进行绑定。切换模式的时候，会导致该物理接口下所有的在线用户被强制下线，需要重新认证。
Step 4	Ruijie(config-if)**# show web-auth port-control**	显示端口的对应 Web 认证信息。

如果要在端口上关闭 Web 认证功能，在接口配置模式下，使用 **no web-auth port-control**。

配置举例：

在端口 *FastEthernet 0/14* 上启动 Web 认证功能。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# interface FastEthernet 0/14
Ruijie(config-if-FastEthernet 0/14)# web-auth port-control
Ruijie(config-if-FastEthernet 0/14)# show web-auth port-control
```

接入用户在 WEB 认证通过后不下线的情况下更改 IP 地址，将导致无法上网。

5.3.3 查看配置

命令	作用
show web-auth control	查看 Web 认证配置和统计信息。
show web-auth user {{{all | v1 | v2} [online-only] [start-from *index*] [*display-amount*]} **| statistics | ip-address** *ip-address* **}**	显示所有用户或是指定用户的在线信息，包括用户 IP 地址、接口、在线时间等信息。各个关键字的含义请参考 Web 认证的命令参考手册的说明。

5.4 配置锐捷一代Web认证相关参数

必须完成本章节要求的参数配置，一代 Web 认证才能正常工作。以下章节描述如何配置一代 Web 认证的相关参数：

- 配置 Portal 服务器的 IP
- 配置 Portal 服务器的认证页面 URL（可选）
- 配置设备和 Portal 服务器之间的通信密钥
- 配置设备和 Portal 服务器之间的 SNMP 网管参数

5.4.1 配置Portal服务器的IP

要成功应用锐捷一代 Web 认证，必须配置 Portal 服务器的 IP 地址。缺省情况下，设备没有配置 Portal 服务器的 IP 地址。配置步骤如下：

	命令	作用
Step 1	Ruijie**# configure terminal**	进入全局配置模式。
Step 2	Ruijie(config)**# http redirect** *ip-address*	配置 HTTP 重定向的 IP 地址，即 Portal 服务器的 IP 地址。
Step 3	Ruijie(config)**# show http redirect**	查看 HTTP 重定向信息的配置。

如果要清除 Portal 服务器的 IP 地址配置，在全局配置模式下，执行 **no http redirect**。

配置举例：

设置 Portal 服务器的 IP 地址为 176.10.0.1。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# http redirect 176.10.0.1
Ruijie(config)# show http redirect
```

如果配置了 Portal 服务器 IP 地址，则该 IP 地址可以直接访问的，也即用户无需认证即可直接访问该 IP。

5.4.2 配置Portal服务器的认证页面URL

Portal 服务器的 URL 是在用户进行 Web 认证时，重定向给用户浏览器的 URL，浏览器通过这个 URL 进行 Web 认证。如果没有配置该参数，则重定向时将 Portal 服务器的 IP 地址作为 URL 发给浏览器，格式为：http://Portal 服务器 IP/（比如:http://192.168.5.3/）。Portal 服务器认证页面的 URL 配置步骤如下：

	命令	作用
Step 1	Ruijie# **configure terminal**	进入全局配置模式。
Step 2	Ruijie(config)# **http redirect homepage** *url-string*	设置认证页面的主页 URL 为 *url-string*，必须以“http://”或“https://”开头，不区分大小写，最大长度为 255 个字符。允许在 URL 里面指定 Portal 服务器的 HTTP 监听端口号（一般服务器默认的都是监听 80 端口）。
Step 3	Ruijie(config)# **show http redirect**	查看 HTTP 重定向的配置。

如果要清除 Portal 的认证页面 URL，在全局配置模式下，执行 **no http redirect homepage**。

配置举例：

设置 Portal 认证页面的主页为 http://*www.web-auth.net/login.html*。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# http redirect homepage http://www.web-auth.net/login.html
Ruijie(config)# show http redirect
```

由于 Portal 服务器的 IP 是可直接访问的，如果用户在浏览器的地址栏上直接输入服务器的主页地址，则可以不经过重定向直接访问该主页，也可以下载该页面上的资源。但是，由于未经重定向，这种访问报文内部缺少接入设备和认证服务器之间必要的安全参数(设备重定向时会在重定向 URL 里面添加安全参数)，这会导致用户的认证操作将会失败。因此，如果是要进行认证的话，不要直接访问服务器的页面。

配置 portal 加密密钥情况下，必须要配置 homepage 参数，否则无法重定向。如果没有配置加密密钥，则 homepage 参数可选，不配置情况下用 portal 服务器的 ip 地址作为重地向 url。

5.4.3 配置设备和Portal服务器之间的通信密钥

Portal 服务器和接入设备之间再交互用户信息时需要做加密，以加强安全性。因此，要成功应用一代 Web 认证，必须配置设备与认证服务器进行通信的密钥。

缺省情况下，没有配置设备与认证服务器进行通信的密钥。配置步骤如下：

	命令	作用
Step 1	Ruijie# **configure terminal**	进入全局配置模式。
Step 2	Ruijie(config)# **web-auth portal key** *key-string*	设置设备与 Portal 服务器进行通信的密钥；密钥最大长度为 255 个字符。

Step 5	Ruijie(config)# **show web-auth**	查看 Web 认证全局配置信息和统计信息。

如果要清除设备与认证服务器进行通信的密钥，在全局配置模式下，执行 **no web- portal key**。

配置举例：

#设置接入设备与服务器进行通信的密钥为 web-auth。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# web-auth portal key web-auth
Ruijie(config)# show running-config
```

5.4.4 配置设备和Portal服务器之间的SNMP网管参数

从一代 Web 认证的流程中可以看出，Portal 服务器和接入设备之间操作用户上下线需要使用 SNMP 网管协议。。

因此，要成功应用锐捷一代 Web 认证，必须配置设备与 Portal 服务器之间的 SNMP 网管参数。

缺省情况下，设备没有配置与 Portal 服务器之间的 SNMP 网管参数。配置步骤如下：

	命令	作用
Step 1	Ruijie# **configure terminal**	进入全局配置模式。
Step 2	Ruijie(config)# **snmp-server community** *community-string* rw	设置 SNMP Community，Portal 服务器可以使用这个 Community 管理接入设备上的在线用户。 *community-string*：Community 字符串； rw：由于需要对 MIB 进行 Set 操作，因此需要设置成 RW，支持读写操作；
Step 3	Ruijie(config)# **snmp-server enable traps web-auth**	设置检测到用户掉线时需要向 Portal 服务器发送消息，利用 SNMP 网管协议的 Trap 和 Inform 实现。 web-auth：即允许发 Web 认证消息；
Step 4	Ruijie(config)# **snmp-server host** *ip-address* **inform version** 2c *community-string* web-auth	设置发送 Web 认证消息的目的主机，类型、版本、Community 等参数。 *ip-address*：目的主机地址，也就是一代 portal 服务器的地址； **informs**：设置发送 SNMP-Inform 类型的消息。由于设备在用户下线的时候向一代 portal 服务器发送消息，为了防止消息丢失，所以采用 SNMP-Inform 而不是 SNMP-Trap。 version 2c：SNMPv2 以后的版本才支持 SNMP-Inform 类型，因此这里不能设置为 SNMPv1。 *community-string*：发送 SNMP-Inform 消息使用的 Community 字符串。 web-auth：指明发送 Web 认证消息采用上述的参数；
Step 5	Ruijie(config)# **show running-config**	查看设备的运行配置信息。

SNMP 的配置命令和其他具体内容参见“SNMP 配置指南”中的相关章节。

配置举例：

#设置接入设备与服务器（IP 地址为 176.10.0.1）的 SNMP 网管通信参数，设置 SNMP Community 为 web-auth，以及发送 SNMP-Inform 消息使用的参数。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# snmp-server community web-auth rw
Ruijie(config)# snmp-server enable traps web-auth
Ruijie(config)# snmp-server host 176.10.0.1 informs version 2c web-auth web-auth
```

这里列出的 SNMP 通信参数是以 SNMPv2 的设置为例的，如果要求设备和 Portal 服务器之间的 SNMP 网管通信有更高的安全性，可以考虑采用 SNMPv3。这样，SNMP Community 的设置需要改为 SNMP User，并且 SNMP-Inform 的版本也需要改为 SNMPv3 版本的，另外还需要设置和 SNMPv3 相关的安全参数，具体参见“SNMP 配置”中相关的章节，这里不再进行详细介绍。

5.4.5 查看配置

命令	作用
show http redirect	显示 Portal 服务器的配置信息。

5.5 配置锐捷二代Web认证相关参数

二代 Web 认证缺省处于关闭的状态。同样的，为了能够正常使用二代 Web 认证，必须完成相关参数配置，二代 Web 认证才能正常工作。以下章节描述如何配置二代 Web 认证的参数：

- 创建 Portal 服务器
- 配置 AAA 的 Web 认证的认证方法列表
- 配置 AAA 的 Web 认证的记账方法列表
- 配置设备和 Portal 服务器之间的通信密钥
- 配置全局的认证方法列表（可选）
- 配置全局使用的 Portal 服务器（可选）
- 配置记账更新间隔时间（可选）

5.5.1 创建Portal服务器

要成功应用二代 Web 认证，需要创建一个 Portal 服务器。

缺省情况下，没有 Portal 服务器信息。若要创建 Portal 服务器，请按如下步骤：

	命令	作用
Step 1	Ruijie# **configure terminal**	进入全局配置模式。
	Ruijie(config)# **portal-server eportalv2 ip** {*ip-address* } [**url** *url-string*] [**port** *port-num*]	配置锐捷二代 Web 认证的 Portal 服务器的信息，包括服务器的名字，IP 地址，认证页面 URL 和服务器的监听端口号。 监听端口号参数是 Portal 服务器和设备间交互用户认证信息时所采用的私有协议的 UDP 端口号，可选配置，默认值为 50100。
Step 4	Ruijie(config)# **show web-auth portal**	查看 Portal 服务器的配置情况。

在清除 Portal 服务器的配置之前，需要先取消对该 Portal 服务器的使用，否则会导致 Web 认证用户的上、下线错误。

二代 Web 认证的 Portal 服务器遵循的是先创建服务器再使用服务器的顺序，因此必须先保证服务器信息被正确创建。

配置举例：

下面的例子创建一个二代 Web 认证的 Portal 服务器，IP 为 172.20.1.10，认证页面 URL 为 http://172.20.1.10:7080/index.php。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# portal-server eportalv2 ip 172.20.1.10 url http://172.20.1.10:7080/index.php
Ruijie(config)# show web-auth portal
```

5.5.2 配置AAA的Web认证的认证方法列表

由于二代 Web 认证需要由设备端发起 radius 认证，因此，如果选择使用二代 Web 认证，就需要在设备上为二代 Web 认证配置 AAA 的认证方法列表。

缺省情况下，AAA 中没有 Web 认证的认证方法列表。配置步骤如下：

	命令	作用
Step 1	Ruijie# **configure terminal**	进入全局配置模式。
Step 2	Ruijie(config)# **aaa new-model**	配置启用 AAA 安全服务功能。
Step 3	Ruijie(config)# **aaa authentication web-auth** {**default** | *list-name*} *method1* [*method2*...]	配置二代 Web 认证的认证方法列表。
Step 4	Ruijie(config)# **show aaa method-list**	查看 AAA 所有方法列表。

AAA 的配置命令和其他具体内容参见“AAA 配置”中的相关章节。

配置举例：

设置 AAA 的 Web 认证方法列表名为 default，使用默认的 RADIUS 组（组名为 radius）。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# aaa new-model
Ruijie(config)# aaa authentication web-auth default group radius
Ruijie(config)# show aaa method-list
```

关于 AAA 和 RADIUS 的配置，具体详见“AAA 配置”和“RADIUS 配置”中相关的章节。

5.5.3 配置AAA的Web认证的记账方法列表

由于二代 Web 认证需要由设备端发起认证，因此，当用户上下线的时候，就需要由设备向 Radius 服务器发记账报文。如果选择了二代 Web 认证，就需要在设备上配置 AAA 的记账方法列表。

缺省情况下，AAA 中无 Web 认证的记账方法列表。配置步骤如下：

	命令	作用
Step 1	Ruijie**# configure terminal**	进入全局配置模式。
Step 2	Ruijie(config)**# aaa new-model**	配置启用 AAA 安全服务功能。
Step 3	Ruijie(config)**# aaa accounting network** {**default** | *list-name*} **start-stop** *method1* [*method2*...]	配置 network 类型的记账方法列表。
Step 4	Ruijie(config)**# show aaa method-list**	查看 AAA 所有方法列表。

配置举例：

设置 AAA 的 network 类型的名为 default 的记账方法列表，使用默认的 RADIUS 组（组名为 radius）。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# aaa new-model
Ruijie(config)# aaa accounting network default start-stop group radius
Ruijie(config)# show aaa method-list
```

设备使用 RADIUS 组进行用户记账处理，需要为具体的 RADIUS 组配置记账 RADIUS 服务器的信息。具体详见“AAA 配置”和“RADIUS 配置”中相关的章节。

5.5.4 配置设备和Portal服务器之间的通信密钥

Portal 服务器和接入设备之间再交互用户信息时需要做加密，以加强安全性。因此，要成功应用一代 Web 认证，必须配置设备与认证服务器进行通信的密钥。

缺省情况下，没有配置设备与认证服务器进行通信的密钥。配置步骤如下：

	命令	作用

Step 1	Ruijie# **configure terminal**	进入全局配置模式。
Step 2	Ruijie(config)# **web-auth portal key** *key-string*	设置设备与 Portal 服务器进行通信的密钥；密钥最大长度为 255 个字符。
Step 5	Ruijie(config)# **show web-auth**	查看 Web 认证全局配置信息和统计信息。

如果要清除设备与认证服务器进行通信的密钥，在全局配置模式下，执行 **no web-auth portal key**。

配置举例：

设置接入设备与服务器进行通信的密钥为 web-auth。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# web-auth portal key web-auth
Ruijie(config)# show running-config
```

5.5.5 配置全局使用的认证方法列表

配置 Web 认证的认证方法列表需要分 2 个步骤，第一步是在前面章节提到的，在 AAA 下面配置一个认证方法列表。第二步，将此方法列表应用到 Web 认证。

缺省情况下，全局 Web 认证的认证方法列表名为 **default**。配置全局 Web 认证使用的认证方法列表的步骤如下：

	命令	作用
Step 1	Ruijie# **configure terminal**	进入全局配置模式。
Step 2	Ruijie(config)# **web-auth authentication v2** {**default** | *list-name*}	配置二代 Web 认证的全局认证方法列表名。
Step 3	Ruijie(config)# **show web-auth portal v2 aaa**	查看 Web 认证的 AAA 方法列表的配置。

如果要删除全局认证方法列表，在全局配置模式下，执行 **no web-auth authentication v2**。

配置举例：

配置 Web 认证的全局认证方法列表为 edu-web。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# web-auth authentication v2 edu-web
Ruijie(config)# show web-auth portal v2 aaa
```

配置方法类表之前必须确保 AAA 已经有配置此方法类表。

删除认证方法列表之后，默认将使用名字为 default 的认证方法列表。

5.5.6 配置全局使用的记账方法列表

记账方法列表和认证方法列表具有相同的配置约束，可参考前面章节的说明。

缺省情况下，全局的记账方法列表名为 **default**。配置全局 Web 认证使用的记账方法列表的步骤如下：

	命令	作用
Step 1	Ruijie**# configure terminal**	进入全局配置模式。
Step 2	Ruijie(config)**# web-auth accounting v2** {**default** | *list-name*}	配置 Web 认证的全局记账方法列表。
Step 3	Ruijie(config)**# show web-auth portal v2 aaa**	查看 Web 认证的 AAA 方法列表的配置。

如果要删除全局记账方法列表，在全局配置模式下，执行 **no web-auth accounting v2**。

配置举例：

配置 Web 认证的全局记账方法列表为 edu-acct。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# web-auth accounting v2 edu-acct
Ruijie(config)# show web-auth portal v2 aaa
```

5.5.7 配置全局使用的Portal服务器

前面章节已经介绍如何通过 **portal-server** 命令创建 Portal 服务器。Portal 服务器创建之后，需要被应用到 Web 认证才能生效。本章介绍如何应用 Portal 服务器。

如果要指定其它 Portal 服务器，配置步骤如下：

	命令	作用
Step 1	Ruijie**# configure terminal**	进入全局配置模式。
	Ruijie(config)**# portal-server eportalv2 ip** {*ip-address* [**port** *port-num*] [**url** *url-string*]	创建 Portal 服务器
Step 2	Ruijie(config)**# web-auth portal eportalv2**	指定全局使用的 Portal 服务器。
Step 3	Ruijie(config)**# show running-config**	查看设备的运行配置信息。

如果要恢复使用一代 Web 认证，可执行全局命令 **no web-auth portal**。

配置举例：

创建二代 Web 认证的全局 Portal 服务器。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# portal-server eportalv2 ip 172.20.1.10 url http://172.20.1.10:7080/index.php
Ruijie(config)#web-auth portal eportalv2
Ruijie(config)# show running-config
```

配置使用某个 Portal 服务器之前，该服务器必须已经被创建好，否则会导致配置失败。

删除 Portal 服务器信息之前，需要先删除对 Portal 服务器的应用，否则会导致认证和记账的异常。

5.5.8 配置记账更新间隔时间

如果实际网络环境需要部署记账功能且服务器需要设备定时发送记账更新报文，则需要在设备上配置记账更新间隔时间。

缺省情况下，记账更新间隔时间为 0 分钟，表示不发送记账更新报文。配置记账更新间隔时间的步骤如下：

	命令	作用
Step 1	Ruijie# **configure terminal**	进入全局配置模式。
Step 2	Ruijie(config)# **web-auth acct-update-interval** *minutes*	配置 Web 认证的记账更新间隔。
Step 3	Ruijie(config)# **show web-auth portal v2 parameters**	查看 Web 认证的参数信息。

如果要恢复默认记账更新时间，在全局配置模式下，执行 **no web-auth portal acct-update-interval**。

配置举例：

配置 Web 认证的记账更新时间为 3 分钟。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# web-auth acct-update-interval 3
Ruijie(config)# show web-auth portal parameters
```

如果 Radius 服务器返回的认证成功报文（Access-Accept）中，携带记账更新间隔时间属性，并且属性值非 0 时，则使用该值作为记账更新间隔时间；否则使用设备上配置的记账更新间隔时间。

5.5.9 配置 Portal协议扩展

锐捷二代 web 认证使用的 portal 协议兼容中移动 portal 规范，但是由于标准的 Portal 协议无法满足我司相关安全方案的需求，故我司对 Portal 协议进行了扩展

缺省情况下，我司设备是使用扩展之后的 Portal 协议与 Portal 服务器进行通讯，如果想关闭扩展，使用标准 portal 协议，则需要配置 no 命令：

	命令	作用
Step 1	Ruijie# **configure terminal**	进入全局配置模式。
Step 2	Ruijie(config)# **no web-auth portal extension**	配置 Portal 协议的扩展，使用标准的 Portal 协议。

如果要恢复使用 Portal 协议扩展功能，执行 **web-auth portal extension**。

配置举例：

配置使用标准的 Portal 协议与服务器通讯。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# no web-auth portal extension
Ruijie(config)# show web-auth portal parameters
```

1、在和非我司的产品对接时，需要关闭对 Portal 协议的扩展功能。因为第三方的 Portal 服务器并不一定支持我司对 Portal 协议的扩展，对接使用的时候有可能出现不兼容的情况。

5.5.10 配置支持Radius服务器踢线功能

锐捷二代 web 认证支持使用 Radius 服务器进行 DM 踢线的功能

缺省情况下，设备不支持 Radius 服务器进行 DM 踢线的功能，需要配置如下命令开启：

	命令	作用
Step 1	Ruijie# **configure terminal**	进入全局配置模式。
Step 2	Ruijie(config)# **radius dynamic-authorization-extension enable**	配置设备支持 Radius 服务器进行 DM 踢线的功能。

如果要取消支持 Radius 进行 DM 踢线的功能，则需要执行命令 no radius dynamic-authorization-extension enable。

配置举例：

配置设备支持 Radius 服务器进行 DM 踢线的功能。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# radius dynamic-authorization-extension enable
```

5.5.11 查看配置

命令	作用
show web-auth portal [parameters]	显示二代 Web 认证相关的配置和统计信息。

5.6 配置Web认证可选特性

前面描述的是使用 Web 认证时必须要做的配置，除此以外 Web 认证还提供了一些可选特性，这些可选特性对一代 Web 认证、二代 Web 认证均适用。这些可选特性在一些网络环境下能够帮助用户解决一些实际问题。以下章节描述如何配置 Web 认证的可选特性：

- 配置重定向的 HTTP 端口（可选）
- 配置每个未认证用户的最大 HTTP 会话数（可选）
- 配置维持重定向连接的超时时间（可选）
- 配置免认证的网络资源范围（可选）
- 配置已认证用户信息的更新时间间隔（可选）
- 配置免认证 IP 范围（可选）
- 配置流量检测功能（可选）
- 配置 Portal 检测功能（可选）

5.6.1 配置重定向的HTTP端口

Web 认证的基础是拦截未认证终端发出的 HTTP 报文并将其重定向到 Portal 服务器，由于 HTTP 协议规定默认使用 TCP 的 80 端口进行通信，因此设备也是默认拦截目的端口号为 80 的 TCP 报文。但是在某些网络环境中，终端发出的 HTTP 报文的目的端口号并不是 80，比如可以通过浏览器设置，修改 HTTP 的通信端口号。对于这种情况，就需要在设备上将这些非标准的端口号加入拦截列表，以便设备可以识别。

缺省情况下，设备只拦截 TCP 端口号为 80 的报文。要新增拦截端口号，请按照如下步骤：

	命令	作用
Step 1	Ruijie# **configure terminal**	进入全局配置模式。
Step 2	Ruijie(config)# **http redirect port** *port-num*	设置拦截特定目的 TCP 端口号的 HTTP 请求。 最大允许配置 10 个不同的拦截端口。
Step 3	Ruijie(config)# **show http redirect**	查看 HTTP 重定向的配置。

如果删除拦截端口，在全局配置模式下，使用 **no http redirect port** *port-num*。

配置举例：

设置对用户发出的特定目的端口号为 8080 的 HTTP 请求进行重定向。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# http redirect port 8080
Ruijie(config)# show http redirect
```

接入设备上常用的管理协议端口（例如 22、23、53）以及系统内部保留的端口，不允许被设置为重定向端口。实际上，除了 80 端口外，HTTP 协议很少会使用小于 1000 的端口号。为了避免与知名 TCP 协议端口冲突，除非必要，尽量不要设置较小端口号的端口作为重定向端口。

80 端口虽然是默认端口，但是也允许用户删除，不过考虑到 80 端口是标准的 HTTP 通信端口，建议不要删除。

5.6.2 配置每个未认证用户的最大HTTP会话数

未认证的用户在访问网络资源时，用户 PC 会发出 HTTP 会话连接请求，HTTP 报文会被设备拦截，并通过重定向要求用户进行 Web 认证。为了防止同一个未认证用户发起过多的 HTTP 连接请求，以节约接入设备的资源，需要在设备上限制未认证用户的最大 HTTP 会话数。

由于用户在认证时，会占用一个 HTTP 会话，而用户的其他应用程序也可能占用着 HTTP 会话，比如一些下载软件也会使用 HTTP 协议，因而不建议设置未认证用户的最大 HTTP 会话数为 1，否则有可能导致用户无法 Web 认证。

。缺省情况下，未认证用户的最大 HTTP 会话数为 255。

要更改未认证用户的最大 HTTP 会话数，请按照如下步骤：

	命令	作用
Step 1	Ruijie**# configure terminal**	进入全局配置模式。
Step 2	Ruijie(config)# **http redirect session-limit** *session-num* [**port** *port-session-num*]	设置每个未认证的最大 HTTP 全局会话数为 *session-num*，默认 255 个，取值范围 1-255。 设置每个二层端口上未认证的最大 HTTP 会话数为 *port-session-num*，默认 1000 个，取值范围 1-65535。
Step 3	Ruijie(config)**# show http redirect**	查看 HTTP 重定向的配置。

如果要恢复默认未认证用户的最大 HTTP 会话数，在全局配置模式下，使用 **no http redirect session-limit**。

配置举例：

设置未认证用户的最大 HTTP 会话数为 104。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z..
Ruijie(config)# http redirect session-limit 104
Ruijie(config)# show http redirect
```

如果一个用户在进行 Web 认证时，出现经常无法弹出认证页面的情况，则很可能是受到最大 HTTP 会话数的限制了。此时，应该建议用户暂时关闭一些可能会占用 HTTP 会话的应用程序，然后再进行 Web 认证。

5.6.3 设置维持重定向连接的超时时间

未认证的用户通过 HTTP 访问网络资源时，其 TCP 连接请求将被拦截，实际上是与设备建立起 TCP 连接。在连接建立后，设备需要等待用户发出的 HTTP 的 GET/HEAD 报文，然后回复 HTTP 重定向报文后才能关闭连接。设置这个限制可以防止用户不发 GET/HEAD 报文，而又长时间占用 TCP 连接。此功能可以防止一些恶意攻击

缺省情况下，维持重定向连接的超时时间为 3 秒。要更改维持重定向连接的超时时间，请按照如下步骤：

	命令	作用
Step 1	Ruijie# **configure terminal**	进入全局配置模式。
Step 2	Ruijie(config)# **http redirect timeout** *seconds*	设置维持重定向连接的超时时间（秒）*seconds*。
Step 3	Ruijie(config)# **show http redirect**	查看 HTTP 重定向的配置。

如果要恢复维持重定向连接的超时时间为 3 秒，在全局配置模式下，使用 **no http redirect timeout**。

配置举例：

设置维持重定向连接的超时时间为 4 秒。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# http redirect timeout 4
Ruijie(config)# show http redirect
```

在配置自动获取客户端时需要进行该配置

5.6.4 配置免认证的网络资源范围

启动 Web 认证后，未认证用户需先通过 Web 认证，才能访问网络资源。由于某些情况下，可能会允许未认证用户也可以访问一些网络资源，比如下载系统安全补丁、访问一些公告栏等等。针对这种需求，需要使用本章节提供的命令设置免认证即可访问的网络资源。设置为免认证访问的网络资源，那么所有用户（包括未认证用户）都可以访问该资源。

。缺省情况下，没有设置免认证的网络资源，未认证用户不能访问网络资源。

要设置免认证的网络资源，请按照如下步骤：

	命令	作用
Step 1	Ruijie# **configure terminal**	进入全局配置模式。
Step 2	Ruijie(config)# **http redirect direct-site** *ipv6-address* | *ip-address* [*ip-mask*] [**arp**] }	1. 免认证的网络资源最多允许配置 50 个。 2. 如果设备启用了 ARP CHECK 功能，并且免认证的网络资源(包括 portal 服务器)和认证用户在同一个网段内，那么需要对免认证的网络资源进行 ARP 绑定，需要配置 **arp** 关键字（ARP 绑定基于端口生效）。 利用 *ip-mask* 参数可以指定某个 IP 段为面认证访问的网络资源

Step 3	Ruijie(config)# **show http redirect**	查看 HTTP 重定向的配置。

如果要取消设置免认证的网络资源，在全局配置模式下，使用 **no http redirect direct-site** *ip-address* [*ip-mask*]。

配置举例：

设置校园网内某免费网址 172.16.x.x 为免认证的网络资源。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# http redirect direct-site 172.16.0.0 255.255.0.0
Ruijie(config)# show http redirect
```

设置免认证的网络资源和设置无需认证用户共享资源，这两者各自都不能超过 50 个。此外，实际可用数量也会受其它安全功能占用表项的影响而减少。因此，如果需要设置的地址较多，请尽量使用 IP 地址+掩码（或者 IPv6 地址前缀+前缀长度）的方式进行设置。

对于开启 ARP Check 情况，需要将二层接入设备下联 PC 的网关设置为免认证的网络资源。

在配置自动获取客户端是需要进行该配置。

http redirect direct-site 是配置免认证访问地址，http redirect 是配置 web 认证的服务器地址。从效果上看，用这两条命令配置的地址都是可以不用认证就直接访问的，但是实际用途是不一样的，因此实际使用时建议不要用 http redirect direct-site 来配置 web 认证服务器地址，否则会引起误解。

配置自动获取客户端时需要注意以下问题:

1）设置免认证的网络资源功能，只有在打开全局客户端下载功能后，在 802.1x 受控口上生效。

2）该功能不受 GSN、ACL 设置影响，即无法使用 GSN 阻断或使用 ACL 过滤该免认证的 IP 地址。

5.6.5 配置已认证用户信息的更新时间间隔

设备维护着已认证用户的信息，由于业务上的需要，比如监控用户的流量是否超标、在线时间是否超标等，设备需要定时地更新在线用户信息。

缺省情况下，设备每 180 秒更新一次已认证用户的信息（包括用户的在线时长、已产生的流量等）。要更改已认证用户信息的更新时间间隔，请按照如下步骤：

	命令	作用
Step 1	Ruijie# **configure terminal**	进入全局配置模式。
Step 2	Ruijie(config)# **web-auth update-interval** *seconds*	设置已认证用户信息的更新时间间隔为 *seconds* 秒，取值范围 30-3600 秒。
Step 3	Ruijie(config)# **show running-config**	查看设备的运行配置。

如果要恢复默认的已认证用户信息的更新时间间隔，在全局配置模式下，使用 **no web-auth update-interval**。

配置举例：

设置已认证用户信息的更新时间间隔为 60 秒。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# web-auth update-interval 60
Ruijie(config)# show running-config
```

用户更新时间必须配置为 60 的倍数，否则实际配置自动向上取最近的 60 倍数来生效。

5.6.6 配置免认证IP范围

某些情况下，需要允许一些 IP 地址无需 Web 认证即可访问网络。缺省情况下，所有接入用户的 IP 地址都会被控制并要求进行 Web 认证。要设置免认证 IP 地址，请按照如下步骤：

	命令	作用
Step 1	Ruijie# **configure terminal**	进入全局配置模式。
Step 2	Ruijie(config)# **web-auth direct-host** *ipv6-address* | *{ip-address* [*ip-mask*] [**arp**]}	1. 设置免认证 IP，最大允许配置 50 个。 2. 利用 *ip-mask* 参数可配置一个 IP 地址段为免认证 IP。 3. 如果设备启用了 ARP CHECK 功能，且需要对免认证的用户 IP 范围进行 ARP 绑定，需要配置 **arp** 关键字。 4. 面认证 ip 和免认证可访问网络资源共享 50 条表项的容量限制。
Step 3	Ruijie(config)# **show http redirect**	查看 Web 认证全局配置信息和统计信息。

如果要取消免认证 IP，在全局配置模式下，使用 **no web-auth direct-host** *ip-address* [*ip-mask*]。

配置举例：

设置 IP 地址为 176.10.0.1 的用户为无需认证的用户。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# web-auth direct-host 176.10.0.1
Ruijie(config)# show http redirect
```

5.6.7 配置流量检测功能

Web 认证提供了一个低流量下线功能，允许设备检测已认证用户在一定时间内的流量值，当用户在指定时间内的流量低于指定的阈值时，则认为该用户处于低流量状态（比如处于待机状态等），此时将该用户下线。

缺省情况下，流量检测功能打开，默认值是 15 分钟 0 字节。要配置流量检测功能，请按照如下步骤：

	命令	作用
Step 1	Ruijie**# configure terminal**	进入全局配置模式。
Step 2	Ruijie(config)**# web-auth offline-detect flow** [**idle-timeout** *minutes*] [**threshold** *bytes*]	配置流量检测功能。 *minutes* 默认 15 分钟。*threshold* 默认 0，这 2 个参数为可选，不指定则使用默认值。
Step 3	Ruijie(config)**# show running-config**	查看设备的运行配置。

要恢复流量检测功能的默认参数，在全局配置模式下，使用 **no web-auth offline-detect flow**。

配置举例：

设置流量检测功能，并配置检测时间长度为 3 分钟，低流量阀值为 1024 字节。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# web-auth offline-detect flow idle-timeout 3 threshold 1024
Ruijie(config)# show running-config
```

5) Web 认证支持三种下线检测方式:

- 基于链路状态的检测。当用户的物理信号断开时判断用户下线。
- 基于流量的检测。也就是本章节介绍的功能。
- 基于保活页面的检测。此功能需要在 Portal 服务器上开启，用户认证通过之后，浏览器会弹出一个认证通过页面，此页面会和 Portal 服务器保持通信，当用户关闭这个页面一段时间后，Portal 服务器会判断用户已经下线，于是会通告设备用户下线。
- S5750L、S5750S、S29E、S29S 因为硬件限制，流量统计存在不准的问题，因此这些设备上配置流量检测时，threshold 参数需要配置为 0，否则会因为统计错误导致误判。

5.6.8 查看配置

命令	作用
show http redirect	显示 HTTP 重定向的配置。
show web-auth control	显示 WEB 认证相关控制信息。

5.6.9 一代Web认证典型配置举例组网拓扑

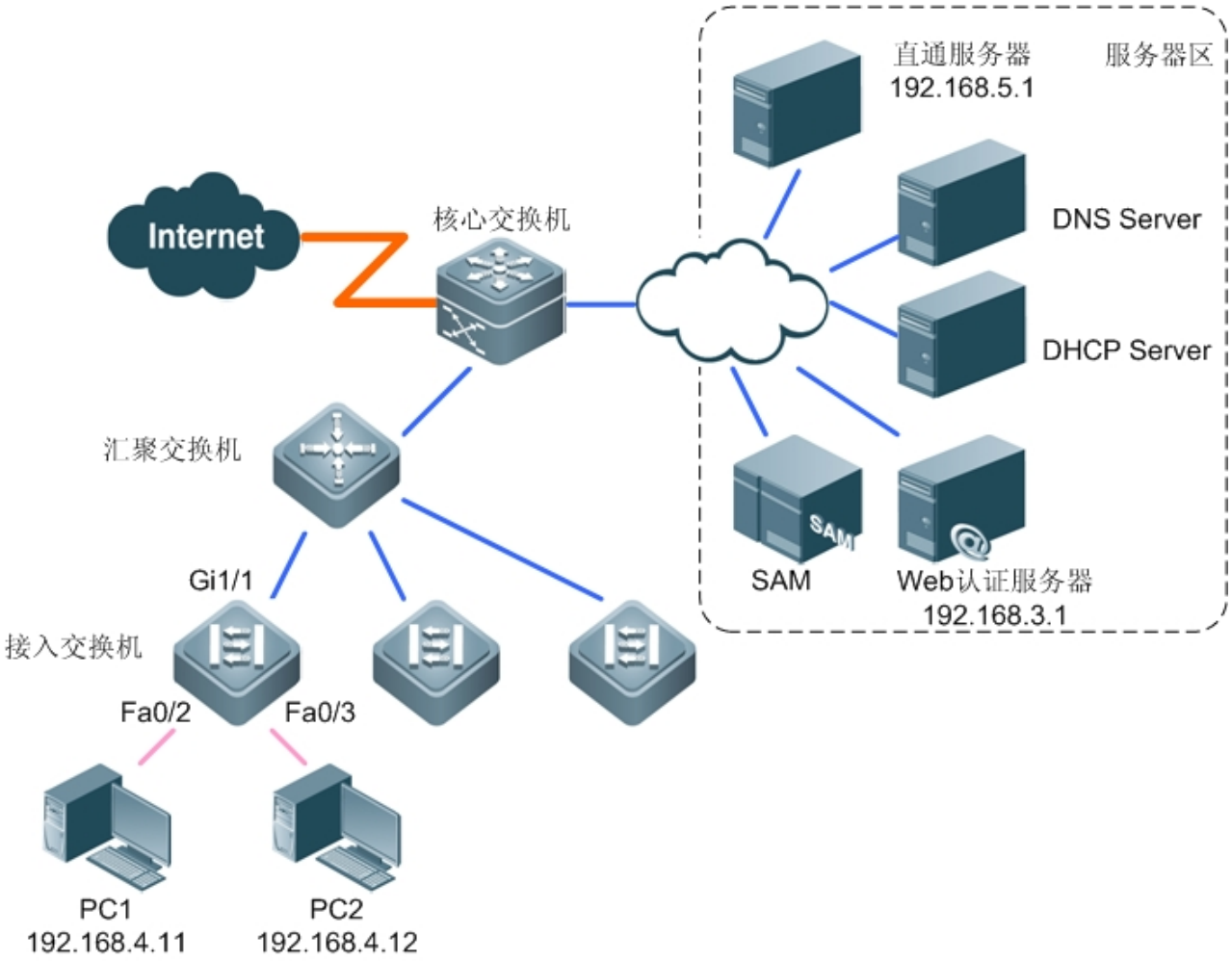
组网需求

1. 网络中包括 Radius 服务器、Portal 服务器（有些 Portal 服务器集成了 Radius 服务器功能）、DHCP 服务器、直通服务器（网站），DNS 服务器、核心设备、汇聚设备，若干台接入设备，若干台用户 PC。

2. 接入设备需要支持一代 Web 认证功能。

组网拓扑

图 5-2 Web 认证方案网络拓扑图



3) 用户 PC 连接在接入设备下，接入设备上链端口连接汇聚接入设备，汇聚接入设备连接核心接入设备，通过核心接入设备可以访问 Internet。

4) 服务器部署在服务器区内，通过内部网络与核心接入设备相连。

5) PC1 从 DHCP 服务器获得 IP 地址为 192.168.4.11，PC2 从 DHCP 服务器获得 IP 地址为 192.168.4.12；它们的网关是 192.168.4.1。

6) Portal 服务器的域名为 www.web_auth.com，通过内部 DNS 服务器可以进行解析，Web 认证页面的 URL 为：http://www.web_auth.com/webportal/index.jsp。如果未部署内部 DNS 服务器，可以在 URL 中直接设置 Web 认证服务器的 IP。

7) SAM 服务器作为 Radius 服务器，提供认证和计费服务。

8) 服务器区内存在公共服务器，无需认证均可访问。

配置要点

Web 认证方案的注意事项：

- 端口上打开了 Web 认证后，该端口下即使是未认证的用户，其发出的 DHCP 和 DNS 报文是可以通过的。不会影响到用户获取 IP 地址，以及进行域名解析。
- 为了防止 TCP 攻击，限制用户在认证前的最大连接数以防止 TCP 攻击，缺省值是全局每 IP 是 255（随着连接数量总数的增加，每 IP 可用的连接数可能会缩小）。但用户 PC 可能发起多个 HTTP 连接，但不一定是浏览器发出的，有可能是其他软件，例如聊天、下载或视屏软件，甚至可能是木马病毒。这种情况下，可能会因其他软件占用了连接，导致浏览器无法建立连接，因此无法完成认证。这种限制的解决，需要在部署时注意，这个值不要设置得太小。使用 Web 认证的用户，若上网前开启的自动连接软件过多，要先关掉。
- 由于 Web 认证必须依靠客户 PC 能发起 HTTP 连接，而在进行连接之前，必须要能让客户 PC 获取到 DNS 解析的 IP 地址，以及网关的 ARP 报文。在这种情况下，接入设备放行未认证用户发给网关的 ARP 请求报文。因此，有可能出现一种 ARP 欺骗情况，即如果某个用户冒充同一个 VLAN 下的其它用户的 IP，给网关发送 ARP 报文，就会造成网关学习到错误的 ARP，对同一 VLAN 下的其它用户产生影响。
- 一代 Web 认证设备和 Portal 服务器间采用 snmp 协议通信，因此需要使能 snmp 协议并配置好相关通信参数。

配置步骤

1. 在接入设备上设置认证服务器的 IP 地址及与认证服务器进行通信的密钥

```
Ruijie# config
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# http redirect 192.168.3.1
Ruijie(config)# web-auth portal key web_auth_s26_1
```

2. 在接入设备上设置认证页面的主页地址

```
Ruijie(config)# http redirect homepage http://www.web_auth.com/webportal/index.jsp
```

3. 设置接入设备与认证服务器之间的 SNMP 网管参数

```
Ruijie(config)# snmp-server community web_auth_key
Ruijie(config)# snmp-server enable traps web-auth
Ruijie(config)# snmp-server host 192.168.3.1 inform version 2c web_auth_key web-auth
Ruijie(config)# exit
```

4. 在接入设备上对 Fa0/2、Fa0/3 两个端口上开启 Web 认证功能

```
Ruijie(config)# interface range fa0/2-3
Ruijie(config-if-range)# web-auth port-control
Ruijie(config-if-range)# exit
```

5. 在接入设备上设置免认证的网络资源范围，将公共服务器设置为直通的网站

```
Ruijie(config)# http redirect direct-site 192.168.5.1
```

如果打开了 ARP Check 功能，则需要加上 arp 选项：

```
Ruijie(config)# http redirect direct-site 192.168.5.1 arp
```

6. 若开启 ARP 功能，则还必须将网关 IP 地址设置为免认证的网络资源范围，并开启 arp 选项，以保证在认证前，PC 能完成 DNS 及 ARP 请求。

在接入设备上将下联 PC 的网关 192.168.4.1 设置免认证的网络资源范围

```
Ruijie(config)# http redirect direct-site 192.168.4.1 arp
```

7. 在接入设备上设置无需认证用户 IP 地址范围

```
Ruijie(config)# web-auth direct-host 192.168.4.12
```

如果打开了 ARP Check 功能，则需要加上 arp 选项：

```
Ruijie(config)# web-auth direct-host 192.168.4.12 arp
```

至此 PC1 如果要访问 internet 就会先重定向到 Web 认证服务器，通过认证后，才能访问 internet；而 PC2 不需要进行认证就可以访问 internet

显示验证

1. 显示 HTTP 重定向的配置：

```
Ruijie# show http redirect
http redirect settings
 server         : 192.168.3.1
 port           : 80
 homepage       : http://www.web_auth.com/webportal/index.jsp
 session-limit : 255
 timeout        : 3

direct-site
  Address           Mask               ARP Binding
  --------------- ---------------- -----------
  192.168.4.1       255.255.255.255    On
  192.168.5.1       255.255.255.255    On

direct-host
  Address           Mask               Port        ARP Binding
  --------------- ---------------- ---------- ----------
  192.168.4.12      255.255.255.255  Fa0/3        On
```

2. 显示免 Web 认证的用户范围：

```
Ruijie# show web-auth direct-host
direct-host
  Address           Mask               Port        ARP Binding
```

```
--------------- ---------------- ---------- ----------
192.168.4.12      255.255.255.255  Fa0/3         On
```

3. 显示接口上的认证配置和统计信息：

```
Ruijie# show web-auth port-control
 Port                         Control
------------------------- ----------
FastEthernet 0/1           Off
 FastEthernet 0/2           On
 FastEthernet 0/3           On
```

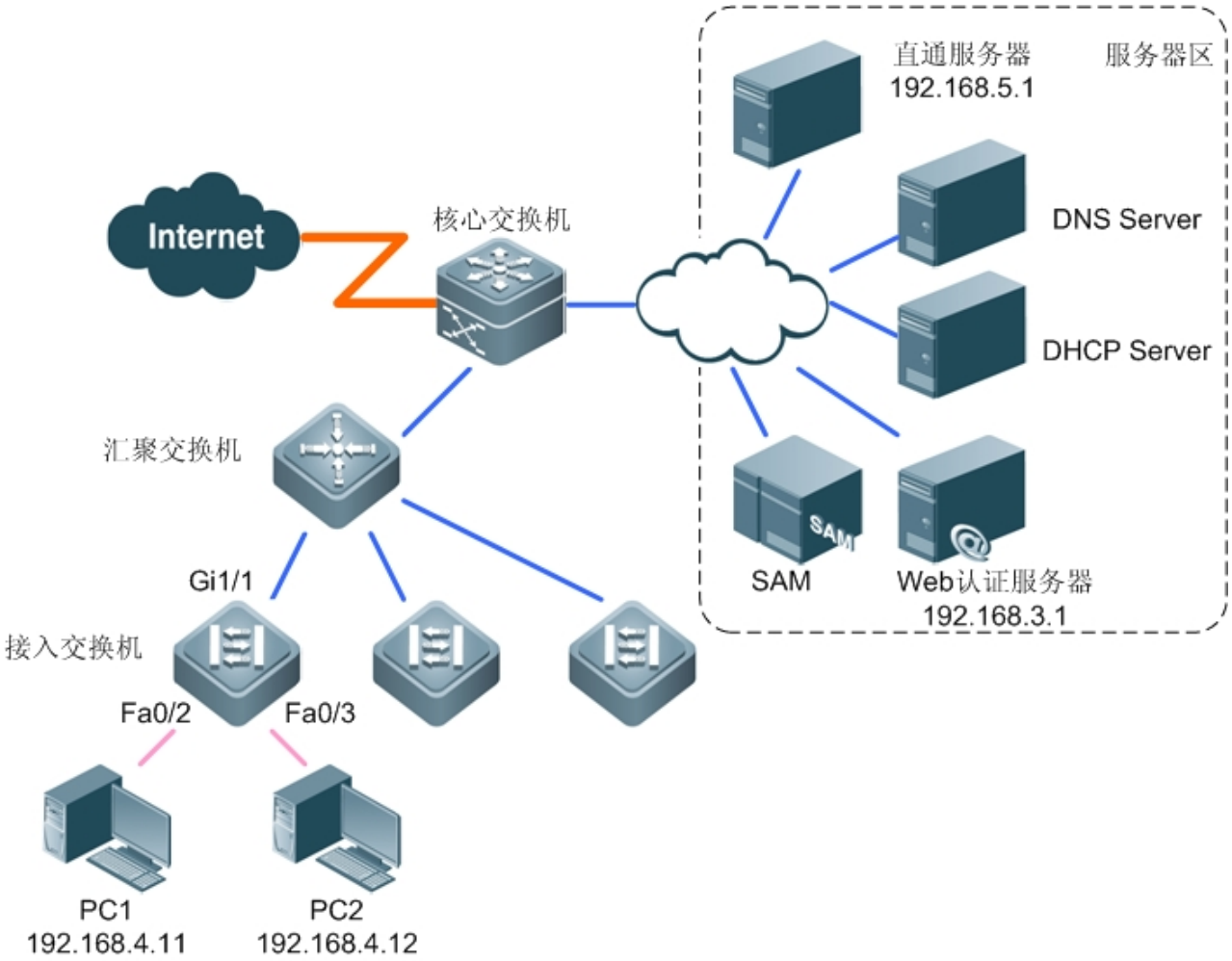
5.6.10 二代Web认证典型配置举例组网拓扑

组网需求

1. 网络中包括 Radius 服务器、Portal 服务器（有些 Portal 服务器集成了 Radius 服务器功能）、DHCP 服务器、直通服务器（网站），DNS 服务器、核心设备、汇聚设备，若干台接入设备，若干台用户 PC 。
2. Portal 服务器需要支持二代 Web 认证。
3. 接入设备需要支持二代 Web 认证功能。

组网拓扑

图 5-3 Web 认证方案网络拓扑图



9) 用户 PC 连接在接入设备下，接入设备上链端口连接汇聚接入设备，汇聚接入设备连接核心接入设备，通过核心接入设备可以访问 Internet。

10) 服务器部署在服务器区内，通过内部网络与核心接入设备相连。

11) PC1 从 DHCP 服务器获得 IP 地址为 192.168.4.11，PC2 从 DHCP 服务器获得 IP 地址为 192.168.4.12；它们的网关是 192.168.4.1。

12) Portal 服务器的域名为 www.web_auth.com，通过内部 DNS 服务器可以进行解析，Web 认证页面的 URL 为：http://www.web_auth.com/webportal/index.jsp。如果未部署内部 DNS 服务器，可以在 URL 中直接设置 Web 认证服务器的 IP。

13) SAM 服务器作为 Radius 服务器，提供认证和计费服务。

14) 服务器区内存在公共服务器，无需认证均可访问。

配置要点

Web 认证方案的注意事项：

- 端口上打开了 Web 认证后，该端口下即使是未认证的用户，其发出的 DHCP 和 DNS 报文是可以通过的。不会影响到用户获取 IP 地址，以及进行域名解析。
- 为了防止 TCP 攻击，限制用户在认证前的最大连接数以防止 TCP 攻击，缺省值是全局每 IP 是 255（随着连接数量总数的增加，每 IP 可用的连接数可能会缩小）。但用户 PC 可能发起多个 HTTP 连接，但不一定是浏览器发出的，有可

能是其他软件，例如聊天、下载或视屏软件，甚至可能是木马病毒。这种情况下，可能会因其他软件占用了连接，导致浏览器无法建立连接，因此无法完成认证。这种限制的解决，需要在部署时注意，这个值不要设置得太小。使用 Web 认证的用户，若上网前开启的自动连接软件过多，要先关掉。

- 由于 Web 认证必须依靠客户 PC 能发起 HTTP 连接，而在进行连接之前，必须要能让客户 PC 获取到 DNS 解析的 IP 地址，以及网关的 ARP 报文。在这种情况下，接入设备放行未认证用户发给网关的 ARP 请求报文。因此，有可能出现一种 ARP 欺骗情况，即如果某个用户冒充同一个 VLAN 下的其它用户的 IP，给网关发送 ARP 报文，就会造成网关学习到错误的 ARP，对同一 VLAN 下的其它用户产生影响。
- 需要使能 DM 功能，详细配置可参考 DM-SCG 中的配置说明。

配置步骤

1. 创建二代 portal 服务器

```
Ruijie# config
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# portal-server eportalv2 ip 192.168.3.1 url http://www.web_auth.com/webportal/index.jsp
```

2. 配置使用锐捷二代 Web 认证功能

```
Ruijie# config
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# web-auth portal eportalv2
```

3. 配置 AAA

```
Ruijie# config
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# aaa new-model
Ruijie(config)# radius-server host 172.20.1.20 key aaatest
        Ruijie(config)# aaa authentication web-auth default group radius
Ruijie(config)# aaa accounting network default start-stop group radius
```

4. 端口使能 web 认证

```
Ruijie(config)# interface range fa0/2-3
Ruijie(config-if-range)# web-auth port-control
```

显示验证

显示接口上的认证配置信息：

```
Ruijie# show web-auth port-control
 Port                        Control
-------------------------- ----------
FastEthernet 0/1           Off
 FastEthernet 0/2           On
 FastEthernet 0/3           On
```

5.6.11 设置在线用户信息的更新时间间隔

接入/汇聚设备维护着在线用户信息，设备需要定时地更新在线用户信息，包括在线时间等，以监控在线用户使用网络资源的情况，比如：用户的在线时间大于或等于在线时限，该用户会被停止使用网络。缺省情况下，设备每 60 秒更新一次在线用户的信息。

要更改在线用户信息的更新时间间隔，请按照如下步骤：

命令	作用
Ruijie**# configure terminal**	进入全局配置模式。
Ruijie(config)**# web-auth update-interval** *seconds*	设置在线用户信息的更新时间间隔为 *seconds* 秒，取值范围 30-3600 秒。

如果要恢复在线用户信息的更新时间间隔为 60 秒，在全局配置模式下，使用 **no web-auth update-interval**。

配置举例：

设置在线用户信息的更新时间间隔为 30 秒。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# web-auth update-interval 30
```

5.6.12 设置基于VLAN的Web认证

汇聚层设备下联接入设备（二层设备），它们之间使用 TRUNK 相连，用户（PC）连接在接入设备上。在汇聚层设备上开启 Web 认证，并可以设置允许认证的 VLAN，如果用户的 VLAN 属于允许认证的 VLAN，即可进行认证，否则拒绝。认证通过后，可以将用户的 IP、MAC 和 VLAN ID 进行绑定。

要启动基于 VLAN 的 Web 认证功能，并设置允许认证的 VLAN 列表，请按照如下步骤：

命令	作用
Ruijie**# configure terminal**	进入全局配置模式。
Ruijie(config)**# web-auth allow-vlan** *list*	设置支持基于 VLAN 的 web 认证。
Ruijie(config)**# show web-auth allow-vlan**	查看支持基于 VLAN 的 Web 认证的 VLAN 列表。

如果要取消基于 VLAN 的 Web 认证功能，在全局配置模式下，使用 **no web-auth allow-vlan**。

配置举例：

设置允许认证的 VLAN 为 VLAN1、2、3、5。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# web-auth allow-vlan 1-3,5
Ruijie(config)# show web-auth allow-vlan
```

- 设置基于 VLAN 的 Web 认证功能的生效条件如下:
- 汇聚层设备和下联的接入层设备直接连接的端口，必须开启 Web 认证功能;

汇聚层设备和下联的接入层设备直接连接的端口，必须是 TRUNK 模式;

该功能只能在作为汇聚层的设备上开启 Web 认证功能时支持。

5.7 配置自动获取客户端

在实际部署 802.1x 过程中 IT 实施人员往往因为客户端（锐捷的 Supplicant 软件，以下简称 SU）的部署工作量太大而感到头痛。而通过自动获取客户端的解决方案的推出，使得 IT 人员能够对客户端进行快速部署，省时省力省心，提高了工作效率。

自动获取 SU 客户端功能的原理是，当未认证用户通过浏览器访问网路资源时，会被自动重定向到下载服务器页面上，这样就可以下载客户端软件，轻松解决客户端部署难的问题。

我们将通过以下章节详细说明如何配置自动获取 SU 客户端。

受接入设备硬件容量影响，打开 ARP CHECK 或安全通道功能，将导致可用认证用户数量减少（尤其是安全通道功能），如果以上两个功能都打开，再打开客户端自动获取功能，在极端情况下可能耗尽硬件资源，802.1x 认证将无法进行。同时，在已开启 802.1x 认证的情况下，再打开上述功能时可能失败。因此不建议客户端自动获取方案与安全通道功能共用。

5.7.1 设置全局客户端下载功能开关

要成功应用自动获取客户端功能，必须打开全局的客户端下载功能的开关。缺省情况下，全局客户端下载功能是关闭的。若要开启客户端下载功能，请按如下的步骤：

命令	作用
Ruijie**#configure terminal**	进入全局配置模式
Ruijie(config)**#dot1x redirect**	配置全局的客户端下载功能
Ruijie(config)**#end**	退出到特权模式
Ruijie**#write**	保存配置
Ruijie**#show run**	显示配置

使用 **no dot1x redirect** 命令将关闭全局客户端下载功能。以下例子是设置打开全局自动获取客户端功能：

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# dot1x redirect
```

如果在开启客户端下载功能之前，已经开启了 802.1x 认证功能，则在开启客户端下载功能开关后，将导致所有的 802.1x 用户下线，需要重新认证才能上线

5.7.2 设置HTTP重定向地址

要成功应用自动获取客户端功能，必须设置 HTTP 重定向的 IP 地址。当接入设备发现未认证用户试图通过 HTTP 访问网络资源时，接入设备将用户的访问请求重定向到客户端下载页面，通过下载页面，引导用户下载客户端，安装并进行认证。

一般情况下，客户端下载页面是下载服务器所提供的，因此 HTTP 重定向的地址就应该是下载服务器的地址。设置了这个 HTTP 重定向地址以后，这个地址将被设置为一个特殊的免认证的网络资源，未认证用户可以直接与这个地址进行 HTTP 通讯。

缺省情况下，没有设置 HTTP 重定向的 IP 地址。设置 HTTP 重定向的 IP 地址，请参照“配置 Web 认证基本特性”中的“设置 HTTP 重定向地址”的相关配置命令。

5.7.3 设置重定向的HTTP端口

当用户访问网络资源时（例如使用浏览器上网），此时用户会发出 HTTP 报文，接入设备通过拦截来自用户的 HTTP 报文，来判断用户是否在访问网络资源。当接入设备检测到未认证的用户在访问网络资源时，将阻止用户访问网络资源，并向用户弹出客户端下载页面。

缺省情况下，接入设备通过拦截用户发出的端口号为 80 的 HTTP 报文，来检测用户是否在访问网络资源。

要新增接入设备拦截用户发出的特定端口号的 HTTP 报文，请参照“配置 Web 认证可选特性”中“设置重定向的 HTTP 端口”的配置。

5.7.4 设置客户端下载服务器页面的主页地址

在启动自动获取客户端功能前，必须先配置客户端下载服务页面的主页地址。当未认证用户在进行网络访问时，将向用户弹出这个页面的信息，用户通过这个页面进行客户端的下载。

缺省时，没有设置客户端下载服务页面的主页地址。设置客户端下载服务页面的主页地址，请参照“配置 Web 认证基本特性”中“设置 HTTP 重定向主页”的配置。

5.7.5 设置每个未认证用户的最大HTTP会话数

未认证的用户在访问网络资源时，用户 PC 会发出 HTTP 会话连接请求，HTTP 报文会被接入设备拦截，并要求用户进行 Web 认证。为了防止未认证用户发起 HTTP 攻击，而导致接入设备的 TCP 连接耗尽，需要在接入设备上限制未认证用户的最大 HTTP 会话数。

由于用户在认证时，会占用一个 HTTP 会话，而用户的其他应用程序也可能占用着 HTTP 会话，因而不建议设置未认证用户的最大 HTTP 会话数为 1。缺省情况下，全局每个未认证用户的最大 HTTP 会话数为 255，而每个端口下的未认证用户的 HTTP 会话总数最大为 300。

要更改未认证用户的最大 HTTP 会话数，请参照“配置 Web 认证可选特性”中“设置每个未认证用户的最大 HTTP 会话数”的配置。

5.7.6 设置维持重定向连接超时时间

设置维持重定向连接的超时时间请参照“配置 Web 认证可选特性”的“设置维持重定向连的接超时时间”的配置。

5.7.7 设置免认证的网络资源范围

设置免认证网络资源范围请参照“配置 Web 认证可选特性”中“设置免认证的网络资源范围”的配置。

5.7.8 查看客户端自动获取的HTTP重定向的配置信息

在特权模式下使用如下命令查看客户端自动获取的 HTTP 重定向的配置信息：

命令	作用
show http redirect	查看客户端自动获取的 HTTP 重定向的配置信息

以下例子是查看查看客户端自动获取的 HTTP 重定向的配置信息：

```
Ruijie# show http redirect
http redirect settings
 server         : 172.16.0.1
 port           : 80 8080
 homepage       : http://www.su-download.net/
 session-limit : 3
 timeout        : 3

direct-site
  Address            Mask                ARP Binding
  ---------------- ----------------- -----------
  176.10.0.1       255.255.255.255     On
  176.10.5.0       255.255.255.128     Off
```

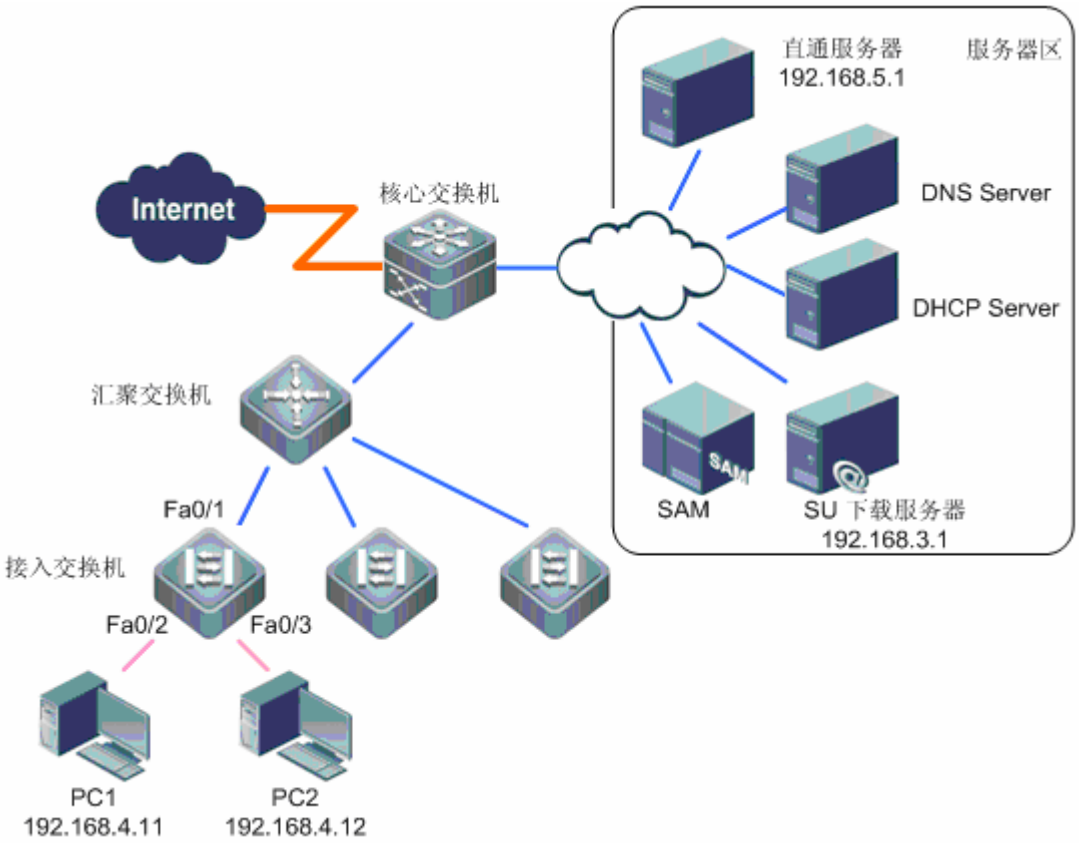
5.8 自动获取客户端典型配置举例

组网需求

- 网络中包括客户端下载服务器、DHCP 服务器、直通服务器（网站），DNS 服务器、核心交换机、汇聚交换机，若干台接入交换机，若干台用户 PC。
- 接入交换机需要支持自动获取客户端功能。

组网拓扑

图 5-2



- 用户 PC 连接在接入交换机下，接入交换机上链端口连接汇聚交换机，汇聚交换机连接核心交换机，通过核心交换机可以访问 Internet；
- 服务器部署在服务器区内，通过内部网络与核心交换机相连。
- PC1 从 DHCP 服务器获得 IP 地址为 192.168.4.11，PC2 从 DHCP 服务器获得 IP 地址为 192.168.4.12；他们的网关是 192.168.4.1
- 客户端下载服务器的域名为 www.su_download.com，通过内部 DNS 服务器可以进行解析，客户端下载页面的 URL 为：http://www.su_download.com/su/index.jsp。如果未部署内部 DNS 服务器，可以在 URL 中直接设置客户端下载服务器的 IP；
- 服务器区内存在公共服务器，无需认证均可访问；

配置要点

客户端自动获取方案的注意事项：

- 打开了全局客户端下载功能后，802.1x 受控端口下即使是未认证的用户，其发出的 DHCP 和 DNS 报文是可以通过的。不会影响到用户获取 IP 地址，以及进行域名解析；
- 为了防止 TCP 攻击，限制用户在认证前的最大连接数以防止 TCP 攻击，缺省值是 3，最大能配置成 10。但用户 PC 可能发起多个 HTTP 连接，但不一定是浏览器发出的，有可能是其他软件，例如聊天、下载或视屏软件，甚至可能是木马病毒。这种情况下，可能会因其他软件占用了连接，导致浏览器无法建立连接，因此无法弹出客户端下载页面。这种限制的解决，需要在部署时注意，需要自动下载客户端的用户，若上网前开启的自动连接软件过多，要先关掉；

- 由于弹出客户端下载页面必须依靠客户 PC 能发起 HTTP 连接，而在进行连接之前，必须要能让客户 PC 获取到 DNS 解析的 IP 地址，以及网关的 ARP 报文。在这种情况下，接入设备放行未认证用户发给网关的 ARP 请求报文。因此，有可能出现一种 ARP 欺骗情况，即如果某个用户冒充同一个 VLAN 下的其它用户的 IP，给网关发送 ARP 报文，就会造成网关学习到错误的 ARP，对同一 VLAN 下的其它用户产生影响；

配置步骤

打开全局客户端下载功能

```
Ruijie# config
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# dot1x redirect
```

在接入交换机上设置认证服务器的 IP 地址

```
Ruijie(config)# http redirect 192.168.3.1
```

在接入交换机上设置客户端下载的主页地址

```
Ruijie(config)# http redirect homepage http://www.su_download.com/su/index.jsp
```

在接入交换机上对 Fa0/2、Fa0/3 两个端口上开启 dot1x 认证功能

```
Ruijie(config)# interface range fa0/2-3
Ruijie(config-if-range)# dot1x port-control auto
Ruijie(config-if-range)# exit
```

在接入交换机上设置免认证的网络资源范围，将公共服务器设置为直通的网站

```
Ruijie(config)# http redirect direct-site 192.168.5.1
```

如果打开了 ARP Check 功能，则需要加上 arp 选项：

```
Ruijie(config)# http redirect direct-site 192.168.5.1 arp
```

若开启 ARP 功能，则还必须将网关 IP 地址设置为免认证的网络资源范围，并开启 arp 选项，以保证在认证前，PC 能完成 DNS 及 ARP 请求。

在接入交换机上将下联 PC 的网关 192.168.4.1 设置免认证的网络资源范围

```
Ruijie(config)# http redirect direct-site 192.168.4.1 arp
```

至此 PC1/PC2 如果未认证要访问 internet 就会先重定向到客户端下载服务器，通过客户端的下载及认证后，才能访问 internet。

显示验证

显示 HTTP 重定向的配置：

```
Ruijie# show http redirect
http redirect settings
 server          : 192.168.3.1
 port            : 80
```

```
 homepage       : http://www.su_download.com/su/index.jsp
 session-limit : 3
 timeout        : 3

direct-site
  Address           Mask              ARP Binding
  --------------- ---------------- -----------
  192.168.4.1      255.255.255.255    On
  192.168.5.1      255.255.255.255    On
```

6 SSH 终端服务

6.1 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	SSH1	SSH2
签名认证算法	RSA	RSA、DSA
密钥交换算法	基于 RSA 公钥加密的密钥交换算法。	KEX_DH_GEX_SHA1 KEX_DH_GRP1_SHA1 KEX_DH_GRP14_SHA1
加密算法	DES、3DES、Blowfish	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	基于用户口令的认证方式
消息认证算法	不支持	MD5、SHA1、SHA1-96、MD5-96
压缩算法	NONE（无压缩）	NONE（无压缩）

6.2 SSH配置

6.2.1 缺省的 SSH 配置

项目	缺省值
SSH 服务端状态	关闭
SSH 版本	兼容模式（支持版本 1 和 2）
SSH 用户认证超时时间	120s
SSH 用户重认证次数	3 次

6.2.2 用户认证配置

- 基于 SSH 连接安全性的考虑，禁止使用无认证方式登录。因此在用户登录认证时，所使用的登录认证方式必须设置密码；（Telnet 可以设置无认证登录）
- 每次输入的用户名(Username)与密码(Password)长度必须大于零。如果当前认证方式不需要用户名时，用户名可以任意输入，但是输入长度必须大于零。

6.2.3 打开 SSH Server

缺省情况下，SSH Server 处于关闭状态。打开 SSH Server，需要在全局配置模式下，执行 **enable service ssh-server** 命令，同时需要生成 SSH 密钥，使 SSH Server 的状态成为 ENABLE。

命令	作用
Ruijie**# configure terminal**	进入配置模式
Ruijie(config)**# enable service ssh-server**	打开 SSH Server
Ruijie(config)**# crypto key generate** {**rsa**|**dsa**}	生成密钥

删除密钥时，不存在命令**[no] crypto key generate**；而是通过命令 **crypto key zeroize** 命令删除密钥。

SSH 模块不支持热备，因此在支持管理板热备份的产品中，管理板切换动作发生后，若新的主板上没有 SSH 密钥文件，则必须通过命令 **crypto key generate** 重新生成密钥后方可使用 SSH。

6.2.4 关闭 SSH Server

关闭 SSH Server，需要在全局配置模式下，执行 **no enable service ssh-server** 命令，使 SSH Server 的状态成为 DISABLE。

命令	作用
Ruijie**# configure terminal**	进入配置模式
Ruijie(config)**# no enable service ssh-server**	关闭 SSH Server

6.2.5 配置 SSH server 支持版本

缺省情况下，SSH Server 兼容版本 1 和 2。使用以下命令配置 SSH 使用版本。

命令	作用
Ruijie**# configure terminal**	进入配置模式
Ruijie(config)**# ip ssh version** {**1**|**2**}	配置 SSH 支持的版本
Ruijie(config)**# no ip ssh version**	恢复 SSH 为缺省配置，支持 SSHv1 与 SSHv2；

6.2.6 配置 SSH 用户认证超时时间

缺省情况下，SSH Server 的用户认证超时时间为 120 秒。使用以下命令配置 SSH 的用户认证超时时间。

命令	作用
Ruijie**# configure terminal**	进入配置模式
Ruijie(config)**# ip ssh time-out** *time*	配置 SSH 的超时时间（范围 1-120sec）
Ruijie(config)**# no ip ssh time-out**	恢复 SSH 的缺省用户认证超时时间为 120 秒；

6.2.7 配置 SSH 重认证次数

该配置命令用来设置 SSH 用户请求连接的认证重试次数，防止恶意猜测等非法行为。缺省情况下，SSH Server 的重认证次数为 3 次，即可以允许用户尝试三次输入用户名与密码进行认证尝试。使用以下命令配置 SSH 的重认证次数。

命令	作用
Ruijie**# configure terminal**	进入配置模式
Ruijie(config)**# ip ssh authentication-retries** *retry times*	配置 SSH 的重认证次数（范围 0-5）
Ruijie(config)**# no ip ssh authentication-retries**	恢复 SSH 的重认证次数为 3 次

上述命令具体配置请参见[SSH 命令参考手册]。

6.2.8 配置 SSH 加密模式

该命令用来配置 SSH 的加密模式，提高 SSH 的安全级别。缺省情况下，SSH 支持的加密模式为兼容模式（支持 cbc、ctr 和其它类）。使用下面命令配置 SSH 的加密模式。

命令	作用
Ruijie**# configure terminal**	进入配置模式
Ruijie(config)**# ip ssh cipher-mode { cbc | ctr | others }**	设置 SSH Server 支持的加密模式
Ruijie(config)**# no ip ssh cipher-mode**	恢复 SSH Server 支持的加密模式为缺省设置

上述命令具体配置请参见《SSH 命令》手册。

6.2.9 配置 SSH 消息认证算法

该命令用来配置 SSH 的消息认证算法，用户可以依据实际需要选择 SSH Server 支持的消息认证算法。缺省情况下 SSH Server 支持的消息认证算法为：SSHv1 不支持，SSHv2 支持 4 种（MD5、SHA1、SHA1-96、MD5-96）。使用下面命令配置 SSH 的消息认证算法。

命令	作用
Ruijie**# configure terminal**	进入配置模式
Ruijie(config)**# ip ssh hmac-algorithm { md5 | md5-96 | sha1 | sha1-96 }**	设置 SSH Server 支持的消息认证算法
Ruijie(config)**# no ip ssh hmac-algorith**	恢复 SSH Server 支持的消息认证算法为缺省设置

上述命令具体配置请参见《SSH 命令》手册。

6.2.10 配置 SSH 基于公钥的认证

根据 SSH 协议，只有 SSHv2 才支持基于公钥的认证，SSHv1 不支持。以下命令将客户端的公钥文件和用户名关联，客户端登录认证时，通过用户名指定使用的公钥文件。

命令	作用

Ruijie**# configure terminal**	进入配置模式
Ruijie(config)**# ip ssh peer** *test* **public-key rsa flash**:*rsa.pub*	设置用户 *test* 关联的 RSA 公钥文件
Ruijie(config)**# ip ssh peer** *test* **public-key dsa flash**:*dsa.pub*	设置用户 *test* 关联的 DSA 公钥文件

上述命令具体配置请参见《SSH 命令》手册。

6.2.11 配置 SCP 服务功能

在网络设备上打开 SCP 服务器功能，用户可以直接对网络设备上的文件进行下载，以及将本地文件上传至网络设备，同时所有交互数据以密文形式进行传输，具有认证和安全性等特性。

命令	作用
Ruijie**# configure terminal**	进入配置模式
Ruijie(config)**#ip scp server enable**	开启 SCP 服务器功能
Ruijie(config)**# no ip scp server enable**	关闭 SCP 服务器功能

上述命令具体配置请参见《SSH 命令》手册。

6.3 SSH Client配置

6.3.1 配置 SSH Client 源接口

该命令用于指定接口上的 IP 地址作为 SSH Client 连接的全局源地址。缺省情况下，SSH 协议报文将使用目的地址的发包源地址，作为报文的源地址。使用下面命令配置 SSH Client 源接口。

命令	作用
Ruijie**# configure terminal**	进入配置模式
Ruijie(config)**# ip ssh source-interface *interface-name***	指定 SSH Client 的源接口
Ruijie(config)**# no ip ssh source-interface**	清除 SSH Client 的源接口配置

上述命令具体配置请参见《SSH 命令》手册。

6.3.2 使用 SSH Client 与 SSH Server 建立连接

该命令用于需要在设备上通过 SSH Client 向远端服务器发起 SSH 连接。使用该命令前，需要在服务器端开启 SSH server 功能，配置 SSH 密钥和认证方式。使用下面命令建立 SSH Client 和 SSH Server 的连接。

命令	作用

Ruijie# **ssh** [**-v** { **1** | **2** }] [**-c** { **3des** | **aes128-cbc** | **aes192-cbc** | **aes256-cbc** }] [**-l** *username*] [**-m** { **hmac-md5-96** | **hmac-md5-128** | **hmac-sha1-96** | **hmac-sha1-160** }] [**-p** *port-num*] { *ip-addr* | *hostname* } [**/vrf** *vrf-name*]	建立 SSH Client 和 SSH Server 的连接

上述命令具体配置请参见《SSH 命令》手册。

6.3.3 恢复已建立的 SSH Client 会话连接

该命令用于恢复已经建立的 SSH Client 会话连接。使用下面命令建立 SSH Client 和 SSH Server 的连接。当使用 **ssh** 命令发起 SSH Client 会话连接时，可以使用热键（ctrl+shift+6 x）暂时退出该连接。如果需要恢复该连接，可以使用 **ssh-session** 命令进行恢复。使用下面命令恢复已经建立的 SSH Client 会话连接。

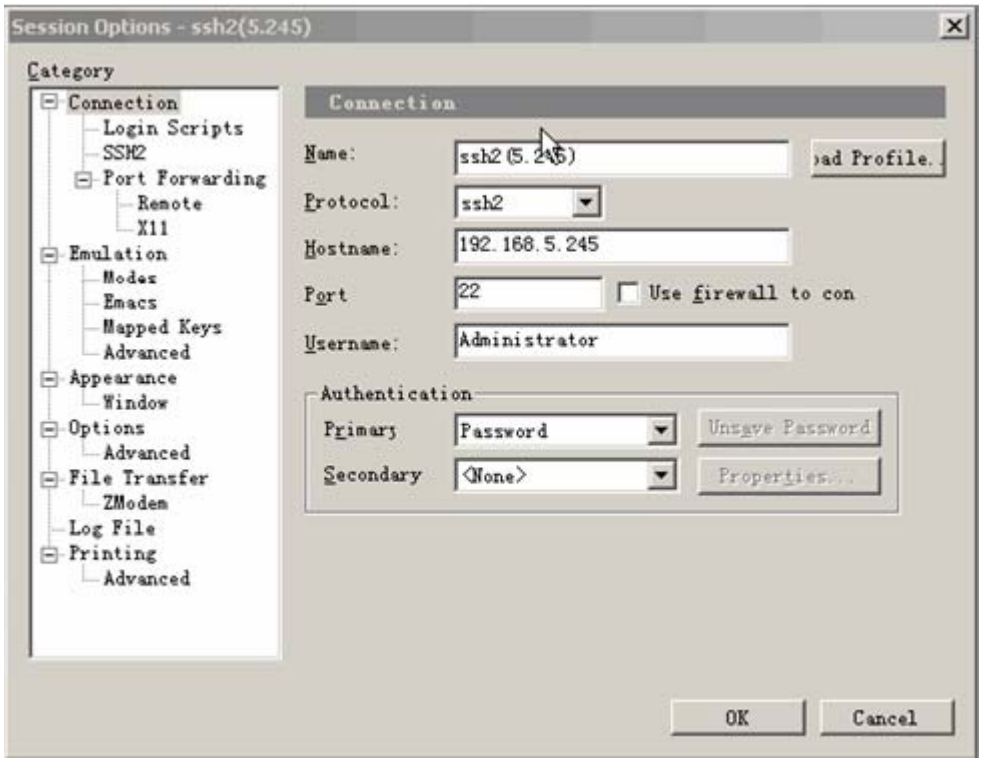
命令	作用
Ruijie# **ssh-session *session-id***	恢复已经建立的 SSH Client 会话连接

上述命令具体配置请参见《SSH 命令》手册。

6.4 使用SSH进行设备管理

您可以使用 SSH 对设备进行管理，前提是必须打开 SSH Server 功能，默认情况下是关闭该功能的。由于 Windows 自带的 Telnet 组件不支持 SSH，因此必须使用第三方客户端软件，当前兼容性较好的客户端包括：Putty，Linux，SecureCRT。下面以客户端软件 SecureCRT 为例介绍 SSH 客户端的配置，配置界面如下图：

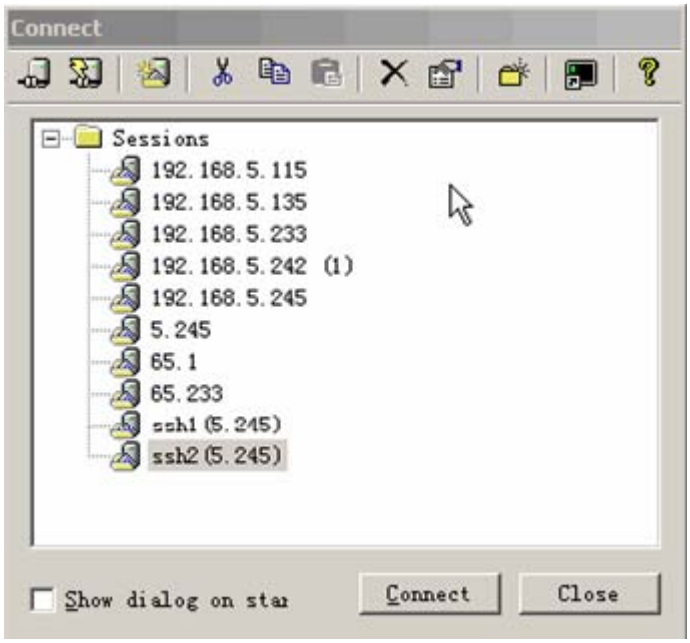
图 6-1



如图使用协议 2 进行登陆，因此在 Protocol 选择 SSH2，Hostname 就是要登陆的主机的 IP 地址，这里为 192.168.5.245，端口为 22 即 SSH 监听的默认端口号，Username 为用户名，当设备只要求密码时，该用户名不会起作用，Authentication 为认证方式，我们只支持用户名密码的认证方式。使用的密码和 Telnet 密码是一致的。

然后点击 OK，进入出现以下的对话框：

图 6-2



点击 Connect，登陆我们刚才配置的主机，如下图：

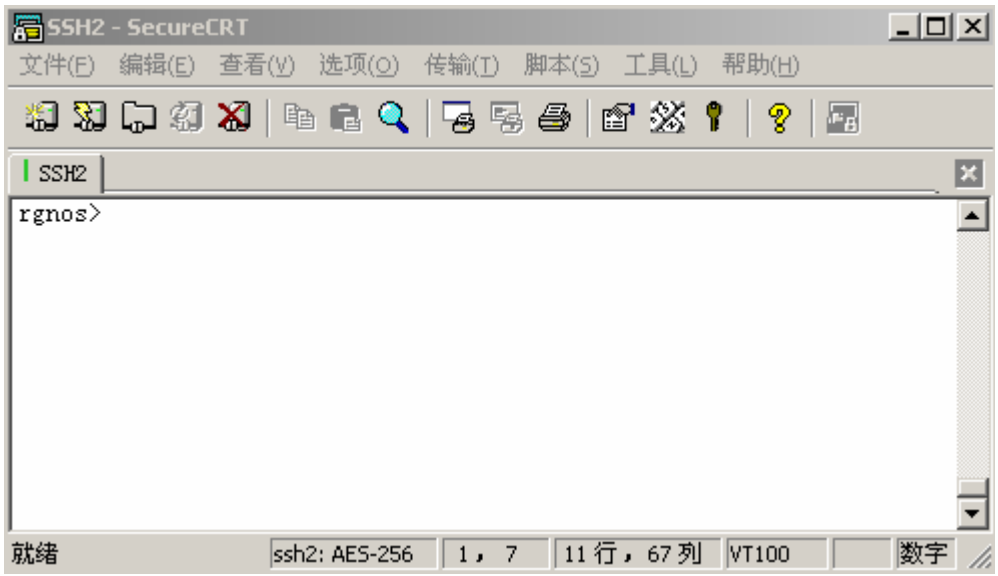
图 6-3

询问正在登陆主机 192.168.5.245 的机器，是否接收服务端发送过来的密钥，选择 Accept & Save（接受而且保存）或者 Accept Once（只接受一次），接着会出现下面的密码认证对话框，如下图：

图 6-4

此时输入 Telnet 登陆密码就可以进入和 Telnet 一样的界面了。如下图显示：

图 6-5



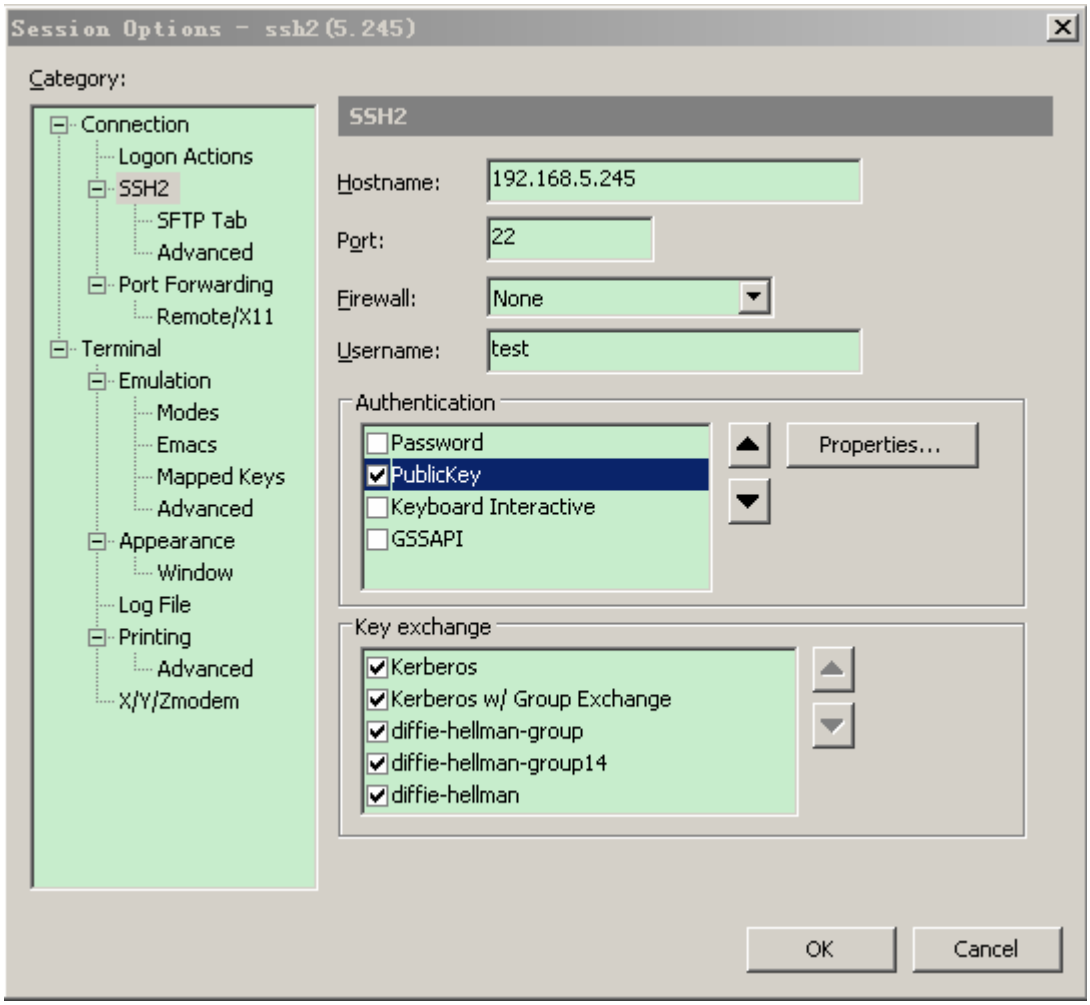
6.5 使用SSH基于公钥的认证

客户端操作

客户端公钥认证方式，首先要在客户端生成一个密钥对（RSA 或 DSA），然后将其中的公钥放置在 SSH 服务器上，然后选择使用 PublicKey 认证方式。下面以以客户端软件 SecureCRT 为例，介绍在客户端生成密钥对的方法。

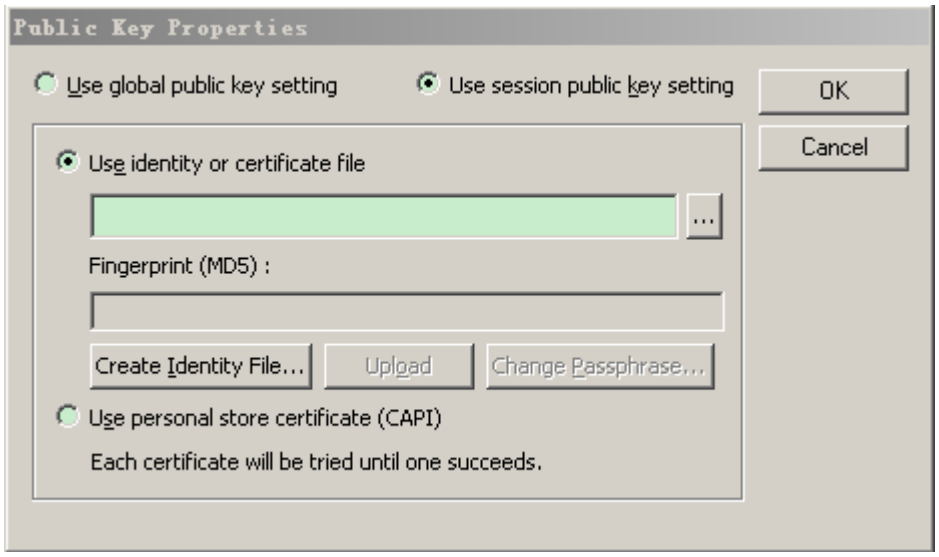
首先，在 Session Option 中 Authentication 选项，选择 PublicKey，然后选择 Properties。如下：

图 6-6



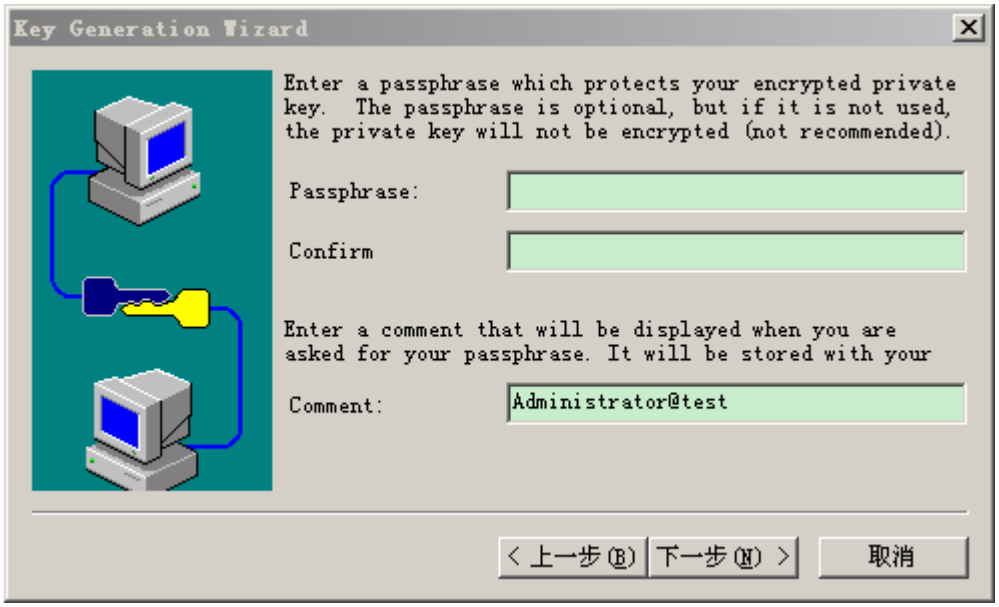
然后点击 Properties...。如果已经生成过密钥对，则可以选择使用的私钥（Use identity or certificate file），注意这个私钥一定要和服务器上的公钥是一对的，否则不能认证通过。如下：

图 6-7



如果没有生成过，可以生成一个新的密钥对（Create Identity File）。在生成密钥中，可以为私钥再设置一个口令（可以为空），如果设置，则每次认证都需要输入这个口令。如下：

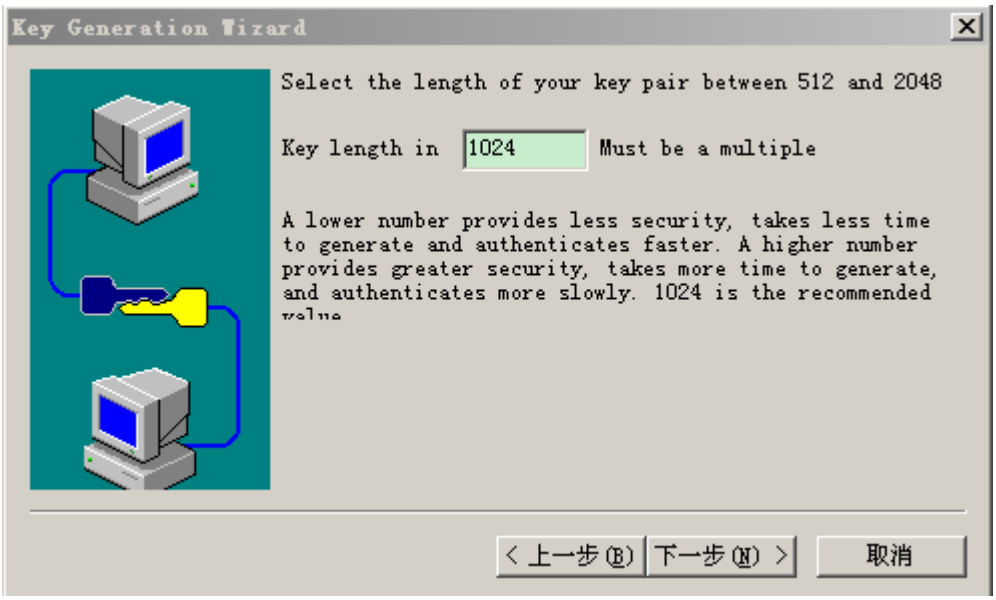
图 6-8



生成密钥的时候要不断晃动鼠标，否则速度极慢;

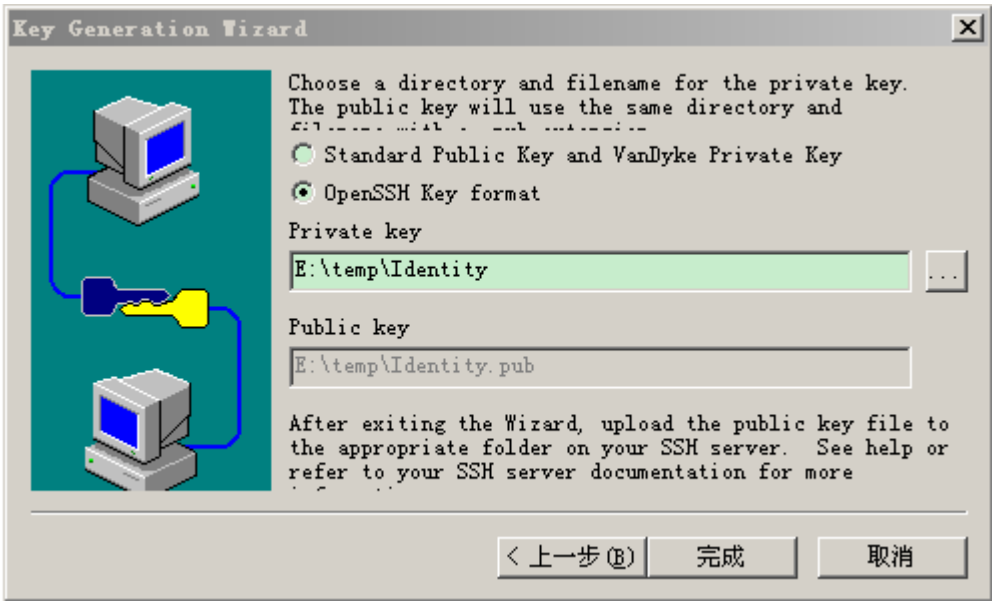
一定要选择使用 OpenSSH 格式的密钥文件，否则不能使用。如果使用 Putty 作为客户端，还需要使用 puttygen.exe 工具把私钥转换成 Putty 格式（puttygen.exe 能生成 OpenSSH 格式的密钥对，但是 Putty 却不能直接使用）。放在服务器上的公钥文件不需要转换，还是 OpenSSH 格式。如下:

图 1-9



为了保证 RSA 公钥认证的安全性，生成 RSA 密钥对时，RSA 密钥对的长度必须大于或等于 768 位。

图 6-10



服务器端操作

在客户端生成了密钥以后，SSH 服务器端（即网络设备）需要将客户端的公钥文件复制到 flash 中，并且与 SSH 用户名关联。每个用户可以关联一个 RSA 公钥和一个 DSA 公钥。如下：

```
Ruijie# configure terminal
Ruijie(config)# ip ssh peer test public-key rsa flash:rsa.pub
Ruijie(config)# ip ssh peer test public-key dsa flash:dsa.pub
```

这样，客户端就可以使用公钥认证方式登录网络设备了。

6.6 使用SSH进行文件传输

服务器端操作

SSH 文件传输使用是 SCP 协议（Secure CoPy），客户端要使用 SCP，将文件传输到网络设备上，或者从网络设备上下载文件，首先需要在网络设备上开启 SCP 服务器功能。如下：

```
Ruijie# configure terminal
Ruijie(config)# ip scp server enable
```

这样，客户端就可以使用 SCP 连接服务器并传输文件了。SCP 服务器使用的是 SSH 线程，客户端连接网络设备进行 SCP 传输时候会占用一个 VTY 连接（通过 show user 命令查看的时候，会发现用户类型为 SSH）。

客户端操作

在 Unix 和 Linux 平台上都带有 SCP 命令，以 Ubuntu Linux 为例，介绍 SCP 命令的使用。如下：

```
SCP 命令的语法：
    scp [-1246BCpqrv] [-c cipher] [-F ssh_config] [-i identity_file]
```

```
        [-l limit] [-o ssh_option] [-P port] [-S program]
        [[user@]host1:]file1 [...] [[user@]host2:]file2
```

部分选项说明：

-1 ： 使用 SSH1 版本（若不指定则默认使用 SSH2）；

-2 ： 使用 SSH2 版本（默认）；

-C ： 指定使用压缩传输；

-c ： 指定使用的加密算法；

-r ： 指定传输整个目录；

-i ： 指定使用的密钥文件；

-l ： 限制传输速度（单位 Kbits）；

其他具体的参数可以查看 scp.0 文件。

文件传输举例，以在 Ubuntu 7.10 系统上操作为例：

指定用户名是 test，从 IP 为 192.168.195.188 的网络设备上，将 config.text 文件复制到本地的/root 目录下。如下：

```
root@dhcpd:~# scp test@192.168.195.188:/config.text /root/config.text
test@192.168.195.188's password:
config.text                   100% 1506     1.5KB/s   00:00
Read from remote host 192.168.195.188: Connection reset by peer
```

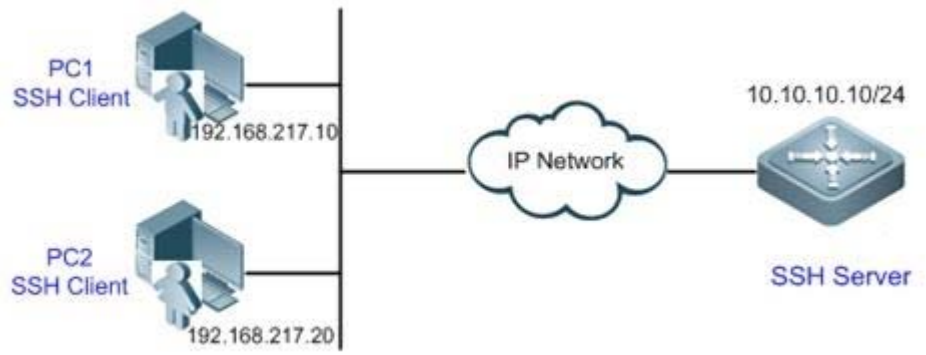
选项大部分与客户端有关，少数是客户端和服务器都需要支持的选项，但我司网络设备上的 SCP 服务器端不支持-d -p –q -r 选项，使用这些选项时候会提示不支持。

下载文件时候，如果没有进行限速（即使用-l 选项），则下载过程中会导致网络设备的 CPU 利用率升高，下载结束以后恢复正常。控制台仍然可以使用，但其他应用态的任务会受到影响。

6.7 SSH典型配置举例

6.7.1 SSH 本地线路认证配置举例

图 6-9 SSH 本地线路口令保护组网图



应用需求

如上图所示，为了保证数据信息交换的安全，PC1、PC2 作为 SSH 客户端，采用 SSH 协议登录到打开 SSH Server 的网络设备上。具体要求如下：

- SSH 用户采用的认证方式为线路口令认证。
- 同时启用 0-4 这五条线路，其中线路 0 的登录口令为“passzero”，其余四条线路的登录口令均为“pass”，用户名任意。

配置要点

- SSH Server 的配置要点如下：

1) 全局打开 SSH Server。SSH Server 默认支持 SSH1 和 SSH2 两个版本。

2) 配置密钥。通过该密钥，SSH 服务器将从 SSH 客户端那收到的口令密文进行解密，将解密后的明文同服务器上保存的口令进行比较，并返回认证成功或失败的消息。SSH 1 使用 RSA 密钥；SSH 2 使用 RSA 或者 DSA 密钥。

3) 配置 SSH 服务器 Gi 1/1 接口的 IP 地址。SSH 客户端通过该地址连接 SSH 服务器。SSH 客户端至 SSH 服务器路由可达。

- SSH Client 的设置：

SSH 客户端软件有多种，例如 Putty、Linux、OpenSSH 等，本文中仅以客户端软件 SecureCRT 为例，说明 SSH 客户端的配置方法。具体配置方法请参见“配置步骤”

配置步骤

- SSH Server 的配置

配置 SSH 相关功能之前，请先确保 SSH 用户到 SSH 服务器所在网段的路由可达。接口 IP 配置如拓扑图所示。具体 IP 及路由配置过程此处省略。

第一步，打开 SSH Server 功能

```
Ruijie(config)# enable service ssh-server
```

第二步，生成 RSA 密钥

```
Ruijie(config)#crypto key generate rsa
% You already have RSA keys.
% Do you really want to replace them? [yes/no]:
Choose the size of the key modulus in the range of 360 to 2048 for your
Signature Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]:
% Generating 512 bit RSA1 keys ...[ok]
% Generating 512 bit RSA keys ...[ok]
```

第三步，配置 Gi 1/1 的接口地址，客户端将通过该地址连接 SSH 服务器。

```
Ruijie(config)#interface gigabitEthernet 1/1
Ruijie(config-if-gigabitEthernet 1/1)#ip address 10.10.10.10 255.255.255.0
```

```
Ruijie(config-if-gigabitEthernet 1/1)#exit
```

第四步，配置线路登录口令

！配置线路 0 的登录口令为“passzero”

```
Ruijie(config)#line vty 0
Ruijie(config-line)#password passzero
Ruijie(config-line)#privilege level 15
Ruijie(config-line)#exit
```

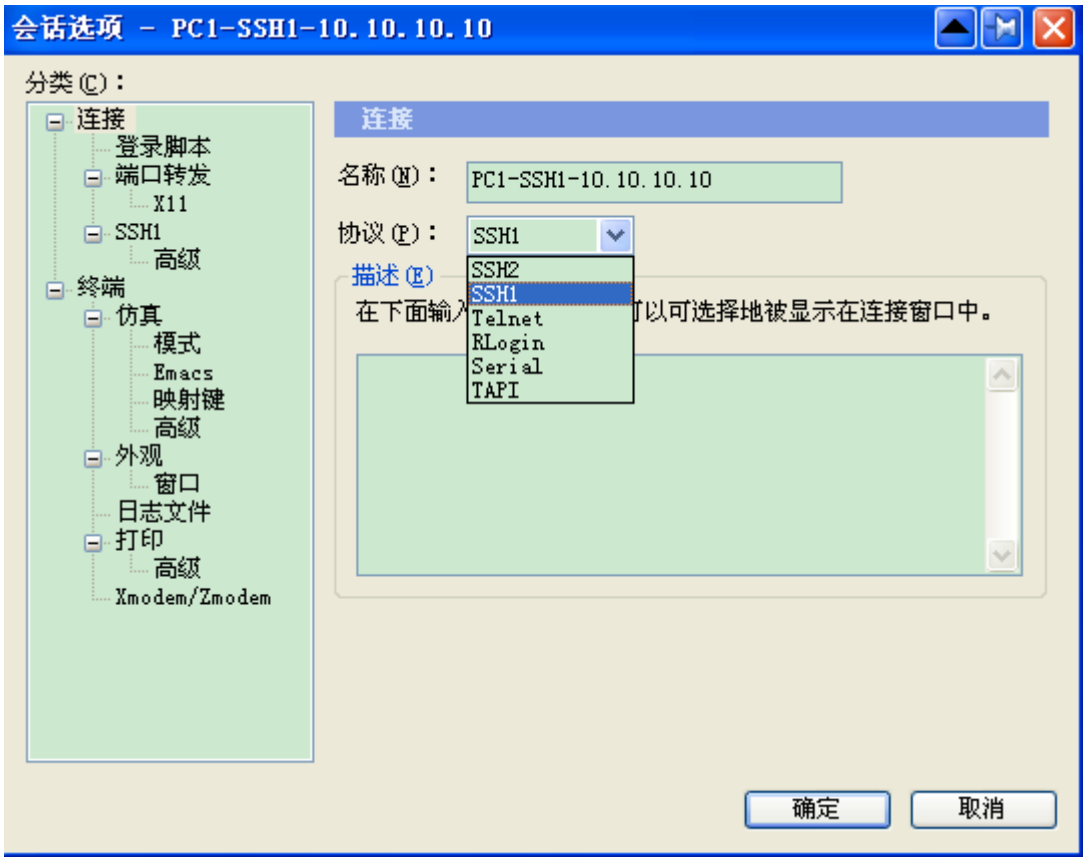
！配置线路 1 - 4 的登录口令为“pass”

```
Ruijie(config)#line vty 1 4
Ruijie(config-line)#password pass
Ruijie(config-line)#privilege level 15
Ruijie(config-line)#exit
```

■ SSH Client（PC1/PC2）的配置

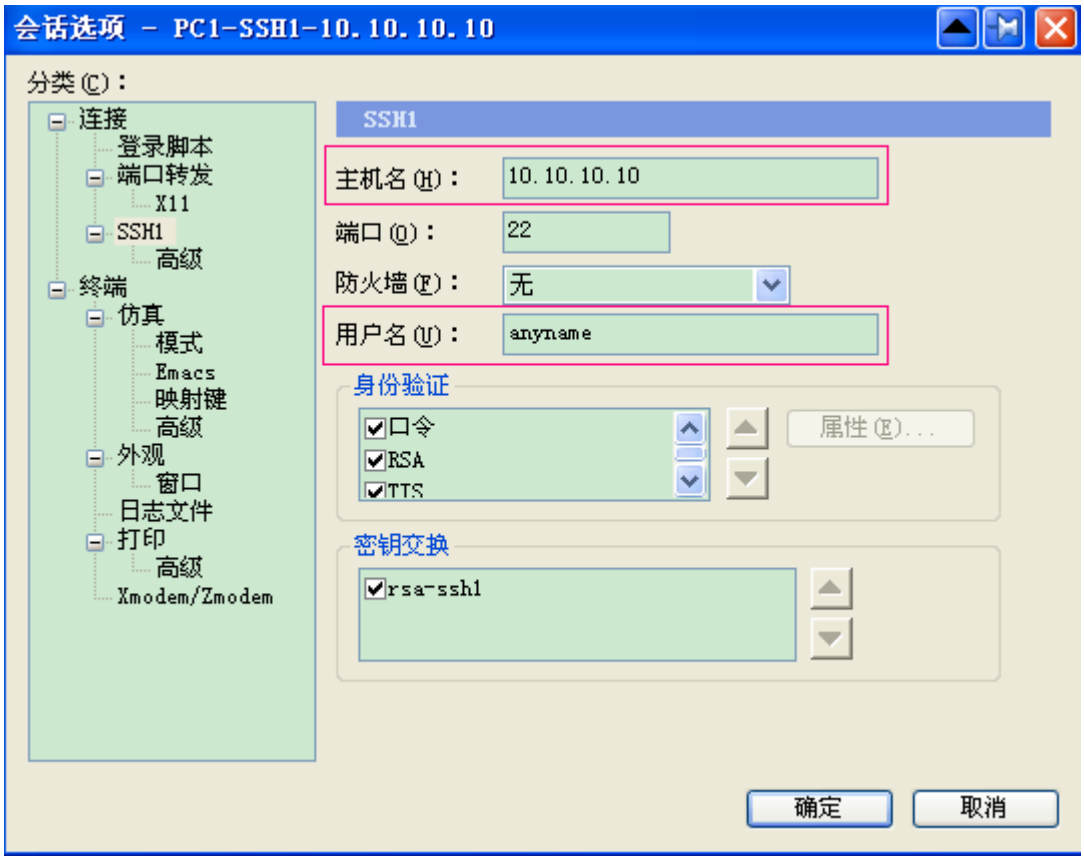
打开 SecureCRT 的连接框，如下图所示，选择使用 SSH1 进行认证登录。会话名称任意（本例名称设置为 PC1-SSH1-10.10.10.10）。

图 6-10



进行 SSH 属性设置。主机名为 SSH 服务器的 IP 地址，本例为 10.10.10.10。由于当前认证方式不需要用户名，此处“用户名”文本框中的用户名信息可以任意输入，但是不能为空（本例用户名设置为 anyname）。

图 6-11



配置验证

- 验证 SSH Server 的配置

第一步，可通过 **show running-config** 命令来查看当前配置信息的正确性：

```
Ruijie#show running-config
Building configuration...
!
enable secret 5 $1$eyy2$xs28FDw4s2q0tx97
enable service ssh-server
!
interface gigabitEthernet 1/1
 ip address 10.10.10.10 255.255.255.0
!
line vty 0
privilege level 15
 login
 password passzero
line vty 1 4
privilege level 15
 login
```

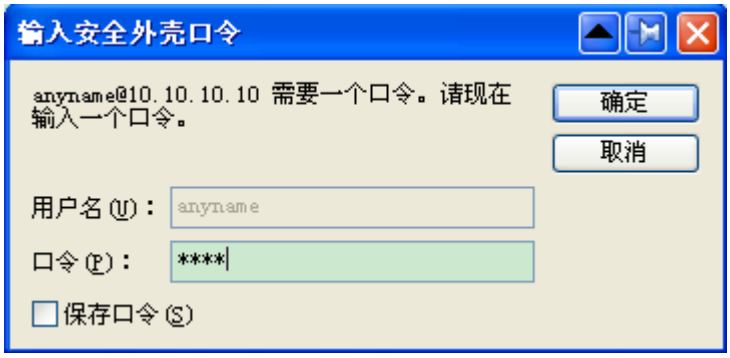
```
 password pass
!
end
```

■ 验证 SSH Client 的配置

第一步，建立远程连接。

建立连接，输入正确的口令。线路 0 的登录口令线路 0 的登录口令为“passzero”，其余四条线路的登录口令均为“pass”，即可进入 SSH Server 的操作界面。

图 6-12

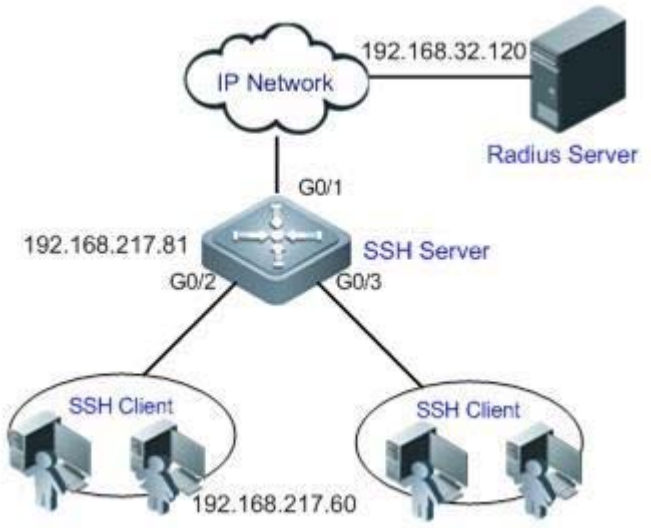


第二步，查看登录用户。

```
Ruijie#show users
    Line         User         Host(s)              Idle       Location
   0 con 0                   idle                 00:03:16
   1 vty 0                   idle                 00:02:16   192.168.217.10
*  2 vty 1                   idle                 00:00:00   192.168.217.20
```

6.7.2 SSH 的 AAA 认证配置举例

图 6-13 SSH AAA 认证组网图



应用需求

如上图所示，为了保证数据信息交换的安全，PC 作为 SSH 客户端，采用 SSH 协议登录到打开 SSH Server 的网络设备上。

为了更好地进行安全管理，SSH 客户端登录用户界面采用 AAA 认证方式；同时出于稳定性方面考虑，在 AAA 认证方法列表中配置两种认证方法：Radius 服务器认证和本地认证。优先选择 Radius 服务器，当 Radius 服务器没有响应时选择本地认证方法。

配置要点

- SSH 客户端到 SSH 服务器端的路由可达，SSH 服务器到 Radius 服务器端的路由可达。
- 在网络设备上进行 SSH Server 相关配置。配置要点在上一个例子中已有描述，不再重复说明。
- 在网络设备上进行 AAA 认证相关配置。AAA 通过创建方法列表来定义身份认证、类型，然后将这些方法列表应用于特定的服务或接口上。具体说明请参见“配置步骤”章节。

配置步骤

SSH 客户端到 SSH 服务器、Radius 服务器间的路由可达。有关路由相关配置本例不具体说明，请参见本手册路由配置部分。

- 在网络设备上配置 SSH 相关功能

第一步，打开 SSH Server 功能

```
Ruijie(config)# enable service ssh-server
```

第二步，生成密钥

！生成 RSA 密钥

```
Ruijie(config)#crypto key generate rsa
% You already have RSA keys.
```

```
% Do you really want to replace them? [yes/no]:
Choose the size of the key modulus in the range of 360 to 2048 for your
Signature Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]:
% Generating 512 bit RSA1 keys ...[ok]
% Generating 512 bit RSA keys ...[ok]
```

！生成 DSA 密钥

```
Ruijie(config)#crypto key generate dsa
Choose the size of the key modulus in the range of 360 to 2048 for your
Signature Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]:
% Generating 512 bit DSA keys ...[ok]
```

第三步，配置设备的 IP 地址，客户端将通过该地址连接 SSH 服务器。

```
Ruijie(config)#interface gigabitEthernet 1/1
Ruijie(config-if-gigabitEthernet 1/1)#ip address 192.168.217.81 255.255.255.0
Ruijie(config-if-gigabitEthernet 1/1)#exit
```

■ 在网络设备上配置 AAA 认证相关功能

第一步，设备启用 AAA 功能

```
Ruijie#configure terminal
Ruijie(config)#aaa new-model
```

第二步，配置 Radius 服务器信息(设备和 RADIUS 服务器进行通讯的共享密码为“aaaradius”

```
Ruijie(config)#radius-server host 192.168.32.120
Ruijie(config)#radius-server key aaaradius
```

第三步，配置 AAA 认证方法列表

！配置 login 认证方法列表（按 Radius、Local 的次序），方法列表名为“*method*”

```
Ruijie(config)#aaa authentication login method group radius local
```

第四步，在线路上应用该方法列表

```
Ruijie(config)#line vty 0 4
Ruijie(config-line)#login authentication method
Ruijie(config-line)#exit
```

第五步，配置本地用户数据库

！ 配置本地用户数据库（配置用户名和口令信息并绑定用户级别）

```
Ruijie(config)#username user1 privilege 1 password 111
Ruijie(config)#username user2 privilege 10 password 222
```

```
Ruijie(config)#username user3 privilege 15 password 333
```

！ 配置本地 enable 口令，用于本地 enable 认证

```
Ruijie(config)#enable secret w
```

配置验证

第一步，可通过 **show running-config** 命令来查看当前配置信息的正确性：

```
Ruijie#show run
aaa new-model
!
aaa authentication login method group radius local
!
username user1 password 111
username user2 password 222
username user2 privilege 10
username user3 password 333
username user3 privilege 15
no service password-encryption
!
radius-server host 192.168.32.120
radius-server key aaaradius
enable secret 5 $1$hbgz$ArCsyqty6yyzzp03
enable service ssh-server
!
interface gigabitEthernet 1/1
 no ip proxy-arp
 ip address 192.168.217.81 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 192.168.217.1
!
line con 0
line vty 0 4
 login authentication method
!
end
```

第二步，在 Radius Server 上的设置。本例以 SAM 服务器为例进行说明。

【系统管理】-【设备管理】中，添加设备 IP 地址：192.168.217.81，添加设备 Key：aaaradius

【安全管理】-【设备管理权限】中，设置登录用户的权限。

【安全管理】-【设备管理员】中，添加用户名：user；口令：pass。

第三步，在 PC 机上建立远程 SSH 连接。

SSH 客户端软件设置、建立连接；SSH 客户端的创建方法请参见上例。

输入正确的口令，SSH 用户名为：user；口令为：pass。登录成功。

第四步，查看登录用户。

```
Ruijie#show users
    Line         User         Host(s)              Idle       Location
   0 con 0                    idle                 00:00:31
 * 1 vty 0      user          idle                 00:00:33   192.168.217.60
```

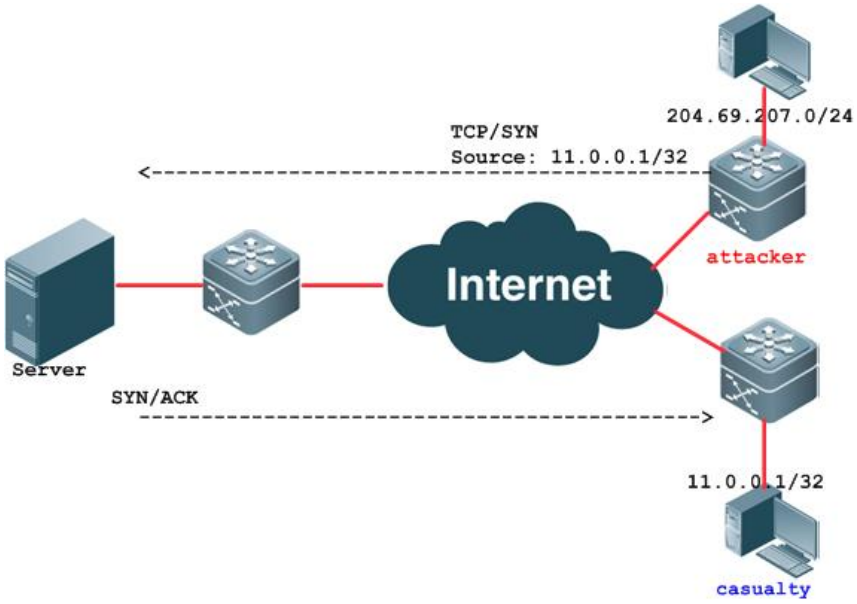
7 URPF

7.1 URPF概述

近来，采用伪造源地址产生的 DOS (Denial of service，拒绝服务)攻击常常发生，给 ISP 和网络维护带来了许多问题。

下图为一种常见的采用伪造源地址进行 DOS 攻击的场景：

图 7-1 源地址攻击场景



攻击者伪造真实存在的源地址 11.0.0.1 的报文发起攻击，导致服务器发送大量的 SYN/ACK 报文给与攻击无关的主机上，使得拥有真实源地址的主机也遭受了影响。更严重的是，如果网络管理员判定该地址对网络产生了攻击，而关闭所有来自该源地址的数据流，则对该源地址产生了拒绝服务的现象。

URPF (Unicast Reverse Path Forwarding，单播反向路径转发)技术的提出，有效的解决了上述问题。

我们知道，报文转发是根据接收到的 IP 报文的目的地址，查找转发表，根据找到的转发表项进行报文转发。URPF 技术，通过获取接收报文的源地址和入接口，根据源地址在转发表中查找转发表项，如果表项不存在，那么报文丢弃；如果转发表项的出接口与报文的入接口不匹配，那么报文丢弃。否则，认为匹配，允许报文转发。

通过 URPF 技术，能够一定程度地阻断源地址欺骗攻击，达到保护网络的效果。

7.2 URPF特性

7.2.1 URPF 严格模式

传统意义上的 URPF 技术要求：通过获取接收报文的源地址和入接口，根据源地址在转发表中查找转发表项，如果表项不存在，那么报文丢弃；如果转发表项的出接口与报文的入接口不匹配，那么报文丢弃。即要求“接收报文的入口一定是到达该报文源地址的路由表项的出口”。我们把严格遵守这种要求的 URPF 检查方式称为 URPF 严格模式。

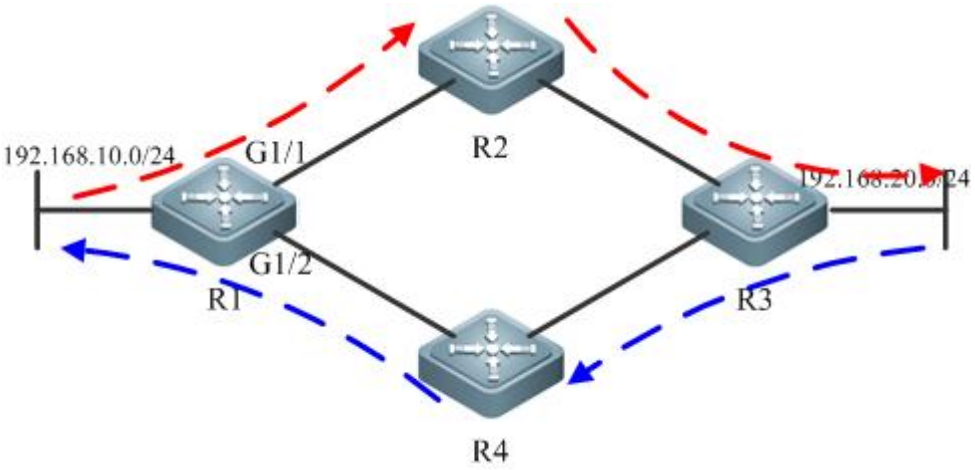
URPF 严格模式通常部署在点对点的接口上，并且数据流双向都需要通过该点对点接口。

7.2.2 URPF 宽松模式

URPF 严格模式在网络应用上存在着局限性，典型的情况包括非对称路由环境以及多宿主网络环境下，URPF 严格模式无法适用。

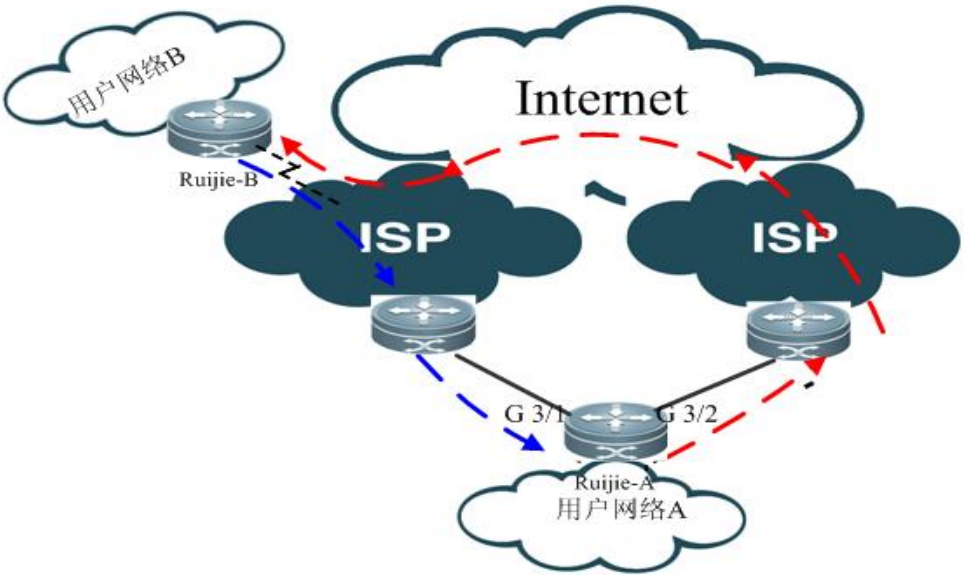
由于控制网络流量或者路由策略需要，非对称路由是比较常见的网络应用。图 2 是非对称路由的一个例子，如果在 R1 设备的 G1/2 设备上启动 URPF 严格模式，那么如果在 G1/2 设备收到 192.168.20.0/24 网段的数据包时，进行 URPF 检查得到的接口为 G1/1，该报文将无法通过 URPF 检查。启动 URPF 严格模式，那么会导致数据流丢失。

图 7-2 非对称路由



多宿主网络常见在用户同 ISP 之间，或者 ISP 之间的网络应用。如图 3 所示，用户网络 A 同时连接有多个 ISP，往返的流量也常常是不对称的，如图所示的用户网络 A 访问用户网络 B。

图 7-3 多宿主网络



在上述两种应用场景中，如果使用 URPF 严格模式，会使得合法的报文被过滤，所以在这种情况下，引入了 URPF 宽松模式的概念。

URPF 宽松模式：根据接收报文的源 IP 进行反向路由查找，只要找到路由即可，不要求路由的下一跳出口一定是接收报文的入口。通过引入 URPF 宽松模式能够解决了上述非对称路由和多宿主网络存在的流量非对称问题。

7.3 工作原理

URPF的工作原理在 URPF特性一章已经描述。

URPF 特性能够根据配置应用于 IPv4/IPv6 报文，但注意，如下报文将不会被 URPF 检查：

- URPF 检查只对目的地址为 IPv4/IPv6 报文的源地址进行检查，对目的地址为多播报文将跳过检查。
- 对于源 IP 地址为 0.0.0.0，目的 IP 地址为 255.255.255.255 的 DHCP/BOOTP 报文，跳过检查。
- 对于源 IP 地址为 Link local address 的 IPv6 报文，跳过检查。

7.3.1 应用限制

URPF 特性功能在交换机产品和路由器产品中还存在如下特征：

- 启动 URPF 特性后，源地址匹配到 NULL 口的路由，仍然会进行 URPF 检查，而不是进行丢弃处理。
- 启动 URPF 特性后，URPF 将先于安全 ACL(接口配置模式：**ip access-group in**)对报文进行检查。
- 启动 URPF 严格特性，在接口上接收到源地址为该接收接口地址的报文，报文将被丢弃。如果启动 URPF 宽松模式，报文将被放过。

7.3.2 协议规范

和 URPF 特性相关的协议规范有：

- RFC 2827, Network Ingress Filtering: DDOS Attacks which employ IP Source Address Spoofing
- RFC 3704, Ingress Filtering for Multi-homed Networks

7.4 配置URPF特性

以下章节描述如何配置 URPF 的基本特性：

- 缺省配置
- （必选）缺省配置
- 下表用来描述 URPF 的缺省配置。

功能特性	缺省值
URPF 全局配置模式	关闭

- 配置 URPF(全局配置模式)
- 查看 URPF 信息

7.4.1 缺省配置

下表用来描述 URPF 的缺省配置。

功能特性	缺省值
URPF 全局配置模式	关闭

7.4.2 配置 URPF(全局配置模式)

交换机产品插入 MPLS 线卡后，报文将通过 MPLS 线卡进行转发，此时要启动 URPF 特性，请按照如下步骤执行：

命令	作用
Ruijie**# configure terminal**	进入全局配置模式
Ruijie(config)**# ip verify unicast source reachable-via rx**	启动 URPF 特性 rx，使用严格模式进行 URPF 检查
Ruijie(config)**# end**	退出全局配置模式
Ruijie**# show ip urpf**	显示 URPF 配置及统计

如果要关闭全局 URPF 特性，请在全局配置模式下使用 **no ip verify** 命令进行设置。

- 全局配置模式配置 URPF 特性只在交换机产品插入 MPLS 线卡后才生效。URPF 特性生效后，将对 IPv4 报文启动 URPF 检查。
- 全局配置模式配置 URPF 特性只支持严格模式，但如果匹配等价路由，将转换为宽松模式处理。
- 全局配置模式配置 URPF 特性不支持使用缺省路由进行 URPF 检查。
- 不支持全局配置 URPF 特性和接口配置 URPF 特性共存。

配置举例：

配置在全局启动 URPF 特性：

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# ip verify unicast source reachable-via rx
```

7.4.3 查看 URPF 信息

URPF 提供了如下显示命令用于查看各种配置信息及统计信息：

命令	作用
show ip urpf [**interface** *interface-name*]	显示 URPF 配置及统计信息

此外，URPF 还提供如下命令用于清除 URPF 统计信息：

命令	作用
clear ip urpf [**interface** *interface-name*]	清除 URPF 检查丢包的统计信息

8 GSN

8.1 锐捷 GSN 安全方案简介

8.1.1 锐捷安全策略管理平台（RG Security policy Management Platform）

锐捷安全策略管理平台通过配置策略，来决定是否允许或者禁止某种条件范围内的数据报文通过安全设备进行传输。安装策略就是将策略设置到设备上，卸载策略就是将策略从设备上移除。

8.1.2 锐捷安全客户端

锐捷安全客户端是运行在企业网络中的每一台接入网络的主机上的一个软件，它负责收集客户端信息、认知用户的网络行为、监控客户机的网络通讯和安全状态并将收集到的信息发送到安全策略管理平台以便管理员针对性地制定相应的安全策略。同时安全客户端也将自动地从安全策略管理平台中下载新的安全策略并在本地执行指定的安全策略。

8.1.3 锐捷安全修复系统

安全修复系统对异常行为做如下操作：

对于不符合企业安全策略的用户，管理员在安全策略管理平台上预先配置相应的策略，这些策略可屏蔽这些“非法用户”的绝大部分的网络访问权限，只留下一条绿色的安全通道。这个安全通道连接到的主机只能是企业安全策略升级服务器。包括：Windows 补丁升级服务器、防病毒软件的病毒升级库服务器，或是企业的其他升级服务器。

当安全客户端在检测到自己的安全策略不符合管理平台制定的安全等级之后，安全代理会立即将自己的安全日志上传至安全策略管理平台，安全策略管理平台根据接收到安全客户端传来的报警日志从预先配置好的策略集中选择相应的一条，将此条策略下发到所有的安全设备，安全设备接受最新的策略配置后立即应用配置，使该报警的用户只能根据策略服务器规定的恢复动作访问指定的升级服务器，自动安装这些补丁程序。

当用户已经完成了策略服务器规定的一切恢复动作之后，安全客户端会再次对客户端操作平台进行安全检测，如果此时客户端满足所有的安全策略集，安全客户端会通知安全策略管理平台解除对此客户端的访问列表限制，将客户端设置成正常的用户。

8.1.4 锐捷安全设备

做为锐捷安全解决方案的一部分，锐捷安全设备负责从锐捷安全策略管理平台上接收策略，并且实现策略的安装，并根据安装的策略对用户进行控制。

8.2 GSN 安全设备配置

8.2.1 配置设备支持安全方案的开关

缺省情况下，设备的 GSN 安全方案的开关是关闭的

命令	作用
Ruijie(config)# **[no] security gsn enable**	打开 GSN 全局配置开关

下边是配置打开设备的 GSN 功能：

```
Ruijie# configure terminal
Ruijie(config)# security gsn enable
```

8.2.2 配置同SMP server之间的通讯

设备必须配置 SMP Server 的 IP 地址以及安全认证名才实现同 SMP Server 的通讯。

命令	作用
Ruijie(config)# **[no] security** { **[v1 | v2] community** *community* | **v3 user** *username* }	配置和 smp 服务器通信的安全名.该命令支持 snmp v1、v2、v3.默认使用没有配置通讯 community。**security v1 community 和 security community** 效果一样,都是配置 v1，只是为了方便用户配置.如果选择了 v3,则需要在 snmp-server 命令下配置相应的 v3 用户,相关配置命令请参看《SNMP 配置指南》
Ruijie(config)# **[no] smp-server host** *ip-address*	配置 SMP 服务器地址

在配置 security v3 user 时,需要在 SNMP 部分配置对应的 v3 user。

8.2.3 配置安全事件传输最小时间间隔

为了避免非法用户通过伪造安全事件，频繁地发送安全事件信息对安全设备和 SMP 进行攻击，用户可以通过配置安全事件传输最小时间间隔来限制用户通告安全事件的最小时间间隔。

根据实际情况，用户可以通过以下命令设置安全事件传输最小时间间隔：

命令	作用
Ruijie(config)# **[no] security event interval** *interval*	配置安全事件传输最小时间间隔配置, *interval*：1-65535s 缺省情况下该时间间隔为 5 秒

8.2.4 配置端口支持地址绑定开关

用户可以通过该命令来控制是否在端口产生地址绑定策略，当认证端口连接着多个用户时管理员必须打开该认证端口的地址绑定：

命令	作用
Ruijie(config)**#interface** *interface*	进入接口配置模式
Ruijie(config-if-*type ID*)**# [no] security address-bind enable**	配置端口启用地址绑定策略

只有全局 GSN 支持功能打开并且配置的端口是认证端口时该功能才能起作用。另外需要注意的是当使用该功能时，需要关闭 802.1x 的 IP 授权功能，否则会影响安全策略的实际运行效果。

8.3 GSN 配置显示

8.3.1 显示smp server

您可以通过以下步骤显示 smp sverver 内容

命令	作用
show smp-server	显示 smp server

例如：

```
Ruijie# show smp-server
SMP-Server IP:192.168.217.220
```

8.3.2 显示security event interval

您可以通过以下步骤显示 policy-map 内容

命令	作用
show security event interval	查看安全事件传输最小时间间隔的配置

例如：

```
Ruijie# show security event interval
Event sending interval(Seconds):5
```

8.4 GSN 配置使用相关注意事项

8.4.1 GSN支持的表项数目

由于 GSN 的策略安装实现是通过设置到硬件，由硬件过滤来实现的，所以 GSN 能够实际支持的策略数目由于各产品的芯片不同而不同，另外由于 GSN 使用的硬件表项资源有可能被其他模块所占用，所以当开启相关功能（如端口的防 ARP 欺骗功能等）时也会减少可用的表项数，GSN 支持的表项数也相应减少。为了能够支持更多的动态策略，增强 GSN 的控制能力，所以在开启 GSN 时尽量不要开启其他耗用硬件表项的功能。

8.4.2 与GSN使用冲突的一些功能

由于 GSN 应用的特性，GSN 与下边的一些功能存在着使用上的冲突，需要在应用时加以注意，避免同时打开出现功能异常。

- GSN 不能与 1x 的 ip 授权共用。
- GSN 不能同端口安全共用。
- GSN 不支持在 AP 口上安装策略，而安装了策略的端口不能加入 AP 口，如果把已经安装了 GSN 策略的端口加入 AP 口可能会导致对应的口的应用功能出现错误，如果一个已经安装了策略的端口需要加入 AP 口需要先删除对应端口上已经安装的策略。

8.4.3 GSN使用的其他注意事项

由于 GSN 最终实现是通过硬件过滤来实现用户的配置，所以对于下边的一些配置可能会影响 GSN 的使用：

全局 IP+MAC 绑定：如配置了某个全局 IP+MAC 的绑定后，放过了某个 MAC 的用户，而 GSN 又设置对此 MAC 的用户进行隔离，这时候由于全局 IP+MAC 绑定已经放过用户，从而导致 GSN 的隔离可能失效。

ACL：当 ACL 设置的表项内容与 GSN 下放的策略出现冲突时也会导致 GSN 的功能失效，在 GSN 启用时建议不要启用 ACL。

9 基于端口的流控制

9.1 风暴控制

9.1.1 概述

当 LAN 中存在过量的广播、多播或未知名单播数据流时，就会导致网络变慢和报文传输超时机率大大增加。这种情况我们称之为 LAN 风暴。拓朴协议的执行错误或对网络的错误配置都有可能导致风暴的产生。

我们可以分别针对广播、多播和未知名单播数据流进行风暴控制。当交换机端口接收到的广播、多播或未知名单播数据流的速率超过所设定的带宽时，设备将只允许通过所设定带宽的数据流，超出带宽部分的数据流将被丢弃，直到数据流恢复正常，从而避免过量的泛洪数据流进入 LAN 中形成风暴。

9.1.2 配置风暴控制

在接口配置模式下，请使用如下命令配置风暴控制：

命令	作用
Ruijie(config-if)# **storm-control** {**broadcast** | **multicast** | **unicast**} [{ **level** *percent* | **pps** *packets* | *rate-bps*]	**broadcast** 打开对广播风暴的控制功能。 **multicast** 打开对未知名多播风暴的控制功能 **unicast** 打开对未知名单播风暴的控制功能。 **level** *percent*： 以带宽的百分比进行设置 如 20 表示端口速率限制为 20%带宽。 **pps** *packet*：以报文为单位进行设置 即 packets per second，每秒允许通过的报文数。 *rate-bps*：以 bit 为单位进行设置，即 Kbits per second，每秒允许通过的千比特数。

接口配置模式下通过命令 **no storm-control broadcast** ， **no storm-control multicast** ， **no storm-control unicast** 来关闭接口相应的风暴控制功能。

下面的例子打开 GigabitEthernet 0/1 上的多播风暴控制功能，并且设置允许的速 率为 4M。

```
Ruijie# configure terminal
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# storm-control multicast 4096
Ruijie(config-if)# end
```

- 设备基于 level 的风暴控制，带宽基准值直接采用设置风暴控制的物理口支持的最大带宽值，不采用物理口实际工作时的带宽值进行换算。
- 如果仅使能风暴控制功能，如配置 **storm-control broadcast**，这时风暴控制采用缺省设置，缺省设置值为端口带宽的百分之一。

9.1.3 查看风暴控制使能状态

查看接口的风暴控制使能状态：

命令	作用
show storm-control [*interface-id*]	显示风暴控制信息。

下面的例子为显示接口 Gi0/3 的风暴控制功能的使能状态：

```
Ruijie# show storm-control gigabitEthernet 0/3
Interface  Broadcast Control  Multicast Control  Unicast Control action
GigabitEthernet 0/3 Disabled  Disabled   Disabled    none
```

一次查看所有接口的风暴控制功能的使能状态：

```
Ruijie# show storm-control
Interface  Broadcast Control  Multicast Control  Unicast Control Action
---------  -----------------  -----------------  -------  -------
GigabitEthernet 0/1   Disabled   Disabled   Disabled   none
GigabitEthernet 0/2   Disabled   Disabled   Disabled   none
GigabitEthernet 0/3   Disabled   Disabled   Disabled   none
GigabitEthernet 0/4   Disabled   Disabled   Disabled   none
GigabitEthernet 0/5   Disabled   Disabled   Disabled   none
GigabitEthernet 0/6   Disabled   Disabled   Disabled   none
GigabitEthernet 0/7   Disabled   Disabled   Disabled   none
GigabitEthernet 0/8   Disabled   Disabled   Disabled   none
GigabitEthernet 0/9   Disabled   Disabled   Disabled   none
GigabitEthernet 0/10  Disabled   Disabled   Disabled   none
GigabitEthernet 0/11  Disabled   Disabled   Disabled   none
GigabitEthernet 0/12  Disabled   Disabled   Disabled   none
GigabitEthernet 0/13  Disabled   Disabled   Disabled   none
GigabitEthernet 0/14  Disabled   Disabled   Disabled   none
GigabitEthernet 0/15  Disabled   Disabled   Disabled   none
GigabitEthernet 0/16  Disabled   Disabled   Disabled   none
GigabitEthernet 0/17  Disabled   Disabled   Disabled   none
GigabitEthernet 0/18  Disabled   Disabled   Disabled   none
GigabitEthernet 0/19  Disabled   Disabled   Disabled   none
GigabitEthernet 0/20  Disabled   Disabled   Disabled   none
GigabitEthernet 0/21  Disabled   Disabled   Disabled   none
GigabitEthernet 0/22  Disabled   Disabled   Disabled   none
GigabitEthernet 0/23  Disabled   Disabled   Disabled   none
GigabitEthernet 0/24  Disabled   Disabled   Disabled   none
```

9.2 Protected Port

9.2.1 概述

有些应用环境下，要求交换机上的部分端口间不能互相通讯，可以通过将某些端口设置为保护口(Protected Port)来达到目的。

当端口设为保护口之后，保护口之间互相无法通讯，保护口与非保护口之间可以正常通讯。

保护口有两种模式，一种是阻断保护口之间的二层交换，但允许保护口之间进行路由，第二种是同时阻断保护口之间的二层交换和阻断路由；在两种模式都支持的情况下，第一种模式将作为缺省配置模式。

当两个保护口设为一个 SPAN 端口对时，SPAN 的源端口发送或接收的帧依然能够 静像到 SPAN 目的端口.

设备支持将 Aggregated Port 设置为保护口，当一个 Aggregated Port 被设置为保护口时，Aggregated Port 的所有成员口都被设置为保护口。

9.2.2 配置Protected Port

设置接口为保护口：

命令	作用
Ruijie(config-if)# **switchport protected**	将该接口设置为保护口

通过命令 **no switchport protected** 接口配置命令将一个端口重新设置为非保护口。

下面的例子说明了如何把 Gigabitethernet 0/3 设置为保护口

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitethernet 0/3
Ruijie(config-if)# switchport protected
Ruijie(config-if)# end
```

9.2.3 配置保护口之间三层路由阻断

命令	作用
Ruijie(config)# **protected-ports route-deny**	设置保护口之间不能进行路由

通过命令 **no protected-ports route-deny** 接口配置命令重新打开保护口之间的 3 层路由

下面的例子说明了如何关闭保护口之间的 3 层路由

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# protected-ports route-deny
Ruijie(config)# end
```

9.2.4 显示Protected Port配置

命令	作用
Ruijie(config-if)# **show interfaces Switchport**	显示交换口配置

通过命令 **show interfaces switchport** 来查看保护口设置

```
Ruijie# show interfaces gigabitethernet 0/3 switchport
Interface   Switchport  Mode   Access Native Protected   VLAN lists
---------   ----------  ----   ------  -----  --------   ----
GigabitEthernet 0/3  enabled   Trunk  1    1    Enabled    ALL
```

9.3 端口安全

9.3.1 概述

端口安全功能通过报文的源 MAC 地址来限定报文是否可以进入交换机的端口，你可以静态设置特定的 MAC 地址或者动态学习限定个数的 MAC 地址来控制报文是否可以进入端口，使能端口安全功能的端口称为安全端口。只有源 MAC 地址为端口安全地址表中配置或者学习到的 MAC 地址的报文才可以进入交换机通信，其他报文将被丢弃。您还可以设定端口安全地址绑定 IP+MAC，或者仅绑定 IP，用来限制必须符合绑定的以端口安全地址为源 MAC 地址的报文才能进入交换机通信；符合 IP+MAC 或者 IP 绑定的安全地址的 IP 报文和 ARP 报文可以进入交换机，不符合绑定的 IP 和 ARP 报文将被丢弃。

端口安全还支持 Sticky MAC 地址功能，通过使能该功能，可以将动态学习到的安全地址转换为静态配置的，在 show running-config 中可以看到配置，保存配置后，重启不用重新学习这些动态安全地址，而如果没有启用该功能，那么动态学习到的安全 MAC 地址在交换机重启后要重新学习。

您可以为每个安全端口配置最大可允许的安全地址数，最大安全地址数指的是静态配置与动态学习的安全地址总数，当安全端口下安全地址没有达到最大安全地址数时，安全端口能够动态学习新的动态安全地址，当安全地址数达到最大数时，安全端口将不再学习动态安全地址，如果此时有新的用户接入安全端口，将产生安全违例事件。您可以按照如下 3 种方式处理安全违例事件：

- **protect**：当安全地址个数满后，安全端口将丢弃所有新接入的用户数据流。该处理模式为默认的对违例的处理模式。
- **restrict**：当违例产生时，将发送一个 Trap 通知。
- **shutdown**：当违例产生时，将关闭端口并发送一个 Trap 通知。

端口安全的安全地址支持老化配置，您可以指定只老化动态学习的地址或同时老化静态配置与动态学习的安全地址。

9.3.2 缺省配置

下表显示的端口安全的缺省配置：

功能特性	缺省值
端口安全开关	所有端口均关闭端口安全功能
最大安全地址个数	128

安全地址	无
违例处理方式	保护(protect)
安全地址绑定方式	无
Sticky MAC 地址学习	关闭

9.3.3 配置指导

配置端口安全时有如下一些限制：

- 一个安全端口不能是 SPAN 的目的端口；
- 当安全地址绑定 IP+MAC，同时设定静态安全 MAC 地址时，设定的静态安全 MAC 地址必须和 IP+MAC 绑定的 MAC 地址相同，否则将因为不符合绑定而无法通信；同理，设定仅 IP 绑定之后，只有符合静态设置或者学习的安全 MAC 地址，同时源 IP 为绑定 IP 的报文才可以进入交换机；
- 端口安全和其他接入控制功能如 802.1x，IP+MAC 绑定，IP SOURCE GUARD 共用，当这些功能共用时，报文必须同时满足所有的安全检查才能进入交换机；如果端口设置了安全通道，那么符合安全通道的报文将绕过端口安全的检查。

9.3.4 配置安全端口及违例处理方式

在接口配置模式下，请使用如下命令配置安全端口及违例处理方式：

命令	作用
Ruijie(config-if)# **switchport port-security**	打开该接口的端口安全功能
Ruijie(config-if)# **switchport port-security maximum** *value*	设置接口上安全地址的最大个数，缺省值为 128。
Ruijie(config-if)# **switchport port-security violation {protect | restrict | shutdown}**	设置处理违例的方式： protect：保护端口，当安全地址个数满后，安全端口将丢弃未知名地址(不是该端口的安全地址中的任何一个)的包； **restrict**：当违例产生时，将发送一个 Trap 通知； **shutdown**：当违例产生时，将关闭端口并发送一个 Trap 通知。当端口因为违例而被关闭后，在全局配置模式下使用命令 errdisable recovery 来将接口从错误状态中恢复过来。
Ruijie(config-if)# **switchport port-security mac-address sticky**	启用 Sticky MAC 地址学习功能
Ruijie(config)# **errdisable recovery** [**interval** *time*]	当端口因为违例而被关闭后，在全局配置模式下使用该命令来将接口从错误状态中恢复过来。 **Interval**：命令生效的间隔时间，单位为秒，范围是 30-86400。

在接口配置模式下，使用命令 **no switchport port-security** 来关闭一个接口的端口安全功能。使用命令 **no switchport port-security** *maximum* 来恢复为缺省个数。使用命令 **no switchport port-security violation** 来将违例处理置为缺省模式。使用命令 **no switchport port-security mac-address sticky** 来将 Sticky MAC 学习功能设置为缺省模式。

下面的例子说明了如何使能接口 gigabitethernet 0/3 上的端口安全功能，设置最大地址个数为 8，设置违例方式为 protect

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitethernet 0/3
Ruijie(config-if)# switchport mode access
Ruijie(config-if)# switchport port-security
Ruijie(config-if)# switchport port-security maximum 8
Ruijie(config-if)# switchport port-security violation protect
Ruijie(config-if)# switchport port-security mac-address sticky
Ruijie(config-if)# end
```

下面的例子说明了如何将违例端口从错误状态中恢复过来：

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# errdisable recovery
Ruijie(config)# end
```

- 如果端口 DOT1X 开启并且已认证的用户数大于端口安全的最大用户数，此时开启端口安全将会提示失败；
- 端口安全和 DOT1X 同时开启时，如果安全地址老化，则 DOT1X 对应的用户必须重新认证才可以继续通信；
- 静态端口安全地址不需要认证即可上网，如果存在授权，则必须同时符合授权绑定才可以上网；
- 如果在违例后修改端口的违例模式，新的违例模式必须在安全端口恢复成非违例状态后，再次违例，才会生效。

9.3.5 配置安全端口上的安全地址

全局配置模式下，请使用如下命令为安全端口添加安全地址：

命令	作用
Ruijie(config)# **switch portport-security interface** *interface-id* **mac-address** *mac-address* **vlan** [*vlan_id*]	全局模式下，手工配置接口上的安全地址。

接口配置模式下，请使用如下命令为安全端口添加安全地址：

命令	作用
Ruijie(config-if)# **switchportport-security** [**mac-address** *mac-address*] **vlan** [*vlan_id*]	接口模式下，手工配置接口上的安全地址。
Ruijie(config-if)# **switchportport-security** [**mac-address sticky** *mac-address*] **vlan** [*vlan_id*]	接口模式下，手工配置接口上的 Sticky 安全地址

在接口配置模式下，使用命令 **no switchport port-security mac-address** *mac-address* 来删除该接口的安全地址，使用命令 **no switchport port-security sticky mac-address** *mac-address* 来删除该接口的 Sticky 安全地址。

下面的例子说明了如何为接口 gigabitethernet 0/3 配置一个源 MAC 地址模式的安全地址：00d0.f800.073c。

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

```
Ruijie(config)# interface gigabitethernet 0/3
Ruijie(config-if)# switchport mode access
Ruijie(config-if)# switchport port-security
Ruijie(config-if)# switchport port-security mac-address 00d0.f800.073c  vlan 1
Ruijie(config-if)# end
```

下面的例子说明了如何为使能了 Sticky MAC 学习功能的接口 gigabitethernet 0/3 配置一个源 MAC 地址模式的安全地址：00d0.f800.073c。

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitethernet 0/3
Ruijie(config-if)# switchport mode access
Ruijie(config-if)# switchport port-security
Ruijie(config-if)# switchport port-security mac-address sticky
Ruijie(config-if)# switchport port-security mac-address sticky 00d0.f800.073c  vlan 1
Ruijie(config-if)# end
```

9.3.6 配置安全端口上的安全地址绑定

全局配置模式下，请使用如下命令为安全端口添加安全地址绑定：

命令	作用
Ruijie(config)# **switchport port-security interface** *interface-id* **binding** [*mac-address* **vlan** *vlan_id*] [*ipv4-address*]| [*ipv6-address*]	全局模式下，手工配置接口上的安全地址绑定

接口配置模式下，请使用如下命令为安全端口添加安全地址绑定：

命令	作用
Ruijie(config-if)# **switchport port-security binding** [*mac-address* **vlan** *vlan_id*] [*ipv4-address*]|[*ipv6-address*]	接口模式下，手工配置接口上的安全地址绑定

下面的例子说明了如何为接口 gigabitethernet 0/3 配置一个源 IP 地址模式的安全地址：192.168.12.202

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitethernet 0/3
Ruijie(config-if)# switchport mode access
Ruijie(config-if)# switchport port-security
Ruijie(config-if)# switchport port-security binding 192.168.12.202
Ruijie(config-if)# end
```

下面的例子说明了如何为接口 gigabitethernet 0/3 配置一个源 IP 与源 MAC 组合模式的安全地址：源 IP 为 192.168.12.202，源 MAC 为 00d0.f800.073c

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitethernet 0/3
```

```
Ruijie(config-if)# switchport mode access
Ruijie(config-if)# switchport port-security
Ruijie(config-if)# switchport port-security binding 00d0.f800.073c vlan 1 192.168.12.202
Ruijie(config-if)# end
```

符合端口安全 IP+MAC，或者仅 IP 绑定的报文，其源 MAC 地址必须同时是端口安全地址才可以被转发；对于动态安全地址来说，在安全地址添加到安全地址表之前，符合安全地址绑定或者仅 IP 绑定的任何报文不能被转发。

9.3.7 配置安全地址的老化时间

为一个接口上的所有安全地址配置老化时间。打开这个功能，需要设置安全地址的最大个数，这样就可以让设备自动的增加和删除接口上的安全地址。

在接口配置模式下，请使用如下命令配置安全地址老化时间：

命令	作用
Ruijie(config-if)# **switchport port-security aging** {**static** | **time** *time* }	static：加上这个关键字，表示老化时间将同时应用于手工配置的安全地址和自动学习的地址，否则只应用于自动学习的地址。 time ：表示这个端口上安全地址的老化时间，范围是 0—1440，单位是分钟。如果设置为 0，则老化功能实际上被关闭。老化时间按照绝对的方式计时，也就是一个地址成为一个端口的安全地址后，经过 Time 指定的时间后，这个地址就将被自动删除。*Time* 的缺省值为 0。

可以在接口配置模式下使用命令 **no switchport port-security aging time** 来关闭一个接口的安全地址老化功能，使用命令 **no switchport port-security aging static** 来使老化时间仅应用于动态学习到的安全地址。

下面的例子说明了如何配置一个接口 gigabitethernet 0/3 上的端口安全的老化时间，老化时间设置为 8 分钟，老化时间同时应用于静态配置的安全地址：

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitthernet 0/3
Ruijie(config-if)# switchport port-security aging time 8
Ruijie(config-if)# switchport port-security aging static
Ruijie(config-if)# end
```

Sticky MAC 地址是一种特殊的 MAC 地址，不受老化机制影响，无论是配置了动态的老化还是静态的老化，Sticky MAC 地址均不会老化。

◆ 端口安全IP+MAC唯一性检查

在全局模式下开启端口安全 IP+MAC 唯一性检查：

命令	作用
switchport port-security ipmac-only	开启端口安全 IP+MAC 唯一性检查

开启此模式后设置同一个 IP 但 MAC 地址不同，或者同一个 MAC 地址 IP 不同的 MAC 的时候会提示冲突。

下面这个例子在开启端口安全 IP+MAC 唯一性检查并在 gigabitethernet 0/1 上配置了 switchport port-security binding 0001.0001.0001 vlan 1 1.1.1.1 后，若在配置一个 MAC 地址同为 0001.0001.0001 但 IP 不通为 1 1.1.1.2 时提示配置冲突且配置失败。

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#switchport port-security ipmac-only
ruijie(config)#interface gigabitEthernet 0/1
ruijie(config-if-GigabitEthernet 0/1)#switchport port-security binding 0001.0001.0001 vlan 1 1.1.1.1
ruijie(config-if-GigabitEthernet 0/1)#switchport port-security binding 0001.0001.0001 vlan 1 1.1.1.2
Secure Address < mac:0001.0001.0001 vid:1  ip:1.1.1.2 > of interface Gi0/1 is removed. Because it's in conflict
with Secure Address < mac:0001.0001.0001 vid:1  ip:1.1.1.1 > on interface Gi0/1.
ruijie(config-if-GigabitEthernet 0/1)#show this

Building configuration...
 !
 switchport port-security binding 0001.0001.0001 vlan 1 1.1.1.1
 switchport port-security
 ip access-group 100 in
 !
end
ruijie(config-if-GigabitEthernet 0/1)#
```

9.3.8 查看端口安全信息

在特权模式下，通过如下命令来查看端口安全的信息：

命令	作用
show port-security interface [*interface-id*]	查看接口的端口安全配置信息
show port-security address	查看安全地址信息
show port-security binding	查看安全地址绑定信息
show port-security address [*interface-id*]	显示某个接口上的安全地址信息
show port-security	显示所有安全端口的统计信息，包括最大安全地址数，当前安全地址数以及违例处理方式等

下面的例子显示了接口 Gigabitethernet 0/3 上的端口安全配置：

```
Ruijie# show port-security interface gigabitethernet 0/3
Interface : Gi0/3
Port Security: Enabled
Port status : down
Violation mode:Shutdown
Maximum MAC Addresses:8
```

```
Total MAC Addresses:0
Configured MAC Addresses:0
Aging time : 8 mins
SecureStatic address aging : Enabled
```

下面的例子显示了系统中的所有安全地址

```
Ruijie# show port-security address
Vlan  Mac Address      IP Address        Type          Port        Remaining Age(mins)
----  ---------------  ----------------  --------      ---------   -----------------
1     00d0.f800.073c   192.168.12.202    Configured    Gi0/3       8
1     00d0.f800.3cc9   192.168.12.5      Configured    Gi0/1       7
```

可以只显示一个接口上的安全地址，下面的例子显示了接口 gigabitstethernet 0/3 上的安全地址

```
Ruijie# show port-security address interface gigabitethernet 0/3
Vlan  Mac Address     IP Address       Type         Port    Remaining Age(mins)
----  --------------  ---------------  -----------  ------  -----------------
1     00d0.f800.073c  192.168.12.202   Configured   Gi0/3   8
```

下面的例子显示的是安全端口的统计信息

```
Ruijie# show port-security
Secure Port  MaxSecureAddr  CurrentAddr  MaxIPSecureAddr  CurrentIPAddr  Security Action
                   (Count)      (Count)          (Count)        (Count)
-----------  -------------  -----------  ---------------  -------------  ---------------
Gi 0/1       128            1            128              1              Restrict
-----------  -------------  -----------  ---------------  -------------  ---------------
Total Secure Addresses in System : 1
Max Secure Addresses limit in System : 1024
```

端口安全与 Private Vlan 功能共用时，由于端口安全地址会分布在主 Vlan 和从 Vlan 上，所以实际会占用 2 个安全地址容量，即一个用户将占用 2 个安全地址。可以通过 **show port-security-address** 命令查看。

9.4 ARP-Check 功能

9.4.1 概述

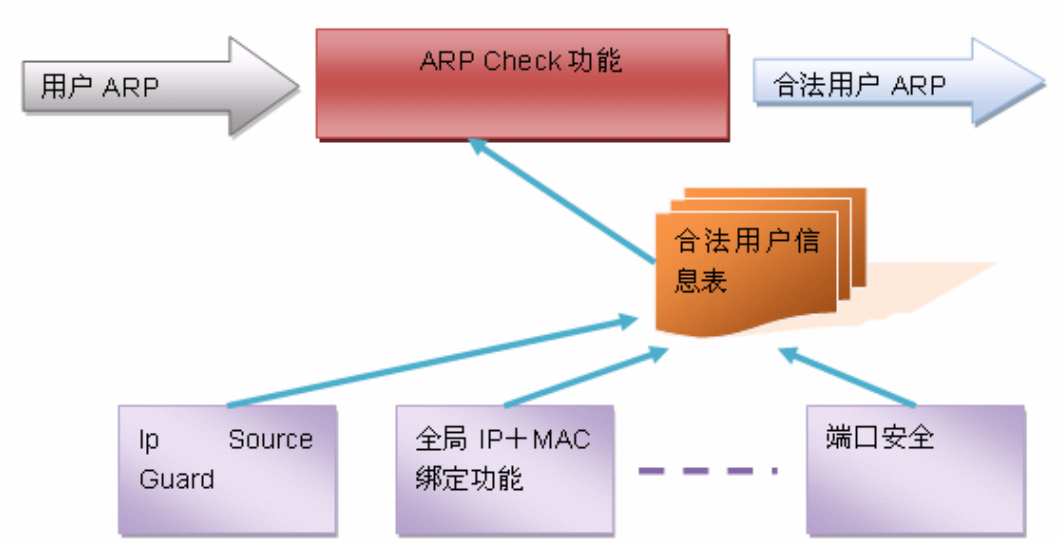
ARP 报文检查（ARP-Check）功能，对逻辑端口下的所有的 ARP 报文进行过滤，对所有非法的 ARP 报文进行丢弃，能够有效的防止网络中 ARP 欺骗，提高网络的稳定性。

9.4.2 功能简述

锐捷交换机支持多种 IP 安全应用（例如 Ip Source Guard、全局 IP+MAC 绑定、端口安全等等）这些安全应用通过对用户 IP 报文进行有效的数据过滤，从而避免网络中的非法用户使用网络资源。在支持 ARP Check 功能的交换机中，ARP Check

功能能够根据这些应用模块所合法用户信息(IP 或 IP+MAC)产生相应的 ARP 过滤信息，从而实现对网络中的非法 ARP 报文的过滤。

图 9-1 Arp Check 功能与其它安全功能



如上图所示，交换机各安全功能模块产生的合法用户信息(仅有 IP 或 IP＋MAC)，ARP Check 功能使用这些信息用于检测逻辑端口下的所有的 ARP 报文中的 Sender IP 字段或<Sender IP, Sender MAC>是否满足合法用户信息表中的匹配关系，所有不在合法用户信息表中的 ARP 报文将被丢弃，目前 ARP Check 支持的安全功能模块包括：

1) 仅检测 IP 字段：端口安全的仅 IP 模式，Ip Source Guard 手工配置的仅 IP 模式。

2) 检测 IP+MAC 字段：端口安全的 IP＋MAC 绑定模式，全局 IP＋MAC 绑定功能，802.1x IP 授权功能，Ip Source Guard 功能，GSN 绑定功能。

ARP-Check 有 2 种模式：打开和关闭，默认为关闭。

■ 打开模式

ARP Check 功能根据交换机当前各安全功能运行的状态来打开、关闭 ARP 报文的检测功能。

如下功能打开(关闭)可能触发 ARP Check 打开(关闭)检测：

1) 全局 IP＋MAC 绑定

2) 802.1X 的 IP 授权

3) Ip Source Guard

4) GSN 绑定

如下功能第一次添加(删除最后一个)合法用户后将触发 ARP Check 打开(关闭)检测：

1) 端口安全 IP+MAC

2) 端口安全仅 IP

无论端口上有没有安全配置都检查 ARP 报文。如果端口上没有合法用户，则来自这个端口的所有 arp 报文都将被丢弃。

■ 关闭模式

不检查端口上的 ARP 报文。

打开 ARP Check 检测功能，可能会使相关安全应用的策略数/用户数减少。

转发面检查 ARP 报文以太网首部的源 MAC 地址和 Sender Ip 字段，控制面检查 ARP 协议内部的 Sender Mac 和 Sender Ip 字段。

9.4.3 配置ARP-Check

从特权模式下开始配置 ARP-Check 功能

命令	作用
Ruijie(config)#**interface** *interface-id*	进入接口模式
Ruijie(config-if)# **arp-check**	设置 ARP-Check 为打开模式
Ruijie(config-if)# **no arp-check**	设置 ARP-Check 为关闭模式

9.4.4 查看接口下实际生效的ARP Check表项

ARP-Check 功能支持查询实际端口的 ARP-Check 所产生的 ARP-Check 的表项信息：

命令	作用
show interface { *interface-type interface-number* } **arp-check list**	查看 ARP-Check 所产生成的表项

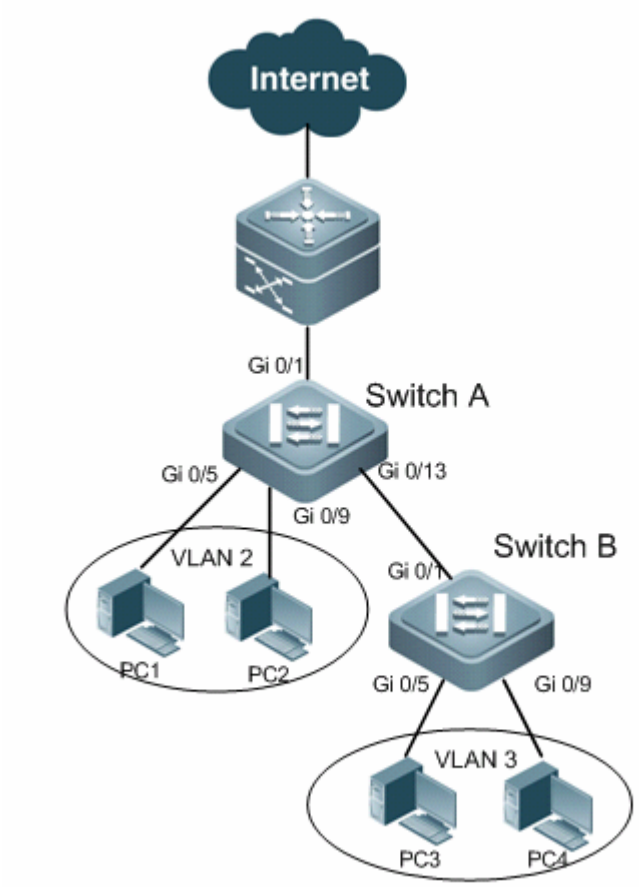
例如，查看 ARP-Check 产生表项信息如下：

```
Ruijie#show interfaces arp-check list
   Interface              Sender MAC        Sender IP       Policy Source
------------------------ ----------------- ----------------- --------------------
   Gi 0/1                 00D0.F800.0003    192.168.1.3       address-bind
   Gi 0/1                 00D0.F800.0001    192.168.1.1       port-security
   Gi 0/4                                   192.168.1.3       port-security
   Gi 0/5                 00D0.F800.0003    192.168.1.3       address-bind
   Gi 0/7                 00D0.F800.0006    192.168.1.6       AAA ip-auth-mode
   Gi 0/8                 00D0.F800.0007    192.168.1.7       GSN
```

9.5 基于端口的流控制组合配置用例

拓扑图

图 9-2



应用需求

上图是典型企业网络的简化拓扑，组网需求如下：

1) 防止设备受到广播、多播、未知名单播报文攻击。

2) 只允许直连用户（本例指 Switch A 的直连用户）以指定的 IP/MAC 地址上网，源地址与指定 IP/MAC 不匹配的报文将被丢弃，防止源 IP,/源 MAC 欺骗。

3) 不允许接入用户（本例为 Switch B 的接入用户）之间进行二层报文通信，避免接入用户之间互相干扰（如 ARP 欺骗或 DOS 攻击等）

配置要点

1) 在所有接入设备（本例为 Switch A、Switch B）的端口上开启风暴控制。

2) 在接入设备（本例为 Switch A）的端口（本例为 Gi 0/5 和 Gi 0/9）上配置端口安全功能可满足第二个需求。

3) 在接入设备（本例为 Switch B）上配置端口保护功能，可满足第三个需求。

开启端口安全功能并配置 IP/MAC 表项后，ARP CHECK 功能将自动生效，根据设置的 IP/MAC 对 ARP 报文的源地址进行检查。

配置步骤

■ 配置 Switch A

第一步，创建交换机的 VLAN，并设置端口属性。

！创建 VLAN 2

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#vlan 2
Ruijie(config-vlan)#exit
```

！设置端口属性

```
Ruijie(config)#interface gigabitEthernet 0/5
Ruijie(config-if-GigabitEthernet 0/5)#switchport access vlan 2
Ruijie(config-if-GigabitEthernet 0/5)#exit
Ruijie(config)#interface gigabitEthernet 0/9
Ruijie(config-if-GigabitEthernet 0/9)#switchport access vlan 2
Ruijie(config-if-GigabitEthernet 0/9)#exit
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#switchport mode trunk
Ruijie(config-if-GigabitEthernet 0/1)#exit
Ruijie(config)#interface gigabitEthernet 0/13
Ruijie(config-if-GigabitEthernet 0/13)#switchport mode trunk
Ruijie(config-if-GigabitEthernet 0/13)#exit
```

第二步，在所有接入端口上开启风暴控制。

```
Ruijie(config)#interface range gigabitEthernet 0/1,0/5,0/9,0/13
Ruijie(config-if-range)#storm-control broadcast
Ruijie(config-if-range)#storm-control multicast
Ruijie(config-if-range)#storm-control unicast
Ruijie(config-if-range)#exit
```

第三步，在直连用例的端口上开启端口安全，并绑定 IP 和 MAC

！绑定接入用户：IP（1.1.1.1）/MAC（0000.0000.0001）

```
Ruijie(config)#interface gigabitEthernet 0/5
Ruijie(config-if-GigabitEthernet 0/5)#switchport port-security
Ruijie(config-if-GigabitEthernet 0/5)#switchport port-security mac-address 0000.0000.0001 ip-address 1.1.1.1
Ruijie(config-if-GigabitEthernet 0/5)#exit
```

！绑定接入用户：IP（1.1.1.2）/MAC（0000.0000.0002）

```
Ruijie(config)#interface gigabitEthernet 0/9
Ruijie(config-if-GigabitEthernet 0/9)#switchport port-security
Ruijie(config-if-GigabitEthernet 0/9)#switchport port-security mac-address 0000.0000.0002 ip-address 1.1.1.2
Ruijie(config-if-GigabitEthernet 0/9)#exit
```

■ 配置 Switch B

第一步，创建交换机的 VLAN，并设置端口属性

！创建 VLAN 3

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#vlan 3
Ruijie(config-vlan)#exit
Ruijie(config)#interface gigabitEthernet 0/5
Ruijie(config-if-GigabitEthernet 0/5)#switchport access vlan 3
Ruijie(config-if-GigabitEthernet 0/5)#exit
Ruijie(config)#interface gigabitEthernet 0/9
Ruijie(config-if-GigabitEthernet 0/9)#switchport access vlan 3
Ruijie(config-if-GigabitEthernet 0/9)#exit
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#switchport mode trunk
Ruijie(config-if-GigabitEthernet 0/1)#exit
```

第二步，在所有接入端口上开启风暴控制

```
Ruijie(config)#interface range gigabitEthernet 0/1,0/5,0/9
Ruijie(config-if-range)#storm-control broadcast
Ruijie(config-if-range)#storm-control multicast
Ruijie(config-if-range)#storm-control unicast
Ruijie(config-if-range)#exit
```

第三步，在接入端口上开启端口保护功能。

```
Ruijie(config)#interface gigabitEthernet 0/5
Ruijie(config-if-GigabitEthernet 0/5)#switchport protected
Ruijie(config-if-GigabitEthernet 0/5)#exit
Ruijie(config)#interface gigabitEthernet 0/9
Ruijie(config-if-GigabitEthernet 0/9)#switchport protected
Ruijie(config-if-GigabitEthernet 0/9)#exit
```

配置验证

第一步，查看 Switch A 的配置情况，关注点：是否在各端口上开启风暴控制、是否在直连用户的端口上配置端口安全功能并静态绑定 IP+MAC 地址。

```
Ruijie#show running-config
vlan 2
!
interface GigabitEthernet 0/1
 switchport mode trunk
 storm-control broadcast
 storm-control multicast
 storm-control unicast
```

```
!
interface GigabitEthernet 0/5
 switchport access vlan 2
 switchport port-security mac-address 0000.0000.0001 ip-address 1.1.1.1
 switchport port-security
 storm-control broadcast
 storm-control multicast
 storm-control unicast
!
interface GigabitEthernet 0/9
 switchport access vlan 2
 switchport port-security mac-address 0000.0000.0002 ip-address 1.1.1.2
 switchport port-security
 storm-control broadcast
 storm-control multicast
 storm-control unicast
!
interface GigabitEthernet 0/13
 switchport mode trunk
 storm-control broadcast
 storm-control multicast
 storm-control unicast
```

第二步，查看 Switch B 的配置情况，关注点：是否在各端口开启风暴控制、是否在直连用户的端口上开启端口保护功能。

```
Ruijie#show running-config
vlan 3
!
interface GigabitEthernet 0/1
 switchport mode trunk
 storm-control broadcast
 storm-control multicast
 storm-control unicast
!
interface GigabitEthernet 0/5
 switchport access vlan 3
 switchport protected
 storm-control broadcast
 storm-control multicast
 storm-control unicast
!
interface GigabitEthernet 0/9
 switchport access vlan 3
 switchport protected
 storm-control broadcast
 storm-control multicast
```

```
storm-control unicast
```

第三步，在 Switch A 查看端口安全地址绑定信息，以及 ARP CHECK 使能情况。

```
Ruijie#show port-security all
Vlan Port    Arp-Check     Mac Address     IP Address  Type          remaining Age (mins)
---- ------  ------------ ---------------  ----------  ------------  ---------------
2    Gi0/5   Enabled      0000.0000.0001   1.1.1.1     Configured       -
2    Gi0/9   Enabled      0000.0000.0002   1.1.1.2     Configured       -
```

第四步，在 Switch B 查看端口 GigabitEthernet 0/5 的端口保护配置信息，其它端口的端口保护配置信息不再举例说明。

```
Ruijie#show interfaces gigabitEthernet 0/5 switchport
Interface            Switchport  Mode       Access   Native  Protected   VLAN lists
-------------------  ----------  ---------  -------  ------  ----------  ----------
GigabitEthernet0/5   enabled     ACCESS     3        1       Enabled      ALL
```

9.6 端口 IP 地址接入数量限定

9.6.1 概述

锐捷交换机支持多种接入控制应用（例如：Ip Source Guard、端口安全、全局 IP+MAC 绑定等等），这些安全接入应用通过用户源 IP 地址信息进行接入控制，对用户 IP 报文进行有效的数据过滤，从而避免网络中的非法用户使用网络资源。

端口 IP 地址接入数量限定功能用于限定这些安全接入应用在端口上绑定的接入 IP 地址个数，用于限定共享交换机端口带宽的用户数量。

可以为每个端口配置可允许接入网络的 IP 地址数量，当端口下各个接入应用绑定的 IP 地址没有达到限定数量时，各个接入应用能够继续进行合法用户绑定和添加；当端口下 IP 地址数达到限定数量时，各个接入应用将不能再进行合法用户绑定。

当端口下的接入 IP 地址个数超出限定数量时，超出的 IP 地址不允许进行通行。

- 端口 IP 接入数限定需要在接入控制应用的 IP+MAC 绑定或仅 IP 绑定生效情况下才有效，当端口下没有配置任何接入应用（或为全局 IP+MAC 绑定的例外口）时，限定的 IP 地址数不生效；
- IP+MAC 绑定和仅 IP 绑定同时绑定了同一个 IP 地址时，将被统计为 2 个用户 IP；
- 端口 IP 地址接入数量限定仅对 IPV4 报文生效；
- 除全局 IP+MAC 绑定的例外口外，全局 IP+MAC 绑定添加的用户将被统计到各个端口限定的 IP 地址数中；

9.6.2 端口IP地址接入数量限定的缺省配置

下表显示端口 IP 地址接入数量限定的缺省配置：

功能特性	缺省值
端口 IP 地址接入数量限定开关	所有端口均关闭 IP 地址接入数量限定功能，缺省值为 0

9.6.3 配置端口IP地址接入数量限定

从特权模式下开始配置端口 IP 地址接入数量限定：

命令	作用
Ruijie(config)#**interface** *interface-id*	进入接口模式
Ruijie(config-if)#**nac-author-user maximum** *value*	限定端口 IP 地址接入数量
Ruijie(config-if)#**no nac-author-user maximum**	关闭端口 IP 地址接入数量限定

9.6.4 查看端口IP地址接入数量

端口 IP 地址接入数量限定功能支持查询实际端口配置限定的接入 IP 地址数，以及已绑定的 IP 地址个数：

命令	作用
show nac-author-user	查看端口限定的 IP 地址接入数量配置及已绑定的 IP 地址个数

如下：

```
Ruijie#show nac-author-user
 Port      Cur_num  Max_num
 --------  -------  -------
 Fa0/1     2         50
 Fa0/2     0         0
 Fa0/3     2         100
 Fa0/4     0         0
 Fa0/5     0         200
 Fa0/6     0         0
 Fa0/7     0         0
 Fa0/8     0         0
```

10 CPU 保护

10.1 概述

在网络环境中，有各种攻击报文在网络上传播，其会导致交换机的 CPU 利用率过高，影响协议运行，甚至无法正常管理交换机。针对这种情况，必须对交换机的 CPU 进行保护，即对送往交换机的 CPU 处理的各种报文进行流量控制和优先级处理，保护其正常处理能力。

CPU Protect 的实现模型分为 Classifying、Queuing、Scheduling 和 Shaping 四个阶段，下面对这四个阶段进行详细的说明。

- Classifying：

Classifying 对每个需要送到 CPU 的报文进行分类，分类是根据报文的 L2、L3 以及 L4 信息。具体如下表所示：

报文类型	分类标准
bpdu	目的 MAC 地址为 01-80-C2-00-00-00 的报文
arp-request	arp request 报文
arp-reply	arp replayt 报文
tpp	目的 MAC 地址为 01-d0-f8-00-00-04，以太网类型为 0xBEEF 的报文
802.1x	目的 MAC 地址为 01-80-C2-00-00-03 的报文
gvrp	目的 MAC 地址为 01-80-C2-00-00-21 的报文
rldp	目的 MAC 地址为 01-d0-f8-00-00-02，以太网类型为 0x788 的报文
lacp	目的 MAC 地址为 01-80-C2-00-00-02 的报文
rerp	以太网类型为 0x789 的报文
reup	目的 MAC 地址为 01-D0-F8-00-00-07，以太网类型为 0x790
lldp	目的 MAC 地址为 01-80-C2-00-00-0E 的报文
dhcp	dhcp 协议报文,包括 IPv4 和 IPv6 dhcp
qinq	qinq 协议报文
unknown_v6mc	地址表或路由表中不能查找到的 IPv6 多播报文
known_v6mc	地址表或路由表中查找到的 IPv6 多播报文
unknown_v4mc	地址表或路由表中不能查找到的 IPv4 播报文
known_v4mc	地址表或路由表中查找到的 IPv4 播报文
udp-helper	指定端口号的 UDP 广播报文
dvmrp	目的 IP 地址为 224.0.0.4，协议号为 2 的报文
igmp	IPv4 igmp V1/V2/V3 报文
icmp	IPv4 icmp 协议报文
ospf	ospf 协议报文,包括 ospf 和 ospfV3 报文
pim	pim 协议报文,包括 pim 和 pimv6 报文
rip	rip 协议报文,包括 rip 和 ripng 报文
vrrp	vrrp 协议报文,包括 vrrp 和 vrrpv6 报文
error_ttl	IPv4 TTL = 0 或 1 的报文
error_hop_limit	IPv6 Hop Limit = 0 或 1 的报文

local-telnet	telnet 本地管理报文
local-snmp	SNMP 本地管理报文
local-http	HTTP 本地管理报文
local-tftp	Tftp 本地管理报文
local-other	其他本地管理报文
v4uc-route	IPv4 单播报文
v6uc-route	IPv6 单播报文
rt-host	rt-host 报文，组播地址为 224.0.0.1、224.0.0.2 和 FF02::1、FF02::2 的报文
mld	mld 报文
nd	nd 协议报文
erps	erps 协议报文，报文目的 MAC 地址为 01-19-A7-00-00-01
mpls-data	mpls 数据报文
mpls-lspv	mpls lspv 协议报文
isis	isis 协议报文，报文目的 MAC 地址为 ISIS 组播地址
bgp	bgp 协议报文，报文流 4 层端口号为 179
cfm	cfm 协议报文，报文目的 MAC 地址为 01-80-C2-00-00-3x(x 为 0 到 F)，以太网类型为 0x8902
web-auth	web 认证报文
ipfix	ipfix 报文
other	非上述分类的需要送到 CPU 的报文

☑ 二层交换机不支持三层报文，三层报文包括三层协议报文（如 pim，ospf，rip，isis 等）和 udp-helper、error-ttl、error-hop-limit、v4uc-route、v6uc-route 报文。

- Queuing：

Queuing 动作负责将各种不同类型的报文送到指定的队列，在不同队列的报文具有不同的传输优先级。

CPU 端口共有 8 个优先级队列，您可以配置每种类型的报文对应的队列，Queuing 根据您的配置自动地将这种类型的报文的送到指定队列。

- Scheduling：

当多个队列有报文需要传输时，Scheduling 负责从中选择一个队列并传输这个队列的报文。

CPU 端口 Scheduling 采用严格优先级(SP)算法，队列 7 具有最高优先级，队列 6 次之，以此类推，队列 0 具有最低优先级，高优先级队列报文总是先于低优先级队列的报文被传输。这样您可以根据每种报文的重要性将它们对应到不同的优先级的队列，确保重要的报文总是优先被传输。

- Shaping：

Shaping 控制每个传输队列的最大速率，超过最大速率的报文将被丢弃。您可以根据网络实际情况配置每个队列的最大速率，同时，您还可以配置整个 CPU 端口的最大速率。

10.2 配置 CPU Protect

10.2.1 CPU Protect默认配置

由于不同类型的交换机应用在不同的网络环境中，具有不同的网络攻击，CPU 保护也应该采用不同策略对应这些工具。所以对不同的交换机产品，我们精心地给您准备了不同的 CPU 的保护缺省配置。本产品的缺省配置如下：

报文类型和队列的对应关系：

报文类型	队列
bpdu	6
arp-request	2
arp-reply	2
tpp	6
802.1x	1
gvrp	5
rldp	5
lacp	5
rerp	5
reup	5
lldp	5
dhcp	1
qinq	1
unknown_v6mc	0
known_v6mc	0
unknown_v4mc	0
known_v4mc	0
udp-helper	4
dvmrp	4
igmp	1
icmp	3
ospf	4
pim	4
rip	4
vrrp	4
error_ttl	0
error_hop_limit	0
local-telnet	3
local-snmp	3
local-http	3
local-tftp	3
local-other	3
v4uc-route	0

v6uc-route	0
rt-host	4
mld	1
nd	2
erps	5
mpls-data	0
mpls-lspv	3
isis	4
bgp	4
cfm	6
web-auth	0
ipfix	0
other	0

每个队列默认最大速率：

队列	默认速率(pps)
6	3500
5	1500
4	1500
3	1500
2	1500
1	1000
0	1000
CPU 端口	6000

10.2.2 配置报文和队列的对应关系

在配置模式下，按如下步骤设置报文和队列的对应关系：

命令	作用
Ruijie(config)# **cpu-protect type { arp-reply | arp-request | bgp | bpdu | cfm | dhcp | dot1x | dvmrp | erps | error-hop-limit | error-ttl | gvrp | icmp | igmp | ipfix | isis | known-v4mc | known-v6mc | lacp | lldp | local-http | local-other | local-snmp | local-telnet | local-tftp | mld | mpls-data | mpls-lspv | nd | ospf | other | pim | qinq | rerp | reup | rip | rldp | rt-host | tpp | udp-helper | unknown-v4mc | unknown-v6mc | v4uc-route | v6uc-route | vrrp | web-auth } traffic-class** *traffic-class-num*	设置报文对应的队列，*traffic-class-num* 的取值范围为 0－6。

如果要恢复其中一种类型报文对应的队列，可以用 **no cpu-protect type { arp-reply | arp-request | bgp | bpdu | cfm | dhcp | dot1x | dvmrp | erps | error-hop-limit | error-ttl | gvrp | icmp | igmp | ipfix | isis | known-v4mc | known-v6mc | lacp | lldp | local-http | local-other | local-snmp | local-telnet | local-tftp | mld | mpls-data | mpls-lspv | nd | ospf |**

other | pim | qinq | rerp | reup | rip | rldp | rt-host | tpp | udp-helper | unknown-v4mc | unknown-v6mc | v4uc-route | v6uc-route | vrrp | web-auth } traffic-class 来执行。

以下例子是表示报文对应的队列的配置过程：

```
Ruijie(config)# cpu-protect type bpdu traffic-class 5

Ruijie(config)# end

Ruijie # show cpu-protect type bpdu

Packet Type       Traffic-class  Bandwidth(pps)  Rate(pps)  Drop(pps)

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

bpdu              5              1000            0          0
```

按以上配置，bpdu 报文就对应到队列 5。

对于不同的产品，通过 cpu-protect type 命令可以配置的报文类型可能也不同，具体能够支持的类型参考 Classifying 章节。

队列 7 保留作为系统保留队列。

10.2.3 配置每个队列的最大速率

在配置模式下，按如下步骤设置一个队列的最大速率：

命令	作用
Ruijie(config)# **cpu-protect traffic-class id id_num bandwidth** *bandwidth_value*	配置每个队列的最大速率（kbps），*id_num* 取值范围为 0－6，*bandwidth-value* 取值范围为 32－131072(pps)
Ruijie(config)# **cpu-protect traffic-class all bandwidth** *bandwidth_value*	配置所有队列的最大速率（kbps），*bandwidth-value* 取值范围为 32－131072(pps)

如果要恢复每个队列的缺省最大速率值，可以用 **no cpu-protect traffic-class** 来执行

以下例子是设置队列 6 的最大速率为 3500(pps)：

```
Ruijie# configure terminal

Ruijie(config)# cpu-protect traffic-class id 6  bandwidth 3500

Ruijie(config)#end

Ruijie# show cpu-protect traffic-class id 6

Traffic-class   Bandwidth(pps)  Rate(pps)

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

6               3500            0
```

速率配置单位为 pps。

10.2.4 配置CPU端口的最大速率

在配置模式下，按如下步骤配置 CPU 端口最大速率：

命令	作用
Ruijie(config)# **cpu-protect cpu bandwidth** *bandwidth_value*	配置 CPU 端口的最大速率（pps），*bandwidth-value* 取值范围为 64－1000000(pps)。

您可以通过 **no cpu-protect cpu** 命令来恢复 CPU 端口的最大速率值。

以下是配置 CPU 端口最大速率为 6000（pps）的实例：

```
Ruijie# configure terminal

Ruijie(config)# cpu-protect cpu bandwidth 6000

Ruijie(config)# end

Ruijie# show cpu-protect cpu

%cpu port bandwidth: 6000(pps)
```

10.2.5 配置地址学习风暴控制

在配置模式下，按如下步骤地址学习风暴控制功能：

命令	作用
Ruijie(config)# **cpu-protect mac-address storm-control enable** *value*	配置地址学习风暴控制，*value* 取值范围为 200－51200((address/second kbps))。

您可以通过 **no cpu-protect mac-address storm-control** 命令来恢复 CPU 端口的最大速率值。

以下是配置 MAC 地址学习风暴控制为 3000 个每秒的例子

```
Ruijie# configure terminal
Ruijie(config)# cpu-protect mac-address storm-control enable 3000
Ruijie(config)#end
Ruijie# show cpu-protect mac-address storm-control
%MAC address storm control state: enable
%MAC address storm control rate:  3000(address/second)
```

10.3 显示 CPU Protect 配置

10.3.1 查看每种类型报文对应的队列

在特权模式下使用如下命令查看每种类型报文对应的队列：

命令	作用

show cpu-protect type { bpdu | arp-request | arp-reply | tpp | dot1x | gvrp | rldp | lacp | rerp | reup | lldp | dhcp | qinq | unknown-v6mc | known-v6mc | unknown-v4mc | known-v4mc | udp-helper | dvmrp | igmp | icmp | ospf | pim | rip | vrrp | error-ttl | error-hop-limit_| local-telnet | local-snmp | local-http | local-tftp | local-other | v4uc-route | v6uc-route | rt-host | mld | nd | erps | mpls-data | mpls-lspv | isis | bgp | cfm | web-auth | ipfix | other | bfd | dldp }	查看每种类型报文对应的队列。

使用 **show cpu-protect type all** 命令查看所有报文对应的队列：

Packet Type	Traffic-class	Bandwidth(pps)	Rate(pps)	Drop(pps)
bpdu	6	1000	0	0
arp-request	2	1000	0	0
arp-reply	2	1000	0	0
tpp	6	1000	0	0
dot1x	1	1000	0	0
gvrp	5	1000	0	0
rldp	5	1000	0	0
lacp	5	1000	0	0
rerp	5	1000	0	0
reup	5	1000	0	0
lldp	5	180	0	0
dhcp	1	1000	0	0
qinq	0	1000	0	0
unknown-v6mc	0	180	0	0
known-v6mc	0	180	0	0
unknown-v4mc	0	180	0	0
known-v4mc	0	180	0	0
udp-helper	0	1000	0	0
dvmrp	4	180	0	0
igmp	1	180	0	0
icmp	3	1000	0	0
ospf	4	1000	0	0
pim	4	180	0	0
rip	4	1000	0	0
vrrp	4	1000	0	0
error-ttl	0	1000	0	0
error-hop-limit	0	1000	0	0
local-telnet	3	1000	0	0
local-snmp	3	1000	0	0
local-http	3	1000	0	0
local-tftp	3	1000	0	0

```
local-other       3              1000           0          0
v4uc-route        0              1000           0          0
v6uc-route        0              1000           0          0
rt-host           4              1000           0          0
mld               1              180            0          0
nd                2              1000           0          0
erps              5              1000           0          0
mpls-data         0              1000           0          0
mpls-lspv         3              1000           0          0
isis              4              1000           0          0
bgp               4              128            0          0
cfm               6              1000           0          0
web-auth          0              1000           0          0
ipfix             0              1000           0          0
other             0              1000           0          0
bfd               6              3500           0          0
dldp              6              1000           0          0
```

对于不同的产品，由于支持的类型不同，所以通过 **show cpu-protect type all** 命令显示的的类型也不完全相同，具体能够支持的类型参考 **Classifying** 章节.

10.3.2 查看每个队列的最大速率

在特权模式下使用如下命令查看每个队列的最大速率：

命令	作用
Ruijie# **show cpu-protect traffic-class id** *id_num*	查看每个队列的最大速率。*id_num* 的取值范围为 0—7
Ruijie# **show cpu-protect traffic-class all**	查看所有队列的最大速率

以下例子使用 **show cpu-protect traffic-class all** 命令查看所有队列的最大速率：

```
Ruijie# show cpu-protect traffic-class all
Traffic-class   Bandwidth(pps)  Rate(pps)
-------------   --------------  ---------
0               1000            0
1               1000            0
2               1500            0
3               1500            0
4               1500            0
5               1500            0
6               3500            0
```

10.3.3 查看CPU端口最大速率

在特权模式下使用如下命令查看 CPU 端口最大速率：

命令	作用
show cpu-protect cpu	查看 CPU 端口最大速率。

以下例子是查看 CPU 端口最大速率：

```
Ruijie# show cpu-protect cpu
%cpu port bandwidth: 6000(pps)
```

10.3.4 查看地址学习风暴控制

在特权模式下使用如下命令查看地址学习风暴控制：

命令	作用
show cpu-protect mac-address storm-control	查看地址学习风暴控制。

以下例子是查看 CPU 端口最大速率：

```
Ruijie# show cpu-protect mac-address storm-control
%MAC address storm control state: enable

%MAC address storm control rate:  8000(address/second)
```

11 DoS 保护

11.1 概述

DoS 保护功能支持防 Land 攻击、防非法 TCP 报文攻击、防非法 L4 报文攻击。

11.1.1 Land 攻击

Land 攻击主要是攻击者将一个 SYN 包的源地址和目的地址都设置为目标主机的地址，源和目的端口号设置为相同值，造成被攻击主机因试图与自己建立 TCP 连接而陷入死循环，甚至系统崩溃。

11.1.2 非法TCP报文攻击

在 TCP 报文的报头中，有几个标志字段：

1) SYN：连接建立标志，TCP SYN 报文就是把这个标志设置为 1，来请求建立连接。

2) ACK：回应标志，在一个 TCP 连接中，除了第一个报文（TCP SYN）外，所有报文都设置该字段作为对上一个报文的响应。

3) FIN： 结束标志，当一台主机接收到一个设置了 FIN 标志的 TCP 报文后，会拆除这个 TCP 连接。

4) RST：复位标志，当 IP 协议栈接收到一个目标端口不存在的 TCP 报文的时候，会回应一个 RST 标志设置的报文。

5) PSH：通知协议栈尽快把 TCP 数据提交给上层程序处理。

6) 非法 TCP 报文攻击是通过非法设置标志字段致使主机处理的资源消耗甚至系统崩溃，例如以下几种经常设置的非法 TCP 报文：

   - SYN 比特和 FIN 比特同时设置的 TCP 报文

     正常情况下，SYN 标志（连接请求标志）和 FIN 标志（连接拆除标志）不能同时出现在一个 TCP 报文中，而且 RFC 也没有规定 IP 协议栈如何处理这样的畸形报文。因此各个操作系统的协议栈在收到这样的报文后的处理方式也不相同，攻击者就可以利用这个特征，通过发送 SYN 和 FIN 同时设置的报文，来判断操作系统的类型，然后针对该操作系统，进行进一步的攻击。

   - 没有设置任何标志的 TCP 报文

     正常情况下，任何 TCP 报文都会设置 SYN，FIN，ACK，RST，PSH 五个标志中的至少一个标志，第一个 TCP 报文（TCP 连接请求报文）设置 SYN 标志，后续报文都设置 ACK 标志。有的协议栈基于这样的假设，没有针对不设置任何标志的 TCP 报文的处理过程，因此这样的协议栈如果收到了这样的报文可能会崩溃。攻击者利用了这个特点，对目标主机进行攻击。

   - 设置了 FIN 标志却没有设置 ACK 标志的 TCP 报文

正常情况下，除了第一报文（SYN 报文）外，所有的报文都设置 ACK 标志，包括 TCP 连接拆除报文（FIN 标志设置的报文）。但有的攻击者却可能向目标主机发送设置了 FIN 标志却没有设置 ACK 标志的 TCP 报文，这样可能导致目标主机崩溃。

11.1.3 自身消耗攻击

自身消耗攻击主要事攻击者向目标主机发送与目标主机服务的 4 层端口号相同的报文，导致目标主机给自己发送 TCP 请求和连接。该攻击会使得目标主机的资源很快耗尽，甚至系统崩溃。

11.2 配置 DoS 保护

11.2.1 缺省的Dos保护设置

下面列出 DoS 缺省配置：

功能特性	缺省值
防 Land 攻击	缺省关闭
防非法 TCP 报文攻击	缺省关闭
防自身消耗报文攻击	缺省关闭

11.2.2 防Land攻击

在全局配置模式下，执行如下命令可以在设备上开启防 Land 攻击功能：

命令	作用
Ruijie**# configure terminal**	进入全局配置模式
Ruijie(config)**# ip deny land**	开启防 Land 攻击功能
Ruijie(config)**# end**	退回到特权模式

11.2.3 预防非法TCP报文攻击

在全局配置模式下，执行如下命令可以在设备上开启防非法 TCP 报文攻击功能：

命令	作用
Ruijie**# configure terminal**	进入全局配置模式
Ruijie(config)**# ip deny invalid-tcp**	开启防非法 TCP 报文攻击功能
Ruijie(config)**# end**	退回到特权模式

11.2.4 预防自身消耗攻击

在全局配置模式下，执行如下命令可以在设备上开启防自身消耗攻击功能：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式
Ruijie(config)# **ip deny invalid-l4port**	开启防自身消耗攻击功能
Ruijie(config)# **end**	退回到特权模式

11.3 显示 DoS 保护的状态

显示防Land攻击的状态

在任意模式下，执行如下命令可以显示防 Land 攻击的状态：

命令	作用
show ip deny land	显示防 Land 攻击的状态

下面的例子显示了如何查看防 Land 攻击的状态：

```
Ruijie# show ip deny land
          DoS Protection Mode               State
-----------------------------------     -----
  protect against land attack             On
```

11.3.1 显示防非法TCP报文攻击的状态

在特权用户模式下，执行如下命令可以显示防非法 TCP 报文攻击的状态：

命令	作用
show ip deny invalid-tcp	显示防非法 TCP 报文攻击的状态

下面的例子显示了如何查看预防非法 TCP 报文攻击的状态：

```
Ruijie# show ip deny invalid-tcp
          DoS Protection Mode                State
-----------------------------------     -----
  protect against invalid tcp attack      On
```

11.3.2 显示防自身消耗攻击的状态

在特权用户模式下，执行如下命令可以显示防自身消耗攻击的状态：

命令	作用
show ip deny invalid-l4port	显示防自身消耗攻击的状态

下面的例子显示了如何查看预防自身消耗攻击的状态：

```
Ruijie# show ip deny invalid-l4port
          DoS Protection Mode                State
```

```
-----------------------------------     -----
  protect against invalid l4port attack  On
```

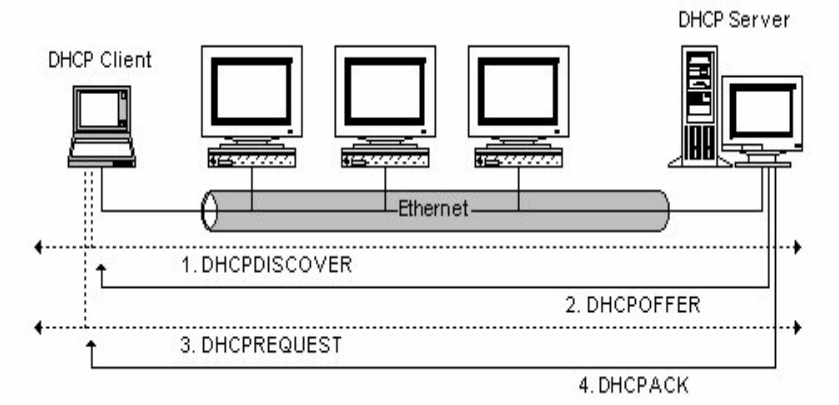
12 DHCP Snooping

12.1 DHCP Snooping 简介

12.1.1 理解DHCP

DHCP 协议被广泛用来动态分配可重用的网络资源，如 IP 地址。一次典型的 DHCP 获取 IP 地址的过程如下所示：

图 12-1



- DHCP Client 发出 DHCP DISCOVER 广播报文给 DHCP Server，若 Client 在一定时间内没有收到服务器的响应，则重发 DHCP DISCOVER 报文。
- DHCP Server 收到 DHCP DISCOVER 报文后，根据一定的策略来给 Client 分配 IP 地址，然后发出 DHCP OFFER 报文。
- DHCP Client 收到 DHCP OFFER 报文后，发出 DHCP REQUEST 请求，请求租用服务器地址池中的 IP 地址，并通告其他服务器已接受此服务器分配的 IP 地址。
- 服务器收到 DHCP REQUEST 报文，验证资源是否可以分配，如果可以分配，则发送 DHCP ACK 报文；如果不可分配，则发送 DHCP NAK 报文。DHCP Client 收到 DHCP ACK 报文，就开始使用服务器分配的 IP 地址。如果收到 DHCP NAK，则重新发送 DHCP DISCOVER 报文。

12.1.2 理解DHCP Snooping

DHCP Snooping：意为 DHCP 窥探，通过对 Client 和服务器之间的 DHCP 交互报文进行窥探，实现对用户 IP 地址使用情况的监控，同时 DHCP Snooping 起到一个 DHCP 报文过滤的功能，通过合理的配置实现对非法的 DHCP 服务的过滤。下边对 DHCP Snooping 内使用到的一些术语及功能进行解释：

1) **DHCP 请求报文**：DHCP 客户端发往 DHCP 服务器的报文。

2) **DHCP 应答报文**：DHCP 服务器发往 DHCP 客户端的报文。

3) **DHCP Snooping TRUST 口：**由于 DHCP 获取 IP 的交互报文是使用广播的形式，从而存在着非法的 DHCP 服务影响用户正常 IP 的获取，更有甚者通过非法的 DHCP 服务欺骗窃取用户信息的现象，为了防止非法的 DHCP 服务的问题，DHCP Snooping 把端口分为两种类型，TRUST 口和 UNTRUST 口，设备只转发 TRUST 口收到的 DHCP 应答报文，而丢弃所有来自 UNTRUST 口的 DHCP 应答报文，这样我们把合法的 DHCP Server 连接的端口设置为 TRUST 口，则其他口为 UNTRUST 口，就可以实现对非法 DHCP Server 的屏蔽。

4) **DHCP Snooping 报文过滤：**在对个别用户禁用 DHCP 报文的情况下，需要评估用户设备发出的任何 DHCP 报文，那么我们可以在端口模式下配置 DHCP 报文过滤功能，过滤掉该端口收到的所有 DHCP 报文。

5) **基于 VLAN 的 DHCP Snooping：**DHCP Snooping 功能生效是以 VLAN 为单位的，默认情况下打开 DHCP Snooping 功能，会在当前设备上的所有 VLAN 上使能 DHCP Snooping 功能，可以通过配置灵活的控制 DHCP Snooping 生效的 VLAN。

6) **DHCP Snooping 绑定数据库：**在 DHCP 环境的网络里经常会出现用户随意设置静态 IP 地址的问题，用户随意设置的 IP 地址不但使网络难以维护，而且会导致一些合法的使用 DHCP 获取 IP 的用户因为冲突而无法正常使用网络，DHCP Snooping 通过窥探 Client 和 Server 之间交互的报文，把用户获取到的 IP 信息以及用户 MAC、VID、PORT、租约时间等信息组成用户记录表项，从而形成 DHCP Snooping 的用户数据库，配合 ARP 检测功能或 ARP CHECK 功能的使用，进而达到控制用户合法使用 IP 地址的目的。

7) **DHCP Snooping 速率限制：**DHCP Snooping 需要对所有非信任端的 DHCP 请求报文进行检查，同时将合法的 DHCP 请求报文转发到信任口所在的网络。为了防止在非信任端出现 DHCP 请求报文攻击、控制流向信任网络的 DHCP 请求报文速率。DHCP Snooping 支持在端口对收到的 DHCP 报文进行速率限制，当接口收到的 DHCP 报文速率超过设定的限制时，丢弃超过限制速率的那部分 DHCP 报文。DHCP Snooping 的速率限制基于接口配置，可以选择通过 DHCP Snooping 的速率限制命令配置，也可以选择通过 NFPP 的速率限制命令配置，效果是一样的。对于支持 CPP 的产品来说，如果同时配置了 CPP 的 DHCP 报文速率限制和 DHCP Snooping 的报文速率限制，CPP 的配置将优先于 DHCP Snooping 的速率限制生效，因此为了确保 DHCP Snooping 速率限制生效，需要注意 CPP 的速率上限不小于 DHCP Snooping 的限制或者 NFPP 的限制。 CPP 的配置请查看配置指南《配置 CPU 保护》，NFPP 的配置请查看 NFPP 配置指导。

DHCP Snooping 通过对经过设备的 DHCP 报文进行合法性检查，丢弃不合法的 DHCP 报文，记录用户信息并生成 DHCP Snooping 绑定数据库供其他功能（如：ARP 检测功能）查询使用。以下几种类型的报文被认为是非法的 DHCP 报文：

- UNTRUST 口收到的 DHCP 应答报文，包括 DHCPACK、DHCPNACK、DHCPOFFER 等。
- UNTRUST 口收到的带有网关信息[giaddr]的 DHCP request 报文。
- 打开 mac 校验时，源 MAC 与 DHCP 报文携带的 chaddr 字段值为不同的报文。
- DHCPRELEASE 报文中的用户在 DHCP Snooping 绑定数据库中存在，但是 DHCPRELEASE 报文的接收端口和保存在 DHCP Snooping 绑定数据库中的端口不一致，那么这个 DHCPRELEASE 报文是非法的。

12.1.3 理解DHCP Snooping information option

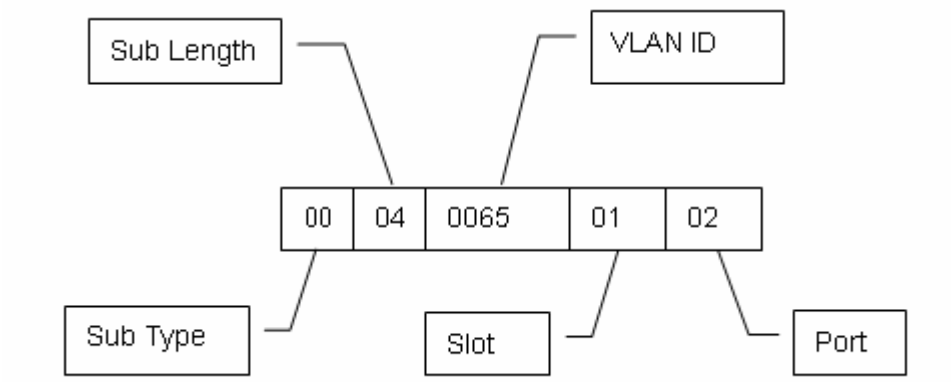
部分网络管理员在对当前的用户进行 IP 管理时，希望能够根据用户所处的位置来给用户分配 IP，即希望能够根据用户所连接的网络设备的信息进行用户的 IP 分配，从而交换机在进行 DHCP 窥探的同时把一些用户相关的设备信息以 DHCP option 的方式加入到 DHCP 请求报文中，根据 RFC3046，所使用的 option 选项号为 82。Option 82 选项最多可以包含 255 个子选项。若定义了 Option 82，则至少要定义一个子选项。目前设备只支持 Circuit ID（电路 ID 子选项）和 Remote ID（远程 ID 子选项）两个子选项。在 DHCP Server 服务器配置对 option82 内容的解析，这个服务器就可以通过 option82 上传的内容，获取到更多用户的信息，从而更准确地给用户分配 IP。

- Circuit ID：

Circuit ID 的默认填充内容是接收到 DHCP 客户端请求报文的端口所属 VLAN 的编号以及端口索引（端口索引的取值为端口所在槽号和端口号），扩展填充内容是自定义的字符串。

Circuit ID 填充格式有两种，一种是标准填充格式，一种是扩展填充格式，在同一个网络域中，只能使用其中的一种，不能混合使用。标准填充格式时，Circuit ID 子选项只能填充默认的填充内容，如下所示：

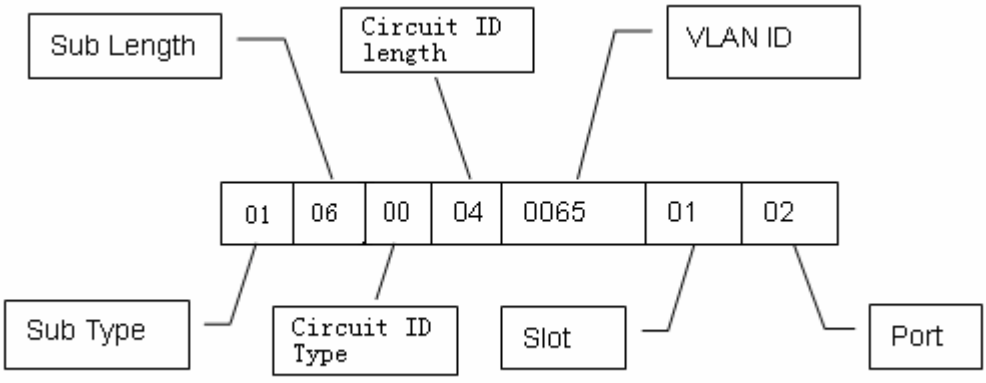
图 12-2



如果需要使用自定义的填充内容，那么可以使用扩展填充格式。扩展填充格式的填充内容可以是默认填充内容，也可以是扩展填充内容。为了区分填充内容的不同，在子选项长度后增加一个字节的内容类型字段和一个字节的内容长度字段，如果是默认填充内容，则设置内容类型为 0；如果是扩展填充内容，则设置内容类型为 1。

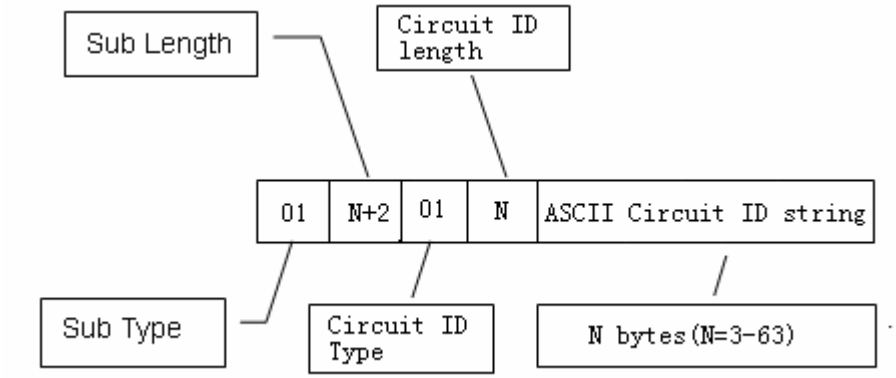
默认填充内容的格式如下：

图 12-3



扩展填充内容的格式如下：

图 12-4

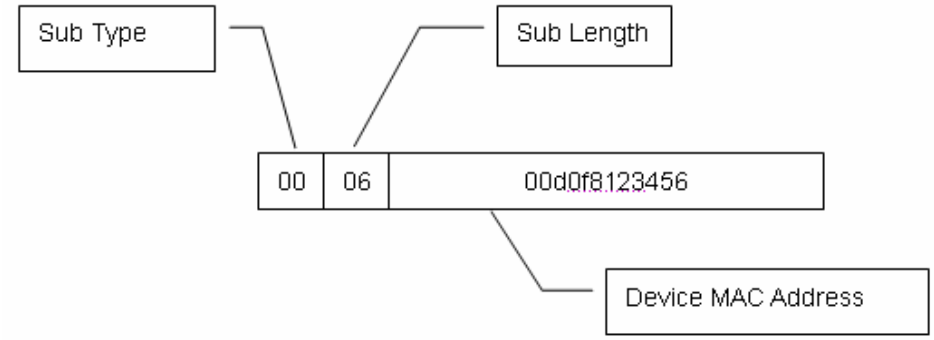


- Remote ID：

Remote ID 的默认填充内容是接收到 DHCP 客户端请求报文的 DHCP 中继设备的桥 MAC 地址。扩展填充内容是自定义的字符串。

Remote ID 填充格式有两种，一种是标准填充格式，一种是扩展填充格式，在同一个网络域中，只能使用其中的一种，不能混合使用。标准填充格式时，Remote ID 子选项只能填充默认的填充内容，如下所示：

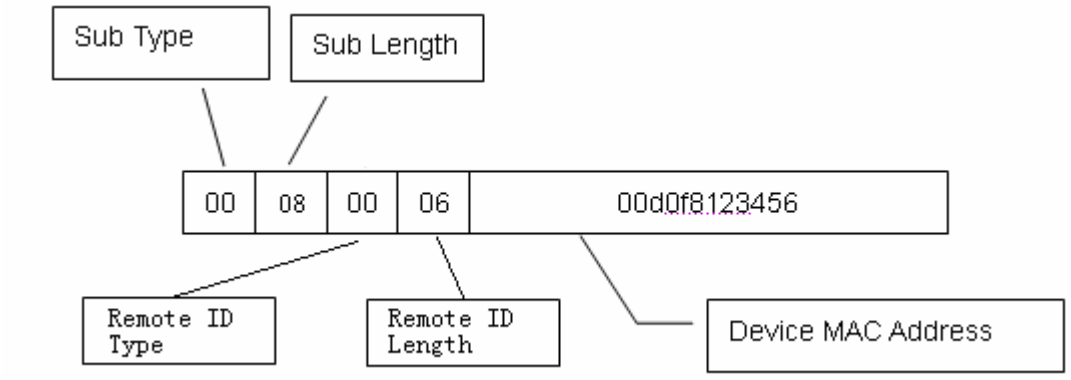
图 12-5



如果需要使用自定义的填充内容，那么可以使用扩展填充格式。扩展填充格式的填充内容可以是默认填充内容，也可以是扩展填充内容。为了区分填充内容的不同，在子选项长度后增加一个字节的内容类型字段和一个字节的内容长度字段，如果是默认填充内容，则设置内容类型为 0；如果是扩展填充内容，则设置内容类型为 1。

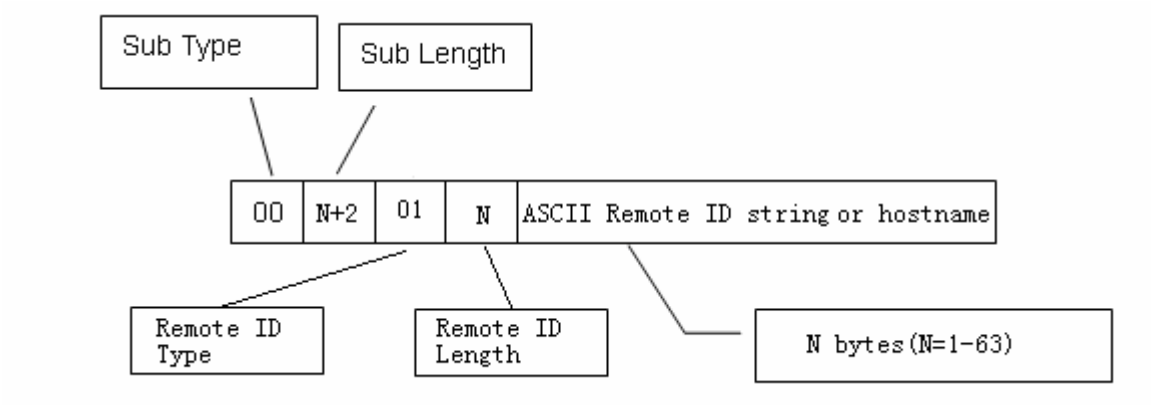
默认填充内容的格式如下：

图 12-6



扩展填充内容的格式如下：

图 12-7



Circuit ID 中端口索引的取值为端口所在槽号和端口号。其中端口号是指端口在槽上的序号，AP 口（聚合口）的端口号就是 AP 号。例如 Fa0/10，端口号就是 10，AP 11 的端口号就是 11。其中槽号是设备（堆叠认为是一台设备）上所有槽排序的序号，AP 口的槽号在最后。槽排序的序号从 0 开始，可用 show slots 命令查看。例如：

例 1：

```
Ruijie#show slots  （只列出 Dev、slot 示例）
  Dev Slot
  --- ----
  1   0    ------>槽号为 0
  1   1    ------>槽号为 1
  1   2    ------>槽号为 2
```

此时 AP 口的槽号为 3。

例 2：

```
Ruijie#show slots （只列出 Dev、slot 示例）
  Dev Slot
  --- ----
  1   0    ------>槽号为 0
  1   1    ------>槽号为 1
  1   2    ------>槽号为 2
  2   0    ------>槽号为 3
  2   1    ------>槽号为 4
  2   2    ------>槽号为 5
```

此时 AP 口的槽号为 6。

12.2 DHCP snooping 的相关安全功能

在 DHCP 的网络环境中，管理员经常碰到的一个问题就是一些用户随意修改使用静态的 IP 地址，而不去使用动态获取的 IP 地址。这会导致一些使用动态获取 IP 的用户的无法正常使用网络，并且会使网络环境变复杂。因为 DHCP 动态绑定是设备在 DHCP snooping 的过程通过记录的合法用户的 IP 信息，所以对 DHCP 动态绑定进行相关的安全处理，可以解决用户随

意使用静态 IP 地址的问题。当前的安全控制存在三种方式，一种是结合 IP Source Guard 功能对合法用户进行地址绑定，第二种就是使用软件的 DAI（动态 ARP 检测），通过对 ARP 的控制进行用户的合法性校验，第三种结合 ARP CHECK 的功能，来对合法用户的 ARP 报文进行绑定。

DHCP Snooping 模块和其他安全功能的优先级关系，可参考《锐捷新安全方案技术白皮书》。

结合 IP Source Guard 功能进行地址绑定时由于受硬件表项的限制，交换机能够支持的 DHCP 用户数目有限，当交换机上用户过多时，可能出现合法用户也无法添加硬件表项而不能正常使用网络的现象，而使用 DAI 功能时，由于所有的 ARP 报文都需要通过 CPU 转发和处理，所以会降低交换机的转发性能。

12.2.1 理解DHCP Snooping和IP Source Guard地址绑定的关系

IP Source Guard 功能维护一个 IP 源地址数据库，通过将数据库中的用户信息[VLAN、MAC、IP、PORT]设置为硬件过滤表项，只允许对应的用户使用网络，更多信息请参考《配置 IP Source Guard》。

DHCP Snooping 维护一个用户 IP 的数据库，并将该数据提供给 IP Source Guard 功能进行过滤，从而限制只有通过 DHCP 获取 IP 的用户才能够使用网络，这样就阻止了用户随意设置静态 IP。

12.2.2 DHCP Snooping和DAI的关系

DAI(Dynamic ARP Inspection,动态 ARP 检测)就是对经过设备的所有 ARP 报文进行检查。由于 DHCP 绑定过滤只针对 IP 报文，不能进行 ARP 报文的过滤，所以为了增加安全性，防止 ARP 欺骗等问题，对于 DHCP 绑定的用户进行 ARP 合法性检查，DHCP Snooping 提供数据库信息给 ARP 探测使用，在开启 DAI 功能的设备上，当开启 IP Source Guard 地址绑定的端口收到 ARP 报文时，DAI 模块就根据报文查询 DHCP snooping 的绑定数据库，只有当收到的 ARP 报文数据字段的源 MAC、源 IP 和端口信息都匹配时才认为收到的 ARP 报文是合法的，才进行相关的学习和转发操作，否则丢弃该报文，更多信息参考《DAI 配置指导》。

12.2.3 DHCP Snooping和ARP CHECK的关系

ARP CHECK 是对经过设备的所有 ARP 报文进行检查，DHCP Snooping 提供数据库信息供 ARP CHECK 使用，在开启 ARP CHECK 功能的设备上，当收到 ARP 报文时，ARP CHECK 模块就根据报文查询 DHCP snooping 的绑定数据库，只有当开启 IP Source Guard 地址绑定的端口收到的 ARP 报文数据字段的源 MAC、源 IP 和端口信息都匹配时才认为收到的 ARP 报文是合法的，才进行相关的学习和转发操作，否则丢弃该报文。

12.3 配置 DHCP Snooping 的其他注意事项

DHCP Snooping 功能与 DOT1x 的 DHCP Option 82 功能是互斥的，不能同时使用 DHCP Snooping 和 DHCP Option82。

DHCP Snooping 和 DAI 功能或 ARP CHECK 功能共用，可以控制用户必须使用 DHCP 分配的 IP 上网。

12.4 DHCP Snooping 配置

12.4.1 配置打开和关闭DHCP Snooping

缺省情况下，设备的 DHCP Snooping 功能是关闭,当配置 **ip dhcp snooping** 命令后，设备就打开了 dhcp snooping 功能

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# [**no**] **ip dhcp snooping**	DHCP snooping 打开和关闭

下边是配置打开设备 DHCP snooping 功能：

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping
Ruijie(config)# end
Ruijie# show ip dhcp snooping
Switch DHCP snooping  status                      :   ENABLE
DHCP snooping  Verification of hwaddr status  :   DISABLE
DHCP snooping database write-delay time        :   0 seconds
DHCP snooping option 82 status                    :   DISABLE
DHCP snooping Support bootp bind status        :   DISABLE
Interface              Trusted           Rate limit (pps)
------------------      ---------     ----------------
GigabitEthernet 0/1       YES                unlimited
```

12.4.2 配置端口DHCP报文过滤

缺省情况下，设备端口的 DHCP 请求报文过滤功能是关闭的。当不想对某个端口下的用户提供 DHCP 服务时，可配置此功能，配置后，就会对这个端口上来的 DHCP 请求报文进行过滤。

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **interface** *interface*	进入接口配置模式
Ruijie(config-if)# [**no**] **ip dhcp snooping suppression**	配置接口过滤 DHCP 报文功能

下边是配置打开设备端口的 DHCP 请求报文过滤功能：

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# ip dhcp snooping suppression
```

12.4.3 配置DHCP Snooping功能生效的VLAN

缺省情况下，DHCP Snooping 功能对所有 VLAN 生效。如果要配置 DHCP Snooping 在某个 VLAN 上失效，将该 VLAN 从 DHCP Snooping 生效的 VLAN 范围中去除。

命令	作用
Ruijie**# configure terminal**	进入配置模式
Ruijie(config)**# [no] ip dhcp snooping vlan** {*vlan-rng* | {*vlan-min* [*vlan-max*]}}	配置DHCP Snooping功能生效的VLAN

下边是配置 DHCP snooping 功能在 VLAN1000 上生效：

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping vlan 1000
Ruijie(config)# end
```

打开 DHCP Snooping 功能，默认情况下会在设备上的所有 VLAN 上打开 DHCP Snooping 功能，如果需要基于 VLAN 打开关闭 DHCP Snooping 功能，只需要在 DHCP Snooping 生效范围中添加/删除该 VLAN。

12.4.4 配置DHCP源MAC检查功能

配置此命令后，设备就会对 UNTRUST 口送上来的 DHCP Request 报文进行源 MAC 和 Client 字段的 MAC 地址校验检查，丢弃 MAC 值不相同的不合法的 DHCP 请求报文。默认不检查。

命令	作用
Ruijie**# configure terminal**	进入配置模式
Ruijie(config)**# [no] ip dhcp snooping verify mac-address**	打开和关闭源 MAC 检查功能

下边的是打开 DHCP 源 MAC 检查的功能

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping verify mac-address
Ruijie(config)# end
Ruijie# show ip dhcp snooping
Switch DHCP snooping  status                        :   ENABLE
DHCP snooping  Verification of hwaddr status   :   ENABLE
DHCP snooping database write-delay time         :   0 seconds
DHCP snooping option 82 status                    :   DISABLE
DHCP snooping Support bootp bind status         :   DISABLE
Interface              Trusted           Rate limit (pps)
-----------------      ---------     ---------------
GigabitEthernet 0/1       YES                unlimited
```

12.4.5 配置静态DHCP snooping information option

通过配置如下命令，在进行 DHCP 窥探转发时，给每个 DHCP 请求添加 option82 选项。缺省情况下该功能是关闭的。

命令	作用
Ruijie**# configure terminal**	进入配置模式
Ruijie(config)**# [no] ip dhcp snooping Information option [standard-format]**	设置 DHCP snooping information option；standard-format：有此关键字时，填充的格式为标准格式，否则为扩展格式。

Ruijie(config)# [**no**] **ip dhcp snooping information option format remote-id** [**string** *ASCII-string* | **hostname**]	在扩展格式下配置 remote-id。 string：填充内容为自定义字符串； hostname：填充内容为主机名。
Ruijie(config)# **interface** *interface*	进入接口配置模式
Ruijie(config-if)# [**no**] **ip dhcp snooping vlan** *vlan-id* **information option format-type circuit-id string** *ASCII-string*	在扩展格式下配置 circuit-id 的自定义字符串。
Ruijie(config-if)# [**no**] **ip dhcp snooping vlan** *vlan-id* **information option change-vlan-to vlan** *vlan-id*	在扩展格式下配置 circuit-id 的 vlan 映射，和 Step 5 的命令互斥。

下边是配置打开 DHCP information option 功能：

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping information option
Ruijie(config)# end
Ruijie# show ip dhcp snooping
Switch DHCP snooping  status                    :   ENABLE
DHCP snooping  Verification of hwaddr status    :   ENABLE
DHCP snooping database write-delay time         :   0 seconds
DHCP snooping option 82 status                    :   ENABLE
DHCP snooping Support bootp bind status         :   DISABLE
Interface              Trusted           Rate limit (pps)
-----------------      ---------     ---------------
GigabitEthernet 0/1       YES                unlimited
```

当配置此功能后，DHCP relay 的 information option82 功能就会失效。

12.4.6 配置定时写DHCP Snooping数据库信息到flash

为了防止设备断电重启，设备上的 DHCP 用户信息丢失，而导致设备重启后，重启前已成功获取 IP 地址的用户不能通信，DHCP Snooping 提供可配置的定时把 DHCP Snooping 数据库信息写入 flash 的命令来保存 DHCP 用户信息。默认情况下，定时为 0，即不定时写 flash。

命令	作用
Ruijie**# configure terminal**	进入配置模式
Ruijie(config)# [**no**] **ip dhcp snooping database write-delay** [*time*]	设置 DHCP 延迟写 flash 的时间 *time*：600s--86400s.缺省为 0

下边的是设置 DHCP Snooping 延迟写 flash 的时间为 3600s：

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping database write-delay 3600
Ruijie(config)# end
Ruijie# show ip dhcp snooping
Switch DHCP snooping  status                    :   ENABLE
DHCP snooping  Verification of hwaddr status    :   ENABLE
DHCP snooping database write-delay time         :   3600 seconds
```

```
DHCP snooping option 82 status                    :   ENABLE
DHCP snooping Support bootp bind status         :   DISABLE
Interface              Trusted           Rate limit (pps)
-----------------      ---------     ---------------
GigabitEthernet 0/1       YES                unlimited
```

由于不停擦写 flash 会造成 flash 的使用寿命缩短，所以在设置延迟写 flash 时间时需要注意，设置时间较短有利于设备信息更有效的保存，设置时间较长能够减少写 flash 的次数，延长 flash 的使用寿命。

12.4.7 手动把DHCP snooping数据库信息写到flash

为了防止设备断电重启导致设备上的 DHCP 用户信息丢失而使用户不能上网，除了配置定时写 flash 外，也可以根据需要手动地把当前的 DHCP Snooping 绑定数据库信息写入 flash。

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **ip dhcp snooping database write-to-flash**	把 DHCP snooping 数据库信息写入 flash

下边的是手动的把 DHCP Snooping 数据库信息写入 flash：

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping database write-to-flash
Ruijie(config)# end
```

12.4.8 手动把flash中的信息导入DHCP snooping数据库

在开启 DHCP snooping 功能时，可以根据需要手动地把当前 flash 中的信息导入 DHCP Snooping 绑定数据库。

命令	作用
Ruijie# **renew ip dhcp snooping database**	把 flash 中信息导入 DHCP snooping 数据库。

下边的是手动的把 flash 中信息导入 DHCP Snooping 数据库：

```
Ruijie# renew ip dhcp snooping database
```

12.4.9 配置端口为TRUST口

用户通过配置此命令来设置一个端口为 TRUST 口，默认情况下所有端口全部为 UNTRUST 口：

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **interface** *interface*	进入接口配置模式
Ruijie(config-if)# **[no] ip dhcp snooping trust**	将端口设置为 trust 口

下边是配置设备的 1 端口为 TRUST 口：

```
Ruijie# configure terminal
```

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# ip dhcp snooping trust
Ruijie(config-if)# end
Ruijie# show ip dhcp snooping
Switch DHCP snooping  status                    :   ENABLE
DHCP snooping  Verification of hwaddr status    :   DISABLE
DHCP snooping database write-delay time         :   3600 seconds
DHCP snooping option 82 status                  :   DISABLE
DHCP snooping Support bootp bind status         :   DISABLE
Interface              Trusted           Rate limit (pps)
-----------------      ---------     ----------------
GigabitEthernet 0/1       YES                unlimited
```

打开 DHCP Snooping 后，只有配置为 TRUST 口连接的服务器发出的 DHCP 响应报文才能够被转发。

12.4.10 配置端口接收DHCP报文的速率

用户通过配置此命令可以设置端口收到 DHCP 报文的速率：

命令	作用
Ruijie**# configure terminal**	进入配置模式
Ruijie(config)**# interface** *interface*	进入接口配置模式
Ruijie(config-if)**# [no] ip dhcp snooping limit rate** *rate-pps*	设置端口接收 DHCP 报文的速率，会转化成 NFPP 的命令 **nfpp dhcp-guard policy per-port** *rate -pps 200*，详见《CPP 配置指导》。

下边是配置设备的 1 端口接收 DHCP 报文的速率为 100：

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# ip dhcp snooping limit rate 100
Ruijie(config-if)# end
Ruijie(config-if)#sh run interface gigabitEthernet 0/1
interface GigabitEthernet 0/1
 nfpp dhcp-guard policy per-port 100 200
```

设置 DHCP Snooping 速率限制的时候，请确认 CPP 设置的 DHCP 报文的速率限制；如果 CPP 设置比较低，即使在 DHCP Snooping 速率限制范围内仍然会出现 DHCP 报文丢弃的现象；缺省情况下不进行 DHCP Snooping 的速率限制。

从上面的 **show run interface** 结果可以看出，从 RGOS10.4(2)开始，DHCP Snooping 的速率配置命令被 NFPP 的速率限制命令取代，为了保持升级兼容性,DHCP Snooping 速率命令仍然可以使用，但是配置后将生效到 NFPP。另外，由于 NFPP 只能基于物理端口配置，而 DHCP Snooping 支持 AP 口的配置，因此在 AP 上配置 DHCP Snooping 的速率限制命令,实际将生效到该 AP 的所有成员口。而这也意味，如果原先是在一个没有成员口的 AP 上配置了 DHCP Snooping 速率限制命令，升级之后，由于该 AP 无成员口，该配置将丢失。但由于在没有成员口上配置速率限制并无实际意义，因此该问题并不会对实际的网络使用产生影响。

12.4.11 清空DHCP Snooping数据库动态用户信息

如果 DHCP Snooping 的数据库需要重新生成时，可用此命令删除当前的 DHCP Snooping 数据库的信息。

命令	作用
Ruijie# **clear ip dhcp snooping binding** [**vlan** *vlan-id* | *mac* | *ip* | **interface** *interface-id*]	清空当前数据库的信息，可基于 VLAN、MAC、IP、接口删除，并可组合使用。

下边的是手动清空当前数据库的信息：

```
Ruijie# clear ip dhcp snooping binding
```

12.5 DHCP snooping 配置显示

12.5.1 显示DHCP snooping

您可以通过以下步骤显示 **ip dhcp snooping** 内容

命令	作用
show ip dhcp snooping	显示 dhcp snooping 的相关配置信息

例如：

```
Ruijie# show ip dhcp snooping
Switch DHCP snooping  status                    :   ENABLE
DHCP snooping  Verification of hwaddr status    :   ENABLE
DHCP snooping database write-delay time         :   3600 seconds
DHCP snooping option 82 status                  :   ENABLE
DHCP snooping Support bootp bind status         :   ENABLE
Interface               Trusted           Rate limit (pps)
------------------      ---------     ----------------
GigabitEthernet 0/1       YES                 unlimited
```

12.5.2 显示DHCP snooping 数据库信息

您可以通过以下步骤显示 **ip dhcp snooping** 数据库信息的相关内容

命令	作用
show ip dhcp snooping binding	查看 DHCP Snooping 绑定数据库的用户信息

例如：

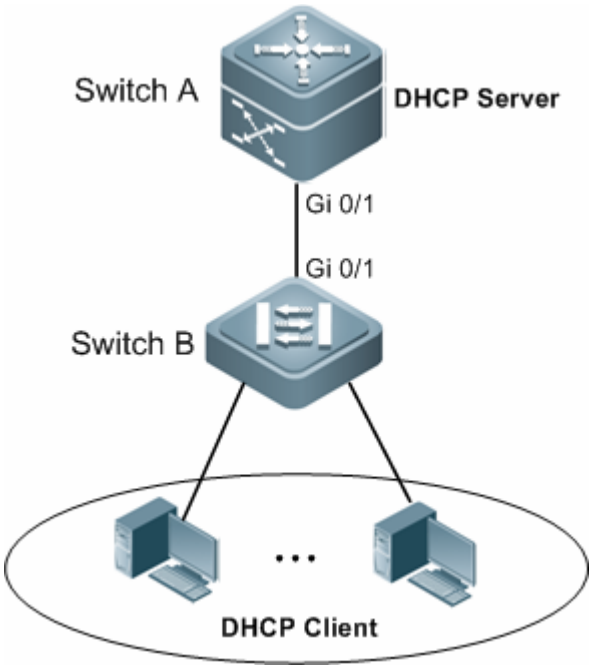
```
Ruijie# show ip dhcp snooping binding
Total number of bindings: 1
MacAddress         IpAddress       Lease(sec)   Type          VLAN  Interface
---------------- --------------- ------------ -------------
```

```
001b.241e.6775      192.168.12.9     7200          dhcp-snooping 1      GigabitEthernet 0/5
```

12.6 DHCP Snooping 典型配置用例

拓扑图

图 12-8 DHCP Snooping 用例示意图



应用需求

1) DHCP 客户端用户通过合法 DHCP 服务器动态获取 IP 地址。

2) 避免其他用户私设 DHCP 服务器。

配置要点

在接入设备（本例为 Switch B）上开启 DHCP Snooping 功能，将上链口（本例为端口 Gi 0/1）设置为信任口。

配置步骤

- 配置 Switch B

第一步，打开 DHCP Snooping 功能。

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#ip dhcp snooping
```

第二步，配置上链口为信任口。

```
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#ip dhcp snooping trust
```

配置验证

第一步，确认 Switch B 的配置，关注点：是否开启 DHCP Snooping 功能、配置的 DHCP Snooping 信任口是否为上链口。

```
Ruijie#show running-config
!
ip dhcp snooping
!
interface GigabitEthernet 0/1
 ip dhcp snooping trust
```

第二步，查看 Switch B 的 DHCP Snooping 配置情况，关注点为信任口是否正确。

```
Ruijie#show ip dhcp snooping
Switch DHCP snooping  status                    :   ENABLE
DHCP snooping  Verification of hwaddr status    :   DISABLE
DHCP snooping database write-delay time         :   0 seconds
DHCP snooping option 82 status                  :   DISABLE
DHCP snooping Support bootp bind status         :   DISABLE
Interface                      Trusted       Rate limit (pps)
-------------------------      -------       ----------------
GigabitEthernet 0/1            YES           unlimited
```

第三步，查看 DHCP Snooping 地址绑定数据库信息（用户的 MAC 地址、动态分配的 IP 地址、地址租期、对应的 VLAN 和端口号等）。

```
Ruijie#show ip dhcp snooping binding
Total number of bindings: 1
MacAddress          IpAddress       Lease(sec)   Type           VLAN  Interface
------------------ --------------- ------------ -------------- ----- --------------------
0013.2049.9014      172.16.1.2      86207        dhcp-snooping 1     GigabitEthernet 0/11
```

13 动态 ARP 检测

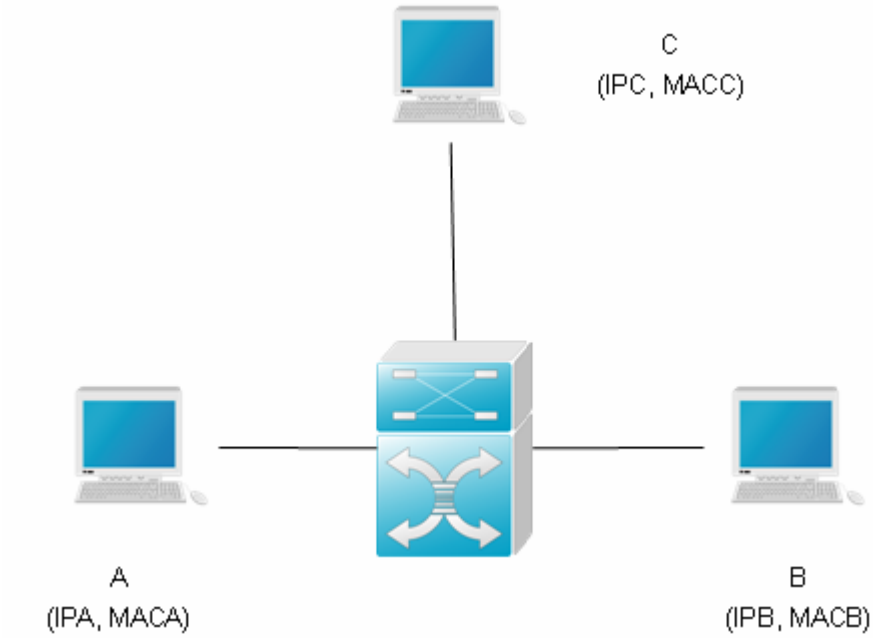
13.1 理解DAI

DAI 的全称是 Dynamic ARP Inspection，中文名为动态 ARP 检测。即对接收到的 ARP 报文进行合法性检查。不合法的 ARP 报文会被丢弃。

13.1.1 理解 ARP 欺骗攻击

由于 ARP 协议本身的缺陷，ARP 协议不对收到的 ARP 报文进行合法性检查。这就造成了攻击者利用协议的漏洞轻易的进行 ARP 欺骗攻击。这其中，最典型的就是中间人攻击。中间人攻击描述如下：

图 13-1



如上图所示：设备 A、B、C 均连接在锐捷设备上，并且它们位于同一个子网。它们的 IP 和 MAC 分别表示为（IPA, MACA）(IPB, MACB) (IPC, MACC)。当设备 A 需要和设备 B 进行网络层通信时，设备 A 将会在子网内广播一个 ARP 请求，询问设备 B 的 MAC 值。当设备 B 接收到此 ARP 请求报文时，会更新自己的 ARP 缓存，使用的是 IPA 和 MACA,并发出 ARP 应答。设备 A 收到此应答后，会更新自己的 ARP 缓存，使用的是 IPB 和 MACB。

在这种模型下，设备 C 可以使设备 A 和设备 B 中的对应 ARP 表项对应关系不正确。使用的策略是，不断向网络中广播 ARP 应答。此应答使用的 IP 地址是 IPA 和 IPB，而 MAC 地址是 MACC，这样，设备 A 中就会存在 ARP 表项(IPB、MACC)，设备 B 中就会存在 ARP 表项(IPA, MACC)。这样，设备 A 和 B 之间的通信就变成了和设备 C 之间的通信，而设备 A、B 对此都一无所知。设备 C 充当了中间人的角色，只需要把发给自己的报文做合适的修改，转给另一方即可。这就是有名的中间人攻击。

13.1.2 理解 DAI 和 ARP 欺骗攻击

DAI 确保了只有合法的 ARP 报文才会被设备转发。它主要执行以下几个步骤：

- 在打开 DAI 检查功能的 VLAN 所对应的非信任端口上拦截住所有 ARP 请求和应答报文
- 在做进一步相关处理之前，根据 DHCP 数据库的设置，对拦截住的 ARP 报文进行合法性检查。
- 丢弃没有通过检查的报文。
- 检查通过的报文继续做相应的处理，送给相应的目的地。
- ARP 报文是否合法的依据是 DHCP snooping binding 数据库，具体请参考《DHCP snooping 配置指导》。

13.1.3 接口信任状态和网络安全

基于设备上每一个端口的信任状态，对 ARP 报文作出相应的检查，从受信任端口接收到的报文将跳过 DAI 检查，被认为是合法的 ARP 报文； 而从非信任端口接收到的 ARP 报文，将严格执行 DAI 检查。

在一个典型的网络配置中，应该将连接到网络设备的二层端口设置为受信任端口，连接到主机设备的二层端口设置为非信任端口。

将一个二层端口错误的配置成非信任端口可能会影响到网络正常通信。

具体配置命令请参考 **ip arp inspection trust**，**show ip arp inspection interface**。

13.2 配置DAI

DAI 是一个基于 ARP 协议的安全过滤技术，简而言之就是配置一系列的过滤策略使得经过设备的 ARP 报文的合法性得到比传统更加有效的检验。

要使用 DAI 相关功能，可选择性地执行以下各项任务：

- 启用指定 VLAN 的 DAI 功能（必须）
- 设置端口的信任状态（可选）
- DHCP snooping database 相关配置（可选）

13.2.1 启用指定 VLAN 的 DAI 报文检查功能

如果没有启用了 VLAN vid 的 DAI 报文检查功能，vlan-id = vid 的 ARP 报文会跳过 DAI 相关的安全检查（不会跳过 ARP 报文限速）。

可以通过 **show ip arp inspection vlan** 查看所有 VLAN 是否启用了 DAI 报文检查功能

要配置 VLAN 的 DAI 报文检查功能，在接口配置模式中执行以下命令：

命令	作用

Ruijie(config)# **ip arp inspection vlan** *vlan-id*	启用 VLAN *vlan-id* 的 DAI 报文检查功能开关
Ruijie(config)# **no ip arp inspection vlan** [*vlan-id*]	关闭 VLAN *vlan-id* 的 DAI 报文检查功能开关。缺省情况下，所有 VLAN 的 DAI 报文检查功能是关闭的。 省略 *vlan-id* 时关掉所有 VLAN 的 DAI 报文检查功能

13.2.2 设置 DAI 不检查 ARP 报文源端口功能

默认情况下 DAI 会检查 ARP 报文的源端口是否和 DHCP snooping 表项中记录的端口一致，如果不一致则认为是非法 ARP 报文。在无线场景下用户发生迁移后，源端口发生变化，如果用户没有重新获取地址，则该用户的 ARP 报文会被 DAI 过滤掉而导致无法上网，针对该场景，需要设置 DAI 不检查源端口信息。

要配置 DAI 不检查 ARP 报文的源端口信息，可以在全局模式下执行以下命令：

命令	作用
Ruijie(config)# **ip arp inspection validate interface**	DAI 检查源端口信息，缺省情况下 DAI 检查源端口信息。
Ruijie(config)# **no ip arp inspection validate interface**	DAI 不检查源端口信息

13.2.3 设置端口的信任状态

此功能应用在二层接口配置模式，且此二层接口为一个 SVI 的成员口。

如果端口是可信任的，ARP 报文将跳过进一步的检查，否则，会使用 DHCP snooping 数据库的信息来检查当前 ARP 报文的合法性

要设置端口信任状态，在接口配置模式中执行以下命令：

命令	作用
Ruijie(config-if)# **ip arp inspection trust**	设置端口是可信任的
Ruijie(config-if)# **no ip arp inspection trust**	设置端口是不可信任的。缺省情况下，所有二层端口都是不可信任的。

13.2.4 DHCP snooping database 相关配置

参考《DHCP Snooping 配置指导》。

如果没有配置 DHCP Snooping database，则所有 ARP 报文通过检查

13.3 显示DAI

13.3.1 显示 VLAN 是否启用 DAI 功能

要显示各 VLAN 的启用状态，在全局配置模式中执行以下命令：

命令	作用
show ip arp inspection vlan	显示各 VLAN 的启用状态

13.3.2 显示各二层接口 DAI 配置状态

要显示各二层接口 DAI 配置状态，在全局配置模式中执行以下命令：

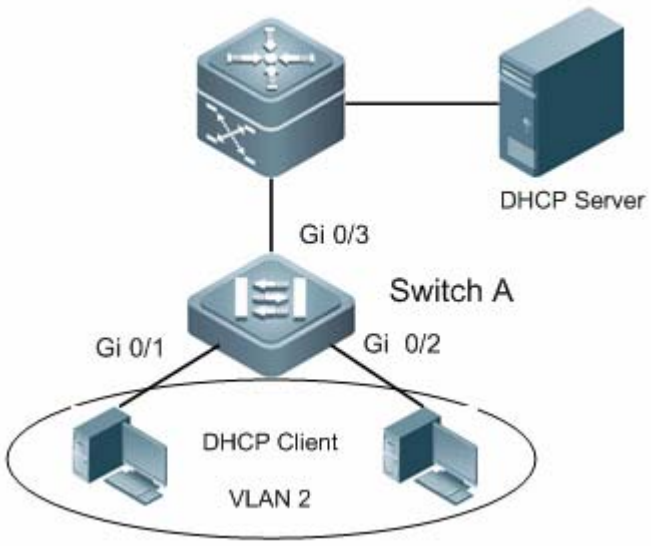
命令	作用
show ip arp inspection interface	显示各二层接口的 DAI 配置（包括信任状态，和速率限制）

支持 NFPP(网络基础保护策略)的产品，速率限制由 NFPP 完成，不再通过 DAI 进行设置，因此上述命令只显示接口的信任状态。

13.4 DAI典型配置用例

拓扑图

图 13-2



应用需求

如上图所示，用户 PC 的 IP 地址是 DHCP 服务器自动分配的，为了保证用户能够正常上网，有如下要求：

1) 用户 PC 只能从指定的 DHCP 服务器获取 IP 地址，不允许私设 DHCP 服务器。

2) 用户 PC 只能使用合法 DHCP 服务器分配的 IP 地址上网，不允许随意设置 IP 地址。

配置要点

- 在接入交换机(本例为Switch A)上启用DHCP Snooping并将连接合法DHCP服务器的上链口(本例为GigabitEthernet 0/3）设置为信任口可满足第一个需求。
- 在接入设备（本例为 Switch A）启用 DHCP Snooping 基础上再开启 DAI，可满足第二需求。

在汇聚或核心交换上如有其他 PC 接入并存在私设 DHCP 服务器可能，也需要开启 DHCP Snooping。

配置步骤

- 配置 Switch A

第一步，设置直连用户 PC 的端口的 VLAN。

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#interface range gigabitEthernet 0/1-2
Ruijie(config-if-range)#switchport access vlan 2
```

第二步，开启 DHCP SNOOPING 功能。

```
Ruijie(config-if-range)#exit
Ruijie(config)#ip dhcp snooping
```

第三步，在对应的 VLAN 上开启 DAI 功能。

```
Ruijie(config)#ip arp inspection vlan 2
```

第四步，将上链口设置为 DHCP SNOOPING 信任口

```
Ruijie(config)#interface gigabitEthernet 0/3
Ruijie(config-if-GigabitEthernet 0/3)#ip dhcp snooping trust
```

第五步，将上链口设置为 DAI 信任口。

```
Ruijie(config-if-GigabitEthernet 0/3)#ip arp inspection trust
```

配置验证

第一步，确认配置是否正确，关注点为 DHCP Snooping/DAI 是否启用，信任接口是否正确。

```
Ruijie#show running-config
ip dhcp snooping
!
ip arp inspection vlan 2
!
interface GigabitEthernet 0/1
 switchport access vlan 2
!
interface GigabitEthernet 0/2
 switchport access vlan 2
!
```

```
interface GigabitEthernet 0/3
ip dhcp snooping trust
 ip arp inspection trust
```

第二步，查看 DHCP SNOOPING 的使能状态以及对应的信任端口，关注点为上链口是否设置为可信任接口。

```
Ruijie#show ip dhcp snooping
Switch DHCP snooping  status                    :   ENABLE
DHCP snooping  Verification of hwaddr status    :   DISABLE
DHCP snooping database write-delay time         :   0 seconds
DHCP snooping option 82 status                  :   DISABLE
DHCP snooping Support bootp bind status         :   DISABLE
Interface                      Trusted       Rate limit (pps)
-------------------------      -------       -----------------
GigabitEthernet 0/3            YES           unlimited
```

第三步，查看 DAI 状态，关注点为对应的 VLAN 的使能情况和上链口是否设置为可信任接口。

```
Ruijie#show ip arp inspection vlan
Vlan     Configuration
----     -------------
2         Enable
Ruijie#show ip arp inspection interface
       Interface         Trust State
---------------------    -----------
GigabitEthernet 0/1      Untrusted
GigabitEthernet 0/2      Untrusted
GigabitEthernet 0/3      Trusted
```

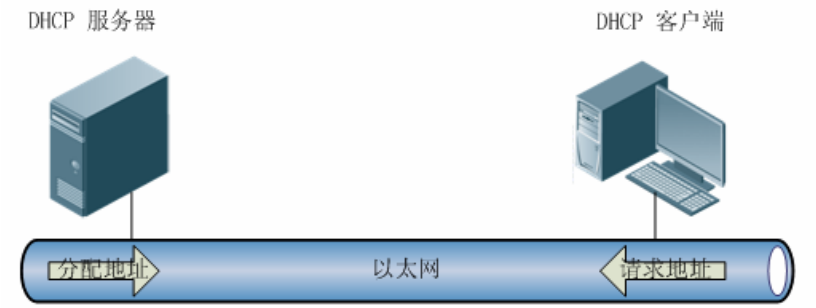
如果需要查看 DHCP Snooping 形成的数据库绑定信息，可以通过 **show ip dhcp snooping binding** 命令，在此不再列举。

14 IP Source Guard

14.1.1 理解DHCP

在典型的 DHCP 环境中，DHCP 服务器负责网络中地址的管理和分配，网络中的主机如果想要使用网络资源，必须向 DHCP 服务器申请合法的网络地址，只有获得了合法地址的客户端才能正常使用网络；

图 14-1 正常的 DHCP 地址分配



然而仅仅依靠服务器/客户端这种模型完全无法保证网络中地址资源的有效管理，以及地址管理的安全性；来自客户端的攻击[非法报文]，以及网络中可能存在的各种伪装服务器，对传统的 DHCP 模型提出了更高的安全要求；

DHCP Snooping 的引入解决这一问题，在连接 DHCP 服务器与客户端的设备上开启 DHCP Snooping 功能，就可以解决传统 DHCP 模型中的大部分安全；DHCP Snooping 将网络分为两个部分：客户端网络-非信任网络，对来自该网络上的客户端请求进行安全检测；服务器网络-信任网络，将收到的合法的客户端请求转发到配置的信任服务器网络，由服务器完成地址的统一管理分配；通过这种方式，DHCP Snooping 解决了传统 DHCP 模型中的几个典型的安全问题：

图 14-2 存在伪装 DHCP 服务器的网络

图 14-3 存在伪装 DHCP 客户端进行攻击的网络

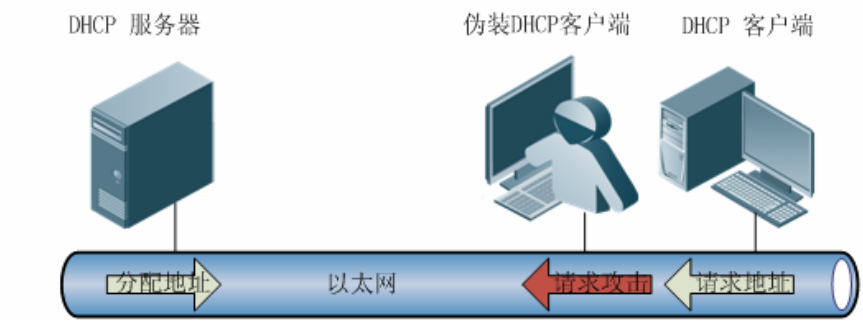
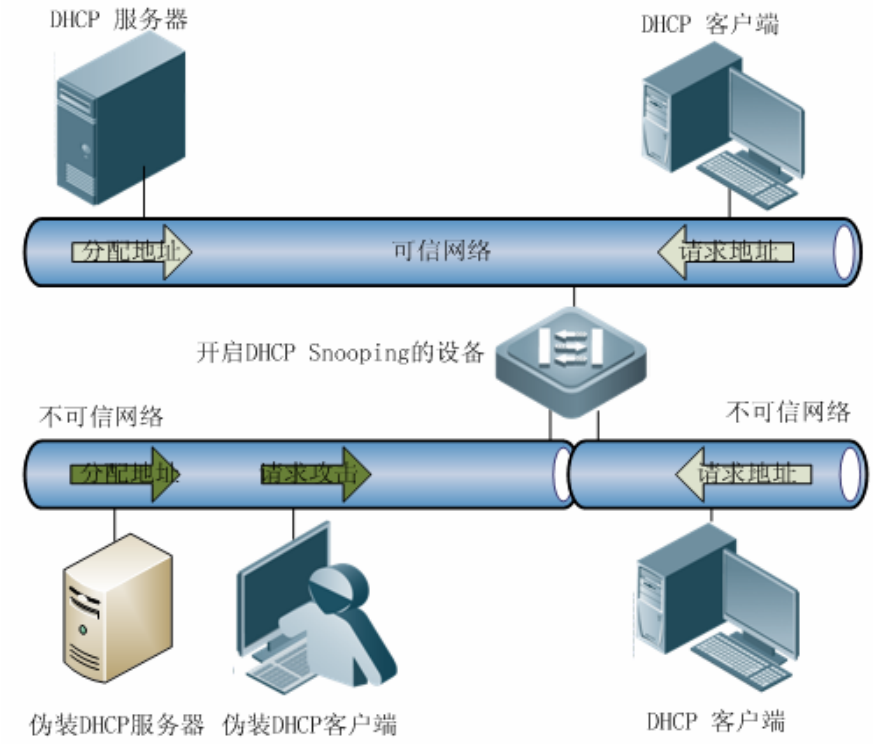


图 14-4 通过 DHCP Snooping 进行保护的网络



然而，虽然依靠 DHCP Snooping 的过滤，最大限度的过滤了来自客户端的攻击，杜绝了网络中的伪装服务器；但却无法对客户端网络中的非 DHCP 客户端进行有效的限制，也就是说无法检测有私设 IP 的客户端，这在一个纯 DHCP 的网络应用中，是无法接受的；为了防止这种 DHCP 网络中客户端私设 IP，可以在连接服务器与客户端网络之间的设备上开启 IP Source Guard 功能，IP Source Guard 是基于 DHCP Snooping 的，在 DHCP 模型中可以有效的保证网络中 DHCP 客户端能够正常使用网络。

14.1.2 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 Source Guard 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 过虑， ARP Check 功能对 ARP 报文中的 Sender IP+Sender MAC 或仅对 Sender IP 检查过虑。

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。

14.1.3 IP Source Guard配置的其他注意事项

IP Source Guard 功能的应用是和 DHCP Snooping 结合起来的，也就是说基于接口的 IP Source Guard 仅仅在 DHCP Snooping 控制范围内的非信任口上生效，在其他信任口或者非 DHCP Snooping 控制范围内的接口上配置该功能，功能将不生效。

14.2 IP Source Guard配置

14.2.1 配置接口IP Source Guard功能

缺省情况下，接口的 IP Source Guard 功能是关闭的，接口下联的所有用户都可以使用网络；打开接口 IP Source Guard 功能之后，将会根据 IP 源地址绑定数据库对接口下联客户端进行过滤

命令	作用
Ruijie(config)# **interface interface**	进入接口配置模式
Ruijie(config-if-*type ID*)# [**no**] **ip verify source** [*port-security*]	打开接口上的 IP Source Guard 功能 默认为基于仅 IP 的过虑 port-security 将配置基于 IP+MAC 的过滤

下边是配置打开接口 1 的 IP Source Guard 功能：

```
Ruijie(config)# interface FastEthernet 0/1
Ruijie(config-if)# ip verify source
Ruijie(config-if)# end
```

- IP Source Guard 功能和 DHCP Snooping 功能结合应用，该功能仅仅在 DHCP Snooping 控制范围的接口上生效;
- IP Source Guard 功能仅仅在 DHCP Snooping 控制的非信任口上生效。
- IP Source Guard 支持在 AP 口上配置，但不支持在 AP 成员端口上配置。

14.2.2 配置静态IP源地址绑定用户

在某些应用情况下，某些端口下的用户希望能够静态使用某些 IP，就可以通过添加静态用户信息到 IP 源地址绑定数据库中来实现

命令	作用
Ruijie(config)# [**no**] **ip source binding mac-address vlan** *vlan_id ip-address* [**interface** *interface-id* **| ip-mac | ip-only**]	配置静态的 IP 源地址绑定用户到数据库。当没有接口选项时，绑定表项在 VLAN 内的所有绑定端口上生效。 **interface**：绑定到接口； **ip-mac**：全局绑定为 IP+MAC 绑定； **ip-only**：全局绑定为仅 IP 绑定。

下边是添加一个静态的用户到设备的 9 端口：

```
Ruijie# configure terminal
Ruijie(config)# ip source binding 00d0.f801.0101 vlan 1 192.168.4.243 interface FastEthernet 0/9
```

端口必需在 **vlan** *vlan_id* 参数所指定的 VLAN 中，否则无法进行有效的用户绑定。

14.3 IP Source Guard配置显示

14.3.1 显示IP Source Guard过滤表项

您可以通过以下步骤显示 IP Source Guard 过滤表项

命令	作用
show ip verify source [**interface** *interface*]	显示 IP Source Guard 过滤表项

例如：

```
Ruijie # show ip verify source
Interface       Filter-type Filter-mode Ip-address  Mac-address  VLAN
---------------   ---------   -----------  ----------  ----------- ------
FastEthernet 0/3  ip       active     3.3.3.3                1
FastEthernet 0/3  ip       active     deny-all
FastEthernet 0/4    ip+mac     active        4.4.4.4     0000.0000.0001    1
FastEthernet 0/4    ip+mac     active        deny-all
```

14.3.2 显示IP源地址绑数据库信息

您可以通过以下步骤显示 IP 源地址数据库信息的相关内容

命令	作用

show ip source binding [*ip-address*] [*mac-address*] [**dhcp-snooping**] [**static**] [**vlan** *vlan-id*] [**interface** *interface-id*]	查看 IP 源地址绑定数据库

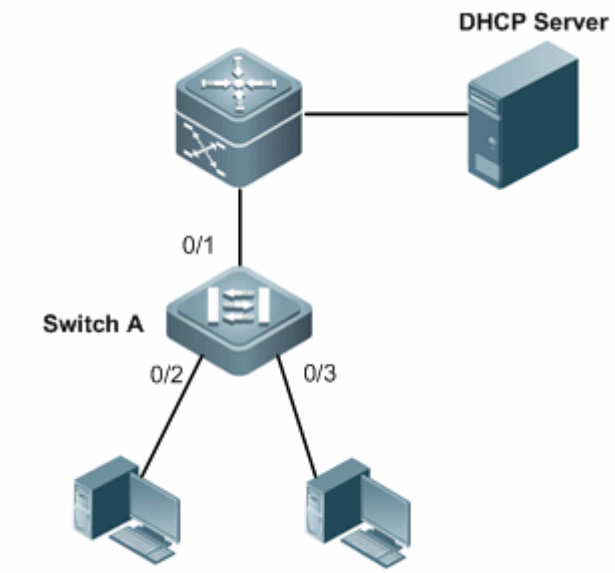
例如：

```
Ruijie# sh ip source binding
MacAddress      IpAddress    Lease(sec)  Type       VLAN  Interface
-----------     ----------   ----------  -------   ----  ------
0000.0000.0001  1.0.0.1      infinite     static    1     FastEthernet2/1
Total number of bindings: 1
```

14.4 IP Source Guard配置用例

拓扑图

图 14-5 DHCP 部署环境



应用需求

用户只能使用合法 DHCP 服务器动态分配或管理员静态分配的 IP 地址访问网络，源 IP 地址与交换机硬件过滤列表中的 IP 地址不匹配的 IP 报文被阻断，保证网络安全

配置要点

在接入设备（本例为 Switch A）上配置 IP Source Guard 和 DHCP Snooping 组合功能可满足需求：

1) 设置上链口（本例为 GigabitEthernet 0/1）为信任口，避免 DHCP 服务器欺骗

2) 在直连 PC 的端口上（本例为 GigabitEthernet 0/2 、GigabitEthernet 0/3）启用 IP Source Guard 功能

3) 管理员指定 IP 地址的用户可通过 IP Source Guard 静态绑定来实现（本例静态绑定 IP 地址为 192.168.216.4、MAC 地址为 0000.0000.0001）

配置步骤

- 配置 Swtich A

第一步，开启 DHCP Snooping 功能。

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#ip dhcp snooping
```

第二步，将上链口设置为 DHCP SNOOPING 信任口。

```
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#ip dhcp snooping trust
Ruijie(config-if-GigabitEthernet 0/1)#exit
```

第三步，在直连 PC 的端口上开启 IP Source Guard 功能

```
Ruijie(config)#interface range gigabitEthernet 0/2-3
Ruijie(config-if-range)#ip verify source port-security
Ruijie(config-if-range)#exit
```

第四步，配置静态绑定用户

```
Ruijie(config)#ip source binding 0000.0000.0001 vlan 1 192.168.216.4 interface gigabitEthernet 0/2
```

配置验证

第一步，查看 Switch A 的配置情况，关注点：是否开启 DHCP Snooping、是否将上链口配置为信任口、是否在直连用户的端口上开启 IP Source Guard 功能以及静态绑定用户的表项是否正确

```
Ruijie#show running-config
ip dhcp snooping
!
ip source binding 0000.0000.0001 vlan 1 192.168.216.1 interface GigabitEthernet 0/2
!
interface GigabitEthernet 0/1
 ip dhcp snooping trust
!
interface GigabitEthernet 0/2
 ip verify source port-security
!
interface GigabitEthernet 0/3
 ip verify source port-security
```

第二步，查看 DHCP Snooping 用户绑定数据库

```
Ruijie#show ip dhcp snooping binding
Total number of bindings: 2
MacAddress          IpAddress       Lease(sec)   Type           VLAN  Interface
------------------ --------------- ------------ -------------
0013.2049.9014      192.168.216.4   86233        dhcp-snooping 1     GigabitEthernet 0/3
00e0.4c70.b7e2      192.168.216.3   86228        dhcp-snooping 1     GigabitEthernet 0/2
```

第三步，查看通过 DHCP Snooping 用户绑定数据库和静态绑定用户共同生成的 IP 硬件过滤库：

```
Ruijie#show ip source binding
MacAddress          IpAddress       Lease(sec)   Type           VLAN  Interface
------------------ --------------- ------------ -------------
0000.0000.0001      192.168.216.4   infinite     static         1     GigabitEthernet 0/2
0013.2049.9014      192.168.216.4   86176        dhcp-snooping 1     GigabitEthernet 0/3
00e0.4c70.b7e2      192.168.216.3   86171        dhcp-snooping 1     GigabitEthernet 0/2
Total number of bindings: 3
```

第四步，查看 IP Source Guard 过滤表项如下：

```
Ruijie#show ip verify source
Interface            Filter-type Filter-mode Ip-address      Mac-address    VLAN
-------------------- ----------- ----------- --------------- -------------- --------
GigabitEthernet 0/2  ip+mac      active      192.168.216.4   0000.0000.0001  1
GigabitEthernet 0/2  ip+mac      active      192.168.216.3   00e0.4c70.b7e2  1
GigabitEthernet 0/2  ip+mac      active      deny-all        deny-all
GigabitEthernet 0/3  ip+mac      active      192.168.216.4   0013.2049.9014  1
GigabitEthernet 0/3  ip+mac      active      deny-all        deny-all
```

15 ND Snooping

15.1 理解ND Snooping

15.1.1 概述

在 IPv6 网络中，网络节点使用 ND（Neighbor Discovery，邻居发现）协议进行路由器发现与自动配置，重复地址探测，链路层地址解析，邻居可达性探测，链路层地址改变通告和路由重定向等操作。

由于 ND 协议缺乏内在的安全性，因此其面临地址解析攻击和路由信息攻击问题，而通过部署外在的加密认证体系来增加安全性又很复杂。IPv6 使用 ND 协议实现的无状态地址自动配置机制在带来更易用的网络的时，使得无法对网络用户进行有效的监管。

ND snooping 技术的提出就是为了解决上述问题。

15.1.2 ND防攻击

在使用无状态地址自动配置时，IPv6 节点使用路由器公告信息配置接口 IPv6 地址，并获取直连网段前缀，网关 IP 地址，链路 MTU 等信息。路由器还可使用 ND 重定向报文修改主机路由表中相关路由的下一跳信息。因此攻击者可发送非法的 RA 报文和重定向报文，修改被攻击主机的路由表信息（例如网关 IP 地址），从而达到拒绝服务攻击、中间人攻击等目的。此类以欺骗主机路由信息为目的的攻击，我们称之为“路由信息攻击”。

为了解决上述问题，ND Snooping 特性将网络设备的接口划分为 trust 接口和 untrust 接口。trust 接口用于接 Router 或服务器等可信节点，untrust 接口用于接用户 PC 等不可信任节点。对于 trust 接口接收到的 ND 报文可任意通过，而对于 untrust 接口上接收到的重定向报文和 RA 报文一律丢弃，这样就防止了路由信息攻击。若从 Untrust 接口上接收到 NA 报文中携带路由器才能设置的信息（R 位被设置），也认为其是非法的。

ND 防路由信息攻击随 ND Snooping 特性的开启而始终开启。

15.1.3 ND Snooping与CPP

网络设备执行 ND 报文安全检查需要消耗一定的 CPU 资源，为了防止攻击者发送大量的 ND 报文对网络设备进行拒绝服务攻击，设备使用 CPP 功能对 ND 报文进行整机限速和优先级控制。ND Snooping 特性开启后，CPP 对 ND 报文的控制将自动开启。关于 CPP 的 ND 报文限速配置，ND 报文与其它报文之间的优先级关系，请参见 CPP 功能配置章节。

15.1.4 ND Snooping与NFPP

除了用 CPP 对 ND 报文进行整机控制，设备还支持使用 NFPP 功能以接口为粒度对 ND 报文进行更精准的限速，NFPP 仅对送 CPU 检查的 ND 报文有效。该特性由 NFPP 功能提供，具体配置方法请参考“配置 NFPP”章节。ND 报文速率限制同时满足接口和整机限制。

15.1.5 ND Snooping与IPv6 兼容模式

某些 IPv4 安全策略为对 IPv6 报文进行控制，提供 IPv6 兼容模式配置项，ND Snooping 特性只能工作在 IPv6 兼容模式的严格模式下，关于 IPv6 兼容模式的说明请参见 IPv4+MAC 绑定章节。

15.1.6 协议规范

- RFC 2464: Transmission of IPv6 Packets over Ethernet Networks
- RFC 4861: Neighbor Discovery for IP version 6 (IPv6)
- RFC 4862: IPv6 Stateless Address Autoconfiguration

15.2 缺省配置

功能特性	缺省值
ND Snooping 全局使能	关闭
接口信任模式	Untrust

15.3 使能ND Snooping

15.3.1 全局使能

命令	作用
Ruijie**# configure terminal**	进入全局配置模式。
Ruijie(config)# [**no**] **ipv6 nd snooping**	全局打开和关闭 IPv6 ND Snooping

例如：全局开启 IPv6 ND snooping

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# ipv6 nd snooping
```

15.4 配置ND防攻击

15.4.1 配置接口信任状态

在默认情况下，所有接口的信任状态为 untrust，您可以使用如下命令将某一接口的信任状态设置为 trust：

命令	作用
Ruijie**# configure terminal**	进入全局配置模式。
Ruijie(config)**# Interface** *interface_id*	进入接口配置模式。
Ruijie(config-if)**# ipv6 nd snooping trust**	配置接口 IPv6 ND Snooping 信任状态为 trust

例如：配置接口 FastEthernet 0/1 为 Trust 接口。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# interface fastethernet 0/1
Ruijie(config-if)# ipv6 nd snooping trust
```

15.5 显示ND Snooping

15.5.1 显示ND Snooping配置

命令	作用
show ipv6 nd snooping [interface]	显示 ND snooping 配置项，interface 表示仅显示接口信息。

例如：显示 ND snooping 配置

```
Ruijie# show ipv6 nd snoopingGlobal switch: enabled
ND Snooping is disabled in following VLANs:
    None
Address resolution check: disabled, software
Route information check: enabled, software
Stateless-user monitor: disabled
Stateless-user bind: disabled, loose, IP-only
Interface    Trusted  Combine-security
---------    -------  ----------------
Gi0/1        Y        N
```

例如：显示 ND snooping 接口配置

```
Ruijie# show ipv6 nd snooping interface
Interface    Trusted  Combine-security
```

```
---------    -------  ----------------
Gi0/1        Y        N
```

15.6 ND Snooping典型配置举例

组网需求

用户使用无状态自动配置方式分配 IPv6 地址，现准备部署 IPv6 ND Snooping 特性，以实现如下目的：

- 防 ND 路由信息攻击。

组网拓扑

1) 网络采用无状态地址自动配置的方式配置接口 IPv6 地址。

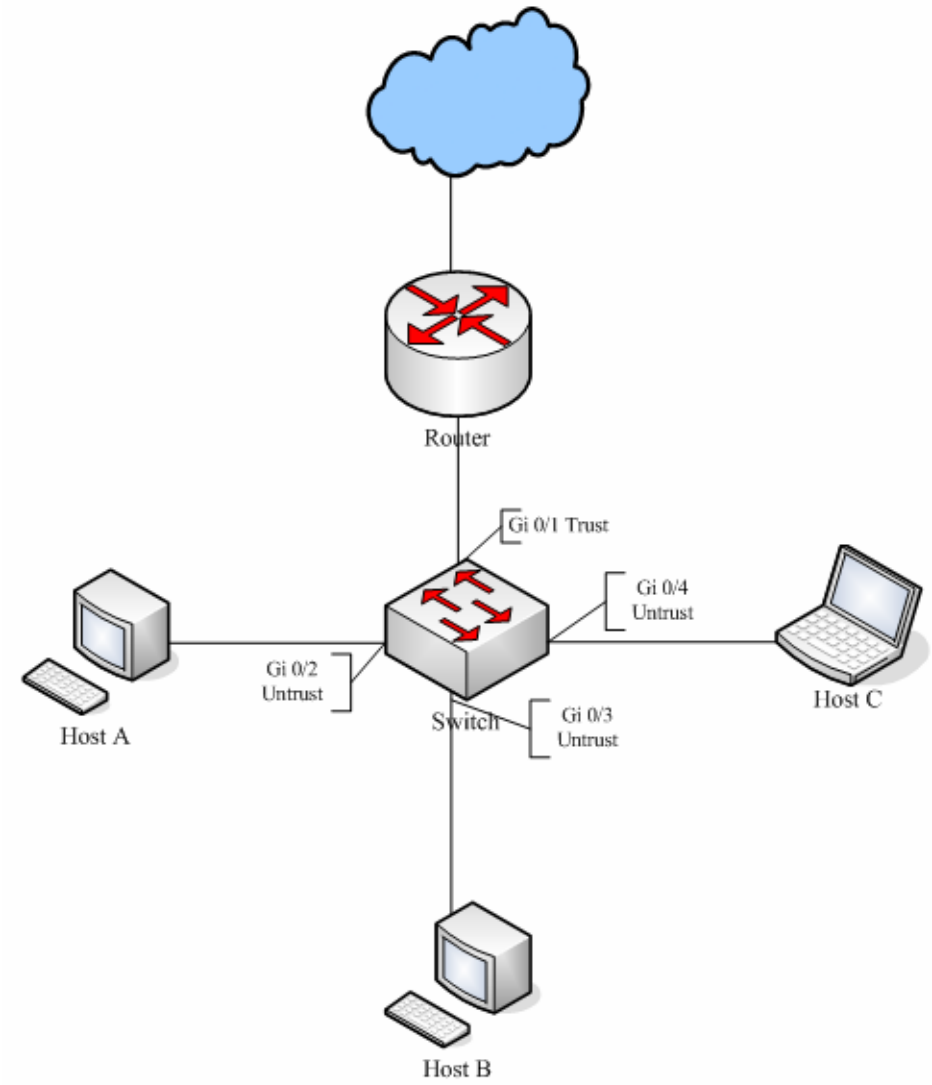
2) Switch 接口 FA 0/1 与路由器互连。

3) 主机 A 与 Switch 接口 FA 0/2 互连，属于 VLAN1。

4) 主机 B 与 Switch 接口 FA 0/3 互连，属于 VLAN2。

5) 主机 C 与 Switch 接口 FA 0/4 互连，属于 VLAN3。

图 15-1



配置步骤

- 开启 IPv6 ND Snooping 功能

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#ipv6 nd snooping
```

- 配置接口的 trust 属性

```
Ruijie(config)#interface fastethernet 0/1
Ruijie(config-if)#ipv6 nd snooping trust
Ruijie(config-if)#exit
```

显示验证

```
Ruijie# show ipv6 nd snoopingGlobal switch: enabled
```

```
ND Snooping is disabled in following VLANs:
    None
Address resolution check: disabled, software
Route information check: enabled, software
Stateless-user monitor: disabled
Stateless-user bind: disabled, loose, IP-only
Interface    Trusted  Combine-security
---------    -------  ----------------
Gi0/1        Y        N
```

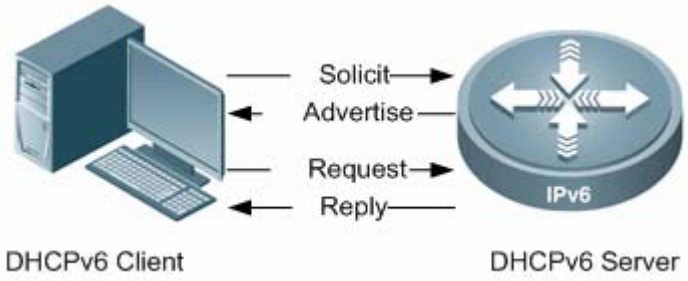
16 DHCPv6 Snooping

16.1 理解DHCPv6 Snooping

16.1.1 DHCPv6 概述

作为 IPv6 在设计之初就提出的框架，网络节点的自动配置成为了 IPv6 网络的一个主要特点。在新的网络框架中，提出了无状态配置和有状态配置的概念。通过无状态自动配置，网络中新加入的节点可以通过路由通告(Router Advertisement)完成所有的配置。而在有状态自动配置中，网络节点需要通过和网络中的 DHCPv6 服务器交互完成地址以及其他参数的配置。DHCPv6 作为目前唯一提出的有状态配置模型，在 RFC3315 中进行了详细的描述。一次典型的 DHCPv6 交互过程如下图所示：

图 16-1 DHCPv6 典型过程

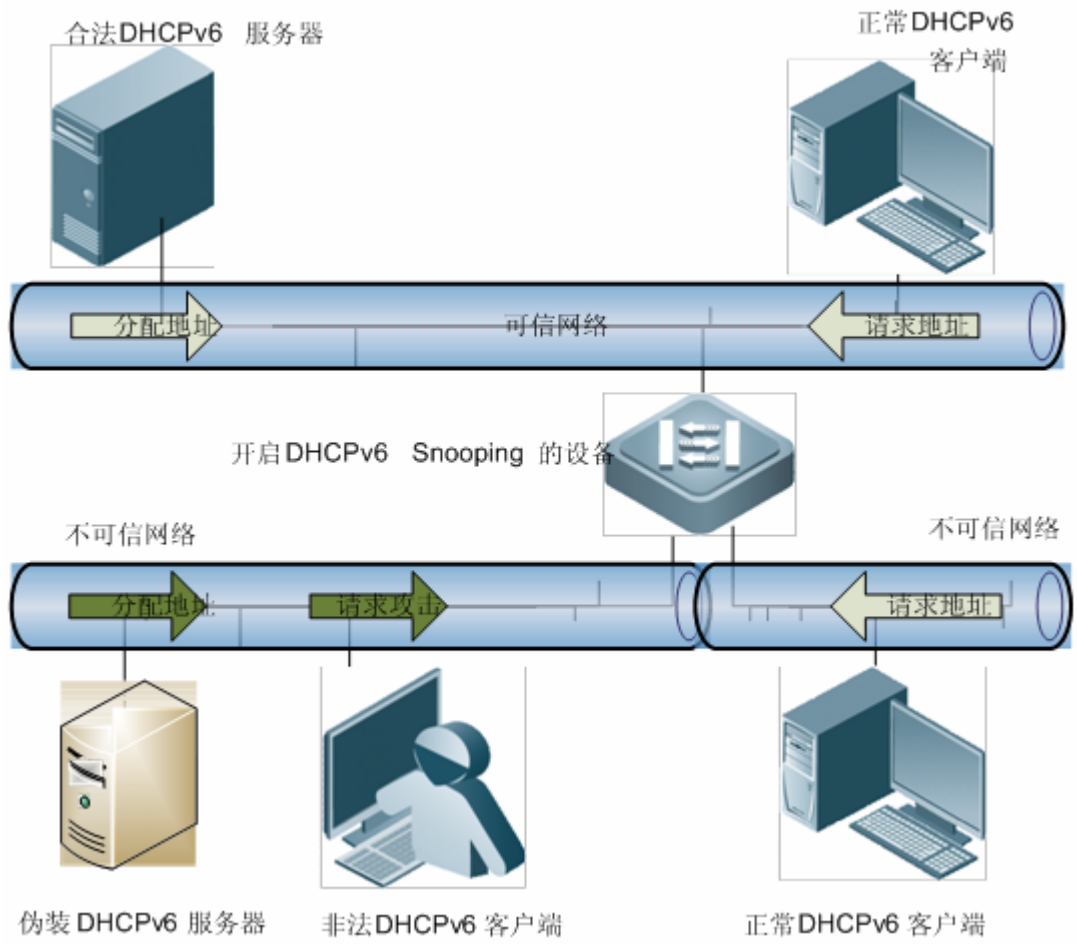


- DHCPv6 客户端在本地链路内发送一个目的地址为 FF02::1:2、目的 UDP 端口为 547 的多播 Solicit 请求报文，本地链路内所有的 DHCPv6 服务器和 DHCPv6 中继都会收到。
- DHCPv6 服务器收到多播 Solicit 请求报文后，单播回应 Advertise 响应报文。
- DHCPv6 客户端选择服务器后，在本地链路内发送一个目的地址为 FF02::1:2、目的 UDP 端口为 547 的多播 Request 请求报文。
- DHCPv6 服务器收到 Request 报文后，单播发送 Reply 响应报文，完成配置过程。

16.1.2 DHCPv6 Snooping概述

DHCPv6 窥探，窥探 DHCPv6 客户端和服务器之间的 DHCPv6 交互报文，实现对非法服务器响应报文的过滤。

图 16-2 通过 DHCPv6 Snooping 进行保护的网络



如上图，DHCPv6 Snooping 可以阻止在不可信网络中的伪装 DHCP 服务器和非法 DHCP 客户端的异常报文攻击；可以根据 DHCPv6 服务器分配的 IPV6 前缀、用户 MAC、用户所在端口、端口所属 VLAN ID、租约时间等信息组成一个用户表项，从而形成 DHCPv6 Snooping 的 IPv6 地址前缀数据库；还可以根据 DHCPv6 服务器分配的 IPV6 地址、用户 MAC、用户所在端口、端口所属 VLAN ID、租约时间等信息组成一个用户表项，从而形成 DHCPv6 Snooping 的 IPv6 地址绑定数据库。

16.1.3 DHCPv6 Snooping information option概述

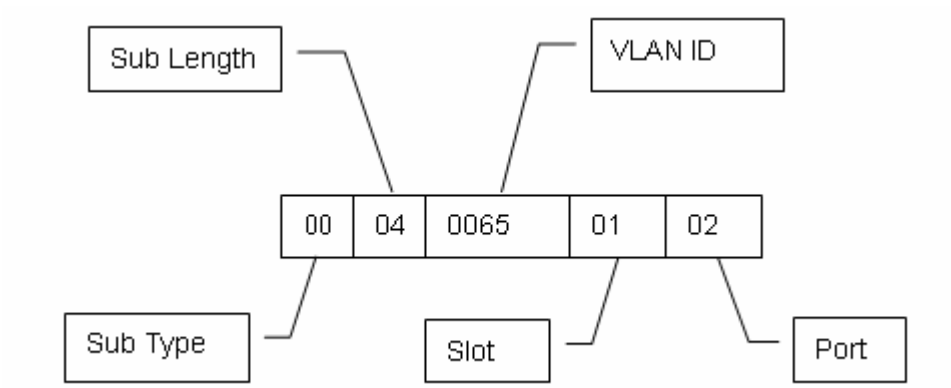
部分网络管理员在对当前的用户进行 IP 管理时，希望能够根据用户所处的位置来确定给用户分配 IP，即希望能够根据用户所连接的网络设备的信息进行用户的 IP 分配，从而交换机在进行 DHCPv6 窥探的同时把一些用户相关的设备信息以 DHCPv6 option 的方式加入到 DHCP 请求报文中，根据 RFC3315，所使用的 option 选项号为 18，根据 RFC4649，所使用的 option 选项号为 37。在 DHCPv6 Server 服务器配置对 option18/37 内容的解析，这个服务器就可以通过 option18/37 上传的内容，获取到更多用户的信息，从而更准确地给用户分配 IP。

- Option18: Interface ID

Interface ID 的默认填充内容是接收到 DHCP 客户端请求报文的端口所属 VLAN 的编号以及端口索引（端口索引的取值为端口所在槽号和端口号），扩展填充内容是自定义的字符串。

Interface ID 填充格式有两种，一种是标准填充格式，一种是扩展填充格式，在同一个网络域中，只能使用其中的一种，不能混合使用。标准填充格式时，Interface ID 子选项只能填充默认的填充内容，如下所示：

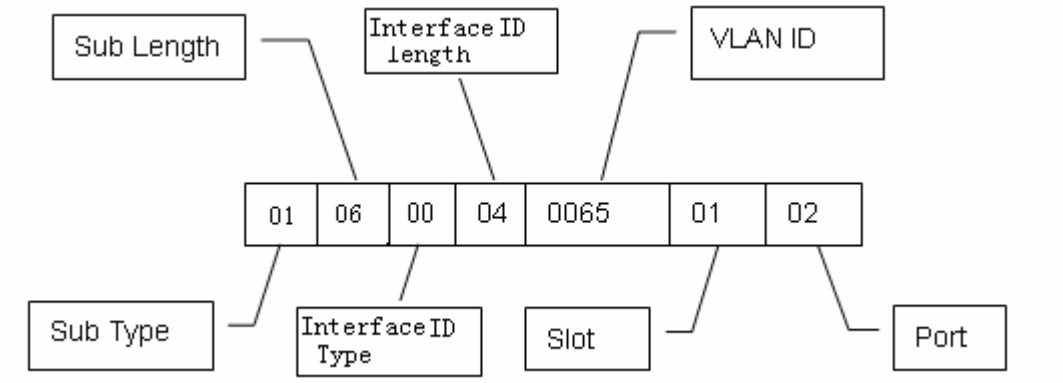
图 16-3



如果需要使用自定义的填充内容，那么可以使用扩展填充格式。扩展填充格式的填充内容可以是默认填充内容，也可以是扩展填充内容。为了区分填充内容的不同，在子选项长度后增加一个字节的内容类型字段和一个字节的内容长度字段，如果是默认填充内容，则设置内容类型为 0；如果是扩展填充内容，则设置内容类型为 1。

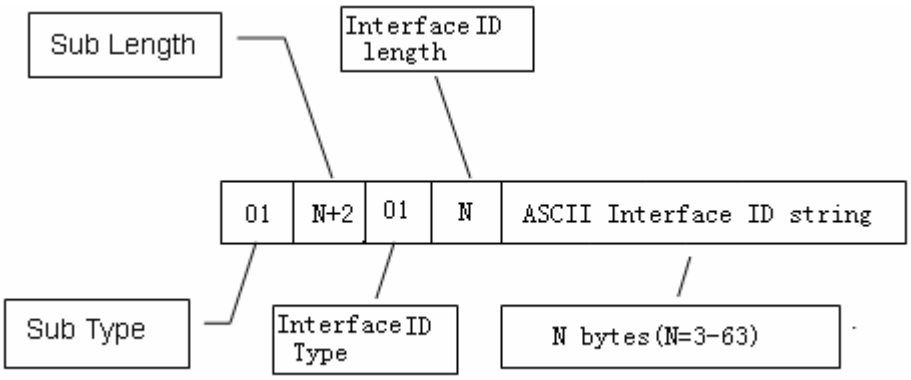
默认填充内容的格式如下：

图 16-4



扩展填充内容的格式如下：

图 16-5

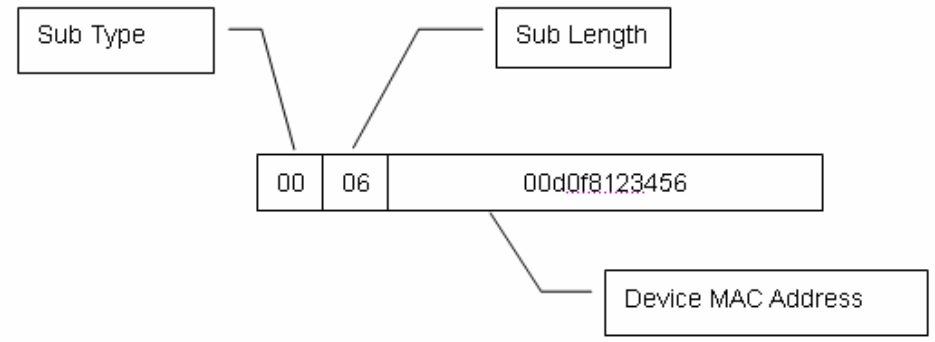


- Option37: Remote ID

Remote ID 的默认填充内容是接收到 DHCP 客户端请求报文的 DHCP 中继设备的桥 MAC 地址。扩展填充内容是自定义的字符串。

Remote ID 填充格式有两种，一种是标准填充格式，一种是扩展填充格式，在同一个网络域中，只能使用其中的一种，不能混合使用。标准填充格式时，Remote ID 子选项只能填充默认的填充内容，如下所示：

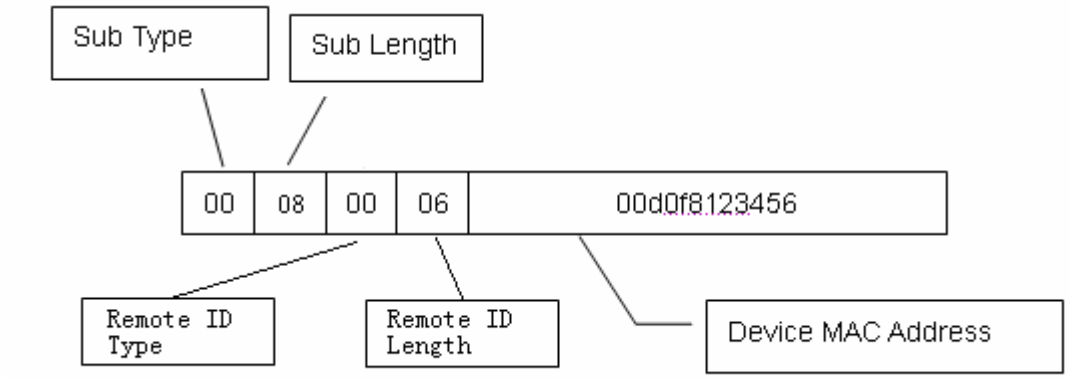
图 16-6



如果需要使用自定义的填充内容，那么可以使用扩展填充格式。扩展填充格式的填充内容可以是默认填充内容，也可以是扩展填充内容。为了区分填充内容的不同，在子选项长度后增加一个字节的内容类型字段和一个字节的内容长度字段，如果是默认填充内容，则设置内容类型为 0；如果是扩展填充内容，则设置内容类型为 1。

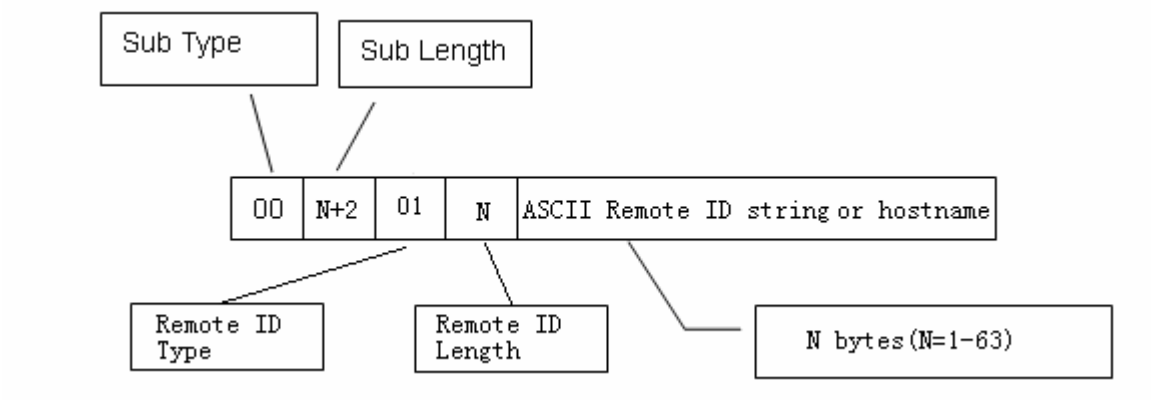
默认填充内容的格式如下：

图 16-7



扩展填充内容的格式如下：

图 16-8



■ 注意

Option18: Interface ID 中端口索引的取值为端口所在槽号和端口号。

其中端口号是指端口在槽上的序号，AP 口（聚合口）的端口号就是 AP 号。例如 Fa0/10，端口号就是 10，AP 11 的端口号就是 11。

其中槽号是设备(堆叠认为是一台设备)上所有槽排序的序号，AP 口的槽号在最后。槽排序的序号从 0 开始，可用 show slots 命令查看。例如：

例 1：

```
Ruijie#show slots  （只列出 Dev、slot 示例）
  Dev Slot
  --- ----
  1   0    ------>槽号为 0
  1   1    ------>槽号为 1
  1   2    ------>槽号为 2
```

此时 AP 口的槽号为 3。

例 2：

```
Ruijie#show slots （只列出 Dev、slot 示例）
  Dev Slot
  --- ----
  1   0    ------>槽号为 0
  1   1    ------>槽号为 1
  1   2    ------>槽号为 2
  2   0    ------>槽号为 3
  2   1    ------>槽号为 4
  2   2    ------>槽号为 5
```

此时 AP 口的槽号为 6。

16.1.4 DHCPv6 Snooping基本概念

TRUST 端口

由于 DHCPv6 客户端发出的请求报文可能是组播形式，所以在同一局域网中存在着的非法 DHCPv6 服务器将影响正常的 DHCPv6 交互过程。为了防止非法服务器，DHCPv6 Snooping 通过将端口划分为两种类型，TRUST 端口和 UNTRUST 端口（缺省情况下所有端口均为 UNTRUST 口）。设备只转发 TRUST 端口收到的 DHCPv6 服务器响应报文，而丢弃所有来自 UNTRUST 端口的 DHCPv6 服务器响应报文。

于是，将连接合法 DHCPv6 服务器的端口配置为 TRUST 端口，其他端口配置为 UNTRUST 端口，就可以实现对非法 DHCPv6 服务器的屏蔽。

DHCPv6 服务器响应报文，按 RFC3315 和 RFC5007 及其他协议规定，有 ADVERTISE、REPLY、RECONFIGURE、RELAY-REPLY、LEASEQUERY-REPLY、 LEASEQUERY-DATA、 LEASEQUERY-DONE 几种，因此将在 UNTRUST 端口上过滤这几类报文。

Ipv6 source guard

Ipv6 source guard，相当于在端口上添加了一条硬件 ACL 表项，默认过滤该端口上除 DHCPv6 报文外的其它所有用户发送的 IPV6 报文。当用户通过 DHCPv6 交互申请 IPV6 地址或者管理员手工添加静态绑定表项后，会在该端口上添加一条硬件过滤表项，允许该用户使用该地址进行 IPV6 的通讯，其他用户依然禁止通讯。

> 打开 **ipv6 source guard** 开关后，所有 IPv6 报文将缺省不能转发，如果用户需要让链路本地地址能正常通讯，则请配置上“安全通道”，关联上相应 ACL。具体请参见《配置 ACL》。

16.2 协议规范

相关的协议规范有：

- RFC3315 Dynamic Host Configuration Protocol For Ipv6
- RFC5007 DHCPv6 Leasequery

16.3 配置DHCPv6 Snooping基本特性

以下章节描述如何配置 DHCPv6 Snooping 的基本特性：

- DHCPv6 Snooping 的缺省配置
- （必选）全局开启/关闭 DHCPv6 Snooping
- （可选）基于 VLAN 开启/关闭 DHCPv6 Snooping
- （可选）配置定时将绑定数据库信息写入 FLASH 文件
- （可选）配置实时将绑定数据库信息写入 FLASH 文件
- （可选）配置手工添加静态绑定表项

- （必选）配置端口 TRUST 属性
- （可选）配置端口 DHCPv6 请求报文过滤
- （可选）配置 ipv6 source guard 开关
- （可选）配置忽略目的端口查找失败的开关
- （可选）配置端口 DOWN 时，清除动态绑定表项的开关
- （可选）配置将绑定表项延迟添加到硬件过滤表中

16.3.1 DHCPv6 Snooping的缺省配置

下表用来描述 DHCPv6 Snooping 的缺省配置。

功能特性	缺省值
全局开关	关闭
基于 VLAN 的开关	开启（全局开关打开后，dhcpv6 snp 作用在所有 vlan 上）
定时将绑定数据库信息写 FLASH 文件	关闭
手工添加静态绑定表项	不存在静态绑定表项
端口 TRUST 属性	UNTRUST
端口 DHCPv6 报文速率限制	未限制
端口 DHCPv6 请求报文过滤	关闭
端口地址绑定开关	关闭
目的端口查找失败的开关	关闭
端口 DOWN 时，清除动态绑定表项的开关	关闭
动态绑定表项延迟添加到硬件过滤表	关闭

16.3.2 全局开启/关闭DHCPv6 Snooping

缺省情况下，设备关闭 DHCPv6 Snooping 功能，进入特权模式，按以下步骤开启 DHCPv6 Snooping 功能：

命令	作用
Ruijie**# configure terminal**	进入全局配置模式
Ruijie(config)**# ipv6 dhcp snooping**	开启 DHCPv6 Snooping 功能

如果要恢复默认值，可以在全局配置模式下执行 **no ipv6 dhcp snooping** 命令。

- 配置举例：

全局开启 DHCPv6 Snooping 功能，并查看相应功能的配置情况。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# ipv6 dhcp snooping
Ruijie(config)# show ipv6 dhcp snooping
Switch DHCPv6 Snooping status : ENABLE
```

```
DHCPv6 Snooping vlan: 1-4094
DHCPv6 Snooping database write-delay time: 0 seconds
DHCPv6 ignore dest-not-found :DISABLE
DHCPv6 Snooping link detection: DISABLE
Interface                Trusted    Filter DHCP
-----------------------  -------    ----------
FastEthernet0/10           yes        DISABLE
```

16.3.3 基于VLAN开启/关闭DHCPv6 Snooping

在全局打开 DHCPv6 默认情况下，所有 VLAN 均开启 DHCPv6 Snooping 功能，可根据用户需要关闭某些 VLAN 的 DHCPv6 Snooping 功能。

进入特权模式，按以下步骤配置基于 VLAN 的 DHCPv6 Snooping 功能：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **ipv6 dhcp snooping vlan** {*vlan-list* | {*vlan-min* [*vlan-max*]}}	基于 VLAN 配置 DHCPv6 Snooping 的开启状态

如果要恢复默认值，可以在全局配置模式下执行 **default ipv6 dhcp snooping vlan** {*vlan-list* | {*vlan-min* [*vlan-max*]}}命令。

如果要禁止 DHCPv6 Snooping 生效在某些 VLAN 上，可以在全局配置模式下执行 **no ipv6 dhcp snooping vlan** {*vlan-list* | {*vlan-min* [*vlan-max*]}}命令。

配置举例：

配置在 VLAN 1,3,4,5,7,9,10,11 上开启 DHCPv6 Snooping 功能。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# ipv6 dhcp snooping vlan 1,3-5,7,9-11
```

创建新的 VLAN 后，在此 VLAN 上默认开启 DHCPv6 Snooping。如果不需要开启，则需要手动在此 VLAN 上关闭 DHCPv6 Snooping。

16.3.4 配置定时将绑定数据库信息写入FLASH文件

将绑定数据库信息写入 FLASH 文件，设备重启后，FLASH 中的数据会导回绑定数据库，这样就可以防止设备意外重启后，原来已经绑定的用户无法正常通讯。默认情况下，DHCPv6 Snooping 绑定数据库不会定时写入 FLASH 文件。

进入特权模式，按以下步骤配置定时将绑定数据库信息写入 FLASH 文件功能：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **ipv6 dhcp snooping database write-delay** *seconds*	配置定时将绑定数据库信息写入 FLASH 的间隔时间(单位：秒)

如果要恢复默认值，可以在全局配置模式下执行 **no ipv6 dhcp snooping database write-delay** 命令。

■ 配置举例：

配置每 10 分钟(600 秒)，将绑定数据库写入 FLASH 文件一次。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# ipv6 dhcp snooping database write-delay 600
```

16.3.5 配置实时将绑定数据库信息写入FLASH文件

管理在重启设备前，可以手动将绑定数据库信息实时写入 FLASH 文件，可以防止设备意外重启后，原来已经绑定的用户无法正常通讯。

进入特权模式，按以下步骤配置实时将绑定数据库信息写入 FLASH 文件功能：

命令	作用
Ruijie**# configure terminal**	进入全局配置模式。
Ruijie(config)**# ipv6 dhcp snooping database write-to-flash**	配置实时将绑定数据库信息写入 FLASH 文件

配置举例：

配置实时将绑定数据库信息写入 FLASH 文件。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# ipv6 dhcp snooping database write-to-flash
```

16.3.6 手动把flash中的信息导入DHCPv6 Snooping数据库

在开启 DHCPv6 Snooping 功能时，可以根据需要手动地把当前 flash 中的信息导入 DHCPv6 Snooping 绑定数据库。

命令	作用
Ruijie**# renew ipv6 dhcp snooping database**	把 flash 中信息导入 DHCPv6 Snooping 数据库。

下边的是手动的把 flash 中信息导入 DHCPv6 Snooping 数据库：

```
Ruijie# renew ipv6 dhcp snooping database
```

16.3.7 配置手工添加静态绑定表项

对于需要使用静态 IPV6 地址，而不通过 DHCPv6 交互获取 IPV6 地址的用户，管理员可以通过手工添加静态绑定表项，使该用户在端口打开 ipv6 source guard 开关后，可以正常通讯。

进入特权模式，按以下步骤添加静态绑定表项：

命令	作用
Ruijie**# configure terminal**	进入全局配置模式。

Ruijie(config)# **ipv6 source binding** *mac-address* **vlan** *vlan-id ipv6-address* [**interface** *interface-id* **| ip-mac | ip-only**]	添加静态绑定表项，使用户可以使用静态 IPV6 地址，而不再需要通过 DHCPv6 交互获取 IPV6 地址。当没有接口选项时，绑定表项在 VLAN 内的所有绑定端口上生效。 **interface**：绑定到接口； **ip-mac**：全局绑定为 IP+MAC 绑定； **ip-only**：全局绑定为仅 IP 绑定。

要删除静态绑定表项，可以在全局配置模式下执行 **no ipv6 source binding** *mac-address* **vlan** *vlan-id ipv6-address* **interface** *interface-name* 命令。

配置举例：

添加一个静态绑定用户

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# ipv6 source binding 00d0.f866.4777 vlan 10 2001:2002::2003 interface fastethernet 0/10
Ruijie(config)# end
Ruijie# show ipv6 source binding
Total number of bindings: 1

Mac Address      Ipv6 Address     Lease(s)   type    Vlan   Interface
--------------  --------------   --------   ----   -----  ---------
00d0.f866.4777   2001:2002::2003   57       static   10     fa 0/10
```

16.3.8 配置端口TRUST属性

默认情况下，所有端口均为 UNTRUST 端口。开启 DHCPv6 Snooping 功能的设备，仅将 DHCPv6 请求报文转发到 VLAN 内的所有 TRUST 端口上。

进入特权模式，按以下步骤配置端口 TRUST 属性：

命令	作用
Ruijie**# configure terminal**	进入全局配置模式。
Ruijie(config)# **interface** *interface-name*	进入端口配置模式。
Ruijie(config-if)**# ipv6 dhcp snooping trust**	配置端口属性为 TRUST。

如果要恢复默认值，可以端口配置模式下执行 **no ipv6 dhcp snooping trust** 命令。

配置举例：

配置端口 interface fastethernet 0/10 为 TRUST 端口

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# interface fastethernet 0/10
Ruijie(config-if)# ipv6 dhcp snooping trust
Ruijie(config-if)# end
Ruijie# show ipv6 dhcp snooping
```

```
Switch DHCPv6 Snooping status : ENABLE
DHCPv6 Snooping vlan: 1-4094
DHCPv6 Snooping database write-delay time: 300 seconds
DHCPv6 ignore dest-not-found :DISABLE
DHCPv6 Snooping link detection :DISABLE
Interface                Trusted    Filter DHCP
-----------------------  -------    ---------
FastEthernet0/10           yes       DISABLE
```

锐捷设备全局开启 DHCPv6 Snooping 功能，并在对指定 VLAN 上开启 DHCPv6 Snooping 功能后，如果希望指定 VLAN 内的用户能够正常完成 DHCPv6 交互，必须在 VLAN 内配置连接 DHCPv6 服务器方向的端口为 TRUST 端口。

16.3.9 配置端口DHCPv6 请求报文过滤

如果管理员需要限制某一端口下的用户，不允许进行 DHCPv6 报文交互。可以在端口上配置 DHCPv6 请求报文过滤功能。

进入特权模式，按以下步骤配置端口 DHCPv6 请求报文过滤功能：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **interface** *interface-name*	进入端口的配置模式。
Ruijie(config-if)# **ipv6 dhcp snooping filter-dhcp-pkt**	配置端口 DHCPv6 请求报文过滤功能，该端口接收到的 DHCPv6 请求报文将全部被丢弃。

如果要恢复默认值，可以在端口配置模式下执行 **no ipv6 dhcp snooping filter-dhcp-pkt** 命令。

- 配置举例：

配置端口 FastEthernet 0/1 过滤所有 DHCPv6 请求报文。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# interface fastEthernet 0/10
Ruijie(config-if)# ipv6 dhcp snooping filter-dhcp-pkt
Ruijie# show ipv6 dhcp snooping
Switch DHCPv6 Snooping status : ENABLE
DHCPv6 Snooping vlan: 1-4094
DHCPv6 Snooping database write-delay time: 0 seconds
DHCPv6 ignore dest-not-found :DISABLE
DHCPv6 Snooping link detection :DISABLE
Interface                Trusted    Filter DHCP
-----------------------  -------    ---------
FastEthernet0/10           YES        ENABLE
```

16.3.10 配置ipv6 source guard开关

端口上打开 ipv6 source guard 开关后，默认会过滤该端口上 IN 方向所有的 IPv6 报文（除了 DHCPv6 报文）。如果网络中有可能存在 IPv6 地址冲突，需要通过 ND 协议报文发现 IPv6 地址冲突，因此需要在端口上放过 ND 协议报文。配置安全通道或开启 ND Snooping 功能，使 ND 协议报文可以通过，以完成地址冲突检测过程，具体配置请参考相关功能的配置章节。用户通过 DHCPv6 交互申请到 IPV6 地址后，DHCPv6 Snooping 会将相应的用户绑定信息添加到硬件过滤表中，则该用户的 IPv6 报文可以正常转发。默认情况下，端口 ipv6 source guard 开关关闭，端口上的所有 IPv6 报文正常转发。

进入特权模式，按以下步骤配置端口地址绑定功能：

命令	作用
Ruijie**# configure terminal**	进入全局配置模式。
Ruijie(config)**# interface** *interface-name*	进入端口配置模式。
Ruijie(config-if)**# ipv6 verify source** [**port-security**]	配置端口地址绑定开关。port-security 选项表示进行 IPv6+MAC+端口绑定，无该选项则表示 IPv6+端口绑定。

如果要恢复默认值，可以在端口配置模式下执行 **no ipv6 verify source** 命令。

- 配置举例：

配置端口 interface fastethernet 0/10 打开地址绑定开关。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# interface fastethernet 0/10
Ruijie(config-if)# ipv6 verify source port-security
Ruijie(config-if)# end
```

16.3.11 配置忽略目的端口查找失败的开关

DHCPv6 的响应报文转发，需要依赖 MAC 地址表的搜索，如果 DHCPv6 的响应报文在交换机上查找不到 MAC 地址对应的端口，为了安全考虑，将不转发相关报文。

但在极个别的网络环境中，可能因网络拥塞、网络拓扑振荡、设备堆叠过多等原因，MAC 地址学习发生延迟或丢失，有可能发生上述事情，这时在设备上会打印出系统日志“DHCPV6_Snooping-5-DEST_NOT_FOUND: Could not find destination port. Destination MAC [mac-address]”，一般情况下可这时，为了能让整网的 DHCPv6 能正常工作，可以打开如下开关，这时查找不到 MAC 地址对应端口的报文将以广播形式发送到相关 VLAN 的所有端口，或者直接转发到记录在 DHCPv6 Snooping 数据库里的 DHCP 请求的源端口上。

进入特权模式，按以下步骤配置端口地址绑定功能：

命令	作用
Ruijie**# configure terminal**	进入全局配置模式。
Ruijie(config)**# ipv6 dhcp snooping ignore dest-not-found**	配置忽略目的端口查找失败的开关。

如果要恢复默认值，可以在全局配置模式下执行 no ipv6 dhcp snooping ignore dest-not-found 命令。

- 配置举例：

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# ipv6 dhcp snooping ignore dest-not-found
Ruijie(config)# end
```

16.3.12 配置端口LINK DOWN时，清除动态绑定表项的开关

端口 LINK DOWN 时，该端口下的用户不能与外界正常通信，但是用户动态绑定表项依然存在，等待租约的超时后才删除表项。不根据端口 LINK DOWN 直接清除绑定表项的这种做法主要是为了防止临时的链路 LINK 抖动而导致整体表项失效，因此我们缺省不启用这个功能。

但有时在稳定的网络连接里，为了节约硬件表项的占用，期望能及时的清除 LINKDOWN 端口的表项，我们提供了这个开关以供管理员配置选择。在此要特别注意相应的网络连接稳定性，不要经常出现网线连接抖动的情况。

进入特权模式，按以下步骤配置端口 LINK DOWN 时，清除该端口下动态绑定表项的功能：

命令	作用
Ruijie**# configure terminal**	进入全局配置模式。
Ruijie(config)**# ipv6 dhcp snooping link-detection**	配置端口 LINK DOWN 时，清除动态绑定表项的功能。

如果要恢复默认值，可以在全局配置模式下执行 **no ipv6 dhcp snooping link-detection** 命令。

- 配置举例：

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# ipv6 dhcp snooping link-detection
Ruijie(config)# end
```

16.3.13 配置将动态绑定表项延迟添加到硬件过滤表中

缺省情况下，将动态生成绑定表项实时添加到硬件过滤表中。如果 DHCPv6 客户端检测到 IPv6 地址存在冲突，则回应 DHCPv6 DECLINE 报文，DHCPv6 Snooping 根据 DHCPv6 DECLINE 报文删除之前生成的动态绑定表项。配置延迟绑定功能后，只有在指定时间内没有检测到 IPv6 地址冲突时，才会将动态生成的绑定表项添加到硬件过滤表中。在 IPv6 地址冲突较少的环境中，如果配置延迟绑定功能，客户端分配到 IPv6 地址后，在指定延迟时间内，仍无法访问网络，因此缺省情况下，我们实时将动态绑定表项添加到硬件过滤表中。

在 IPv6 地址冲突较多的环境中，为了防止反复操作硬件过滤表占用大量的系统资源，可以配置延迟绑定功能，在指定的延迟时间内没有检测到 IPv6 地址冲突后，才将动态绑定表项添加到硬件过滤表中。

进入特权模式，按以下步骤配置将动态绑定表项延迟添加到硬件过滤表中的功能：

命令	作用
Ruijie**# configure terminal**	进入全局配置模式。
Ruijie(config)**# ipv6 dhcp snooping binding-delay** *seconds*	配置将动态绑定表项延迟添加到硬件过滤表中的功能。(单位：秒)缺省是没有延时绑定的。

如果要恢复默认值，可以在全局配置模式下执行 **no ipv6 dhcp snooping binding-delay** 命令。

配置举例：

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# ipv6 dhcp snooping binding-delay 10
Ruijie(config)# end
```

16.3.14 配置DHCPv6 Snooping information option

通过配置如下命令，在进行 DHCPv6 窥探转发时，给每个 DHCPv6 请求添加 option18/37 选项。缺省情况下该功能是关闭的。

命令	作用
Ruijie**# configure terminal**	进入配置模式
Ruijie(config)**# [no] ipv6 dhcp snooping Information option [standard-format]**	打开 option18/37 功能； standard-format：有此关键字时，填充的格式为标准格式，否则为扩展格式。
Ruijie(config)**# [no] ipv6 dhcp snooping information option format remote-id [string** *ASCII-string* **| hostname]**	在扩展格式下配置 remote-id。 string：填充内容为自定义字符串； hostname：填充内容为主机名。
Ruijie(config)**# interface** *interface*	进入接口配置模式
Ruijie(config-if)**# [no] ipv6 dhcp snooping vlan** *vlan-id* **information option format-type** *interface-id* **string** *ASCII-string*	在扩展格式下配置 interface-id 的自定义字符串。
Ruijie(config-if)**# [no] ipv6 dhcp snooping vlan** *vlan-id* **information option change-vlan-to vlan** *vlan-id*	在扩展格式下配置 interface-id 的 vlan 映射，和 **[no] ipv6 dhcp snooping vlan** *vlan-id* **information option format-type** *interface-id* **string** *ASCII-string* 命令互斥。

下边是配置打开 DHCPv6 information option 功能：

```
Ruijie# configure terminal
Ruijie(config)# ipv6 dhcp snooping information option
Ruijie(config)# end
```

16.4 显示或清除DHCPv6 Snooping配置和状态

DHCPv6 Snooping 提供了如下的显示命令用于查看各种配置信息及运行时信息，各命令的功能说明如下：

命令	作用
show ipv6 dhcp snooping	显示 DHCPv6 Snooping 的配置情况
show ipv6 dhcp snooping statistics	显示 DHCPv6 Snooping 对报文处理的统计信息
show ipv6 dhcp snooping binding	显示 DHCPv6 Snooping 绑定数据库的所有动态绑定表项
show ipv6 dhcp snooping prefix	显示 DHCPv6 Snooping 前缀数据库的所有表项
show ipv6 source binding	显示手工添加的所有静态绑定表项和 DHCPv6 Snooping 绑定数据库中所有的动态绑定表项

clear ipv6 dhcp snooping statistics	清除 DHCPv6 Snooping 处理 DHCPv6 报文的统计信息
clear ipv6 dhcp snooping binding [**vlan** *vlan-id* | *mac* | *ip* | **interface** *interface-id*]	清除 DHCPv6 Snooping 绑定数据库的绑定表项，可基于 VLAN、MAC、IP、接口删除，并可组合使用。
clear ipv6 dhcp snooping prefix	清除 DHCPv6 Snooping 前缀数据库的所有表项

17 防网关 ARP 欺骗

17.1 概述

在交换机上，默认情况下 ARP 报文是在本 VLAN 内广播的，因此这就为针对网关的 ARP 欺骗提供了机会。

针对网关的 ARP 欺骗是指用户 A 发送 ARP 报文请求网关的 MAC 地址，这时处于同一 VLAN 的用户 B 也会收到该 ARP 报文，因此用户 B 可以发送 ARP 响应报文，将报文的源 IP 填为网关 IP，而源 MAC 填为自己的 MAC 地址。用户 A 收到该 ARP 响应后，就会认为用户 B 的机器就是网关，因此用户 A 通讯中发往网关的报文都将发往用户 B， 这样用户 A 的通讯实际上都被截取了，造成 ARP 欺骗的效果。

因此我们可以在交换机的逻辑端口(包括物理端口与及 AP 口)上配置防网关 ARP 欺骗来防止针对网关的 ARP 欺骗。防网关 ARP 欺骗配置后，可以在逻辑端口上检查 ARP 报文的源 IP 是否是我们配置的网关 IP，如果是，则将该报文丢弃，防止用户收到错误的 ARP 响应报文。 这样只有交换机上连设备能够下发网关的 ARP 报文，其它 PC 发送的假冒网关 ARP 响应报文将被交换机过滤。

17.2 配置防网关ARP欺骗

17.2.1 设置防网关ARP欺骗

设置防网关 ARP 欺骗地址。

命令	作用
Ruijie(config-if)# **anti-arp-spoofing ip** *ip-address*	在逻辑端口下配置防网关 ARP 欺骗，网关 IP 地址为指定 IP。

你可以在端口配置模式下通过命令 **no anti-arp-spoofing ip** *ip-address* 来将防网关 ARP 配置清除。

在上链口上不能配置防网关 ARP 欺骗。

17.2.2 查看防网关ARP欺骗信息

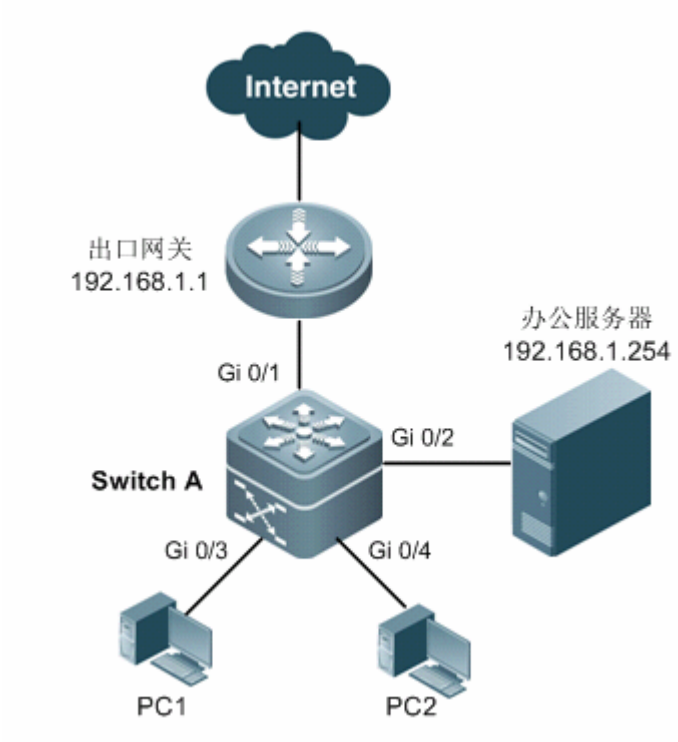
查看交换机的防网关 ARP 欺骗信息。

命令	作用
show anti-arp-spoofing	显示所有接口下的防网关 arp 欺骗信息

17.3 配置举例

拓扑图

图 17-1 防网关 ARP 欺骗典型拓扑



应用需求

上图为中小型公司或单位的简化典型网络拓扑，PC 用户通过接入设备 Switch A 访问办公服务器，以及通过网关设备连接外网。如果存在非法用户冒充网关 IP 地址或服务器 IP 地址进行 ARP 欺骗，将导致其它用户无法正常上网以及访问服务器。

基于以上应用分析，组网需求如下：

- 阻断伪造网关和内网服务器 ARP 欺骗报文，保证用户能正常上网

配置要点

在接入交换机（本例为 Switch A）直连 PC 的端口(本例为 Gi 0/3, Gi 0/4)上启用防网关欺骗，网关地址为内网网关地址和内网服务器地址。

上链口、连接出口网关或服务器的端口不能启用防网关欺骗，否则将导致源地址为网关 IP 或服务器 IP 的 ARP 报文被阻断，造成网络不通

如果端口不够，需在接入交换机下挂一台 8 口的 hub（集线器），也可在接入交换机上开启防网关欺骗，缺陷是同一台 hub 上的电脑之间的网关 ARP 欺骗无法阻断。

配置步骤

第一步，在直连电脑的端口上启用防网关欺骗

```
SwitchA# configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)#interface range gigabitEthernet 0/2-4
SwitchA(config-if-range)# anti-arp-spoofing ip 192.168.1.1
SwitchA(config-if-range)# anti-arp-spoofing ip 192.168.1.254
```

配置验证

第一步，确认配置是否正确，关注点：是否启用防网关欺骗、网关地址是否正确、上链口是否启用防网关欺骗

```
SwitchA (config-if)#show running-config
interface GigabitEthernet 0/1
!
interface GigabitEthernet 0/2
 anti-arp-spoofing ip 192.168.1.1
 anti-arp-spoofing ip 192.168.1.254
!
interface GigabitEthernet 0/3
 anti-arp-spoofing ip 192.168.1.1
 anti-arp-spoofing ip 192.168.1.254
!
interface GigabitEthernet 0/4
 anti-arp-spoofing ip 192.168.1.1
 anti-arp-spoofing ip 192.168.1.254
!
```

第二步，查看防网关欺骗状态，再次确认。关注点同第一步

```
SwitchA#show anti-arp-spoofing
Anti-arp-spoofing
port           ip
-------        -------
Gi 0/2         192.168.1.1
Gi 0/2         192.168.1.254
Gi 0/3         192.168.1.1
Gi 0/3         192.168.1.254
Gi 0/4         192.168.1.1
Gi 0/4         192.168.1.254
```

第三步，如果可能，将 PC1 的 IP 地址配置为网关的 IP 地址，然后观察网关是否报告 IP 地址冲突，PC2 是否能正常上网。

如果一切正常，说明防网关欺骗配置生效。

18 NFPP

18.1 概述

网络基础保护策略 (Network Foundation Protection Policy)，简称 NFPP。

18.1.1 NFPP的作用

在网络环境中经常发现一些恶意的攻击，这些攻击会给交换机带来过重的负担，引起交换机 CPU 利用率过高，导致交换机无法正常运行。这些攻击具体表现在：

拒绝服务攻击可能导致大量消耗交换机内存、表项或者其它资源，使系统无法继续服务。

大量的报文流砸向 CPU，占用了整个送 CPU 的报文的带宽，导致正常的协议流和管理流无法被 CPU 处理, 带来协议震荡或者无法管理，从而导致数据面的转发受影响，并引起整个网络无法正常运行。

大量的报文砸向 CPU 会消耗大量的 CPU 资源，使 CPU 一直处于高负载状态，从而影响管理员对设备进行管理或者设备自身无法运行。

NFPP 可以有效地防止系统受这些攻击的影响。在受攻击情况下，保护系统各种服务的正常运行，以及保持较低的 CPU 负载，从而保障了整个网络的稳定运行。

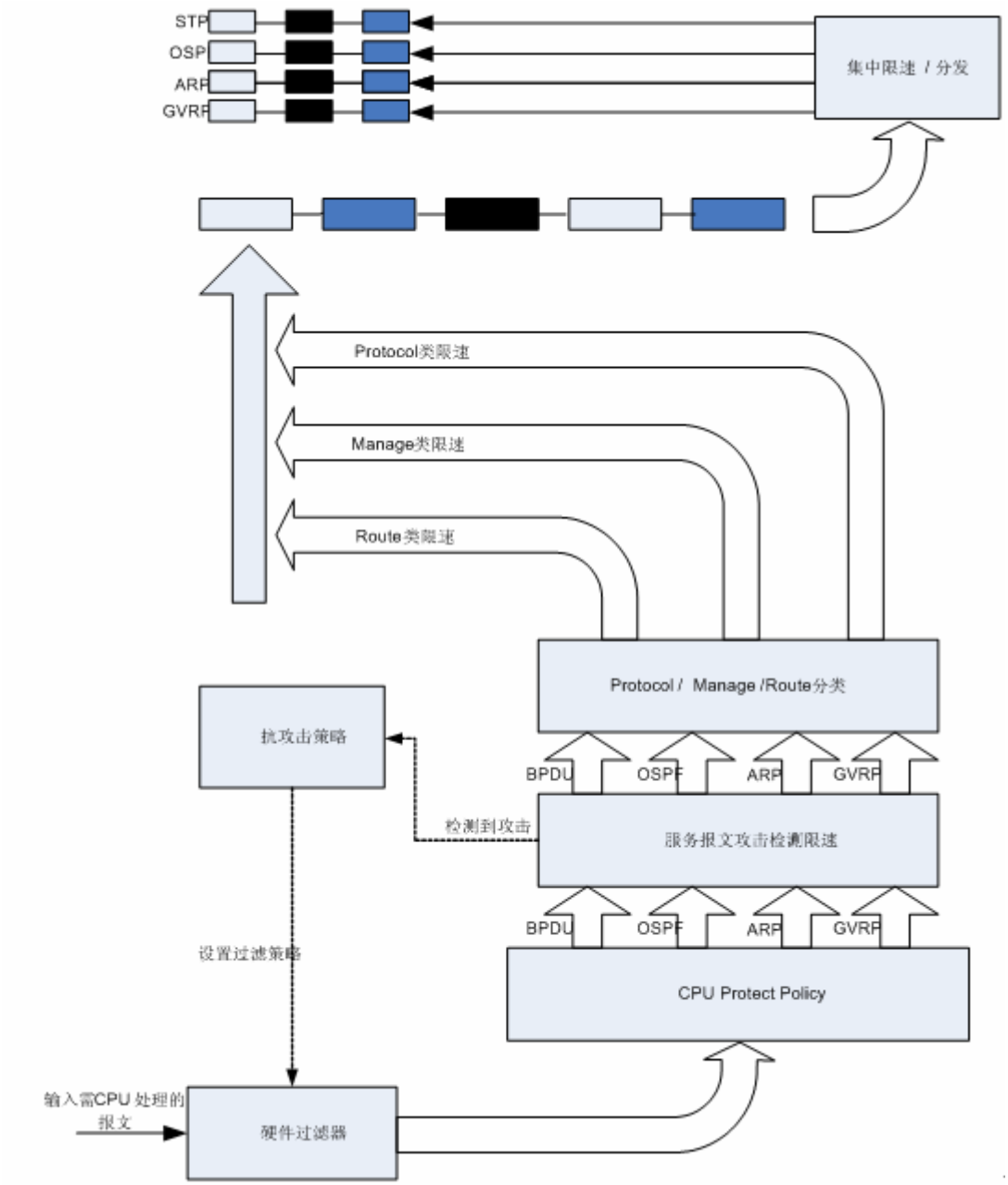
18.1.2 NFPP的原理

如下图所描述的，NFPP 系统处理数据流时，需要经过硬件过滤、CPU Protect Policy（简称 CPP）、报文攻击检测/限速、Protocol/Manage/route 流分类和集中限速等几个流程，并最终交给各个应用模块处理。

首先，需要进行 CPP 的分类和限速，这样 CPU 处理的数据流不仅根据 CPP 的服务分类原则进行了分类，而且这些服务报文还经过了硬件和软件的限速，从而避免了不同的服务报文之间相互抢占带宽，有效地解决了某一种服务报文的大流量攻击情况下，其他服务报文无法及时得到处理的问题。例如设备中同时存在 OSPF 服务报文和 BPDU 服务报文时，当其中某一个服务报文需要消耗大量 CPU 带宽的情况下，可以保证另一个服务报文的接收不受影响。

为了最大限度地利用 NFPP 中抗攻击功能，请根据具体的应用环境修改 CPU Protect Policy 中各种服务的限速值，也可以使用系统提供的推荐配置，这些推荐值可以通过命令 **show cpu-protect summary** 查看。

图 18-1 NFPP 系统的数据流向图



然后，针对报文所属的服务类型，对具体的报文服务类型实施不同的监控方式和策略，NFPP 提供各种服务监控水线和策略的配置，管理员可以根据具体的网络环境灵活配置某一个服务报文的告警水线和限速水线，这些水线的设置可以基于端口，也可以基于网络中的主机，这里的告警水线是指当端口或者某台主机的某种服务报文接收速率达到需要向管理员发出警告或者进行隔离的阈值；限速水线是指当端口或者某台主机的某种服务报文接收速率达到需要进行限速的阈值。告警或者隔离动作是在检测到攻击后交由抗攻击策略执行的。如果是隔离，抗攻击策略会利用硬件的过滤器实现，这样保证该攻击报文不会再被送到 CPU 处理，从而保证了设备正常运行。

- NFPP 在检测到某种服务的某个具体报文的攻击后，可以向管理员发出告警信息，但是为了防止告警信息频繁出现，如果攻击流持续存在，NFPP 在发出告警后的连续 60 秒时间内不再重复告警。
- 防止频繁打印日志消耗 CPU 资源，NFPP 把攻击检测的日志信息写到缓冲区，然后以指定速率从缓冲区取出来打印。NFPP 对 TRAP 没有限速。

监控后的服务报文再经过 Protocol/Manage/Route 流分类，这里的分类是指将 CPP 中定义的各种服务按照管理类(Manage) 、转发类(Route)和协议类(Protocol)的原则进行的分类（具体分类如表 1 所列），每一类都拥有独立的带宽，不同类别之间的带宽不能共享，超过带宽阈值的流将被丢弃。这样将不同的服务区分类别后，可以保证属于某类的各种服务报文在设备上得到优先处理。NFPP 允许管理员根据实际的网络环境灵活分配三类报文的带宽，从而保障 protocol 类和 manage 类能得到优先处理，protocol 类的优先处理保证了协议的正确运行，而 manage 类的优先处理保证了管理员能够实施正常管理，从而保障了设备的各种重要功能的正常运行，提高设备的抗攻击能力。

三种属性分类	CPU Protect Policy 中定义服务类型 （服务类型具体含义参见 CPU Protect Policy 配置指南）
Protocol	tp-guard，dot1x，rldp，rerp，slow-packet，bpdu，isis dhcps，gvrp，ripng，dvmrp，igmp，mpls，ospf, pim，pimv6，rip，vrrp，ospf3，dhcp-relay-s，dhcp-relay-c，option82，tunnel-bpdu，tunnel-gvrp
Route	unknown-ipmc，unknown-ipmcv6，ttl1，ttl0, udp-helper，ip4-packet-other，ip6-packet-other，non-ip-packet-other，arp
Manage	ip4-packet-local，ip6-packet-local

经过以上的分类限速后，再将所有的分类流集中一个队列中，这样当某一类服务处理效率较低时，队列上就会堆积该服务对应的报文，并可能最终耗尽该队列资源，NFPP 允许管理员配置该队列中三类所占百分比，当某一类占用的队列长度超过总队列长度和该类所占百分比的乘积时，报文就会被丢弃。这样就有效地解决了某一类独占队列资源的问题。

18.2 配置NFPP

18.2.1 NFPP的默认值

- 管理类(Manage)的缺省流量带宽 3000PPS，占用缓冲区百分比为 30；
- 转发类(Route) 的缺省流量带宽 3000PPS，占用缓冲区百分比为 25；
- 协议类(Protocol) 的缺省流量带宽 3000PPS，占用缓冲区百分比为 45。

18.2.2 配置每类报文允许的最大带宽

在配置模式下，按如下步骤设置每类报文的流量带宽：

命令	作用
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#cpu-protect sub-interface { manage | protocol|route} pps** *pps_vaule*	设置报文对应的队列的限速水线，*pps* 为整数。有效值范围是 1-8192
Ruijie(config)**#end**	退回到特权模式。
Ruijie**#show running-config**	查看全局配置
Ruijie**#copy running-config startup-config**	保存配置。

18.2.3 配置每类报文占用队列的最大百分比

在配置模式下，按如下步骤设置每种类型报文占用队列的百分比：

命令	作用
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#cpu-protect sub-interface { manage | protocol | route} percent** *percent_vaule*	设置报文对应的类型所占的队列的百分比，*percent _vaule* 为整数。有效值范围是 1-100
Ruijie(config)**#end**	退回到特权模式。
Ruijie**#show running-config**	查看全局配置
Ruijie**#copy running-config startup-config**	保存配置。

配置某类型所占百分比的有效值区间，必须小于等于百分之百减去其它两种类型百分比之和的差值。

18.3 ARP抗攻击

18.3.1 ARP抗攻击简介

在局域网中，通过 ARP 协议把 IP 地址转换为 MAC 地址。ARP 协议对网络安全具有重要的意义。通过网络向网关发送大量非法的 ARP 报文，造成网关不能为正常主机提供服务，这就是基于 ARP 的拒绝服务攻击。对于这种攻击，防范措施是一方面对 ARP 报文限速，另一方面检测出攻击源，对攻击源头采取隔离措施。

ARP 攻击识别分为基于主机和基于物理端口两个类别。基于主机又细分为基于源 IP 地址/VLAN ID/物理端口和基于链路层源 MAC 地址/ VLAN ID /物理端口。每种攻击识别都有限速水线和告警水线。当 ARP 报文速率超过限速水线时，超限报文将被丢弃。当 ARP 报文速率超过告警水线时，将打印警告信息，发送 TRAP，基于主机的攻击识别还会对攻击源头采取隔离措施。

ARP 抗攻击还能检测出 ARP 扫描。ARP 扫描是指链路层源 MAC 地址固定而源 IP 地址变化，或者链路层源 MAC 地址和源 IP 地址固定而目标 IP 地址不断变化。由于存在误判的可能，对检测出有 ARP 扫描嫌疑的主机不进行隔离，只是提供给管理员参考。

需要说明的是，ARP 抗攻击只是针对攻击交换机本身的 ARP 拒绝服务服务攻击，而不是针对 ARP 欺骗或者是解决网络中的 ARP 攻击问题。

18.3.2 打开ARP抗攻击功能

您可以在 **nfpp** 配置模式或者接口配置模式下打开 ARP 抗攻击功能，缺省情况下是打开的。

命令	作用
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#nfpp**	进入 NFPP 配置模式。
Ruijie(config-nfpp)**#arp-guard enable**	全局打开 ARP 抗攻击功能，缺省情况下打开。
Ruijie(config-nfpp)**#end**	退回到特权模式。
Ruijie**#configure terminal**	进入全局配置模式。

Ruijie(config)**#interface** *interface-name*	进入接口配置模式。
Ruijie(config-if)**#nfpp arp-guard enable**	在端口上打开 ARP 抗攻击功能，缺省情况是端口没有配置局部开关，采用全局开关。
Ruijie(config-if)**#end**	退回到特权模式。
Ruijie**#show nfpp arp-guard summary**	核对配置参数
Ruijie**#copy running-config startup-config**	保存配置。

当关闭 ARP 抗攻击功能时，系统将自动清除受监控的主机和扫描主机。

18.3.3 设置对攻击者的隔离时间

对攻击者的隔离时间分为全局隔离时间和基于端口的隔离时间（即局部隔离时间）。对于某个端口，如果没有配置基于端口的隔离时间，那么采用全局隔离时间；否则，采用基于端口的隔离时间。

命令	作用
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#nfpp**	进入 NFPP 配置模式
Ruijie(config-nfpp)**#arp-guard isolate-period** [*seconds* | **permanent**]	配置对攻击者的全局隔离时间。 取值范围为 0 秒，30 秒到 86400 秒（即一天），缺省值为 0 秒，表示不隔离；**permanent** 表示永久隔离。
Ruijie(config-nfpp)**#end**	返回特权模式
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#interface** *interface-name*	进入接口配置模式。
Ruijie(config-if)**#nfpp arp-guard isolate-period** [*seconds* | **permanent**]	在端口上配置对攻击者的隔离时间。 取值范围为 0 秒，180 秒到 86400 秒（即一天），缺省情况是没有配置局部隔离时间，采用全局隔离时间。0 秒表示不隔离；**permanent** 表示永久隔离。
Ruijie(config-if)**#end**	退回到特权模式。
Ruijie**#show nfpp arp-guard summary**	核对配置参数
Ruijie**#copy running-config startup-config**	保存配置。

如果要把全局隔离时间恢复成缺省值，在 **nfpp** 配置模式执行命令“**no arp-guard isolate-period**”。如果一个端口原来配置了局部隔离时间，现在想采用全局隔离时间，那么在端口配置模式下执行命令“**no nfpp arp-guard isolate-period**”把局部隔离时间配置删除。

18.3.4 设置对攻击者的监控时间

如果隔离时间为 0（即不隔离），防攻击模块将自动根据配置的监控时间对攻击者进行软件监控，提供当前系统中存在哪些攻击者的信息。当把隔离时间配置成非零值后，防攻击模块将自动对软件监控的主机采取硬件隔离。

命令	作用
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#nfpp**	进入 NFPP 配置模式

Ruijie(config-nfpp)**#arp-guard monitor-period** *seconds*	配置对攻击者的监控时间。 取值范围为 180 秒到 86400 秒（即一天），缺省值为 600 秒。
Ruijie(config-nfpp)**#end**	退回到特权模式。
Ruijie**#show nfpp arp-guard summary**	核对配置参数
Ruijie**#copy running-config startup-config**	保存配置。

如果要把监控时间恢复成缺省值，在 nfpp 配置模式执行命令“**no arp-guard monitor-period**”。

检测出攻击者的时候，如果隔离时间为 0，将对攻击者进行软件监控，超时为监控时间。在软件监控过程中，当隔离时间被配置为非零值时，将自动对软件监控的攻击者采取硬件隔离，并且把超时设置为隔离时间。监控时间在隔离时间为 0 的情况下才有意义。

如果把隔离时间从非零值改成零，将直接把相关端口的攻击者删除，而不是进行软件监控。

18.3.5 设置受监控主机的最大数目

命令	作用
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#nfpp**	进入 NFPP 配置模式。
Ruijie(config-nfpp)**#arp-guard monitored-host-limit** *number*	配置受监控主机的最大数目。 取值范围为 1 到 4294967295，缺省情况下受监控主机的最大数目为 1000 个。
Ruijie(config-nfpp)**#end**	退回到特权模式。
Ruijie**#show nfpp arp-guard summary**	核对配置参数
Ruijie**#copy running-config startup-config**	保存配置。

如果要把配置的受监控主机数恢复成缺省值，在 nfpp 配置模式执行命令“**no arp-guard monitored-host-limit**”。

如果受监控主机数已经达到默认的 1000 个，此时管理员把受监控主机的最大数目设置成小于 1000，不会删除已有的受监控主机，而是打印信息“%ERROR： The value that you configured is smaller than current monitored hosts 1000（配置的受监控主机数），please clear a part of monitored hosts.”来提醒管理员配置没有生效，需要删除部分已经被监控的主机。

当受监控主机表满时，打印日志“% NFPP_ARP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000（配置的受监控主机数） monitored hosts.”提醒管理员。

18.3.6 基于主机限速和识别攻击

识别主机有源 IP/VLAN ID/端口和链路层源 MAC/VLAN ID/端口两种识别方法。每台主机都有限速水线和攻击阈值（也称为告警水线），限速水线必须低于攻击阈值。当单台主机的 ARP 报文速度超过限速水线时，将丢弃这些超出限速水线的报文；如果单台主机的 ARP 报文速度超过攻击阈值，将采取隔离措施，记录到日志中，发送 TRAP。

支持识别 ARP 扫描，单位时间是 10 秒，缺省值是 15，如果 10 秒钟收到 15 个及以上 ARP 报文，链路层源 MAC 地址固定而源 IP 地址变化，或者链路层源 MAC 地址和源 IP 地址固定而目标 IP 地址不断变化，就认为有扫描嫌疑，将记录到日志中，发送 TRAP。

当检测到攻击行为时，打印的日志信息格式如下：

```
%NFPP_ARP_GUARD-4-DOS_DETECTED: Host<IP=N/A,MAC=0000.0000.0004,port=Gi4/1,VLAN=1> was
detected.(2009-07-01 13:00:00)
```

日志内容最后面括号中的时间是检测到攻击的时间。

发送的 TRAP 报文的数据中包含如下描述信息：

```
ARP DoS attack from host<IP=N/A,MAC=0000.0000.0004,port=Gi4/1,VLAN=1> was detected.
```

如果管理员把隔离时间配置成非零值，当硬件隔离成功时，打印的日志信息格式如下所示：

```
%NFPP_ARP_GUARD-4-ISOLATED:Host <IP=N/A,MAC=0000.0000.0004,port=Gi4/1,VLAN=1> was isolated.
(2009-07-01 13:00:00)
```

发送的 TRAP 报文的数据包含如下描述信息：

```
Host<IP=N/A,MAC=0000.0000.0004,port=Gi4/1,VLAN=1> was isolated.
```

当硬件隔离失败（原因通常是内存不足或者硬件资源不足）时，打印的日志信息格式如下所示：

```
%NFPP_ARP_GUARD-4-ISOLATE_FAILED: Failed to isolate host <IP=N/A,MAC=0000.0000.0004,port=Gi4/1,VLAN=1>.
(2009-07-01 13:00:00)
```

发送的 TRAP 报文的数据包含如下描述信息：

```
Failed to isolate host<IP=N/A,MAC=0000.0000.0004,port=Gi4/1,VLAN=1>.
```

当检测到 ARP 扫描时，打印的日志信息格式如下所示：

```
%NFPP_ARP_GUARD-4-SCAN: Host<IP=1.1.1.1,MAC=0000.0000.0004,port=Gi4/1,VLAN=1> was detected.
(2009-07-01 13:00:00)
```

发送的 TRAP 报文的数据包含如下描述信息：

```
ARP scan from host< IP=1.1.1.1,MAC=0000.0000.0004,port=Gi4/1,VLAN=1> was detected.
```

ARP 扫描表只保存最新的 256 条记录。当 ARP 扫描表满的时候，会打印日志提醒管理员：

```
%NFPP_ARP_GUARD-4-SCAN_TABLE_FULL: ARP scan table is full.
```

当管理员配置的限速水线大于攻击阈值时，打印命令提示信息“%ERROR：rate limit is higher than attack threshold 500pps(配置的攻击阈值).”提醒管理员。

当管理员配置的攻击阈值小于限速水线时，打印命令提示信息“%ERROR：attack threshold is smaller than rate limit 300pps(配置的限速水线).”提醒管理员。

- 对攻击者进行隔离，会设置一条策略到硬件中，但是硬件资源有限，当硬件资源耗尽的时候，会打印日志提醒管理员。
- 当无法为检测到的攻击者分配内存时，打印日志“%NFPP_ARP_GUARD-4-NO_MEMORY: Failed to alloc memory..”提醒管理员。
- ARP 扫描表只记录最新的 256 条记录。当 ARP 扫描表满了以后，最新记录将覆盖最旧记录。

管理员可以在 **nfpp** 配置模式和接口配置模式下进行配置。

命令	作用
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#nfpp**	进入 NFPP 配置模式
Ruijie(config-nfpp)**#arp-guard rate-limit {per-src-ip | per-src-mac}** *pps*	全局对每台主机的 ARP 报文速度进行限制。 取值范围是 1 到 9999，缺省值为 4 个。 “**per-src-ip**”是基于源 IP/VID/端口识别主机，“**per-src-mac**”是基于链路层源 MAC/VID/端口识别主机。
Ruijie(config-nfpp)**#arp-guard attack-threshold {per-src-ip | per-src-mac}** *pps*	全局配置攻击阈值。当某台主机的 ARP 报文超过攻击阈值时，就认为是在进行攻击，立即对这台主机采取隔离措施，记录到日志，发送 TRAP。 取值范围是 1 到 9999，缺省值为 8 个。 “**per-src-ip**”是基于源 IP/VID/端口识别主机，“**per-src-mac**”是基于链路层源 MAC/VID/端口识别主机。
Ruijie(config-nfpp)**#arp-guard scan-threshold** *pkt-cnt*	全局配置 ARP 扫描阈值，取值范围是 1 到 9999，缺省值为 15 个。单位值是 10 秒。如果 10 秒钟收到 15 个以上 ARP 报文，链路层源 MAC 地址固定而源 IP 地址变化，或者链路层源 MAC 地址和源 IP 地址固定而目标 IP 地址不断变化，就认为有扫描嫌疑。 ARP 扫描的特征是链路层源 MAC 地址固定而源 IP 地址变化，或者链路层源 MAC 地址和源 IP 地址固定而目标 IP 地址不断变化。
Ruijie(config-nfpp)**#end**	退回到特权模式。
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#interface** *interface-name*	进入接口配置模式。
Ruijie(config-if)**#nfpp arp-guard policy {per-src-ip | per-src-mac}** *rate-limit-pps attack-threshold-pps*	配置局部的限速水线和攻击水线，只在该配置所属端口上生效。 *rate-limit-pps* 是限速水线，取值范围是 1 到 9999，缺省是没配置基于端口的速率，采用全局的速率。 *attack-threshold-pps* 是攻击水线，取值范围是 1 到 9999。 缺省情况是端口没有自己的限速水线和攻击水线，采用全局的限速水线和限速水线。 “**per-src-ip**”是基于源 IP/VID/端口识别主机，“**per-src-mac**”是基于链路层源 MAC/VID/端口识别主机。
Ruijie(config-if)**#nfpp arp-guard scan-threshold** *pkt-cnt*	在每个端口上配置 ARP 扫描阈值，取值范围是 1 到 9999，缺省是没配置基于端口的 ARP 扫描阈值，采用全局 ARP 扫描阈值。单位值是 10 秒。
Ruijie(config-if)**#end**	退回到特权模式。
Ruijie**#show nfpp arp-guard summary**	核对配置参数
Ruijie**#copy running-config startup-config**	保存配置。

18.3.7 基于端口限速和识别攻击

每个端口都有限速水线和攻击阈值，限速水线必须低于攻击阈值。当某个端口的 ARP 报文速度超过限速水线时，就丢弃 ARP 报文。如果某个端口的 ARP 报文速度超过攻击阈值，将记录到日志中，发送 TRAP。

当端口遭受 ARP 拒绝服务攻击时，打印的警告信息格式如下：

```
%NFPP_ARP_GUARD-4-PORT_ATTACKED: ARP DoS attack was detected on port Gi4/1. (2009-07-01 13:00:00)
```

发送的 TRAP 报文的数据包含如下描述信息：

```
ARP DoS attack was detected on port Gi4/1.
```

管理员可以在 **nfpp** 配置模式和接口配置模式下进行配置。

命令	作用
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#nfpp**	进入 NFPP 配置模式
Ruijie(config-nfpp)**#arp-guard rate-limit per-port** *pps*	对每个端口的 ARP 报文速度进行限制。 取值范围是 1 到 9999，缺省值为 100 个。
Ruijie(config-nfpp)**#arp-guard attack-threshold per-port** *pps*	配置攻击阈值，当某个端口的 ARP 报文超过阈值时，记录到日志，发送 TRAP。 取值范围是 1 到 9999，缺省值为 200 个。
Ruijie(config-nfpp)**#end**	退回到特权模式。
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#interface** *interface-name*	进入接口配置模式。
Ruijie(config-if)**#nfpp arp-guard policy per-port** *rate-limit-pps attack-threshold-pps*	配置局部的限速水线和攻击水线，只在该配置所属端口上生效。 *rate-limit-pps* 是限速水线，取值范围是 1 到 9999。 *attack-threshold-pps* 是攻击水线，取值范围是 1 到 9999。 缺省情况是端口没有自己的限速水线和攻击水线，采用全局的限速水线和攻击水线。
Ruijie(config-if)**#end**	退回到特权模式。
Ruijie**#show nfpp arp-guard summary**	核对配置参数
Ruijie**#copy running-config startup-config**	保存配置。

- 基于 MAC 地址限速的优先级高于基于 IP 地址限速，而基于 IP 地址限速又高于基于端口限速。
- 为了使 ARP 抗攻击得到最佳的防攻击效果，建议管理员配置基于主机的限速水线和告警水线时遵循以下原则：
- 基于 IP 地址的限速水线 < 基于 IP 地址的告警水线 < 基于源 MAC 地址的限速水线 < 基于源 MAC 地址的告警水线。
- 配置端口限速水线时，可以参考这个端口上的主机数量，比如某个端口上有 500 台主机，那么可以把端口的限速水线设置成 500。

18.3.8 清除受监控主机

已被隔离的主机在一段时间后自动恢复，如果管理员要手动清除该主机，可以在特权模式下用以下命令清除。

命令	作用
Ruijie**#clear nfpp arp-guard hosts** [**vlan** *vid*] [**interface** *interface-id*] [*ip-address*	*mac-address*]	不带参数表示清除所有已被检测到攻击的主机，带参数表示清除符合条件的主机。

18.3.9 清除ARP扫描表

如果管理员要手动清除 ARP 扫描表，可以在特权模式下用以下命令清除。

命令	作用
Ruijie**#clear nfpp arp-guard scan**	清空 ARP 扫描表

18.3.10 查看ARP抗攻击的配置参数

使用 **show nfpp arp-guard summary** 查看 ARP 抗攻击的配置参数：

命令	作用
show nfpp arp-guard summary	查看 ARP 抗攻击配置参数

下面是一个例子：

```
Ruijie# show nfpp arp-guard summary
 (Format of column Rate-limit and  Attack-threshold is per-src-ip/per-src-mac/per-port.)
Interface  Status  Isolate-period Rate-limit Attack-threshold Scan-threshold
Global      Enable  300             4/5/60     8/10/100          15
G 0/1       Enable  180             5/-/-       8/-/-              -
G 0/2       Disable 200             4/5/60     8/10/100          20

Maximum count of monitored hosts: 1000
Monitor period：300s
```

字段 Interface 为 Global 表示全局配置。

字段 Status 表示是否打开抗攻击功能。

字段 Rate-limit 的格式为（对源 IP 地址的限速水线/对源 MAC 地址的限速水线/端口的限速水线值），字段 Attack-threshold 的显示格式类似。“-”表示没有配置。举例说明：

“4/5/60”表示对源 IP 地址的限速水线是 4，对源 MAC 地址的限速水线是 5，对每个端口的限速水线是 60。

G 0/1 这一行的字段 Rate-limit 为“5/-/-”，表示端口 G 0/1 对源 IP 地址的限速水线是 5，没有配置对源 MAC 地址的限速水线和端口的限速水线。

18.3.11 查看受监控主机的信息

命令	作用

show nfpp arp-guard hosts statistics	查看受监控主机表的统计信息，包括主机总数、隔离成功的主机数量和隔离失败的主机数量。
show nfpp arp-guard hosts [**vlan** *vid*] [**interface** *interface-id*] [*ip-address* |*mac-address*]	查看已被检测到攻击的主机。 不带参数表示显示所有已被检测到攻击的主机，带参数则只显示符合条件的主机。

```
Ruijie#show nfpp arp-guard hosts statistics
success    fail    total
-------    ----    -----
100          20        120
```

意思是：“总共有 120 台主机被隔离，其中 100 台主机隔离成功，20 台主机隔离失败”。

```
Ruijie# show nfpp arp-guard hosts
If column 1 shows '*', it means "hardware do not isolate user".
VLAN  interface IP address   MAC address      remain-time(s)
----  --------  ---------    -----------      -------------
1      Gi0/1       1.1.1.1      -                  110
2      Gi0/2       1.1.2.1      -                  61
*3     Gi0/3       -              0000.0000.1111   110
4      Gi0/4       -              0000.0000.2222    61
Total: 4 hosts

Ruijie# show nfpp arp-guard hosts vlan 1 interface G 0/1 1.1.1.1
If column 1 shows '*', it means "hardware do not isolate user".
VLAN  interface IP address   MAC address      remain-time(s)
---- --------  ---------     -----------      -------------
1     Gi0/1       1.1.1.1       -                  110
Total: 1 host
```

上述几个字段分别表示 VLAN 号、端口、IP 地址、MAC 地址，以及隔离剩余时间。

如果某一行的第一列显示“*”， 表示这台主机目前只是软件监控或者硬件因为资源不足而隔离失败。

如果“MAC address”栏显示“-”，表示这台主机是以源 IP 地址标识的；如果“IP address”栏显示“-”，表示这台主机是以源 MAC 地址标识的。

18.3.12 查看ARP扫描表

命令	作用
show nfpp arp-guard scan statistic	查看 ARP 扫描表的记录条数
show nfpp arp-guard scan [**vlan** *vid*] [**interface** *interface-id*] [*ip-address*] [*mac-address*]	查看 ARP 扫描表的记录 不带参数表示查看整张 ARP 扫描表，带参数表示只查看符合条件的表项。

```
Ruijie# show nfpp arp-guard scan statistics
```

```
ARP scan table has 4 record(s).
```

意思是：“ARP 扫描表总共有 4 条记录”。

```
Ruijie# show nfpp arp-guard scan
VLAN    interface   IP address   MAC address      timestamp
----    --------    ----------  -----------      ----------
1        Gi0/1       N/A           0000.0000.0001   2008-01-23 16:23:10
2        Gi0/2       1.1.1.1      0000.0000.0002   2008-01-23 16:24:10
3        Gi0/3       N/A           0000.0000.0003   2008-01-23 16:25:10
4        Gi0/4       N/A           0000.0000.0004   2008-01-23 16:26:10
Total：4 record(s)
```

“timestamp”记录的是检测出 ARP 扫描的时间，如“2008-01-23 16:23:10”表示在 2008 年 1 月 23 日 16 点 23 分 10 秒检测出 ARP 扫描。

```
Ruijie# show nfpp arp-guard scan vlan 1 interface G 0/1 0000.0000.0001
VLAN    interface   IP address   MAC address      timestamp
----    --------    ----------    -----------      ----------
1        Gi0/1       N/A           0000.0000.0001   2008-01-23 16:23:10
Total：1 record(s)
```

18.4 IP防扫描

18.4.1 IP防扫描简介

众所周知，许多黑客攻击、网络病毒入侵都是从扫描网络内活动的主机开始的。因此大量的扫描报文急剧占用了网络带宽，导致网络通讯无法正常进行。

为此，锐捷三层设备提供了防 IP 攻击的功能，用以防止黑客扫描和类似“冲击波”病毒的攻击，还能减少三层设备的 CPU 负担。

目前发现的 IP 攻击主要有两种：

1) 目的 IP 地址变化的扫描。这种扫描是最危害网络的，不但消耗网络带宽，增加设备的负担，而且更是大部分黑客攻击手段的前奏。

2) 向不存在目的 IP 地址高速发送 IP 报文。这种攻击主要是针对设备 CPU 的负担来设计。对三层设备来说，如果目的 IP 地址存在，则报文会被交换芯片直接转发，不会占用设备 CPU 的资源，而如果目的 IP 地址不存在，IP 报文会送到 CPU，由 CPU 发送 ARP 请求询问目的 IP 地址对应的 MAC 地址，如果送到 CPU 的报文太多，会消耗 CPU 资源。当然，这种攻击的危害比第一种小得多了。

对于“向不存在的目的 IP 地址高速发 IP 报文”这种 IP 攻击，防范措施是一方面对 IP 报文限速，另一方面检测出攻击源，对攻击源头采取隔离措施。

IP 攻击识别分为基于主机和基于物理端口两个类别。基于主机是采用源 IP 地址/VLAN ID/物理端口三者结合识别的。每种攻击识别都有限速水线和告警水线。当 IP 报文速率超过限速水线时，超限报文将被丢弃。当 IP 报文速率超过告警水线时，将打印警告信息，发送 TRAP，基于主机的攻击识别还会对攻击源头采取隔离措施。

需要特别说明的是，IP 防扫描针对的是目的 IP 地址不是本机 IP 地址的 IP 报文攻击。对于目的 IP 地址是本机 IP 地址的 IP 报文，则由 CPP（CPU Protect Policy）限速。

对检测出有 IP 扫描嫌疑的主机，如果在端口上打开 IP 防扫描功能，并且配置的隔离时间是非零值，将采取隔离措施。，

18.4.2 打开IP防扫描功能

您可以在 **nfpp** 配置模式或者接口配置模式下打开 IP 防扫描功能，缺省情况下是打开的。

命令	作用
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#nfpp**	进入 NFPP 配置模式。
Ruijie(config-nfpp)**#ip-guard enable**	全局打开 IP 防扫描功能，缺省情况下打开。
Ruijie(config-nfpp)**#end**	退回到特权模式。
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#interface** *interface-name*	进入接口配置模式。
Ruijie(config-if)**#nfpp ip-guard enable**	在端口上打开 IP 防扫描功能，缺省情况是端口没有配置局部开关，采用全局开关。
Ruijie(config-if)**#end**	退回到特权模式。
Ruijie**#show nfpp ip-guard summary**	核对配置参数
Ruijie**#copy running-config startup-config**	保存配置。

当关闭 IP 防扫描功能时，系统将自动清除受监控的主机。

18.4.3 设置对攻击者的隔离时间

对攻击者的隔离时间分为全局隔离时间和基于端口的隔离时间（即局部隔离时间）。对于某个端口，如果没有配置基于端口的隔离时间，那么采用全局隔离时间；否则，采用基于端口的隔离时间。

命令	作用
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#nfpp**	进入 NFPP 配置模式
Ruijie(config-nfpp)**#ip-guard isolate-period** [*seconds* | **permanent**]	配置对攻击者的全局隔离时间。 取值范围为 0 秒，30 秒到 86400 秒（即一天），缺省值为 0 秒，表示不隔离；**permanent** 表示永久隔离。
Ruijie(config-nfpp)**#end**	返回特权模式
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#interface** *interface-name*	进入接口配置模式。
Ruijie(config-if)**#nfpp ip-guard isolate-period** [*seconds* | **permanent**]	在端口上配置对攻击者的隔离时间。 取值范围为 0 秒，180 秒到 86400 秒（即一天），缺省情况是没有配置局部隔离时间，采用全局隔离时间。0 秒表示不隔离；**permanent** 表示永久隔离。
Ruijie(config-if)**#end**	退回到特权模式。
Ruijie**#show nfpp ip-guard summary**	核对配置参数

Ruijie**#copy running-config startup-config**	保存配置。

如果要把全局隔离时间恢复成缺省值，在 **nfpp** 配置模式执行命令“**no ip-guard isolate-period**”。如果一个端口原来配置了局部隔离时间，现在想采用全局隔离时间，那么在端口配置模式下执行命令“**no nfpp ip-guard isolate-period**”把局部隔离时间配置删除。

18.4.4 设置对攻击者的监控时间

如果隔离时间为 0（即不隔离），防攻击模块将自动根据配置的监控时间对攻击者进行软件监控，提供当前系统中存在哪些攻击者的信息。当把隔离时间配置成非零值后，防攻击模块将自动对软件监控的主机采取硬件隔离。

命令	作用
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#nfpp**	进入 NFPP 配置模式
Ruijie(config-nfpp)**#ip-guard monitor-period** *seconds*	配置对攻击者的监控时间。 取值范围为 180 秒到 86400 秒（即一天），缺省值为 600 秒。
Ruijie(config-nfpp)**#end**	退回到特权模式。
Ruijie**#show nfpp ip-guard summary**	核对配置参数
Ruijie**#copy running-config startup-config**	保存配置。

如果要把监控时间恢复成缺省值，在 nfpp 配置模式执行命令“**no ip-guard monitor-period**”。

检测出攻击者的时候，如果隔离时间为 0，将对攻击者进行软件监控，超时为监控时间。在软件监控过程中，当隔离时间被配置为非零值时，将自动对软件监控的攻击者采取硬件隔离，并且把超时设置为隔离时间。监控时间在隔离时间为 0 的情况下才有意义。

如果把隔离时间从非零值改成零，将直接把相关端口的攻击者删除，而不是进行软件监控。

18.4.5 设置受监控主机的最大数目

命令	作用
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#nfpp**	进入 NFPP 配置模式。
Ruijie(config-nfpp)**#ip-guard monitored-host-limit** *number*	配置受监控主机的最大数目。 取值范围为 1 到 4294967295，缺省情况下受监控主机的最大数目为 1000 个。
Ruijie(config-nfpp)**#end**	退回到特权模式。
Ruijie**#show nfpp ip-guard summary**	核对配置参数
Ruijie**#copy running-config startup-config**	保存配置。

如果要把配置的受监控主机数恢复成缺省值，在 nfpp 配置模式执行命令“**no ip-guard monitored-host-limit**”。

如果受监控主机数已经达到默认的 1000 个，此时管理员把受监控主机的最大数目设置成小于 1000，不会删除已有的受监控主机，而是打印信息“%ERROR： The value that you configured is smaller than current monitored hosts 1000（配置的受监控主机数），please clear a part of monitored hosts.”来提醒管理员配置没有生效，需要删除部分已经被监控的主机。

当受监控主机表满时，打印日志“% NFPP_IP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000（配置的受监控主机数） monitored hosts.”提醒管理员。

18.4.6 基于主机限速和识别攻击

识别主机的方法为源 IP 地址/VID/端口。每台主机都有限速水线和攻击阈值（也称为告警水线），限速水线必须低于攻击阈值。当单台主机的 IP 报文速度超过限速水线时，就丢弃超限的 IP 报文。如果单台主机的 IP 报文速度超过攻击阈值，将采取隔离措施，记录到日志中，发送 TRAP。

当检测到攻击行为时，打印的日志信息格式如下：

```
%NFPP_IP_GUARD-4- DOS_DETECTED:Host<IP=1.1.1.1,MAC= N/A,port=Gi4/1,VLAN=1> was detected.
(2009-07-01 13:00:00)
```

发送的 TRAP 报文的数据中包含如下描述信息：

```
IP DoS attack from host<IP=1.1.1.1,MAC= N/A,port=Gi4/1,VLAN=1> was detected.
```

如果管理员把隔离时间配置成非零值，当硬件隔离成功时，打印的日志信息格式如下所示：

```
%NFPP_IP_GUARD-4-ISOLATED:Host<IP=1.1.1.1, MAC= N/A ,port=Gi4/1,VLAN=1> was isolated. (2009-07-01 13:00:00)
```

发送的 TRAP 报文的数据包含如下描述信息：

```
Host<IP=1.1.1.1,MAC=N/A,port=Gi4/1,VLAN=1> was isolated.
```

当硬件隔离失败（原因通常是内存不足或者硬件资源不足）时，打印的日志信息格式如下所示：

```
%NFPP_IP_GUARD-4-ISOLATE_FAILED:Failed to isolate host<IP=1.1.1.1, MAC=
N/A ,port=Gi4/1,VLAN=1>.(2009-07-01 13:00:00)
```

发送的 TRAP 报文的数据包含如下描述信息：

```
Failed to isolate host<IP=1.1.1.1,MAC= N/A,port=Gi4/1,VLAN=1>.
```

当检测到 IP 扫描时，打印的日志信息格式如下所示：

```
%NFPP_IP_GUARD-4-SCAN: Host<IP=1.1.1.1,MAC=N/A,port=Gi4/1,VLAN=1> was detected.
```

发送的 TRAP 报文的数据包含如下描述信息：

```
IP scan from host< IP=1.1.1.1,MAC=N/A,port=Gi4/1,VLAN=1> was detected.
```

对攻击者进行隔离，会设置一条策略到硬件中，但是硬件资源有限，当硬件资源耗尽的时候，会打印日志提醒管理员。

当无法为检测到的攻击者分配内存时，打印日志“%NFPP_IP_GUARD-4-NO_MEMORY: Failed to alloc memory..”提醒管理员。

管理员可以在 **nfpp** 配置模式和接口配置模式下进行配置。

命令	作用
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#nfpp**	进入 NFPP 配置模式

Ruijie(config-nfpp)**#ip-guard rate-limit per-src-ip** *pps*	全局对每台主机的 IP 报文速度进行限制。 取值范围是 1 到 9999，缺省值为 20 个。 “**per-src-ip**”是基于源 IP/VID/端口识别主机。
Ruijie(config-nfpp)**#ip-guard attack-threshold per-src-ip** *pps*	全局配置攻击阈值。当某台主机的 IP 报文超过攻击阈值时，就认为是在进行攻击，立即对这台主机采取隔离措施，记录到日志，发送 TRAP。 取值范围是 1 到 9999，缺省值为 20。 “**per-src-ip**”是基于源 IP/VID/端口识别主机。
Ruijie(config-nfpp)**#ip-guard scan-threshold** *pkt-cnt*	全局配置 IP 扫描阈值，取值范围是 1 到 9999，缺省值为 100 个，时间单位是 10 秒。
Ruijie(config-nfpp)**#end**	退回到特权模式。
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#interface** *interface-name*	进入接口配置模式。
Ruijie(config-if)**#nfpp ip-guard policy per-src-ip** *rate-limit-pps attack-threshold-pps*	配置局部的限速水线和攻击水线，只在该配置所属端口上生效。 *rate-limit-pps* 是限速水线，取值范围是 1 到 9999，缺省是没有配置基于端口的速率，采用全局速率。 *attack-threshold-pps* 是攻击水线，取值范围是 1 到 9999。缺省情况是端口没有自己的限速水线和攻击水线，采用全局的限速水线和攻击水线。 “per-src-ip”是基于源 IP/VID/端口识别主机。
Ruijie(config-if)**#nfpp ip-guard scan-threshold** *pkt-cnt*	配置局部的 IP 扫描阈值，取值范围是 1 到 9999。 缺省情况是端口没有自己的扫描阈值，采用全局的扫描阈值。
Ruijie(config-if)**#end**	退回到特权模式。
Ruijie**#show nfpp ip-guard summary**	核对配置参数
Ruijie**#copy running-config startup-config**	保存配置。

18.4.7 基于端口限速和识别攻击

每个端口都有限速水线和攻击阈值，限速水线必须低于攻击阈值。当某个端口的 IP 报文速度超过限速水线时，就丢弃 IP 报文。如果某个端口的 IP 报文速度超过攻击阈值，将记录到日志中，发送 TRAP。

当端口遭受 IP 拒绝服务攻击时，打印的警告信息格式如下：

```
%NFPP_IP_GUARD-4-PORT_ATTACKED: IP DoS attack was detected on port Gi4/1. (2009-07-01 13:00:00)
```

发送的 TRAP 报文的数据包含如下描述信息：

```
IP DoS attack was detected on port Gi4/1.
```

管理员可以在 **nfpp** 配置模式和接口配置模式下进行配置。

命令	作用
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#nfpp**	进入 NFPP 配置模式

Ruijie(config-nfpp)**#ip-guard rate-limit per-port** *pps*	全局对每个端口的 IP 报文速度进行限制。 取值范围是 1 到 9999，缺省值为 100 个。
Ruijie(config-nfpp)**#ip-guard attack-threshold per-port** *pps*	配置攻击阈值，当某个端口的 IP 报文超过阈值时，记录到日志，发送 TRAP。 取值范围是 1 到 9999，缺省值为 200 个。
Ruijie(config-nfpp)**#end**	退回到特权模式。
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#interface** *interface-name*	进入接口配置模式。
Ruijie(config-if)**#nfpp ip-guard policy per-port** *rate-limit-pps attack-threshold-pps*	配置局部的限速水线和攻击水线，只在该配置所属端口上生效。 *rate-limit-pps* 是限速水线，取值范围是 1 到 9999。 *attack-threshold-pps* 是攻击水线，取值范围是 1 到 9999。 缺省情况是端口没有自己的限速水线和攻击水线，采用全局的限速水线和攻击水线。
Ruijie(config-if)**#end**	退回到特权模式。
Ruijie**#show nfpp ip-guard summary**	核对配置参数
Ruijie**#copy running-config startup-config**	保存配置。

基于源 IP 地址限速优先级高于基于端口限速。

18.4.8 设置不监控的可信主机

如果管理员希望对某台主机不进行监控，即对该主机表示信任，则可以通过该命令配置。该可信主机发往 CPU 的 IP 报文将被允许发往 CPU。

命令	作用
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#nfpp**	进入 NFPP 配置模式
Ruijie(config-nfpp)**#ip-guard trusted-host** *ip mask*	配置不进行监控的 IP 地址范围。 最多能够配置 500 条。
Ruijie(config-nfpp)**#end**	退回到特权模式。
Ruijie**#show nfpp ip-guard trusted-host**	查看配置的可信主机
Ruijie**#copy running-config startup-config**	保存配置。

在 **nfpp** 配置模式下，可以使用该命令的 **no** 选项删除一条可信主机表项。使用命令的 **no** 和 **all** 选项可以删除所有可信主机。

例如删除所有可信主机：

```
Ruijie(config-nfpp)# no ip-guard trusted-host all
```

或删除单条可信主机表项：

```
Ruijie(config-nfpp)# no ip-guard trusted-host 1.1.1.1 255.255.255.255
```

当不监控的可信主机表满时，打印提示信息“%ERROR: Attempt to exceed limit of 500 trusted hosts.”提醒管理员。

当受监控主机表中存在与可信主机相匹配的表项（IP 地址相同）时，系统将自动删除此 IP 地址对应的表项。

- 当删除可信主机失败时，打印提示信息“%ERROR: Failed to delete trusted host 1.1.1.0 255.255.255.0（配置的可信主机）.”提醒管理员。
- 当添加可信主机失败时，打印提示信息“%ERROR: Failed to add trusted host 1.1.1.0 255.255.255.0（配置的可信主机）.”提醒管理员。
- 当添加的可信主机已经存在时，打印提示信息“%ERROR: Trusted host 1.1.1.0 255.255.255.0（配置的可信主机）has already been configured.”提醒管理员。
- 当要删除的可信主机不存在时，打印提示信息“%ERROR: Trusted host 1.1.1.0 255.255.255.0（配置的可信主机）is not found.”提醒管理员。
- 当无法为可信主机分配内存时，打印提示信息“%ERROR: Failed to alloc memory.”提醒管理员。

18.4.9 清除受监控主机

已被隔离的主机在一段时间后自动恢复，如果管理员要手动清除该主机，可以在特权模式下用以下命令清除。

命令	作用
Ruijie# **clear nfpp ip-guard hosts** [**vlan** *vid*] [**interface** *interface-id*] [*ip-address*]	不带参数表示清除所有已被检测到攻击的主机，带参数表示清除符合条件的主机。

18.4.10 查看IP防扫描的配置参数

使用 **show nfpp ip-guard summary** 查看 IP 抗攻击的配置参数：

命令	作用
show nfpp ip-guard summary	查看 IP 抗攻击配置参数

下面是一个例子：

```
Ruijie# show nfpp ip-guard summary
 (Format of column Rate-limit and  Attack-threshold is per-src-ip/per-src-mac/per-port.)
Interface  Status  Isolate-period Rate-limit Attack-threshold Scan-threshold
Global      Enable  300             4/-/60     8/-/100          15
G 0/1       Enable  180             5/-/-       8/-/-             -
G 0/2       Disable 200             4/-/60     8/-/100          20

Maximum count of monitored hosts: 1000
Monitor period：300s
```

- 字段 Interface 为 Global 表示全局配置。
- 字段 Status 表示是否打开抗攻击功能。
- 字段 Rate-limit 的格式为（对源 IP 地址的限速水线/对源 MAC 地址的限速水线/端口的限速水线值），字段 Attack-threshold 的显示格式类似。“-”表示没有配置。举例说明：

“4/-/60”表示对源 IP 地址的限速水线是 4，对每个端口的限速水线是 60。

G 0/1 这一行的字段 Rate-limit 为“5/-/-”，表示端口 G 0/1 对源 IP 地址的限速水线是 5，没有配置对端口的限速水线。

18.4.11 查看受监控主机的信息

命令	作用
show nfpp ip-guard hosts statistics	查看受监控主机表的统计信息，包括主机总数、隔离成功的主机数量和隔离失败的主机数量。
show nfpp ip-guard hosts [vlan *vid*] [**interface** *interface-id*] [*ip-address* |*mac-address*]	查看已被检测到攻击的主机。 不带参数表示显示所有已被检测到攻击的主机，带参数则只显示符合条件的主机。

```
Ruijie#show nfpp ip-guard hosts statistics
success    fail    total
-------    ----    -----
100         20       120
```

意思是：“总共有 120 台主机被隔离，其中 100 台主机隔离成功，20 台主机隔离失败”。

```
Ruijie#show nfpp ip-guard hosts
If column 1 shows '*', it means "hardware do not isolate host".
VLAN  interface IP address   Reason      remain-time(s)
----  ---------  ----------   -------      -------------
1      Gi0/1       1.1.1.1      ATTACK      110
2      Gi0/2       1.1.2.1      SCAN         61
Total: 2 host(s)
```

```
Ruijie#show nfpp ip-guard hosts vlan 1 interface g 0/1 1.1.1.1
If column 1 shows '*', it means "hardware do not isolate host".
VLAN  interface IP address   Reason      remain-time(s)
----  ---------  ----------   -------      -------------
1      Gi0/1       1.1.1.1      ATTACK      110
Total: 1 host(s)
```

上述几个字段分别表示 VLAN 号、端口、IP 地址、被监控原因，以及隔离剩余时间。

如果某一行的第一列显示“*”， 表示这台主机目前只是软件监控或者硬件因为资源不足而隔离失败。

第四个字段“Reason”描述主机被监控的原因，“ATTACK”表示主机发送 IP 报文的速度超过攻击水线，“SCAN”表示主机在扫描某个网段。

18.4.12 查看不监控的可信主机

命令	作用

show nfpp ip-guard trusted-host	查看不受监控的可信主机

下面是一个例子：

```
Ruijie#show nfpp ip-guard trusted-host
IP address      mask
---------       ------
1.1.1.0         255.255.255.0
1.1.2.0         255.255.255.0
Total：2 record(s)
```

18.5 ICMP抗攻击

18.5.1 ICMP抗攻击简介

ICMP 协议作为诊断网络故障的常用手段，它的基本原理是主机发出 ICMP 回音请求报文（ICMP echo request），路由器或者交换机接收到这个请求报文后会回应一个 ICMP 回音应答（ICMP echo reply）报文。在上述这个处理过程中需要设备的 CPU 进行处理，这样就必然需要消耗 CPU 的一部分资源。如果攻击者向目标设备发送大量的 ICMP 回音请求，这样势必会导致设备的 CPU 资源被大量消耗，严重的情况可能导致设备无法正常工作，这种攻击方式也被人们命名为“ICMP 洪水”。对于这种攻击，防范措施是一方面对 ICMP 报文限速，另一方面检测出攻击源，对攻击源头采取隔离措施。

ICMP 攻击识别分为基于主机和基于物理端口两个类别。基于主机方式是采用源 IP 地址/虚拟局域网号/端口三者结合来识别的。每种攻击识别都有限速水线和告警水线。当 ICMP 报文速率超过限速水线时，将被丢弃。当 ICMP 报文速率超过告警水线时，将打印警告信息，发送 TRAP，基于主机的攻击识别还会对攻击源头采取隔离措施。

18.5.2 打开ICMP抗攻击功能

管理员可以在 **nfpp** 配置模式或者接口配置模式下打开 ICMP 抗攻击功能，缺省情况下就是打开的。

命令	作用
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#nfpp**	进入 NFPP 配置模式。
Ruijie(config-nfpp)**#icmp-guard enable**	打开 ICMP 抗攻击功能，缺省情况下启动。
Ruijie(config-nfpp)**#end**	退回到特权模式。
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#interface** *interface-name*	进入接口配置模式。
Ruijie(config-if)**#nfpp icmp-guard enable**	在端口上打开 ICMP 抗攻击功能，缺省情况是端口没有配置局部开关，采用全局开关。
Ruijie(config-if)**#end**	退回到特权模式。
Ruijie**#show nfpp icmp-guard summary**	核对配置参数
Ruijie**#copy running-config startup-config**	保存配置。

当关闭 ICMP 抗攻击功能时，系统将自动清除已经被监控的主机。

18.5.3 设置对攻击者的隔离时间

对攻击者的隔离时间分为全局隔离时间和基于端口的隔离时间（即局部隔离时间）。对于某个端口，如果没有配置基于端口的隔离时间，那么采用全局隔离时间；否则，采用基于端口的隔离时间。

命令	作用
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#nfpp**	进入 NFPP 配置模式
Ruijie(config-nfpp)**#icmp-guard isolate-period** [*seconds* | **permanent**]	配置对攻击者的全局隔离时间。 取值范围为 0 秒，30 秒到 86400 秒（即一天），缺省值为 0 秒，表示不隔离；**permanent** 表示永久隔离。
Ruijie(config-nfpp)**#end**	退回到特权模式。
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#interface** *interface-name*	进入接口配置模式。
Ruijie(config-if)**#nfpp icmp-guard isolate-period**[*seconds* | **permanent**]	在端口上配置对攻击者的隔离时间。 取值范围为 0 秒，180 秒到 86400 秒（即一天），缺省情况是没有配置局部隔离时间，采用全局隔离时间。0 秒表示不隔离；**permanent** 表示永久隔离。
Ruijie(config-if)**#end**	退回到特权模式。
Ruijie**#show nfpp icmp-guard summary**	核对配置参数
Ruijie**#copy running-config startup-config**	保存配置。

如果要把全局隔离时间恢复成缺省值，在 **nfpp** 配置模式执行命令“**no icmp-guard isolate-period**”。如果一个端口原来配置了局部隔离时间，现在想采用全局隔离时间，那么在接口配置模式下执行命令“**no nfpp icmp-guard isolate-period**”把局部隔离时间配置删除。

18.5.4 设置对攻击者的监控时间

如果不配置全局隔离时间和基于端口的隔离时间（包括端口隔离时间配置成 0 秒），这种情况下，防攻击模块将自动采用监控时间对攻击者进行软件监控，提供当前系统中存在哪些攻击用户的信息。当配置全局隔离时间或者基于端口的隔离时间后，防攻击模块将自动对软件监控的用户采取硬件隔离。

命令	作用
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#nfpp**	进入 NFPP 配置模式
Ruijie(config-nfpp)**#icmp-guard monitor-period** *seconds*	配置对攻击者的监控时间。 取值范围为 180 秒到 86400 秒（即一天），缺省值为 600 秒。
Ruijie(config-nfpp)**#end**	退回到特权模式。
Ruijie**#show nfpp icmp-guard summary**	核对配置参数
Ruijie**#copy running-config startup-config**	保存配置。

如果要把监控时间恢复成缺省值，在 nfpp 配置模式执行命令“**no icmp-guard monitor-period**”。

检测出攻击者的时候，如果隔离时间为 0，将对攻击者进行软件监控，超时为监控时间。在软件监控过程中，当隔离时间被配置为非零值时，将自动对软件监控的攻击者采取硬件隔离，并且把超时设置为隔离时间。监控时间在隔离时间为 0 的情况下才有意义。

如果把隔离时间从非零值改成零，将直接把相关端口的攻击者删除，而不是进行软件监控。

18.5.5 设置受监控主机的最大数目

命令	作用
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#nfpp**	进入 NFPP 配置模式。
Ruijie(config-nfpp)**#icmp-guard monitored-host-limit** *number*	配置受监控主机的最大数目。 取值范围为 1 到 4294967295 个，缺省情况下受监控主机的最大数目为 1000 个。
Ruijie(config-nfpp)**#end**	退回到特权模式。
Ruijie**#show nfpp icmp-guard summary**	核对配置参数
Ruijie**#copy running-config startup-config**	保存配置。

如果要把配置的最大受监控主机数恢复成缺省值，在 nfpp 配置模式执行命令“**no icmp-guard monitored-host-limit**”。

如果受监控主机数已经达到默认的 1000 个，此时管理员把受监控主机的最大数目设置成小于 1000，不会删除已有的受监控主机，而是打印信息“%ERROR： The value that you configured is smaller than current monitored hosts 1000（配置的受监控主机数），please clear a part of monitored hosts.”来提醒管理员配置没有生效，需要删除部分已经被监控的主机。

当受监控主机满时，打印日志“% NFPP_ICMP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000（配置的受监控主机数） monitored hosts.”提醒管理员。

18.5.6 基于主机限速和识别攻击

识别主机的方法为源 IP/VID/端口。每个用户都有限速水线和攻击阈值（也称为告警水线），限速水线必须低于攻击阈值。当单台主机的 ICMP 报文速度超过限速水线时，就丢弃超限的 ICMP 报文。如果单台主机的 ICMP 报文速度超过攻击阈值，将采取隔离措施，记录到日志中，发送 TRAP。

如果检测到攻击行为，打印的日志信息格式如下：

```
%NFPP_ICMP_GUARD-4-DOS_DETECTED: Host<IP=1.1.1.1,MAC= N/A,port=Gi4/1,VLAN=1> was detected.
(2009-07-01 13:00:00)
```

发送的 TRAP 报文的数据包含如下描述信息：

```
ICMP DoS attack from host<IP=1.1.1.1,MAC= N/A,port=Gi4/1,VLAN=1> was detected.
```

如果管理员把隔离时间配置成非零值，当硬件隔离成功时，打印的日志信息格式如下所示：

```
%NFPP_ICMP_GUARD-4-ISOLATED:Host<IP=1.1.1.1, MAC= N/A ,port=Gi4/1,VLAN=1> was isolated. (2009-07-01 13:00:00)
```

发送的 TRAP 报文的数据包含如下描述信息：

```
Host<IP=1.1.1.1,MAC= N/A,port=Gi4/1,VLAN=1> was isolated.
```

当硬件隔离失败（原因通常是内存不足或者硬件资源不足）时，打印的日志信息格式如下所示：

```
%NFPP_ICMP_GUARD-4-ISOLATE_FAILED: Failed to isolate host<IP=1.1.1.1, MAC=
N/A ,port=Gi4/1,VLAN=1>.(2009-07-01 13:00:00)
```

发送的 TRAP 报文的数据包含如下描述信息：

```
Failed to isolate host<IP=1.1.1.1,MAC= N/A,port=Gi4/1,VLAN=1>.
```

> 当无法为检测到的攻击者分配内存时，打印日志“%NFPPP_ ICMP_GUARD -4-NO_MEMORY: Failed to alloc memory.”提醒管理员。

管理员可以在 **nfpp** 配置模式和接口配置模式下进行配置。

命令	作用
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#nfpp**	进入 NFPP 配置模式。
Ruijie(config-nfpp)**#icmp-guard rate-limit per-src-ip** *pps*	全局对每台主机的 ICMP 报文速度进行限制。 取值范围是 1 到 9999，缺省值是基于端口的全局限速水线（将在下一节说明）的一半。 “**per-src-ip**”是基于源 IP/VID/端口识别主机。
Ruijie(config-nfpp)**#icmp-guard attack-threshold per-src-**ip *pps*	配置攻击阈值。当某台主机的 ICMP 报文超过攻击阈值时，就认为是在进行攻击，立即对这台主机采取隔离措施，记录到日志，发送 TRAP。 取值范围是 1 到 9999，缺省值和基于源 IP 地址的缺省限速水线相同。 “**per-src-ip**”是基于源 IP/VID/端口识别主机。
Ruijie(config-nfpp)**#end**	退回到特权模式。
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#interface** *interface-name*	进入接口配置模式。
Ruijie(config-if)**#nfpp icmp-guard policy per-src-ip** *rate-limit-pps attack-threshold-pps*	配置局部的限速水线和攻击水线，只在该配置所属端口上生效。 *rate-limit-pps* 是限速水线，取值范围是 1 到 9999，缺省是没有配置基于端口的速率，采用全局速率。 *attack-threshold-pps* 是攻击水线，取值范围是 1 到 9999。 缺省情况是端口没有自己的限速水线和攻击水线，采用全局的限速水线和攻击水线。 “per-src-ip”是基于源 IP/VID/端口识别主机。
Ruijie(config-if)**#end**	退回到特权模式。
Ruijie**#show nfpp icmp-guard summary**	核对配置参数
Ruijie**#copy running-config startup-config**	保存配置。

18.5.7 基于端口限速和识别攻击

每个端口都有限速水线和攻击阈值，限速水线必须低于攻击阈值。当某个端口的 ICMP 报文速度超过限速水线时，就丢弃 ICMP 报文。如果某个端口的 ICMP 报文速度超过攻击阈值，将记录到日志中，发送 TRAP。

当端口遭受 ICMP 拒绝服务攻击时，打印的警告信息格式如下：

```
%NFPP_ICMP_GUARD-4-PORT_ATTACKED: ICMP DoS attack was detected on port Gi4/1. (2009-07-01 13:00:00)
```

发送的 TRAP 报文的数据包含如下描述信息：

```
ICMP DoS attack was detected on port Gi4/1.
```

管理员可以在 **nfpp** 配置模式和接口配置模式下进行配置。

命令	作用
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#nfpp**	进入 NFPP 配置模式。
Ruijie(config-nfpp)**#icmp-guard rate-limit per-port** *pps*	对每个端口的 ICMP 报文速度进行限制。 取值范围是 1 到 9999，缺省值因产品而异，S5750-S 的缺省值为 400。
Ruijie(config-nfpp)**#icmp-guard attack-threshold per-port** *pps*	配置攻击阈值，当某个端口的 ICMP 报文超过阈值时，记录到日志，发送 TRAP。 取值范围是 1 到 9999，缺省值和基于端口的缺省限速水线相同。
Ruijie(config-nfpp)**#end**	退回到特权模式。
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#interface** *interface-name*	进入接口配置模式。
Ruijie(config-if)**#nfpp icmp-guard policy per-port** *rate-limit-pps attack-threshold-pps*	配置局部的限速水线和攻击水线，只在该配置所属端口上生效。 *rate-limit-pps* 是限速水线，取值范围是 1 到 9999。 *attack-threshold-pps* 是攻击水线，取值范围是 1 到 9999。 缺省情况是端口没有自己的限速水线和攻击水线，采用全局的限速水线和攻击水线。
Ruijie(config-if)**#end**	退回到特权模式。
Ruijie**#show nfpp icmp-guard configuration**	核对配置参数
Ruijie**#copy running-config tartup-config**	保存配置。

基于源 IP 地址限速优先级高于基于端口限速。

18.5.8 设置不监控的可信主机

如果管理员希望对某台主机不进行监控，即对该主机表示信任，则可以通过该命令配置。该可信主机发往 CPU 的 ping 报文将被允许发往 CPU。

命令	作用
Ruijie**#configure terminal**	进入全局配置模式。

Ruijie(config)**#nfpp**	进入 NFPP 配置模式。
Ruijie(config-nfpp)**#icmp-guard trusted-host** *ip mask*	配置不进行监控的 IP 地址范围。 最多能够配置 500 条。
Ruijie(config-nfpp)**#end**	退回到特权模式。
Ruijie**#show nfpp icmp-guard trusted-host**	查看不监控的可信主机。
Ruijie**#copy running-config startup-config**	保存配置。

在 **nfpp** 配置模式下，可以使用该命令的 **no** 选项删除一条可信主机表项。使用命令的 **no** 和 **all** 选项可以删除所有可信主机。

例如删除所有可信主机：

```
Ruijie(config-nfpp)# no icmp-guard trusted-host all
```

或删除单条可信主机：

```
Ruijie(config-nfpp)# no icmp-guard trusted-host 1.1.1.1 255.255.255.255
```

- 当不监控的可信主机表满时，打印提示信息“%ERROR: Attempt to exceed limit of 500 trusted hosts.”提醒管理员。
- 当受监控主机表中存在与可信主机相匹配的表项（IP 地址相同）时，系统将自动删除此 IP 地址对应的表项。
- 当删除可信主机失败时，打印提示信息“%ERROR: Failed to delete trusted host 1.1.1.0 255.255.255.0（配置的可信主机）.”提醒管理员。
- 当添加可信主机失败时，打印提示信息“%ERROR: Failed to add trusted host 1.1.1.0 255.255.255.0（配置的可信主机）.”提醒管理员。
- 当添加的可信主机已经存在时，打印提示信息“%ERROR: Trusted host 1.1.1.0 255.255.255.0（配置的可信主机）has already been configured.”提醒管理员。
- 当要删除的可信主机不存在时，打印提示信息“%ERROR: Trusted host 1.1.1.0 255.255.255.0（配置的可信主机）is not found.”提醒管理员。
- 当无法为可信主机分配内存时，打印提示信息“%ERROR: Failed to alloc memory.”提醒管理员。

18.5.9 清除受监控主机

已被隔离的主机在一段时间后自动恢复，如果管理员要手动清除该主机，可以在特权模式下用以下命令清除。

命令	作用
Ruijie**#clear nfpp icmp-guard hosts** [**vlan** *vid*] [**interface** *interface-id*] [*ip-address*]	不带参数表示清除所有已被检测到攻击的主机，带参数表示清除符合条件的主机。

18.5.10 查看ICMP抗攻击的配置参数

使用 **show nfpp icmp-guard summary** 查看 ICMP 抗攻击的配置参数：

命令	作用
show nfpp icmp-guard summary	查看 ICMP 抗攻击配置参数

下面是一个例子：

```
Ruijie# show nfpp icmp-guard summary
（Format of column Rate-limit and  Attack-threshold is per-src-ip/per-src-mac/per-port.）
Interface  Status  Isolate-period Rate-limit Attack-threshold
Global      Enable  300             4/-/60     8/-/100
G 0/1       Enable  180             5/-/-       8/-/-
G 0/2       Disable 200             4/-/60     8/-/100

Maximum count of monitored hosts: 1000
Monitor period：300s
```

字段 Interface 为 Global 表示全局配置。

字段 Status 表示是否打开抗攻击功能。

字段 Rate-limit 的格式为（对源 IP 地址的限速水线/对源 MAC 地址的限速水线/端口的限速水线值），字段 Attack-threshold 的显示格式类似。“-”表示没有配置。举例说明：

“4/-/60”表示对源 IP 地址的限速水线是 4，对每个端口的限速水线是 60。

G 0/1 这一行的字段 Rate-limit 为“5/-/-”，表示端口 G 0/1 对源 IP 地址的限速水线是 5，没有配置对端口的限速水线。

18.5.11 查看受监控主机的信息

命令	作用
show nfpp icmp-guard hosts statistics	查看受监控主机表的统计信息，包括主机总数、隔离成功的主机数量和隔离失败的主机数量。
show nfpp icmp-guard hosts [**vlan** *vid*] [**interface** *interface-id*] [*ip-address*]	查看已被检测到攻击的主机。 不带参数表示显示所有已被检测到攻击的主机，带参数则只显示符合条件的主机。

```
Ruijie#show nfpp icmp-guard hosts statistics
success    fail    total
-------    ----    -----
100         20        120
```

表示：“总共有 120 台主机被监控，其中 100 台主机隔离成功，20 台主机隔离失败”。

```
Ruijie# show nfpp icmp-guard hosts
If column 1 shows '*', it means "hardware failed to isolate host".
VLAN  interface IP address     remain-time(s)
----  --------   ---------     -------------
1     Gi0/1      1.1.1.1       110
2     Gi0/2      1.1.2.1       61
Total：2 host(s)
```

```
Ruijie# show nfpp icmp-guard hosts vlan 1 interface g 0/1 1.1.1.1
If column 1 shows '*', it means "hardware failed to isolate host".
VLAN  interface IP address     remain-time(s)
---- --------   ---------      -------------
1    Gi0/1      1.1.1.1        80
Total：1 host(s)
```

上述几个字段分别表示 VLAN 号、端口、IP 地址、MAC 地址，以及隔离剩余时间。

如果某一行的第一列显示“*”， 表示这台主机目前只是软件监控或者硬件因为资源不足而隔离失败。

18.5.12 查看不监控的可信主机

使用 **show nfpp icmp-guard trusted-host** 查看不受监控的可信主机：

命令	作用
show nfpp icmp-guard trusted-host	查看不受监控的可信主机。

下面是一个例子：

```
Ruijie# show nfpp icmp-guard trusted-host
IP address      mask
---------       ------
1.1.1.0         255.255.255.0
1.1.2.0         255.255.255.0
Total：2 record(s)
```

18.6 DHCP抗攻击

18.6.1 DHCP抗攻击简介

DHCP 协议被广泛地应用在局域网环境里来动态分配 IP 地址。DHCP 协议对网络安全起着非常重要的意义。目前，存在的最广泛的 DHCP 攻击就是称为“DHCP 耗竭”的攻击，这种攻击通过伪造的 MAC 地址来广播 DHCP 请求的方式进行。目前网络上存在多种这样的攻击工具都可以很容易地实现上述攻击。如果发出的 DHCP 请求足够多的话，网络攻击者就可以在一段时间内耗竭 DHCP 服务器所提供的地址空间，这样当一台合法的主机请求一个 DHCP IP 地址的时候无法成功，从而无法访问网络。对于这种攻击，防范措施是一方面对 DHCP 报文限速，另一方面检测出攻击源，对攻击源头采取隔离措施。

DHCP 攻击识别分为基于主机和基于物理端口两个类别。基于主机方式是采用链路层源 MAC 地址/虚拟局域网号/端口三者结合来识别的。每种攻击识别都有限速水线和告警水线。当 DHCP 报文速率超过限速水线时，超限的 DHCP 报文将被丢弃。当 DHCP 报文速率超过告警水线时，将打印警告信息，发送 TRAP，基于主机的攻击识别还会对攻击源头采取隔离措施。

18.6.2 打开DHCP抗攻击功能

管理员可以在 **nfpp** 配置模式或者接口配置模式下打开 DHCP 抗攻击功能，缺省情况下就是打开的。

命令	作用
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#nfpp**	进入 NFPP 配置模式。
Ruijie(config-nfpp)**#dhcp-guard enable**	打开 DHCP 抗攻击功能，缺省情况下就是打开的。
Ruijie(config-nfpp)**#end**	退回到特权模式。
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#interface** *interface-name*	进入接口配置模式。
Ruijie(config-if)**#nfpp dhcp-guard enable**	在端口上打开 DHCP 抗攻击功能，缺省情况是端口没有配置局部开关，采用全局开关。
Ruijie(config-if)**#end**	退回到特权模式。
Ruijie**#show nfpp dhcp-guard summary**	核对配置参数
Ruijie**#copy running-config startup-config**	保存配置。

当关闭 DHCP 抗攻击功能时，系统将自动清除已经被监控的主机。

18.6.3 设置对攻击者的隔离时间

对攻击者的隔离时间分为全局隔离时间和基于端口的隔离时间（即局部隔离时间）。对于某个端口，如果没有配置基于端口的隔离时间，那么采用全局隔离时间；否则，采用基于端口的隔离时间。

命令	作用
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#nfpp**	进入 NFPP 配置模块
Ruijie(config-nfpp)**#dhcp-guard isolate-period** [*seconds* | **permanent**]	配置对攻击者的全局隔离时间。 取值范围为 0 秒，30 秒到 86400 秒（即一天），缺省值为 0 秒，表示不隔离；**permanent** 表示永久隔离。
Ruijie(config-nfpp)**#end**	退回到特权模式。
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#interface** *interface-name*	进入接口配置模式。
Ruijie(config-if)**#nfpp dhcp-guard isolate-period** [*seconds* | **permanent**]	在端口上配置对攻击者的隔离时间。 取值范围为 0 秒，180 秒到 86400 秒（即一天），缺省情况是没有配置局部隔离时间，采用全局隔离时间。0 秒表示不隔离；**permanent** 表示永久隔离。
Ruijie(config-if)**#end**	退回到特权模式。
Ruijie**#show nfpp dhcp-guard summary**	核对配置参数
Ruijie**#copy running-config startup-config**	保存配置。

如果要把全局隔离时间恢复成缺省值，在 **nfpp** 配置模式执行命令“**no dhcp-guard isolate-period**”。如果一个端口原来配置了局部隔离时间，现在想采用全局隔离时间，那么在接口配置模式下执行命令“**no nfpp dhcp-guard isolate-period**”把局部隔离时间配置删除。

18.6.4 设置对攻击者的监控时间

如果隔离时间为 0（即不隔离），防攻击模块将自动根据配置的监控时间对攻击者进行软件监控，提供当前系统中存在哪些攻击者的信息。当把隔离时间配置成非零值后，防攻击模块将自动对软件监控的主机采取硬件隔离。

命令	作用
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#nfpp**	进入 NFPP 配置模式
Ruijie(config-nfpp)**#dhcp-guard monitor-period** *seconds*	配置对攻击者的监控时间。 取值范围为 180 秒到 86400 秒（即一天），缺省值为 600 秒。
Ruijie(config-nfpp)**#end**	退回到特权模式。
Ruijie**#show nfpp dhcp-guard summary**	核对配置参数
Ruijie**#copy running-config startup-config**	保存配置。

如果要把监控时间恢复成缺省值，在 nfpp 配置模式执行命令“**no dhcp-guard monitor-period**”。

检测出攻击者的时候，如果隔离时间为 0，将对攻击者进行软件监控，超时为监控时间。在软件监控过程中，当隔离时间被配置为非零值时，将自动对软件监控的攻击者采取硬件隔离，并且把超时设置为隔离时间。监控时间在隔离时间为 0 的情况下才有意义。

如果把隔离时间从非零值改成零，将直接把相关端口的攻击者删除，而不是进行软件监控。

18.6.5 设置受监控主机的最大数目

命令	作用
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#nfpp**	进入 NFPP 配置模式。
Ruijie(config-nfpp)**#dhcp-guard monitored-host-limit** *number*	配置受监控主机的最大数目。 取值范围为 1 到 4294967295，缺省情况下受监控主机的最大数目为 1000 个。
Ruijie(config-nfpp)**#end**	退回到特权模式。
Ruijie**#show nfpp dhcp-guard summary**	核对配置参数
Ruijie**#copy running-config startup-config**	保存配置。

如果要把配置的最大受监控主机数恢复成缺省值，在 nfpp 配置模式执行命令“**no dhcp-guard monitored-host-limit**”。

如果受监控主机数已经达到默认的 1000 个，此时管理员把受监控主机的最大数目设置成小于 1000，不会删除已有的受监控主机，而是打印信息“%ERROR：The value that you configured is smaller than current monitored hosts 1000（配置的受监控主机数），please clear a part of monitored hosts.”来提醒管理员配置没有生效，需要删除部分已经被监控的主机。

当受监控主机表满时，打印日志“% NFPP_DHCP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000（配置的受监控主机数） monitored hosts.”提醒管理员。

18.6.6 基于主机限速和识别攻击

识别主机的方法为链路层源 MAC/VID/端口。每台主机都有限速水线和攻击阈值（也称为告警水线），限速水线必须低于攻击阈值。当单台主机的 DHCP 报文速度超过限速水线时，就丢弃超限的 DHCP 报文。如果单台主机的 DHCP 报文速度超过攻击阈值，将采取隔离措施，记录到日志中，发送 TRAP。

如果检测到攻击行为，打印的日志信息格式如下：

```
%NFPP_DHCP_GUARD-4-DOS_DETECTED: Host<IP=N/A,MAC=0000.0000.0001,port=Gi4/1,VLAN=1> was detected.
(2009-07-01 13:00:00)
```

发送的 TRAP 报文的数据包含如下描述信息：

```
DHCP DoS attack from host<IP=N/A,MAC=0000.0000.0001,port=Gi4/1,VLAN=1> was detected.
```

如果管理员把隔离时间配置成非零值，当硬件隔离成功时，打印的日志信息格式如下所示：

```
%NFPP_DHCP_GUARD-4-ISOLATED:Host<IP=N/A, MAC=0000.0000.0001,port=Gi4/1,VLAN=1> was isolated.
(2009-07-01 13:00:00)
```

发送的 TRAP 报文的数据包含如下描述信息：

```
Host<IP=N/A, MAC=0000.0000.0001,port=Gi4/1,VLAN=1> was isolated.
```

当硬件隔离失败（原因通常是内存不足或者硬件资源不足）时，打印的日志信息格式如下所示：

```
%NFPP_DHCP_GUARD-4-ISOLATE_FAIL:Failed to isolate host<IP=N/A,
MAC=0000.0000.0001,port=Gi4/1,VLAN=1>.(2009-07-01 13:00:00)
```

发送的 TRAP 报文的数据包含如下描述信息：

```
Failed to isolate host<IP=N/A, MAC=0000.0000.0001,port=Gi4/1,VLAN=1>.
```

当无法为检测到的攻击者分配内存时，打印日志“%NFPP_DHCP_GUARD-4-NO_MEMORY: Failed to alloc memory.”提醒管理员。

管理员可以在 **nfpp** 配置模式和接口配置模式下进行配置。

命令	作用
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#nfpp**	进入 NFPP 配置模式。
Ruijie(config-nfpp)**#dhcp-guard rate-limit per-src-mac** *pps*	全局对每台主机的 DHCP 报文速度进行限制。 取值范围是 1 到 9999，缺省值为 5 个。 “**per-src-mac**”是基于链路层源 MAC/VID/端口识别主机。
Ruijie(config-nfpp)**#dhcp-guard attack-threshold per-src-mac** *pps*	配置攻击阈值。当某台主机的 DHCP 报文超过攻击阈值时，就认为是在进行攻击，立即对这台主机采取隔离措施，记录到日志，发送 TRAP。 取值范围是 1 到 9999，缺省值为 10 个。 “**per-src-mac**”是基于链路层源 MAC/VID/端口识别主机。

Ruijie(config-nfpp)**#end**	退回到特权模式。
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#interface** *interface-name*	进入接口配置模式。
Ruijie(config-if)**#nfpp dhcp-guard policy per-src-mac** *rate-limit-pps attack-threshold-pps*	配置局部的限速水线和攻击水线，只在该配置所属端口上生效。 *rate-limit-pps* 是限速水线，取值范围是 1 到 9999。 *attack-threshold-pps* 是攻击水线，取值范围是 1 到 9999。 缺省情况是端口没有自己的限速水线和攻击水线，采用全局的限速水线和攻击水线。 “per-src-mac”是基于链路层源 MAC/VID/端口识别主机。
Ruijie(config-if)**#end**	退回到特权模式。
Ruijie**#show nfpp dhcp-guard summary**	核对配置参数
Ruijie**#copy running-config startup-config**	保存配置。

18.6.7 基于端口限速和识别攻击

每个端口都有限速水线和攻击阈值，限速水线必须低于攻击阈值。当某个端口的 DHCP 报文速度超过限速水线时，就丢弃超限 DHCP 报文。如果某个端口的 DHCP 报文速度超过攻击阈值，将记录到日志中，发送 TRAP。

当端口遭受 DHCP 拒绝服务攻击时，打印的警告信息格式如下：

```
%NFPP_DHCP_GUARD-4-PORT_ATTACKED: DHCP DoS attack was detected on port Gi4/1. (2009-07-01 13:00:00)
```

发送的 TRAP 报文的数据包含如下描述信息：

```
DHCP DoS attack was detected on port Gi4/1.
```

管理员可以在 **nfpp** 配置模式和接口配置模式下进行配置。

命令	作用
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#nfpp**	进入 NFPP 配置模式。
Ruijie(config-nfpp)**#dhcp-guard rate-limit per-port** *pps*	对每个端口的 DHCP 报文速度进行限制。 取值范围是 1 到 9999，缺省值为 150 个。
Ruijie(config-nfpp)**#dhcp-guard attack-threshold per-port** *pps*	配置攻击阈值，当某个端口的 DHCP 报文超过阈值时，记录到日志，发送 TRAP。 取值范围是 1 到 9999，缺省值为 300 个。
Ruijie(config-nfpp)**#end**	退回到特权模式。
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#interface** *interface-name*	进入接口配置模式。
Ruijie(config-if)**#nfpp dhcp-guard policy per-port** *rate-limit-pps attack-threshold-pps*	配置局部的限速水线和攻击水线，只在该配置所属端口上生效。 *rate-limit-pps* 是限速水线，取值范围是 1 到 9999。 *attack-threshold-pps* 是攻击水线，取值范围是 1 到 9999。 缺省情况是端口没有自己的限速水线和攻击水线，采用全局的限速水线和攻击水线。

Ruijie(config-if)#**end**	退回到特权模式。
Ruijie#**show nfpp dhcp-guard summary**	核对配置参数
Ruijie#**copy running-config startup-config**	保存配置。

基于链路层源 MAC 地址限速优先于基于端口限速处理。

18.6.8 清除受监控主机

已被隔离的主机在一段时间后自动恢复，如果管理员要手动清除该主机，可以在特权模式下用以下命令清除。

命令	作用
Ruijie#**clear nfpp dhcp-guard hosts** [**vlan** *vid*] [**interface** *interface-id*] [*mac-address*]	不带参数表示清除所有已被检测到攻击的主机，带参数表示清除符合条件的主机。

18.6.9 查看DHCP抗攻击的配置参数

使用 **show nfpp dhcp-guard summary** 查看 DHCP 抗攻击的配置参数：

命令	作用
show nfpp dhcp-guard summary	查看 DHCP 抗攻击配置参数

下面是一个例子：

```
Ruijie# show nfpp dhcp-guard summary
 (Format of column Rate-limit and  Attack-threshold is per-src-ip/per-src-mac/per-port.)
Interface  Status  Isolate-period Rate-limit Attack-threshold
Global      Enable  300             -/5/150      -/10/300
G 0/1       Enable  180             -/6/-        -/8/-
G 0/2       Disable 200             -/5/30      -/10/50

Maximum count of monitored hosts: 1000
Monitor period：300s
```

字段 Interface 为 Global 表示全局配置。

字段 Status 表示是否打开抗攻击功能。

字段 Rate-limit 的格式为（对源 IP 地址的限速水线/对源 MAC 地址的限速水线/端口的限速水线值），字段 Attack-threshold 的显示格式类似。“-”表示没有配置。举例说明：

“-/5/150”表示对源 MAC 地址的限速水线是 5，对每个端口的限速水线是 150。

G 0/1 这一行的字段 Rate-limit 为“-/6/-”，表示端口 G 0/1 对源 MAC 地址的限速水线是 6，没有配置对端口的限速水线。

18.6.10 查看受监控主机的信息

命令	作用

show nfpp dhcp-guard hosts statistics	查看受监控主机表的统计信息，包括主机总数、隔离成功的主机数量和隔离失败的主机数量。
show nfpp dhcp-guard hosts [**vlan** *vid*] [**interface** *interface-id*] [*mac-address*]	查看已被检测到攻击的主机。 不带参数表示显示所有已被检测到攻击的主机，带参数则只显示符合条件的主机。

```
Ruijie# show nfpp dhcp-guard hosts statistics
success    fail    total
------     ----     -----
100         20        120
```

表示：“总共有 120 台主机被监控，其中 100 台主机隔离成功，20 台主机隔离失败”。

```
Ruijie# show nfpp dhcp-guard hosts
If column 1 shows '*', it means "hardware failed to isolate host".
VLAN  interface   MAC address      remain-time(s)
----  --------    -----------      -------------
*1     Gi0/1       0000.0000.0001  110
2      Gi0/2       0000.0000.2222   61
Total: 2 host(s)
```

```
Ruijie# show nfpp dhcp-guard hosts vlan 1 interface g 0/1 0000.0000.0001
If column 1 shows '*', it means "hardware failed to isolate host".
VLAN  interface   MAC address      remain-time(s)
---- --------     -----------      -------------
 *1     Gi0/1      0000.0000.0001  110
Total: 1 host(s)
```

上述几个字段分别表示 VLAN 号、端口、IP 地址、MAC 地址，以及隔离剩余时间。

如果某一行的第一列显示“*”， 表示这台主机目前只是软件监控或者硬件因为资源不足而隔离失败。

18.7 DHCPv6 抗攻击

18.7.1 DHCPv6 抗攻击简介

DHCPv6 协议被广泛地应用在局域网环境里来动态分配 IPv6 地址。和 DHCPv4 协议一样，DHCPv6 协议存在安全问题，对 DHCPv4 协议的攻击方法同样适用于 DHCPv6 协议。网络攻击者可以发出大量 DHCPv6 请求，在一段时间内耗竭 DHCPv6 服务器所提供的地址空间，这样当一台合法的主机请求一个 IPv6 地址的时候无法成功，从而无法访问网络。对于这种攻击，防范措施是一方面对 DHCPv6 报文限速，另一方面检测出攻击源，对攻击源头采取隔离措施。

DHCPv6 攻击识别分为基于主机和基于物理端口两个类别。基于主机方式是采用链路层源 MAC 地址/虚拟局域网号/端口三者结合来识别的。每种攻击识别都有限速水线和告警水线。当 DHCP 报文速率超过限速水线时，超限的 DHCPv6 报文将被丢弃。当 DHCPv6 报文速率超过告警水线时，将打印警告信息，发送 TRAP，基于主机的攻击识别还会对攻击源头采取隔离措施。

18.7.2 打开DHCPv6 抗攻击功能

管理员可以在 **nfpp** 配置模式或者接口配置模式下打开 DHCPv6 抗攻击功能，缺省情况下就是打开的。

命令	作用
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#nfpp**	进入 NFPP 配置模式。
Ruijie(config-nfpp)**#dhcpv6-guard enable**	打开 DHCPv6 抗攻击功能，缺省情况下就是打开的。
Ruijie(config-nfpp)**#end**	退回到特权模式。
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#interface** *interface-name*	进入接口配置模式。
Ruijie(config-if)**#nfpp dhcpv6-guard enable**	在端口上打开 DHCPv6 抗攻击功能，缺省情况是端口没有配置局部开关，采用全局开关。
Ruijie(config-if)**#end**	退回到特权模式。
Ruijie**#show nfpp dhcpv6-guard summary**	核对配置参数
Ruijie**#copy running-config startup-config**	保存配置。

当关闭 DHCPv6 抗攻击功能时，系统将自动清除已经被监控的主机。

18.7.3 设置对攻击者的隔离时间

对攻击者的隔离时间分为全局隔离时间和基于端口的隔离时间（即局部隔离时间）。对于某个端口，如果没有配置基于端口的隔离时间，那么采用全局隔离时间；否则，采用基于端口的隔离时间。

命令	作用
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#nfpp**	进入 NFPP 配置模块
Ruijie(config-nfpp)**#dhcpv6-guard isolate-period** [*seconds* | **permanent**]	配置对攻击者的全局隔离时间。 取值范围为 0 秒，30 秒到 86400 秒（即一天），缺省值为 0 秒，表示不隔离；**permanent** 表示永久隔离。
Ruijie(config-nfpp)**#end**	退回到特权模式。
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#interface** *interface-name*	进入接口配置模式。
Ruijie(config-if)**#nfpp dhcpv6-guard isolate-period** [*seconds* | **permanent**]	在端口上配置对攻击者的隔离时间。 取值范围为 0 秒，180 秒到 86400 秒（即一天），缺省情况是没有配置局部隔离时间，采用全局隔离时间。0 秒表示不隔离；**permanent** 表示永久隔离。
Ruijie(config-if)**#end**	退回到特权模式。
Ruijie**#show nfpp dhcpv6-guard summary**	核对配置参数
Ruijie**#copy running-config startup-config**	保存配置。

如果要把全局隔离时间恢复成缺省值，在 **nfpp** 配置模式执行命令“**no dhcpv6-guard isolate-period**”。如果一个端口原来配置了局部隔离时间，现在想采用全局隔离时间，那么在接口配置模式下执行命令“**no nfpp dhcpv6-guard isolate-period**”把局部隔离时间配置删除。

18.7.4 设置对攻击者的监控时间

如果隔离时间为 0（即不隔离），防攻击模块将自动根据配置的监控时间对攻击者进行软件监控，提供当前系统中存在哪些攻击者的信息。当把隔离时间配置成非零值后，防攻击模块将自动对软件监控的主机采取硬件隔离。

命令	作用
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#nfpp**	进入 NFPP 配置模式
Ruijie(config-nfpp)**#dhcpv6-guard monitor-period** *seconds*	配置对攻击者的监控时间。 取值范围为 180 秒到 86400 秒（即一天），缺省值为 600 秒。
Ruijie(config-nfpp)**#end**	退回到特权模式。
Ruijie**#show nfpp dhcpv6-guard summary**	核对配置参数
Ruijie**#copy running-config startup-config**	保存配置。

如果要把监控时间恢复成缺省值，在 nfpp 配置模式执行命令“**no dhcpv6-guard monitor-period**”。

检测出攻击者的时候，如果隔离时间为 0，将对攻击者进行软件监控，超时为监控时间。在软件监控过程中，当隔离时间被配置为非零值时，将自动对软件监控的攻击者采取硬件隔离，并且把超时设置为隔离时间。监控时间在隔离时间为 0 的情况下才有意义。

如果把隔离时间从非零值改成零，将直接把相关端口的攻击者删除，而不是进行软件监控。

18.7.5 设置受监控主机的最大数目

命令	作用
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#nfpp**	进入 NFPP 配置模式。
Ruijie(config-nfpp)**#dhcpv6-guard monitored-host-limit** *number*	配置受监控主机的最大数目。 取值范围为 1 到 4294967295，缺省情况下受监控主机的最大数目为 1000 个。
Ruijie(config-nfpp)**#end**	退回到特权模式。
Ruijie**#show nfpp dhcpv6-guard summary**	核对配置参数
Ruijie**#copy running-config startup-config**	保存配置。

如果要把配置的最大受监控主机数恢复成缺省值，在 nfpp 配置模式执行命令“**no dhcpv6-guard monitored-host-limit**”。

如果受监控主机数已经达到默认的 1000 个，此时管理员把受监控主机的最大数目设置成小于 1000，不会删除已有的受监控主机，而是打印信息“%ERROR：The value that you configured is smaller than current monitored hosts 1000（配置的受监控主机数），please clear a part of monitored hosts.”来提醒管理员配置没有生效，需要删除部分已经被监控的主机。

当受监控主机表满时，打印日志“% NFPP_DHCPV6_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000（配置的受监控主机数） monitored hosts.”提醒管理员。

18.7.6 基于主机限速和识别攻击

识别主机的方法为链路层源 MAC/VID/端口。每台主机都有限速水线和攻击阈值（也称为告警水线），限速水线必须低于攻击阈值。当单台主机的 DHCPv6 报文速度超过限速水线时，就丢弃超限的 DHCPv6 报文。如果单台主机的 DHCPv6 报文速度超过攻击阈值，将采取隔离措施，记录到日志中，发送 TRAP。

如果检测到攻击行为，打印的日志信息格式如下：

```
%NFPP_DHCPV6_GUARD-4-DOS_DETECTED: Host<IP=N/A,MAC=0000.0000.0001,port=Gi4/1,VLAN=1> was detected.
(2009-07-01 13:00:00)
```

发送的 TRAP 报文的数据包含如下描述信息：

```
DHCPv6 DoS attack from host<IP=N/A,MAC=0000.0000.0001,port=Gi4/1,VLAN=1> was detected.
```

如果管理员把隔离时间配置成非零值，当硬件隔离成功时，打印的日志信息格式如下所示：

```
%NFPP_DHCPV6_GUARD-4-ISOLATED:Host<IP=N/A, MAC=0000.0000.0001,port=Gi4/1,VLAN=1> was isolated.
(2009-07-01 13:00:00)
```

发送的 TRAP 报文的数据包含如下描述信息：

```
Host<IP=N/A, MAC=0000.0000.0001,port=Gi4/1,VLAN=1> was isolated.
```

当硬件隔离失败（原因通常是内存不足或者硬件资源不足）时，打印的日志信息格式如下所示：

```
%NFPP_DHCPV6_GUARD-4-ISOLATE_FAIL:Failed to isolate host<IP=N/A,
MAC=0000.0000.0001,port=Gi4/1,VLAN=1>.(2009-07-01 13:00:00)
```

发送的 TRAP 报文的数据包含如下描述信息：

```
Failed to isolate host<IP=N/A, MAC=0000.0000.0001,port=Gi4/1,VLAN=1>.
```

当无法为检测到的攻击者分配内存时，打印日志“%NFPP_DHCPV6_GUARD-4-NO_MEMORY: Failed to alloc memory.”提醒管理员。

管理员可以在 **nfpp** 配置模式和接口配置模式下进行配置。

命令	作用
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#nfpp**	进入 NFPP 配置模式。
Ruijie(config-nfpp)**#dhcpv6-guard rate-limit per-src-mac** *pps*	全局对每台主机的 DHCPv6 报文速度进行限制。 取值范围是 1 到 9999，缺省值为 5 个。 “**per-src-mac**”是基于链路层源 MAC/VID/端口识别主机。
Ruijie(config-nfpp)**#dhcpv6-guard attack-threshold** per-src-mac *pps*	配置攻击阈值。当某台主机的 DHCPv6 报文超过攻击阈值时，就认为是在进行攻击，立即对这台主机采取隔离措施，记录到日志，发送 TRAP。 取值范围是 1 到 9999，缺省值为 10 个。 “**per-src-mac**”是基于链路层源 MAC/VID/端口识别主机。
Ruijie(config-nfpp)**#end**	退回到特权模式。
Ruijie**#configure terminal**	进入全局配置模式。

Ruijie(config)**#interface** *interface-name*	进入接口配置模式。
Ruijie(config-if)**#nfpp dhcpv6-guard policy per-src-mac** *rate-limit-pps attack-threshold-pps*	配置局部的限速水线和攻击水线，只在该配置所属端口上生效。 *rate-limit-pps* 是限速水线，取值范围是 1 到 9999。 *attack-threshold-pps* 是攻击水线，取值范围是 1 到 9999。 缺省情况是端口没有自己的限速水线和攻击水线，采用全局的限速水线和攻击水线。 “**per-src-mac**”是基于链路层源 MAC/VID/端口识别主机。
Ruijie(config-if)**#end**	退回到特权模式。
Ruijie**#show nfpp dhcpv6-guard summary**	核对配置参数
Ruijie**#copy running-config startup-config**	保存配置。

18.7.7 基于端口限速和识别攻击

每个端口都有限速水线和攻击阈值，限速水线必须低于攻击阈值。当某个端口的 DHCPv6 报文速度超过限速水线时，就丢弃超限 DHCPv6 报文。如果某个端口的 DHCP 报文速度超过攻击阈值，将记录到日志中，发送 TRAP。

当端口遭受 DHCPv6 拒绝服务攻击时，打印的警告信息格式如下：

```
%NFPP_DHCPV6_GUARD-4-PORT_ATTACKED: DHCPv6 DoS attack was detected on port Gi4/1. (2009-07-01 13:00:00)
```

发送的 TRAP 报文的数据包含如下描述信息：

```
DHCPv6 DoS attack was detected on port Gi4/1.
```

管理员可以在 **nfpp** 配置模式和接口配置模式下进行配置。

命令	作用
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#nfpp**	进入 NFPP 配置模式。
Ruijie(config-nfpp)**#dhcpv6-guard rate-limit per-port** *pps*	对每个端口的 DHCPv6 报文速度进行限制。 取值范围是 1 到 9999，缺省值为 150 个。
Ruijie(config-nfpp)**#dhcpv6-guard attack-threshold per-port** *pps*	配置攻击阈值，当某个端口的 DHCPv6 报文超过攻击阈值时，记录到日志，发送 TRAP。 取值范围是 1 到 9999，缺省值为 300 个。
Ruijie(config-nfpp)**#end**	退回到特权模式。
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#interface** *interface-name*	进入接口配置模式。
Ruijie(config-if)**#nfpp dhcpv6-guard policy per-port** *rate-limit-pps attack-threshold-pps*	配置局部的限速水线和攻击水线，只在该配置所属端口上生效。 *rate-limit-pps* 是限速水线，取值范围是 1 到 9999。 *attack-threshold-pps* 是攻击水线，取值范围是 1 到 9999。 缺省情况是端口没有自己的限速水线和攻击水线，采用全局的限速水线和攻击水线。
Ruijie(config-if)**#end**	退回到特权模式。
Ruijie**#show nfpp dhcpv6-guard summary**	核对配置参数

Ruijie**#copy running-config startup-config**	保存配置。

基于链路层源 MAC 地址限速优先于基于端口限速处理。

18.7.8 清除受监控主机

已被隔离的主机在一段时间后自动恢复，如果管理员要手动清除该主机，可以在特权模式下用以下命令清除。

命令	作用
Ruijie**#clear nfpp dhcpv6-guard hosts** [**vlan** *vid*] [**interface** *interface-id*] [*mac-address*]	不带参数表示清除所有已被检测到攻击的主机，带参数表示清除符合条件的主机。

18.7.9 查看DHCPv6 抗攻击的配置参数

使用 **show nfpp dhcpv6-guard summary** 查看 DHCP 抗攻击的配置参数：

命令	作用
Ruijie**#show nfpp dhcpv6-guard summary**	查看 DHCP 抗攻击配置参数

下面是一个例子：

```
Ruijie# show nfpp dhcpv6-guard summary
 (Format of column Rate-limit and  Attack-threshold is per-src-ip/per-src-mac/per-port.)
Interface  Status  Isolate-period Rate-limit Attack-threshold
Global      Enable  300             -/5/150     -/10/300
G 0/1       Enable  180             -/6/-       -/8/-
G 0/2       Disable 200             -/5/30     -/10/50

Maximum count of monitored hosts: 1000
Monitor period：300s
```

字段 Interface 为 Global 表示全局配置。

字段 Status 表示是否打开抗攻击功能。

字段 Rate-limit 的格式为（对源 IP 地址的限速水线/对源 MAC 地址的限速水线/端口的限速水线值），字段 Attack-threshold 的显示格式类似。“-”表示没有配置。举例说明：

“-/5/150”表示对源 MAC 地址的限速水线是 5，对每个端口的限速水线是 150。

G 0/1 这一行的字段 Rate-limit 为“-/6/-”，表示端口 G 0/1 对源 MAC 地址的限速水线是 6，没有配置对端口的限速水线。

18.7.10 查看受监控主机的信息

命令	作用
show nfpp dhcpv6-guard hosts statistics	查看受监控主机表的统计信息，包括主机总数、隔离成功的主机数量和隔离失败的主机数量。

show nfpp dhcpv6-guard hosts [vlan *vid*] [**interface** *interface-id*] [*mac-address*]	查看已被检测到攻击的主机。 不带参数表示显示所有已被检测到攻击的主机，带参数则只显示符合条件的主机。

```
Ruijie# show nfpp dhcpv6-guard hosts statistics
success    fail    total
------     ----     -----
100         20        120
```

表示：“总共有 120 台主机被监控，其中 100 台主机隔离成功，20 台主机隔离失败”。

```
Ruijie# show nfpp dhcpv6-guard hosts
If column 1 shows '*', it means "hardware failed to isolate host".
VLAN  interface   MAC address      remain-time(s)
----  --------    -----------      -------------
*1     Gi0/1       0000.0000.0001  110
2      Gi0/2       0000.0000.2222   61
Total: 2 host(s)
```

```
Ruijie# show nfpp dhcpv6-guard hosts vlan 1 interface g 0/1 0000.0000.0001
If column 1 shows '*', it means "hardware failed to isolate host".
VLAN  interface   MAC address      remain-time(s)
---- --------     -----------      -------------
 *1     Gi0/1      0000.0000.0001  110
Total: 1 host(s)
```

上述几个字段分别表示 VLAN 号、端口、IP 地址、MAC 地址，以及隔离剩余时间。

如果某一行的第一列显示“*”， 表示这台主机目前只是软件监控或者硬件因为资源不足而隔离失败。

18.8 ND抗攻击

18.8.1 ND抗攻击简介

ND 的全称是 Neighbor Discovery，翻译成汉语是“邻居发现”，在 IPv6 网络中主要负责地址解析、路由器发现、前缀发现和重定向。邻居发现使用 5 类报文：邻居请求、邻居公告、路由器请求、路由器公告和重定向报文，英语名称分别为 Neighbor Solicitation、Neighbor Advertisement、Router Solicitation、Router Advertisement 和 Redirect，前四类报文的英语缩写分别为 NS、NA、RS 和 RA。下文把邻居发现使用的 5 类报文统称为 ND 报文。

ND snooping 通过监听网络中的 ND 报文，过滤非法的 ND 报文，监听网络中的 IPv6 用户，并将监听到的 IPv6 用户绑定到端口，防止 IPv6 地址盗用。ND snooping 要求把 ND 报文送 CPU，如果 ND 报文的速率很高，会造成对 CPU 的攻击，所以需要实现 ND guard，对 ND 报文进行限速。

ND guard 按用途把 ND 报文分成 3 类：邻居请求和邻居公告为第一类，路由器请求为第二类，路由器公告和重定向报文为第三类。第一类报文用于地址解析；第二类报文用于主机发现网关；路由器公告用于通告网关和前缀，重定向报文用于通告更优的下一跳，都和路由有关系。所以划分到第三类。

目前仅实现基于物理端口识别 ND 报文攻击。可以对三类报文分别配置限速水线和告警水线。当 ND 报文速率超过限速水线时，超限的 ND 报文将被丢弃。当 ND 报文速率超过告警水线时，将打印警告信息，发送 TRAP。

18.8.2 打开ND抗攻击功能

管理员可以在 **nfpp** 配置模式或者接口配置模式下打开 ND 抗攻击功能，缺省情况下就是打开的。

命令	作用
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#nfpp**	进入 NFPP 配置模式。
Ruijie(config-nfpp)**#nd-guard enable**	打开 ND 抗攻击功能，缺省情况下就是打开的。
Ruijie(config-nfpp)**#end**	退回到特权模式。
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#interface** *interface-name*	进入接口配置模式。
Ruijie(config-if)**#nfpp nd-guard enable**	在端口上打开 ND 抗攻击功能，缺省情况是端口没有配置局部开关，采用全局开关。
Ruijie(config-if)**#end**	退回到特权模式。
Ruijie**#show nfpp nd-guard summary**	核对配置参数
Ruijie**#copy running-config startup-config**	保存配置。

18.8.3 基于端口限速和识别攻击

每个端口都有限速水线和攻击阈值，限速水线必须低于攻击阈值。当某个端口的 ND 报文速度超过限速水线时，就丢弃超限 ND 报文。如果某个端口的 ND 报文速度超过攻击阈值，将记录到日志中，发送 TRAP。

ND snooping 把端口划分为非信任端口和信任端口，非信任端口连接主机，信任端口连接网关。由于通常信任端口的流量大于非信任端口的流量，所以信任端口的限速水线应该高于非信任端口的限速水线，开启 ND snooping 功能时，对于信任端口，ND snooping 将通告 ND guard 把端口的三类报文限速水线都设置成每秒 800 个，把攻击水线都设置成每秒 900 个。

ND guard 同等对待 ND snooping 设置的限速水线和管理员配置的限速水线，后配置的值覆盖先配置的值。具体的说，就是：“如果管理员在该端口上先配置限速水线，然后 ND snooping 设置限速水线，那么 ND snooping 设置限速水线覆盖管理员配置的限速水线；如果 ND snooping 先设置限速水线，然后管理员在该端口上配置限速水线，那么管理员配置的限速水线覆盖 ND snooping 设置的限速水线。”

在管理员保存配置的时候，将把 ND snooping 设置的限速水线保存到配置文件中。

ND snooping 设置的攻击水线和管理员配置的攻击水线的关系类似。

当端口遭受邻居请求/公告拒绝服务攻击时，打印的警告信息格式如下：

```
%NFPP_ND_GUARD-4-PORT_ATTACKED: NS-NA DoS attack was detected on port Gi4/1. (2009-07-01 13:00:00)
```

发送的 TRAP 报文的数据包含如下描述信息：

```
NS-NA DoS attack was detected on port Gi4/1.
```

当端口遭受路由器请求拒绝服务攻击时，打印的警告信息格式如下：

```
%NFPP_ND_GUARD-4-PORT_ATTACKED: RS DoS attack was detected on port Gi4/1. (2009-07-01 13:00:00)
```

发送的 TRAP 报文的数据包含如下描述信息：

```
RS DoS attack was detected on port Gi4/1.
```

当端口遭受路由器公告/重定向报文拒绝服务攻击时，打印的警告信息格式如下：

```
%NFPP_ND_GUARD-4-PORT_ATTACKED: RA-REDIRECT DoS attack was detected on port Gi4/1. (2009-07-01 13:00:00)
```

发送的 TRAP 报文的数据包含如下描述信息：

```
RA-REDIRECT DoS attack was detected on port Gi4/1.
```

管理员可以在 **nfpp** 配置模式和接口配置模式下进行配置。

命令	作用
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#nfpp**	进入 NFPP 配置模式。
Ruijie(config-nfpp)**#nd-guard rate-limit per-port** [**ns-na** | **rs** | **ra-redirect**] *pps*	对每个端口的 ND 报文速度进行限制。 取值范围是 1 到 9999，缺省值为 15 个。
Ruijie(config-nfpp)**#nd-guard attack-threshold per-port** [**ns-na** | **rs** | **ra-redirect**] *pps*	配置攻击阈值，当某个端口的 ND 报文超过攻击阈值时，记录到日志，发送 TRAP。 取值范围是 1 到 9999，缺省值为 30 个。
Ruijie(config-nfpp)**#end**	退回到特权模式。
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#interface** *interface-name*	进入接口配置模式。
Ruijie(config-if)**#nfpp nd-guard policy per-port** [**ns-na** | **rs** | **ra-redirect**] *rate-limit-pps attack-threshold-pps*	配置局部的限速水线和攻击水线，只在该配置所属端口上生效。 *rate-limit-pps* 是限速水线，取值范围是 1 到 9999。 *attack-threshold-pps* 是攻击水线，取值范围是 1 到 9999。
Ruijie(config-if)**#end**	退回到特权模式。
Ruijie**#show nfpp nd-guard summary**	核对配置参数
Ruijie**#copy running-config startup-config**	保存配置。

18.8.4 查看ND抗攻击的配置参数

使用 **show nfpp nd-guard summary** 查看 ND 抗攻击的配置参数：

命令	作用
show nfpp nd-guard summary	查看 ND 抗攻击配置参数

下面是一个例子：

```
Ruijie# show nfpp nd-guard summary
（Format of column Rate-limit and  Attack-threshold is NS-NA/RS/RA-REDIRECT.）
Interface  Status  Rate-limit Attack-threshold
Global      Enable  20/5/10     40/10/20
G 0/1       Enable  15/15/15    30/30/30
G 0/2       Disable -/5/30       -/10/50
```

字段 Interface 为 Global 表示全局配置。

字段 Status 表示是否打开抗攻击功能。

字段 Rate-limit 的格式为（对邻居请求/公告的限速水线/对路由器请求的限速水线/对路由器公告/重定向报文的限速水线），字段 Attack-threshold 的显示格式类似。“-”表示没有配置。

举例说明：“-/5/30”表示在端口 G 0/2 上没有配置邻居请求/公告的限速水线，对路由器请求的限速水线是 5，对路由器公告/重定向报文的限速水线是 30。

18.9 自定义抗攻击

18.9.1 自定义抗攻击简介

网络协议种类繁多，仅路由协议就有 OSPF、BGP、RIP 等。各种协议需要在不同设备之间进行报文交互，交互报文必须送 CPU 交由各个协议进行处理，网络设备一运行某种协议，就相当于开了一扇窗口，给了攻击者可趁之机。如果攻击者向网络设备发送大量的协议报文，将会导致设备的 CPU 资源被大量消耗，严重的情况可能导致设备无法正常工作。

考虑到网络协议多种多样，并且在持续发展中，不同的用户环境下需要使用不同的协议。为此，锐捷设备提供了自定义抗攻击的功能，允许用户自定义抗攻击的类型，灵活配置，以满足不同用户环境下的抗攻击需求。

18.9.2 自定义抗攻击策略

管理员可以在 nfpp 配置模式下自定义一种抗攻击类型。自定义抗攻击要求用户必须配置自定义报文的类型、限速水线、攻击水线及如何识别用户这些基本信息。基本信息配置完以后，才能使自定义抗攻击类型生效。

自定义报文的类型可以由以太网链路层类型字段 etype、源 MAC 地址 smac、目的 MAC 地址 dmac、IPv4/v6 协议号 protocol、源 IPv4/v6 地址 sip、目的 IPv4/v6 地址 dip、源传输层端口 sport 和目的传输层端口 dport 这些字段组合而成。

自定义抗攻击必须配置如何对自定义类型报文速率进行分类统计。分类有基于源 IP/VID/端口、基于源 MAC/VID/端口的主机速率统计及基于端口的速率统计，可以是三者的任意组合。并且必须为这些分类配置相应的限速水线及攻击水线。只有配置了分类的限速水线和攻击水线，该分类才会生效。

命令	作用
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#nfpp**	进入 NFPP 配置模式。
Ruijie(config-nfpp)**#define** *name*	配置自定义抗攻击类型名称

Ruijie(config-nfpp-define)# **match** [**etype** *type*] [**src-mac** *smac* [**src-mac-mask** *smac_mask*]] [**dst-mac** *dmac* [**dst-mac-mask** *dst_mask*]] [**protocol** *protocol*] [**src-ip** *sip* [**src-ip-mask** *sip-mask*]] [**src-ipv6** *sipv6* [**src-ipv6-masklen** *sipv6-masklen*]] [**dst-ip** *dip* [**dst-ip-mask** *dip-mask*]] [**dst-ipv6** *dipv6* [**dst-ipv6-masklen** *dipv6-masklen*]][**src-port** *sport*] [**dst-port** *dport*]	配置自定义抗攻击类型需要匹配的报文字段。 **src-mac-mask** 、 **dst-mac-mask** 、 **src-ip-mask** 、 **dst-ip-mask** 默认均为全 1， **src-ipv6-masklen** 、 **dst-ipv6-masklen** 默认为 128。 **protocol** 仅在 **etype** 为 ipv4 或者 ipv6 时才有效；**src-ip**、**dst-ip** 仅在 **etype** 为 ipv4 时有效；**src-ipv6**、**dst-ipv6** 仅在 **etype** 为 ipv6 时有效；**src-port**、**dst-port** 仅在 **protocol** 为 tcp 或者 udp 时有效。
Ruijie(config-nfpp-define)# **global-policy** {**per-src-ip** | **per-src-mac** | **per-port**} *rate-limit-pps attack-threshold-pps*	配置基于主机或者基于端口的限速水线和攻击水线。 **per-src-ip** 表示基于源 IP/VID/端口识别主机进行速率统计。**per-src-mac** 表示基于源 MAC/VID/端口识别主机进行速率统计。 **per-port** 表示基于每个报文接收的物理端口进行速率统计。**per-src-ip**、**per-src-mac** 和 **per-port** 三者至少要配置一个，否则策略无法生效。 **per-src-ip** 仅在 **etype** 为 ipv4 或者 ipv6 时有效。 *rate-limit-pps* 是限速水线，取值范围是 1 到 9999，缺省是不需要进行速率限制。自定义报文超过限速水线后的报文将被丢弃。 *attack-threshold-pps* 是攻击水线，取值范围是 1 到 9999。 缺省是不需要进行速率限制。 攻击水线必须大于或者等于限速水线。
Ruijie**#show nfpp define summary** *name*	核对配置参数
Ruijie**#copy running-config startup-config**	保存配置。

如果要把自定义抗攻击类型删除，在 nfpp 配置模式下执行“**no define** *name*”。删除自定义抗攻击类型将会清除该自定义抗攻击的所有配置，包含全局和端口下的配置，及所有隔离主机及可信主机。

- 自定义抗攻击类型的名字不能重复，match 匹配的字段及值也不能完全相同，也不能与 arp、icmp、dhcp、ip、dhcpv6 抗攻击类型相同。当配置类型重复时，将提示配置失败。
- 当自定义抗攻击类型的 match 字段及值与已存在的抗攻击类型完全一样时，打印提示信息：“%ERROR: the match type and value are the same with define name(已存在的的抗攻击类型名).”，提示管理员配置失败。
- 当 match 配置了 protocol，但 etype 不是 IPv4 或者 IPv6 时，打印提示信息：“%ERROR: protocol is valid only when etype is IPv4(0x0800) or IPv6(0x86dd).”
- 当 match 配置了 src-ip、dst-ip，但 etype 不是 IPv4 时，打印提示信息：“%ERROR: IP address is valid only when etype is IPv4(0x0800).”
- 当 match 配置了 src-ipv6、dst-ipv6，但 etype 不是 IPv6 时，打印提示信息：“%ERROR: IPv6 address is valid only when etype is IPv6(0x86dd).”
- 当 match 配置了 src-port、dst-port，但 protocol 不是 TCP 或者 UDP 时，打印提示信息：“%ERROR: Port is valid only when protocol is TCP(6) or UDP(17).”

18.9.3 常用自定义抗攻击策略

下面列出一些常用的网络协议对应的抗攻击策略。其中对应的限速水线与攻击水线能满足大部分网络应用场景需求，仅供参考。网络管理员应该根据实际应用场景配置有效的限速水线与攻击水线。

协议名	match	policy per-src-ip	policy per-src-mac	policy per-port
RIP	etype 0x0800 protocol 17 dst-port 520	rate-limit 100 attatch-threshold 150	不适用本策略	rate-limit 300 attatch-threshold 500
RIPng	etype 0x86dd protocol 17 dst-port 521	rate-limit 100 attatch-threshold 150	不适用本策略	rate-limit 300 attatch-threshold 500
BGP	etype 0x0800 protocol 6 dst-port 179	rate-limit 1000 attatch-threshold 1200	不适用本策略	rate-limit 2000 attatch-threshold 3000
BPDU	dst-mac 0180.c200.0000	不适用本策略	rate-limit 20 attatch-threshold 40	rate-limit 100 attatch-threshold 100
RERP	dst-mac 01d0.f800.0001	不适用本策略	rate-limit 20 attatch-threshold 40	rate-limit 100 attatch-threshold 100
REUP	dst-mac 01d0.f800.0007	不适用本策略	rate-limit 20 attatch-threshold 40	rate-limit 100 attatch-threshold 100
BGP	etype 0x0800 protocol 6 dst-port 179	不适用本策略	不适用本策略	不适用本策略
OSPFv2	etype 0x0800 protocol 89	rate-limit 800 attatch-threshold 1200	不适用本策略	rate-limit 2000 attatch-threshold 3000
OSPFv3	etype 0x86dd protocol 89	rate-limit 800 attatch-threshold 1200	不适用本策略	rate-limit 2000 attatch-threshold 3000
VRRP	etype 0x0800 protocol 112	rate-limit 64 attatch-threshold 100	不适用本策略	rate-limit 1024 attatch-threshold 1024
IPv6 VRRP	etype 0x86dd protocol 112	rate-limit 64 attatch-threshold 100	不适用本策略	rate-limit 1024 attatch-threshold 1024
SNMP	etype 0x0800 protocol 17 dst-port 161	rate-limit 1000 attatch-threshold 1200	不适用本策略	rate-limit 2000 attatch-threshold 3000
RSVP	etype 0x0800 protocol 46	rate-limit 800 attatch-threshold 1200	不适用本策略	rate-limit 1200 attatch-threshold 1500

LDP (UDP hello)	etype 0x0800 protocol 17 dst-port 646	rate-limit 10 attatch-threshold 15	不适用本策略	rate-limit 100 attatch-threshold 150

自定义抗攻击为了最大限度地包含已有的协议类型，同是便于新的协议类型的扩展，开放允许用户自由组合报文的类型字段。若是配置不当，则可能导致网络出现异常。因此要求网络管理员对网络协议有较好的掌握。常用自定义抗攻击策略列出了当前已知协议的有效配置，管理员可参照进行配置。对于表中未列出的其它协议，需要谨慎配置使用。

18.9.4 设置对攻击者的隔离时间

对攻击者的隔离时间默认为 0，即不对攻击者进行隔离。

命令	作用
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#nfpp**	进入 NFPP 配置模式
Ruijie(config-nfpp)**#define** *name*	进入自定义抗攻击配置模式
Ruijie(config-nfpp)**#isolate-period** {*seconds* | **permanent**}	配置对攻击者的隔离时间。 取值范围为 0 秒，30 秒到 86400 秒（即一天），缺省值为 0 秒，表示不隔离；**permanent** 表示永久隔离。
Ruijie(config-nfpp)**#end**	退回到特权模式。
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#interface** *interface-name*	进入接口配置模式。
Ruijie(config-if)**# nfpp define name isolate-period** {*seconds* | **permanent**}	在端口上配置对攻击者的隔离时间。 取值范围为 0 秒，180 秒到 86400 秒（即一天），缺省情况是没有配置局部隔离时间，采用全局隔离时间。0 秒表示不隔离；**permanent** 表示永久隔离。
Ruijie(config-if)**#end**	退回到特权模式。
Ruijie**#show nfpp define summary** *name*	核对配置参数
Ruijie**#copy running-config startup-config**	保存配置。

如果要把全局隔离时间恢复成缺省值，在 nfpp 自定义抗攻击配置模式执行命令“**no isolate-period**”。如果一个端口原来配置了局部隔离时间，现在想采用全局隔离时间，那么在接口配置模式下执行命令“**no nfpp define** *name*(自定义抗攻击名字**) isolate-period**”把局部隔离时间配置删除。

配置了隔离时间就是打开了 NFPP 硬件隔离功能，若有用户攻击则会消耗硬件表项资源，与其它安全功能（如 Web 认证、端口安全等）进行硬件资源的竞争。因此配置隔离时间将会打印如下日志提醒管理员：

```
%NFPP-4-RESOURCE_COMPETITION: NFPP isolation will compete for hardware resources with other security features.
```

18.9.5 设置对攻击者的监控时间

如果隔离时间为 0（即不隔离），防攻击模块将自动根据配置的监控时间对攻击者进行软件监控，提供当前系统中存在哪些攻击者的信息。当把隔离时间配置成非零值后，防攻击将自动对软件监控的主机采取硬件隔离。

命令	作用

Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#nfpp**	进入 NFPP 配置模式
Ruijie(config-nfpp)**#define** *name*	进入自定义抗攻击配置模式
Ruijie(config-nfpp)**# monitor-period** *seconds*	配置对攻击者的监控时间。 取值范围为 180 秒到 86400 秒（即一天），缺省值为 600 秒。
Ruijie(config-nfpp)**#end**	退回到特权模式。
Ruijie**#show nfpp define summary** *name*	核对配置参数
Ruijie**#copy running-config startup-config**	保存配置。

如果要把监控时间恢复成缺省值，在 nfpp 自定义配置模式执行命令“**no monitor-period**”。

检测出攻击者的时候，如果隔离时间为 0，将对攻击者进行软件监控，超时为监控时间。在软件监控过程中，当隔离时间被配置为非零值时，将自动对软件监控的攻击者采取硬件隔离，并且把超时设置为隔离时间。监控时间在隔离时间为 0 的情况下才有意义。

如果把隔离时间从非零值改成零，将直接把相关端口的攻击者删除，而不是进行软件监控。

18.9.6 设置受监控主机的最大数目

命令	作用
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#nfpp**	进入 NFPP 配置模式。
Ruijie(config-nfpp)**#define** *name*	进入自定义抗攻击配置模式
Ruijie(config-nfpp)**#monitored-host-limit** *number*	配置受监控主机的最大数目。 取值范围为 1 到 4294967295，缺省情况下受监控主机的最大数目为 1000 个。
Ruijie(config-nfpp)**#end**	退回到特权模式。
Ruijie**#show nfpp define summary** *name*	核对配置参数
Ruijie**#copy running-config startup-config**	保存配置。

如果要把配置的最大受监控主机数恢复成缺省值，在 nfpp 自定义配置模式执行命令“**no monitored-host-limit**”。

如果受监控主机数已经达到默认的 1000 个，此时管理员把受监控主机的最大数目设置成小于 1000，不会删除已有的受监控主机，而是打印信息“%ERROR：The value that you configured is smaller than current monitored hosts 1000（配置的受监控主机数），please clear a part of monitored hosts.”来提醒管理员配置没有生效，需要删除部分已经被监控的主机。

当受监控主机表满时，打印日志“% NFPP_DEFINE_GUARD-4-SESSION_LIMIT：Attempt to exceed limit of name(自定义抗攻击类型名字)'s 1000（配置的受监控主机数） monitored hosts.”提醒管理员。

18.9.7 设置不监控的可信主机

如果管理员希望对某台主机不进行监控，即对该主机表示信任，则可以通过该命令配置。该可信主机发往 CPU 的 IP 报文将被允许发往 CPU。必须在配置 match 规则后才能添加不监控的可信主机。

命令	作用

Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#nfpp**	进入 NFPP 配置模式
Ruijie(config-nfpp)**#define** *name*	进入 NFPP 自定义抗攻击配置模式
Ruijie(config-nfpp-define)**#trusted-host** {*mac mac_mask* | *ip mask* | *IPv6/prefixlen*}	配置不进行监控的主机。 最多能够配置 500 条。
Ruijie(config-nfpp-define)**#end**	退回到特权模式。
Ruijie**# show nfpp define trusted-host** *name*	查看配置的可信主机
Ruijie**#copy running-config startup-config**	保存配置。

在 nfpp 自定义抗攻击配置模式下，可以使用该命令的 **no** 选项删除一条可信主机表项。使用命令的 **no** 和 **all** 选项可以删除所有可信主机。

例如删除所有可信主机：

```
Ruijie(config-nfpp-define)# no trusted-host all
```

或删除单条可信主机表项：

```
Ruijie(config-nfpp-define)# no trusted-host 1.1.1.1 255.255.255.255
```

- 当还未配置 match 类型时，打印提示信息 “%ERROR: Please configure match rule first.”
- 当添加 IPv4 可信主机，但 match 规则的 etype 不为 IPv4 时，打印提示信息 “%ERROR: Match type can’t support IPv4 trusted host.”
- 当添加 IPv6 可信主机，但 match 规则的 etype 不为 IPv6 时，打印提示信息 “%ERROR: Match type can’t support IPv6 trusted host.”
- 当不监控的可信主机表满时，打印提示信息 “％ERROR: Attempt to exceed limit of 500 trusted hosts.” 提醒管理员。
- 当受监控主机表中存在与可信主机相匹配的表项（IP 地址相同）时，系统将自动删除此 IP 地址对应的表项。
- 当删除可信主机失败时，打印提示信息 “％ERROR: Failed to delete trusted host 1.1.1.0 255.255.255.0（配置的可信主机）.” 提醒管理员。
- 当添加可信主机失败时，打印提示信息 “％ERROR: Failed to add trusted host 1.1.1.0 255.255.255.0（配置的可信主机）.” 提醒管理员。
- 当添加的可信主机已经存在时，打印提示信息 “％ERROR: Trusted host 1.1.1.0 255.255.255.0（配置的可信主机）has already been configured.” 提醒管理员。
- 当要删除的可信主机不存在时，打印提示信息 “％ERROR: Trusted host 1.1.1.0 255.255.255.0（配置的可信主机）is not found.” 提醒管理员。
- 当无法为可信主机分配内存时，打印提示信息 “％ERROR: Failed to allocate memory.” 提醒管理员。

18.9.8 基于主机限速和识别攻击

识别主机的方法根据配置的抗攻击策略而定，包含源 IP 地址/VID/端口(per-src-ip)识别主机和源 MAC/VID/端口(per-src-mac)识别主机，两种方法可以同时生效，也可以都不生效。识别主机的方法是否生效的依据是用户是否配置了该方法的限速水线和攻击水线。每台主机都有限速水线和攻击阈值（也称为告警水线），限速水线必须低于攻击阈值。当单台主机的自定义类

型报文速度超过限速水线时，就丢弃超限的自定义类型报文。如果单台主机的自定义类型报文速度超过攻击阈值，将采取隔离措施，记录到日志中，发送 TRAP。

当检测到攻击行为时，打印的日志信息格式如下：

```
%NFPP_DEFINE_GUARD-4- DOS_DETECTED: Host<IP=1.1.1.1,MAC= N/A,port=Gi4/1,VLAN=1> was detected by name(自定义抗攻击名字). (2009-07-01 13:00:00)
```

发送的 TRAP 报文的数据中包含如下描述信息：

```
name(自定义抗攻击名字) DoS attack from host<IP=1.1.1.1,MAC= N/A,port=Gi4/1,VLAN=1> was detected.
```

如果管理员把隔离时间配置成非零值，当硬件隔离成功时，打印的日志信息格式如下所示：

```
%NFPP_DEFINE_GUARD-4-ISOLATED:Host<IP=1.1.1.1, MAC= N/A ,port=Gi4/1,VLAN=1> was isolated by name(自定义抗攻击名字). (2009-07-01 13:00:00)
```

发送的 TRAP 报文的数据包含如下描述信息：

```
Host<IP=1.1.1.1,MAC=N/A,port=Gi4/1,VLAN=1> was isolated by name(自定义抗攻击名字).
```

当硬件隔离失败（原因通常是内存不足或者硬件资源不足）时，打印的日志信息格式如下所示：

```
%NFPP_DEFINE_GUARD-4-ISOLATE_FAILED:Failed to isolate host<IP=1.1.1.1, MAC= N/A ,port=Gi4/1,VLAN=1> by name(自定义抗攻击名字).(2009-07-01 13:00:00)
```

发送的 TRAP 报文的数据包含如下描述信息：

```
Failed to isolate host<IP=1.1.1.1,MAC= N/A,port=Gi4/1,VLAN=1> by name(自定义抗攻击名字).
```

管理员可以在 **nfpp** 自定义配置模式下和接口配置模式下进行配置。

命令	作用
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#nfpp**	进入 NFPP 配置模式。
Ruijie(config-nfpp)**#define** *name*	进入 nfpp 自定义抗攻击配置模式
Ruijie(config-nfpp-define)# **global-policy** {**per-src-ip** | **per-src-mac**} *rate-limit-pps attack-threshold-pps*	配置基于主机的限速和攻击水线。 **per-src-ip** 表示基于源 IP/VID/端口识别主机进行速率统计。**per-src-mac** 表示基于源 MAC/VID/端口识别主机进行速率统计。 *rate-limit-pps* 是限速水线，取值范围是 1 到 9999，缺省是不需要进行速率限制。自定义报文超过限速水线后的报文将被丢弃。 *attack-threshold-pps* 是攻击水线，取值范围是 1 到 9999。自定义报文超过攻击水线，将会认为存在攻击，打印日志，发送 trap，并根据配置的隔离时间对用户进行隔离。 缺省是不需要进行速率限制。 攻击水线必须大于或者等于限速水线。
Ruijie(config-nfpp)**#end**	退回到特权模式。

Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#interface** *interface-name*	进入接口配置模式。
Ruijie(config-if)**#nfpp define** *name* **policy** {**per-src-ip** | **per-src-mac**} *rate-limit-pps attack-threshold-pps*	配置局部的限速水线和攻击水线，只在该配置所属端口上生效。 **per-src-ip** 表示基于源 IP/VID/端口识别主机进行速率统计。**per-src-mac** 表示基于源 MAC/VID/端口识别主机进行速率统计。 *rate-limit-pps* 是限速水线，取值范围是 1 到 9999，缺省是不需要进行速率限制。自定义报文超过限速水线后的报文将被丢弃。 *attack-threshold-pps* 是攻击水线，取值范围是 1 到 9999。自定义报文超过攻击水线，将会认为存在攻击，打印日志，发送 trap，并根据配置的隔离时间对用户进行隔离。 缺省是使用全局配置的限速水线和攻击水线。 攻击水线必须大于或者等于限速水线。
Ruijie(config-if)**#end**	退回到特权模式。
Ruijie**#show nfpp define summary** *name*	核对配置参数
Ruijie**#copy running-config startup-config**	保存配置。

- 基于源 MAC/VID/端口的限速优先级高于基于源 IP/VID/端口的限速。
- 自定义抗攻击的端口识别主机策略要与全局的保持一致。
- 若全局没配置 per-src-ip 策略，端口配置 per-src-ip 策略时，打印提示“%ERROR: name(自定义抗攻击名字) has not per-src-ip policy.”，提醒管理员配置失败。
- 若全局没配置 per-src-mac 策略，端口配置 per-src-mac 策略时，打印提示“%ERROR: name(自定义抗攻击名字) has not per-src-mac policy.”，提醒管理员配置失败。
- 当无法为检测到的攻击者分配内存时，打印日志“%NFPP_DEFINE_GUARD-4-NO_MEMORY: Failed to allocate memory.”提醒管理员。

18.9.9 基于端口限速和识别攻击

抗攻击策略可以设置端口的限速水线和攻击阈值，限速水线必须低于攻击阈值。当某个端口的自定义类型报文速度超过限速水线时，就丢弃超限的自定义类型报文。如果某个端口的自定义类型报文速度超过攻击阈值，将记录到日志中，发送 TRAP。

当端口遭受 ARP 拒绝服务攻击时，打印的警告信息格式如下：

```
%NFPP_DEFINE_GUARD-4-PORT_ATTACKED: name(自定义抗攻击名字) DoS attack was detected on port Gi4/1.
(2009-07-01 13:00:00)
```

发送的 TRAP 报文的数据包含如下描述信息：

```
name(自定义抗攻击名字) DoS attack was detected on port Gi4/1.
```

管理员可以在 **nfpp** 自定义配置模式下和接口配置模式下进行配置。

命令	作用

Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#nfpp**	进入 NFPP 配置模式。
Ruijie(config-nfpp)**#define** *name*	进入 nfpp 自定义抗攻击配置模式
Ruijie(config-nfpp-define)# **global-policy per-port** *rate-limit-pps attack-threshold-pps*	配置基于主机的限速和攻击水线。 **per-port** 表示基于每个报文接收的物理端口进行速率统计。 *rate-limit-pps* 是限速水线，取值范围是 1 到 9999，缺省是不需要进行速率限制。自定义报文超过限速水线后的报文将被丢弃。 *attack-threshold-pps* 是攻击水线，取值范围是 1 到 9999。自定义报文超过攻击水线，将会认为存在攻击，打印日志，发送 trap，并根据配置的隔离时间对用户进行隔离。 缺省是使用全局配置的限速水线和攻击水线。 攻击水线必须大于或者等于限速水线。
Ruijie(config-nfpp)**#end**	退回到特权模式。
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#interface** *interface-name*	进入接口配置模式。
Ruijie(config-if)**#nfpp define** *name* **policy per-port** *rate-limit-pps attack-threshold-pps*	配置局部的限速水线和攻击水线，只在该配置所属端口上生效。 **per-port** 表示基于每个报文接收的物理端口进行速率统计。 *rate-limit-pps* 是限速水线，取值范围是 1 到 9999，缺省是不需要进行速率限制。自定义报文超过限速水线后的报文将被丢弃。 *attack-threshold-pps* 是攻击水线，取值范围是 1 到 9999。自定义报文超过攻击水线，将会认为存在攻击，打印日志，发送 trap。 缺省是不需要进行速率限制。 攻击水线必须大于或者等于限速水线。
Ruijie(config-if)**#end**	退回到特权模式。
Ruijie**#show nfpp define summary** *name*	核对配置参数
Ruijie**#copy running-config startup-config**	保存配置。

基于主机的限速优先级高于基于端口限速。

若自定义抗攻击全局没配置 per-port 策略，端口配置 per-port 策略时，打印提示“%ERROR: name(自定义抗攻击名字) has not per-port policy.”，提醒管理员配置失败。

18.9.10 应用自定义抗攻击功能

管理员可以在 **nfpp** 配置模式或者接口配置模式下应用自定义抗攻击功能，缺省情况下是关闭的。

命令	作用
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#nfpp**	进入 NFPP 配置模式。

Ruijie(config-nfpp)# **define** *name* **enable**	全局打开自定义抗攻击功能。默认情况下所有端口都打开自定义抗攻击功能。
Ruijie(config-nfpp)**#end**	退回到特权模式。
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#interface** *interface-name*	进入接口配置模式。
Ruijie(config-if)**#nfpp define** *name* **enable**	在端口上打开自定义抗攻击功能，缺省情况是端口没有配置局部开关，采用全局开关。
Ruijie(config-if)**#end**	退回到特权模式。
Ruijie**#show nfpp define summary** *name*	核对配置参数
Ruijie**#copy running-config startup-config**	保存配置。

如果要关闭抗功能功能，可以在 NFPP 配置模式下执行”**no define** *name* **enable**”命令关闭全局自定义抗攻击功能，或者在接口配置模式下执行”**no nfpp define** *name* **enable**”命令关闭接口下的自定义抗攻击功能。如果想恢复接口配置，使接口使用全局的自定义抗攻击功能开关，需要在接口配置模式下执行”**default nfpp define** *name* **enable**”。

- 当自定义抗攻击策略还没配置完全时，无法打开自定义抗攻击功能，并提示用户缺少相应的策略配置。
- 当自定义抗攻击名字不存在时，打印提示信息：“%ERROR: The name is not exist.”。
- 当自定义抗攻击未配置 match 类型时，打印提示信息：“%ERROR: name（自定义抗攻击类型名字）doesn’t match any type.”
- 当自定义抗攻击未配置 policy 策略时，打印提示信息：“%ERROR: name（自定义抗攻击类型名字）doesn’t specify any policy.”

18.9.11 清除受监控主机

已被隔离的主机在一段时间后自动恢复，如果管理员要手动清除该主机，可以在特权模式下用以下命令清除。

命令	作用
Ruijie# **clear nfpp define hosts** *name* [**vlan** *vid*] [**interface** *interface-id*] [*ip-address*] [*mac-address*] [*ipv6-address*]	带参数表示清除符合条件的主机。

18.9.12 查看自定义抗攻击的配置参数

使用 **show nfpp define summary** 查看自定义抗攻击的配置参数：

命令	作用
show nfpp define summary [*name*]	查看自定义抗攻击配置参数，不带 *name* 表示显示所有自定义抗攻击的配置信息。

下面是一个例子：

```
Ruijie# show nfpp define summary tcp
Define tcp summary:
```

```
match etype 0x800 protocol 6
Maximum count of monitored hosts: 1000
Monitor period: 300s
 (Format of column Rate-limit and  Attack-threshold is per-src-ip/per-src-mac/per-port.)
Interface  Status  Isolate-period Rate-limit Attack-threshold
Global      Enable  300             -/5/150      -/10/300
G 0/1       Enable  180             -/6/-        -/8/-
G 0/2       Disable 200             -/5/30      -/10/50
```

18.9.13 查看受监控主机的信息

命令	作用
show nfpp define hosts *name* **[statistics** | **[[vlan** *vid*] **[interface** *interface-id*] [*ip-address*] [*mac-address*] [*ipv6-address*]]]	查看已被检测到攻击的主机。 不带参数表示显示所有已被检测到攻击的主机，带参数则只显示符合条件的主机。

下面是一个例子：

```
Ruijie#show nfpp define hosts tcp statistics
Define tcp:
success    fail    total
-------    ----    -----
100         20        120
```

意思是：“总共有 120 台主机被隔离，其中 100 台主机隔离成功，20 台主机隔离失败”。

```
Ruijie#show nfpp define hosts tcp
Define tcp:
If column 1 shows '*', it means "hardware do not isolate host".
VLAN  interface    IP address  remain-time(s)
----    --------   ---------    -------------
1      Gi0/1          1.1.1.1      110
*2      Gi0/2          1.1.2.1      61
Total: 2 host(s)
```

上述几个字段分别表示 VLAN 号、端口、IP 地址、MAC 地址，以及隔离剩余时间。

如果某一行的第一列显示“*”， 表示这台主机目前只是软件监控或者硬件因为资源不足而隔离失败。当 etype 为 IPv6 时，对于基于源 IP 的主机隔离用户将以 IPv6 地址形式显示，基于源 MAC 的主机隔离用户将以 MAC 地址形式显示。

18.9.14 查看不监控的可信主机

使用 **show nfpp define trusted-host** 查看不受监控的可信主机：

命令	作用
show nfpp define trusted-host *name*	查看不受监控的可信主机。

下面是一个例子：

```
Ruijie# show nfpp define trusted-host tcp
Define tcp:
IP address      mask
---------       ------
1.1.1.0         255.255.255.0
1.1.2.0         255.255.255.0
Total：2 record(s)
```

18.10 NFPP日志信息

18.10.1 NFPP日志信息简介

当 NFPP 检测到攻击后，在专用日志缓冲区生成一条日志。NFPP 以一定速率从专用缓冲区取出日志，生成系统消息，并且从专用日志缓冲区清除这条日志。

18.10.2 配置日志缓冲区容量

管理员可以在 **nfpp** 配置模式下配置日志缓冲区的容量。

命令	作用
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#nfpp**	进入 NFPP 配置模式。
Ruijie(config-nfpp)**# log-buffer entries** *number*	配置 NFPP 日志缓冲区大小（范围 0-1024），单位是日志条数，缺省值为 256。
Ruijie(config-nfpp)**#end**	退回到特权模式。
Ruijie**# show nfpp log summary**	核对配置参数。

18.10.3 配置生成系统消息的速率

管理员可以在 **nfpp** 配置模式下配置生成系统消息的速率。

命令	作用
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#nfpp**	进入 NFPP 配置模式。

Ruijie(config-nfpp)# **log-buffer logs** *number_of_message* **interval** *length_in_seconds*	配置从专用日志缓冲区取日志生成系统消息的速率。生成系统消息的速率为 *number_of_message* */length_in_seconds*，生成系统消息的同时还会删除专用缓冲区中的对应信息 *number_of_message*，缺省值为 1，范围为 0-1024，0 表示日志全部记录在专用缓冲区，不生成系统消息。 *length_in_seconds*，缺省值为 30，范围为 0-86400s（1 天），0 表示日志立即生成系统消息。 *number_of_message* 和 *length_in_seconds* 都为 0 表示日志立即生成系统消息。
Ruijie(config-nfpp)**#end**	退回到特权模式。
Ruijie**# show nfpp log summary**	核对配置参数。

18.10.4 配置日志过滤

管理员可以对日志进行过滤，只记录指定 VLAN 或指定端口的日志信息。

命令	作用
Ruijie**#configure terminal**	进入全局配置模式。
Ruijie(config)**#nfpp**	进入 NFPP 配置模式。
Ruijie(config-nfpp)# **logging vlan** *vlan-range*	指定需要记录哪些 VLAN 的日志。 缺省情况是所有日志都记录。
Ruijie(config-nfpp)# **logging interface** *interface-id*	指定需要记录哪个端口的日志。 缺省情况是所有日志都记录。
Ruijie(config-nfpp)**#end**	退回到特权模式。
Ruijie**# show nfpp log summary**	核对配置参数。

18.10.5 清除日志

命令	作用
clear nfpp log	清空日志缓冲区。

18.10.6 显示日志

命令	作用
show nfpp log summary	查看 NFPP 日志信息配置。
show nfpp log buffer [**statistics**]	显示 NFPP 的日志缓冲区。 带参数 statistics 表示显示日志缓冲区中的日志条数。

查看 NFPP 日志信息配置。

```
Ruijie#show nfpp log summary
Total log buffer size : 10
```

```
Syslog rate : 1 entry per 2 seconds
Logging:
VLAN  1-3, 5
interface Gi 0/1
interface Gi 0/2
```

查看 NFPP 日志缓冲区中日志条数。

```
Ruijie#show nfpp log buffer statistics
There are 6 logs in buffer.
```

查看 NFPP 的日志缓冲区。

```
Ruijie#show nfpp log buffer
Protocol VLAN  Interface IP address MAC address     Reason          Timestamp
-------- ----  --------- ---------- -----------     ------          ---------
ARP    1      Gi0/1       1.1.1.1      -             DoS             2009-05-30 16:23:10
ARP    1      Gi0/1       1.1.1.1      -             ISOLATED        2009-05-30 16:23:10
ARP    1      Gi0/1       1.1.1.2      -             DoS             2009-05-30 16:23:15
ARP    1      Gi0/1       1.1.1.2      -             ISOLATE_FAILED 2009-05-30 16:23:15
ARP    1      Gi0/1       -          0000.0000.0001  SCAN            2009-05-30 16:30:10
ARP    -      Gi0/2       -          -                 PORT_ATTACKED   2009-05-30 16:30:10
```

Protocol 有以下取值：

- ARP（对应 ARP 抗攻击）
- IP（对应 IP 防扫描）
- ICMP（对应 ICMP 抗攻击）
- DHCP（对应 DHCP 抗攻击）
- DHCPv6（对应 DHCPv6 抗攻击）
- NS-NA（对应 ND 抗攻击中的邻居请求和邻居公告）
- RS（对应 ND 抗攻击中的路由器请求）
- RA-REDIRECT（对应 ND 抗攻击中的路由器公告和重定向报文）
- name (自定义抗攻击的名称)

Reason 表示原因，有 5 种取值：

- DoS 表示检测到拒绝服务攻击
- ISOLATED 表示攻击者被硬件成功地隔离
- ISOLATE_FAILED 表示隔离攻击者失败
- SCAN 表示检测到扫描

- PORT_ATTACKED 表示端口被攻击

当日志缓冲区溢出时，后续的日志将被丢弃，同时在日志缓冲区中显示一条所有属性都为"-"的表项。管理员需要增加日志缓冲区容量或者提高生成系统消息的速率。

从日志缓冲区取日志生成的系统消息带有事件发生的时间戳，如下所示：

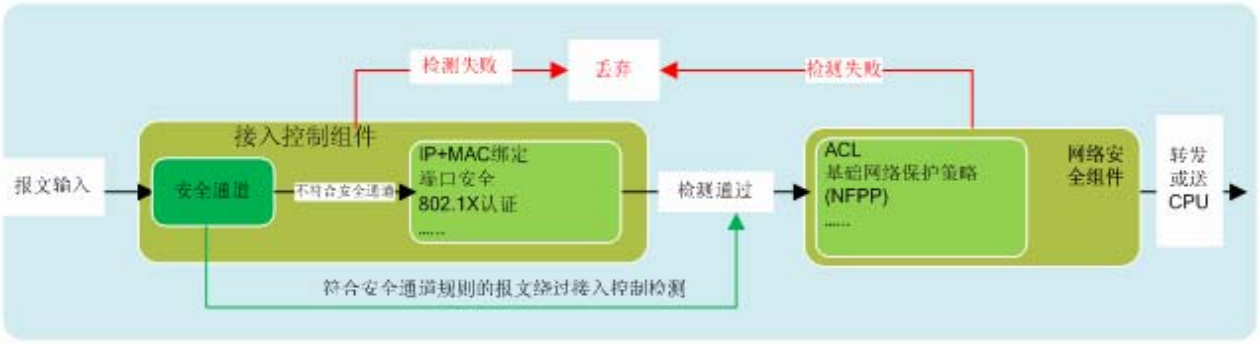
%NFPP_ARP_GUARD-4-DOS_DETECTED: Host<IP=N/A,MAC=0000.0000.0004,port=Gi4/1,VLAN=1> was detected.(2009-07-01 13:00:00)

19 锐捷交换机安全功能兼容模式

19.1 锐捷交换机安全功能概述

随着业务应用的扩展，用户对网络安全的要求越来高，对安全功能的差异性需求越来越苛刻。锐捷以太网交换机产品系列为用户提供了丰富的安全功能来满足用户的不同要求。锐捷交换机的安全功能从逻辑上分成两部分:接入控制组件、网络安全组件。报文进入交换机先经过接入控制组件的检查，然后进入网络安全组件的检查，如果都合法，进入后续的处理（参见下图）。

图 19-1 锐捷交换机安全功能转发示意



19.2 锐捷交换机安全功能基本概念

19.2.1 接入控制组件

接入控制组件包含：

- 安全通道：安全通道也称为逃生通道，符合安全通道规则的报文跳过接入组件的安全检查，直接进入后续网络安全组件的检查；
- 全局 IP 和 MAC 绑定：要求报文符合全局 IP+MAC 绑定的报文才可以通过，否则被丢弃；
- 端口安全：要求符合端口安全地址的报文通过，如果存在安全地址和 IP 绑定，必须是同时符合绑定的安全地址报文才可以通过；
- 802.1X 认证：要求通过认证的报文转发；
- IP Source Guard：要求符合 IP Source Guard 绑定的报文转发；
- ARP Check：存在全局 IP 和 MAC 绑定/端口安全绑定/802.1X 授权绑定/GSN 绑定/IP Souce Guard 的 IPV4 绑定时，如果 ARP Check 开启，则必须同时符合 IP+MAC 绑定的 ARP 报文才可以转发；

以上组件的详细配置指南请参照相应功能的配置章节。

19.2.2 网络安全组件

网络安全组件包含：

- 防网关 ARP 欺骗：符合防网关 ARP 欺骗设置的 ARP 报文直接被丢弃；
- 基础网络保护策略(NFPP)：符合 NFPP 保护的报文直接被丢弃；
- 防源 IP 欺骗：主要指源 IP 检查，只有合法的源 IP 报文才允许转发；
- CPP：CPU Protect Policy，CPU 保护策略，通过报文识别、报文带宽控制、报文优先级队列映射以及队列调度等技术对送往交换机处理器的报文进行处理，实现交换机处理器资源保护以及重要报文保障。
- ACL：符合 ACL Pemit 的报文被转发，符合 ACL Deny 的报文被丢弃；
- 多播源 IP/源端口检查：符合多播源 IP/源端口检查的报文被转发，不符合的报文被丢弃；

以上组件的详细配置指南请参照相应功能的配置章节。

19.2.3 安全功能兼容模式

锐捷交换机的接入控制组件内部各功能，网络安全组件内部各功能，接入控制组件和网络安全组件以两种形式共存：RGOS 兼容模式共存和 RGOS 非兼容模式共存，缺省情况下，共存的形式为 RGOS 兼容模式。

- RGOS 兼容模式共存：

☑ 转发面上，接入控制组件和安全 ACL 共用时，安全 ACL 的 Pemit 和 Deny 同时生效；控制面上，除 DHCP 报文外其他所有符合 CPP 的报文都必须通过接入组件和网络安全组件的检测。

- RGOS 非兼容模式共存：

☑ 转发面上，接入控制组件和安全 ACL 共用时，安全 ACL 的 Pemit 和 Deny 同时生效；控制面上，所有符合 CPP 的报文都必须通过接入组件和网络安全组件的检测。

19.2.4 锐捷交换机安全功能兼容模式工作原理

锐捷交换机安全功能共存的兼容模式以 RGOS 兼容和 RGOS 非兼容两种模式的形式存在。缺省情况下，为 RGOS 兼容模式。设置 **no security-mode compatible** 命令并保存配置重启，安全功能共存的兼容模式切换成 RGOS 非兼容模式。反之，设置 **security-mode compatible** 命令并保存配置重启，安全共存的兼容模式切换成 RGOS 兼容模式。

19.3 安全功能兼容模式的缺省配置

下表用来描述安全功能兼容模式的缺省配置。

功能特性	缺省值
安全功能以 RGOS 兼容模式共存	开启

19.4 配置安全功能兼容模式

缺省情况下，锐捷交换机的安全功能共存方式为 RGOS 兼容模式共存，进入特权模式，按以下步骤设置安全功能的共存模式：

命令	作用
Ruijie**# configure terminal**	进入全局配置模式
Ruijie(config)**# security-mode compatible**	设置安全功能共存模式为 RGOS 兼容模式共存，使用 **no security-mode compatible** 设置成 RGOS 非兼容模式共存
Ruijie(config)**# exit**	退出全局配置模式。

请注意，执行命令之后，必须保存配置重启才能使安全兼容模式配置生效。

19.5 查看安全功能兼容模式配置

安全功能兼容模式没有专门的 show 命令来查看当前兼容模式，用户可以通过 **show running-config** 来查看当前的兼容模式，如果是非兼容模式，**show running-confg** 中将会看到到 **no security-mode compatible** 的配置：

命令	作用
show running-config	通过 show running-config 命令查看安全功能兼容模式的配置

配置指南-ACL&QOS

本分册介绍 ACL&QOS 配置指南相关内容，包括以下章节：

1. ACL
2. IP QOS

1 ACL

1.1 访问控制列表概述

作为锐捷产品安全解决方案的一部分，使用访问控制列表提供强大的数据流过滤功能。锐捷产品目前支持多种访问列表。您可以根据网络具体情况选择不同的访问控制列表对数据流进行控制。

1.1.1 访问控制列表简介

ACLs 的全称为接入控制列表(Access Control Lists)，也称为访问列表（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该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。

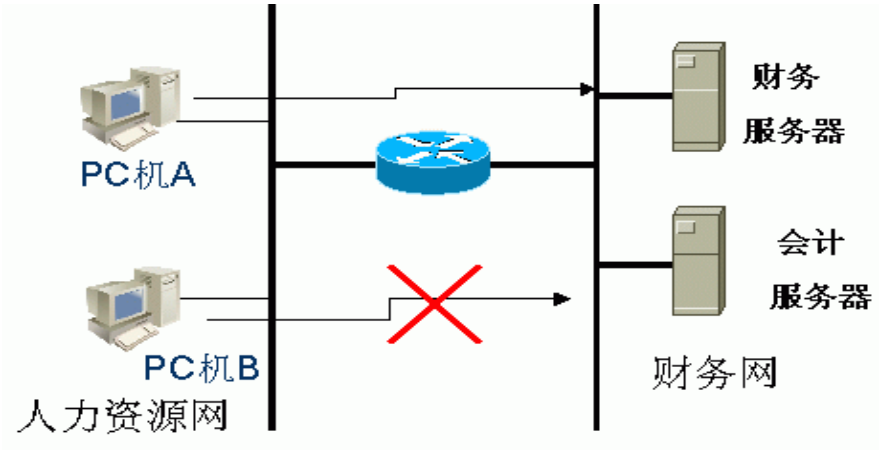
1.1.2 为什么要配置访问列表

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，在该案例中，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。

图 1-1 使用访问列表控制网络访问



1.1.3 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。

1.1.4 输入/输出ACL、过滤域模板及规则

输入 ACL 在设备接口接收到报文时，检查报文是否与该接口输入 ACL 的某一条 ACE 相匹配；输出 ACL 在设备准备从某一个接口输出报文时，检查报文是否与该接口输出 ACL 的某一条 ACE 相匹配。

在制定不同的过滤规则时，多条规则可能同时被应用，也可能只应用其中几条。只要是符合某条 ACE，就按照该 ACE 定义的处理报文(Permit 或 Deny)。ACL 的 ACE 根据以太网报文的某些字段来标识以太网报文的，这些字段包括：

二层字段(Layer 2 Fields)：

- 48 位的源 MAC 地址(必须申明所有 48 位)
- 48 位的目的 MAC 地址(必须申明所有 48 位)
- 16 位的二层类型字段

三层字段(Layer 3 Fields)：

- 源 IP 地址字段(可以申明全部源 IP 地址值，或申明您所定义的子网来定义一类流)
- 目的 IP 地址字段(可以申明全部目的 IP 地址值，或申明您所定义的子网来定义一类流)
- 协议类型字段

四层字段(Layer 4 Fields)：

- 可以申明一个 TCP 的源端口、目的端口或者都申明
- 可以申明一个 UDP 的源端口、目的端口或者都申明

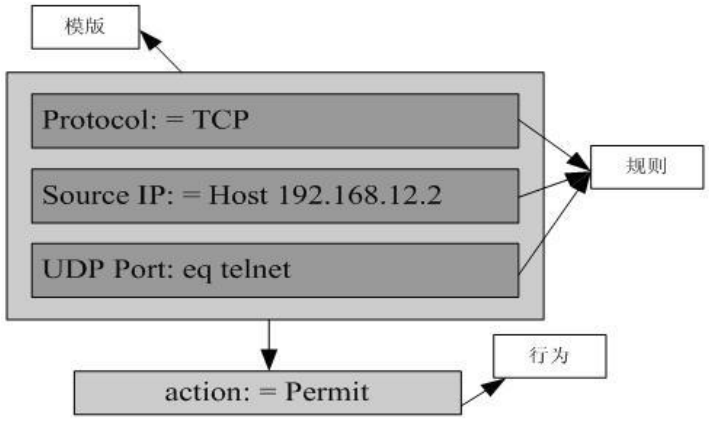
过滤域指的就是您在生成一条 ACE 时，根据报文中的哪些字段用以对报文进行识别、分类。过滤域模板就是这些字段组合的定义。比如，您在生成某一条 ACE 时希望根据报文的目的 IP 字段对报文进行识别、分类，而在生成另一条 ACE 时，希望根据的是报文的源 IP 地址字段和 UDP 的源端口字段，这样，这两条 ACE 就使用了不同的过滤域模板。

规则(Rules)，指的是 ACE 过滤域模板对应的值。 比如有一条 ACE 内容如下：

```
permit tcp host 192.168.12.2 any eq telnet
```

在这条 ACE 中，过滤域模板为以下字段的集合：源 IP 地址字段、IP 协议字段、目的 TCP 端口字段。对应的值(Rules)分别为：源 IP 地址＝Host 192.168.12.2；IP 协议＝TCP；TCP 目的端口＝Telnet。

图 1-2 对 ACE：permit tcp host 192.168.12.2 any eq telnet 的分析



过滤域模板可以是三层字段(Layer 3 Field)和四层字段(Layer 4 Field)字段的集合，也可以是多个二层字段(Layer 2 Field)的集合，但标准与扩展的 ACL 的过滤域模板不能是二层和三层、二层和四层、二层和三层、四层字段的集合。要使用二层、三层、四层字段集合，可以应用 Expert 扩展访问控制列表（Expert ACLs）。

OUT 方向 ACL 关联 SVI 的注意事项：支持 IP 标准，IP 扩展，MAC 扩展，专家级 ACL 应用。

对 ACL 中匹配目的 IP 和目的 MAC 有一些限制，如果在 MAC 扩展和专家级 ACL 中匹配目的 MAC，将这样的 ACL 应用到 SVI 的 OUT 方向时，表项会被设置，但无法生效。如果想要在 IP 标准，IP 扩展，专家级 ACL 中匹配目的 IP，而目的 IP 不在所关联的 SVI 的子网 IP 范围内时，该配置的 ACL 将无法生效。比如 VLAN 1 的地址为 192.168.64.1 255.255.255.0 现在，创建一条 IP 扩展的 ACL， ace 为 deny udp any 192.168.65.1 0.0.0.255 eq 255，将该 ACL 应用到 VLAN 1 的出口，将无法生效，因为目的 IP 不在 VLAN 1 子网 IP 范围内，如果 ace 为 deny udp any 192.168.64.1 0.0.0.255 eq 255 将可以生效，因为目的 IP 符合规定。

当配置专家级的 ACL，并应用在接口的 out 方向时，如果该 ACL 中的某些 ACE 包含三层匹配信息（比如 IP，L4port 等），将导致从应用接口进入的非 IP 报文无法受该 ACL 的 permit 和 deny 规则控制。

应用 ACL 时，如果 ACL（包括 IP 访问列表和 Expert 扩展访问列表）中的 ACE 匹配了非 L2 字段，比如 SIP，DIP 时，对于带标签的 MPLS 报文匹配是无效的。

1.1.5 ACL logging

为了让用户更好的掌握 ACL 在设备中的运行状态，在添加规则时可以根据需要决定是否指定报文匹配日志输出选项，如果指定了该选项，则在规则匹配到报文时会输出匹配日志信息。ACL logging 信息是基于 ACE 来打印 log 信息的，也即设备周期性的打印命中报文的 ACE 信息，以及该 ACE 命中的报文数量。如下：

```
*Sep  9 16:23:06: %ACL-6-MATCH: ACL 100 ACE 10 permit icmp any any, match 78 packets.
```

为合理控制 log 输出的数量和频率，ACL logging 支持配置 log 输出间隔的配置，并且支持分别配置 IPv4 ACL 和 IPv6 ACL 的 log 输出间隔。

默认 ACL logging 的 log 输出间隔是 0，也即不输出 log。在为 ACE 指定了报文匹配日志输出选项后，若要输出相应的 log，需要配置 ACL logging 的输出间隔。

对于带 ACL logging 选项的 ACE，如果指定的时间间隔内没有匹配到任何报文，则不会输出与该 ACE 有关的报文匹配日志。如果指定的时间间隔内有匹配到报文，则时间间隔到期后，会输出与该 ACE 有关的报文匹配日志。其中的报文命中数目为该时间间隔内该 ACE 匹配到的报文总数，即为该 ACE 上一次输出 log 到本次输出 log 之间命中的报文数。

ACL logging 中的报文匹配计数只会输出安全 ACL 的匹配计数。如果非安全 ACL 如 QoS、PBR 等引用的 ACL 中有 ACE 带有 log 选项，log 选项不会对这些非安全 ACL 起作用，输出的报文匹配日志的计数也不会包含非安全 ACL 的报文匹配计数。

1.1.6 ACL报文匹配计数

由于网络管理的需要，有时用户可能会想知道某条 ACE 有没有匹配到报文，匹配了多少个。因此，ACL 提供了基于 ACE 的报文匹配计数，用户可以基于 ACL 开启和关闭该 ACL 下的所有的 ACE 的报文匹配计数功能，支持的 ACL 类型包括：IP 访问列表、MAC 访问列表、Expert 访问列表和 IPv6 访问列表。此外，用户可通过 ACL 的统计清除命令将 ACL 规则的报文匹配计数器清 0，以便重新统计。

ACL 报文匹配计数只针对安全 ACL，对于非安全 ACL 的报文匹配不会进行计数。

1.2 配置IP访问列表

要在设备上配置访问列表，必须为协议的访问列表指定一个唯一的名称或编号，以便在协议内部能够唯一标识每个访问列表。下表列出了可以使用编号来指定访问列表的协议以及每种协议可以使用的访问列表编号范围。

协议	编号范围
标准 IP	1-99，1300 - 1999
扩展 IP	100-199，2000 - 2699

1.2.1 IP访问列表配置指导

创建访问列表时，定义的规则将应用于设备上所有的分组报文，设备通过判断分组是否与规则匹配来决定是否转发或阻断分组报文。

基本访问列表包括标准访问列表和扩展访问列表，访问列表中定义的典型规则主要有以下：

- 源地址
- 目标地址
- 上层协议
- 时间区域

标准 IP 访问列表（编号为 1 - 99，1300 - 1999）主要是根据源 IP 地址来进行转发或阻断分组的，扩展 IP 访问列表（编号为 100 – 199，2000 - 2699）使用以上四种组合来进行转发或阻断分组的。其他类型的访问列表根据相关代码来转发或阻断分组的。

对于单一的访问列表来说，可以使用多条独立的访问列表语句来定义多种规则，其中所有的语句引用同一个编号或名字，以便将这些语句绑定到同一个访问列表。不过，使用的语句越多，阅读和理解访问列表就越来越困难。

隐含“拒绝所有数据流”规则语句

在每个访问列表的末尾隐含着一条“拒绝所有数据流”规则语句，因此如果分组与任何规则都不匹配，将被拒绝。

如下例：

```
Access-list 1 permit host 192.168.4.12
```

此列表只允许源主机为 192.168.4.12 的报文通过，其它主机都将被拒绝。因为这条访问列表最后包含了一条规则语句：access-list 1 deny any。

又如：

```
Access-list 1 deny host 192.168.4.12
```

如果列表只包含以上这一条语句，则任何主机报文通过该端口时都将被拒绝。

> 在定义访问列表的时候，要考虑到路由更新的报文。由于访问列表末尾“拒绝所有数据流”，可能导致所有的路由更新报文被阻断。

输入规则语句的顺序

加入的每条规则都被追加到访问列表的最后，语句被创建以后，就无法单独删除它，而只能删除整个访问列表。所以访问列表语句的次序非常重要。设备在决定转发还是阻断分组时，设备按语句创建的次序将分组与语句进行比较，找到匹配的语句后，便不再检查其他规则语句。

假设创建了一条语句，它允许所有的数据流通过，则后面的语句将不被检查。

如下例：

```
access-list 101 deny ip any any
access-list 101 permit tcp 192.168.12.0 0.0.0.255  eq  telnet any
```

由于第一条规则语句拒绝了所有的 IP 报文，所以 192.168.12.0/24 网络的主机 Telnet 报文将被拒绝，因为设备在检查到报文和第一条规则语句匹配，便不再检查后面的规则语句。

1.2.2 配置IP访问列表

基本访问列表的配置包括以下两步：

- 定义基本访问列表
- 将基本访问列表应用于特定接口

要配置基本访问列表，有以下两种方式：

方式一　在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)# **access-list** *id* {**deny	permit**} {src *src-wildcard*	**host** *src*	**any** } [**time-range** *tm-rng-name*] [**log**]	定义访问列表
Ruijie(config)# **interface** *interface*	选择要应用访问列表的接口
Ruijie(config-if)# **ip access-group** *id* { **in	out** }	将访问列表应用特定接口

方式二　在 ACL 配置模式下执行以下命令：

命令	作用
Ruijie(config)# **ip access-list** { **standard	extended** } { *id*	*name* }	进入配置访问列表模式
Ruijie (config-xxx-nacl)# [*sn*] { **permit	deny** } {src *src-wildcard*	**host** *src*	**any** } [**time-range** *tm-rng-name*] [**log**]	为 ACL 添加表项,具体内容请参见命令参考
Ruijie(config-xxx-nacl)# **exit**	退出访问控制列表模式
Ruijie(config)# **interface** *interface*	选择要应用访问列表的接口
Ruijie(config-if)# **ip access-group** *id* { **in	out** }	将访问列表应用特定接口

方式一只对数值 ACL 进行配置，方式二可以对命名和数值 ACL 进行配置，还可以指定表项的优先级(在支持 ACE 优先级的设备中)。

1.2.3 显示IP访问列表的配置

要监控访问列表，请在特权用户模式执行以下命令：

命令	作用
show access-lists [*id*	*name*]	可以查看基本访问列表

配置举例：

```
Ruijie #show access-lists
Extended IP access list 101
    10 deny ip any host 11.1.1.2 log (3 matches)
```

```
    20 permit ip any any log (10690 matches)
    30 deny ip host 192.168.21.59 any log (101 matches)
    40 permit tcp host 192.168.21.59 any eq ftp log
50 permit ip host 192.168.21.59 any log
```

1.3 配置MAC扩展访问列表

要在设备上配置 MAC 访问列表，必须给协议的访问列表指定一个唯一的名称或编号，以便在协议内部能够唯一标识每个访问列表。下表列出可以使用编号来指定 MAC 访问列表编号范围。

协议	编号范围
MAC 扩展访问列表	700-799

1.3.1 MAC扩展访问列表配置指导

创建 MAC 访问列表时，定义的规则将可以应用于所有的分组报文，通过判断分组是否与规则匹配来决定是否转发或阻断分组报文。

MAC 访问列表中定义的典型规则主要有以下：

- 源 MAC 地址
- 目标 MAC 地址
- 以太网协议类型
- 时间区

MAC 扩展访问列表（编号 700 -799）主要是根据源和目的 MAC 地址来进行转发或阻断分组的，也可以对以太网协议类型匹配。

对于单一的 MAC 访问列表来说，可以使用多条独立的访问列表语句来定义多种规则，其中所有的语句需引用同一个编号或名字，以便将这些语句绑定到同一个访问列表。

1.3.2 配置MAC扩展访问列表

MAC 访问列表的配置包括以下两步：

- 定义 MAC 访问列表
- 应用列表于特定接口

要配置 MAC 访问列表，有以下两种方式：

方式一，在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)# **access-list** *id* {**deny** | **permit**}{**any** | **host** *src-mac-addr*} {**any** | **host** *dst-mac-addr*} [*ethernet-type*] [**cos** *cos*]	定义访问列表,命令的具体内容请参见命令参考

Ruijie(config)# **interface** *interface*	选择选择要应用访问列表的接口
Ruijie(config-if)# **mac access-group** *id* { **in** | **out** }	将访问列表应用特定接口

方式二，在 ACL 配置模式下执行以下命令：

命令	作用
Ruijie(config)# **mac access-list extended** {*id* | *name*}	进入配置访问列表模式
Ruijie (config-mac-nacl)# [*sn*] { **permit** | **deny** }{**any** | **host** *src-mac-addr*} {**any** | **host** *dst-mac-addr*} [*ethernet-type*] [**cos** *cos*]	为 ACL 添加表项,命令的具体内容请参见命令参考
Ruijie(config-mac-nacl)# **exit**	退出访问控制列表模式
Ruijie(config)# **interface** *interface*	选择要应用访问列表的接口
Ruijie(config-if)# **mac access-group** {*id* | *name*} { **in** | **out**}	将访问列表应用特定接口

方式一只对数值 ACL 进行配置；方式二可以对命名和数值 ACL 进行配置，还可以指定表项的优先级（支持优先级 ACE 产品）。

交换机的 MAC 扩展 ACL 只对非 IP 及非 ARP 报文生效。

1.3.3 显示MAC扩展访问列表的配置

要监控访问列表，请在特权模式执行以下命令：

命令	作用
show access-lists [*id* | *name*]	可以查看基本访问列表

1.4 配置Expert扩展访问列表

要在设备上配置 Expert 扩展访问列表，必须给协议的访问列表指定一个唯一的名称或编号，以便在协议内部能够唯一标识每个访问列表。下表列出 Expert 访问列表的编号范围。

协议	编号范围
Expert 扩展访问列表	2700-2899

1.4.1 Expert扩展访问列表配置指导

创建 expert 扩展访问列表时，定义的规则可以应用于所有的分组报文，通过判断分组是否与规则匹配来决定是否转发或阻断分组报文。

Expert 访问列表中定义的典型规则主要有以下：

- 基本访问列表和 MAC 扩展访问列表所有的信息
- VLAN ID

Expert 扩展访问列表（编号 2700 -2899）为基本访问列表和 MAC 扩展访问列表的综合体，并且能对 VLAN ID 进行过滤。

对于单一的 Expert 访问列表来说，可以使用多条独立的访问列表语句来定义多种规则，其中所有的语句需引用同一个编号或名字，以便将这些语句绑定到同一个访问列表。

1.4.2 配置Expert扩展访问列表

Expert 访问列表的配置包括以下两步：

- 定义 Expert 访问列表
- 应用列表于特定接口(应用特例)

要配置 Expert 访问列表，有以下两种方式

方式一 在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)# **access-list** *id* {**deny** | **permit**} [*prot* |{[*ethernet-type*] [**cos** *cos*]}] [**VID** *vid*] {src *src-wildcard* | **host** *src* } {**host** *src-mac-addr* | **any**} {dst *dst-wildcard* | **host** *dst* | **any**}{**host** *dst-mac-addr*|**any**}] [**precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*] [**fragment**] [**range** *lower upper*] [**time-range** *tm-rng-name*]	定义访问列表,命令的具体内容请参见命令参考
Ruijie(config)# **interface** *interface*	选择选择要应用访问列表的接口
Ruijie(config-if)# **expert access-group** *id* {**in | out** }	将访问列表应用特定接口

方式二， 在 ACL 配置模式下执行以下命令：

命令	作用
Ruijie(config)# **expert access-list extended** {*id* | *name*}	进入配置访问列表模式
Ruijie(config-exp-nacl)# [*sn*]{ **permit** | **deny** }[*prot* | {[*ethernet-type*] [**cos** *cos*]}] [**VID** *vid*]{src *src-wildcard*|**host** *src*}{**host** *src-mac-addr* | **any**} {dst *dst-wildcard* | **host** *dst* | **any**}{**host** *dst-mac-addr* | **any** }] [**precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*] [**fragment**] [**range** *lower upper*] [**time-range** *tm-rng-name*]	为 ACL 添加表项,命令的具体内容请参见命令参考
Ruijie(config-exp-nacl)# **exit**	退出访问控制列表模式
Ruijie(config)# **interface** *interface*	选择要应用访问列表的接口
Ruijie(config-if)# **expert access-group** {*id*|*name*} {**in**|**out**}	将访问列表应用特定接口

方式一只对数值 ACL 进行配置；方式二可以对命名和数值 ACL 进行配置，在支持优先级表项的版本中，还可以指定表项的优先级(命令中[sn]选项)。

对于交换机，专家级扩展 ACL 的非默认 ACE 不明确指定 etype（或为 etype-any）时只针对非 IP_ARP 报文生效，但默认 deny 表项对所有类型报文生效。

1.4.3 显示Expert扩展访问列表的配置

要监控访问列表，请在特权用户模式执行以下命令：

命令	作用
show access-lists [*id*	*name*]	可以查看 Expert 访问列表

1.5 配置IPv6 扩展访问列表

1.5.1 配置IPv6 扩展访问列表

IPv6 访问列表的配置包括以下两步：

- 定义 IPv6 访问列表
- 应用列表于特定接口(应用特例)

要配置基本访问列表，有以下方式，在 ACL 配置模式下执行以下命令：

命令	作用
Ruijie(config)# **ipv6 access-list** *name*	进入配置访问列表模式
Ruijie (config-ipv6-nacl)# [*sn*] {**permit**	**deny** } *prot* {*src-ipv6-prefix/prefix-len*	**host** *src-ipv6-addr*	**any**} {*dst-ipv6-pfix/pfix-len*	**any**	**host** *dst-ipv6-addr*} [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragments**] [**range** lower upper] [**time-range***tm-rng-name*] [**log**]	为 ACL 添加表项,命令的具体内容请参见命令参考
Ruijie(config-exp-nacl)# **exit**	退出访问控制列表模式
Ruijie(config)# **interface** *interface*	选择要应用访问列表的接口
Ruijie(config-if)# **ipv6 traffic-filter** *name* {**in**	**out**}	将访问列表应用特定接口

1.5.2 显示IPv6 扩展访问列表的配置

要监控访问列表，请在特权用户模式执行以下命令：

命令	作用
show access-lists [*name*]	可以查看基本访问列表

配置举例：

```
Ruijie #show access-lists
ipv6 access-list extended v6-list
petmit ipv6 ::192.168.4.11 any (203 matches)
deny any any (1 matches)
```

1.6 其他相关配置

1.6.1 配置TCP Flag过滤控制

TCP Flag 过滤特性提供了一种灵活机制，当前 TCP Flag 过滤控制支持 Match-All 选项，接收到的报文匹配到有 TCP Flag 与 ACL 表项中定义的 TCP Flag 每一位均吻合，就由 ACL 规则来检验，使用者可以定义 TCP Flag 的任意组合，用来过滤某些具有特定 TCP Flag 的报文。当指定 established 选项时，如果接收到的报文中携带的 TCP Flag 带有 rst 或者 ack 标志，就表示符合 established 特征。

例如：

```
permit tcp any any match-all rst
```

允许 TCP Flag RST 置位，其他位为 0 的报文通过。

```
permit tcp any any  established
```

允许 TCP Flag 中的 RST 或 ACK 置位的报文通过，而不管其他位是否被置上。

这种过滤特性可以在命名 ACL，数值 ACL 配置协议号为 TCP 的情况下可选配置。MAC 扩展和 IP 标准没有此项功能。

请按照如下步骤配置 TCP Flag

命令	作用
Ruijie(config)# **ip access-list extended** { *id* | *name* }	进入配置访问列表模式
Ruijie(config-ext-nacl)# [*sn*] {**permit** | **deny**} **tcp** *source source-wildcard* [*operator port*] *destination destination-wildcard [operator port]* [**match-all** *flag-name* | **established**] [**precedence** *precedence*]	为 ACL 添加表项,命令的具体内容请参见命令参考
Ruijie(config-exp-nacl)# **exit**	退出访问控制列表模式，选择要应用访问列表的接口
或	
Ruijie(config)# **interface** *interface*	退出访问控制列表模式，选择要应用访问列表的接口
Ruijie(config-if)# **ip access-group** {*id* | *name*} {**in** | **out**}	将访问列表应用特定接口

下面的例子说明如何配置 TCP Flag

- enable 权限和密码

```
Ruijie> enable
Ruijie#
```

- 进入全局配置模式

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

- 进入 ACL 配置模式

```
Ruijie(config)# ip access-list extended test-tcp-flag
Ruijie(config-ext-nacl)#
```

- 添加 ACL 表项

```
Ruijie(config-ext-nacl)# permit tcp any any match-all rst
Ruijie(config-ext-nacl)# permit tcp host 1.1.1.1 any  established
```

- 添加 deny 表项

```
Ruijie(config-ext-nacl)# deny tcp any any match-all fin
```

- end

```
Ruijie(config-ext-nacl)# end
```

- 显示

```
Ruijie# show  access-list test-tcp-flag
ip access-lists extended test-tcp-flag
10 permit tcp any any match-all rst
20 permit tcp host 1.1.1.1 any established30 deny tcp any any match-all fin
```

1.6.2 按优先级配置ACL表项

为了体现 ACE 的优先级，对每个 ACL 列表提出标准，以规范该 ACL 列表下的 ACE 的编排方式，采用序号的起点-增量方式，具体描述如下：

- ACE 在链表中以序号自小至大方式排列；
- 以起点序号开始，如不指定序号均以前一 ACE 的序号为基础以增量递增。
- 指定序号时将该 ACE 以排序方式插入，增量保证了在两个相邻 ACE 之间能够插入新的 ACE。
- ACL 列表指定序号起点和序号增量。

提供 **ip access-list resequence** {*acl-id*| *acl-name*} *sn-start sn-inc* 命令，相关命令见命令参考。

每运行以上命令，便对 ACL list 下的 ace 重新排列，如名字为 tst_acl 的 ACL 下 ace 序号为：

初始时

```
ace1: 10
ace2: 20
ace3: 30
```

运行 **ip access-list resequence** *tst_acl 100 3*，ACE 的序号如下

```
Ruijie(config)# ip access-list resequence tst_acl 100 3
ace1: 100
ace2: 103
ace3: 106
```

不输入 sn-num 添加 ace4 时，序号如下

```
Ruijie(config-std-nacl)# permit 。。。
ace1: 100
```

```
ace2: 103
ace3: 106
ace4: 109
```

输入 seq-num = 105 添加 ace5 时，序号如下

```
Ruijie(config-std-nacl)# 105 permit 。。。
ace1: 100
ace2: 103
ace5: 105
ace3: 106
ace4: 109
```

序号的引用是为了实现优先级添加 ace 的方式。

删除 ACE

```
Ruijie(config-std-nacl)# no 106
ace1: 100
ace2: 103
ace5: 105
ace4: 109
```

如上序号也可以方便 ACE 的删除。

1.6.3 配置基于时间区的ACL

您可以使 ACL 基于时间运行，比如让 ACL 在一个星期的某些时间段内生效等。为了达到这个要求，您必须首先配置一个 Time-Range。

Time-Range 的实现依赖于系统时钟，如果您要使用这个功能，必须保证系统有一个可靠的时钟。

从特权模式开始，您可以通过以下步骤来设置一个 Time-Range：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **time-range** *time-range-name*	通过一个有意义的显示字符串作为名字来标识一个
Ruijie(config-time-range)# **absolute** [**star**t *time date*] **end** *time date*	设置绝对时间区间(可选)，具体可参见 time range 的配置指南
Ruijie(config-time-range)# **periodic** *day-of-the-week time* **to** [*day-of-the-week*] *time*	设置周期时间(可选)
Ruijie# **show time-range**	验证您的配置
Ruijie# **copy running-config startup-config**	保存配置
Ruijie(config)# **ip access-list extended** *101*	进入 ACL 配置模式
Ruijie(config-ext-nacl)# **permit ip any any time-range** *time-range-name*	配置时间区的 ACE

Time Range 名字的长度为 1－32 个字符，不能包含空格；绝对的运行时间区间只能设置一个或不设置，基于 Time Range 的应用将仅在这个时间区间内有效；您可以设置一个或多个周期性运行的时间段。如果您已经为这个 Time Range 设置了一个运行时间区间，则将在时间区间内周期性的生效。

由于硬件表项资源有限，注意不要配置太多带时间区的 ACL 表项，否则当时间区生效时，可能会因为硬件资源不足而导致大量表项下发失败。对于带时间区的 ACL 表项，系统每隔 30 秒尝试将未下发的表项（包括之前未下发成功的表项）下发到硬件芯片。如果每次都有大量的表项因硬件资源限制而下发失败，尝试重新下发这些表项的过程中将会显著提高系统的 CPU 利用率，从而在这期间会使得控制台出现没响应的情况。

下面的例子以时间区 ACL 应用为例，说明如何在每周工作时间段内禁止 HTTP 的数据流：

```
Ruijie(config)# time-range no-http
Ruijie(config-time-range)# periodic weekdays 8:00 to 18:00
Ruijie(config)# end
Ruijie(config)# ip access-list extended limit-udp
Ruijie(config-ext-nacl)# deny tcp any any eq www time-range no-http
Ruijie(config-ext-nacl)# exit
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# ip access-group no-http in
Ruijie(config)# end
```

下面为 Time Range 的显示范例：

```
Ruijie# show time-range
time-range entry: no-http(inactive)
periodic Weekdays 8:00 to 18:00
time-range entry: no-udp
periodic Tuesday 15:30 to 16:30
```

1.6.4 配置安全通道

由于应用上的需要，您可能会希望符合某些特征的报文能够绕过接入控制的检查，比如 dot1x 认证前，DHCP 协议报文绕过 dot1x 的入口检测，PC 在认证前申请到 IP 地址。使用安全通道可以帮您达到这个目的。将安全 ACL 通过安全通道配置命令应用到全局或者接口，就表示该 ACL 是一条安全通道。安全通道也是一个访问控制列表，一般的 ACL 是基于接口或 VLAN 安装的，安全通道可以基于全局或者接口配置。报文进入到接口时，首先进行安全通道的检查，如果满足安全通道的匹配条件，将绕过接入控制比如端口安全，dot1x，Ip+MAC 绑定的检查直接进入交换机。应用于全局的安全通道对所有非例外口的接口都生效。如果接口上应用了安全通道，并且还存在全局的安全通道，那么全局安全通道不在这个接口上生效。

需要注意的是，应用于安全通道的访问控制列表的 deny 行为不生效，并且不存在末尾隐含着一条“拒绝所有数据流”规则的语句，如果报文不符合安全通道的匹配条件，将按流程进行接入控制的检查。

全局安全通道的例外口最多可以设置 8 个且全局安全通道的例外口不能用来设置基于接口的安全通道。

现有的接入控制功能包含：802.1x 认证，端口安全，全局 Ip+MAC 绑定，GSN 绑定，Ip Source Guard。

基于端口可迁移认证模式和安全通道共用时，安全通道不生效。

S5750S 系列产品，安全通道只支持对源 MAC、源 IP、目的 IP、四层目的端口号、VID 的匹配。

从特权模式开始，您可以通过以下步骤来设置一个全局的安全通道。

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)#**security global access-group** *1*	配置全局的安全通道

从特权模式开始，您可以通过以下步骤设置安全通道设置的例外口：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)#**interface** *idx*	进入接口模式
Ruijie(config-if)# **security uplink enable**	配置为例外口

从特权模式开始，您可以通过以下步骤配置接口下的安全通道：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)#**interface** *idx*	进入接口模式
Ruijie(config-if)# **security access-group** *1*	配置接口下的安全通道

下面的例子表明在配置 IP+MAC 绑定的安全端口上配置一个安全通道，使得 IPX 报文可以通过：

将端口 4 设置成安全端口，并绑定 IP+MAC：

```
Ruijie(config)#interface FastEthernet 0/4
Ruijie(config-if)#switchport port-security
Ruijie(config-if)#switchport port-security binding 0000.0000.0011 vlan 1 192.168.6.3
```

这样，只有源 IP 为 192.168.6.3 而且 MAC 地址为 0000.0000.0011 的报文才能从端口 4 进入设备。如果您希望端口还能够收发 IPX 报文，可以设置一个安全通道允许 IPX 报文通过，步骤如下：

```
Ruijie #configure
Ruijie (config)#expert access-list extended safe_channel
Ruijie (config-exp-nacl)#permit ipx any any
Ruijie (config-exp-nacl)#exit
Ruijie (config)#security global access-group safe_channel
```

也可以配置一个基于接口的安全通道如下：

```
Ruijie #configure
Ruijie (config-if)#expert access-list extended safe_channel
Ruijie (config-exp-nacl)#permit ipx any any
Ruijie (config-exp-nacl)#exit
Ruijie(config)#interface FastEthernet 0/4
Ruijie (config-if)#security access-group safe_channel
```

通过以上配置基于全局或者接口的安全通道，端口 4 就可以收发 IPX 报文了。

1.6.5 配置注释

为了便于浏览和理解 ACL 配置，ACL 模块提供了针对 ACL 和 ACE 的注释功能。

一个 ACL 中最多配置 1 个 ACL 注释和 2048 条 ACE 注释。

每个注释长度为 100 字节，不允许一个 ACL 内出现 2 条相同内容的 ACE 注释。。

从特权模式开始，您可以通过以下步骤给 ACL 配置注释：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **ip access-list standard** *id*	进入 ACL 配置模式(其他类型 ACL 类似)
Ruijie(config-std-nacl)# **list-remark** *comment*	给 ACL 配置注释

也可以通过以下步骤给 ACL 配置注释：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **access-list** *id* **list-remark** *comment*	直接给 ACL 配置注释(其他类型 ACL 类似)

从特权模式开始，您可以通过以下步骤给 ACE 配置注释：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **ip access-list standard** *id*	进入 ACL 配置模式(其他类型 ACL 类似)
Ruijie(config-std-nacl)# **remark** *comment*	给 ACL 配置一条 ACE 注释

也可以通过以下步骤给 ACE 配置注释：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **access-list** *id* **remark** *comment*	直接给 ACL 配置一条 ACE 注释(其他类型 ACL 类似)

下面的例子说明了如何配置 ACL 注释和 ACE 注释：

```
Ruijie(config)#ip access-list standard 1
Ruijie(config-std-nacl)#remark ace_remark_permit_62_start
Ruijie(config-std-nacl)#permit 192.168.197.62 0.0.0.0
Ruijie(config-std-nacl)#remark ace_remark_permit_62_end
Ruijie(config-std-nacl)#list-remark acl_remark_foo
Ruijie(config-std-nacl)#end
Ruijie#write
Ruijie#show access-lists 1
ip access-list standard 1
 remark ace_remark_permit_62_start
 10 permit host 192.168.197.62
 remark ace_remark_permit_62_end
list-remark acl_remark_foo
```

```
Ruijie#
```

1.6.6 SVI Router ACLs使能配置

作用在三层接口的安全 ACL 称为 Router ACLs，Router ACLs 仅对三层转发的路由报文生效。

为满足 SVI ACL 的 Router ACLs 特性，锐捷交换系列产品开发了 SVI Router ACLs 使能指令。开启该功能后，作用在 SVI 上的安全 ACL 仅对 VLAN 间的三层转发报文生效，而不对 VLAN 内的桥转发报文进行控制。

缺省配置

缺省情况下，SVI Router ACLs 默认关闭，SVI ACL 同时对 VLAN 间的三层转发报文及 VLAN 内的桥转发报文生效。

配置 SVI Router ACLs

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie# [**no**] **svi router-acls enable**	开启[关闭]SVI Router ACLs

1.6.7 配置ACL日志更新间隔

为了合理控制配置了 ACL logging 的 ACE 输出的 log 数量和频率，可以通过如下命令来设置 ACL 日志的更新间隔：

命令	作用
Ruijie(config)# { **ip | ipv6** } **access-list log-update inerval** *time*	配置 ACL 日志更新间隔，其中 time 取范围为 [0, 1440]，默认值为 0，表示该无需输出 ACL logging，配置的间隔时间必须是 5 分钟的倍数。

如果要恢复 ACL 日志更新间隔的默认值，可用 **no {ip | ipv6} access-list log-update interval** 全局配置命令设置。

配置举例：

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# ip access-list log-update interval 10
*Sep  9 16:23:06: %ACL-6-MATCH: ACL 120 ACE 10 permit icmp any any, match 78 packets.
*Sep  9 16:23:06: %ACL-6-MATCH: ACL 120 ACE 20 permit tcp any any, match 100 packets.
*Sep  9 16:33:06: %ACL-6-MATCH: ACL 120 ACE 10 permit icmp any any, match 345 packets.
*Sep  9 16:33:06: %ACL-6-MATCH: ACL 120 ACE 20 permit tcp any any, match 678 packets.
Ruijie(config)# no ip access-list log-update interval
```

1.6.8 配置、查看和清除ACL报文匹配计数

通过如下命令可以开启 ACL 报文匹配技术功能：

命令	作用

Ruijie(config)# { **mac | expert | ip** } **access-list counter** { *id* | *name* }	开启指定 MAC ACL、Expert ACL 或者 IPv4 ACL 下的所有 ACE 报文匹配计数功能
Ruijie(config)# **ipv6 access-list counter** *name*	开启指定 IPv6 ACL 下的所有 ACE 报文匹配计数功能

如果要取消 ACL 下的所有 ACE 的报文匹配技术功能，请使用 **no { mac | expert | ip } access-list counter** { *id* | *name* } 或者 **no ipv6 access-list counter** *name* 来设置。

使用ACL的查看命令可以看到ACL规则匹配到的报文计数，具体请参见相应类型访问列表的配置和显示章节。

对于如何清除 ACL 报文匹配计数，请按照如下步骤进行操作：

命令	作用
Ruijie# **clear counters access-list** [*id* | *name*]	清除 ACL 报文匹配计数

配置举例：

```
Ruijie(config)# ip access-list counter 101
Ruijie(config)# end
Ruijie #show ip access-lists
Extended IP access list 101
    10 deny ip any host 11.1.1.2 log (3 matches)
    20 permit ip any any log (10690 matches)
    30 deny ip host 192.168.21.59 any log (101 matches)
    40 permit tcp host 192.168.21.59 any eq ftp log
    50 permit ip host 192.168.21.59 any log
    (1080 packets filtered)
Ruijie# clear counters access-list
Ruijie #show ip access-lists
Extended IP access list 101
    10 deny ip any host 11.1.1.2 log
    20 permit ip any any log
    30 deny ip host 192.168.21.59 any log
    40 permit tcp host 192.168.21.59 any eq ftp log
    50 permit ip host 192.168.21.59 any log
```

使用 clear 相关的命令来清除 ACL 的报文匹配计数时，可能会造成该 ACL 丢失最多 1 秒钟到 5 秒的报文匹配计数，该 ACL 中带 logging 的 ACE 统计的匹配报文数也会受此影响。

如果有报文被上层软件 ACL 过滤掉，在显示 ACL 报文信息时，会将该 ACL 在软件上过滤掉的报文计数显示出来，这部分只会统计被 deny 的报文，不统计被 permit 的报文。注意，这里只会统计被软件 ACL 过滤掉的报文，不会统计被硬件 ACl 过滤掉的报文。

1.6.9 配置分片报文匹配模式

对于 IP 报文，在网络传输时中可能会被分片。报文发生分片时，只有首片报文带有四层信息，比如 TCP 或 UDP 端口号、ICMP 类型和 ICMP 编码等，其他的分片报文都不带有这些四层信息。默认情况下，如果 ACL 规则带有 fragment 标识，则

只会去匹配非首片报文；如果 ACL 规则不带有 fragment 标识，则匹配所有报文，包括首片报文和后续的所有分片报文。除了这种默认的分片报文匹配模式外，锐捷交换机产品还提供了一种新的分片报文匹配方法，用户可以根据需要在指定的 ACL 上进行切换。新的分片报文匹配模式与默认的分片报文匹配模式的区别就在于：当 ACL 规则中不带有 fragment 标识时，如果报文被分片，首片报文会去匹配 ACL 规则中用户定义的所有匹配域(包括三层和四层信息)，而非首片报文则只会去匹配 ACL 规则中的非四层信息。

从特权模式开始，您可以通过以下步骤切换分片报文的匹配模式：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)#{**ip** | **expert**} **access-list new-fragment-mode** { *id* | *name* }	将 IPv4 ACL 或 expert 扩展 ACL 的分片报文匹配模式从默认过滤模式切换到新匹配模式

使用 **no** { **ip** | **expert** } **access-list new-fragment-mode** { *id* | *name* }命令来将指定 IPv4 ACL 或 expert 扩展 ACL 的分片报文匹配模式切换回默认的过滤模式。

分片报文新匹配模式下，如果 ACL 规则不带 fragment 标识并且需要匹配报文的四层信息时，当匹配动作为 permit 时，ACL 规则会检查首片报文三层和四层信息，对于非首片报文只会检查报文的三层信息；当匹配动作为 deny 时，ACL 规则只会检查首片报文，不会去检查分片报文。

分片报文新匹配模式下，如果 ACL 规则带有 fragment 标识，不论 ACL 规则的匹配动作是 permit 还是 deny，都只检查非首片报文，而不会去检查首片报文。

分片报文新匹配模式下，如果 ACL 规则不带 fragment 标识，且匹配动作是 permit，这样的 ACL 规则需要使用更多的硬件表项，极端情况下会使得硬件表项容量减半；如果这样的 ACE 配置了 TCP flag 过滤控制的 established，则还会占用更多的硬件表项。

执行分片报文匹配模式切换时，会导致 ACL 的短时失效。

仅在 IP 扩展 ACL、Expert 扩展 ACL 上支持分片报文匹配模式的切换。不支持在 IP 标准 ACL 和 IPv6 扩展 ACL 上进行分片报文匹配模式的切换。

配置举例：

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# access-list new-fragment-mode
```

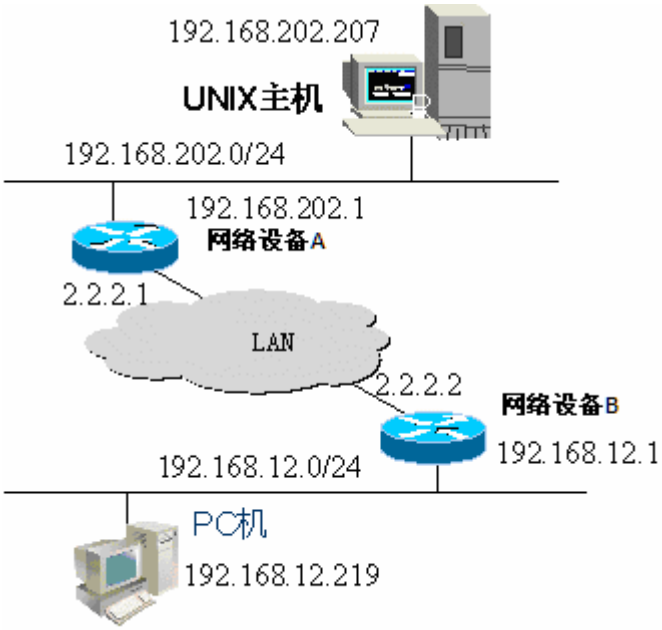
1.7 典型配置举例

1.7.1 IP访问列表示例

配置要求

有两台网络设备 A 和 B，如下图：

图 1-3 基本访问列表示例



要求通过在设备 B 上配置访问列表，实现以下安全功能：

192.168.12.0/24 网段的主机只能在正常上班时间访问远程 UNIX 主机 TELNET 服务，拒绝 PING 服务。

在设备 B 控制台上不能访问 192.168.202.0/24 网段主机的所有服务。

以上案例是银行系统应用的简化，即只允许分行或储蓄点局域网上的主机访问中心主机，不允许在设备上访问中心主机。

设备配置

设备 B 的配置：

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# ip address 192.168.12.1 255.255.255.0
Ruijie(config-if)# exit
Ruijie(config)# interface GigabitEthernet 0/2
Ruijie(config-if)# ip address 2.2.2.2 255.255.255.0
Ruijie(config-if)# ip access-group 101 in
Ruijie(config-if)# ip access-group 101 out
```

按照要求，配置一个编号为 101 的扩展访问列表

```
Ruijie(config)# access-list 101 permit tcp 192.168.12.0 0.0.0.255 any eq telnet time-range check
Ruijie(config)# access-list 101 deny icmp 192.168.12.0 0.0.0.255 any
Ruijie(config)# access-list 101 deny ip 2.2.2.0 0.0.0.255 any
Ruijie(config)# access-list 101 deny ip any any
```

配置 Time-Range 时间区

```
Ruijie(config)# time-range check
Ruijie(config-time-range)# periodic weekdays 8:30 to 17:30
```

访问列表 101 最后一条规则语句 access-list 101 deny ip any any 可以不要，因为访问列表最后隐含一条拒绝所有的规则语句。

设备 A 的配置：

```
A(config)# hostname Ruijie
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# ip address 192.168.202.1 255.255.255.0
Ruijie(config)# interface GigabitEthernet 0/2
Ruijie(config-if)# ip address 2.2.2.1 255.255.255.0
```

1.7.2 MAC扩展访问列表示例

要求通过配置 MAC 访问列表，实现以下安全功能：

- 使用 IPX 协议的主机 0013.2049.8272 不能访问设备 giga 0/1 端口
- 其他可以访问

```
Ruijie> enable
Ruijie# configure terminal
Ruijie(config)# mac access-list extended mac-list
Ruijie(config-mac-nacl)# deny host 0013.2049.8272 any ipx
Ruijie(config-mac-nacl)# permit any any
Ruijie(config-mac-nacl)# exit
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# mac access-group mac-list in
Ruijie(config-if)# end
Ruijie# show access-lists
mac access-list extended mac-list
deny host 0013.2049.8272 any ipx
permit any any
```

访问列表语句 permit any any 不能不要，因为访问列表最后隐含一条拒绝所有的规则语句。

1.7.3 Expert扩展访问列表示例

要求通过配置 Expert 访问列表，实现以下安全功能：

- VLAN20 的 0013.2049.8272 的主机能访问设备 Giga 0/1 端口
- 其他的不能访问

```
Ruijie> enable
Ruijie# config terminal
Ruijie(config)# expert access-list extended expert-list
Ruijie(config-exp-nacl)# permit ip vid 20 any host 0013.2049.8272 any any
```

```
Ruijie(config-exp-nacl)# deny any any any any
Ruijie(config-exp-nacl)# exit
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# expert access-group expert-list in
Ruijie(config-if)# end
Ruijie# show access-lists
expert access-list extended expert-list
permit ip vid 20 any host 0013.2049.8272 any any
deny any any any any
```

1.7.4 IPv6 扩展访问列表示例

要求通过配置访问列表，实现以下安全功能：

- 192.168.4.12 的主机能访问设备 gi 0/1 端口
- 其他的不能访问

```
Ruijie> enable
Ruijie# config terminal
Ruijie(config)# ipv6 access-list v6-list
Ruijie(config-ipv6-nacl)# permit ipv6 ::192:68:4:12/24 any
Ruijie(config-ipv6-nacl)# deny ipv6 any any
Ruijie(config-ipv6-nacl)# exit
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# ipv6 traffic-filter v6-list in
Ruijie(config-if)# end
Ruijie# show access-lists
ipv6 access-list extended v6-list
petmit ipv6 ::192.168.4.12 any
deny any any
```

☑ 对于 S5750S 系列交换机，IPV6 扩展 ACL 不支持 flow label 以及 fragment 字段。

1.7.5 配置TCP单向连接

通过配置 TCP Flag 过滤实现单向 ACL 的功能。

配置要求

为了在一定程度上保证网络 A 的安全，要求只允许网络 A 的主机向网络 B 主机发起的 TCP 通信请求，但是不允许网络 B 的主机发起到网络 A 的 TCP 通信请求。

拓扑图

图 1-4 配置 TCP 单向连接

如上图所示，通过一台中间设备连接两个网络，网络 A 与设备的 G3/1 口相连，网络 B 与设备的 G3/2 口相连。

分析

环境要求阻止网络 B 的主机发起到网络 A 的 TCP 通信请求，只要过滤从网络 B 发起经过中间设备 G3/2 口转发的 TCP 连接请求报文即可。分析 TCP 连接过程可知，TCP 初始请求报文的 TCP 首部标志字段的 SYN 置位且 ACK 标志位为 0。因此，我们可以通过配置扩展访问控制列表的 Match-all 选项，在 G3/2 端口的入口方向，对 TCP 首部 SYN 标志位置 1 且 ACK 标志位为 0 的报文进行过滤，即可实现网络 A 单向访问网络 B 的应用。

配置步骤

1) 定义访问控制列表

进入配置模式

```
Ruijie# configure terminal
```

在配置模式下创建扩展访问列表 ACL101

```
Ruijie(config)# ip access-list extended 101
```

拒绝 TCP Flag 的 SYN=1，且其它（包含 ACK 标志位）标志位为 0 的报文通过

```
Ruijie(config-ext-nacl)# deny tcp any any match-all syn
```

允许其它 IP 报文通过

```
Ruijie(config-ext-nacl)# permit ip any any
```

2) 把访问控制列表应用在接口上

退出访问控制列表模式

```
Ruijie(config-ext-nacl)# exit
```

进入应用此访问列表的接口 G3/2

```
Ruijie(config)# interface gigabitEthernet 3/2
```

将 ACL 101 应用于 G3/2 入方向的包过滤

```
Ruijie(config-if)# ip access-group 101 in
```

3) 显示访问列表的配置

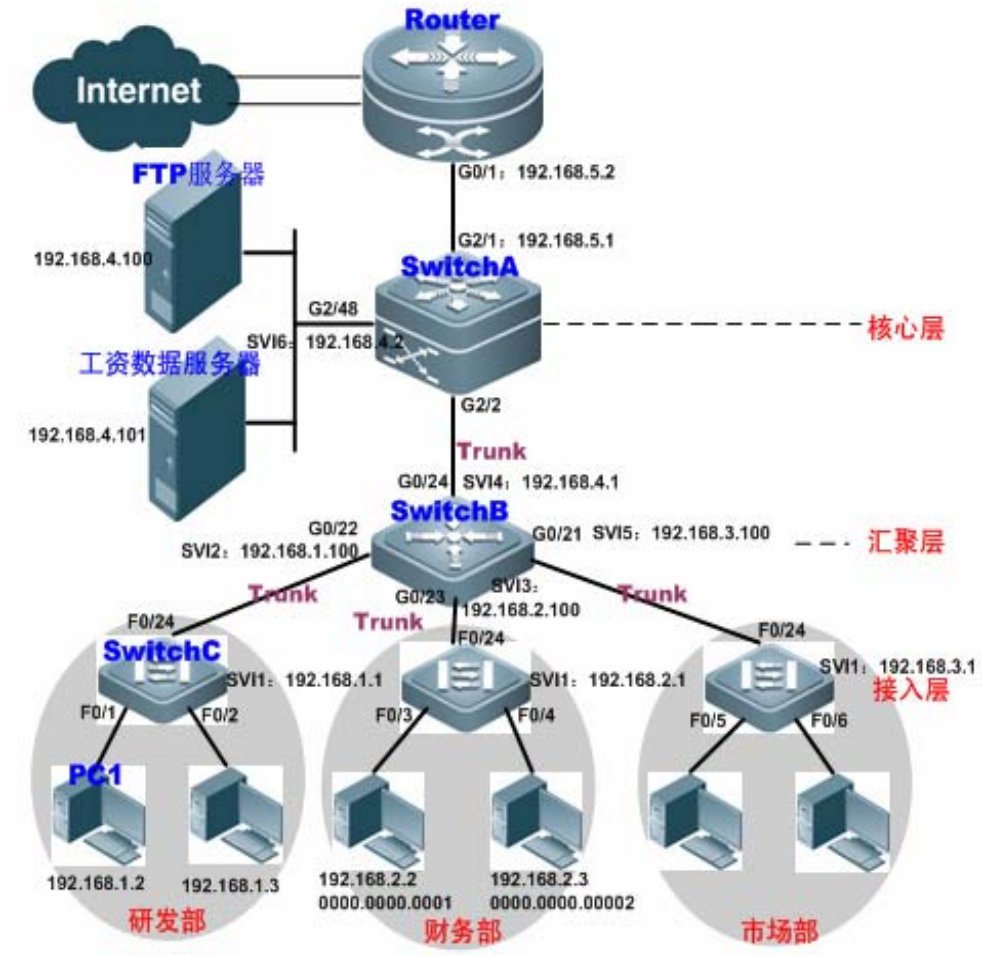
在特权模式下，使用 **show** 命令显示 ACL 相关配置

```
Ruijie# show access-lists 101
ip access-list extended 101
10 deny tcp any any match-all syn
20 permit ip any any
```

1.7.6 企业网ACL典型应用

组网图

图 1-5 企业网 ACL 应用场景拓扑图



上图是典型的企业网络拓扑：

接入层设备 C：连接各部门的 PC，通过千兆光纤(trunk 方式)连接汇聚层设备。

汇聚层设备 B：划分多个 VLAN，每个部门为一个 VLAN，通过万兆光纤(trunk 方式)上连核心层设备。

核心层设备 A：连接各种服务器，如 FTP，HTTP 服务器等，通过防火墙与 Internet 相连。

应用需求

上述企业网 ACL 应用场景主要有以下组网需求：

Internet 病毒无处不在，需要封堵各种病毒的常用端口，以保障内网安全。

只允许内部 PC 访问服务器，不允许外部 PC 访问服务器；

不允许非财务部门 PC 访问财务部 PC；不允许非研发部门 PC 访问研发部 PC

不允许研发部门人员在上班时间（即 9:00~18:00）使用 QQ、MSN 等聊天工具；

配置要点

- 通过在核心层设备（本例为设备 A）上联 Router 的端口（本例为 G2/1 口）上设置扩展 ACL 来过滤相关端口的数据包来达到防病毒的目的。
- 要求内部 PC 对服务器进行访问，不允许外部 PC 访问服务器，可以通过定义 IP 扩展 ACL 并应用到核心层设备（本例为设备 A）的下联汇聚层设备和服务器的接口（本例为 G2/2 口/SVI 2）上实现。
- 要求特定部门间不能互访，可通过定义 IP 扩展 ACL 实现(本例中分别在设备 B 的 G0/22、G0/23 上应用 IP 扩展 ACL)；
- 可通过配置时间 IP 扩展 ACL，限制研发部门在特定时间内使用 QQ/MSN 等聊天工具（本例中在设备 B 的 SVI 2 上应用时间 IP 扩展 ACL）。

配置步骤

- 配置核心层设备 A

第一步：定义阻断病毒访问控制列表 *Virus_Defence*

> 网络中的蠕虫病毒会在本地的 udp/69 端口上建立一个 tftp 服务器，用来向其它受侵害的系统上传送病毒的二进制程序。蠕虫选择目标 IP 地址的时候会首先选择受感染系统所在子网的 IP，然后再按照一定算法随机在互连网上选择目标攻击。一旦连接建立，蠕虫会向目标的 TCP 的 136、445、593、1025、5554、9995、9996，UDP 的 136、445、593、1433、1434，UDP/TCP 的 135、137、138、139 端口发送攻击数据。如果攻击成功，会监听目标系统的 TCP/4444 端口作为后门。然后蠕虫会连接到这个端口，发送 tftp 命令，回连到发起进攻的主机，将病毒文件传到目标系统上，然后运行它。中毒的服务器会向网络发送大量无效的数据包，浪费有效的网络带宽，甚至使网络设备死机，导致网络瘫痪。此时可以使用扩展访问列表来过滤这些端口的数据包来达到防病毒的目的。

```
A#configure terminal
A(config)#ip access-list extended Virus_Defence
```

！阻止来自内网外网可能被病毒利用的 TCP 端口报文

```
A(config-ext-nacl)#deny tcp any any eq 135
A(config-ext-nacl)#deny tcp any eq 135 any
A(config-ext-nacl)#deny tcp any any eq 136
A(config-ext-nacl)#deny tcp any eq 136 any
A(config-ext-nacl)#deny tcp any any eq 137
A(config-ext-nacl)#deny tcp any eq 137 any
```

……！中间的配置类似，此处省略说明

```
A(config-ext-nacl)#deny tcp any any eq 9996
A(config-ext-nacl)#deny tcp any eq 9996 any
```

！阻止来自内网外网可能被病毒利用的 UDP 端口报文

```
A(config-ext-nacl)#deny udp any any eq 69
A(config-ext-nacl)#deny udp any eq 69 any
A(config-ext-nacl)#deny udp any any eq 135
A(config-ext-nacl)#deny udp any eq 135 any
A(config-ext-nacl)#deny udp any any eq 137
A(config-ext-nacl)#deny udp any eq 137 any
```

……！中间的配置类似，此处省略说明

```
A(config-ext-nacl)#deny udp any any eq 1434
A(config-ext-nacl)#deny udp any eq 1434 any
```

！阻止 ICMP 报文

```
A(config-ext-nacl)#deny icmp any any
```

！允许其它所有 ip 数据包

```
A(config-ext-nacl)#permit ip any any
A(config-ext-nacl)#exit
```

第二步：将访问控制列表 *Virus_Defence* 应用在核心设备上联 Router 的接口上

```
A(config)#interface gigabitEthernet 2/1
A(config-if)#no switchport
A(config-if)#ip address 192.168.5.1 255.255.255.0
```

！将 ACL *Virus_Defence* 应用于 G2/1 入方向，阻断外网的病毒报文

```
A(config-if)#ip access-group Virus_Defence in
A(config-if)#exit
```

第三步，定义只允许内网 PC 访问服务器的访问控制列表 *access_server*

```
A(config)#ip access-list extended access_server
```

！只允许指定内网 IP 网段 PC 访问服务器(IP 地址为 192.168.4.100)

```
A(config-ext-nacl)#permit ip 192.168.2.0 0.0.0.255 host 192.168.4.100
A(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.255 host 192.168.4.100
A(config-ext-nacl)#permit ip 192.168.3.0 0.0.0.255 host 192.168.4.100
A(config-ext-nacl)#deny ip any any
```

第四步，将访问控制列表 *access_server* 应用在下联汇聚设备和服务器的接口上

```
A(config)#interface gigabitEthernet 2/2
A(config-if)#switch mode trunk
```

！应用于连接汇聚层设备接口的入方向

```
A(config-if)#ip access-group access_server in
A(config-if)#exit
```

！创建 vlan

```
A(config)#vlan 2
A(config-vlan)#exit
A(config)#interface gigabitEthernet 2/48
```

！连接服务器的接口 G2/48 属于 vlan2

```
A(config-if)#switch access vlan 2
A(config-if)#exit
```

！应用于连接服务器接口的入方向

```
A(config)#interface vlan 2
A(config-if-VLAN 2)# ip access-group access_server in
A(config-if-VLAN 2)# ip address 192.168.4.2 255.255.255.0
A(config-ext-nacl)#end
```

■ 配置汇聚设备 B

第一步，创建 vlan2-4

```
B#configure terminal
```

！创建 vlan2-4

```
B(config)#vlan range 2-4
B(config-vlan-range)#exit
```

第二步，定义访问控制列表

！定义 IP 扩展 ACL（vlan_access1 和 vlan_access2）

```
B(config)#ip access-list extended vlan_access1
```

！不允许财务部、市场部访问研发部

```
B(config-ext-nacl)#deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
B(config-ext-nacl)#deny ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
B(config-ext-nacl)#permit ip any any
B(config)#ip access-list extended vlan_access2
```

！不允许研发部、市场部访问财务部

```
B(config-ext-nacl)#deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
B(config-ext-nacl)#deny ip 192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255
B(config-ext-nacl)#permit ip any any
B(config-ext-nacl)#exit
```

第三步，将访问控制列表(vlan_access1 和 vlan_access2)应用在对应接口上

！配置 G0/22 口为 trunk 口，并应用 vlan_access1

```
B(config)#interface GigabitEthernet 0/22
B(config-if)#switchport mode trunk
```

```
B(config-if)#ip access-group vlan_access1 in
```

！配置 G0/23 口为 trunk 口，并应用 vlan_access2

```
B(config)# interface GigabitEthernet 0/23
B(config-if)# switchport mode trunk
B(config-if)# ip access-group vlan_access2 in
```

！配置 G0/24 为 trunk 口。

```
B(config)#interface GigabitEthernet 0/24
B(config-if)#switchport mode trunk
```

！配置 SVI2 的 IP 地址。

```
B(config)#interface vlan 2
B(config-if)#ip address 192.168.1.100 255.255.255.0
```

！配置 SVI3 的 IP 地址。

```
B(config)#interface vlan 3
B(config-if)#ip address 192.168.2.100 255.255.255.0
```

！配置 SVI4 的 IP 地址

```
B(config)#interface vlan 4
B(config-if)#ip address 192.168.4.1 255.255.255.0
```

第四步，定义时间段

！定义周一至周五的 9：00~18：00 的周期时间段

```
B#configure terminal
B(config)#time-range worktime
B(config-time-range)#periodic weekdays 9:00 to 18:00
```

第五步，定义研发部门数据流向规则

```
B#configure terminal
```

！在配置模式下创建扩展访问列表 ACL *yanfa*

```
B(config)#ip access-list extended yanfa
```

！禁止研发部的所有主机在工作日的 9：00 至 18：00 使用 QQ、MSN 等聊天工具。

```
B(config-ext-nacl)#deny tcp 192.168.1.0 0.0.0.255 eq 8000 any time-range worktime
B(config-ext-nacl)#deny tcp 192.168.1.0 0.0.0.255 eq 8001 any time-range worktime
B(config-ext-nacl)#deny tcp 192.168.1.0 0.0.0.255 eq 443 any time-range worktime
B(config-ext-nacl)#deny tcp 192.168.1.0 0.0.0.255 eq 1863 any time-range worktime
B(config-ext-nacl)#deny tcp 192.168.1.0 0.0.0.255 eq 4000 any time-range worktime
B(config-ext-nacl)#deny udp 192.168.1.0 0.0.0.255 eq 8000 any time-range worktime
B(config-ext-nacl)#deny udp 192.168.1.0 0.0.0.255 eq 1429 any time-range worktime
B(config-ext-nacl)#deny udp 192.168.1.0 0.0.0.255 eq 6000 any time-range worktime
```

```
B(config-ext-nacl)#deny udp 192.168.1.0 0.0.0.255 eq 6001 any time-range worktime
B(config-ext-nacl)#deny udp 192.168.1.0 0.0.0.255 eq 6002 any time-range worktime
B(config-ext-nacl)#deny udp 192.168.1.0 0.0.0.255 eq 6003 any time-range worktime
B(config-ext-nacl)#deny udp 192.168.1.0 0.0.0.255 eq 6004 any time-range worktime
```

！ 允许其它 IP 流量

```
B(config-ext-nacl)#permit ip any any
```

！ 将列表应用在 SVI2 的入方向上

```
B(config)#interface vlan 2
B(config-if)#ip access-group yanfa in
```

配置验证

第一步，确认 ACE 条目是否正确，关注点为配置项先后顺序是否正确和是否生效。

```
A#show access-lists
ip access-list extended Virus_Defence
 10 deny tcp any any eq 135
 20 deny tcp any eq 135 any
 30 deny tcp any eq 4444 any
 40 deny tcp any any eq 5554
 50 deny tcp any eq 5554 any
 60 deny tcp any any eq 9995
 70 deny tcp any eq 9995 any
 80 deny tcp any any eq 9996
 90 deny tcp any eq 9996 any
 100 deny udp any any eq tftp
 110 deny udp any eq tftp any
 120 deny udp any any eq 135
 130 deny udp any eq 135 any
 140 deny udp any any eq netbios-ns
 150 deny udp any eq netbios-ns any
 160 deny udp any any eq netbios-dgm
 170 deny udp any eq netbios-dgm any
 180 deny udp any any eq netbios-ss
 190 deny udp any eq netbios-ss any
 200 deny udp any any eq 445
 210 deny udp any eq 445 any
 220 deny udp any any eq 593
 230 deny udp any eq 593 any
 240 deny udp any any eq 1433
 250 deny udp any eq 1433 any
 260 deny udp any any eq 1434
 270 deny udp any eq 1434 any
```

```
 280 deny tcp any any eq 136
 290 deny tcp any eq 136 any
 300 deny tcp any any eq 137
 310 deny tcp any eq 137 any
 320 deny tcp any any eq 138
 330 deny tcp any eq 138 any
 340 deny tcp any any eq 139
 350 deny tcp any eq 139 any
 360 deny tcp any any eq 445
 370 deny tcp any eq 445 any
 380 deny tcp any any eq 593
 390 deny tcp any eq 593 any
 400 deny tcp any eq 1025 any
 410 deny tcp any any eq 4444
420 deny icmp any any
 430 permit tcp any any
 440 permit udp any any
 450 permit ip any any
ip access-list extended access_server
 10 permit ip 192.168.2.0 0.0.0.255 host 192.168.4.100
 20 permit ip 192.168.1.0 0.0.0.255 host 192.168.4.100
 30 permit ip 192.168.3.0 0.0.0.255 host 192.168.4.100
 40 deny ip any any
B#show access-lists
ip access-list extended vlan_access1
 10 deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
 20 deny ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
 30 permit ip any any
ip access-list extended vlan_access2
 10 deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
 20 deny ip 192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255
 30 permit ip any any
ip access-list extended yanfa
 10 deny tcp 192.168.1.0 0.0.0.255 eq 8000 any time-range worktime (active)
 20 deny tcp 192.168.1.0 0.0.0.255 eq 8001 any time-range worktime (active)
 30 deny tcp 192.168.1.0 0.0.0.255 eq 443 any time-range worktime (active)
 40 deny tcp 192.168.1.0 0.0.0.255 eq 1863 any time-range worktime (active)
 50 deny tcp 192.168.1.0 0.0.0.255 eq 4000 any time-range worktime (active)
 60 deny udp 192.168.1.0 0.0.0.255 eq 8000 any time-range worktime (active)
 70 deny udp 192.168.1.0 0.0.0.255 eq 1429 any time-range worktime (active)
 80 deny udp 192.168.1.0 0.0.0.255 eq 6000 any time-range worktime (active)
 90 deny udp 192.168.1.0 0.0.0.255 eq 6001 any time-range worktime (active)
 100 deny udp 192.168.1.0 0.0.0.255 eq 6002 any time-range worktime (active)
 110 deny udp 192.168.1.0 0.0.0.255 eq 6003 any time-range worktime (active)
 120 deny udp 192.168.1.0 0.0.0.255 eq 6004 any time-range worktime (active)
```

第二步，确认 ACL 配置是否完整，关注点为是否将正确的 ACL 应用到指定的接口上。

设备 A 配置：

```
A#show run
interface GigabitEthernet 2/1
 no switchport
 no ip proxy-arp
 ip access-group Virus_Defence in
 ip address 192.168.5.1 255.255.255.0
!
interface GigabitEthernet 2/2
 switchport mode trunk
 ip access-group access_server in
!
interface VLAN 2
 no ip proxy-arp
 ip access-group access_server in
 ip address 192.168.4.2 255.255.255.0
```

设备 B 配置：

```
B#show run
!
interface GigabitEthernet 0/22
 switchport mode trunk
 ip access-group vlan_access1 in
!
interface GigabitEthernet 0/23
 switchport mode trunk
 ip access-group vlan_access2 in
!
interface VLAN 2
 no ip proxy-arp
 ip access-group yanfa in
 ip address 192.168.1.100 255.255.255.0
```

2 IP QOS

2.1 QOS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，这就要求网络应能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。

2.1.1 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 实现以 IETF（Internet Engineering Task Force）的 DiffServ（Differentiated Servece Mode），差分服务模型） 体系为基础。DiffServ 体系规定网络中的每一个传输报文将被划分成不同的类别，分类信息被包含在了 IP 报文头中，DiffServ 体系使用了 IPv4 报文头中的 TOS（Type Of Service）或者 Ipv6 报文头中的 Traffic Class 字段的前 6 个比特来携带报文的分类信息。当然分类信息也可以被携带在链路层报文头上。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，通常称这三个比特为 User Priority bits。
- 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、设备或者其它网络设备赋予。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 QoSsolution。

2.1.2 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，当某个端口关联了一个表示 QoS 策略的 Policy-map 后，分类就在该端口上生效，它对所有从该端口输入的报文起作用。

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 User Priority bits，那么可以根据报文输入端口的缺省 CoS 值来获得报文的 QoS 信息。端口的缺省 CoS 值和报文的 User Priority bits 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 User Priority bits，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 QoS 信任模式打开的时候才起作用。打开端口的 QoS 的信任模式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。

如果端口关联的 Policy-map 中使用了基于 Mac access-list extended 的 ACLs 归类，那么在该端口上，将通过提取报文的源 MAC 地址、目的 MAC 地址以及 Ethertype 域来匹配关联的 ACLs，以确定报文的 DSCP 值。要注意的是，如果端口关联了某个 Policy-map，但又没有为其设置相应的 DSCP 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，在这个时候，如果端口的 QoS 信任模式打开，则根据准则 2 和 1 直接从报文中或者从端口上获得 QoS 信息；如果端口的 QoS 信任模式关闭，那么那些归类失败的报文将被赋予 DSCP 的缺省值 0。

对于 IP 报文，可以将根据以下准则来归类报文：

- 如果端口信任模式为 Trust ip-precedence，则直接从 IP 报文的 Ip precedence 字段（3 个比特）提取出来，填充到输出报文的 CoS 字段（3 个比特）。
- 如果端口信任模式为 Trust cos，则将报文的 CoS 字段（3 个比特）直接提取出来覆盖报文 Ip Precedence 字段（3 个比特）。这有两种情况，一是第二层报文头中不包含 User Priority bits，那么可以根据报文输入端口的缺省 CoS 值来获得报文的 CoS 值。另外一种是第二层报文头中包含 User Priority bits，则直接从报文头中取得 CoS 值。
- 如果端口关联的 Policy-map 中使用了基于 Ip access-list (Extended)的 ACLs 归类，那么该在该端口上，将通过提取报文的源 IP 地址、目的 IP 地址、Protocol 字段、以及第四层 TCP/UDP 端口字段来匹配相关联的 ACLs，以确定报文的 DSCP 值。要注意的是，如果端口关联了某个 Policy-map，但又没有为其设置相应的 DSCP 值，则设备将按照按照前面的规则 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。

有关上面提到的 CoS-to-DSCP map、IP-precedence-to-DSCP map 映射表的详细描述见随后描述。

Policing

Policing 即策略，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。Policing 动作检查被归类的数据流中的每一个报文，如果该报文超出了作用于该数据流的 Police 所允许的限制带宽，那么该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，Policing 动作是可选的。如果没有 Policing 动作，那么被分类的数据流中的报文的 DSCP 值将不会作任何修改，报文也不会在送往 Marking 动作之前被丢弃。

Marking

Marking 即标识，经过 Classifying 和 Policing 动作处理之后，为了确保被分类报文对应 DSCP 的值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，可以使用 QoS ACLs 改变报文的 QoS 信息，也可以使用 Trust 方式直接保留报文中 QoS 信息，例如，选择 Trust DSCP 从而保留 IP 报文头的 DSCP 信息。

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 DSCP-to-CoS Map 和 Cos-to-Queue Map 两张映射表来将报文的 DSCP 值转化成输出队列号，以便确定报文应该被送往的输出队列。

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 或者其它算法发送 8 个队列中的报文。

可以通过设置 WRR 算法的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。或通过设置 DRR 算法的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字节数,从而影响传输带宽。

2.1.3 QOS逻辑端口组

可以指定一系列端口为一个 QOS 逻辑端口组（这里端口可以是 AP，也可以是物理口，下文简称为逻辑端口组），并针对这个逻辑端口组关联 Policy-map 进行 QOS 处理，以限速为例，对符合限速条件的报文，在同一个逻辑端口组内所有的端口共享 Policy-map 所限定的带宽值。

加入逻辑端口组的成员必须是物理口或者是 Aggregate Port。

交换机逻辑端口组的支持数量为 128 个。

2.2 配置QOS

2.2.1 缺省QOS设置

用户在进行 QoS 配置之前，需要清楚和 QoS 有关的几点信息，如下：

- 一个接口最多关联 1 个 Policy-map
- 一个 Policy-map 可以拥有多个 Class-map

- 一个 Class-map 最多关联 1 个 ACL，该 ACL 的所有 ACE 必须具有相同过滤域模板
- 一个接口上关联的 ACE 的个数服从“配置安全 ACL”章节的限制

缺省情况下，QoS 功能是关闭的，即设备对所有的报文同等处理。但当您将一个 Policy Map 关联到某一个接口上，并设置了接口的信任模式时，该接口的 QoS 功能即被打开。要关闭该接口的 QoS 功能，您可以通过解除该接口的 Policy Map 设置，并将接口的信任模式设为 Off 即可。以下为 QOS 的缺省配置：

缺省 CoS 值	0
队列个数	8
队列轮转算法	WRR
QueueWeight	1:1:1:1:1:1:1:1
WRR Weight Range	1:254
DRR Weight Range	1:254
信任模式	No Trust

Cos 值到队列的默认映射表

CoS 值	0	1	2	3	4	5	6	7
队列	1	2	3	4	5	6	7	8

CoS to DSCP 默认映射表

CoS 值	0	1	2	3	4	5	6	7
DSCP 值	0	8	16	24	32	40	48	56

IP-Precedence to DSCP 默认映射表

IP-Precedence	0	1	2	3	4	5	6	7
DSCP	0	8	16	24	32	40	48	56

DSCP to CoS 的默认映射表

DSCP	0	8	16	24	32	40	48	56
CoS	0	1	2	3	4	5	6	7

2.2.2 配置接口的Qos信任模式

缺省情况下，接口的 Qos 信任模式是不信任

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **interface** *interface*	进入接口配置模式
Ruijie(config-if)# **mls qos trust {cos | ip-precedence | dscp}**	配置接口的 Qos 信任模式 cos，dscp 或 ip-precedence
Ruijie(config-if)# **no mls qos trust**	恢复接口默认 Qos 信任模式

以下命令将端口 interface GigabitEthernet 0/4 信任模式设置为 DSCP：

```
Ruijie(config)# interface gigabitEthernet 0/4
```

```
Ruijie(config-if)# mls qos trust dscp
Ruijie(config-if)# end
Ruijie# show mls qos interface g0/4
Interface: GigabitEthernet 0/4
Attached input  policy-map:
Default trust: trust dscp
Default COS: 0
Ruijie#
```

不支持在 SVI 口上配置 QoS 信任模式。

2.2.3 配置接口的缺省CoS值

您可以通过下面的设置步骤来配置每一个接口的缺省 CoS 值

缺省情况下，接口的缺省 CoS 值为 0

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **interface** *interface*	进入接口配置模式
Ruijie(config-if)# **mls qos cos default-cos**	配置接口的缺省 CoS 值, default-cos 为要设置的缺省 CoS 值, 取值范围为 0～7
Ruijie(config-if)# **no mls qos cos**	默认的缺省 CoS 值

下面的例子将接口 Interface g0/4 缺省 CoS 值设置为 6

```
Ruijie# configure terminal
Ruijie(config)# interface g 0/4
Ruijie(config-if)# mls qos cos 6
Ruijie(config-if)# end
Ruijie# show mls qos interface g 0/4
Interface: GigabitEthernet 0/4
Attached input  policy-map:
Default trust: trust dscp
Default COS: 6
Ruijie#
```

2.2.4 配置逻辑端口组

在接口配置模式下，请按如下步骤将端口加入逻辑端口组：

命令	作用
Ruijie(config-if)# [**no**] **virtual-group** *virtual-group-number*	将该接口加入一个逻辑端口组或退出一个逻辑端口组。*virtual-group-number* 表示逻辑端口组成员端口组的编号，即逻辑端口组号。

在接口配置模式下使用 **no virtual-group** *virtual-group-number* 命令将一个物理端口退出逻辑端口组。

下面的例子是将以太网接口 0/1 配置成逻辑端口组 5 的成员：

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-range)# virtual-group 5
Ruijie(config-if-range)# end
```

2.2.5 配置Class Maps

您可以通过下面的设置步骤来创建并配置 Class Maps

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **ip access-list extended** {*id* | *name*} Ruijie(config)# **ip access-list standard** {*id* | *name*} Ruijie(config)# **mac access-list extended** {*id* | *name*} Ruijie(config)# **expert access-list extended** {*id* | *name*} Ruijie(config)# **ipv6 access-list extended** *name* Ruijie(config)# **access-list** *id* […]	创建 ACL 请参见 ACL 章节
Ruijie(config)# [**no**] **class-map** *class-map-name*	创建并进入 class map 配置模式,class-map-name 是要创建的 class map 的名字 no 选项 删除一个已经存在的 class map
Ruijie(config-cmap)# [**no**] **match access-group** {*acl-num* | *acl-name* }	设置匹配 ACL, acl-name 为已经创建的 ACL 名字， acl-num 为已经创建的 ACL id，no 选项删除该匹配
Ruijie(config-cmap)# [**no**] **match ip dscp** *dscp-value1* [*dscp-value2* [*dscp-valueN*]]	设置要匹配的报文的 ip dscp 值，dscp-valueN 为要匹配的 DSCP 值，一次最多可以匹配 8 个不同的值。
Ruijie(config-cmap)# [**no**] **match ip precedence** *ip-pre-value1* [*ip-pre-value2* [*ip-pre-valueN*]]	设置要匹配的报文的 ip precedence 值，ip-pre-valueN 为要匹配的 EXP 值，一次最多可以匹配 8 个不同的值。

例如，以下设置步骤创建了一个名为 Class1 的 Class-map，它关联一个 ACL:acl_1。这个 Class-map 将分类所有端口号为 80 的 TCP 报文

```
Ruijie(config)# ip access-list extended acl_1
Ruijie(config-ext-nacl)# permit tcp any any eq 80
Ruijie(config-ext-nacl)# exit
Ruijie(config)# class-map class1
Ruijie(config-cmap)# match access-group acl_1
Ruijie(config-cmap)# end
```

☑ 设备支持匹配报文的 DSCP，IP-PRECEDENCE 值。

2.2.6 配置Policy Maps

您可以通过下面的设置步骤来创建并配置 Policy Maps

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# [**no**] **policy-map** *policy-map-name*	创建并进入 policymap 配置模式，policy-map-name 是要创建的 policymap 的名字 no 选项 删除一个已经存在的 policy map
Ruijie(config-pmap)# [**no**] **class** *class-map-name*	创建并进入数据分类配置模式，class-map-name 是已经创建的 class map 名字 no 选项 删除该数据分类
Ruijie(config-pmap-c)# [**no**] **set** { **ip dscp** *new-dscp* | **cos** *new-cos* [**none-tos**]}	为该数据流中的 IP 报文设置新的 ip dscp 值或者设置新的 cos 值；对于非 IP 报文，设置新的 ip dscp 不起作用； new-dscp 是要设置的新 DSCP 值，取值范围依产品不同而不同； new-cos 是要设置的新 CoS 值，取值范围为 0-7； none-tos 是代表设置新的 CoS 值，同时不修改报文的 DSCP 值。
Ruijie(config-pmap-c)# **police** *rate-bps burst-byte* [**exceed-action** {**drop** | **dscp** *dscp-value* | **cos** *cos-value* [**none-tos**]}]	限制该数据流的带宽和为带宽超限部分指定处理动作，rate-bps 是每秒钟带宽限制量(kbps)，burst-byte 猝发流量限制值(Kbyte)，drop 来丢弃带宽超限部分的报文，dscp dscp-value 改写带宽超限部分报文的 DSCP 值，dscp-value 取值范围依产品不同而不同，cos cos-value 改写带宽超限部分的报文的 CoS 值，cos-vlaue 取值范围为 0-7，none-tos 选项代表改写报文的 CoS 值时，不修改报文的 DSCP 值。
Ruijie(config-pmap-c)# **no police**	取消限制该数据流的带宽和为带宽超限部分指定处理动作

☑ 设备不支持对带宽超限部分报文改写 DSCP 值，带宽超限部分报文只能被丢弃。

☑ 设备同一个 policy map 应用于多个端口时，每个端口速率限制的带宽都是独立。

☑ CLASS MAP 所匹配的 ACL 表项中的 DENY 行为表项将被忽略，不会起作用。交换机中 CLASS MAP 所匹配的 ACL 表项中的 DENY 行为表示排除范围，表示匹配该 ACL 表项的范围内的 QOS 策略不生效

例如，以下的设置步骤创建了一个名为 Policy1 的 Policy-map，并将该 Policy-map 关联接口 Gigabitethernet 1/1

```
Ruijie(config)# policy-map policy1
Ruijie(config-pmap)# class class1
Ruijie(config-pmap-c)# set ip dscp 48
Ruijie(config-pmap-c)# exit
Ruijie(config-pmap)# exit
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# mls qos trust cos
Ruijie(config-if)# service-policy input policy1
```

2.2.7 配置接口应用Policy Maps

您可以通过下面的设置步骤将 Policy Maps 应用到端口上

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **interface** *interface*	进入接口配置模式
Ruijie(config-if)# [**no**] **service-policy** {**input** | **output**} *policy-map-name*	将创建的 Policy Map 应用到接口上；policy-map-name 是已经创建的 policy map 的名字，input 为输入,output 为输出

2.2.8 配置逻辑端口组应用Policy Maps

您可以通过下面的设置步骤将 Policy Maps 应用到逻辑端口组上

命令	说明
Ruijie#**configure terminal**	进入配置模式
Ruijie(config)#**virtual-group** *virtual-group-number*	进入逻辑端口组配置模式
Ruijie(config)# [**no**] **service-policy** {**input | output**} **policy-map-name**	将创建的 Policy Map 应用到逻辑端口组上；policy-map-name 是已经创建的 policy map 的名字，input 为输入限速,output 为输出限速

目前 output 方向应用在逻辑端口组上未被支持。由于 class map 需要关联 acl，所以 acl 配置的所有限制均适用于 qos，具体请参考 acl 配置指南。

2.2.9 配置输出队列调度算法

您可以为端口的输出队列调度算法：WRR，SP 和 DRR，缺省情况下，输出队列算法为 WRR（带权重的队列轮转)

您可以通过以下步骤对端口优先级队列调度方式进行设置,详细算法请参照 QOS 概述。

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **mls qos scheduler** {**sp | wrr | drr** }	端口优先级队列调度方式，sp 为绝对优先级调度，wrr 为带帧数量权重轮转调度，drr 为带帧长度权重轮转调度
Ruijie(config)# **no mls qos scheduler**	恢复为缺省 wrr 调度

例如，以下的设置步骤将端口的输出轮转算法设置成 SP：

```
Ruijie# configure terminal
Ruijie(config)# mls qos scheduler sp
Ruijie(config)# end
Ruijie# show mls qos scheduler
Global Multi-Layer Switching scheduling
Strict Priority
```

```
Ruijie#
```

2.2.10 配置输出轮转权重

您可以通过以下步骤设置端口的输出轮转权重

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# {**wrr-queue | drr-queue**} **bandwidth weight1...weightn**	weight1...weightn 为指定的输出队列的权重值，个数及取值范围见缺省 QOS 设置
Ruijie(config)# **no** {**wrr-queue | drr-queue**} **bandwidth**	no 选项恢复权重的缺省值

☑ S5750S 系列设备中，当（WRR/DRR）权重值设置为 0 时，表示此队列进行 SP 调度；同时队列调度优先级跟队列值一致，即队列 7-0 的调度优先级是从高到低的关系；为了保证调度准确，进行 WRR/DRR 调度的队列应该保持连续，而不应该中间插入 SP 调度，比如：wrr-queue bandwidth 1 2 3 0 4 5 6 7，3 队列配置了 SP 调度，这就会造成调度不准确。

下面的例子将 wrr 调度权重设置为 1:2:3:4:5:6:7:8

```
Ruijie# configure terminal
Ruijie(config)# wrr-queue bandwidth 1 2 3 4 5 6 7 8
Ruijie(config)# end
Ruijie# show mls qos queueing
Cos-queue map:
cos qid
--- ---
0   1
1   2
2   3
3   4
4   5
5   6
6   7
7   8
wrr bandwidth weights:
qid weights
--- -------
0   1
1   2
2   3
3   4
4   5
5   6
6   7
7   8
```

```
Ruijie(config)#
```

2.2.11 配置Cos-Map

您可以通过设置 Cos-Map 来选择报文输出时进入哪个输出队列，Cos-Map 的缺省设置见缺省 QOS 配置

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **priority-queue Cos-Map** *qid cos0* [*cos1* [*cos2* [*cos3* [*cos4* [*cos5* [*cos6* [*cos7*]]]]]]]	qid 为队列 id,cos0..cos7 为指定和这个队列关联的 CoS 值。
Ruijie(config)# **no priority-queue cos-map**	Cos-Map 恢复成缺省值

下面是设置 CoS Map 的例子

```
Ruijie# configure terminal
Ruijie(config)# priority-queue Cos-Map 1 2 4 6 7 5
Ruijie(config)# end
Ruijie# show mls qos queueing
Cos-queue map:
cos qid
--- ---
0   1
1   2
2   1
3   4
4   1
5   1
6   1
7   1

wrr bandwidth weights:
qid weights
--- -------
0   1
1   2
2   3
3   4
4   5
5   6
6   7
7   8
```

2.2.12 配置CoS-to-DSCP Map

CoS-to-DSCP Map 用于将报文的 CoS 值映射到内部 DSCP 值,您可以通过以下步骤对 CoS-to-DSCP Map 进行设置 ,CoS-to-DSCP Map 的缺省设置见缺省 QOS 配置

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **mls qos map cos-dscp** *dscp1...dscp8*	修改 CoS-to-DSCP Map 的设置,dscp1...dscp8 是对应于 CoS 值 0～7 的 DSCP 值,DSCP 取值范围依产品不同而不同
Ruijie(config)# **no mls qos map cos-dscp**	恢复缺省值

例如如下配置：

```
Ruijie# configure terminal
Ruijie(config)# mls qos map cos-dscp 56 48 46 40 34 32 26 24
Ruijie(config)# end
Ruijie# show mls qos maps cos-dscp
cos dscp
--- ----
0   56
1   48
2   46
3   40
4   34
5   32
6   26
7   24
```

2.2.13 配置DSCP-to-CoS Map

DSCP-to-CoS 用于将报文的内部 DSCP 值映射到 CoS 值，以便为报文选择输出队列

DSCP-to-CoS Map 的缺省设置见缺省 QOS 配置, 您可以通过以下步骤对 DSCP-to-CoS Map 进行设置:

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **mls qos map dscp-cos** *dscp-list* to *cos*	设置 DSCP to COS Map， *dscp-list* ：要设置的 DSCP 值的列表，DSCP 值之间用空格分隔，取值范围依产品不同而不同,*cos* ：对应 DSCP 值的 CoS 值，取值范围为：0～7；
Ruijie(config)# **no mls qos map dscp-cos**	设置为默认值

例如，以下的设置步骤将 DSCP 值 0、32、56 设置对应成 6：

```
Ruijie# configure terminal
Ruijie(config)# mls qos map dscp-cos 0 32 56 to 6
```

```
Ruijie(config)# show mls qos maps dscp-cos
dscp cos     dscp cos     dscp cos     dscp cos
---- ---     ---- ---     ---- ---     ---- ---
 0   6        1   0        2   0        3   0
 4   0        5   0        6   0        7   0
 8   1        9   1       10   1       11   1
12   1       13   1       14   1       15   1
16   2       17   2       18   2       19   2
20   2       21   2       22   2       23   2
24   3       25   3       26   3       27   3
28   3       29   3       30   3       31   3
32   6       33   4       34   4       35   4
36   4       37   4       38   4       39   4
40   5       41   5       42   5       43   5
44   5       45   5       46   5       47   5
48   6       49   6       50   6       51   6
52   6       53   6       54   6       55   6
56   6       57   7       58   7       59   7
60   7       61   7       62   7       63   7
```

2.2.14 配置端口速率限制

您可以通过以下步骤对端口速率限制进行设置

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **interface** *interface*	进入接口配置模式
Ruijie(config-if)# **rate-limit** { **input | output** } *bps burst-size*	端口速率限制。input 为输入限速，output 为输出限速。 *bps* 是每秒钟的带宽限制量(kbps) *burst-size* 是猝发流量限制值(Kbyte)
Ruijie(config-if)# **no rate-limit**	取消端口限速

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/4
Ruijie(config-if)# rate-limit input 100 100
Ruijie(config-if)# end
Ruijie#
```

2.2.15 配置IPpre to DSCP Map

IPpre-to-Dscp 用于将报文的 IPpre 值映射到内部 DSCP 值, IPpre-to-DSCP Map 的缺省设置见缺省 QOS 配置,您可以通过以下步骤对 IPpre-to-Dscp Map 进行设置:

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **mls qos map ip-prec-dscp** *dscp1...dscp8*	修改 IP-Precedence-to-Dscp Map 的设置,dscp1...dscp8 是对应于 IP-Precedence 值 0～7 的 DSCP 值
Ruijie(config)# **no mls qos map ip-prec-dscp**	恢复缺省配置。

例如如下配置：

```
Ruijie# configure terminal
Ruijie(config)# mls qos map ip-precedence-dscp 56 48 46 40 34 32 26 24
Ruijie(config)# end
Ruijie# show mls qos maps ip-prec-dscp
ip-precedence dscp
------------- ----
0       56
1       48
2       46
3       40
4       34
5       32
6       26
7       24
```

2.2.16 清除队列统计值

接口的输出队列的统计值可以通过特权模式命令 **show interfaces** 查看。您可通过特权模式下的 **clear counters** 命令清除接口的输出队列统计值。在支持显示接口输出队列统计值的设备上，清除接口的统计值的同时也会将接口上的输出队列统计值清零。清除接口统计值的命令请参考接口配置相关章节。

2.3 QOS显示

2.3.1 显示class-map

您可以通过以下步骤显示 class-map 内容

命令	作用
show class-map [*class-name*]	显示 class map 实体的内容

例如：

```
Ruijie# show class-map
Class Map cc
Match access-group 1
```

```
Ruijie#
```

2.3.2 显示policy-map

您可以通过以下步骤显示 Policy-map 内容

命令	作用
show policy-map [*policy-name* [**class** *class-name*]]	显示 QoS policy map，*policy-name* 为选定的 policy map 名，指定 class *class-name* 时显示相应 policy map 绑定的 class map。

例如：

```
Ruijie# show policy-map
Policy Map pp
Class cc
Ruijie#
```

2.3.3 显示mls qos interface

您可以通过以下步骤显示所有端口 qos 信息

命令	作用
show mls qos interface [*interface*	*policers*]	显示接口的 QoS 信息，Policers 选项显示接口应用的 Policy map

例如：

```
Ruijie# show mls qos interface gigabitEthernet 0/4
Interface: GigabitEthernet 0/4
Attached input  policy-map: pp
Default trust: trust dscp
Default COS: 6
Ruijie# show mls qos interface policers
Interface: GigabitEthernet 0/4
Attached input  policy-map: pp
Ruijie#
```

2.3.4 显示mls qos queueing

您可以通过以下步骤显示 qos 队列信息

命令	作用
show mls qos queueing	显示 QoS 队列信息，CoS-to-queue map，wrr weight 及 drr weight。

举例如下：

```
Ruijie# show mls qos queueing
Cos-queue map:
cos qid
--- ---
0   1
1   2
2   1
3   4
4   1
5   1
6   1
7   1
wrr bandwidth weights:
qid weights
--- -------
0   1
1   2
2   3
3   4
4   5
5   6
6   7
7   8
```

2.3.5 显示mls qos scheduler

您可以通过以下步骤显示 QOS 调度方式

命令	作用
show mls qos scheduler	显示端口优先级队列调度方式

举例如下：

```
Ruijie# show mls qos scheduler
Global Multi-Layer Switching scheduling
Strict Priority
Ruijie#
```

2.3.6 显示mls qos maps

您可以通过以下步骤显示 mls qos maps 对应表

命令	作用
show mls qos maps [cos-dscp|dscp-cos| ip-prec-dscp]	显示 dscp-cos maps；dscp-cos maps；ip-prec-dscp maps

举例如下：

```
Ruijie# show mls qos maps cos-dscp
cos dscp
--- ----
0   0
1   8
2   16
3   24
4   32
5   40
6   48
7   56
Ruijie# show mls qos maps dscp-cos
dscp cos     dscp cos     dscp cos     dscp cos
---- ---     ---- ---     ---- ---     ---- ---
0   6        1   0        2   0        3   0
4   0        5   0        6   0        7   0
8   1        9   1       10   1       11   1
12   1       13   1       14   1       15   1
16   2       17   2       18   2       19   2
20   2       21   2       22   2       23   2
24   3       25   3       26   3       27   3
28   3       29   3       30   3       31   3
32   6       33   4       34   4       35   4
36   4       37   4       38   4       39   4
40   5       41   5       42   5       43   5
44   5       45   5       46   5       47   5
48   6       49   6       50   6       51   6
52   6       53   6       54   6       55   6
56   6       57   7       58   7       59   7
60   7       61   7       62   7       63   7
Ruijie# show mls qos maps ip-prec-dscp
ip-precedence dscp
------------- ----
0       56
1       48
2       46
3       40
4       34
5       32
6       26
7       24
```

2.3.7 显示mls qos rate-limit

您可以通过以下步骤显示端口速率限制信息

命令	作用
show mls qos rate-limit [**interface** *interface*]	显示[端口] 速率限制

举例：

```
Ruijie# show mls qos rate-limit
Interface: GigabitEthernet 0/4
rate limit input bps = 100 burst = 100
```

2.3.8 显示show policy-map interface

您可以通过以下步骤显示端口 policymap 的配置

命令	作用
show policy-map interface *interface*	显示[端口] policymap 配置

举例：

```
Ruijie# show policy-map interface f0/1
FastEthernet 0/1  input (tc policy): pp
Class cc
set ip dscp 22
mark count 0
```

2.3.9 显示virtual-group

在特权模式下，请按如下步骤显示 virtual-group 设置。

命令	作用
show virtual-group [*virtual-group-number* | **summary**]	显示逻辑端口组信息。

举例：

```
Ruijie#show virtual-group 1
  virtual-group        member
  -------------        -------------------------
  1                      Gi0/2 Gi0/3 Gi0/4 Gi0/5
                         Gi0/6 Gi0/7 Gi0/8 Gi0/9 Gi0/10
Ruijie#show virtual-group summary
  virtual-group        member
  -------------        -------------------------
  1                      Gi0/1 Gi0/2 Gi0/3 Gi0/4
                         Gi0/5 Gi0/6 Gi0/7 Gi0/8 Gi0/9
```

```
2                    Gi0/11 Gi0/12 Gi0/13 Gi0/14
                     Gi0/15 Gi0/16 Gi0/17 Gi0/18 Gi0/19
```

2.3.10 显示队列统计值

您可在特权模式下通过以下命令来查看一个接口上的各个输出队列的统计值信息。

命令	作用
show interfaces [*interface-id*]	显示指定接口的全部状态和配置信息。

举例，显示接口 GigabitEthernet0/1 的队列统计值：

```
Ruijie#show interfaces gigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is DOWN  , line protocol is DOWN
Hardware is S5750E GigabitEthernet
Interface address is: no ip address
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Bridge, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  Rxload is 1/255, Txload is 1/255
  Queue:   Transmitted packets    Transmitted bytes      Dropped packets        Dropped bytes
    0                        0                    0                    0                    0
    1                        0                    0                    0                    0
    2                        0                    0                    0                    0
    3                        0                    0                    0                    0
    4                        0                    0                    0                    0
    5                        0                    0                    0                    0
    6                        0                    0                    0                    0
    7                        4                  288                    0                    0
  Switchport attributes:
    interface's description:""
    admin medium-type is Copper, oper medium-type is Copper
    lastchange time:0 Day: 0 Hour: 1 Minute:32 Second
    Priority is 0
    admin duplex mode is AUTO, oper duplex is Unknown
    admin speed is AUTO, oper speed is Unknown
    flow control admin status is OFF, flow control oper status is Unknown
    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
    4 packets input, 256 bytes, 0 no buffer, 0 dropped
```

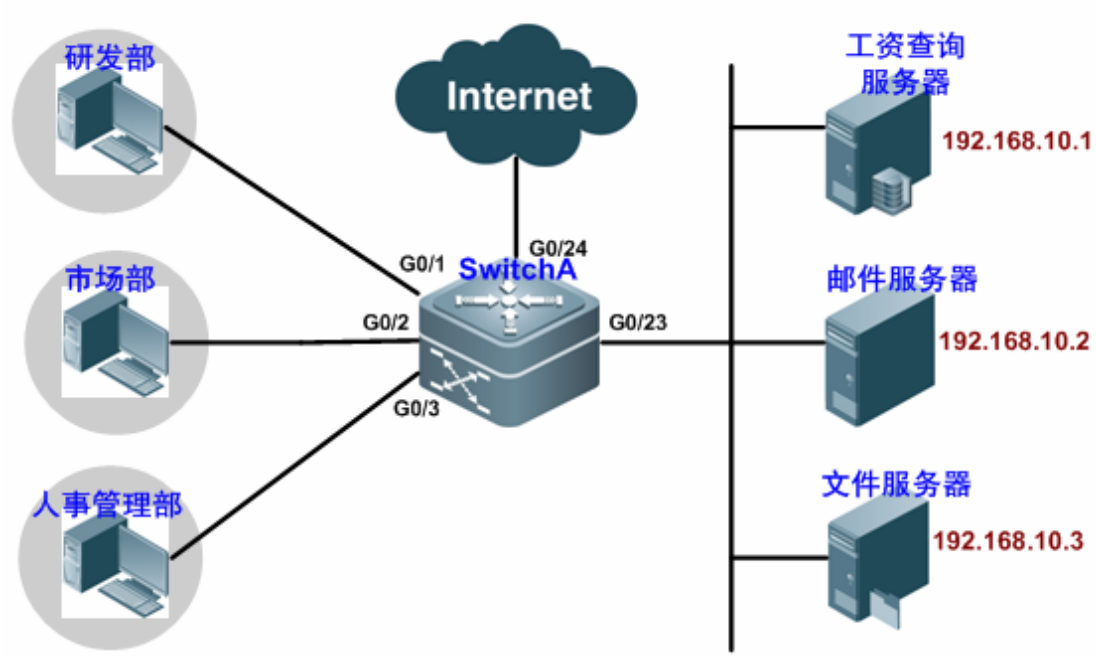
```
Received 0 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
4 packets output, 256 bytes, 0 underruns , 0 dropped
0 output errors, 0 collisions, 0 interface resets
```

2.4 QOS典型配置用例

2.4.1 优先级重标记+队列调度应用

组网图

图 2-1 优先级重标记+队列调度应用图



某公司企业网通过交换机（本例为 SwitchA）实现业务互连。网络环境描述如下：

- 研发部、市场部和人事管理部分别接入 SwitchA 的端口 GigabitEthernet 0/1、GigabitEthernet 0/2 和 GigabitEthernet 0/3；
- 工资查询服务器、邮件服务器和文件服务器连接在 SwitchA 的端口 GigabitEthernet 0/23 下。

应用需求

配置优先级重标记和队列调度，实现下述需求：

- 当研发部和市场部访问服务器时，服务器报文的优先级为：邮件服务器> 文件服务器>工资查询服务器
- 无论人事管理部访问 Internet 或访问服务器，交换机都优先处理。

- 交换机在运行过程中，时常发现网络拥塞，为了保证业务顺利运转，要求使用 WRR 队列调度，使访问邮件数据库、访问文件数据库、访问工资查询数据库的 IP 数据报按照 6：2：1 的比例来调度。

配置要点

- 通过配置访问不同服务器数据流的 cos 值，实现设备处理访问各种服务器报文的优先级；
- 通过配置接口的缺省 CoS 值为特定值，实现设备优先处理人事管理部发出的报文；
- 通过配置 WRR 队列调度实现按特定个数比进行数据报文传输调度；

配置步骤

第一步，创建访问各类服务器的 ACL：

```
SwitchA(config)#ip access-list extended salary
SwitchA(config-ext-nacl)#permit ip any host 192.168.10.1
SwitchA(config-ext-nacl)#exit
SwitchA(config)#ip access-list extended mail
SwitchA(config-ext-nacl)#permit ip any host 192.168.10.2
SwitchA(config-ext-nacl)#exit
SwitchA(config)#ip access-list extended file
SwitchA(config-ext-nacl)#permit ip any host 192.168.10.3
```

第二步，创建匹配各类服务器 ACL 的 class-map：

```
SwitchA(config)#class-map salary
SwitchA(config-cmap)#match access-group salary
SwitchA(config-cmap)#exit
SwitchA(config)#class-map mail
SwitchA(config-cmap)#match access-group mail
SwitchA(config-cmap)#exit
SwitchA(config)#class-map file
SwitchA(config-cmap)#match access-group file
```

第三步，将 policy-map 关联相应的 class-map，并配置访问邮件服务器数据流的 cos 值访问文件服务器数据流的 cos 值访问工资查询服务器数据；流的 cos 值：

```
SwitchA(config)#policy-map toserver
SwitchA(config-pmap)#class mail
SwitchA(config-pmap-c)#set cos 4
SwitchA(config-pmap-c)#exit
SwitchA(config-pmap)#class file
SwitchA(config-pmap-c)#set cos 3
SwitchA(config-pmap-c)#exit
SwitchA(config-pmap)#class salary
SwitchA(config-pmap-c)#set cos 2
SwitchA(config-pmap-c)#end
```

第四步，将 policy-map 应用到相应端口,并配置端口的 Qos 信任模式

```
SwitchA(config)#interface gigabitEthernet 0/1
SwitchA(config-if-GigabitEthernet 0/1)#service-policy input toserver
SwitchA(config-if-GigabitEthernet 0/1)#mls qos trust cos
SwitchA(config-if-GigabitEthernet 0/1)#exit
SwitchA(config)#interface gigabitEthernet 0/2
SwitchA(config-if-GigabitEthernet 0/2)#service-policy input toserver
SwitchA(config-if-GigabitEthernet 0/2)#mls qos trust cos
SwitchA(config-if-GigabitEthernet 0/2)#exit
```

第五步，配置设备的端口优先级队列调度方式为绝对优先级调度：

```
SwitchA(config)#mls qos scheduler sp
```

第六步，配置下联人事管理部接口的缺省 CoS 值为 7，优先保障人事管理部发出的报文，并配置端口的 Qos 信任模式：

```
SwitchA(config)#interface gigabitEthernet 0/3
SwitchA(config-if-GigabitEthernet 0/3)#mls qos cos 7
SwitchA(config-if-GigabitEthernet 0/3)#mls qos trust cos
```

第七步，配置 WRR 队列调度的输出轮转权重：

```
SwitchA(config)#wrr-queue bandwidth 1 1 1 2 6 1 1 1
```

第八步，配置设备的端口优先级队列调度方式为 WRR 调度：

```
SwitchA(config)#mls qos scheduler wrr
```

配置验证

第一步，确认 class-map 的内容是否配置正确：

```
SwitchA(config)#show class-map
 Class Map salary
   Match access-group salary
 Class Map mail
   Match access-group mail
 Class Map file
   Match access-group file
```

第二步，确认 policy-map 的内容是否配置正确：

```
SwitchA(config)#show policy-map
 Policy Map toserver
    Class mail
      set cos 4
    Class file
      set cos 3
    Class salary
      set cos 2
```

第三步，确认对应端口的 QOS 信息是否正确：

```
SwitchA(config)#show mls qos interface gigabitEthernet 0/1
Interface: GigabitEthernet 0/1
Attached input  policy-map: toserver
Attached output policy-map:
Default trust: cos
Default cos: 0
SwitchA(config)#show mls qos interface gigabitEthernet 0/2
Interface: GigabitEthernet 0/2
Attached input  policy-map: toserver
Attached output policy-map:
Default trust: cos
Default cos: 0
```

第四步，确认 QOS 队列信息

```
SwitchA(config)#show mls qos queueing
Cos-queue map:
cos qid
--- ---
0   1
1   2
2   3
3   4
4   5
5   6
6   7
7   8

wrr bandwidth weights:
qid weights
--- -------
1   1
2   1
3   1
4   2
5   6
6   1
7   1
8   1

drr bandwidth weights:
qid weights
--- -------
1   1
```

```
2    1
3    1
4    1
5    1
6    1
7    1
8    1
```

配置指南-可靠性

本分册介绍可靠性配置指南相关内容，包括以下章节：

1. CFM
2. REUP
3. RLDP
4. DLDP
5. VRRP
6. VRRP Plus
7. TPP
8. BFD
9. Rns & track
10. IP Event Dampening
11. GRTD
12. SEM
13. VSU

1 CFM

1.1 概述

以太网技术最初主要应用于局域网，而局域网对可靠性和稳定性的要求都比较低，因此自以太网诞生以来，其 OAM（Operations, Administration, Maintenance，操作、管理、维护）支持能力就比较薄弱，这已成为它在电信级网络（如城域网和广域网）规模应用的严重障碍。为此，诞生了多种以太网 OAM 标准，从应用范围上看，这些标准大概分为两类：链路级 OAM 和网络级 OAM。所谓链路级 OAM 指的是应用于点对点单条链路上的 OAM，如 IEEE802.3ah 定义的 EFM OAM 就属于链路级 OAM; 可以用来监测一个虚拟桥网络的 OAM 就属于网络级 OAM。

CFM（Connectivity Fault Management，连接故障管理）定义在 IEEE 802.1ag 中，从字面上理解，该技术就是为检测网络通路畅通与否而设计的，属于网络级 OAM 范畴。通过 CFM，网络管理者可以对网络中的连接性错误进行有效的检测、验证并对错误连接进行隔离。CFM 的使用环境可跨越多个节点，可以为用户提供端到端的 OAM 监控和管理功能。

IEEE 802.1ag: Connectivity Fault Management

1.1.1 维护域

维护域（Maintenance Domain，简称 MD）用来界定需要纳入管理的网络范围，以“维护域名”来标识。为了准确定位故障点，引入了维护域级别（MD Level）的概念。维护域共分 8 级，用整数 0 到 7 来表示，数字越大级别越高，维护域的范围也就越广。0 级是最低级别，7 级是最高级别。不同的维护域可以相邻（如图 1 所示，维护域 MD1 和维护域 MD2 相邻）；也可以嵌套（如图 2 所示，维护域 MD2 嵌套在维护域 MD1 中）；但不能交叉（如图 3 所示，维护域 MD1 和维护域 MD2 相交）。

图 1-1

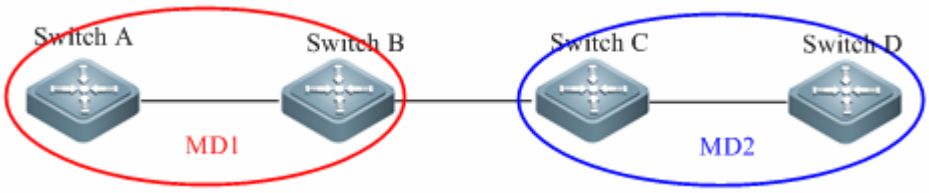


图 1-2

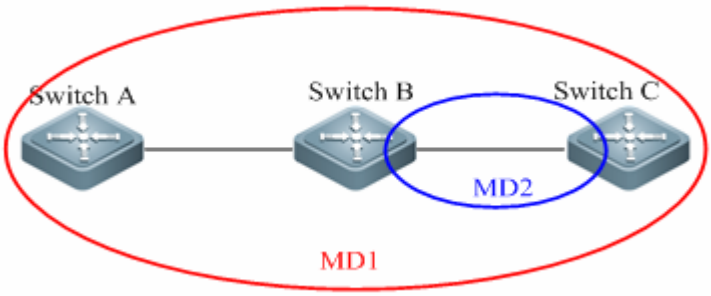
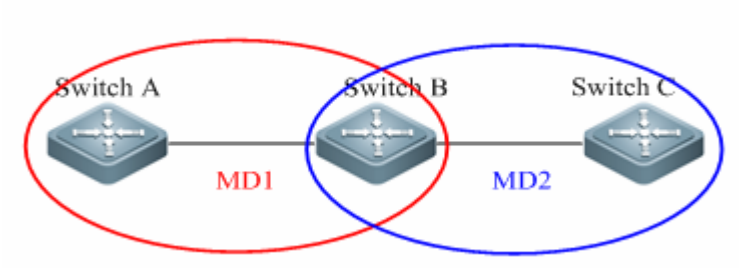


图 1-3



另外，嵌套时只能是级别低的维护域嵌套在级别高的维护域里。低级别的 CFM PDU 进入高级别维护域里将被丢弃；高级别的 CFM PDU 则可以穿过低级别的维护域；相同级别维护域的 CFM PDU 则不能相互穿越。

判断维护域有没有交叉，实际上是根据 VLAN 来区别的，相同 VLAN 对应的两个维护域才不能交叉，不同 VLAN 对应的两个维护域实际上是可以交叉的。

1.1.2 维护集

在一个 MD 内可以根据需要配置多个维护集（Maintenance Association，简称 MA），每个 MA 是特定 MD 内一些维护点的集合，有关维护点的描述请见后面的章节。一般来说，一个 MA 服务于一个特定的子网，所以通常 MA 会跟一个 VLAN 绑定在一起。MA 以“维护域名＋维护集名”组成的 MAID 来标识。

1.1.3 服务实例

服务实例（Service-instance）代表指定维护域中的指定维护集，为了方便配置，也为了便于表示一个维护域所代表的子网，引入了服务实例的概念。不同的服务实例以全局唯一的实例编号来表示。

1.1.4 维护点

维护点（Maintenance Point，简称 MP）配置在端口之上，属于某个 MA。MP 是 CFM 的主体，CFM 正是通过监测一个 MA 中的各 MP 之间的连通与否来确定网络的状况的。MP 又可分为维护端点和维护中间点两种。

维护端点

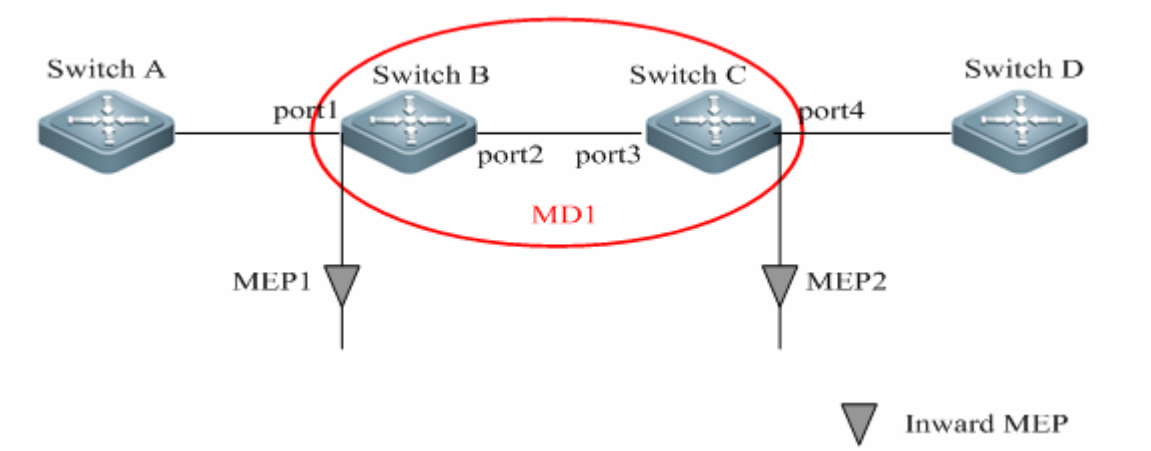
维护端点（Maintenance association End Point，简称 MEP）用来确定一个维护域（MD）的边界和范围。它是 CFM 的核心部件，负责发起所有的 CFM PDU 报文，从而主动负责起路径发现、错误检测、错误隔离和错误通告的功能。MEP 是一个 MA 的终结点，CFM 主要的协议和状态机都发生在 MEP 上。MEP 所在的 MD 级别决定了 MEP 发送的 CFM PDU 的级别；如果它接收到的 CFM PDU 级别比 MEP 所在的 MD 级别高，则转发它；如果收到的 CFM PDU 的级别小于 MEP 所在的 MD 级别，则丢弃报文，以避免属于低级别 MD 的 CFM PDU 进入高级别的 MD。正常情况下，在一个 MD 中，要么没有 MEP，要么至少要有两个。如果一个 MD 只有一个 MEP，那它发出的 OAM 报文就有可能会泄漏到维护域之内。

MEP 分为两种：Inward MEP 和 Outward MEP。

Inward MEP 即内向 MEP 不从其所在端口上往外发送 CFM PDU，而是通过设备上的其他端口发送 CFM PDU，如图 4 所示，Switch B 的 Port1 和 Switch C 的 Port4 是维护域 MD1 的边界，那么就要在这两个端口上为 MD1 都各自配置一个 MEP，

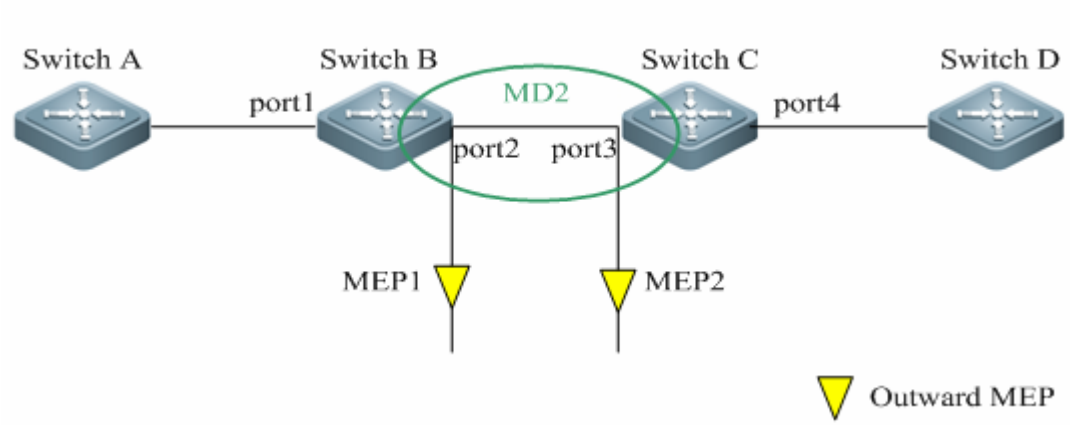
分别为 MEP1 和 MEP2，MEP1 不会在 port1 上往外发送属于维护域 MD1 的 CFM PDU，因为那已经超出了维护域 MD1 的范围，它只会通过本设备上的 port2 往外发送属于 MD1 的 CFM PDU。对于 MEP2 也是一样的。因此 MEP1 和 MEP2 的是内向 MEP 即 Inward MEP。

图 1-4



Outward MEP 则是从 MEP 所在端口上往外发送 CFM PDU。如图 5 所示，Switch B 上的 port2 和 Switch C 上的 port3 是维护域 MD2 的边界，那么就要在这两个端口上为 MD2 都配置一个 Outward MEP，分别为 MEP1 和 MEP2，说它们是 Outward MEP，那是因为它们不是通过设备上的其他端口来发送 CFM PDU，而是在 MEP 所在端口上的发送的。

图 1-5



MEP 以一个整数来标识，MEP 所属的 MD 和 MA 确定了它所发送的 CFM PDU 报文携带的 VLAN 标签。

在配置 MEP 的时候，要确保所要创建的 MEP 在 MEP 列表中已经存在，否则 MEP 不能创建成功。

维护中间点

维护中间点（Maintenance domain Intermediate Point，简称 MIP）位于 MD 内，与 MEP 不同，它不主动发起任何 CFM PDU，但可以处理和响应 CFM PDU。MIP 所属的 MD 和 MA 决定了它所能接收和响应的 CFM PDU 报文的 VLAN 标签。与 MEP 不同，如果一个 MIP 接收到的 CFM PDU 级别与 MIP 所在的 MD 级别不一样，CFM PDU 不会被拦截；如果收到的 CFM PDU 的级别等于 MIP 所有的 MD 级别，则需要对报文进行处理，处理完成以后有可能需要对原有报文进行转发。

1.2 工作原理

由上面的描述知道，CFM 协议的运作需要包括以下几个元素：MD、MA 和 MP（含 MEP 和 MIP）。MD 确定了维护范围; MA 则确定了 MD 中的一个子网络，通常与一个 VLAN 绑定在一起，一个 MD 中可以有多个 MA，因为有可能有多个子网络。而 MP 则确定了一个 MA 中的一个个维护点，在这些维护点之间交互 CFM PDU 来达到监测网络连通的目的，因此也可以说这些维护点的存在是为了在网络链路出问题时能更快地定位故障点。具体来说，CFM 主要提供了以下三项功能：

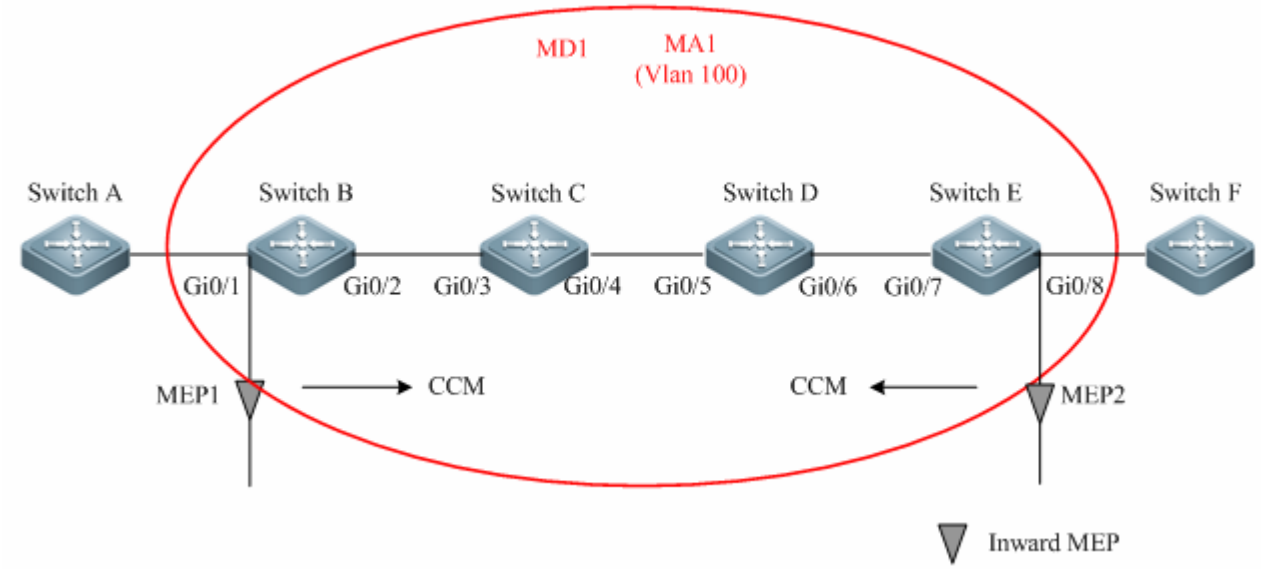
- 连续性检测（Continuity Check）
- 链路跟踪（Linktrace）
- 环回（Loopback）

以下分别对它们的工作原理进行详细的介绍。

1.2.1 连续性检测

连续性检测可用来检测一个 MA 中的各 MEP 之间的连通性。MA 中的各个 MEP 相互之间周期性地发送一种被称为 CCM（Continuity Check Message，连续性检测消息）的 CFM PDU，一个 MEP 如果在 3.5 个 CCM 发送间隔之内没收到远端 MEP 发出的 CCM，则说明已丢失该远端 MEP，即链路的连通性出了问题。如图 6 所示，维护域 MD1 中有一个维护集 MA1，MA1 服务于 Vlan 100，假设图中红圈内的所有交换机标示出来的端口（Gi0/1- Gi0/8）都已加入到 Vlan 100 中。MEP1 和 MEP2 则是维护域 MD1 的边界，假设它们的 CCM 发送间隔都为 1s，则执行连续性检测时，MEP1 和 MEP2 之间每秒周期性地互发带 Vlan 100 标签的 CCM，假设 MEP1 在 3.5 个发送周期内（本例为 3.5 秒）没收到 MEP2 发来的 CCM，则它认为到 MEP2 之间的通路连通性出了问题了，即 Vlan 100 这个虚拟网络的连通性存在问题。

图 1-6



CCM 发送间隔如下：

CCM 发送间隔	远端 MEP 超时时长
10ms	35ms

100ms	350ms
1s	3.5s
10s	35s
60s	210s
600s	2100s

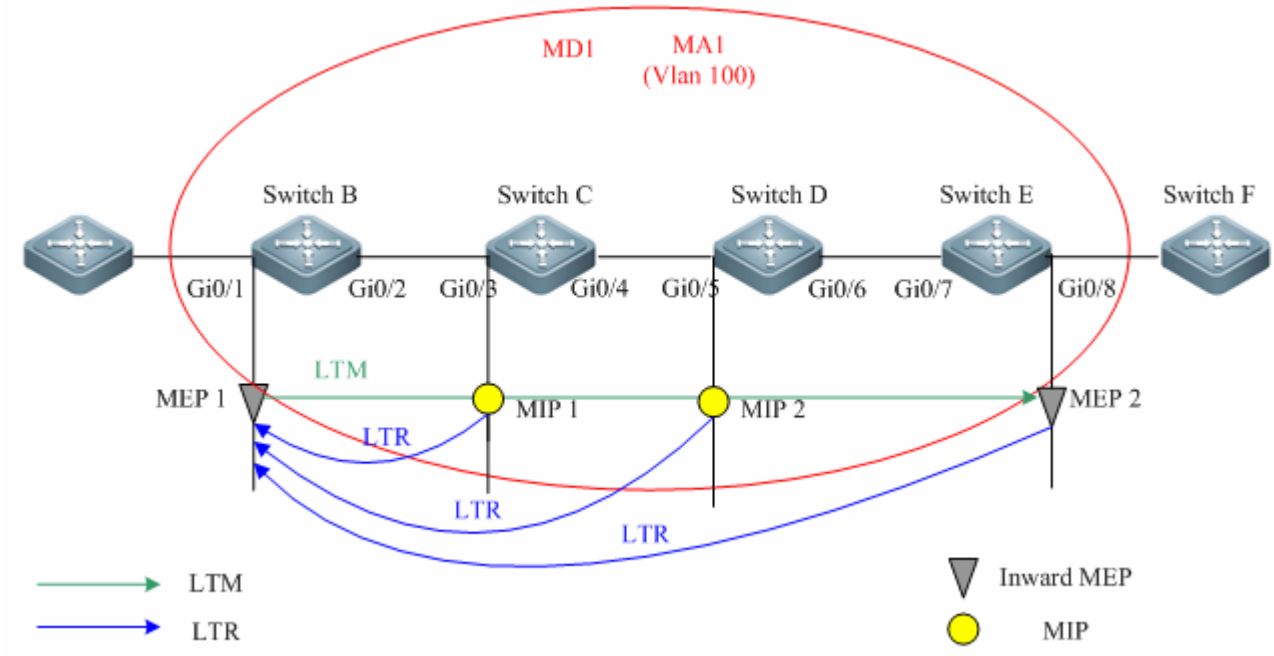
1.2.2 链路跟踪

链路跟踪（Linktrace）功能与 windows 下的 tracert 功能有些相似。通过在一个 MEP 上指定目标 MIP 或者 MEP，发送一种被称为 LTM（Linktrace Message，链路跟踪消息）的 CFM PDU，到达目标 MIP 或 MEP 前沿途的每个 MIP 都向源 MEP 回送一种被称为 LTR（Linktrace Reply，链路跟踪回应）的 CFM PDU，这样就能确定源和目标之间的路径。这可以用来定位故障点。比如在 Continuity Check 中发现两个维护端点（MEP）之间的链路连通性有问题，但故障点在哪里，Continuity Check 是没法给出的，通过执行 Link Trace 功能，就可以具体将故障点定位到某个 MIP 或者 MEP。

链路跟踪的工作原理如图所示，维护域 MD1 中配置了一个维护集 MA1，MA1 服务于 Vlan 100，假设图中红圈内的所有交换机标示出来的端口（Gi0/1- Gi0/8）都已加入到 Vlan 100 中，且如图中配置了 MEP 和 MIP。这里以 MEP 1 执行 Linktrace 功能为例，其执行过程如下：MEP1 设定 Linktrace 的目标是 MEP 2，由于它的方向是 Inward 的，所以它通过设备上的 Gi0/2 端口往外发送 LTM，MIP 1 收到后，产生一个 LTR 回应给 MEP 1;由于 MIP 1 不是 LTM 的目标，所以 MIP 1 会将 LTM 继续往下传播，MIP 2 收到 LTM 后，也会产生一个 LTR 回应给 MEP 1; 由于 MIP 2 也不是 LTM 的目标，所以 MIP 2 将 LTM 继续往下传播，最后 MEP 2 收到这个 LTM，它产生一个 LTR 回应给 MEP 1，确认自己是目标后，终止 LTM 的传播。通过上述的过程，MEP1 就会得到一张通往 MEP 2 的详细通路图。

假设 MEP 1 已经有 3.5 个 CCM 发送周期没有收到 MEP 2 发来的 CCM，说明了 MEP 1 与 MEP 2 之间的链路存在问题，这时就可以执行 Linktrace 功能定位故障发生点，如果 MIP 1 没有回应 LTR，则可以知道 Switch B 和 Switch C 之间的链路有问题; 同样的道理，如果 MIP 2 没有回应 LTR，则可以判断 Switch C 和 Switch D 之间的链路存在问题，以此类推下去。

图 1-7



1.2.3 环回

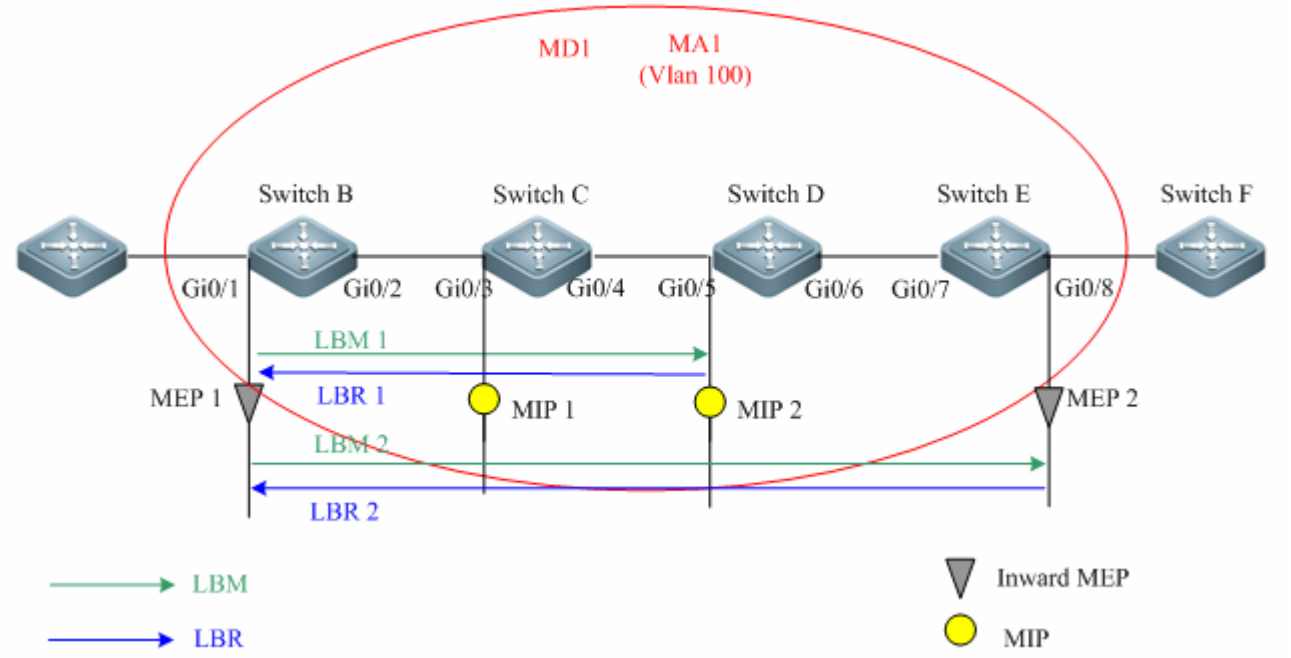
环回（Loopback）功能与我们熟悉的 ping 功能相似，是 CFM 提供的一项功能，通过在一个 MEP 上向目标 MIP 或 MEP 发送一种被称为 LBM（Loopback Message，环回消息）的 CFM PDU，目标 MIP 或 MEP 收到 LBM 后，回应一种被称为 LBR（Loopback Response）的 CFM PDU。所以这个功能类似于我们熟悉的 ping。当在 Continuity Check 中检测到链路上有连通性的问题时，可通过 Loopback 功能来验证这个错误。

如图 8 所示，维护域 MD1 中配置了一个维护集 MA1，MA1 服务于 Vlan 100，假设图中红圈内的所有交换机标示出来的端口（Gi0/1- Gi0/8）都已加入到 Vlan 100 中，且如图中配置了 MEP 和 MIP，该示例里包含了两个环回功能的例子，一个例子目标是 MIP，另一个例子的目标是 MEP。

以目标 MIP 为例，设定目标为 MIP 2，然后执行环回命令，MEP 1 就会构造一个 LBM（本例中的 LBM 1），目的 MAC Address 即为 MIP 2 的 MAC Address，源 MAC Address 指向 MEP 1 自己，由于 MEP 1 方向是 Inward 的，所以它通过端口 Gi0/2 往外传播这个 LBM 1，MIP 1 收到 LBM 1 后发现目的 MAC Address 不是自己，则继续往下传播，MIP 2 收到 LBM 1 后发现目的 MAC Address 指向自己，则生成一个 LBR（本例中的 LBR 1），目的 MAC Address 设为 MEP 1 的 MAC Address，回应给 MEP 1。这样就完成了一次环回功能。

目标是 MEP 的环回过程与目标为 MIP 的环回过程一样。

图 1-8



1.3 配置CFM

功能特性	缺省值
MD	不创建 MD
MA	不创建 MA
Service-instance	不创建 Service-instance
MEP	不创建 MEP

MIP	不创建 MIP
CCM 发送间隔类型值	4，即发送间隔为 1s
Continuity Check Enable State	Disable，关闭连续性检测
LTM TTL	64

1.3.1 配置维护域

缺省情况下，设备上未创建任何维护域。进入特权模式，按以下步骤创建维护域：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **cfm md** *md-name* **level** *level*	创建一个维护域，指定维护域名为 md-name，维护域级别为 level。 维护域名为字符串，长度[1,43]，维护域级别范围[0,7]
Ruijie(config)# **end**	退出配置模式。
Ruijie# **show cfm md**	查看设备上创建的所有维护域信息。

使用 **no cfm md** *md-name* 命令删除一个维护域。

例：配置维护域

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# cfm md md_test1 level 1
Ruijie(config)# end
Ruijie# show cfm md
Total 1 MD(s) configured:
Level: 1 MD Name: md_test1
```

1.3.2 配置维护集

缺省情况下，设备上未创建任何维护集。进入特权模式，按以下步骤创建维护集：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **cfm ma** *ma-name* **md** *md-name*	在指定的维护域中创建一个维护集，指定维护集名为 ma-name，维护集名为字符串，长度 1-43。
Ruijie(config)# **end**	退出配置模式。
Ruijie# **show cfm ma** [[*na-name*] **md** *md-name*]	查看设备上创建的所有维护域信息。

使用 **no cfm ma** *ma-name* **md** *md-name* 命令删除一个维护集。

例：配置维护集

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# cfm ma ma_test1 md md_test0
```

```
Ruijie(config)# end
Ruijie# show cfm ma
Total 2 MD(s) configured.
MD: md_test0
Total 1 MA(s) belong(s) to MD md_test0:
MA: ma_test0
Service instance: None  VLAN: None  Level: 2

MD: md_test1
Total 1 MA(s) belong(s) to MD md_test1:
MA: ma_test1
Service instance: 1  VLAN: 2  Level: 1
```

只有在配置了维护域之后才能配置维护集，而且维护域名长度和维护集名长度之和不能超过 44 个字符。

1.3.3 配置服务实例

缺省情况下，设备上未创建任何服务实例。进入特权模式，按以下步骤创建服务实例：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **cfm service-instance** *instance-id* **vlan** *vlan-id* **md** *md-name* **ma** *ma-name*	创建一个 id 为 instance-id 的服务实例，这个服务实例服务于维护域 md-name 中的维护域 ma-name，对应的 VLAN 为 vlan-id。instance-id 的取值范围 1-32767，vlan id 范围 1-4094。
Ruijie(config)# **end**	退出配置模式。
Ruijie# **show cfm service-instance** *instance-id*	查看设备上创建的所有维护域信息。

使用 **no cfm service-instance** *instance-id* 命令删除一个服务实例。

例：配置服务实例

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# cfm service-instance 1 vlan 2 md md_test1 ma ma_test1
Ruijie(config)# end
Ruijie# show cfm service-instance 1
Service instance 1:
MD name: md_test1
MA name: ma_test1
Level: 1  VLAN: 2  MIP-rule: None  CCM interval: 1s

Ruijie# show cfm ma
Total 1 MD(s) configured.
MD: md_test1
Total 1 MA(s) belong(s) to MD md_test1:
```

```
MA: ma_test1
Service instance: 1  VLAN: 2  Level: 1
```

只有在配置了维护集之后才能配置服务实例，删除服务实例时只是解除与维护集的绑定关系，并不会删除维护集本身。

1.3.4 配置MEP列表

缺省情况下，设备上未创建任何 MEP 列表。进入特权模式，按以下步骤配置 MEP 列表：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **cfm mep-list** *mep-list* **service-instance** *instance-id*	为编号为 instance-id 的服务实例配置一个 mep 列表。参数 mep-list 可以是一个 MEP，也可以是一系列 MEP，如：10－20 或 20-10。基于特权视图。MEP ID 取值范围为 1-8191。
Ruijie(config)# **end**	退出配置模式。
Ruijie# **show cfm mep** *mep-id* **service-instance** *instance-id*	查看指定的 MEP 列表信息。

使用 **no cfm mep** *mep-id* **service-instance** *instance-id* 命令删除一个 mep。

例：配置 MEP

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# cfm mep-list 1-3 service-instance 1
Ruijie(config)# end
Ruijie# show cfm mep-list service-instance 1
Service instance: 1
MEP list: 1 to 3.
```

1.3.5 配置MEP

缺省情况下，设备上未创建任何 MEP。进入特权模式，按以下步骤配置 MEP：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **interface** *interface-name*	进入端口的配置模式，可配置 MEP 的端口包括物理端口和 Aggregate Link

Ruijie(config-if)# **cfm mep** *mep-id* **service-instance** *instance-id* { **inward | outward }**	在指定的端口上配置一个 id 为 mep-id 的 MEP，其 id 为 mep-id，这个 MEP 属于 id 为 instance-id 的服务实例，并且指定 MEP 的方向。mep-id 的取值范围 1-8191，在一台交换机上，可以为一个服务实例配置多个 MEP，但这些 MEP 必须配置在不同的端口上。比如，在一个端口为一个服务实例配置了一个 outward MEP 后，就不能在同一个端口上为该服务实例再配置一个 outward MEP 或 Inward MEP。
Ruijie(config)# **end**	退出配置模式。
Ruijie# **show cfm mep** *mep-id* **service-instance** *instance-id*	查看指定的 MEP 信息。

使用 **no cfm mep** *mep-id* **service-instance** *instance-id* 命令删除一个 mep。

例：配置 MEP

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# interface GigabitEthernet0/2
Ruijie(config-if)# cfm mep 1 service-instance 1 inward
Ruijie(config)# end
Ruijie# show cfm mep 1 service-instance 1
Interface: GigabitEthernet0/2
MD name: mdtest_1
MA name: matest_1
Level: 1        VLAN: 2         Direction: Inward
CCM send: Disable
Alarm priority: CFM_DEF_MAC_STATUS (2)
FNG state: FNG_RESET

CCM:
Current state: CCI_IDLE
Interval: 1s  Send CCM: 0

Loopback:
NextTransId: 1
Send LBR: 0 Recv Ordered LBR: 0 Recv MisOrdered LBR: 0

Linktrace:
NextTransId: 1
SendLTR: 0  ReceiveLTM: 0
```

这里配置的 MEP 必须已经存在于 MEP 列表中，否则 MEP 不能创建成功。

可以在普通交换口上配置 MEP，也可以 AP 口上配置 MEP，还允许在 AP 成员口上配置 MEP。

- 如果一个端口已经成为 AP 成员口，则只允许在该端口上配置 outward MEP，不允许配置 inward MEP。如果在一个端口加入 AP 之前配置了 inward MEP，则加入 AP 之后，则该成员端口上的 inward MEP 会被自动删除。由于 AP 口的成员端口的特殊性，如果成员端口上配置了 MEP，将不允许在其上执行链路跟踪和环回命令。另外，在同一个 vlan 内，AP 成员口上的配置的 MEP 等级必须低于 AP 口上的 MEP 等级，否则配置失败。
- 不能在路由口上配置 MEP，如果试图在路由口上配置 MEP 将会得到错误提示。
- 如果在一个二层口上配置了 MEP，又使用 no switch 命令将该端口转化成路由口，此时配置在该端口上的 MEP 将被清除。

1.3.6 配置MIP

缺省情况下，设备上未创建任何 MIP，创建维护集后，设备也不会自动创建 MIP，进入特权模式，按以下步骤配置 MIP：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **cfm mip-rule { default | explicit } service-instance** *instance-id*	为指定的服务实例创建 MIP 生成规则
Ruijie(config)# **end**	退出配置模式。
Ruijie# **show cfm mp** [**interface** *interface-name*]	查看指定的维护点信息。

使用 **no cfm mip-rule service-instance** *instance-id* 命令删除 mip 生成规则。

例：配置 MIP

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# cfm mip-rule default service-instance 1
Ruijie(config)# end
Ruijie# show cfm mp
Interface GigabitEthernet0/2   VLAN 2
MEP ID: 2  Level: 2  Service instance: 2  Direction: Inward
MD name: md_test10
MA name: ma_test10

MIP Level: 1  Service instance: 1
MD name: md_test1
MA name: ma_test1
```

- 由于 AP 口的成员端口的特殊性，不会为运行了 CFM 协议的 AP 成员口生成 MIP。如果在一个端口上配置了 MIP 生成规则，之后又加入 AP 从而成为一个 AP 成员口时，交换机会将之前在该端口上生成的 MIP 删除，这种情况下，如果该成员口从 AP 口移除时，交换机会根据 MIP 生成规则重新计算该端口上的 MIP 生成。
- 另外，根据生成规则生成的 MIP 总是在指定 VLAN 内的最高级别上。

1.3.7 配置开启连续性检测

在设备上创建了一个 MEP 后，缺省情况下，连续性检测功能关闭。进入特权模式，按以下步骤开启连续性检测功能：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **cfm cc service-instance** *instance-id* [**mep** *mep-id*] **enable**	在指定的服务实例或指定的 MEP 上开启连续性检测功能。新创建的 MEP CC 功能是否开启，依赖于对应服务实例上的 CC 功能是否开启。如果对应的服务实例 CC 功能是开启的，则新创建的 MEP CC 功能就默认开启，否则默认关闭。 另外，如果服务实例上的 CC 功能被关闭，可以通过指定 MEP ID 来开启个别 MEP 的 CC 功能；同理，如果服务实例上的 CC 功能开启，可以通过指定 MEP ID 来关闭个别 MEP 的 CC 功能。
Ruijie(config)# **end**	退出配置模式。
Ruijie# **show cfm mep** *mep-id* **service-instance** *instance-id*	查看指定的 MEP 信息。

使用 **no cfm cc service-instance** *instance-id* [**mep** *mep-id*] **enable** 命令关闭连续性检测功能。

例：配置开启连续性检测功能

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# interface Gi0/1
Ruijie(config)# cfm cc service-instance 1 mep 1 enable
Ruijie(config)# end
Ruijie# show cfm mep 1 service-instance 1
Interface: GigabitEthernet0/2
MD name: md_test1
MA name: ma_test1
Level: 1  VLAN: 2  Direction: Inward
CCM send: Enable
Alarm priority: CFM_DEF_MAC_STATUS (2)
FNG state: FNG_RESET

CCM:
Current state: CCI_IDLE
Interval: 1s  Send CCM: 0

Loopback:
NextTransId: 1
Send LBR: 0 Recv Ordered LBR: 0 Recv MisOrdered LBR: 0

Linktrace:
```

```
NextTransId: 1
SendLTR: 0  ReceiveLTM: 0

One or more remote MEP(s) is missing

One or more  error CCM(s) is received. The last-received CCM:
MD name :md_test3
MA name :ma_test3
MEPID :5  TransId :8000
Received Time: 02/3/6 13:01:34

One or more  cross-connect CCM(s) is received. The last-received CCM:
MD name :md_test4
MA name :ma_test4
MEPID :6  TransId : 8009
Received Time: 02/3/6 13:01:34

Some other MEPs are transmitting the RDI bit

Ruijie# show cfm remote-mep service-instance 1 mep 1
MEP ID  MAC Address     State  Time                Link State  Forward State
2       0001-d0f8-0011  OK     2006/03/06 02:36:38  UP          FWD
3       0001-d0f8-0012  OK     2006/03/06 02:36:38  DOWN        Unkown
```

1.3.8 配置CCM发送间隔

缺省情况下，CCM 的发送间隔为 1s。进入特权模式，按以下步骤配置 CCM 发送间隔：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **cfm cc interval** *interval-type* **service-instance** *instance-id*	对指定的服务实例配置 CCM 发送间隔类型。参数 interval-type 取值范围[4,7]。各种间隔类型代表的 CCM 发送间隔如下： Interval-type CCM 发送间隔 4 1s 5 10s 6 60s 7 600s
Ruijie(config)# **end**	退出配置模式。
Ruijie# **show cfm mep** *mep-id* **service-instance** *instance-id*	查看指定的 MEP 信息。

使用 **no cfm cc interval service-instance** *instance-id* 命令恢复服务实例中的所有 MEP 的 CCM 发送间隔为默认值。

例：配置 CCM 发送间隔

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# interface GigabitEthernet0/2
Ruijie(config)# cfm cc interval 5 service-instance 1
Ruijie(config)# end
Ruijie(config)# show cfm mep 1 service-instance 1
Interface: GigabitEthernet0/2
MD name: md_test1
MA name: ma_test1
Level: 1  VLAN: 2  Direction: Inward
CCM send: Enable
Alarm priority: CFM_DEF_MAC_STATUS (2)
FNG state: FNG_RESET

CCM:
Current state: CCI_IDLE
Interval: 10s  Send CCM: 0

Loopback:
NextTransId: 1
Send LBR: 0 Recv Ordered LBR: 0 Recv MisOrdered LBR: 0

Linktrace:
NextTransId: 1
SendLTR: 0  ReceiveLTM: 0

One or more remote MEP(s) is missing.

One or more  error CCM(s) is received. The last-received CCM:
MD name :md_test3
MA name :ma_test3
MEPID :5  TransId :8000
Received Time: 02/3/6 13:01:34

One or more  cross-connect CCM(s) is received. The last-received CCM:
MD name :md_test4
MA name :ma_test4
MEPID :6  TransId : 8009
Received Time: 02/3/6 13:01:34

Some other MEPs are transmitting the RDI bit
```

IEEE 802.1ag 定义了 7 种 CCM 发送间隔，分别是 3.3ms、10ms、100ms、1s、10s、60s、600s。考虑到 CCM 发送间隔对交换机性能的影响，10.4(3)项目中涉及到的交换机系列产品都只实现 1s 及以上的 CCM 发送间隔。

1.3.9 配置产生告警的最低缺陷等级

MEP 在实施连续性检测时，会检测到网络中的以下缺陷中的一个或多个（缺陷等级由低到高）：收到某个远端 MEP 发来的带 RDI 位 CCM 报文、远端 MEP 所在接口的 MAC 状态不是 UP 的、远端 MEP 丢失即 3.5 个 CCM 发送周期内未收到该远端 MEP 发出的 CCM 报文、收到了错误的 CCM 报文、网络中存在交叉连接错误。用户可以根据需要来配置哪些缺陷需要向网管发送告警信息。

进入特权模式，按以下步骤配置产生告警的最低缺陷等级：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **cfm alarm-priority** *priority-value* **service-instanc**e *instance-id* [**mep** *mep-id*]	配置产生告警的最低缺陷等级，priority-value 的取值范围 1-5。表示当检测到缺陷等级大于等于该值时就向网管发送告警信息。默认值为 2。以下是各个等级对应的缺陷： 缺陷等级 1：收到远端 MEP 发来的带 RDI 位 CCM 报文。 缺陷等级 2：检测到远端 MEP 所在接口的 MAC 状态不是 UP 的。 缺陷等级 3：远端 MEP 丢失。 缺陷等级 4：收到了错误的 CCM 报文。 缺陷等级 5：检测到网络中存在交叉连接错误。
Ruijie(config)# **end**	退出配置模式。
Ruijie# **show cfm mep** *mep-id* **service-instance** *instance-id*	查看指定的 MEP 信息。

使用 **no cfm alarm-priority service-instanc**e *instance-id* [**mep** *mep-id*]命令恢复产生告警的最低缺陷等级。

例：配置开启连续性检测功能

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# cfm alarm-priority  3  service-instance 1 mep 1
Ruijie(config)# end
Ruijie# show cfm mep 1 service-instance 1
Interface: GigabitEthernet0/2
MD name: md_test1
MA name: ma_test1
Level: 1  VLAN: 2  Direction: Inward
CCM send: Enable
Alarm priority: CFM_DEF_REMOTE_CCM (3)
FNG state: FNG_RESET

CCM:
Current state: CCI_IDLE
Interval: 1s  Send CCM: 0

Loopback:
```

```
NextTransId: 1
Send LBR: 0 Recv Ordered LBR: 0 Recv MisOrdered LBR: 0

Linktrace:
NextTransId: 1
SendLTR: 0  ReceiveLTM: 0

One or more remote MEP(s) is missing.

One or more  error CCM(s) is received. The last-received CCM:
MD name :md_test3
MA name :ma_test3
MEPID :5      TransId :8000
Received Time: 02/3/6 13:01:34

One or more  cross-connect CCM(s) is received. The last-received CCM:
MD name :md_test4
MA name :ma_test4
MEPID :6  TransId : 8009
Received Time: 02/3/6 13:01:34

Some other MEPs are transmitting the RDI bit
```

1.3.10 配置链路跟踪

缺省情况下，设备不会自动执行链路跟踪功能。进入特权模式，按以下步骤执行链路跟踪：

命令	作用
Ruijie# **cfm linktrace service-instance** *instance-id* **mep** *mep-id* { **remote-mep** *remote-mep-id* | **remote-mac** *mac-address* } [**ttl** *ttl-value*] [**hw-only**]	在指定服务实例中的指定 MEP 上执行链路跟踪功能。目标如果是一个 MEP，则指定目标 MEP ID; 如果是一个 MIP，则指定目标 MIP MAC Address。
Ruijie# **show cfm linktrace-info** [**service-instance** *instance-id* [**mep** *mep-id*]]	查看链路跟踪结果信息。

例：配置链路跟踪功能

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie# cfm linktrace service-instance 1 mep 1 remote-mep 2
Linktrace to MEP 2 with the sequence number 1-1001
MAC Address  TTL  Last MAC  Relay Action
0010-FC00-6512  63  0010-FC00-6500  Hit
Ruijie# show cfm linktrace-info service-instance 1
Service instance: 1  MEP ID: 1
MAC Address  TTL  Last MAC  Relay Action
```

```
0010-FC00-6512  63  0010-FC00-6500   Hit
```

1.3.11 配置链路跟踪自动执行功能

缺省情况下，当 3.5 个 CCM 发送周期内没收到对端 MEP 发来的 CCM，本端 MEP 不会自动执行链路跟踪功能。进入特权模式，按以下步骤执行对端 MEP 丢失时自动执行链路跟踪的功能：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **cfm linktrace auto-detection** [**size** *entries-count*]	在设备上启动链路跟踪自动执行功能。可以指定保存的链路跟踪结果信息条目。
Ruijie(config)# **end**	退出配置模式。
Ruijie# **show cfm linktrace-info auto-detection** [**size** *entries-count*]	查看链路跟踪自动执行结果信息。

例：配置链路跟踪自动执行功能

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# cfm linktrace auto-detection
Ruijie(config)# end
Ruijie# show cfm linktrace-info auto-detection
Service instance: 1  MEP ID: 1  Time: 2010/02/27 20:10:10
Target MEP ID: 3  TTL: 64
MAC Address  TTL Last MAC Relay Action
0010-FC00-6505 63 0000-FC00-6504    MPDB
0010-FC00-A852 62 0000-FC00-6505    FDB
0000-FC00-6508 61 0010-FC00-A852    Hit
Service instance: 2 MEP ID: 2 Time: 2010/02/27 21:10:10
Target MEP ID: 4 TTL: 64
MAC Address TTL Last MAC Relay Action
0010-FC00-6508 61 0010-FC00-A852 Hit
```

1.3.12 配置环回

缺省情况下，设备不会自动执行环回功能。进入特权模式，按以下步骤执行环回功能：

命令	作用
Ruijie# **cfm loopback service-instance** *instance-id* **mep** *mep-id* { **remote-mep** *remote-mep-id* | **remote-mac** *mac-address* } [**count** *count*]	在指定服务实例中的指定 MEP 上执行环回功能。目标如果是一个 MEP，则指定目标 MEP ID; 如果是一个 MIP，则指定目标 MIP MAC Address。

例：配置环回功能

```
Ruijie# ethernet cfm loopback service-instance 1 mep 1 remote-mep 2
Loopback to 0010-FC00-6512 with the sequence number start from 1-1017:
```

```
Reply from 0010-FC00-6512: sequence number=1-1017
Reply from 0010-FC00-6512: sequence number=1-1018
Reply from 0010-FC00-6512: sequence number=1-1019
Reply from 0010-FC00-6512: sequence number=1-1020
Reply from 0010-FC00-6512: sequence number=1-1021
Loopback Message  Sent:5 Received:5 Lost:0  (%0 loss)
```

1.4 监视与维护

命令	作用
show cfm md	显示设备上配置的维护域信息。
show cfm ma [[*ma-name*] **md** *md-name*]	显示设备上配置的维护集信息。
show cfm meplist [**service-instance** *instance-id*]	显示 MEP 列表信息
show cfm mep *mep-id* **service-instance** *instance-id*	显示 MEP 的详细的配置和运行信息。
show cfm mp [**interface** *interface-Id*]	显示配置的 MP 信息，包括 MEP 和 MIP 的信息。
show cfm remote-mep service-instance *instance-id* **mep** *mep-id*	显示远端 MEP 信息。
show cfm service-instance [*instance-id*]	显示服务实例信息。
show cfm linktrace-info [**service-instance** *instance-id* [**mep** *mep-id*]]	显示链路跟踪结果信息。
show cfm linktrace-info auto-detection [**size** *entries-count*]	显示链路跟踪自动执行结果信息。

1.5 配置举例

为了实现完整的 CFM 功能，本配置举例将分如下几个步骤来进行：

- 配置服务实例
- 配置 MEP 并开启连续性检测功能
- 配置 MIP
- 配置 MEP 的链路跟踪功能
- 配置 MEP 的环回功能

1.5.1 配置服务实例

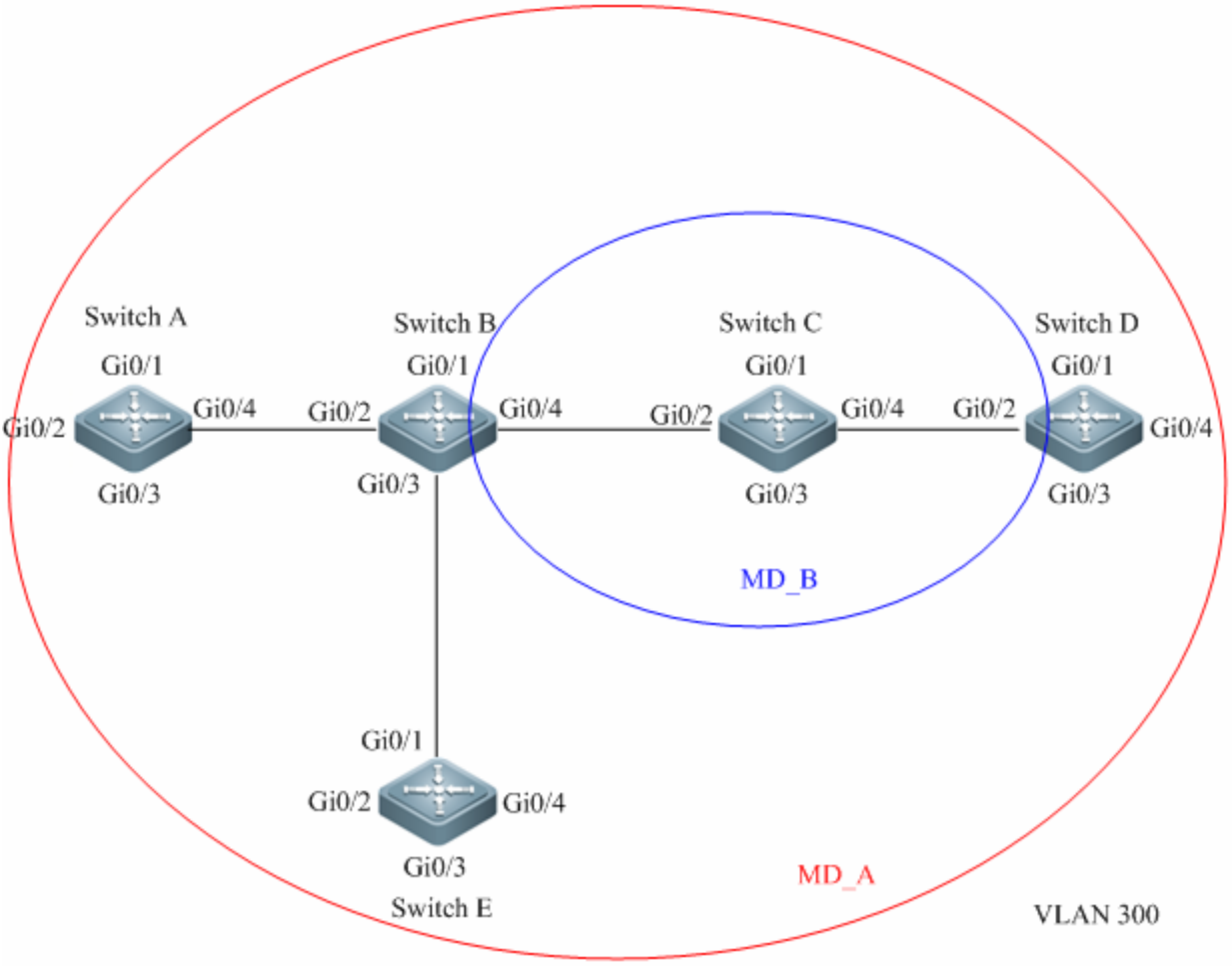
组网需求

- 将五台设备中的四台一字排开相连，另一台设备连在中间的两台设备中的任意一台上。
- 在这五台设备中规划两个维护域 MD_A 和 MD_B，其中维护域 MD_A 可配置 3 个 MEP，维护域 MD_B 可配置 2 个 MEP，MD_A 的级别为 6，MD_B 的级别为 2。MD_B 嵌套在 MD_A 中。

- 维护域中的每个维护集都服务于同一个 VLAN，本例为 VLAN 300。

组网拓扑

图 1-9 维护域示意图



配置要点

根据组网图中的每个端点所属的维护域，需要进行如下的配置：

- Switch A 和 Switch E 上配置维护域 MD_A。
- Switch C 上配置维护域 MD_B。
- Switch B 和 Switch D 上配置维护域 MD_A 和 MD_B。
- 在每台设备上为所在的维护域各配置一个维护集（MA）。
- 为每个维护集配置一个对应的服务实例。

配置步骤

- Switch A 的配置

配置一个级别为 6 的维护域 MD_A，配置一个维护集 MA_A，创建一个实例号为 1 的服务实例，对应于 VLAN 300，该实例服务于维护域 MD_A 中的维护集 MA_A。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# cfm md MD_A level 6
Ruijie(config)# cfm ma MA_A md MD_A
Ruijie(config)# cfm service-instance 1 vlan 300 md MD_A ma MA_A
```

- Switch B 的配置

先配置一个级别为 6 的维护域 MD_A，配置一个维护集 MA_A，创建一个实例号为 1 的服务实例，对应于 VLAN 300，该实例服务于维护域 MD_A 中的维护集 MA_A。 再配置一个级别为 2 的维护域 MD_B，配置一个维护集 MA_B，创建一个实例号为 2 的服务实例，对应于 VLAN 300，该实例服务于维护域 MD_B 中的维护集 MA_B。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# cfm md MD_A level 6
Ruijie(config)# cfm ma MA_A md MD_A
Ruijie(config)# cfm service-instance 1 vlan 300 md MD_A ma MA_A
Ruijie(config)# cfm md MD_B level 2
Ruijie(config)# cfm ma MA_B md MD_B
Ruijie(config)# cfm service-instance 2 vlan 300 md MD_B ma MA_B
```

- Switch C 的配置

配置一个级别为 2 的维护域 MD_B，配置一个维护集 MA_B，然后再创建一个实例号为 2 的服务实例，对应于 VLAN 300，该实例服务于维护域 MD_B 中的维护集 MA_B。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# cfm md MD_B level 2
Ruijie(config)# cfm ma MA_B md MD_B
Ruijie(config)# cfm service-instance 2 vlan 300 md MD_B ma MA_B
```

- Switch D 的配置

先配置一个级别为 6 的维护域 MD_A，配置一个维护集 MA_A，然后创建一个实例号为 1 的服务实例，对应于 VLAN 300，该实例服务于维护域 MD_A 中的维护集 MA_A。 再配置一个级别为 2 的维护域 MD_B，配置一个维护集 MA_B，创建一个实例号为 2 的服务实例，对应于 VLAN 300，该实例服务于维护域 MD_B 中的维护集 MA_B。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# cfm md MD_A level 6
Ruijie(config)# cfm ma MA_A md MD_A
Ruijie(config)# cfm service-instance 1 vlan 300 md MD_A ma MA_A
Ruijie(config)# cfm md MD_B level 2
Ruijie(config)# cfm ma MA_B md MD_B
Ruijie(config)# cfm service-instance 2 vlan 300 md MD_B ma MA_B
```

- Switch E 的配置

配置一个级别为 6 的维护域 MD_A，配置一个维护集 MA_A，创建一个实例号为 1 的服务实例，对应于 VLAN 300，该实例服务于维护域 MD_A 中的维护集 MA_A。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# cfm md MD_A level 6
Ruijie(config)# cfm ma MA_A md MD_A
Ruijie(config)# cfm service-instance 1 vlan 300 md MD_A ma MA_A
```

显示验证

经过上述配置后，在 Switch A-E 这五台设备上分别用以下显示命令来验证配置，这里以 Switch A 为例，其他设备显示验证过程是一样的。

- 显示验证维护域

```
Ruijie(config)# show cfm md
Total 1 MD(s) configured:
Level: 6     MD name: MD_A
```

- 显示验证维护集

```
Ruijie# show cfm ma
Total 1 MD(s) configured.
MD: MD_A
1 MA(s) belong(s) to MD MD_A:
MA: MA_A
Service instance: 1 VLAN: 300 Level: 6
```

- 显示验证服务实例

```
Ruijie# show cfm service-instance 1
Service instance 1:
MD name: MD_A
MA name: MA_A
Level: 6 VLAN: 300 MIP: None CCM interval: 1s
//+MIP:None 表示还没有配置 MIP
```

1.5.2 配置MEP并开启连续性检测功能

组网需求

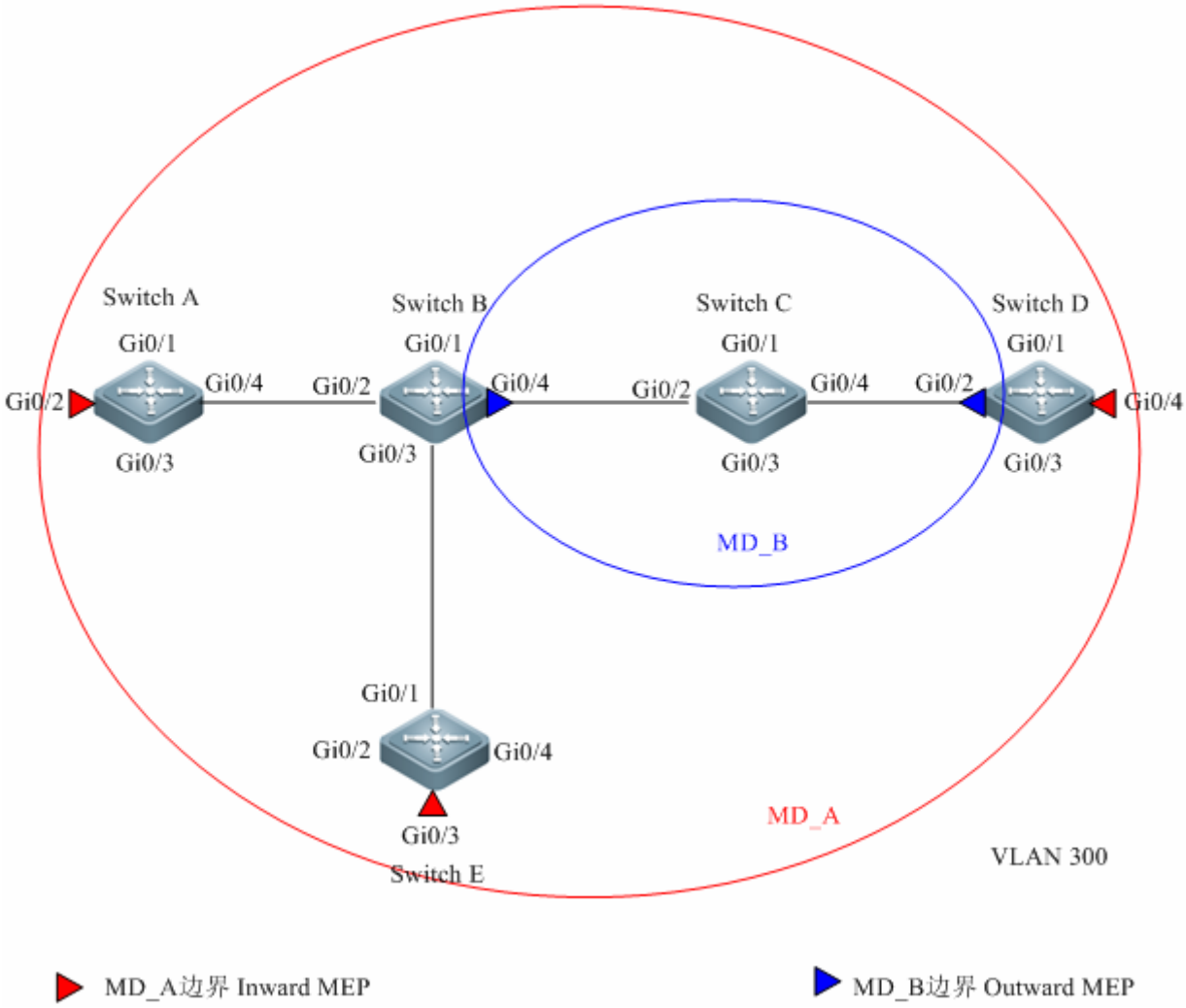
完成服务实例的配置之后，继续规划 MEP。MEP 用来界定维护域的边界，所以要配置在维护域边界的端口上，配置方式如下：

- 确定每个维护域所有的边界端口。

- 对每一个边界端口，根据维护域的位置确定配置在它上面的 MEP 的方向。
- 为每一个 MEP 确定一个维护集内唯一的 ID。
- 确定每个 MEP 所要检测的远端 MEP。

组网拓扑

图 1-10 维护域和维护端点示意图



配置要点

根据组网图中的每个端点所属的维护域，需要进行如下的配置：

- 对于维护域 MD_A，有三个边界端口，分别是 Switch A 上的 Gi0/2、Switch D 上的 Gi0/4 以及 Switch E 上的 Gi0/3，由于它们均不会在自己端口上发送属于 MD_A 级别的 CFM PDU，所以要在这些端口上配置 Inward MEP。
- 对于维护域 MD_B，有两个边界端口，分别是 Switch B 上的 Gi0/4 和 Switch D 上的 Gi0/2，由于它们均在自己端口上发送属于 MD_B 级别的 CFM PDU，所以要在这些端口上配置 Outward MEP。

- 对于某个维护域，每个有边界端口的设备上都要配置一个 MEP 列表，以表示在收到这些 MEP 的 CFM PDU 时才处理。
- 在所有配置的 MEP 上开启连续性检测功能。

配置步骤

- Switch A 的配置

#在该设备上配置一个 MEP 列表，里面包含所在维护域 MD_A 内的所有要配置的 MEP，并 Gi0/2 上配置一个 Inward MEP，开启连续性检测功能。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# cfm mep-list 1-3 service-instance 1
Ruijie(config)# interface Gi0/2
Ruijie(config-if)# cfm mep 1 service-instance 1  inward
Ruijie(config-if)# cfm cc service-instance 1 enable
```

- Switch B 的配置

#在该设备上配置一个 MEP 列表，里面包含所在维护域 MD_B 内的所有要配置的 MEP，并 Gi0/4 上配置一个 Outward MEP，开启连续性检测功能。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# cfm mep-list 4-5 service-instance 2
Ruijie(config)# interface Gi0/4
Ruijie(config-if)# cfm mep 4 service-instance 2  outward
Ruijie(config-if)# cfm cc service-instance 2 enable
```

- Switch D 的配置

#该设备的 Gi0/2 为 MD_B 的边界，Gi0/4 为 MD_A 的边界，因此在该设备上要作如下配置：

先配置一个 MEP 列表，里面包含所在维护域 MD_A 内的所有要配置的 MEP，并 Gi0/4 上配置一个 Inward MEP，开启连续性检测功能。

再配置一个 MEP 列表，里面包含所在维护域 MD_B 内的所有要配置的 MEP，并 Gi0/2 上配置一个 Outward MEP，开启连续性检测功能。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# cfm mep-list 1-3 service-instance 1
Ruijie(config)# interface Gi0/4
Ruijie(config-if)# cfm mep 2 service-instance 1  inward
Ruijie(config-if)# cfm cc service-instance 1 enable
Ruijie(config-if)#end
Ruijie(config)# cfm mep-list 4-5 service-instance 2
Ruijie(config)# interface Gi0/2
```

```
Ruijie(config-if)# cfm mep 5 service-instance 2  outward
Ruijie(config-if)# cfm cc service-instance 2 enable
```

- Switch E 的配置

#在该设备上配置一个MEP列表，里面包含所在维护域MD_A内的所有要配置的MEP，并Gi0/3上配置一个Inward MEP，开启连续性检测功能。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# cfm mep-list 1-3 service-instance 1
Ruijie(config)# interface Gi0/3
Ruijie(config-if)# cfm mep 3 service-instance 1  inward
Ruijie(config-if)# cfm cc service-instance 1 enable
```

显示验证

经过上述配置后，在 Switch A、Switch B、Switch D 和 Switch E 这四台设备上分别用以下显示命令来验证配置，这里以 Switch A 为例，其他设备显示验证过程是一样的。

- 显示验证 MEP 列表

```
Ruijie# show cfm mep-list service-instance 1
Service instance: 1
MEP list: 1 to 3.      //+表明该设备上为服务实例 1 配置了一个 MEP 列表
```

- 显示验证 MEP

```
Ruijie# show cfm mep 1 service-instance 1
Interface: GigabitEthernet0/2
MD name: MD_A
MA name: MA_A
Level: 6  VLAN: 300 Direction: Inward //+所在 MD 的级别,服务的 VLAN ID 以及这个 MEP 的方向
CCM send: Enable                                  //+连续性检测功能开启
Alarm priority: CFM_DEF_REMOTE_CCM (3)     //+当 MEP 检测到缺陷级别大于等于 3 时向网管发送告警信息
FNG state: FNG_DEFECT_REPORTED

CCM:
Current state: CCI_WAITING
Interval: 1s Send CCM: 12          //+CCM 发送间隔,以及发送了多少个 CCM

Loopback:
NextTransId: 120
Send LBR: 0 Recv Ordered LBR: 0 Recv MisOrdered LBR: 0

Linktrace:
NextTransId: 10
```

```
SendLTR: 0  ReceiveLTM: 0
```

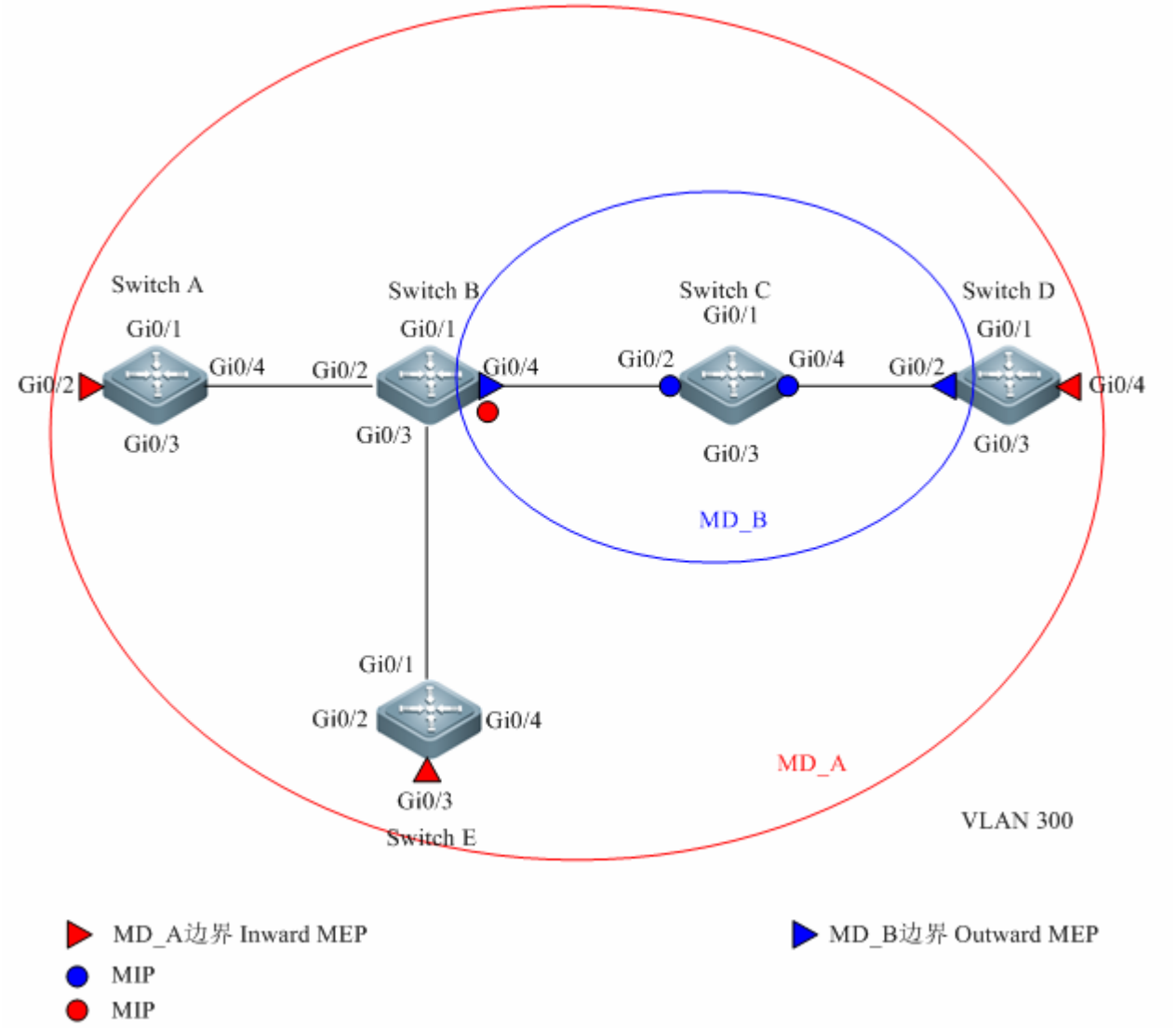
1.5.3 配置MIP

组网需求

完成了 MEP 的配置之后，CFM 功能就可以使用了，但当一个维护域内的两个 MEP 间跨多跳时，如果这两个 MEP 间的链路有问题，不在这两个 MEP 间配置 MIP，就无法将问题定位到某一台设备上。因此本节接前一节配置继续 MIP 的规划。

组网拓扑

图 1-11 维护域和维护中间点图



配置要点

MIP 的生成有两种规则，default 生成规则和 explicit 生成规则。

如果在设备上配置 default 生成规则，满足下面两种情况的端口上会生成 MIP：

- 该设备上没有配置更低级别的维护域。
- 该设备上配置了更低级别的维护域，则只会在配置了低级别的 MEP 所在端口上生成 MIP。

如果在设备上配置 explicit 生成规则，则只会在低级别 MD 上有 MEP 的所在端口上才会生成 MIP。

根据上述 MIP 生成规则，本例配置要点如下：

- 将维护域 MD_A 的 MIP 配置在 Switch B 上，由于 Switch B 上配置了低级别的维护域 MD_B，且在 Gi0/4 上配置了以属于 MD_B 的 MEP，所以在该设备上使用 explicit 规则来生成 MIP。
- 将维护域 MD_B 的 MIP 配置在 Switch C 上，由于 Switch C 上没有更低级别的维护域了，要使它能生成 MIP，则要用 default 规则，这样会在其所有端口上都生成一个 MIP。

配置步骤

- Switch B 的配置

#在该设备上使用 explicit 规则为维护域 MD_A 生成 MIP。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# cfm mip-rule explicit service-instance 1
```

- Switch C 的配置

#在该设备上使用 explicit 规则为维护域 MD_B 生成 MIP

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# cfm mip-rule explicit service-instance 2
```

显示验证

经过上述配置后， 在 Switch B 和 Switch C 上分别用以下显示命令来验证配置，这里以 Switch B 为例，Switch 设备显示验证过程是一样的。

- 在 Switch B 显示验证 MIP 生成规则

```
Ruijie# show cfm service-instance 1
Service instance 1:
MD name: MD_A
MA name: MA_A
Level: 6 VLAN: 300 MIP-rule: Explicit CCM interval: 1s
//+可以看到 MIP 生成规则为 Explicit
```

- 在 Switch C 显示验证 MIP 生成规则

```
Ruijie# show cfm service-instance 2
Service instance 2:
```

```
MD name: MD_B
MA name: MA_B
Level: 2 VLAN: 300 MIP-rule: Default CCM interval: 1s
//+可以看到 MIP 生成规则为 Default
```

1.5.4 配置MEP的链路跟踪功能

组网需求

通过 CFM 的连续性检测功能，设备上的 MEP 可以获得该维护域内其他 MEP 的信息。加上配置的 MIP，共同构成维护点（MP），通过链路跟踪功能可以获取到达维护域内其他 MEP 的详细路径。

组网拓扑

如 图 1-11

配置要点

假设要获得 Switch A 上的 MEP 到处在同一个维护域中的 Switch D 上的 MEP 之间的路径，则在 Switch A 上启动链路跟踪功能，则 Switch A 上的 MEP 就会向 Switch D 上的 MEP 发送 LTM。

配置步骤

- Switch A 的配置

#在该设备上启动链路跟踪功能，发起 MEP 是 MEP 1，目标是 Switch D 上的 MEP，其 MEP ID 根据前面的配置可知是 2。

```
Ruijie# cfm linktrace service-instance 1 mep 1 remote-mep 2
```

显示验证

在 Switch A 上执行了链路跟踪功能后，会形成链路跟踪结果信息并保存下来，在该设备上通过以下命令来显示链路跟踪结果。

- 在 Switch A 显示链路跟踪执行结果

```
Ruijie# show cfm linktrace-info service-instance 1
Service instance: 1 MEPID: 1
MAC Address TTL PreHop MAC Relay Action
00d0-F800-6505 63 00d0-F800-6504 FDB
00d0-F800-A852 62 00d0-F800-6505 Hit
```

1.5.5 配置MEP的环回功能

组网需求

可以使用环回功能来验证网络中的某条链路是否连通。

组网拓扑

如 图 1-11

配置要点

假设要验证 Switch A 到 Switch D 之间的链路是否连通，则在 Switch A 上的 MEP 启动链路跟踪功能，Switch A 上的 MEP 就会向 Switch D 上的 MEP 发送 LBM。

配置步骤

- Switch A 的配置

#在该设备上启动环回功能，发起 MEP 是 MEP 1，目标是 Switch D 上的 MEP，其 MEP ID 根据前面的配置可知是 2。

```
Ruijie# cfm loopback service-instance 1 mep 1 remote-mep 2
Loopback to 00d0-f800-8612 with the sequence number start from 2-1000:
Reply from 00d0-f800-8612: sequence number=2-1000
Reply from 00d0-f800-8612: sequence number=2-1001
Reply from 00d0-f800-8612: sequence number=2-1002
Reply from 00d0-f800-8612: sequence number=2-1003
Reply from 00d0-f800-8612: sequence number=2-1004
Loopback Message  Sent:5 Received:5 Lost:0  (%0 loss)
```

显示验证

环回功能的显示验证看上面的命令执行结果就可以，没有专门的命令用来显示验证。

2 REUP

2.1 概述

REUP(Rapid Ethernet Uplink Protection Protocol)提供一个快速上链保护功能。

REUP 的上链端口是成对配置的，其中一个端口为主端口(Active)，另一个端口为从端口(Backup)。在两个端口都正常的情况下，有一个端口会被设置成转发端口(Forward)，另一个端口会被设置备份端口(Standby)，如何判断哪个端口该设置为 Standby 可以由用户配置决定，请参考“ 配置 REUP 的抢占模式和延迟时间”章节获取相关信息。

两个端口都正常的情况下，有一个端口处于备份状态，处于备份状态的端口是不转发数据报文。当处于转发状态的端口发生故障时，备份端口会马上切换成转发状态，提供数据传输，此外 REUP 还会向上游设备发送地址更新报文，使得上游设备可以即时更新 MAC 地址信息。REUP 的这种功能可以保证当链路出现故障后，用户的二层数据流能够在 50ms 以内恢复。

REUP 和 STP 是基于端口互斥的。此时该设备对下运行 STP 协议，对上使用 REUP 来实现上链的备份以及故障保护。REUP 使得用户在关闭 STP 的情况下，仍提供基本的链路冗余，同时提供比 STP 更快的毫秒级故障恢复。

2.2 配置REUP

在配置 REUP 前，必须注意以下事项：

- 一个端口只能属于一个 REUP 对，每一条活动链路只能有一条备用链路，一条备用链路只能作为一条活动链路的备用链路，活动链路和备用链路必须是不同的端口。
- REUP 支持 2 层物理端口和 2 层 AP 口，但不支持 AP 成员口。
- 主从端口不必为同一类型的端口，主端口和从端口的速率也可以不同。例如，你可以将 AP 口作为主端口，物理口设置为从端口。
- STP 在开启了 REUP 的端口上是关闭的。配置了 REUP 的端口不参与 STP 活动。STP 关闭时支持 BPDU 透传，打开 STP 时不支持 BPDU 透传。
- VLAN 负载均衡不支持 Access 端口，支持和 STP 共用。
- 对于 Link State Tracking 功能，每个端口只能属于一个链路状态跟踪组，每台设备最多可以配置 2 个链路状态跟踪组。每个链路状态跟踪组可以有 8 个上行端口(Up Stream)，256 个下行端口(Down Stream)。
- 每台设备最多可以配置 16 个 REUP 对和 8 个地址更新组。每个地址更新组最多可以有 8 个成员口，一个端口可以属于多个地址更新组。
- 对已经配置 REUP 成功的端口，需要禁止把端口变成 3 层口或者把端口加入 AP。同时对于配置 VLAN 负载均衡成功的端口，禁止修改端口的 VLAN 属性。

REUP 各项缺省值如下：

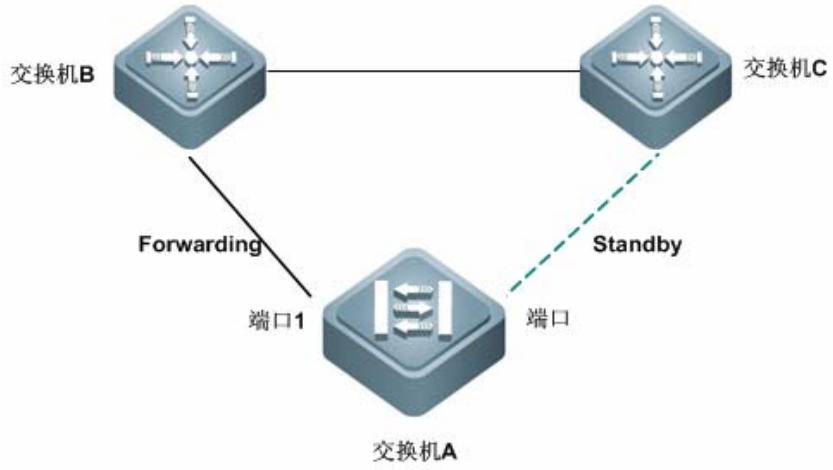
功能特性	缺省值
REUP	Disabled

Preemption mode	Off
Preemption delay	35 seconds
Mac update transit	Disable
MAC update rate	150 *pkts* per second
Mac update receive	Disabled

2.2.1 配置REUP的双链路备份功能

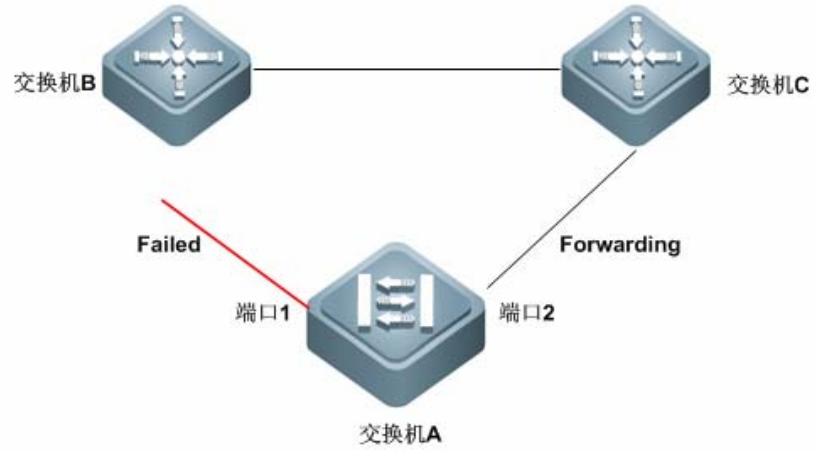
通过指定一个端口作为另外一个端口的备用端口来配置一个 REUP 对。当两个端口正常时，其中的一条链路处于转发状态（转发数据报文），另外一条链路处于备份状态（不转发数据报文）。当活动链路发生故障时，处于备用状态的另外一条链路会迅速切换到转发状态，开始转发数据；当故障链路恢复后，进入备份状态，不转发数据报文。当然了，用户可以通过配置来指定从故障中恢复的链路是否抢占当前处于转发状态的链路。

图 2-1 两条链路都正常的拓扑



例如，如上图拓扑所示，交换机 A 的端口 1，2 连接到上链交换机 B，C 上，在端口 1，2 上配置 REUP。在链路正常的情况下，端口 1 处于转发状态，负责转发数据报文；端口 2 处于备份状态，不转发数据报文。

图 2-2 端口 1 故障后的拓扑



一旦端口 1 发生故障，端口 2 会立即开始转发数据报文，恢复交换机的上链传输。在非抢占模式下，当端口 1 的链路恢复后，端口 1 会处于备份状态，不转发数据报文，端口 2 则继续转发数据报文。

在特权模式下，按下面的步骤去配置一对 REUP：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **interface** *interface-id*	进入接口配置模式
Ruijie(config-if)# **switchport backup interface** *interface-id*	配置一个物理 2 层口(或者二层 AP 口)作为备用端口。
Ruijie(config-if)# **end**	退回到特权模式。
Ruijie# **show interface** [*interface-id*] **switchport backup**	查看配置结果。
Ruijie# **copy running-config startup-config**	保存配置。

例：

```
Ruijie# configure terminal
Enter configuration commands,one per line.  End with CNTL/Z.
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport backup interface gigabitEthernet 0/2
Ruijie(config-if)# show interface switchport backup
Switch Backup Interface Pairs:
Active Interface      Backup Interface      State
------------------------------------------------------------
GigabitEthernet 0/1   GigabitEthernet 0/2   Active Up/Backup Down
```

2.2.2 配置REUP的抢占模式和延迟时间

可以通过配置 REUP 的抢占模式来决定优先使用哪条链路。如果将抢占模式配置为带宽(Bandwith)优先模式，则 REUP 会优先使用一条带宽比较大的链路；当然可以通过把抢占模式设置为强制(Forced)模式，来强制优先使用一条比较稳定可靠的链路。

为了避免异常故障导致频繁的主备链路切换，REUP 提供了一个抢占延迟的功能。当两条链路恢复后，延迟一定时间，等故障链路稳定后再进行链路的切换。

在特权模式下，按下面的步骤去配置一对 REUP 的抢占模式和延迟时间：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **interface** *interface-id*	进入接口配置模式
Ruijie(config-if)# **switchport backup interface** *interface-id*	配置一个物理 2 层口(或者二层 AP 口)作为备用端口。
Ruijie(config-if)# **switchport backup interface** *interface-id* **preemption mode** { **forced** | **bandwidth** | **off** }	设置抢占模式，模式可以是： Forced：主端口一直抢占从端口； Bandwidth：优先使用带宽高的； Off：关闭，不抢占。
Ruijie(config-if)# **switchport backup interface** *interface-id* **preemption delay** *delay-time*	配置抢占的延迟时间，延迟时间只在模式为 Forced 和 Bandwidth 时起作用。
Ruijie(config-if)# **end**	退回到特权模式。

Ruijie# **show interface** [*interface-id*] **switchport backup**	查看配置结果。
Ruijie# **copy running-config startup-config**	保存配置。

例：

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport backup interface gigabitEthernet 0/2 preemption mode forced
Ruijie(config-if)# switchport backup interface gigabitEthernet 0/2 preemption delay  50
Ruijie(config-if)# show interface switchport backup detail
Switch Backup Interface Pairs:
Active Interface      Backup Interface      State
------------------------------------------------------------
GigabitEthernet 0/1   GigabitEthernet 0/2   Active Up/Backup Down
Interface Pair : Gi0/1, Gi0/2
Preemption Mode : forced
Preemption Delay : 50 seconds
Bandwidth : Gi0/1(1000 Mbits), Gi0/2(10 Mbits)
```

REUP 对于 AP 口的 Bandwitdh 属性值采用的是 AP 口的实际带宽，等于 AP 的 Link UP 成员口数*成员口的 Speed 属性值。

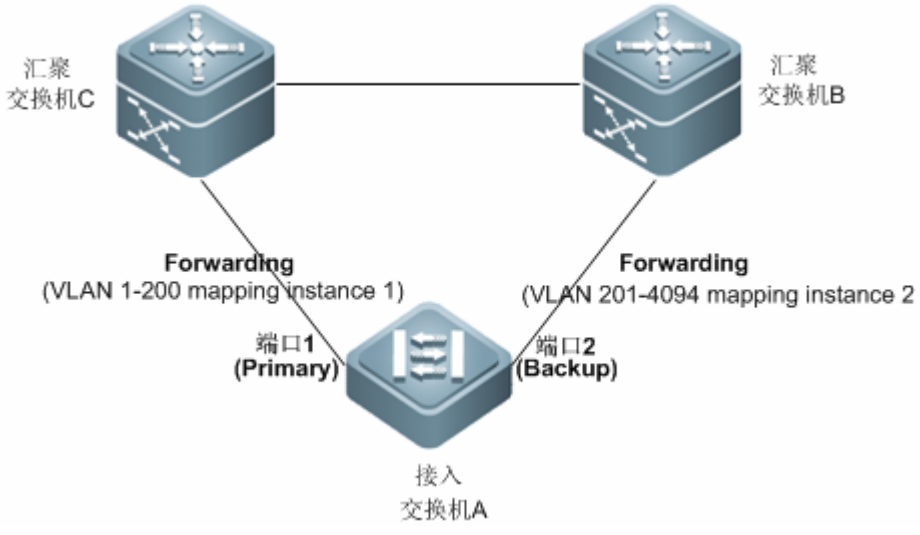
当上链打开 STP 时，REUP 的抢占延迟时间要大于 35 秒。

启用 REUP 的设备，需要关闭所有二层端口的风暴控制功能。

2.2.3 配置REUP的VLAN负载均衡功能

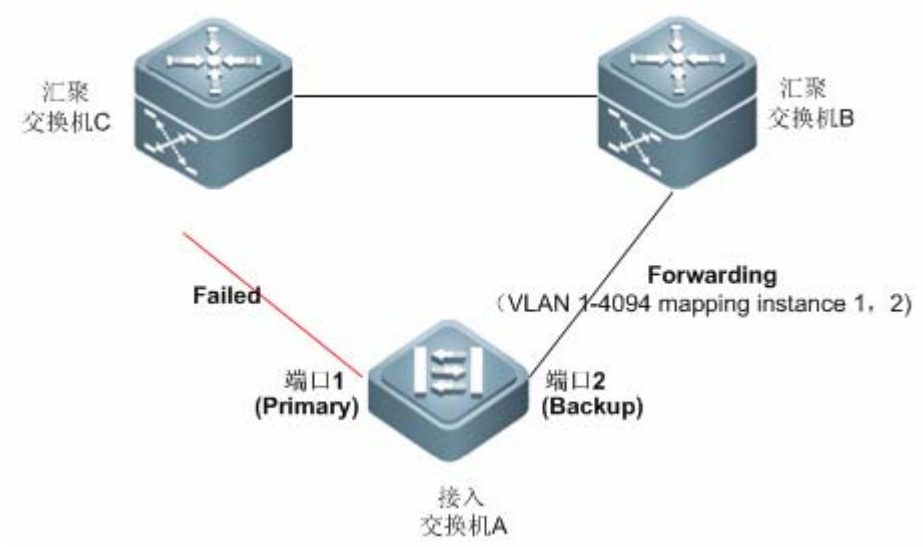
VLAN 负载均衡功能允许 REUP 对的两个端口同时转发互斥 VLAN 的数据报文，以便充分利用链路带宽。

图 2-3 负载均衡两条链路都正常的拓扑



例如，如下图所示拓扑，在交换机 A 的两个端口 1，2 上配置 REUP；启用 REUP 的 VLAN 负载均衡功能，把 VLAN 1-200 映射到实例 1、其它所有 VLAN 映射到实例 2。VLAN 1-200(实例 1)的数据由端口 1 传输，其它所有 VLAN (实例 2)的数据由端口 2 传输。

图 2-4 负载均衡其中一条链路故障的拓扑



当其中的一个端口发生故障时，由另外一个端口负责所有 VLAN 的传输；当发生故障的端口恢复过来，并在抢占延迟内不再故障，则把他负责的 VLAN 的传输从另外一个端口上切换过来。

在特权模式下，按下面的步骤配置 REUP 的 VLAN 负载均衡。

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **interface** *interface-id*	进入接口配置模式
Ruijie(config-if)# **switchport backup interface** *interface-id* **prefer instance** *standby-interface-instance-range*	配置一个 2 层口作为备用端口，并且指明那些实例映射 VLAN 由备用端口负责传输。
Ruijie(config-if)# **end**	退回到特权模式。
Ruijie# **show interface** [*interface-id*] **switchport backup**	查看配置结果。
Ruijie# **copy running-config startup-config**	保存配置。

例：

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#spanning-tree mst configuration
Ruijie(config-mst)#instance 1 vlan 1-200
Ruijie(config-mst)#exit
Ruijie(config)#show spanning-tree mst configuration
Multi spanning tree protocol : Enable
Name      :
Revision : 0
Instance  Vlans Mapped
-------- ---------------------------------------------
```

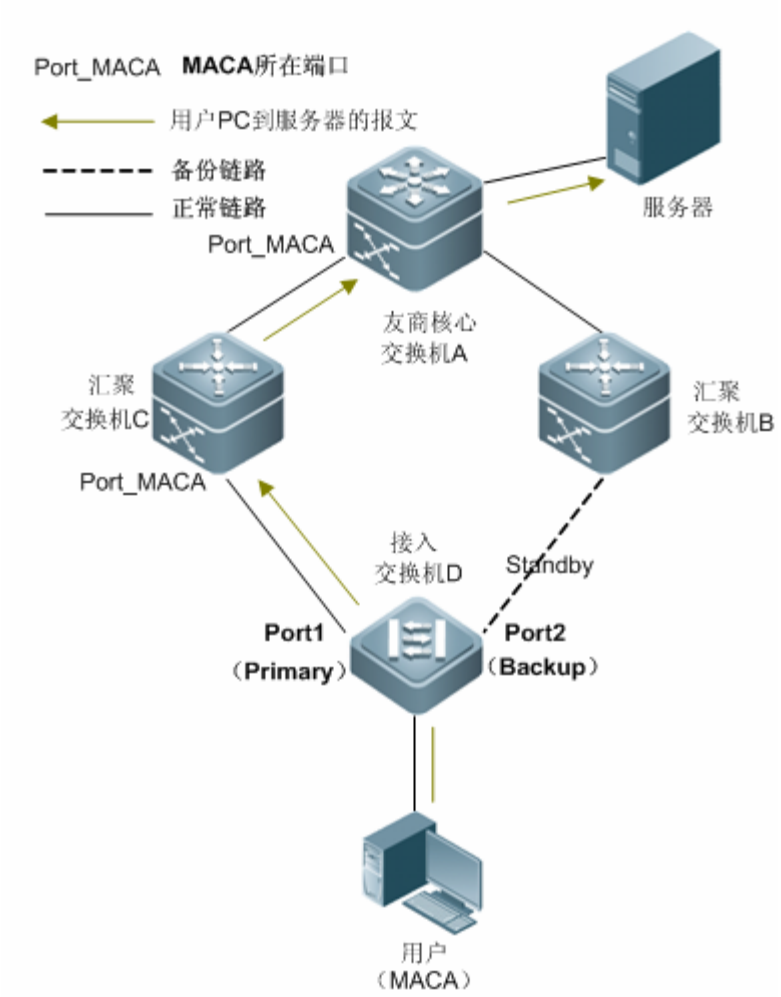
```
0         : 201-4094
1         : 1-200
-------------------------------------------------------
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport backup interface gigabitEthernet 0/2 prefer instance 1
Ruijie(config-if)# end
Ruijie# show interfaces switchport backup
Ruijie(config-if)#show interfaces switchport backup
Switch Backup Interface Pairs:
Active Interface      Backup Interface      State
------------------------------------------------------------------
GigabitEthernet 0/1   GigabitEthernet 0/2   Active Up/Backup Down

Instances Preferred on Active Interface:Instance 0,2-64
          Mapping VLAN 201-4094
Instances Preferred on Backup Interface:Instance 1
          Mapping VLAN 1-200
```

REUP 的 VLAN 负载均衡的实例映射由 MSTP 模块统一控制，具体如何配置实例请参见《配置 MSTP》的说明。

2.2.4 配置REUP的MAC地址更新功能

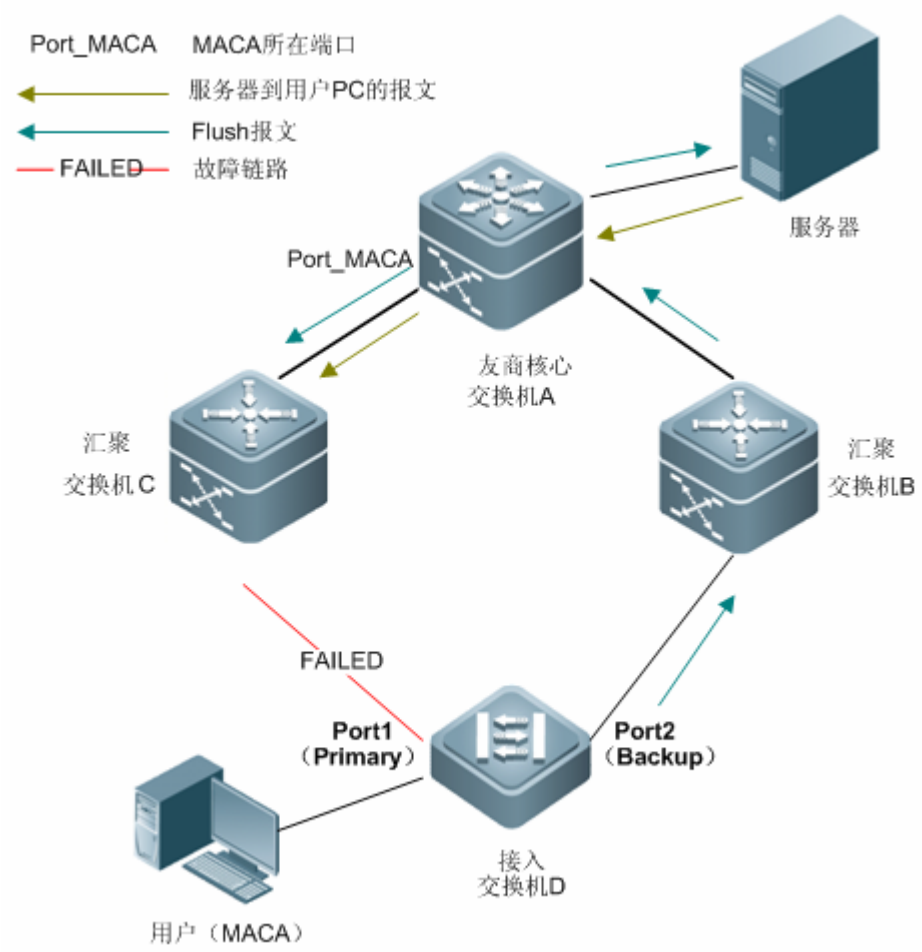
MAC 地址更新功能简介

图 2-5 REUP 的正常工作状态



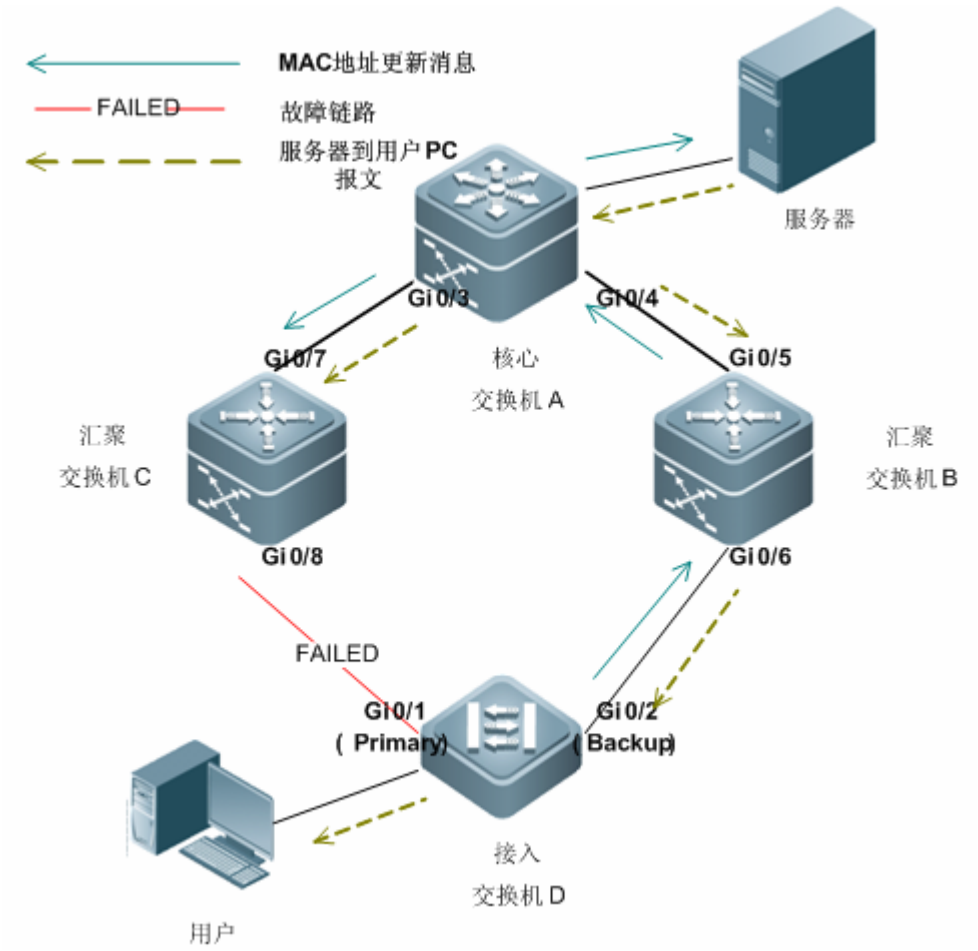
如上图所示拓扑，在交换机 D 的端口 Gi0/1，Gi0/2 上启用 REUP 双链路备份功能，端口 Gi0/1 作为主端口，在正常的通讯过程中，交换机 A 会在连接交换机 C 的端口(Gi0/3)上学习到 PC 的 MAC 地址。

图 2-6 切换过程中的错误状态



在交换机 D 的端口 Gi0/1 发生故障后，端口 Gi0/2 会快速变成转发状态，开始转发数据报文。此时交换机 A 暂时没有从连接交换机 B 的端口(Gi0/4)上学习到 PC 的 MAC 地址，服务器发往 PC 的数据报文会被交换机 A 转发给交换 C，导致服务器到用户 PC 报文丢失。

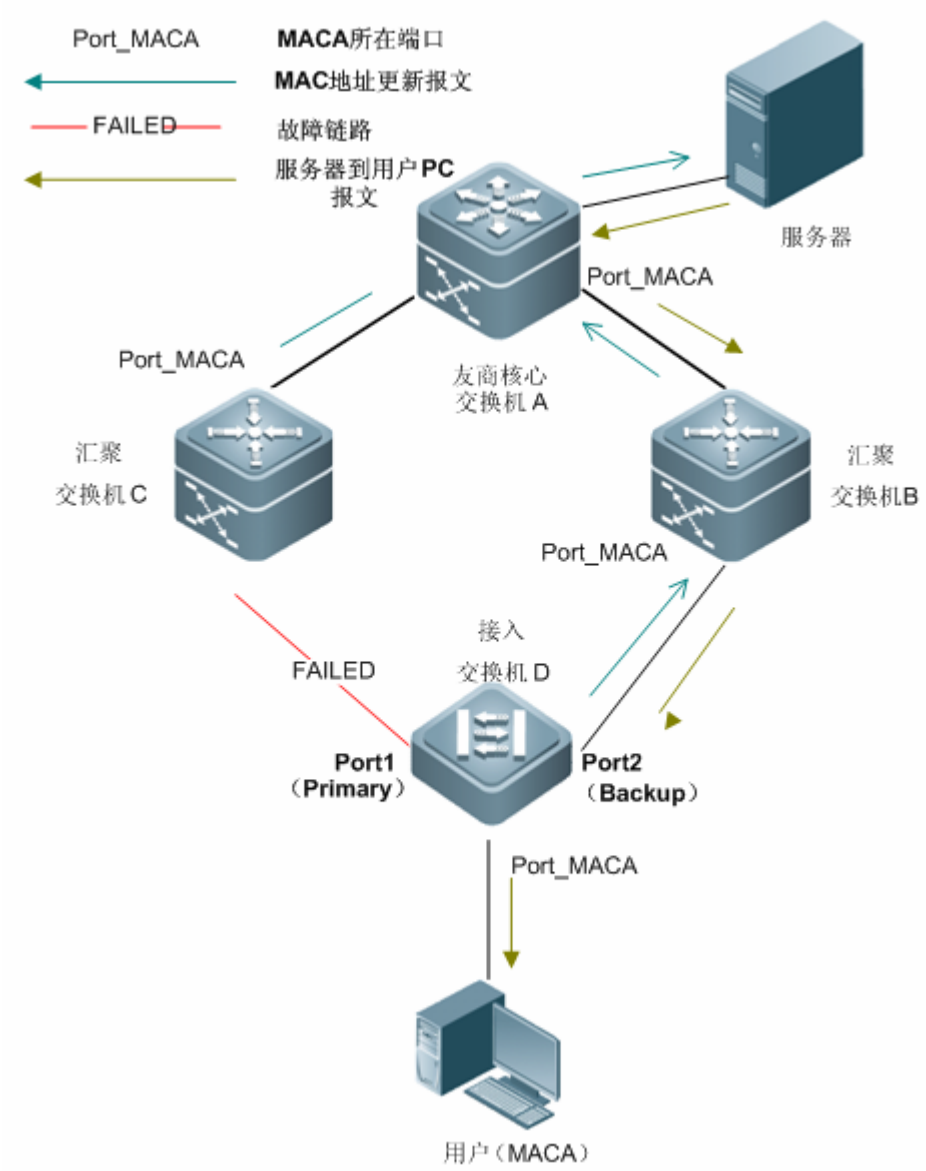
图 2-7 REUP 发送 MAC 地址更新消息后的状态



为了避免上述缺陷，需要在交换机 D 上开启 MAC 地址更新功能，在端口 Gi0/2 开始转发报文时，交换机 D 会往端口 Gi0/2 发送一个 MAC 地址的更新消息。交换机 A 收到 MAC 地址更新消息后，会清除交换机 A 的 Gi0/3 端口上的 MAC 地址。这样交换机 A 就会把服务器发往 PC 的报文转发到连接交换机 B 的端口上，加快报文传输的收敛。

为了减少 MAC 地址更新所引发泛洪的副作用，我们引入一个 MAC 地址更新组的设置。所谓更新组的意思就是，将一组端口归在一个组里，当该组的某个端口收到地址更新消息时，会去更新该组内的其它端口上的 MAC 地址信息。

图 2-8 REUP 发送 MAC 地址更新报文后的状态



为了兼容不支持 MAC 地址更新消息的上游设备，在 Gi0/2 口变成转发状态时，交换机 D 会替用户 PC 往发出 MAC 地址更新报文，让交换机 A 把用户 PC 的 MAC 地址更新到 Gi0/4 口上，恢复交换机 A 的下行数据传输。

配置 REUP 的 MAC 地址更新功能

配置 REUP 的 MAC 地址更新功能，要在交换机上打开发送 MAC 地址消息的功能。

在特权模式开始，按下面的步骤配置交换机发送 MAC 地址更新消息功能。

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **mac-address-table move update transit**	打开交换机的发送 MAC 地址更新消息功能。
Ruijie(config)# **mac-address-table move update max-update-rate** *pkts-per-second*	(可选)配置每秒发送最大 MAC 地址更新报文数量。可选范围为 0-32000，默认为 150。
Ruijie(config)# **interface** *interface-id*	进入接口配置模式

Ruijie(config-if)# **mac-address-table move update transit vlan** *vlan-id*	(可选)配置接口发送 MAC 地址更新消息的 VID。默认在端口的缺省 VLAN 中发送 MAC 地址更新消息。
Ruijie(config-if)# **end**	退回到特权模式。
Ruijie# **show mac-address-table move update**	查看配置结果。
Ruijie# **copy running-config startup-config**	保存配置。

在切换路径上的所有交换机上，打开接收 MAC 地址更新消息的功能，把切换路径上的所有端口加入到同一个 MAC 地址更新组上。

从特权模式开始，按下面的步骤配置交换机接收 MAC 地址更新消息以及地址更新组。

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **mac-address-table move update receive**	打开交换机的接收 MAC 地址更新消息功能。
Ruijie(config)# **no mac-address-table move update receive vlan** *vlan-range*	(可选)配置设备处理 MAC 地址更新消息的 VLAN 范围。默认在所有 VLAN 中处理 MAC 地址更新消息。
Ruijie(config)# **interface** *interface-id*	加入接口模式。
Ruijie(config-if)# **mac-address-table update group** [*number*]	把端口加入 mac 地址更新组。默认加入第一个更新组。
Ruijie(config-if)# **end**	退回到特权模式。
Ruijie(config-if)# **show mac-address-table update group**	查看配置结果。
Ruijie(config-if)# **copy running-config startup-config**	保存配置。

例如，如上图 5 所示拓扑，在交换机 D 的端口 1,2 上开启 REUP 的双链路备份功能

```
Ruijie # configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie (config)# interface gigabitEthernet0/1
Ruijie (config-if)# switchport backup interface gigabitEthernet 0/2
Ruijie (config-if)# end
Ruijie # show interface switchport backup detail
Switch Backup Interface Pairs:
Active Interface       Backup Interface      State
GigabitEthernet 0/1    GigabitEthernet 0/2   Active Up/Backup Standby
Interface Pair : Gi0/1, Gi0/2
Preemption Mode : off
Preemption Delay : 35 seconds
Bandwidth : 100000 Kbit (Gi0/1), 100000 Kbit (Gi0/2)
```

在交换机 D 上打开发送 MAC 地址更新消息的功能。

```
Ruijie # configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie (config)# mac-address-table move update transit
Ruijie (config)# end
Ruijie # show mac-address-table move update
Mac address table move update status:
Transit:enable
```

```
Receive:disable
Pair: Gi0/2,Gi0/1
Members     Status    Transit Count    Last Transit Time
-------------------------------------------------------
Gi0/2       Up        0
Gi0/1       Down      0
```

在上链交换机 A、B、C 上启用接收 MAC 地址更新消息的功能，并把切换路径上的端口设置到同一个地址更新组上。

在交换机 A 上，进行如下配置：

```
Ruijie # configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie (config)# mac-address-table move update receive
Ruijie (config)# interface range gigabitEthernet 0/3-4
Ruijie (config-if-range)# mac-address-table update group
Ruijie (config-if-range)# end
Ruijie # show mac-address-table update group detail
Mac-address-table Update Group:1
Received mac-address-table update message count:0
Group member   Receive Count   Last Receive Switch-ID   Receive Time
-------------------------------------------------------------------
Gi0/3          0               0000.0000.0000
Gi0/4          0               0000.0000.0000
```

在交换机 B 上，进行如下配置：

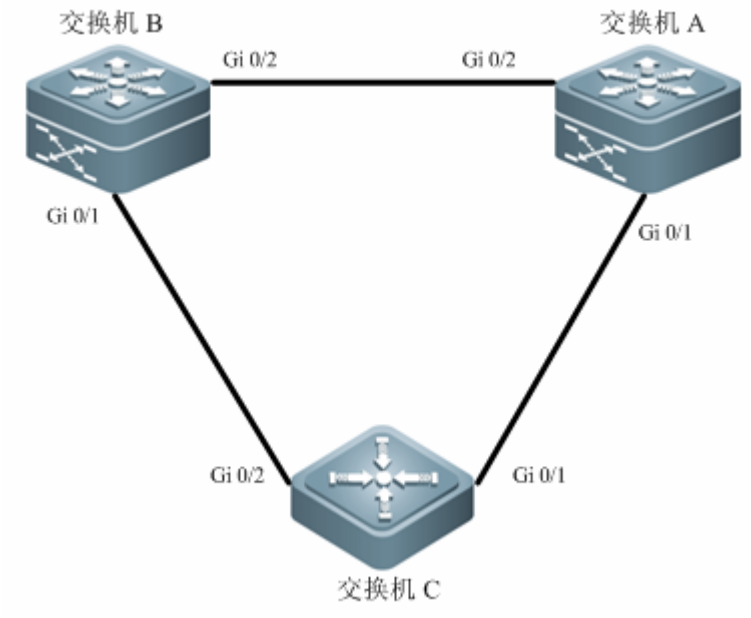
```
Ruijie # configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie (config)# mac-address-table move update receive
Ruijie (config)# interface range gigabitEthernet 0/5-6
Ruijie (config-if-range)# mac-address-table update group
Ruijie (config-if-range)# end
```

在交换机 C 上，进行如下配置：

```
Ruijie # configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie (config)# mac-address-table move update receive
Ruijie (config)# interface range gigabitEthernet 0/7-8
Ruijie (config-if-range)# mac-address-table update group
Ruijie (config-if-range)# end
```

典型应用

图 2-9



拓扑如上图所示，交换机 C 通过端口 Gi 0/1，Gi0/2 连接到上链交换机 A 和 B。为了达到 REUP 的快速双向收敛的效果，我们需要在交换机 C 上打开 REUP 的双链路备份功能，同时在交换机 A 和 B 上打开接收 REUP 的 MAC 地址更新报文功能，并把切换路径上的端口加入到 MAC 地址更新组中。

在交换机 C 上做如下配置：

```
Ruijie # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport backup interface gigabitEthernet 0/2
Ruijie(config-if)# exit
Ruijie(config)# mac-address-table move update transit
Ruijie(config)# end
Ruijie# show mac-address-table move update
Mac address table move update status:
Transit:enable
Receive:disable
Pair: Gi0/1,Gi0/2
Members   Status    Transit Count   Last Transit Time
------------------------------------------------------------------
Gi0/1     Standby   0
Gi0/2     Up        1               Wed Aug 20 10:51:34 2008
```

在交换机 A 和 B 上做如下配置

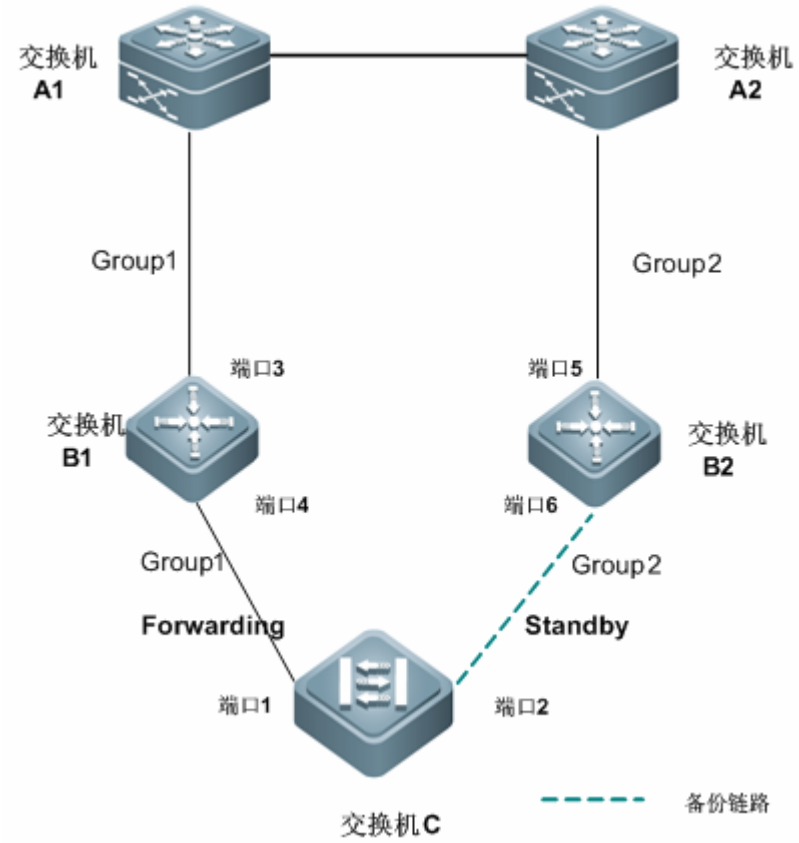
```
Ruijie # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# mac-address-table move update receive
Ruijie(config)# interface range gigabitEthernet 0/1 - 2
Ruijie(config-if-range)# mac-address-table update group
```

```
Ruijie(config-if-range)# end
Ruijie# show mac-address-table update group detail
Mac-address-table Update Group:1
Received mac-address-table update message count:0
Group member    Receive Count    Last Receive Switch-ID    Receive Time
------------------------------------------------------------------------
Gi0/1           0                0000.0000.0000
Gi0/2           0                0000.0000.0000
```

2.2.5 配置链路状态跟踪功能

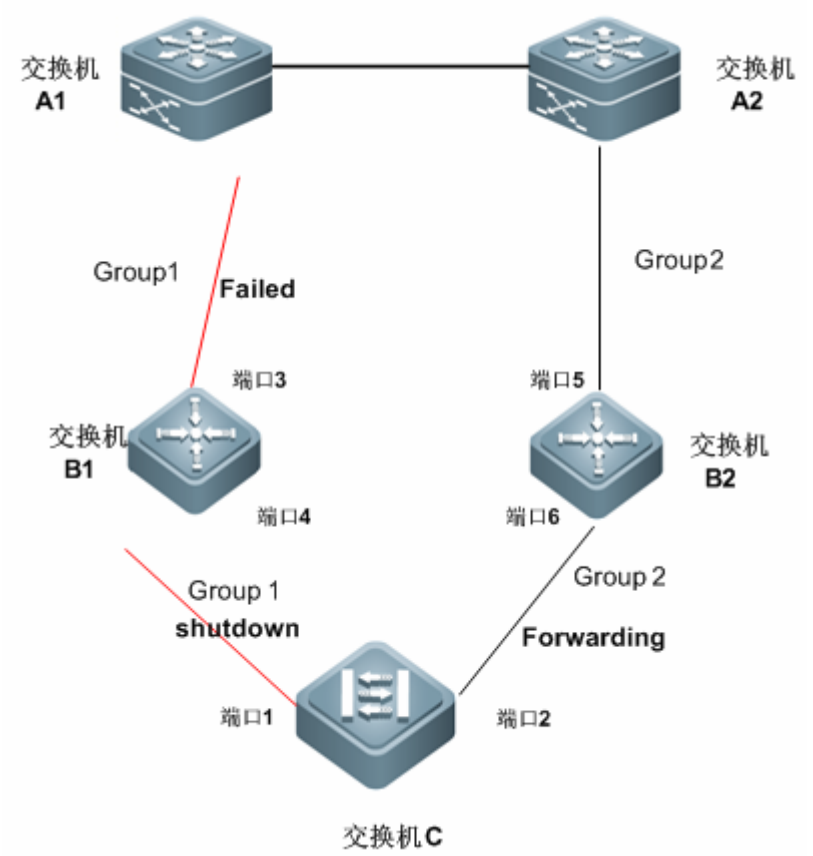
链路状态同步(Link state tracking) 提供上行链路都发生故障，通告下链设备进行链路切换的功能。链路状态同步通过配置链路状态跟踪组的下行端口和下行端口，把多个下行端口的链路状态绑定到多个上行链路的端口上。当跟踪组内所有的上行链路都发生故障，则把下行链路的端口强制 shutdown，使下行链路的传输从主链路切换到备份链路上。

图 2-10 链路跟踪配置例子



如上图所示拓扑：把交换机 B1 的端口 4 设置成组 1 的下行端口，端口 3 设置成上行端口；把交换机 B2 的端 6 设置成组 2 的下行端口，端口 5 设置上行端口；在交换机 C 的端口 1 和端口 2 上开启 REUP 的双链路备份功能。

图 2-11 主链路上链发生故障后的拓扑



当交换机 B1 的上行链路发生故障时，Link State Tracking 会把下行端口 4 快速 Shutdown，使得交换机 C 的上行传输就会被切换到交换机 B2 上。

在特权模式下，按下面的步骤去配置 Link State Tracking。

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **link state track** [*number*]	启用一个链路跟踪组。number 的范围为 1-2，默认启用第一个链路跟踪组(默认 number 的值为 1)。
Ruijie(config)# **interface** *interface-id*	进入接口配置模式
Ruijie(config-if)# **link state group** [*number*] { **upstream** | **downstream** }	设置链路跟踪组的上行端口(upstream)和下行端口(downstream)。number 的范围为 1-2，默认加入第一个链路跟踪组(默认 number 的值为 1)。
Ruijie(config-if)# **end**	退回到特权模式。
Ruijie# **show link state group**	查看配置结果。
Ruijie# **copy running-config startup-config**	保存配置。

例如：在交换机 B1 上，把端口 4 设置成链路跟踪组 1 的下行端口，把端口 3 上行端口。

```
Ruijie# configure terminal
Ruijie(config)# link state track 1
Ruijieconfig)# interface fastethernet 0/4
Ruijie(config-if)# link state group 1 downstream
Ruijie(config)# exit
Ruijie(config-if)# interface fastethernet 0/3
```

```
Ruijie(config-if)# link state group 1 upstream
Ruijie(config-if)# end
```

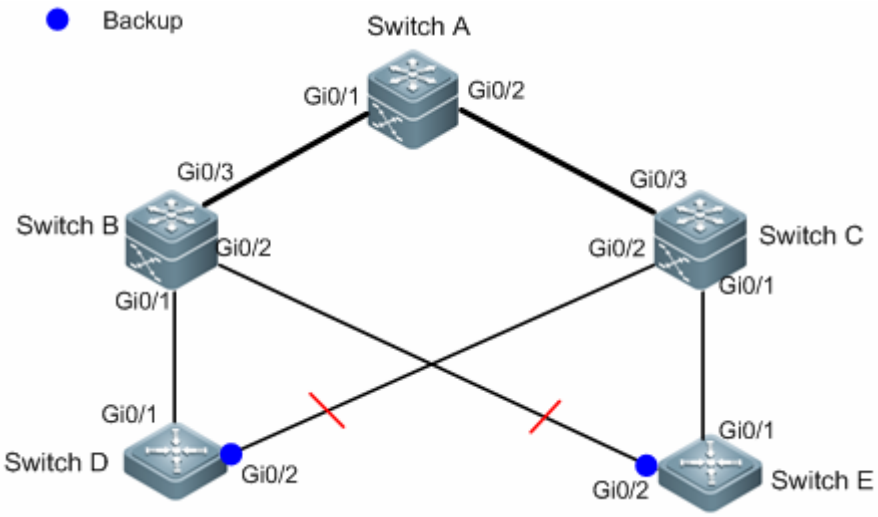
查看 link state group 的状态。

```
Ruijie# show link state group detail
Link State Group:1  Status: Enabled, UP
Upstream Interfaces :Gi0/3(Up)
Downstream Interfaces : Gi0/4(Up)
Link State Group:2  Status: Disabled, Down
Upstream Interfaces :
Downstream Interfaces :
(Up):Interface up   (Dwn):Interface Down   (Dis):Interface disabled
```

2.3 配置举例

拓扑图

图 2-12 REUP 配置拓扑图



应用需求

当下游设备连接到上游设备时，使用单上行方式容易出现单点故障，造成业务中断。通常采用双上行方式，将一台下游设备（Switch D/E）同时连接到两台上游设备（Switch B 和 Switch C），以最大限度地避免单点故障，提高网络可靠性。本例具体要求如下：

- 下游设备（Switch D/E）双上行到上游设备（Switch A），实现链路冗余备份。
- 下游设备（Switch D/E）在链路发生故障时能达到快速双向收敛
- Switch E 的 G0/2 接口为百兆口，G0/1 接口为千兆口。要求当链路故障恢复时能优先选择使用带宽比较大的上行链路。

配置要点

通过运行 REUP 即能满足以上应用需求：

- 通过在下游设备（Switch D/E）上配置 REUP 双链路备份功能，实现主备链路冗余备份。
- 通过在相应的设备上配置 REUP 的 MAC 地址更新功能，来达到网络快速双向收敛的目的：在下游设备（Switch D/E）上打开设备发送 MAC 地址更新消息功能；在上游设备(Switch A/B/C) 打开设备接收 MAC 地址更新消息功能以及配置端口加入同一地址更新组。
- 通过配置 REUP 的抢占模式用来决定优先使用带宽比较大的上行链路。

配置步骤

各设备间均以 Trunk 链路连接，接口相关配置在此不在列举，具体可参考本手册的《接口配置》部分章节。

- Switch D 上的配置

第一步，配置 REUP 对（Gi0/1 口为主端口，Gi0/2 口为从端口）：

```
SwitchD> enable
SwitchD# configure terminal
SwitchD(config)# interface GigabitEthernet 0/1
SwitchD(config-if-GigabitEthernet 0/1)# switchport mode trunk
SwitchD(config-if-GigabitEthernet 0/1)# switchport backup interface GigabitEthernet 0/2
SwitchD(config-if-GigabitEthernet 0/1)# exit
```

第二步，打开发送 MAC 地址更新报文功能：

```
SwitchD(config)# mac-address-table move update transit
```

- Switch E 上的配置

第一步，配置 REUP 对（端口 1 为主端口，端口 2 为从端口）：

```
SwitchE> enable
SwitchE# configure terminal
SwitchE(config)# interface GigabitEthernet 0/1
SwitchE(config-if-GigabitEthernet 0/1)# switchport mode trunk
SwitchE(config-if-GigabitEthernet 0/1)# switchport backup interface GigabitEthernet 0/2
```

第三步， 配置抢占模式：

！配置抢占模式为带宽（bandwidth）模式

```
SwitchE(config-if-GigabitEthernet 0/1)# switchport backup interface gigabitEthernet 0/2 preemption mode
bandwidth
```

！ 配置抢占的延迟时间为 40 秒：

```
SwitchE(config-if-GigabitEthernet 0/1)# switchport backup interface gigabitEthernet 0/2 preemption delay 40
SwitchE(config-if-GigabitEthernet 0/1)# exit
```

第二步，打开发送 MAC 地址更新报文功能：

```
SwitchE(config)# mac-address-table move update transmit
```

- Switch B 上的配置

第一步，打开接收 MAC 地址更新报文功能

```
SwitchB# configure terminal
SwitchB(config)# mac-address-table move update receive
```

第二步，将 REUP 切换路径上的所有端口加入同一个 MAC 地址更新组

本例中，Gi0/1 和 Gi0/3 为 SwitchD 上行链路切换路径上接口，Gi0/3 和 Gi0/2 为 SwitchE 上行链路切换路径上接口；由于一个接口只能加入一个地址更新组，可以把 Gi0/1、Gi0/2 和 Gi0/3 同时加入一个地址更新组。

```
SwitchB(config)# interface range gigabitEthernet 0/1 - 3
SwitchB(config-if-range)# switchport mode trunk
SwitchB(config-if-range)# mac-address-table update group 1
SwitchB(config-if-range)# end
```

- Switch C 上的配置

同 Switch B，不再重复说明。

- Switch A 上的配置

第一步，打开接收 MAC 地址更新报文功能

```
SwitchA# configure terminal
SwitchA(config)# mac-address-table move update receive
```

第二步，将 REUP 切换路径上的所有端口加入同一个 MAC 地址更新组

```
SwitchA(config)# interface range gigabitEthernet 0/1 - 2
SwitchA(config-if-range)# switchport mode trunk
SwitchA(config-if-range)# mac-address-table update group 1
SwitchA(config-if-range)# end
```

配置验证

- 查看 SwitchD 上的 REUP 配置

第一步，查看 SwitchD 端口的双链路备份状态信息

```
SwitchD# show interfaces switchport backup detail
Switch Backup Interface Pairs:
Active Interface   Backup Interface   State
----------------   ----------------   ------------------------
Gi4/1              Gi4/2              Active Up/Backup Standby
Interface Pair : Gi4/1, Gi4/2
Preemption Mode : Off                          //REUP 抢占模式关闭
Preemption Delay : 35 seconds
```

```
Bandwidth : Gi4/1(1000 Mbits), Gi4/2(1000 Mbits)
```

如上信息所示，当链路正常连接（Switch D 的主从端口都 Link up）时，Switch D 的从端口处于 Standby 的备份状态。

第二步，断开 Switch D 的主端口的上行链路，查看设备的状态如下

```
SwitchD# show interfaces switchport backup detail
Switch Backup Interface Pairs:
Active Interface   Backup Interface   State
----------------   ----------------   ---------------------
Gi4/1              Gi4/2              Active down/Backup up
Interface Pair : Gi4/1, Gi4/2
Preemption Mode : Off
Preemption Delay : 35 seconds
Bandwidth : Gi4/1(1000 Mbits), Gi4/2(1000 Mbits)
```

如上信息所示，当 Switch D 的主端口的上行链路出现故障，备份端口会立刻切换成健康转发状态（UP）提供数据传输。

第三步，恢复 Switch D 的主端口的上行链路，查看设备的状态如下

```
SwitchD# show interfaces switchport backup detail
Switch Backup Interface Pairs:
Active Interface   Backup Interface   State
----------------   ----------------   -------------------------
Gi4/1              Gi4/2              Active Standby /Backup up
Interface Pair : Gi4/1, Gi4/2
Preemption Mode : Off
Preemption Delay : 35 seconds
Bandwidth : Gi4/1(1000 Mbits), Gi4/2(1000 Mbits)
```

如上信息所示，由于 Switch D 未配置 REUP 的抢占模式，当的主端口的上行链路恢复，从端口仍然处于转发状态，主端口处于 Standby 的备份状态。

- 查看 SwitchE 上的 REUP 配置

第一步，查看 SwitchE 端口的双链路备份状态信息

```
SwitchE# show interfaces switchport backup detail
Switch Backup Interface Pairs:
Active Interface   Backup Interface   State
----------------   ----------------   ------------------------
Gi4/1              Gi4/2              Active Up/Backup Standby

Interface Pair : Gi0/1, Gi0/2
Preemption Mode : bandwidth              //REUP 带宽优先抢占模式
Preemption Delay : 40 seconds
Bandwidth : Gi0/1(1000 Mbits), Gi0/2(100 Mbits)
```

如上信息所示，当链路正常连接（Switch E 的主从端口都 Link up）时，Switch E 的从端口处于 Standby 状态。

第二步，断开 Switch E 的主端口的上行链路，查看设备的状态如下

```
SwitchD# show interfaces switchport backup detail
Switch Backup Interface Pairs:
Active Interface   Backup Interface   State
----------------   ----------------   ---------------------
Gi0/1              Gi0/2              Active down/Backup up
Interface Pair : Gi0/1, Gi0/2
Preemption Mode : bandwidth
Preemption Delay : 40 seconds
Bandwidth : Gi0/1(1000 Mbits), Gi0/2(100 Mbits)
```

如上信息所示，当 Switch E 的主端口的上行链路出现故障，备份端口会立刻切换成健康转发状态（UP）提供数据传输

第三步，恢复 Switch D 的主端口的上行链路，查看设备的状态如下

上行链路恢复后，延迟时间未到达之前，立即查看设备双链路备份状态信息，主端口的上行链路恢复，处于 Standby 的备份状态；从端口仍然处于转发状态。显示如下：

```
SwitchE# show interfaces switchport backup
Switch Backup Interface Pairs:
Active Interface    Backup Interface   State
----------------    ----------------   ------------------------
Gi0/1               Gi0/2              Active Standby/Backup Up
延迟 40 秒时间到后，CLI 打印如下 LOG 信息：
*Apr 14 22:08:45: %REUP_INTF-5-PREEMPT: Preempting interface Gi0/2 in reup pair (Gi0/1, Gi0/2), preemption mode
is bandwidth
```

再次查看设备双链路备份状态信息，由于配置 REUP 带宽优先抢占模式，REUP 抢占带宽比较大的链路（即 Gi0/1 上行链路）。

```
SwitchE# show interfaces switchport backup
Switch Backup Interface Pairs:
Active Interface   Backup Interface   State
----------------   ----------------   ------------------------
Gi0/1              Gi0/2              Active Up/Backup Standby
Interface Pair : Gi0/1, Gi0/2
Preemption Mode : bandwidth
Preemption Delay : 40 seconds
Bandwidth : Gi0/1(1000 Mbits), Gi0/2(100 Mbits)
```

- 查看上游设备的 REUP 配置

查看 SwitchA 上 MAC 地址更新组信息

```
SwitchA# show mac-address-table update group detail
Mac-address-table Update Group:1
Received mac-address-table update message count:5
Group member   Receive Count   Last Receive Switch-ID   Receive Time
------------   -------------   ----------------------   ------------------------
Gi0/1          2               00d0.f822.35aa           Thu Aug 20 13:42:16 2009
```

```
Gi0/2          3               00d0.f822.33ad          Thu Aug 20 13:43:55 2009
```

查看 SwitchB 上 MAC 地址更新组信息

```
SwitchB# show mac-address-table update group detail
Mac-address-table Update Group:1
Received mac-address-table update message count:5
Group member   Receive Count   Last Receive Switch-ID   Receive Time
------------   -------------   ----------------------   -------------------------
Gi0/1          1               00d0.f822.35ad          Thu Aug  20 13:43:50 2009
Gi0/2          1               00d0.f822.33aa          Thu Aug  20 13:42:44 2009
Gi0/3          3               00d0.f822.35ad          Thu Aug  20 13:43:32 2009
```

查看 SwitchC 上 MAC 地址更新组信息

```
SwitchC# show mac-address-table update group detail
Mac-address-table Update Group:1
Received mac-address-table update message count:6
Group member   Receive Count   Last Receive Switch-ID   Receive Time
------------   -------------   ----------------------   -------------------------
Gi0/1          1               00d0.f822.35aa          Thu Aug  20 13:43:51 2009
Gi0/2          1               00d0.f822.33ad          Thu Aug  20 13:42:43 2009
Gi0/3          3               00d0.f822.35aa          Thu Aug  20 13:43:31 2009
```

3 RLDP

3.1 概述

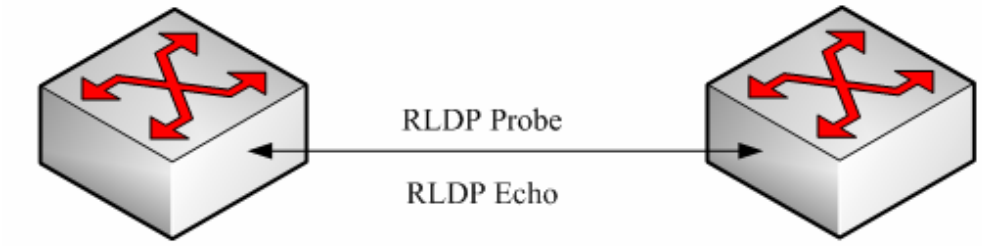
RLDP 全称是 Rapid Link Detection Protocol，是锐捷网络自主开发的一个用于快速检测以太网链路故障的链路协议。

一般的以太网链路检测机制都只是利用物理连接的状态，通过物理层的自动协商来检测链路的连通性。但是这种检测机制存在一定的局限性，在一些情况下无法为用户提供可靠的链路检测信息，比如在光纤口上光纤接收线对接错，由于光纤转换器的存在，造成设备对应端口物理上是 linkup 的，但实际对应的二层链路却是无法通讯的。再比如两台以太网设备之间架设着一个中间网络，由于网络传输中继设备的存在，如果这些中继设备出现故障，将造成同样的问题。

利用 RLDP 协议用户将可以方便快速地检测出以太网设备的链路故障，包括单向链路故障、双向链路故障、环路链路故障。

RLDP 是利用在链路两端交换 RLDP 报文来实现检测的，如下图所示：

图 3-1

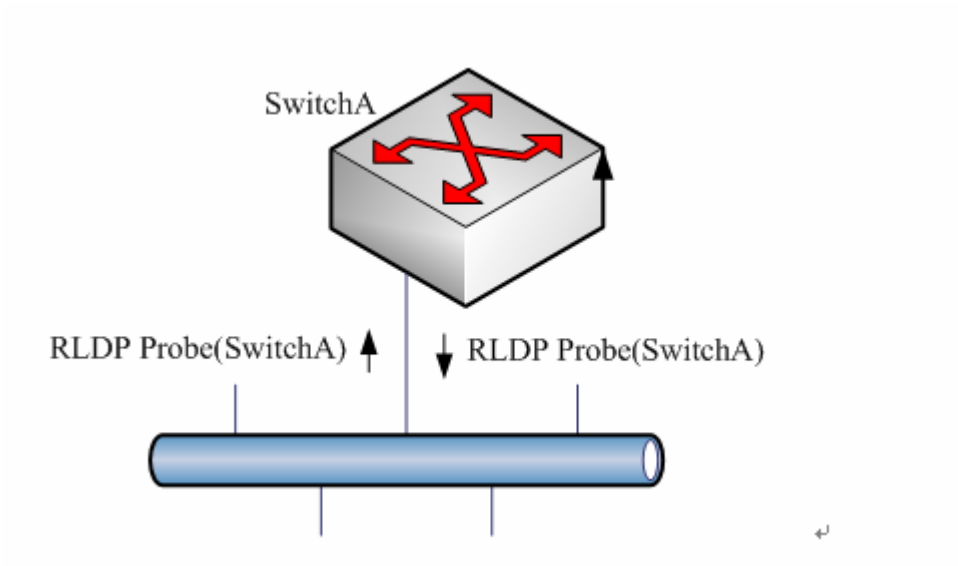


RLDP 定义了两种协议报文：探测报文(Probe)和探测响应报文(Echo)。RLDP 会在每个配置了 RLDP 并且是 linkup 的端口周期性地发送本端口的 Probe 报文，并期待邻居端口响应该探测报文，同时也期待邻居端口也发送自己的 Probe 报文。如果一条链路在物理和逻辑上都是正确的，那么一个端口应该能收到邻居端口的探测响应报文以及邻居端口的探测报文。否则链路将被认定是异常的。

要使用 RLDP 的单向检测和双向检测功能，必须保证链路两端的端口都打开了 RLDP，并且不允许一个开启了 RLDP 的端口下连多个邻居端口，否则 RLDP 无法检测出每个邻居的链路健康状况。

3.1.1 环路检测

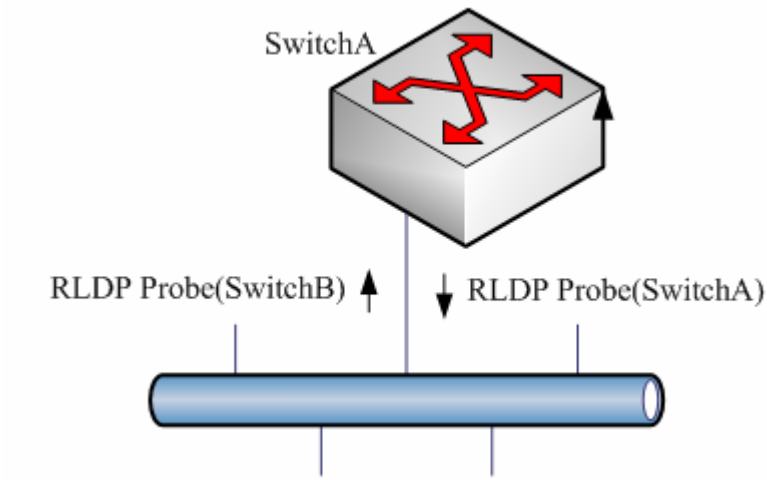
图 3-2 环路检测



所谓的环路故障是指端口连接的链路上出现了环路。如上图所示，RLDP 在某个端口上收到了本机发出的 RLDP 报文，则该端口将被认为是出现了环路故障，于是 RLDP 会根据用户的配置对这种故障做出处理，包括警告、设置端口违例、关闭端口所在的 svi、关闭端口学习转发等。

3.1.2 单向链路检测

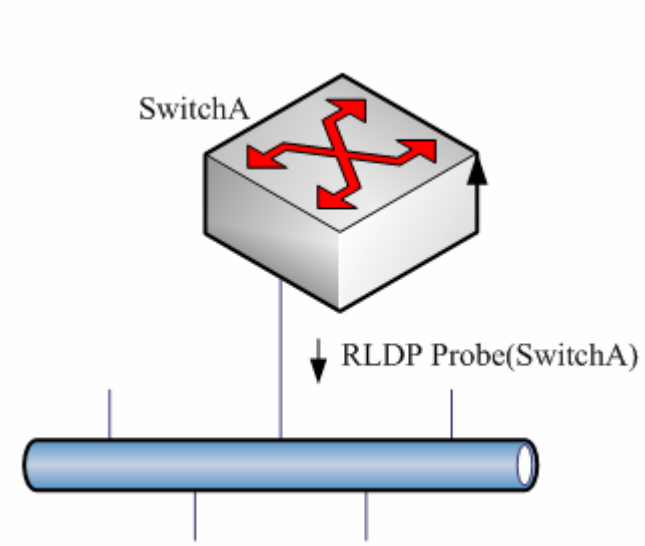
图 3-3 单向链路检测



所谓单向链路故障是指端口连接的链路只能接收报文或者只能发送报文(比如由于光纤接收线对接错误导致的单向接收或单向发送）。如上图所示，RLDP 在某个端口上只收到邻居端口的探测报文则该端口将被认为单向链路故障，于是 RLDP 会根据用户的配置对这种故障做出处理。另外如果端口无法收到任何 RLDP 检测报文，也会被认为是发生了单向链路故障。

3.1.3 双向链路检测

图 3-4 双向链路检测



所谓双向链路故障是指链路两端的帧收发都出现了故障。如上图所示，设备的端口在发出 RLDP 探测报文后，就一直无法接收到响应报文或邻居的探测报文，那么该链路将被认为是双向故障的。从故障性质上讲，双向故障实际上包含了单向故障。

- 如果链路两端有某一方未开启 RLDP 也会被诊断为双向或单向链路故障，因此配置双向链路检测或单向链路检测时需要管理员保证链路两端都开启了 RLDP，以避免出现错误的诊断信息。
- RLDP 协议缺省情况下只发送 SNAP 格式的报文（SNAP 封装中，DSAP 和 SSAP 字段固定为 0xAA，Control 字段固定为 0x03，通过 PID 字段来区分标识协议，对于 RLDP，PID 字段取值为 0x0788）。当收到 Ethernet II 格式的协议报文时，迁移到只发送 Ethernet II 格式的协议报文与邻居交互。因此，版本兼容的前提是需要能收到邻居的协议报文。这样，当 10.4(3)以上软件版本与其他软件版本互连时，如果对端已检测出链路故障，建议先恢复链路的错误状态。

3.2 配置RLDP

功能特性	默认值
全局 RLDP 状态	DISABLE
端口 RLDP 状态	DISABLE
探测间隔	3S
最大探测次数	2 次

- RLDP 只能基于物理端口进行配置，包括 ap 成员口(支持 L2 和 L3 的 AP 成员口)，但无法在 SVI 上配置。对于 AP 口的配置是发散到该 AP 的每个成员口生效。

3.2.1 配置全局RLDP

只有全局的 RLDP 打开，端口 RLDP 才能运行。

在全局配置模式下，按如下步骤打开 RLDP：

命令	作用
Ruijie(config)# **rldp enable**	打开全局的 RLDP 功能开关。
Ruijie(config)# **no rldp enable**	关闭全局的 RLDP。

3.2.2 配置端口RLDP

RLDP 是基于端口运行的，因此用户需要显式配置那些端口需要运行 RLDP。另外在配置端口 RLDP 时，需要同时指定该端口的诊断类型以及故障处理方法。诊断类型包括：unidirection-detect（单向链路检测）、bidirection-detect（双向链路检测）、loop-detect（环路检测）。故障处理方法包括：warning（警告）、block（关闭端口学习转发）、shutdown-port（设置端口违例）、shutdown-svi（关闭端口所在的 svi）。

在配置模式下，按如下步骤设置端口 RLDP 功能：

命令	作用
Ruijie(config)# **interface** *interface-id*	进入接口模式
Ruijie(config-if)# **rldp port** { **unidirection-detect | bidirection-detect | loop-detect** } { **warning | shutdown-svi | shutdown-port | block** }	端口打开 RLDP，同时配置诊断类型和故障处理方法。
no rldp port { **unidirection-detect | bidirection-detect | loop-detect** }	关闭端口的 RLDP。只能逐一关闭已经配置的检测类型。

例：在 AP 成员口 GigabitEthernet 0/5 上配置 RLDP 并指定多个诊断类型和故障处理方法

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/5
Ruijie(config-if)# port-group 1
Ruijie(config-if)# rldp port unidirection-detect shutdown-svi
Ruijie(config-if)# rldp port bidirection-detect warning
Ruijie(config-if)# rldp port loop-detect block
Ruijie(config-if)# end
Ruijie# show rldp interface gigabitEthernet 0/5
port state      : normal
local bridge    : 00d0.f822.33ac
neighbor bridge : 0000.0000.0000
neighbor port   :
unidirection detect information:
action : shutdown svi
state  : normal
bidirection detect information :
action : warnning
```

```
state  : normal
loop detect  information       :
action : block
state  : normal
```

注意事项

配置端口检测有以下注意事项：

- 路由口不支持 shutdown-svi 的错误处理方法，因此该方法在路由口发生检测错误时将不被执行。
- 配置环路检测时要求端口下连的邻居设备不能开启 RLDP 检测，否则该端口将无法做出正确的检测。
- 如果 RLDP 检测出链路错误，则会发出警告信息。用户可以通过配置 log 功能将这些警告信息发到 log 服务器，记录 log 的级别至少要保证可以记录 3 级日志。
- 由于产品特性的不同，某些产品对于 block 的端口仍然会将报文送 cpu, 这就导致在配置诊断类型为环路检测、故障处理方法为 block 时，当设备检测出环路并将端口 block 处理后，仍会有大量的报文送 cpu,这样就未能达到环路检测的效果，所以建议在指定环路检测的诊断类型时选择 shutdown-port 的故障处理方法。
- RLDP 故障处理方法中的 block 功能需要和 STP 互斥。也就是说如果用户配置了端口的故障处理方法为 block，则建议关闭 STP，否则由于 STP 无法识别单向链路，可能会出现 STP 允许端口转发，但 RLDP 却设置端口 block 的情况。如果要和 STP 共用，建议将错误处理方法配置为”shutdown-port”。
- 对于 AP 成员口上的 RLDP 配置，如果是配置环路检测，则会同步配置到该 AP 的所有成员口，如果是配置单向链路检测和双向链路检测，则直接在 AP 成员口生效。
- 对于物理口加入 AP 的情况，新加入的 AP 成员口的环路检测配置需要和该 AP 现有的成员口的环路检测配置一致。这里分 3 种情况：1）如果新加入的 AP 成员口没有配置环路检测，而该 AP 现有的成员口有配置环路检测，则新加入的 AP 成员口同步环路检测的配置和检测结果。2）如果新加入的 AP 成员口有配置环路检测，而该 AP 现在的所有成员口都没有配置环路检测，则新加入的 AP 成员口清除环路检测配置并加入 AP。3）如果新加入的 AP 成员口的环路检测配置和该 AP 现有的成员口的环路检测配置不一致，则新加入的 AP 成员口同步环路检测的配置和检测结果。
- AP 成员口配置 RLDP 时，故障处理方法只能配置为”shutdown-port”，如果故障处理方法配置为非”shutdown-port”时，将转换成”shutdown-port”的配置并生效。

3.2.3 配置RLDP的探测间隔

打开了 RLDP 功能的端口将周期性地发出 RLDP Probe 报文。

在全局配置模式下，按如下步骤配置 RLDP 探测间隔：

命令	作用
Ruijie(config)# **rldp detect-interval** *interval*	配置探测间隔，interval 取值范围是 2-15s,默认是 3s。
Ruijie(config)# **no rldp detect-interval**	探测间隔恢复缺省值。

3.2.4 配置RLDP的最大探测次数

打开了 RLDP 功能的端口如果在最大探测期（最大探测次数×探测间隔）内仍然无法接收到邻居的报文，则该端口将被诊断为故障，具体的故障类型请参考概述章节。

在全局配置模式下，按如下步骤配置 RLDP 最大探测次数：

命令	作用
Ruijie(config)# **rldp detect-max** *num*	配置最大探测次数，num 取值范围是 2-10,默认是 2 次。
Ruijie(config)# **no rldp detect-max**	恢复默认值

最多探测次数只有在单向链路检测和双向链路检测下才会起作用，如果某个端口只开启了环路检测，该值将失效。

3.2.5 恢复端口的RLDP状态

配置了 shutdown-port 故障处理的端口在出现故障后将无法主动恢复 RLDP 检测，如果用户确认故障已经解决了，则可以使用恢复命令重新启动被 shutdown 端口的 RLDP。该命令也会将其它有检测出错误的端口重新恢复。

在特权配置模式下，按如下步骤恢复端口的 RLDP 检测：

命令	作用
Ruijie# **rldp reset**	使所有 RLDP 检测失败的端口重新开始检测。

用户也可以在全局配置模式下使用 **errdisable recover** 命令来即时或定时重新启动被 rlp 设置成违例的端口的 RLDP 检测。

3.2.6 查看RLDP信息

查看所有端口的 RLDP 状态

在特权模式下使用如下命令查看 RLDP 的全局配置和所有配置了 rldp 检测的端口的检测信息：

命令	作用
Ruijie# **show rldp**	查看 RLDP 的全局配置和所有配置了 rldp 检测的端口的检测信息。

以下例子使用 **show rldp** 命令查看 rldp 所有端口的检测信息：

```
Ruijie# show rldp
rldp state          : enable
rldp hello interval : 3
rldp max hello      : 2
rldp local bridge   : 00d0.f8a6.0134
------------------------------------------------

interface GigabitEthernet 0/1
port state:normal
```

```
neighbor bridge : 00d0.f800.41b0
neighbor port   : GigabitEthernet 0/2
unidirection detect information:
action : shutdown svi
state  : normal
interface GigabitEthernet 0/24
port state:error
neighbor bridge : 0000.0000.0000
neighbor port   :
bidirection detect information :
action : warnning
state  : error
```

从上述信息可以看到，端口 GigabitEthernet 0/1 配置了单向检测，并且当前未检测到错误，端口状态为正常(normal)。端口 GigabitEthernet 0/24 配置了双向检测，并且检测到了双向故障。

查看指定端口的 RLDP 状态

在特权模式下使用如下命令查看指定端口的 RLDP 检测信息：

命令	作用
show rldp interface *interface-id*	查看 *interface-id* 的 rldp 检测信息。

以下例子使用 show rldp interface GigabitEthernet *0/1* 命令查看 fas0/1 端口的 rldp 检测信息：

```
Ruijie# show rldp int GigabitEthernet 0/1
port state      : error
local bridge    : 00d0.f8a6.0134
neighbor bridge : 00d0.f822.57b0
neighbor port   : GigabitEthernet 0/1
unidirection detect information:
action: shutdown svi
state : normal
bidirection detect information :
action : warnning
state : normal
loop detect  information    :
action: shutdown svi
state : error
```

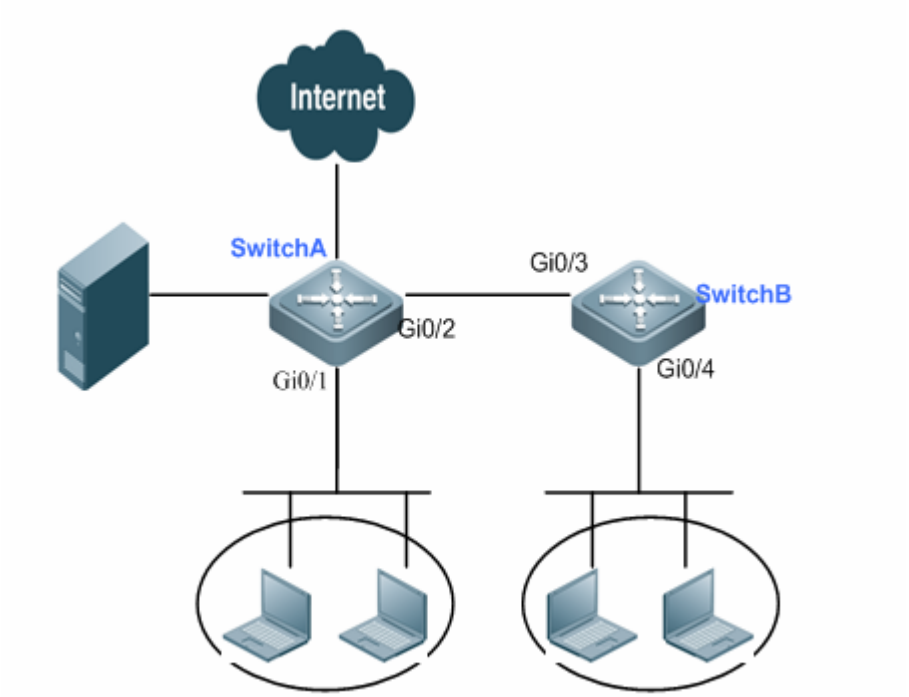
从上述信息可以看到，端口 GigabitEthernet 0/1 配置了三种检测类型：单向检测、双向检测、环路检测,故障时的错误处理分别为关闭端口所在的 svi、产生警告信息、关闭端口所在的 svi，其中环路检测发现了错误，使得当前的端口状态为 error，相应的，该端口所属的 svi 也被 shutdown。

3.3 配置举例

3.3.1 RLDP故障检测与处理

拓扑图

图 3-5 RLDP 应用拓扑图



应用需求

如上图所示，企业各部门用户通过设备 Switch A、Switch B 接入网络。由于链路中断或者用户人为造成网络环路等非设备因素造成网络中断，通过配置 RLDP 环路检测以及单双向链路检测功能，能迅速定位并处理故障，从而及时恢复网络，降低网络中断给企业带来的业务损失。主要需求有：

- 一旦检测到环路故障或者单双向链路故障，则根据配置的故障处理方法作故障处理；
- 若配置了 shutdown-port 故障处理的端口出现故障，要求主动恢复其 RLDP 检测，并使所有 RLDP 检测失败的端口重新开始检测。

配置要点

- 配置全局 RLDP 后再配置端口 RLDP，同时配置诊断类型和故障处理方法。

对环路检测来说，下联端口（在企业各部门用户或服务器上连接设备的端口）不能开启 RLDP；对单双向链路检测来说，设备对接端口 RLDP 都需开启。若端口为路由口，则只能用 warning、block 或 shutdown-port 故障处理方法，不支持 shutdown-svi 故障处理方法。

- 在特权模式下，使用 **rldp reset** 命令使所有 RLDP 检测失败的端口重新开始检测。

配置步骤

第一步，在设备上开启 RLDP。

！在 Switch A 上开启全局 RLDP。

```
SwitchA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)#rldp enable
```

！Switch B 的配置同上。

第二步，在设备端口上配置诊断类型与故障处理方法。

！在 Switch A 上开启端口 RLDP，并在端口 Gi0/1 上配置环路检测及故障处理方法 block，在端口 Gi0/2 上配置单向链路检测及故障处理方法 warning。

```
SwitchA(config)#interface gigabitEthernet 0/1
SwitchA(config-if)#rldp port loop-detect block
SwitchA(config-if)#exit
SwitchA(config)#interface gigabitEthernet 0/2
SwitchA(config-if)#rldp port unidirection-detect warning
SwitchA(config-if)#exit
```

！在 Switch B 上开启端口 RLDP，并在端口 Gi0/4 上配置环路检测及故障处理方法 block，在端口 Gi0/3 上配置双向链路检测及故障处理方法 shutdown-port。

```
SwitchB(config)#interface gigabitEthernet 0/4
SwitchB(config-if)#rldp port loop-detect block
SwitchB(config-if)#exit
SwitchB(config)#interface gigabitEthernet 0/3
SwitchB(config-if)#rldp port bidirection-detect shutdown-port
SwitchB(config-if)#exit
```

第三步，恢复端口 RLDP 检测。

！在 Switch A 上执行 **rldp reset** 命令。

```
SwitchA#rldp reset
```

！Switch B 的配置同上。

配置验证

查看设备所有端口的 RLDP 信息。

！ Switch A 所有端口的 RLDP 信息

```
SwitchA#show rldp
rldp state         : enable
rldp hello interval: 3
rldp max hello     : 2
rldp local bridge  : 00d0.f822.33aa
----------------------------------
Interface GigabitEthernet 0/2
port state      : normal
neighbor bridge : 00d0.f800.41b0
neighbor port   : GigabitEthernet 0/3
unidirection detect information:
     action: warning
     state : normal

Interface GigabitEthernet 0/1
port state      : normal
neighbor bridge : 0000.0000.0000
neighbor port   :
loop detect information   :
     action: block
     state : normal
```

！ Switch B 所有端口的 RLDP 信息

```
SwitchB#show rldp
rldp state         : enable
rldp hello interval: 3
rldp max hello     : 2
rldp local bridge  : 00d0.f800.41b0
----------------------------------
Interface GigabitEthernet 0/3
port state      : normal
neighbor bridge : 00d0.f822.33aa
neighbor port   : GigabitEthernet 0/2
bidirection detect information:
     action: shutdown-port
     state : normal

Interface GigabitEthernet 0/4
port state      : normal
neighbor bridge : 0000.0000.0000
neighbor port   :
loop detect information    :
     action: block
```

```
    state : normal
```

4 DLDP

4.1 概述

DLDP 全称是 Data Link Detection Protocol，是一种基于快速检测以太网链路故障的检测协议。

一般的以太网链路检测机制都只是利用物理连接的状态，通过物理层的自动协商来检测链路的连通性。但是这种检测机制存在一定的局限性，在一些情况下无法为用户提供可靠的链路检测信息，比如在光纤口上光纤接收线对接错，由于光纤转换器的存在，造成设备对应端口物理上是 linkup 的，但实际对应的链路却是无法通讯的。再比如两台以太网设备之间架设着一个中间网络，由于网络传输中继设备的存在，如果这些中继设备出现故障，将造成同样的问题。

这样的问题，通常导致实际链路已经不通，但三层以上的各种协议却收敛很慢，主要依赖于各协议自身的收敛性能。

DLDP 将通过 ICMP echo 报文的检测来解决这类问题。DLDP 通过在三层接口（SVI、Routed Port、L3 AP）下不断的发出 IPv4 ICMP echo 进行通路检测，如果在指定时间内对端设备没有回应 ICMP reply，则 DLDP 认为这个接口通路出现问题，将该接口设置为“三层接口 DOWN”，于是触发各三层上的协议各种收敛、备份切换动作。

由于 DLDP 只是设置“三层接口 DOWN”，实际物理链路还是连通的（STP、802.1x 等二层协议还将继续正常通讯），因此 DLDP 还是可以继续发出 ICMP echo 报文，如果对端设备恢复响应了 ICMP reply，则三层接口恢复 UP，恢复正常通讯。

4.1.1 DLDP的检测IP和下一跳IP

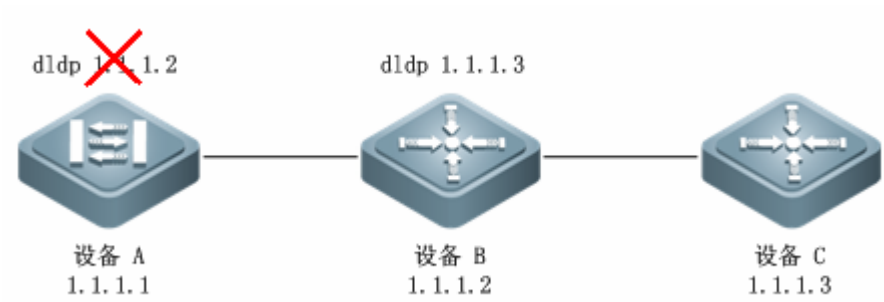
为实现 DLDP 功能，需要在三层接口下配置 DLDP 检测 IP。

一个三层接口下，DLDP 可以配置多个 IP 检测，当所有 IP 都没有 ICMP 响应时，才认为接口 DOWN；而一旦有一个 IP 恢复通讯，则认为接口恢复 UP。

在某些情形下，DLDP 需要检测非直连网段的 IP 可达性。这时需要配置该接口的下一跳 IP，以便 DLDP 能够通过 ARP 报文获取下一跳 MAC 地址，正确的封装 ICMP 报文发出。但这种情形，一定要避免响应报文从其他链路回应的情形，这样就直接造成 DLDP 误判该接口没有收到 ICMP 应答。

对于已配置 DLDP 检测的三层接口，其接口上配置的 IP 地址不宜作为其它设备的 DLDP 检测 IP 地址，以防止该三层接口的 DLDP 检测出现异常时，其它设备的 DLDP 检测也出现异常。如图 1-1 所示，在设备 B 的三层口上配置了检测 IP 地址为 1.1.1.3 的 DLDP 检测(该检测 IP 地址为设备 C 的 IP 地址)，同时在该三层口上配置 IP 地址 1.1.1.2，那么，不应该在设备 A 的三层口上配置检测 IP 地址为 1.1.1.2 的 DLDP 检测，因为当 B 至 C 的链路发生异常时，设备 B 上的三层口就会 DOWN 掉，此时设备 A 的 DLDP 检测也会随之出现异常。

图 1-1 DLDP 检测 IP 错误配置示意图



DLDP 使用该三层接口的第一个 IP 地址作为报文的源 IP 地址进行通讯。

由于交换机有 CPP、NFPP 功能来控制 ICMP 报文的收发速率，所以在进行多个 IP 检测时，一定要注意 CPP、NFPP 所设置的收发包速率要大于 DLDP 报文的总收发包速率。例如：缺省值情况下每个 DLDP 检测点所占用的 ICMP 报文速率为 10pps，当 DLDP 检测 IP 数目为 100 个时，整机设备的 ICMP 报文流量已经到达至少 1000pps 了。这时，对应的 CPP 的 ICMP 控制需要调到适当值。

4.1.2 DLDP的检测周期

DLDP 可以配置“检测报文的发送间隔”、“重传次数”，以便能适用更多样的网络环境。

当网络设备在“检测报文的发送间隔”×“重传次数”的时间周期内没有收到对端的应答报文，则认为三层接口 DOWN。一旦恢复正常通讯，则三层接口 UP。

4.1.3 DLDP的被动模式

在实际网络连接中，如果两端设备都打开 DLDP，双方互发 ICMP echo 也是可以达到通路检测功能的，但这样明显存在多余重复的报文。

实际就只要有一端设备使用 ICMP echo 发包，另一端用同样的检测参数来确认报文的及时可达，一样能达到双方设备检测链路通路的效果，同时也节省了带宽资源和设备 CPU 资源的消耗。

于是，我们称主动发 ICMP echo 的为主动模式（缺省配置即是如此），被动接收对端 ICMP echo 发包的为被动模式。

无论是主动，还是被动模式，都需要确保对端设备的时间参数配置与本设备完全一致，以便同步链路状态效果的检测。否则可能因对端发包间隔、重传次数的不同步而引起链路状态的误判。

4.1.4 DLDP的恢复次数

在有些情形下，检测链路可能不太稳定，比如 PING 断了三次，通一次，又断了多次。如果按简单的逻辑，其中的 DLDP 检测就是 UP、DOWN 多次，实际可能更加剧了不稳定。

恢复次数表示链路从 DOWN 状态为 UP 状态前，需要收到连续的 DLDP 检测报文响应次数。恢复次数缺省为 3 次，即只有该链路上连续 PING 通了 3 次才会 UP。这种情况下，虽然可能使链路检测会相对不那么灵敏，但增加了稳定性，因此相关参数在实际应用中还可根据实际网络情况进行调整。

4.1.5 DLDP的MAC绑定功能

在某些情形下，网络中可能存在 ARP 欺骗现象，用户可以通过将检测 IP 与对应设备的 MAC 地址进行绑定(若 DLDP 检测配置了下一跳 IP，则需要将下一跳 IP 与下一跳 IP 所对应设备的 MAC 地址进行绑定)来防止网络中的 ARP 欺骗对 DLDP 检测功能的影响。

4.2 配置DLDP

4.2.1 启动DLDP检测

缺省情况下，接口关闭 DLDP 功能。

命令	作用
Ruijie(config)# **interface** *interface-name*	进入三层接口
Ruijie(config-if)# **dldp** *ip-address* **route-switch** [**mac-address** *mac-address* | **next-hop** *ip-address* [**mac-address** *nexthop-mac-address*]] [**interval** *tick*] [**retry** *retry-num*] [**resume** *resume-num*]	启动 DLDP 检测，设置对端设备的 IP 地址。 **route-switch**：与静态路由联动功能，可实现静态路由切换 **mac-address** *mac-address*：检测 IP 所绑定的 MAC 地址。 **next-hop** *ip-address*：下一跳 IP 地址。 **mac-address** *nexthop-mac-address*：下一跳 IP 所绑定的 MAC 地址。 **Interval** *tick*：检测报文的发送间隔。取值范围：1-6000 tick（1 tick =10 毫秒），缺省值 100 tick（1s）。 **retry** *retry-num*：检测报文的重传次数。取值范围：1-3600，缺省值 4。 **resume** *resume-num*：恢复次数。取值范围：1-200，缺省值 3。

接口上可以多次配置此命令，启动与多个对端设备的 DLDP 检测。

DLDP 检测依赖 ICMP ECHO 报文，对端设备上必须打开 ICMP 响应功能。

如果跨网段检测，必须指定下一跳。

毫秒级的检测可能会因网络传输延迟等原因出现不稳定性，因此建议将检测报文的发送间隔配置成秒级。

本端设备为热备冗余环境，对端设备开启 DLDP 主动检测功能时，建议对端设备配置的 DLDP“检测报文的发送间隔”与“检测报文的重传次数”的乘积值应该大于或者等于 4s，否则，当本端设备发生主从切换时，可能会导致对端设备 DLDP 检测出现异常。

在接口配置模式下执行 **no dldp** *ip-address* 命令，可以关闭与某对端设备的 DLDP 检测。

例：添加一个 DLDP 检测 IP

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# interface vlan 1
Ruijie(config-if)# ip-address 10.10.10.1 255.255.255.0
Ruijie(config-if)# dldp 10.10.10.2
```

```
Ruijie(config-if)# end
```

4.2.2 配置被动模式

缺省情况下，DLDP 为主动模式。

命令	作用
Ruijie(config)# **interface** *interface-name*	进入三层接口
Ruijie(config-if)# **dldp passive**	配置接口处于被动模式

要删除相关配置，可以在接口配置模式下执行 **no dldp passive** 命令来执行。

> 启动被动模式时，需要确保对端设备的时间参数配置与本设备完全一致，以便同步链路状态效果的检测。否则在被动模式中可能因对端发包的不同步而引起链路状态误判。

例：配置一个接口为 DLDP 被动模式

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# interface vlan 1
Ruijie(config-if)# ip-address 10.10.10.1 255.255.255.0
Ruijie(config-if)# dldp 10.10.10.2 interval 50 retry 10
Ruijie(config-if))# dldp passive
Ruijie(config-if))# end
```

4.3 监视与维护

4.3.1 查看DLDP信息

命令	作用
Ruijie# **show dldp** [**interface** *interface-name*] [**statistic**]	查看 DLDP 相关信息。 **statistic**：查看三层接口 down/up 的统计次数。

例：显示各个 DLDP 配置信息

```
Ruijie# show dldp
Interface  Type     Ip           Next-hop     Interval  Retry  Resume  State
---------  -------  -----------  -----------  --------  -----  ------  -----
V12        Passive  192.168.6.3  192.168.2.2  10        5      3       Up
V13        Passive  192.168.7.3               10        5      3       Up
V14        Passive  192.168.3.3  192.168.4.2  10        5      3       Up
```

例：显示各个 DLDP 的 down/up 统计信息

```
Ruijie# show dldp statistic
Interface  Type     Ip            record-time  Up-count  Down-count
```

```
---------  -------  -----------  ------------  --------  ----------
V12        Passive  192.168.6.3  2h34m5s       10        9
V13        Passive  192.168.7.3  30m34s        9         8
V14        Passive  192.168.3.3  1d2h3m52s     10        9
```

在 **show dldp statistic** 输出信息中包含 record-time 信息，该信息表示统计 up/down 次数的时间段长度。对应时间的显示格式为*y***d**h**m**s，这里的 y 表示年，d 表示天，h 表示小时，m 表示分钟，s 表示秒。结合后面的 Up-count 、Down-count 参数，即说明在这段时间内，up/down 了多少次。

4.3.2 清除DLDP统计信息

命令	作用
Ruijie# **clear dldp** [**interface** *interface-name* [*ip*]	清除指定监测点的 down/up 次数，并重新开始计数统计；用户也可以清除指定三层接口或所有三层接口上监测点的 down/up 次数。

5 VRRP

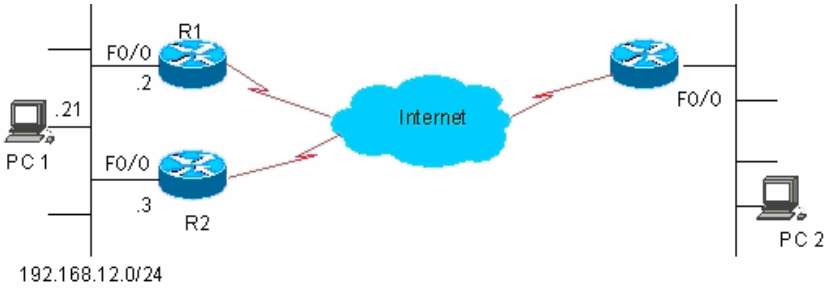
5.1 概述

VRRP (Virtual Router Redundancy Protocol，虚拟路由冗余协议)设计采用主备模式，以保证当主路由设备发生故障时，备份路由设备可以在不影响内外数据通信的前提下进行功能切换，且不需要再修改内部网络的参数。VRRP 组内多个路由设备都映射为一个虚拟的路由设备。VRRP 保证同时有且只有一个路由设备在代表虚拟路由设备进行包的发送，而主机则是把数据包发向该虚拟路由设备，这个转发数据包的路由设备被选择成为主路由设备。如果这个主路由设备在某个时候由于某种原因而无法工作的话，则处于备份状态的路由设备将被选择来代替原来的主路由设备。VRRP 使得局域网内的主机看上去只使用了一个路由设备，并且即使在它当前所使用的首跳路由设备失败的情况下仍能够保持路由的连通性。

RFC 2338、RFC3768、RFC5798 中定义了 VRRP 类型的 IP 报文格式及其运作机制，VRRP 报文是一类指定目的地址的组播报文，该报文由主路由设备定时发出来标志其运行正常同时该报文也用于选举主路由设备。VRRP 允许为 IP 局域网承担路由转发功能的路由设备失效后，局域网中另外一个路由设备将自动接管失效的路由设备，从而实现 IP 路由的热备份与容错，同时也保证了局域网内主机通讯的连续性和可靠性。一个 VRRP 应用组通过多台路由设备来实现冗余，但是任何时候只有一台路由设备作为主路由设备来承担路由转发功能，其他的为备份路由设备，VRRP 应用组中不同路由设备间的切换对局域网内的主机则是完全透明的。RFC 规定了路由设备的切换规则：

- VRRP 协议采用简单竞选的方法选择主路由设备。首先比较同一个 VRRP 组内的各台路由设备对应接口上设置的 VRRP 优先级的大小，优先级最大的为主路由设备，它的状态变为 Master。若路由设备的优先级相同，则比较对应网络接口的主 IP 地址大小，主 IP 地址大的就成为主路由设备，由它提供实际的路由转发服务。
- 主路由设备选出后，其它路由设备作为备份路由设备(状态变为 Backup)，并通过主路由设备定时发出的 VRRP 报文监测主路由设备的状态。当正常工作时，主路由设备会每隔一段时间发送一个 VRRP 组播报文，称为通告报文，以通知备份路由设备：主路由设备处于正常工作状态。如果组内的备份路由设备在设定的时间段没有接收到来自主路由设备的报文，则将自己状态转为 Master。当组内有多台状态为 Master 路由设备时，重复 1)的竞选过程。通过这样一个过程就会将优先级最大的路由设备选成新的主路由设备，从而实现 VRRP 的备份功能。

图 5-1 VRRP 工作原理



一旦在一个 VRRP 备份组选举出它的主路由设备，局域网内的主机将通过主路由设备进行路由转发。通讯过程可以由上图来说明。在图中，路由设备 R1 和 R2 均通过以太网口 Fa0/0 与局域网 192.168.12.0/24 连接，路由设备 R1 与 R2 的 Fa0/0 接口上设置了 VRRP，局域网内的主机都以该 VRRP 组的虚拟路由设备 IP 地址作为默认网关。对于局域网内的主机而言，它们只能感受到由 VRRP 组的虚拟路由设备，而实际承担路由转发功能的 VRRP 组的主路由设备对它们而言则是透明的。譬如，局域网内的主机 PC 1 如果要与其它网络内的主机 PC 2 通讯，PC 1 会以虚拟路由设备为默认网关来发送通向 PC 2 的网络数据包，VRRP 组中的主路由设备在接收到该数据包后会将该数据包转发给 PC 2。在这个通讯过程中，PC 1 只能感

受到虚拟路由设备而不知道扮演虚拟路由设备角色的主路由设备究竟是 R1 还是 R2，在这个 VRRP 组中的主路由设备是在 R1 与 R2 之间选举产生的，一旦主路由设备失效，那么另外一台将自动成为主路由设备。

RFC 5798 标准重新定义了 VRRP 报文的格式，RGOS 的 IPv6 VRRP 遵循该标准。在后面的描述中，我们把该标准简称为 VRRPv3 标准，而原来的 VRRP 实现简称为 VRRPv2 标准。IPv4VRRP 才有严格的 VRRPv2 标准和 VRRPv3 标准区分之说，这两个标准定义的 VRRP 协议报文的字段是不同的，为此 RGOS 的 IPv4 VRRP 会新增对 VRRPv3 标准的支持，并处理与 VRRPv2 标准的兼容问题。IPv6 则没有 VRRPv2 标准和 VRRPv3 标准区分之说，因为只有 VRRPv3 标准才定义了 IPv6 VRRP。

目前 VRRP 的协议规范主要包括如下三个：

- RFC 2338
- RFC 3768
- RFC 5798

RFC 3768 是 RFC2338 的更新，定义了 IPv4 VRRP 的协议机制等。而 RFC 5798

是 RFC3768 的改进和扩展，定义了 IPv4 VRRP 和 IPv6 VRRP 的协议机制。

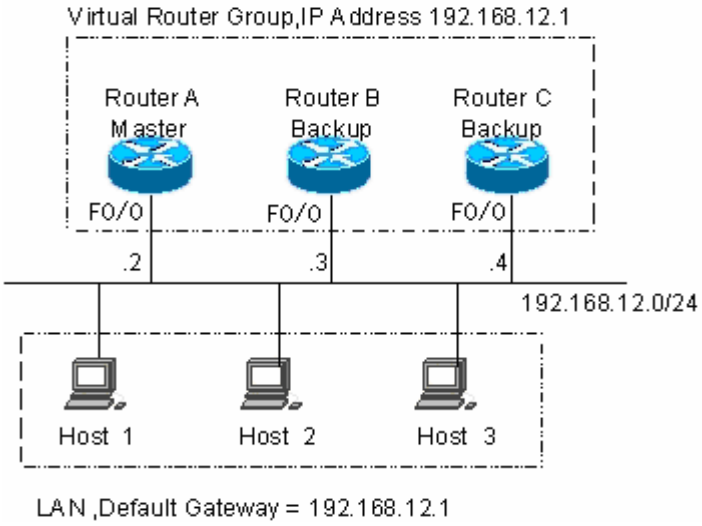
> 为了兼容当前广泛部署的其它不支持 VRRPv3 的设备，锐捷产品 IPv4 VRRP 会提供给用户来选择是使用 VRRPv2 标准，或者是使用 VRRPv3 标准。 IPv6 VRRP 则使用 VRRPv3 标准。

VRRP 有两种应用模式：基本应用与高级应用。其中基本应用是使用单备份组实现简单路由冗余，高级应用是使用多备份组同时实现路由冗余与负载均衡。

5.1.1 路由冗余

VRRP 的基本应用可以通过下图示例来说明。

图 5-2 VRRP 基本应用示意图



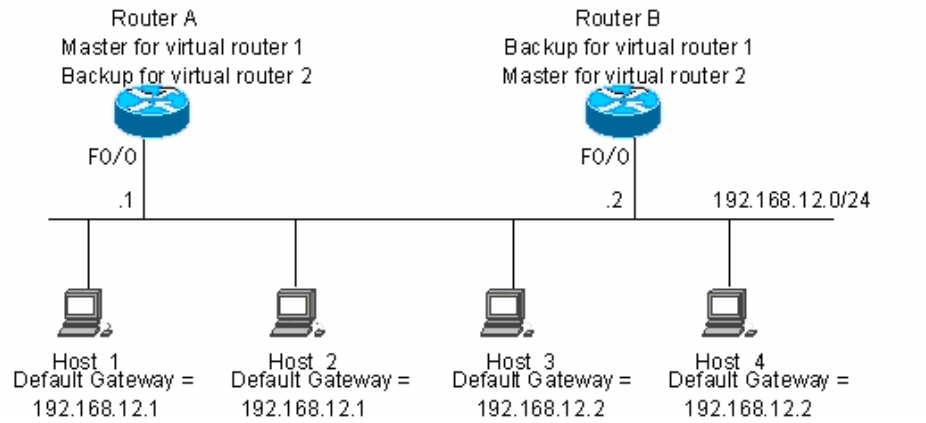
如图，路由设备 A、B 以及 C 均使用以太网口与局域网连接，并在其连接局域网的以太网接口上设置了 VRRP，它们处于同一个 VRRP 组并且该 VRRP 组的虚拟 IP 地址为 192.168.12.1，其中路由设备 A 经选举为 VRRP 的主路由设备，路由设备 B 与 C 作为备份路由设备。局域网内的主机 1、2 以及 3 以虚拟路由设备的 IP 地址 192.168.12.1 作为网关。局域网内主

机发往其它网络的数据包将由主路由设备(在图中是路由设备 A)进行路由转发。一旦路由设备 A 失效，将在路由设备 B 与 C 之间选举出主路由设备来承担虚拟路由设备的路由转发功能，由此实现了简单路由冗余。

5.1.2 负载均衡

VRRP 的高级应用可以通过下图示例来说明。

图 5-3 VRRP 高级应用示意图



如图，设置了两个虚拟路由设备。对于虚拟路由设备 1，路由设备 A 使用以太网口 Fa0/0 的 IP 地址 192.168.12.1 作为虚拟路由设备的 IP 地址，这样路由设备 A 就成为主路由设备，而路由设备 B 成为备份路由设备。对于虚拟路由设备 2，路由设备 B 使用以太网口 Fa0/0 的 IP 地址 192.168.12.2 作为虚拟路由设备的 IP 地址，这样路由设备 B 就成为主路由设备，而路由设备 A 成为备份路由设备。在局域网内，主机 1 和主机 2 使用虚拟路由设备 1 的 IP 地址 192.168.12.1 作为默认网关，主机 3 和主机 4 使用虚拟路由设备 2 的 IP 地址 192.168.12.2 作为默认网关。在 VRRP 这个应用中，路由设备 A 和路由设备 B 实现了路由冗余，并同时分担了来自局域网的流量即实现了负载平衡。

5.2 配置VRRP

VRRP 协议适用于多播或者广播的局域网如以太网等。VRRP 的配置集中在以太网接口上。其配置任务有：

- 启动 VRRP 备份功能(必须)
- 设置 VRRP 备份组的验证字符串(可选)
- 设置 VRRP 备份组的通告发送间隔(可选)
- 设置路由设备在 VRRP 备份组中的抢占模式(可选)
- 设置 IPv6 VRRP 虚拟路由器的 Accept_Mode 模式(可选)
- 设置路由设备在 VRRP 备份组中的优先级(可选)
- 设置 VRRP 备份组监视的接口(可选)
- 设置 VRRP 备份组监视的 IP/IPv6 地址(可选)
- 设置 VRRP 通告定时设备学习功能(可选)

- 设置路由设备在 VRRP 备份组的描述字符串(可选)
- 设置 VRRP 备份组延迟启动(可选)
- 设置 IPv4 VRRP 的 VRRP 报文发送标准（可选）

5.2.1 启动VRRP备份功能

通过设置备份组号和虚拟IP/IPv6地址，可以在指定的局域网段上添加一个备份组，从而启动对应的以太网接口的VRRP备份功能。

命令	作用
Ruijie(config-if)# **vrrp** *group* **ip** *ipaddress* [**secondary**]	启用 IPv4 VRRP
Ruijie(config-if)# **no vrrp** *group* **ip** *ipaddress* [**secondary**]	关闭 IPv4 VRRP
Or：	
Ruijie(config-if)# **vrrp** *group* **ipv6** *ipv6-address*	启用 IPv6 VRRP
Ruijie(config-if)# **no vrrp** *group* **ipv6** *ipv6-address*	关闭 IPv6 VRRP

备份组号 Group 取值范围为 1~255。如果不指定虚拟 IP 地址，路由设备就不会参与 VRRP 备份组。如果不使用 Secondary 参数，那么设置的 IP 地址将成为虚拟路由设备的主 IP 地址。对于 IPv6 地址，不区分是主地址还是从地址。但是 IPv6 VRRP 配置的第一个虚 IP 地址必须是链路本地地址。

如果 VRRP 组的虚拟 IP 地址(Primary 或者 Secondary)与所在以太网接口上的 IP 地址(Primary 或者 Secondary)一致，那么就认为该 VRRP 组占用(Own)了以太网接口实际 IP 地址，此时该 VRRP 组的优先级为 255，如果对应的以太网接口可用，那么该 VRRP 组将自动处于 Master 状态;

5.2.2 设置VRRP备份组的验证字符串

VRRP 支持明文密码验证模式以及无验证模式。设置 VRRP 备份组的验证字符串的同时也设定该 VRRP 组处于明文密码验证模式。VRRP 备份组成员必须处于相同的验证模式下才可能正常通讯。明文密码验证模式下，在同一个 VRRP 组中的路由设备必须设置相同的验证口令。明文验证口令不能保证安全性，它只是用来防止/提示错误的 VRRP 配置。

命令	作用
Ruijie(config-if)# **vrrp group authentication** *string*	设置 IPv4 VRRP 的验证字符串
Ruijie(config-if)# **no vrrp group authentication**	设置 IPv4 VRRP 处于无验证模式

缺省状态下，VRRP 处于无验证模式。在明文密码验证模式下，明文密码长度不能超过 8 个字节。

此验证模式在 RFC 5798 已经被丢弃，新的标准不再采纳验证模式，所以用户配置的验证模式只会适用于 VRRPv2 报文，而不会作用于 VRRPv3 报文。

5.2.3 设置VRRP备份组的通告发送间隔

命令	作用
Ruijie(config-if)# **vrrp group timers advertise** { *advertise-interval* | **csec** *centisecond-interval* }	设置 IPv4 主路由设备 VRRP 通告间隔

Ruijie(config-if)# **no vrrp group timers advertise**	恢复 IPv4 主路由设备 VRRP 通告间隔的默认值
or：	
Ruijie(config-if)# **vrrp ipv6 group timers advertise** { *advertise-interval* | **csec** *centisecond-interval* }	设置 IPv6 主路由设备 VRRP 通告间隔
Ruijie(config-if)# **no vrrp ipv6 group timers advertise**	恢复 Ipv6 主路由设备 VRRP 通告间隔的默认值

如果当前路由设备为 VRRP 组中的主路由设备，它将以设定的间隔发送 VRRP 通告来通告自己的 VRRP 状态、优先级以及其它信息。缺省状态下，系统默认主路由设备的 VRRP 通告发送间隔为 1 秒。RFC 2338、RFC3768、RFC5798 都定义了 VRRP 备份路由器切换为主路由器的时间，备份路由器切换为主路由器的时间为: 3 倍的报文发送间隔时间 + Skew_time；Skew_time = (((256 – VRRP 组的优先值) *VRRP 协议报文发送间隔时间) / 256)。

VRRPv3 支持配置主路由设备的 VRRP 通告发送间隔为厘秒级别，取值范围为 50~99，在不与 BFD 联动的情况下，能够加快 VRRP 收敛时间。如果网络流量过大，不建议配置为厘秒级别，因为网络流量过大可能会导致 Backup 路由器在指定时间内没有收到 Master 路由器的 VRRP 通告报文，从而发生状态转换。

> 在没有设置 VRRP 定时设备学习功能的时候，同一个 VRRP 备份组要设置相同的 VRRP 通告发送间隔，否则处于备份状态的路由设备将会丢弃接收到的 VRRP 通告。

5.2.4 设置路由设备在VRRP备份组中的抢占模式

如果 VRRP 组工作在抢占模式下，一旦它发现自己的优先级高于当前 Master 的优先级，它将抢占成为该 VRRP 组的主路由设备。如果 VRRP 组工作在非抢占模式下，即便它发现自己的优先级高于当前 Master 的优先级，它也不会抢占成为该 VRRP 组的主路由设备。VRRP 组使用以太网接口 IP 地址情况下，抢占模式是否设置意义不大，因为此时该 VRRP 组具有最大优先级，它自动成为该 VRRP 组中的主路由设备。

命令	作用
Ruijie(config-if)# **vrrp group preempt** [**delay** *seconds*]	设置 Ipv4 VRRP 备份组处于抢占模式
Ruijie(config-if)# **no vrrp group preempt** [**delay**]	设置 Ipv4 VRRP 备份组处于非抢占模式或恢复延迟时间默认值
or	
Ruijie(config-if)# **vrrp ipv6 group preempt** [**delay** *seconds*]	设置 IPv6 VRRP 备份组处于抢占模式
Ruijie(config-if)# **no vrrp ipv6 group preempt** [**delay**]	设置 IPv6 VRRP 备份组处于非抢占模式或恢复延迟时间默认值

可选参数 Delay Seconds 定义了处于备份状态的 VRRP 路由设备准备宣告自己拥有 Master 身份之前的延迟，缺省值为 0 秒。一旦启用 VRRP 功能，VRRP 组默认工作在抢占模式下。

5.2.5 设置IPv6 VRRP虚拟路由器的Accept_Mode模式

处于 Master 状态的 IPv6 VRRP 虚拟路由器可以通过 Accept_Mode 来控制是否接收处理目的 IP 地址为虚拟路由器的 IP 地址的报文。如果配置了 Accept_Mode 模式，则表示 Master 状态的 IPv6 VRRP 虚拟路由器需接收处理任何目的 IP 为虚拟路由器的 IP 地址的报文，如果未配置 Accept_Mode 模式，则表示 Master 状态的 IPv6 VRRP 虚拟路由器需丢弃处理任何目的 IP 为虚拟路由器的 IP 地址的报文，但不丢弃 NA 和 NS 报文。默认为未配置 Accept_Mode。另外，Owner 状态的 IPv6 VRRP Master 状态虚拟路由器，不管有没有配置 Accept_Mode 模式，都会接收处理任何目的 IP 为虚拟路由器的 IP 地址的报文。

命令	作用
Ruijie(config-if)# **vrrp ipv6** *group* **accept_mode**	设置 IPv6 VRRP 备份组的 Accept_Mode 模式
Ruijie(config-if)# **no vrrp ipv6** *group* **accept_mode**	取消 IPv6 VRRP 备份组的 Accept_Mode 模式

5.2.6 设置路由设备在VRRP备份组中的优先级

VRRP 协议规定根据路由设备的优先级参数来确定在备份组中每台路由设备的地位。工作在抢占模式下具有最高优先级并且已获得虚拟 IP 地址的路由设备将成为该备份组的活动的(或主)路由设备，同一个备份组中低于该路由设备优先级的其它路由设备将成为备份的(或监听的)路由设备。一旦启用 VRRP 功能，VRRP 组默认其优先级为 100。

命令	作用
Ruijie(config-if)# **vrrp** *group* **priority** *level*	设置 IPv4 VRRP 备份组的优先级
Ruijie(config-if)# **no vrrp** *group* **priority**	恢复 IPv4 VRRP 优先级的默认值
or：	
Ruijie(config-if)# **vrrp ipv6** *group* **priority** *level*	设置 IPv6 VRRP 备份组的优先级
Ruijie(config-if)# **no vrrp ipv6** *group* **priority**	恢复 IPv6 VRRP 优先级的默认值

优先级 Level 的取值范围为 1~254。如果 VRRP 虚拟 IP 地址与所在以太网接口上真实 IP 地址一致，对应的 VRRP 组的优先级就为 255，此时无论 VRRP 组是否处于抢占模式，对应的 VRRP 组都会自动处于 Master 状态(只要对应的以太网接口可用)。

5.2.7 设置VRRP备份组监视的接口

在配置了 VRRP 备份组监视的接口后，系统将根据所监视接口的状态动态地调整本路由设备的优先级。一旦所监视的接口状态变为不可用就按照设置的数值减少本路由设备在 VRRP 备份组中的优先级，而此时同一个备份组中接口状态更稳定并且优先级更高的其它路由设备就可以成为该 VRRP 备份组的活动的(或主)路由设备。

命令	作用
Ruijie(config-if)# **vrrp group track** *interface-type number* [*interface–priority*]	设置 IPv4 VRRP 备份组监视的接口
Ruijie(config-if)# **no vrrp** *group* **track** *interface-type number*	取消 IPv4 VRRP 备份组监视接口设置
Or：	
Ruijie(config-if)# **vrrp ipv6** *group* **track** *interface-type number* [*interface–priority*]	设置 IPv6 VRRP 备份组监视的接口
Ruijie(config-if)# **no vrrp ipv6** *group* **track** *interface-type number*	取消 IPv6 VRRP 备份组监视接口设置

缺省状态下，系统没有设置 VRRP 备份组监视的接口。参数 Interface -Priority 取值范围为 1~255。如果参数 Interface -Priority 缺省，系统会取默认值即 10。

被监视的接口只允许是三层可路由的逻辑接口(如 Routed Port ， SVI ， Loopback，Tunnel 等等)。

5.2.8 设置VRRP备份组监视的IP/IPv6 地址

在配置了 VRRP 备份组监视的 IP 地址后，系统将根据所监视的地址是否可达来动态地调整本设备的优先级。一旦所监视的 IP 地址变为不可达，即 ping 不通，就按照设置的数值减少本设备在 VRRP 备份组中的优先级，而此时同一个备份组中优先

级更高的其它路由设备就可以成为该 VRRP 备份组的活动的(或主)路由设备。该命令的可选参数 interval 是探测该目标地址是否可达的间隔时间，可选参数 timeout 是判定超时、即目标不可达的时间,可选参数 retry 是判定确认不可达的次数。

命令	作用
Ruijie(config-if)# **vrrp** *group* **track** *ip-address* [**interval** *interval-value*] [**timeout** *timeout-value*] [**retry** *retry-value*] [*priority*]	设置 IPv4 VRRP 备份组监视的 IP 地址
Ruijie(config-if)# **no vrrp** *group* **track** *ip-address*	取消 IPv4 VRRP 备份组监视地址设置
Or：	
Ruijie(config-if)# **vrrp ipv6** *group* **track** { *ipv6-global-address* | { *ipv6-linklocal-address interface-type number* } } [**interval** *interval-value*] [**timeout** *timeout-value*] [**retry** *retry-value*] [*priority*]	设置 IPv6 VRRP 备份组监视的 IP 地址,
Ruijie(config-if)# **no vrrp ipv6** *group* **track** { *ipv6-global-address* | { *ipv6-linklocal-address interface-type number* } }	取消 IPv6 VRRP 备份组监视地址设置

缺省状态下，系统没有设置 VRRP 备份组监视的地址。参数 interval-value 取值范围为 1~3600 秒，如果该参数缺省，系统会取其默认值即 3 秒。参数 timeoute-value 取值范围为 1~60 秒，如果该参数缺省，系统会取其默认值，即 1 秒，注意：该值必须小于或等于 interval-value。参数 retry-value 的取值范围是 1~60 次，如果该参数缺省，系统会取其默认值，即 3 次。参数 priority 取值范围为 1~255，如果该参数缺省，系统会取默认值即 10。对于配置 VRRP IPv6 地址必须先配置 VRRP IPv6 链路本地地址。如果配置监视指定的链路本地地址，则还必须配置指定的接口。

5.2.9 设置VRRP通告定时设备学习功能

一旦启用了定时设备学习功能，如果当前路由设备是 VRRP 备份路由设备，在设置了定时设备学习功能后，它会从主路由设备的 VRRP 通告中学习 VRRP 通告发送间隔，并由此来计算 Master 路由设备失效判断间隔，而不是使用自己本地设置的 VRRP 通告发送间隔来计算。本命令可以实现 Backup 路由设备与 Master 路由设备的 VRRP 通告发送定时设备同步。

命令	作用
Ruijie(config-if)# **vrrp** *group* **timers learn**	设置 IPv4 VRRP 定时设备学习功能
Ruijie(config-if)# **no vrrp** *group* **timers learn**	取消 IPv4 VRRP 定时设备学习功能
Or：	
Ruijie(config-if)# **vrrp ipv6** *group* **timers learn**	设置 IPv6 VRRP 定时设备学习功能
Ruijie(config-if)# **no vrrp ipv6** *group* **timers learn**	取消 IPv6 VRRP 定时设备学习功能

缺省状态下，系统没有为 VRRP 组设置定时设备学习功能。

在 VRRP 备份路由设备接收到的 VRRP 通告中的通告发送间隔与本地设置的通告发送间隔不一致的时候，如果 VRRP 备份路由设备上没有设置定时设备学习功能，VRRP 备份路由设备将会丢弃该 VRRP 通告否则 VRRP 备份路由设备会接收该 VRRP 通告并依据其中通告间隔来计算 VRRP 的 Master 路由设备失效判断间隔。

5.2.10 设置路由设备在VRRP备份组的描述字符串

本命令为 VRRP 组设置描述符，可以便于区分 VRRP 组。

命令	作用

Ruijie(config-if)# **vrrp** *group* **description** *text*	设置 IPv4 VRRP 组描述字符串
Ruijie(config-if)# **no vrrp** *group* **description**	取消 IPv4 VRRP 组描述字符串设置
Or：	
Ruijie(config-if)# **vrrp ipv6** *group* **description** *text*	设置 IPv6 VRRP 组描述字符串
Ruijie(config-if)# **no vrrp ipv6** *group* **description**	取消 IPv6 VRRP 组描述字符串设置

缺省状态下，VRRP 备份组没有设置任何描述字符串。VRRP 备份组描述字符串长度不超过 80。

如果 VRRP 备份组描述字符串中包含空格，就必须使用”“以及”“来标识描述字符串。

5.2.11 设置VRRP备份组延迟启动

本命令配置某个接口上 VRRP 备份组的延迟启动时间；延迟时间有两种：系统启动时的延迟时间，与接口状态变为活动时的延迟时间，可以分别配置，也可同时配置。

在非抢占模式下，优先级较高的 VRRP 备份组启动时，不会抢占同一备份组的主设备。但在某些情况下，即使配置了非抢占模式，刚启动的 VRRP 备份组也会抢占成为 VRRP 主设备。这是因为设备启动或者接口刚变为活动时，该接口上的 VRRP 备份组没有及时收到同一备份组的主设备发出的 VRRP 报文。

这时可以通过配置本命令，使 VRRP 备份组延迟启动。配置本命令后，当系统启动，或者接口状态变为活动时，该接口上的 VRRP 备份组不会立即启动；而是等待相应的延迟时间后再启动 VRRP 备份组，保证非抢占配置不会失效。

如果在延迟启动 VRRP 时该接口上接收到 VRRP 报文，则会取消延迟，立即启动 VRRP 协议。

命令	作用
Ruijie(config-if)# **vrrp delay** { **minimum** *min-seconds* | **reload** *reload-seconds* }	设置接口上 VRRP 备份组延迟启动时间
Ruijie(config-if)# **no vrrp delay**	取消接口上 VRRP 备份组延迟启动设置

缺省状态下，接口没有配置 VRRP 备份组延迟启动。两种 VRRP 备份组延迟启动时间的取值范围均为 0~60 秒。配置此命令将对接口的 IPv4 VRRP 和 IPv6 VRRP 备份组同时生效。

5.2.12 设置IPv4 VRRP的VRRP报文发送标准

本命令用于配置 IPv4 VRRP 的 VRRP 报文的发送标准，IPv4 VRRP 的 VRRP 报文的发送标准有两种：VRRPv2 和 VRRPv3。缺省使用 VRRPv2 标准。

命令	作用
Ruijie(config-if)# **vrrp** *group* **version** { **2 | 3** }	设置 IPv4 VRRP 的 VRRP 报文标准
Ruijie(config-if)# **no vrrp** *group* **version**	缺省使用 VRRPv2 标准

5.3 监视与维护

我司产品提供命令 show 命令与 debug 命令来监控与维护 VRRP。

Show

以下的 **show** 命令可以考察本地路由设备的 IPv4 VRRP 状态。

命令	作用
Ruijie# **show** [**ipv6**] **vrrp** [**brief** | *group*]	查看当前的 IPv4 VRRP 状态或者 IPv6 VRRP 状态
Ruijie# **show** [**ipv6**] **vrrp interface** *type number* [**brief**]	显示指定网络接口上 IPv4 VRRP 或者 IPv6 VRRP 状态

下面给出使用这些命令的示例：

- **show** [**ipv6**] **vrrp** 命令

```
Ruijie# show vrrp
FastEthernet 0/0 - Group 1
State is Backup
Virtual IP address is 192.168.201.1 configured
Virtual MAC address is 0000.5e00.0101
Advertisement interval is 3 sec
Preemption is enabled
min delay is 0 sec
Priority is 100
Master Router is 192.168.201.213 , priority is 120
Master Advertisement interval is 3 sec
Master Down interval is 10.82 sec
FastEthernet 0/0 - Group 2
State is Master
Virtual IP address is 192.168.201.2 configured
Virtual MAC address is 0000.5e00.0102
Advertisement interval is 3 sec
Preemption is enabled
min delay is 0 sec
Priority is 120
Master Router is 192.168.201.217 (local), priority is 120
Master Advertisement interval is 3 sec
Master Down interval is 10.59 sec
```

```
Ruijie#show ipv6 vrrp
GigabitEthernet 0/13 - Group 1
  State is Master
  Virtual IPv6 address is as follows:
    FE80::2
    1::2
  Virtual MAC address is 0000.5e00.0201
  Advertisement interval is 1 sec
  Preemption is enabled
    min delay is 0 sec
  Priority is 100
  Master Router is FE80::1 (local), priority is 100
```

```
  Master Advertisement interval is 1 sec
  Master Down interval is 3.60 sec
```

上面的显示信息包括 IPv4 VRRP 和 IPv6 VRRP 以太网口名称、接口上设置的 VRRP 备份组号、状态、优先级、抢占方式、VRRP 通告间隔、虚拟 IP 地址、虚拟 MAC 地址、Master 路由设备 IP 地址、Master 路由设备优先级、Master 路由设备通告间隔、Master 路由设备失效判断间隔、当前 VRRP 备份组监视的接口以及对应的优先级改变尺度。

- **show [ipv6] vrrp brief** 命令

```
Ruijie# show vrrp brief
Interface         Grp  Pri  Time  Own  Pre  State   Master addr      Group addr
FastEthernet 0/0  1    100  3.60  -    P    Backup  192.168.201.213  192.168.201.1
FastEthernet 0/0  2    120  3.53  -    P    Master  192.168.201.217  192.168.201.2
```

```
Ruijie#show ipv6 vrrp brief
Interface             Grp  Pri  timer  Own  Pre  State   Master addr   Group addr
GigabitEthernet 0/13  1    100  3.60   -    P    Master  FE80::1       FE80::2
```

上面的显示信息包括 IPv4 VRRP 和 IPv6 VRRP 以太网口名称、接口上设置的 VRRP 备份组号、状态、优先级、抢占方式、虚拟 IP 地址、Master 路由设备 IP 地址。

- **show [ipv6] vrrp interface** 命令

```
Ruijie# show vrrp interface FastEthernet 0/0
FastEthernet 0/0 - Group 1
State is Backup
Virtual IP address is 192.168.201.1 configured
Virtual MAC address is 0000.5e00.0101
Advertisement interval is 3 sec
Preemption is enabled
VRRP standard version is V3
min delay is 0 sec
Priority is 100
Master Router is 192.168.201.213 , priority is 120
Master Advertisement interval is 3 sec
Master Down interval is 10.82 sec
FastEthernet 0/0 - Group 2
State is Master
Virtual IP address is 192.168.201.2 configured
Virtual MAC address is 0000.5e00.0102
Advertisement interval is 3 sec
Preemption is enabled
min delay is 0 sec
Priority is 120
Master Router is 192.168.201.217 (local), priority is 120
Master Advertisement interval is 3 sec
Master Down interval is 10.59 sec
```

```
Ruijie#show ipv6 vrrp inter gig 0/13
GigabitEthernet 0/13 - Group 1
  State is Master
  Virtual IPv6 address is as follows:
    FE80::2
    1::2
  Virtual MAC address is 0000.5e00.0201
  Advertisement interval is 1 sec
  Preemption is enabled
    min delay is 0 sec
  Priority is 100
  Master Router is FE80::1 (local), priority is 100
  Master Advertisement interval is 1 sec
  Master Down interval is 3.60 sec
```

上面的显示信息包括 IPv4 VRRP 和 IPv6 VRRP 指定的以太网口名称、接口上设置的 VRRP 备份组号、状态、优先级、抢占方式、VRRP 通告间隔、虚拟 IP 地址、虚拟 MAC 地址、Master 路由设备 IP 地址、Master 路由设备优先级、Master 路由设备通告间隔、Master 路由设备失效判断间隔、当前 VRRP 备份组监视的接口以及对应的优先级改变尺度。

debug

以下的 **debug** 命令可以提供本地路由设备的 VRRP 状态调试信息，包括 VRRP 组的状态变化、VRRP 通告收发以及 VRRP 事件等信息。

命令	作用
Ruijie# **debug** [**ipv6**] **vrrp errors**	打开 VRRP 出错提示调试开关
Ruijie# **no debug** [**ipv6**] **vrrp errors**	关闭 VRRP 出错提示调试开关
Ruijie# **debug** [**ipv6**] **vrrp events**	打开 VRRP 事件调试开关
Ruijie# **no debug** [**ipv6**] **vrrp events**	关闭 VRRP 事件调试开关
Ruijie# **debug** [**ipv6**] **vrrp packets**	打开 VRRP 报文调试开关
Ruijie# **no debug** [**ipv6**] **vrrp packets**	关闭 VRRP 报文调试开关
Ruijie# **debug** [**ipv6**] **vrrp state**	打开 VRRP 状态调试开关
Ruijie# **no debug** [**ipv6**] **vrrp state**	关闭 VRRP 状态调试开关
Ruijie# **debug** [**ipv6**] **vrrp**	打开 VRRP 调试开关
Ruijie# **no debug** [**ipv6**] **vrrp**	关闭 VRRP 调试开关

下面给出使用这些命令的示例：

- **debug** [**ipv6**] **vrrp** 命令

```
Ruijie# debug vrrp
Ruijie#
%VRRP-6-STATECHANGE: FastEthernet 0/0 IPv4 VRRP Grp 1 state Master -> Backup
VRRP: IPv4 VRRP Grp 1 Advertisement from 192.168.201.213 has invalid virtual address 192.168.1.1
VRRP: IPv4 VRRP Grp 1 on interface Gi0/13 is sending IPv4 VRRP V2 advertisement checksum a352.
```

```
Ruijie# debug ipv6 vrrp
```

```
Ruijie#
VRRP: IPv6 VRRP Grp 1 Event - Advert higher or equal priority
%VRRP-6-STATECHANGE: FastEthernet 0/0 IPv6 VRRP  Grp 1 state Backup -> Master
Ruijie#
VRRP: IPv6 VRRP Grp 1 on interface Gi0/13 is sending IPv6 VRRP v3 advertisement checksum 6de3.
```

debug [**ipv6**] **vrrp** 命令相当于同时执行命令 **debug** [**ipv6**] **vrrp errors**、**debug** [**ipv6**] **vrrp events**、**debug** [**ipv6**] **vrrp packets** 以及 **debug** [**ipv6**] **vrrp state**。

- **debug** [**ipv6**] **vrrp errors** 命令

```
Ruijie# debug vrrp errors
Ruijie#
VRRP: IPv4 VRRP Grp 1 Advertisement from 192.168.1.1 has wrong checksum.
VRRP: IPv4 VRRP Grp 1 Advertisement from 192.168.1.1 has wrong checksum.
VRRP: IPv4 VRRP Grp 1 Advertisement from 192.168.1.1 has wrong checksum.
```

上面的显示信息表明接收到来自 192.168.1.1 针对 IPv4 VRRP 组 1 的 VRRP 通告校验和错误。

```
Ruijie# debug ipv6 vrrp errors
Ruijie#
VRRP: IPv6 VRRP Grp 1 Advertisement from FE80::2D0:F8FF:FE22:DE00 has different IP address.
VRRP: IPv6 VRRP Grp 1 Advertisement from FE80::2D0:F8FF:FE22:DE00 has different IP address.
VRRP: IPv6 VRRP Grp 1 Advertisement from FE80::2D0:F8FF:FE22:DE00 has different IP address.
```

上面的信息显示同一个 IPv6 VRRP 组，但是组 IPv6 地址不一样。

- **debug** [**ipv6**] **vrrp events** 命令

```
Ruijie# debug vrrp events
Ruijie#
VRRP: IPv4 VRRP Grp 1 Event - Advert higher or equal priority
VRRP: IPv4 VRRP Grp 1 Event - Advert higher or equal priority
```

```
Ruijie# debug ipv6 vrrp events
VRRP: IPv6 VRRP Grp 1 Event - Advert higher or equal priority
Ruijie#
```

上面的显示信息表明本地 IPv4 VRRP 组和 IPv6 VRRP 组接收到的 VRRP 通告(Advertisement)中的优先级不低于本地优先级。

- **debug** [**ipv6**] **vrrp packets** 命令

```
Ruijie# debug vrrp packets
Ruijie#
VRRP: IPv4 VRRP Grp 1 on interface Gi0/13 is sending IPv4 VRRP V2 advertisement checksum a352.
VRRP: IPv4 VRRP Grp 1 on interface Gi0/13 is sending IPv4 VRRP V2 advertisement checksum a352.
```

```
Ruijie# debug ipv6 vrrp packets
VRRP: IPv6 VRRP Grp 1 on interface Gi0/13 is sending IPv6 VRRP v3 advertisement checksum 6de3.
```

```
VRRP: IPv6 VRRP Grp 1 on interface Gi0/13 is sending IPv6 VRRP v3 advertisement checksum 6de3.
```

上面的显示信息表明本地 IPv4 VRRP 组 1 和 IPv6 VRRP 组 1 正在发送 VRRP 通告。

```
Ruijie# debug vrrp packets
Ruijie#
VRRP: IPv4 VRRP Grp 1 on interface Gi0/13 received ipv4 v2 advertisement priority 100, source 192.168.1.1.
Ruijie# debug ipv6 vrrp packets

VRRP: IPv6 VRRP Grp 1 on interface Gi0/13 received ipv6 v3 advertisement priority 100, source FE80::1.
```

上面的显示信息表明本地接收到来自 192.168.1.1 针对 IPv4 VRRP 组 1 的 VRRP 通告，其优先级为 100，同时接收到了来自 fe80：：1 针对 IPv6 VRRP 组 1 的 VRRP 通告。

- **debug** [**ipv6**] **vrrp state** 命令

```
Ruijie# debug vrrp state
Ruijie#
VRRP: IPv4 VRRP Grp 1 add primary virtual IP, startup
```

```
Ruijie# debug ipv6 vrrp state
VRRP: IPv6 VRRP Grp 1 add primary virtual IP, startup.
```

上面的显示信息表明 Fastethernet 0/0 上的 IPv4 VRRP 组和 IPv6 VRRP 组配置了主 IP 地址，启动 VRRP 备份组。

5.4 配置举例

5.4.1 配置IPv6 的VRRP单备份组

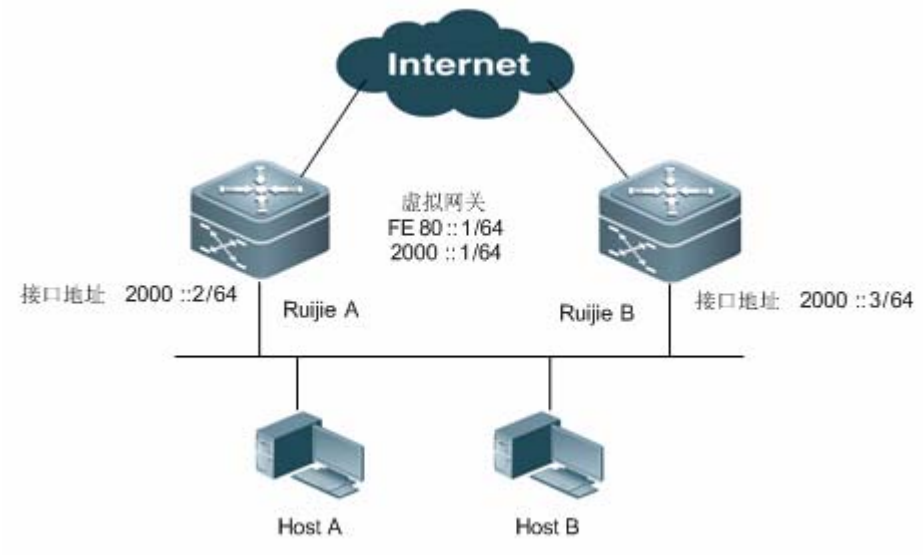
组网需求

本用例即适用于交换机设备，又适用于路由器设备。

- Host A Host B 需要通过网关访问 Internet 上的资源，它们的缺省网关为 2000::1/64；
- Ruijie A 和 Ruijie B 属于虚拟 IPv6 路由器的备份组 1，其虚拟地址为 2000::1/64 和 FE80::1；
- 当 Ruijie A 正常工作时，Host A 访问 Internet 的报文通过 Ruijie A 转发；当 Ruijie A 出现故障时，Host A 访问 Internet 的报文通过 Ruijie B 转发。

组网拓扑

图 5-4 基于 IPv6 的 VRRP 单组备份实例



配置步骤

1）Ruijie A 的配置：

#配置接口的 IPv6 地址以启用接口的 IPv6 服务

```
interface FastEthernet 0/1
```

/* “no switchport”命令只有在交换机上才需要 */

```
no switchport
ipv6 address 2000::2/64
!
```

#创建 VRRP 组 1 并配置虚拟 IPv6 地址 FE80::1 和 2000::1

```
interface FastEthernet 0/0
vrrp 1 ipv6 FE80::1
vrrp 1 ipv6 2000::1
```

#调整 VRRP 组的优先级为 120

```
vrrp ipv6 1 priority 120
```

#调整 VRRP 组的公告间隔为 3s

```
vrrp ipv6 1 timers advertise 3
```

#配置 IPv6 VRRP 的 Accept_mode 模式

```
vrrp ipv6 1 accept_mode
!
```

Ruijie B 的配置：

#创建 VRRP 组 1 并配置虚拟 IPv6 地址 FE80::1 和 2000::1

```
interface FastEthernet 0/1
```

/* “no switchport”命令只有在交换机上才需要 */

```
no switchport
ipv6 address 2000::3/64
!
```

#创建 VRRP 组 1 并配置虚拟 IPv6 地址 FE80::1 和 2000::1

```
interface FastEthernet 0/0
vrrp 1 ipv6 FE80::1
vrrp 1 ipv6 2000::1
```

#调整 VRRP 组的优先级为 120

```
vrrp ipv6 1 priority 100
```

#调整 VRRP 组的公告间隔为 3s

```
vrrp ipv6 1 timers advertise 3
```

#配置 IPv6 VRRP 的 Accept_mode 模式

```
vrrp ipv6 1 accept_mode
```

可见，Ruijie A 与 Ruijie B 同处于 IPv6 VRRP 备份组 1 中，指向相同的虚拟路由设备的 IPv6 地址(2000::1)并且均处于 VRRP 的抢占模式下。由于 Ruijie A 的 IPv6 VRRP 备份组优先级为 120，而 Ruijie B 的 VRRP 备份组优先级取默认值 100，所以 Ruijie A 在正常情况下充当 IPv6 VRRP 的 Master 路由设备。

显示验证

配置完成后，可以通过 show ipv6 vrrp 1 来查看 VRRP 的配置信息。

#显示 Ruijie A 的配置信息

```
Ruijie#show ipv6 vrrp 1
FastEthernet 0/1 - Group 1
  State is Master
  Virtual IPv6 address is as follows:
FE80::1
2000::1
  Virtual MAC address is 0000.5e00.0201
  Advertisement interval is 3 sec
  Accept_Mode is enabled
  Preemption is enabled
    min delay is 0 sec
  Priority is 120
  Master Router is FE80::1234 (local), priority is 120
  Master Advertisement interval is 3 sec
  Master Down interval is 10.59 sec
```

#显示 Ruijie B 的配置信息

```
Ruijie#show ipv6 vrrp 1
FastEthernet 0/1 - Group 1
  State is Backup
  Virtual IPv6 address is as follow:
FE80::1
2000::1
  Virtual MAC address is 0000.5e00.0201
  Advertisement interval is 3 sec
  Accept_Mode is enabled
  Preemption is enabled
    min delay is 0 sec
  Priority is 100
  Master Router is FE80::1234, priority is 120
  Master Advertisement interval is 3 sec
  Master Down interval is 10.82 sec
```

5.4.2 配置IPv6 的VRRP监视接口

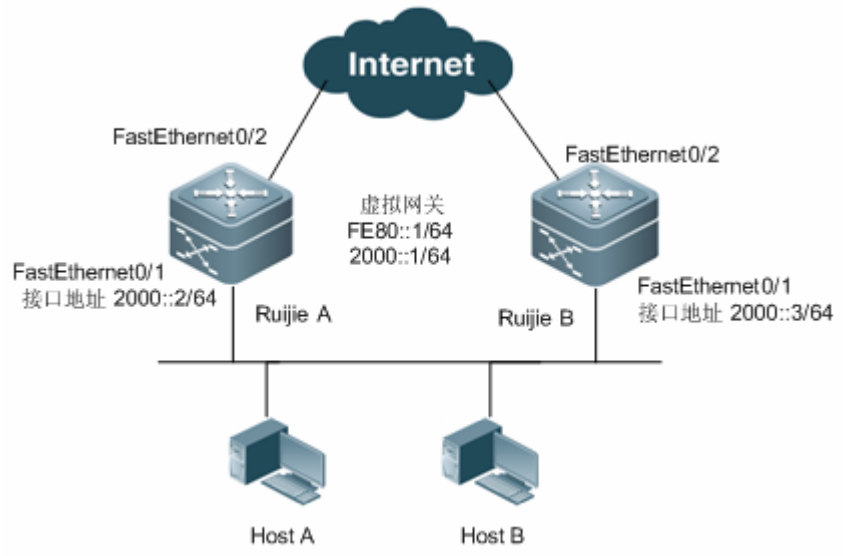
组网需求

本用例即适用于交换机设备，又适用于路由器设备。

- Host A Host B 需要通过网关访问 Internet 上的资源，它们的缺省网关为 2000::1/64；
- Ruijie A 和 Ruijie B 属于虚拟 IPv6 路由器的备份组 1，其虚拟地址为 2000::1/64 和 FE80::1；
- Ruijie A 监视与 Internet 链接的接口 Fastethernet 0/2，当 Fastethernet 0/2 不可用时，Ruijie A Ruijie 的 VRRP 1 降低自己的优先级，由 Ruijie B 执行网关功能。

组网拓扑

图 5-5 基于 IPv6 的 VRRP 监视接口应用实例



配置步骤

1）Ruijie A 的配置：

#配置接口的 IPv6 地址以启用接口的 IPv6 服务

```
interface FastEthernet 0/0
```

/* “no switchport”命令只有在交换机上才需要 */

```
no switchport
ipv6 address 2000::2/64
!
```

#创建 VRRP 组 1 并配置虚拟 IPv6 地址 FE80::1 和 2000::1

```
interface FastEthernet 0/0
vrrp 1 ipv6 FE80::1
vrrp 1 ipv6 2000::1
!
```

#调整 VRRP 组的优先级为 120

```
vrrp ipv6 1 priority 120
!
```

#调整 VRRP 组的公告间隔为 3s

```
vrrp ipv6 1 timers advertise 3
!
```

#配置 VRRP 1 监视接口 FastEthernet 0/2

```
vrrp ipv6 1 track FastEthernet 0/2 50
```

#配置 IPv6 VRRP 的 Accept_mode 模式

```
vrrp ipv6 1 accept_mode
```

Ruijie B 的配置：

#创建 VRRP 组 1 并配置虚拟 IPv6 地址 FE80::1 和 2000::1

```
interface FastEthernet 0/0
```

/* “no switchport”命令只有在交换机上才需要 */

```
no switchport
ipv6 address 2000::3/64
!
```

#创建 VRRP 组 1 并配置虚拟 IPv6 地址 FE80::1 和 2000::1

```
interface FastEthernet 0/0
vrrp 1 ipv6 FE80::1
vrrp 1 ipv6 2000::1
```

#调整 VRRP 组的优先级为 100

```
vrrp ipv6 1 priority 100
!
```

#调整 VRRP 组的公告间隔为 3s

```
vrrp ipv6 1 timers advertise 3
```

#配置 IPv6 VRRP 的 Accept_mode 模式

```
vrrp ipv6 1 accept_mode
```

可见，Ruijie A 与 Ruijie B 同处于 IPv6 VRRP 备份组 1 中，指向相同的虚拟路由设备的 IPv6 地址(2000::1)并且均处于 IPv6 VRRP 的抢占模式下。由于 Ruijie A 的 IPv6 VRRP 备份组优先级为 120，而 Ruijie B 的 IPv6 VRRP 备份组优先级取默认值 100，所以 Ruijie A 在正常情况下充当 IPv6 VRRP 的 Master 路由设备。如果 Ruijie A 在作为 Master 设备状态下发现接口 FastEthernet 0/2 不可用，Ruijie A 将降低自己的 VRRP 备份组优先级 50 成为 70，这样 Ruijie B 就会成为 Master 设备。如果在此后，Ruijie A 发现自己接口 FastEthernet 0/2 恢复可用，就增加自己的 VRRP 备份组优先级 50 而恢复到 120，这样 Ruijie A 将再次成为主路由设备。

显示验证

配置完成后，可以通过 show ipv6 vrrp 1 来查看 VRRP 的配置信息。

#显示 Ruijie A 的配置信息

```
Ruijie#show ipv6 vrrp 1
FastEthernet 0/1 - Group 1
  State is Master
  Virtual IPv6 address is as follows:
FE80::1
2000::1
  Virtual MAC address is 0000.5e00.0201
```

```
  Advertisement interval is 3 sec
  Accept_Mode is enabled
  Preemption is enabled
    min delay is 0 sec
  Priority is 120
  Master Router is FE80::1234 (local), priority is 120
  Master Advertisement interval is 3 sec
  Master Down interval is 10.59 sec
Tracking state of 1 interface, 1 up:
    up FastEthernet 0/2 priority decrement=50
```

#显示 Ruijie B 的配置信息

```
Ruijie#show ipv6 vrrp 1
FastEthernet 0/1 - Group 1
  State is Backup
  Virtual IPv6 address is as follow:
FE80::1
2000::1
  Virtual MAC address is 0000.5e00.0201
  Advertisement interval is 3 sec
  Accept_Mode is enabled
  Preemption is enabled
    min delay is 0 sec
  Priority is 100
  Master Router is FE80::1234, priority is 120
  Master Advertisement interval is 3 sec
  Master Down interval is 10.82 sec
```

5.4.3 配置IPv6 的VRRP多备份组

除了单备份组，我司产品还允许在同一个以太网接口上配置多个 VRRP 备份组。使用多备份组，有着显而易见的好处：可以实现负载均衡同时通过互相备份来提供更稳定可靠的网络服务。

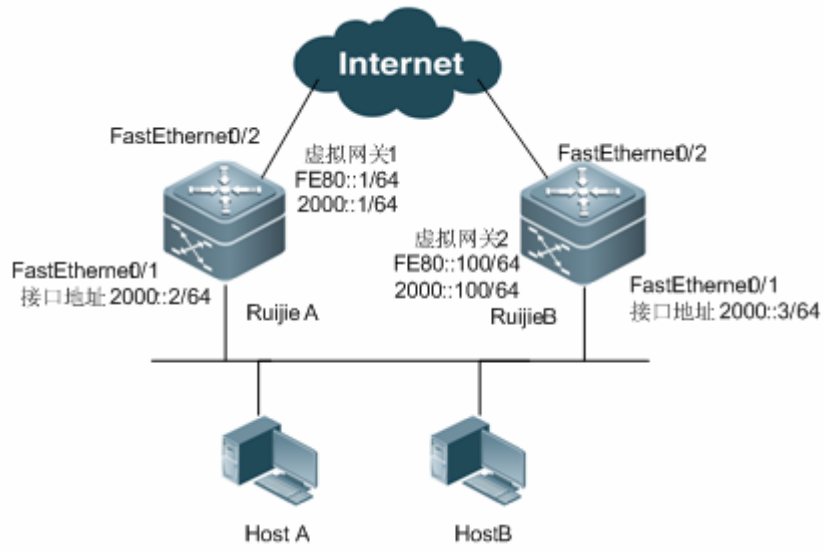
组网需求

本用例即适用于交换机设备，又适用于路由器设备。

- Host A Host B 需要通过网关访问 Internet 上的资源，它们的缺省网关分别为 2000::1/64 和 2000::100/64；
- Ruijie A 和 Ruijie B 属于虚拟 IPv6 路由器的备份组 1，其虚拟地址为 2000::1/64 和 FE80::1；
- 同时，Ruijie A 和 Ruijie B 也属于虚拟 IPv6 路由器的备份组 2，其虚拟地址为 2000::100/64 和 FE80::100；
- Ruijie A 和 Ruijie B 同时作为网关转发流量，同时作为另外一台设备的备份。

组网拓扑

图 5-6 基于 IPv6 的 VRRP 多备份组应用实例



配置步骤

1）Ruijie A 的配置：

#配置接口的 IPv6 地址以启用接口的 IPv6 服务

```
interface FastEthernet 0/0
```

/* “no switchport”命令只有在交换机上才需要 */

```
no switchport
ipv6 address 2000::2/64
!
```

#创建 VRRP 组 1 并配置虚拟 IPv6 地址 FE80::1 和 2000::1

```
interface FastEthernet 0/0
vrrp 1 ipv6 FE80::1
vrrp 1 ipv6 2000::1
!
```

#调整 VRRP 组的优先级为 120

```
vrrp ipv6 1 priority 120
!
```

#调整 VRRP 组的公告间隔为 3s

```
vrrp ipv6 1 timers advertise 3
```

#配置 IPv6 VRRP 的 Accept_mode 模式

```
vrrp ipv6 1 accept_mode
!
```

#创建 VRRP 组 2 并配置虚拟 IPv6 地址 FE80::100 和 2000::100

```
vrrp 2 ipv6 FE80::100
vrrp 2 ipv6 2000::100
!
```

#调整 VRRP 组的优先级为 100

```
vrrp ipv6 2 priority 100
```

#调整 VRRP 组的公告间隔为 3s

```
vrrp ipv6 2 timers advertise 3
```

#配置 IPv6 VRRP 的 Accept_mode 模式

```
vrrp ipv6 2 accept_mode
```

Ruijie B 的配置：

```
interface FastEthernet 0/0
```

/* “no switchport”命令只有在交换机上才需要 */

```
no switchport
ipv6 address 2000::3/64
!
```

#创建 VRRP 组 1 并配置虚拟 IPv6 地址 FE80::1 和 2000::1

```
interface FastEthernet 0/0
vrrp 1 ipv6 FE80::1
vrrp 1 ipv6 2000::1
```

#调整 VRRP 组的优先级为 100

```
vrrp ipv6 1 priority 100
!
```

#调整 VRRP 组的公告间隔为 3s

```
vrrp ipv6 1 timers advertise 3
```

#配置 IPv6 VRRP 的 Accept_mode 模式

```
vrrp ipv6 1 accept_mode
!
!
```

#创建 VRRP 组 2 并配置虚拟 IPv6 地址 FE80::100 和 2000::100

```
vrrp 2 ipv6 FE80::100
vrrp 2 ipv6 2000::100
!
```

#调整 VRRP 组的优先级为 120

```
vrrp ipv6 2 priority 120
```

#调整 VRRP 组的公告间隔为 3s

```
vrrp ipv6 2 timers advertise 3
!
```

#配置 IPv6 VRRP 的 Accept_mode 模式

```
vrrp ipv6 2 accept_mode
!
```

可见，Ruijie A 与 Ruijie B 同处于 IPv6 VRRP 备份组 1 中，指向相同的虚拟路由设备的 IPv6 地址(2000::1)并且均处于 IPv6 VRRP 的抢占模式下。对于备份组 21，由于 Ruijie A 的 VRRP 备份组优先级为 120，而 Ruijie B 的 IPv6 VRRP 备份组优先级取默认值 100，所以 Ruijie A 在正常情况下充当 IPv6 VRRP 备份组 1 的 Master 路由设备。而对于备份组 2, Ruijie A 的 IPv6 VRRP 备份组优先级为 100, Ruijie B 的 IPv6 VRRP 备份组优先级为 120，且备份组 2 处于抢占模式下，所以正常情况下，Ruijie B 充当 IPv6 VRRP 备份组 2 的 Master 路由设备。同一局域网中的主机，Host A 以备份组 1 为默认网关，HostB 以备份组 2 为默认网关，Ruijie A 和 Ruijie B 实现了路由冗余，并同时分担了来自局域网的流量即实现了负载平衡。对于该用例，IPv6 主机需要手动配置默认网关才能实现 IPv6 VRRP 备份组负载分担的功能。

显示验证

配置完成后，可以通过 show ipv6 vrrp 来查看 VRRP 的配置信息。

#显示 Ruijie A 的配置信息

```
Ruijie#show ipv6 vrrp
FastEthernet 0/1 - Group 1
  State is Master
  Virtual IPv6 address is as follows:
FE80::1
2000::1
  Virtual MAC address is 0000.5e00.0201
  Advertisement interval is 3 sec
  Accept_Mode is enabled
  Preemption is enabled
    min delay is 0 sec
  Priority is 120
  Master Router is FE80::1234 (local), priority is 120
  Master Advertisement interval is 3 sec
  Master Down interval is 10.59 sec
FastEthernet 0/1 - Group 2
  State is Backup
  Virtual IPv6 address is as follows:
FE80::100
2000::100
  Virtual MAC address is 0000.5e00.0202
  Advertisement interval is 3 sec
```

```
  Accept_Mode is enabled
  Preemption is enabled
    min delay is 0 sec
  Priority is 100
  Master Router is FE80::5678, priority is 120
  Master Advertisement interval is 3 sec
  Master Down interval is 10.82 sec
```

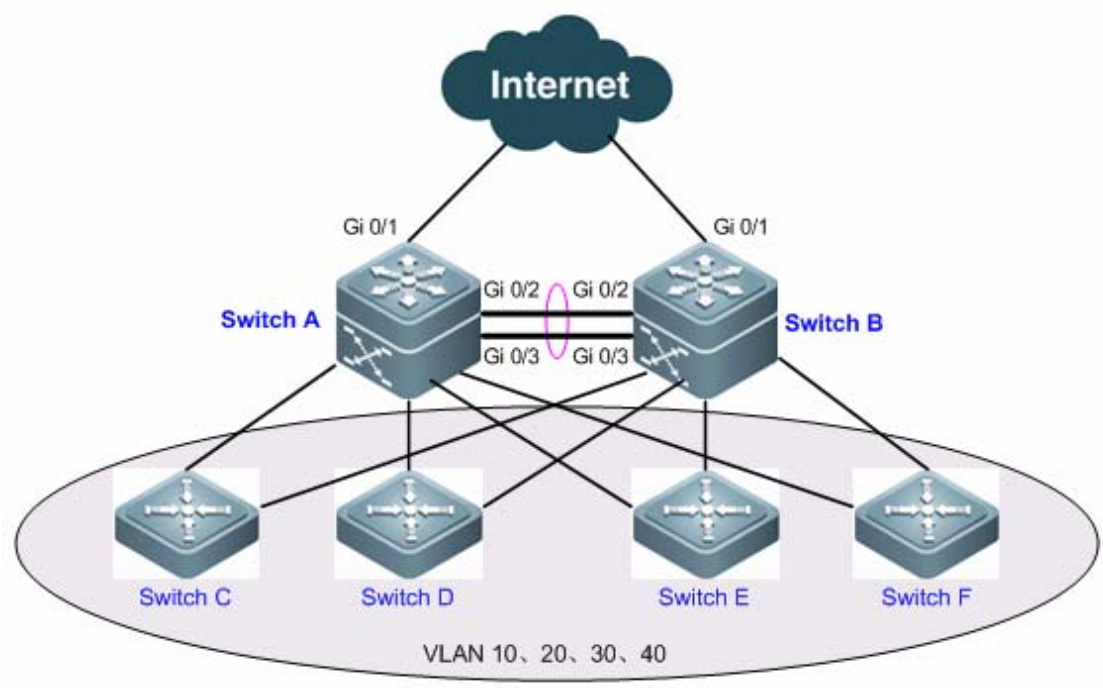
#显示 Ruijie B 的配置信息

```
Ruijie#show ipv6 vrrp 1
FastEthernet 0/1 - Group 1
  State is Backup
  Virtual IPv6 address is as follow:
FE80::1
2000::1
  Virtual MAC address is 0000.5e00.0201
  Advertisement interval is 3 sec
  Accept_Mode is enabled
  Preemption is enabled
    min delay is 0 sec
  Priority is 100
  Master Router is FE80::1234, priority is 120
  Master Advertisement interval is 3 sec
  Master Down interval is 10.82 sec

FastEthernet 0/1 - Group 2
  State is Master
  Virtual IPv6 address is as follows:
FE80::100
2000::100
  Virtual MAC address is 0000.5e00.0202
  Advertisement interval is 3 sec
  Accept_Mode is enabled
  Preemption is enabled
    min delay is 0 sec
  Priority is 120
  Master Router is FE80::5678(local), priority is 120
  Master Advertisement interval is 3 sec
  Master Down interval is 10.59 sec
```

5.4.4 配置VRRP+MSTP

拓扑图

图 5-7 VRRP 双核心应用拓扑



应用需求

上图为典型的双核心拓扑结构，本用例只适用于交换机或路由器交换卡。用户通过接入设备 Switch C、D、E、F 划分属于 VLAN 10、20、30、40；Switch A 和 Switch B 作为网关设备实现用户与外网通讯。具体应用需求如下：

- 通过运行 MSTP，实现物理链路备份，避免环路产生；不同的 VLAN 沿着各自的实例进行数据转发，实现二层流量负载均衡。
- 通过运行 VRRP，实现网关设备的路由备份，同时分担来自局域网的流量。
- 能够监控 Master 路由设备的上行链路，当出现链路故障，Backup 路由设备能够及时切换为 Master 路由设备进行数据转发。

配置要点

- 在设备上(本例为 Switch A、B、C、D、E、F)使能 MSTP 功能，配置 VLAN-Instance 之间的实例映射(本例将 VLAN 10、20 对应 Instance 1，VLAN 30、40 对应 Instance 2，其余 VLAN 对应 Instance 0），并设置网关设备（本例为 Switch A 和 Switch B）为对应实例的根桥。
- 将各 VLAN 的 SVI 加入相应的 VRRP 备份组，并设置网关设备为对应备份组的 Master 路由设备和 Backup 路由设备。本例具体配置如下表所示：

网关设备	VLAN ID	SVI	备份组	虚拟 IP 地址	状态
Switch A	10	192.168.10.2	VRRP 10	192.168.10.1	Master
Switch B		192.168.10.3			Backup
Switch A	20	192.168.20.2	VRRP 20	192.168.20.1	Master

Switch B		192.168.20.3			Backup
Switch A	30	192.168.30.2	VRRP 30	192.168.30.1	Backup
Switch B		192.168.30.3			Master
Switch A	40	192.168.40.2	VRRP 40	192.168.40.1	Backup
Switch B		192.168.40.3			Master

- 将对应备份组的 Master 路由设备的上链口（本例为 Switch A 和 Switch B 的端口 Gi 0/1）设置为 Master 路由设备的监视接口。

在配置 VRRP 备份组的监视接口时，参数 *Priority decrement*（系统根据监视口状态自动降低或增加优先级的值）必须大于 Master 路由设备和 Backup 路由设备的优先级差值。

配置步骤

以下仅列举在 Switch A 和 Switch B 上配置 VRRP+MSTP，对于 Switch C、D、E、F 上的 VLAN 划分以及 MSTP 配置此处不再列举。另外，对于 MSTP 的相关配置说明可参见《MSTP 配置》。

第一步，在设备上创建 VLAN

！在 Switch A 上创建 VLAN 10、20、30、40

```
SwitchA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)#vlan range 10,20,30,40
SwitchA(config-vlan-range)#exit
```

！Switch B 的配置同上

第二步，配置 MST 域

！在 Switch A 上配置 VLAN 10、20 对应 Instance 1，VLAN 20、30 对应 Instance 2，其余 VLAN 对应 Instance 0。

```
SwitchA(config)#spanning-tree mst configuration
SwitchA(config-mst)#instance 1 vlan 10,20
%Warning:you must create vlans before configuring instance-vlan relationship
SwitchA(config-mst)#instance 2 vlan 30,40
%Warning:you must create vlans before configuring instance-vlan relationship
SwitchA(config-mst)#exit
```

！Switch B 的配置同上

第三步，配置 Switch A 为 MST 0 和 MST 1 的根桥，Switch B 为 MST 2 的根桥。

！在 Switch A 上设置 MST 0 和 MST 1 的优先级为 4096，MST 2 的优先级为 8192。

```
SwitchA(config)#spanning-tree mst 0 priority 4096
SwitchA(config)#spanning-tree mst 1 priority 4096
SwitchA(config)#spanning-tree mst 2 priority 8192
```

！在 Switch B 上设置 MST 2 的优先级为 4096，MST 0 和 MST 1 的优先级为 8192

```
SwitchB(config)#spanning-tree mst 2 priority 4096
SwitchB(config)#spanning-tree mst 0 priority 8192
SwitchB(config)#spanning-tree mst 1 priority 8192
```

第四步，使能 MSTP

！在 Switch A 上开启 MSTP

```
SwitchA(config)#spanning-tree
Enable spanning-tree.
```

！Switch B 的配置同上

第五步，配置各 VLAN 的 SVI，并加入对应的备份组，同时设置备份组的虚拟 IP 地址。对应配置参见上表。

！在 Switch A 上配置如下：

```
SwitchA(config)#interface vlan 10
SwitchA(config-if-VLAN 10)#ip address 192.168.10.2 255.255.255.0
SwitchA(config-if-VLAN 10)#vrrp 10 ip 192.168.10.1
SwitchA(config-if-VLAN 10)#exit
SwitchA(config)#interface vlan 20
SwitchA(config-if-VLAN 20)#ip address 192.168.20.2 255.255.255.0
SwitchA(config-if-VLAN 20)#vrrp 20 ip 192.168.20.1
SwitchA(config-if-VLAN 20)#exit
SwitchA(config)#interface vlan 30
SwitchA(config-if-VLAN 30)#ip address 192.168.30.2 255.255.255.0
SwitchA(config-if-VLAN 30)#vrrp 30 ip 192.168.30.1
SwitchA(config-if-VLAN 30)#exit
SwitchA(config)#interface vlan 40
SwitchA(config-if-VLAN 40)#ip address 192.168.40.2 255.255.255.0
SwitchA(config-if-VLAN 40)#vrrp 40 ip 192.168.40.1
SwitchA(config-if-VLAN 40)#exit
```

！在 Switch B 上配置如下：

```
SwitchB(config)#interface vlan 10
SwitchB(config-if-VLAN 10)#ip address 192.168.10.3 255.255.255.0
SwitchB(config-if-VLAN 10)#vrrp 10 ip 192.168.10.1
SwitchB(config-if-VLAN 10)#exit
SwitchB(config)#interface vlan 20
SwitchB(config-if-VLAN 20)#ip address 192.168.20.3 255.255.255.0
SwitchB(config-if-VLAN 20)#vrrp 20 ip 192.168.20.1
SwitchB(config-if-VLAN 20)#exit
SwitchB(config)#interface vlan 30
SwitchB(config-if-VLAN 30)#ip address 192.168.30.3 255.255.255.0
SwitchB(config-if-VLAN 30)#vrrp 30 ip 192.168.30.1
SwitchB(config-if-VLAN 30)#exit
SwitchB(config)#interface vlan 40
```

```
SwitchB(config-if-VLAN 40)#ip address 192.168.40.3 255.255.255.0
SwitchB(config-if-VLAN 40)#vrrp 40 ip 192.168.40.1
SwitchB(config-if-VLAN 40)#exit
```

第六步，配置各备份组对应的 Master 路由设备和 Backup 路由设备。

！将 Switch A 的备份组 10、20 的优先级调高为 120，即设置 Switch A 作为备份组 10、20 的 Master 路由设备。

```
SwitchA(config)#interface vlan 10
SwitchA(config-if-VLAN 10)#vrrp 10 priority 120
SwitchA(config-if-VLAN 10)#exit
SwitchA(config)#interface vlan 20
SwitchA(config-if-VLAN 20)#vrrp 20 priority 120
SwitchA(config-if-VLAN 20)#exit
```

！ 同理，将 Switch B 的 VRRP 30、40 的优先级调高为 120。

```
SwitchB(config)#interface vlan 30
SwitchB(config-if-VLAN 30)#vrrp 30 priority 120
SwitchB(config-if-VLAN 30)#exit
SwitchB(config)#interface vlan 40
SwitchB(config-if-VLAN 40)#vrrp 40 priority 120
SwitchB(config-if-VLAN 40)#exit
```

第七步，将备份组的 Master 路由设备的上链口配置为 VRRP 组的监视接口。注意：监视接口必须为三层接口。

！配置 Switch A 的端口 Gi 0/1 为 Route Port，并设置 IP 地址为 10.10.1.1/24

```
SwitchA(config)#interface gigabitEthernet 0/1
SwitchA(config-if-GigabitEthernet 0/1)#no switchport
SwitchA(config-if-GigabitEthernet 0/1)#ip address 10.10.1.1 255.255.255.0
SwitchA(config-if-GigabitEthernet 0/1)#exit
```

！将 Switch A 的端口 Gi 0/1 配置为备份组 10、20 的监视接口，并设置 *Priority decrement* 为 30。

```
SwitchA(config)#interface vlan 10
SwitchA(config-if-VLAN 10)#vrrp 10 track gigabitEthernet 0/1 30
SwitchA(config-if-VLAN 10)#exit
SwitchA(config)#interface vlan 20
SwitchA(config-if-VLAN 20)#vrrp 20 track gigabitEthernet 0/1 30
SwitchA(config-if-VLAN 20)#exit
```

！配置 Switch B 的端口 Gi 0/1 为 Route Port，并设置 IP 地址为 10.10.2.1/24

```
SwitchB(config)#interface gigabitEthernet 0/1
SwitchB(config-if-GigabitEthernet 0/1)#no switchport
SwitchB(config-if-GigabitEthernet 0/1)#ip address 10.10.2.1 255.255.255.0
SwitchB(config-if-GigabitEthernet 0/1)#exit
```

！将 Switch B 的端口 Gi 0/1 配置为备份组 30、40 的监视接口，并设置 Interface -Priority 为 30。

```
SwitchB(config)#interface vlan 30
```

```
SwitchB(config-if-VLAN 30)#vrrp 30 track gigabitEthernet 0/1 30
SwitchB(config-if-VLAN 30)#exit
SwitchB(config)#interface vlan 40
SwitchB(config-if-VLAN 40)#vrrp 40 track gigabitEthernet 0/1 30
SwitchB(config-if-VLAN 40)#exit
```

第八步，配置双核心设备的互联端口为 AP 口。

！配置 Switch A

配置端口 Gi 0/2 和 Gi 0/3 属于 AP 口，并设置 AP 口为 trunk 口。

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#interface range gigabitEthernet 0/2-3
Ruijie(config-if-range)#port-group 1
Ruijie(config)#interface aggregateport 1
Ruijie(config-if-AggregatePort 1)#switchport mode trunk
```

！Switch B 的配置同上

验证结果

第一步，查看设备的配置信息。

！查看 Switch A

```
SwitchA#show running-config
!
vlan 10
!
vlan 20
!
vlan 30
!
vlan 40
!
spanning-tree
spanning-tree mst configuration
 instance 0 vlan 1-9, 11-19, 21-29, 31-39, 41-4094
 instance 1 vlan 10, 20
 instance 2 vlan 30, 40
spanning-tree mst 0 priority 4096
spanning-tree mst 1 priority 4096
spanning-tree mst 2 priority 8192
interface GigabitEthernet 0/1
 no switchport
 no ip proxy-arp
```

```
 ip address 10.10.1.1 255.255.255.0
!
interface GigabitEthernet 0/2
 port-group 1
!
interface GigabitEthernet 0/3
 port-group 1
!
interface AggregatePort 1
 switchport mode trunk
!
interface VLAN 10
 no ip proxy-arp
 ip address 192.168.10.2 255.255.255.0
 vrrp 10 priority 120
 vrrp 10 ip 192.168.10.1
 vrrp 10 track GigabitEthernet 0/1 30
!
interface VLAN 20
 no ip proxy-arp
 ip address 192.168.20.2 255.255.255.0
 vrrp 20 priority 120
 vrrp 20 ip 192.168.20.1
 vrrp 20 track GigabitEthernet 0/1 30
!
interface VLAN 30
 no ip proxy-arp
 ip address 192.168.30.2 255.255.255.0
 vrrp 30 ip 192.168.30.1
!
interface VLAN 40
 no ip proxy-arp
 ip address 192.168.40.2 255.255.255.0
 vrrp 40 ip 192.168.40.1
```

！查看 Switch B

```
SwitchB#show running-config
!
vlan 10
!
vlan 20
!
vlan 30
!
vlan 40
```

```
!
spanning-tree
spanning-tree mst configuration
 instance 0 vlan 1-9, 11-19, 21-29, 31-39, 41-4094
 instance 1 vlan 10, 20
 instance 2 vlan 30, 40
spanning-tree mst 0 priority 8192
spanning-tree mst 1 priority 8192
spanning-tree mst 2 priority 4096
interface GigabitEthernet 0/1
 no switchport
 no ip proxy-arp
 ip address 10.10.2.1 255.255.255.0
!
interface GigabitEthernet 0/2
 port-group 1!
interface GigabitEthernet 0/3
 port-group 1
!
interface AggregatePort 1
 switchport mode trunk
!
interface VLAN 10
 no ip proxy-arp
 ip address 192.168.10.3 255.255.255.0
 vrrp 10 ip 192.168.10.1
!
interface VLAN 20
 no ip proxy-arp
 ip address 192.168.20.3 255.255.255.0
 vrrp 20 ip 192.168.20.1
!
interface VLAN 30
 no ip proxy-arp
 ip address 192.168.30.3 255.255.255.0
 vrrp 30 priority 120
 vrrp 30 ip 192.168.30.1
 vrrp 30 track GigabitEthernet 0/1 30
!
interface VLAN 40
 no ip proxy-arp
 ip address 192.168.40.3 255.255.255.0
 vrrp 40 priority 120
 vrrp 40 ip 192.168.40.1
 vrrp 40 track GigabitEthernet 0/1 30
```

第二步，查看设备的 VRRP 状态

！查看 Switch A

```
SwitchA#show vrrp brief
Interface  Grp  Pri  timer  Own  Pre  State   Master addr   Group addr
VLAN 10    10   120  3      -    P    Master  192.168.10.2  192.168.10.1
VLAN 20    20   120  3      -    P    Master  192.168.20.2  192.168.20.1
VLAN 30    30   100  3      -    P    Backup  192.168.30.3  192.168.30.1
VLAN 40    40   100  3      -    P    Backup  192.168.40.3  192.168.40.1
```

！查看 Switch B

```
SwitchB#show vrrp brief
Interface  Grp  Pri  timer  Own  Pre  State   Master addr   Group addr
VLAN 10    10   100  3      -    P    Backup  192.168.10.2  192.168.10.1
VLAN 20    20   100  3      -    P    Backup  192.168.20.2  192.168.20.1
VLAN 30    30   120  3      -    P    Master  192.168.30.3  192.168.30.1
VLAN 40    40   120  3      -    P    Master  192.168.40.3  192.168.40.1
```

如上信息所示，当链路正常连接时，Switch A 为备份组 10、20 的 Master 路由设备，相应的优先级为 120；而 Switch B 为备份组 10、20 的 Backup 路由设备。

第三步，断开 Switch A 的上行链路，查看设备的 VRRP 状态如下：

！查看 Switch A

```
SwitchA#show vrrp brief
Interface  Grp  Pri  timer  Own  Pre  State   Master addr   Group addr
VLAN 10    10   90   3      -    P    Backup  192.168.10.3  192.168.10.1
VLAN 20    20   90   3      -    P    Backup  192.168.20.3  192.168.20.1
VLAN 30    30   100  3      -    P    Backup  192.168.30.3  192.168.30.1
VLAN 40    40   100  3      -    P    Backup  192.168.40.3  192.168.40.1
```

！查看 Switch B

```
SwitchB#show vrrp brief
Interface  Grp  Pri  timer  Own  Pre  State   Master addr   Group addr
VLAN 10    10   100  3      -    P    Master  192.168.10.3  192.168.10.1
VLAN 20    20   100  3      -    P    Master  192.168.20.3  192.168.20.1
VLAN 30    30   120  3      -    P    Master  192.168.30.3  192.168.30.1
VLAN 40    40   120  3      -    P    Master  192.168.40.3  192.168.40.1
```

如上信息所示，当 Switch A 的上行链路出现故障，系统自动降低其备份组 10、20 的优先级为 90，并切换状态为 Backup；相应，Switch B 就成为备份组 10、20 的 Master 路由设备。

5.5 故障诊断与排除

VRRP 如果出现故障可以通过考察配置以及调试信息来分析和解决。以下是常见的故障的分析说明：

故障现象：虚拟 IPv4 地址 Ping 不通

故障分析：

- 必须确保备份组内至少有一台路由设备处于活动状态；
- 如果在其它网络设备上 Ping 虚拟 IPv4 地址不通则可能由于以下原因引起: 由于 VRRP 状态的转换需要短暂时间这可以通过 **show vrrp** 命令考察 VRRP 信息来确认；
- 如果本地网络设备与虚拟路由设备位于同一网段就需要考察本地网络设备的 ARP 表/ND 邻居表中是否有虚拟 IPv4 地址的 ARP 项，如果没有就需要检查网络线路；
- 如果本地网络设备与虚拟路由设备不在同一网段则需要确认在本地网络设备上是否有到虚拟 IPv4 地址的路由；

故障现象：虚拟 IPv4/v6 地址 Ping 不通

故障分析：

- 必须确保备份组内至少有一台路由设备处于活动状态；
- 如果在其它网络设备上 Ping 虚拟 IPv4/v6 地址不通则可能由于以下原因引起: 由于 VRRP 状态的转换需要短暂时间这可以通过 **show [ipv6] vrrp** 命令考察 VRRP 信息来确认；
- 如果本地网络设备与虚拟路由设备位于同一网段就需要考察本地网络设备的 ARP 表/ND 邻居表中是否有虚拟 IPv4/IPv6 地址的 ARP 项，如果没有就需要检查网络线路；
- 如果本地网络设备与虚拟路由设备不在同一网段则需要确认在本地网络设备上是否有到虚拟 IPv4/v6 地址的路由；

故障现象：同一个 VRRP 备份组内出现多个 Master 路由设备

故障分析：

- 同一 VRRP 备份组内各路由设备以太网接口上 VRRP 组验证模式不同；
- 对于 VRRPv2，同一 VRRP 备份组内各路由设备以太网接口上 VRRP 组验证模式相同均为明文密码模式，但是验证字符串不一致；
- 同一 VRRP 备份组内存在路由设备的以太网口电缆断开，但是路由设备未能检测到以太网口电缆已经断开；
- 同一个 VRRP 备份组内路由设备上 VRRP 的通告发送间隔不一致，并且未设置定时设备学习功能；
- 同一个 VRRP 备份组内路由设备上 VRRP 的虚拟 IPv4/IPv6 地址不一致。

6 VRRP Plus

6.1 概述

VRRP Plus (Virtual Router Redundancy Protocol Plus，扩展虚拟路由冗余)功能是对 VRRP 协议的扩展，利用 VRRP 协议进行 IEEE 802.3 局域网内的网关备份和负载均衡。

VRRP 协议有个不足之处是：处于备份状态的路由设备，没有承担报文转发的任务。如果要用 VRRP 实现负载均衡，则需要手工配置多个 VRRP 组，将局域网内主机的网关指向不同 VRRP 组的虚拟 IP。这会增大网络管理员的工作量。而 VRRP Plus 就是为了解决上述不足而设计的。

VRRP Plus 的好处：自动实现负载均衡，即自动将不同主机的流量分配到 VRRP Plus 组成员中。从而大大减轻网络管理员的负担。

6.1.1 基本原理

VRRP Plus 的基本原理是：局域网中的主机使用统一的网关 IP，但不同主机在请求网关 ARP 时，由 VRRP Plus 应答不同的虚拟 MAC。从而将不同主机的流量分配到 VRRP Plus 的不同成员上，实现负载均衡。

VRRP Plus 引入两种角色如下：

- BVG：Balancing Virtual Gateway，均衡的虚拟网关。负责 VRRP Plus 组成员虚拟 MAC 的分配，局域网中针对网关 ARP 的应答。同时也承担局域网中主机报文的转发。启用 VRRP Plus 功能后，由于虚 IP 对应多个虚 mac 地址，show arp 等相关命令将看不到虚 ip 的 arp 表项。可以通过 show vrrp balance 查看虚 IP 与虚 mac 的对应关系。
- BVF：Balancing Virtual Forwarder，均衡的虚拟转发者。负责局域网中主机报文的转发。若分配到虚 MAC，则会参与转发，否则不会参与转发。

VRRP Plus 是依赖于 VRRP 协议运行的，其运行规则如下：

VRRP 中 Master 的角色，对应 VRRP Plus 中 BVG 角色，VRRP 中 Backup 的角色，对应 VRRP Plus 中 BVF 角色。局域网内主机的网关还是指向 VRRP 的虚拟 IP。

BVG 负责给 BVF 分配虚拟 MAC。为和 VRRP 兼容，BVG 直接使用 VRRP 的虚拟 MAC，即 00-00-5E-00-01-{VRID}（VRID 为 VRRP 组号）。BVF 使用的虚拟 MAC 为 00-1A-A9-16-{MemberID}-{VRID}。MemberID 为 VRRP Plus 组成员的编号。目前 VRRP Plus 支持 4 个成员，BVG 使用成员编号 01，其它三个 BVF 使用成员编号 02～04。

BVG 负责响应局域网内主机的网关 ARP 请求。根据均衡策略的不同，BVG 使用不同的虚拟 MAC 进行应答。均衡策略有三种：基于主机响应，轮询响应和基于权重响应。基于主机响应是指对于特定的主机，使用特定的虚拟 MAC 地址进行应答；轮流响应是指对于收到的主机的网关地址 ARP 请求，轮流使用备份组的各个虚拟 MAC 地址进行应答；基于权重是指根据设备的转发能力进行 ARP 报文的应答。如果在不同的负载均衡模式下切换，则最终都是在新的模式下实现负载均衡，如之前使用的是基于轮询的负载均衡模式，之后使用基于权重的负载均衡模式，则是在新的模式下实现负载均衡，即不考虑设备之前的应答情况。如果基于权重策略，且 VRRP Plus 组内虚拟路由器总的权重值为 0，则不会应答 arp 请求。

VRRP Plus 同样具有冗余备份功能。BVG 能够利用 VRRP 与 bfd 联动的会话信息，来与 BVF 建立会话，以在毫秒级别内检测 BVF 的活跃状态。如果 BVF 出现故障，BVG 会安排剩下的成员之一，接管故障 BVF 的转发功能。这一功能称为代

理转发。如果 BVF 从故障中恢复，则应该恢复其转发角色，继续承担该虚拟 MAC 地址的报文转发任务。但如果原设备一直未能恢复，则备份组应该停止重定向流量到该虚拟 MAC 地址，即再收到对网关地址的 ARP 请求时，不再使用该虚拟 MAC 地址进行应答；而且，经过足够长的时间后，我们可以认为原来使用该虚拟 MAC 地址作为网关 MAC 的用户已经更新了网关地址的 ARP 表项、流量已经由其他设备承担，此时便可以删除该虚拟 MAC 地址，发往该虚拟 MAC 地址的报文应该被丢弃。为此，VRRP Plus 支持设置备份组的重定向时间和超时时间。当设备出现故障后，备份组将其虚拟 MAC 地址分配给其他设备进行代理。在重定向时间内，备份组继续使用该虚拟 MAC 地址应答 ARP 请求；超过重定向时间后，便不再使用该虚拟 MAC 地址进行应答。经过超时时间后，备份组应删除该虚拟 MAC 地址。

VRRP Plus 支持备份组的权重配置。为不同的设备设置不同的权重值，以使权重值大者分担较多流量，权重值小者分担较少流量，使不同设备的转发性能得到充分利用。当备份组中 BVF 设备的权重值低于下阈值时，将自动退出转发角色，当权重值恢复、高于上阈值时，应该自动申请转发角色，能否恢复转发角色，取决于当前是否有剩余的虚 mac 地址或者代理的虚 mac 地址。

VRRP Plus 支持与链路检测协议联动、根据链路状态调整权重值。备份组中各台设备可以各自关联相应的链路状态，当该链路出现异常、不通时，该设备应自动降低其权重值；如果权重过低、则应该可以退出转发角色。若备份组正在使用基于权重的负载均衡策略，便可以根据其新的权重值为其分配相应的流量。当关联的链路状态得以恢复时，该设备能够自动恢复权重值、恢复转发角色；对于采用基于权重的负载均衡方式的备份组，根据其恢复后的权重值为其分配不同主机的流量。

VRRP Plus 支持转发角色的抢占功能。VRRP Plus 中参与负载均衡的设备数量上限为四台。即一个 VRRP Plus 备份组中最多会产生四个虚拟 MAC 地址，当有超过四台设备加入一个 VRRP Plus 组时，只有四台设备会参与报文转发，其余的设备则不参与，仅监听其他设备的状况；只有当参与转发的设备出现故障时，才会替换其角色，开始对报文进行转发。当已经有四台设备组成 VRRP Plus 备份组，并均在负责报文转发，此时有第五台设备加入 VRRP Plus 组，且这台设备转发能力较强，或者原有转发角色出现链路故障、导致转发能力降低，如果配置允许抢占模式，则第五台设备可以抢占其他权重较低（即转发能力较低）的设备。为转发能力较强的设备配置较高的权重值，当发现处于监听状态的设备的权重值比正在负责转发的设备的权重值更高时，使监听设备自动抢占转发设备的角色，由转发能力更强的设备负责报文转发，较低的设备进行监听。这样可以尽量减少资源的浪费。由于备份组中的 BVG 设备负责管理虚 MAC 地址分配，故 BVG 的角色不可以被抢占；只有 BVF 的转发角色可以被抢占。

如果 BVG 所在的设备出现故障，VRRP 会重新选举 Master，因此 BVG 也会在新的 Master 设备上生成。

在配置了 VRRP Plus 后，若收到主机的 ARP 请求报文，可以基于不同的负载均衡策略进行应答，以实现对这些主机的负载均衡；但是对于配置 VRRP Plus 之前、已经学习到了 VRRP 虚网关地址的主机，不支持对这些主机的负载均衡。因此，如果待 VRRP 状态切换为 Master 之后才配置 VRRP Plus，则在主机学到的 ARP 老化之前，无法真正的实现负载均衡；待主机记录的网关 ARP 老化、重新请求网关地址时，才会负载均衡。

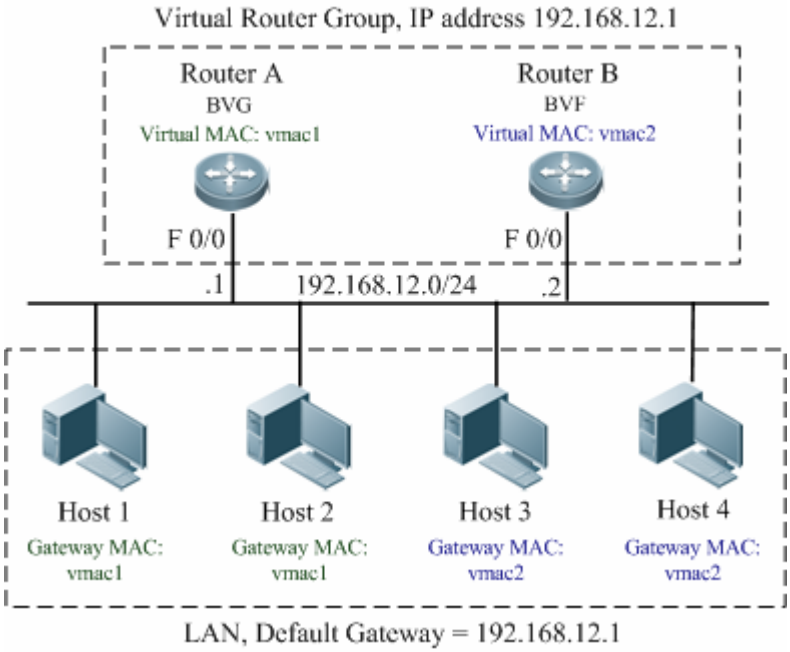
接口的定时发送免费 ARP 的功能也会影响 VRRP Plus 的负载均衡功能。当打开了 VRRP Plus 时，便屏蔽虚地址的免费 ARP 的发送。当虚地址、实地址重叠时，不再发送该地址的免费 ARP 报文。

当发现有主机与本设备地址出现冲突时，ARP 模块也会广播发送该地址的免费 ARP 报文。如果发生冲突的是 VRRP Plus 的虚地址，那么发送的免费 ARP 报文就会导致主机的网关 MAC 地址被重新学习，破坏 VRRP Plus 的负载均衡功能，此情况暂不支持 VRRP Plus 的负载均衡功能。

6.1.2 典型应用

VRRP Plus 的应用拓扑可以通过下图示例来说明：

图 6-1 VRRP Plus 应用拓扑示意图



如图在一个局域网中，IP 网段是 192.168.12.0/24。两台三层设备 A 和 B，组成一个 VRRP Plus 组，虚拟 IP 是 192.168.12.1。三层设备 A 是 VRRP 的 Master，承担 BVG 职责。三层设备 B 是 VRRP 的 Backup，承担 BVF 职责。局域网中的四台主机，网关都指向 192.168.12.1。Host1 和 Host2 请求网关 ARP 后，响应的 MAC 为 0000.5e00.0101。Host3 和 Host4 请求网关 ARP 后，响应的 MAC 为 001A.A916.0201。这样 Host1 和 Host2 与外网通讯的报文就发送到三层设备 A，Host3 和 Host4 与外网通讯的报文就发送到三层设备 B。从而达到了负载均衡的目的。

6.2 配置VRRP Plus

VRRP Plus 协议适用于 IEEE 802.3 局域网，在以太网接口上配置。VRRP Plus 的配置任务有：

- （必须）启动 VRRP Plus 功能
- （可选）设置 VRRP Plus 负载均衡策略
- （可选）设置 VRRP Plus 备份组的代理虚 MAC 地址的重定向时间间隔和重定向的超时时间
- （可选）设置 VRRP Plus 备份组的权重和阈值
- （可选）设置 VRRP Plus 备份组的转发抢占功能
- （可选）设置 VRRP Plus 备份组的权重值的跟踪对象

下表用来描述 VRRP Plus 的缺省配置。

功能特性	缺省值
VRRP Plus 功能	未配置
启动 VRRP Plus 后，负载均衡策略功能	轮询的负载均衡策略
启动 VRRP Plus 后，代理虚 MAC 地址的重定向时间间隔	300 秒（即 5 分钟）
启动 VRRP Plus 后，代理虚 MAC 地址重定向的超时时间	14400 秒（即 4 小时）
启动 VRRP Plus 后，备份组的权重	100

启动 VRRP Plus 后，备份组的权重上限值	100
启动 VRRP Plus 后，备份组的权重下限值	1
启动 VRRP Plus 后，备份组的转发抢占功能	允许抢占
启动 VRRP Plus 后，备份组的权重值的跟踪对象	未配置
启动 VRRP Plus 后，备份组的权重值的跟踪对象罚值	配置跟踪对象后，缺省罚值为 10

6.2.1 启动VRRP Plus功能

以太网接口上配置了 VRRP 功能后，才能启动 VRRP Plus 功能。VRRP Plus 配置的步骤为：

命令	作用
Ruijie(config)# **interface** *interface-id*	进入接口配置模式
Ruijie(config-if)# **vrrp group ip** *address*	配置一个 VRRP 组
Ruijie(config-if)# **vrrp group balance**	在指定组号的 IPv4 VRRP 备份组上启用 VRRP Plus 功能

VRRP Plus 组号 *group* 取值范围为 1~255，与 VRRP 配置相同。

6.2.2 设置VRRP Plus负载均衡策略

VRRP Plus 目前支持三种负载均衡策略。一种是基于主机的不同而使用不同的虚拟 MAC 应答 ARP，一种是轮流使用不同的虚拟 MAC 应答 ARP，一种是基于备份组的设备权重值进行应答。

命令	作用
Ruijie(config-if)# **vrrp group load-balancing** { **host-dependent | round-robin | weighted** }	设置 VRRP Plus 负载均衡策略。host-dependent 是基于主机的均衡，round-robin 是轮询的均衡，weighted 是基于备份组权重的均衡。
Ruijie(config-if)# **no vrrp group load-balancing** { **host-dependent | round-robin | weighted** }	恢复默认的 VRRP Plus 负载均衡策略。

缺省负载均衡策略为 round-robin 方式，即轮询的负载均衡策略。

6.2.3 设置VRRP Plus备份组的重定向时间和超时时间

VRRP Plus 支持设置备份组的重定向时间和超时时间。当设备出现故障后，备份组将其虚拟 MAC 地址分配给其他设备进行代理。在重定向时间内，备份组继续使用该虚拟 MAC 地址应答 ARP 请求；超过重定向时间后，便不再使用该虚拟 MAC 地址进行应答。经过超时时间后，备份组应删除该虚拟 MAC 地址

命令	作用
Ruijie(config-if)# **vrrp group timers redirect** *redirect timeout*	设置 VRRP Plus 备份组的代理虚 MAC 地址的重定向时间间隔和重定向的超时时间。 *redirect*：重定向时间，默认值 300 秒（即 5 分钟），取值范围为 0-3600。 *timeout*：超时时间，默认值 14400 秒（即 4 小时），取值范围为(*redirect* + 600)-64800。

Ruijie(config-if)# **no vrrp** *group* **timers redirect**	恢复 VRRP Plus 备份组的默认重定向时间间隔和超时时间。

6.2.4 设置VRRP Plus备份组的权重和阈值

为不同的设备设置不同的权重值，以使权重值大者分担较多流量，权重值小者分担较少流量，使不同设备的转发性能得到充分利用。当备份组中 BVF 设备的权重值低于下限值时，将自动退出转发角色，当权重值恢复、高于上限值时，应该自动恢复转发角色。

命令	作用
Ruijie(config-if)# **vrrp group weighting** *maximum* [**lower** *lower*] [**upper** *upper*]	设置 VRRP Plus 备份组的权重和上下限值。 *maximum*：权重值，默认值 100，取值范围 2-254 *lower*：权重下限值，默认值 1，取值范围 1-（*maximum* - 1） *upper*：权重上限值，默认值 100，取值范围 *lower-maximum*
Ruijie(config-if)# **no vrrp** *group* **weighting**	恢复 VRRP Plus 备份组的默认权重值。

6.2.5 设置VRRP Plus备份组的转发抢占功能

VRRP Plus 允许设置备份组的转发抢占功能；为转发能力较强的设备配置较高的权重值，当发现处于监听状态的设备的权重值比正在负责转发的设备的权重值更高时，使监听设备自动抢占转发设备的角色，由转发能力更强的设备负责报文转发，较低的设备进行监听

命令	作用
Ruijie(config-if)# **vrrp group forwarder preempt**	设置 VRRP Plus 备份组的转发抢占功能。
Ruijie(config-if)# **no vrrp group forwarder preempt**	关闭转发抢占功能。

默认为允许转发抢占。

6.2.6 设置VRRP Plus备份组的权重值的跟踪对象

支持根据链路检测状态，动态调整备份组的权重值。默认未配置跟踪。

命令	作用
Ruijie(config-if)# **vrrp group weighting track** *object-number* [**decrement** *value*]	设置 VRRP Plus 备份组的权重值的跟踪对象。 *object-numbe* 为 track 跟踪对象号，取值范围 1-700。 *Value* 为跟踪对象 down 时减少的权重值，默认为 10，取值范围 1-255。
Ruijie(config-if)# **no vrrp group weighting track** *object-number*	删除相应的跟踪对象。

配置 track 跟踪对象，可以参考 track 功能配置的相关文档，如《Rns & track 配置》和《配置 Rns & track 命令》。

6.3 监视与维护

debug vrrp balance

为 VRRP Plus 模块增加以下调试开关：

命令	作用
debug vrrp balance errors	监控错误信息
debug vrrp balance messages	监控与 VRRP、TRACK 模块间的消息
debug vrrp balance packets	监控 VRRP Plus 协议报文
debug vrrp balance state	监控 VRRP Plus 组状态
debug vrrp balance timer	监控 VRRP Plus 组的定时器消息
debug vrrp balance event	监控 VRRP Plus 组的事件
debug vrrp balance	监控所有信息

show vrrp balance

查看 VRRP Plus 运行状态可以使用以下两个命令：

命令	作用
Ruijie# **show vrrp balance** [**brief** | *group*]	显示 VRRP Plus 的状态。可以指定组号。可以显示简要信息。
Ruijie# **show vrrp balance interface** *interface-id* [**brief**]	显示指定接口上的 VRRP Plus 信息。brief 参数表示显示简要信息。

下面给出使用这些命令的示例：

1. 命令 **show vrrp balance** [**brief** | *group*]

```
Ruijie# show vrrp balance brief
Interface   Grp   State   Group Addr    MAC addr
VLAN 1      1     BVG     192.168.1.1   0000.5e00.0101
Ruijie#show vrrp balance
VLAN 1 - Group 1
  State is BVG
  Virtual IP address is 192.168.1.54
  Hello time 1 sec, hold time 3 sec
  Load balancing: host-dependent
  Redirect time 300 sec, forwarder time-out 14400 sec
  Weighting 90 (configured 100), thresholds: lower 1, upper 100
Track object 1, state: down, decrement weight: 10
There are 2 forwarders
  Forwarder 1 (local)
    MAC address:
      0000.5e00.0101
    Owner ID is 00d0.f822.33ab
  Forwarder 2
    MAC address:
      001a.a916.0201
    Owner ID is 00d0.f822.8800
```

2. 命令 **show vrrp balance interface** *type number* [**brief**]

```
Ruijie# show vrrp balance interface vlan 1
VLAN 1 - Group 1
  State is BVG
  Virtual IP address is 192.168.1.54
  Hello time 1 sec, hold time 3 sec
  Load balancing: host-dependent
  Redirect time 300 sec, forwarder time-out 14400 sec
  Weighting 90 (configured 100), thresholds: lower 1, upper 100
Track object 1, state: down, decrement weight: 10
There are 2 forwarders
  Forwarder 1 (local)
    MAC address:
      0000.5e00.0101
    Owner ID is 00d0.f822.33ab
  Forwarder 2
    MAC address:
      001a.a916.0201
    Owner ID is 00d0.f822.8800
```

6.4 配置举例

如图 1 所示的典型拓扑中，两台三层设备的配置如下。

三层设备 A：

```
Ruijie(config)#track 1 interface FastEthernet 0/14 line-protocol
interface FastEthernet 0/0
no switchport
ip address 192.168.1.2 255.255.255.0
vrrp 1 ip 192.168.1.1
vrrp 1 balance
vrrp 1 load-balancing weighted
vrrp 1 weighting track 1 decrement 100
```

三层设备 B：

```
Ruijie(config)#track 1 interface FastEthernet 0/14 line-protocolinterface FastEthernet 0/0
no switchport
ip address 192.168.1.3 255.255.255.0
vrrp 1 ip 192.168.1.1
vrrp 1 balance
vrrp 1 load-balancing weighted
vrrp 1 weighting track 1 decrement 100
```

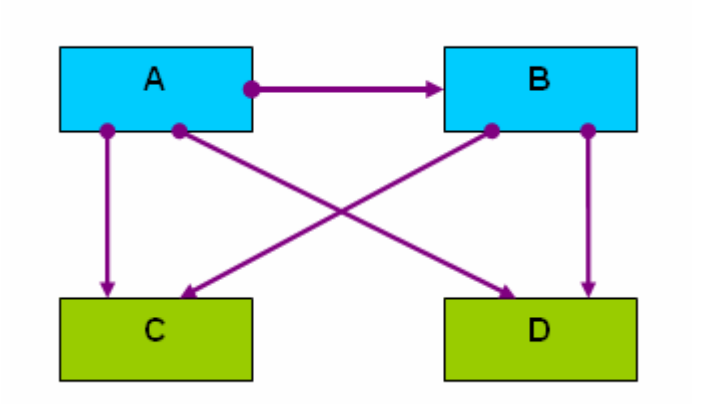
7 TPP

7.1 概述

TPP(Topology Protection Protocol，拓扑保护协议)是一个拓扑稳定保护协议。网络拓扑比较脆弱，当网络中存在非法攻击时，可能造成网络设备的 CPU 利用率异常、帧通路堵塞等现象，这些现象很容易引起网络拓扑的振荡。拓扑防护主要通过检测本地的异常现象（CPU 利用率异常、帧缓冲异常等）和检测邻居设备的异常现象来达到稳定网络拓扑的目的。与邻居设备的交互是通过发送特定的异常通告报文来实现的，该功能拥有较高的运行优先级，可以有效防止网络的拓扑振荡。

拓扑防护主要是针对 MSTP 或 VRRP 以及其他分布式网络协议可能造成的网络拓扑振荡而产生的。MSTP 或 VRRP 等协议均使用定时报文通告机制来自动维护网络拓扑结构，自动适应网络中的拓扑变化。这也造成了网络拓扑易受攻击，当受到人为的网络攻击时，因 CPU 利用率过高或帧通路阻塞等原因，可能造成定时报文的短暂中断，从而造成网络拓扑发生错误的振荡，这给网络的正常通信造成极大危害。而拓扑防护功能正是为了最大限度的防止这种不必要的网络振荡，它与其他分布式协议（MSTP、VRRP 等）协同工作，从而使网络更加稳定、可靠。

图 7-1

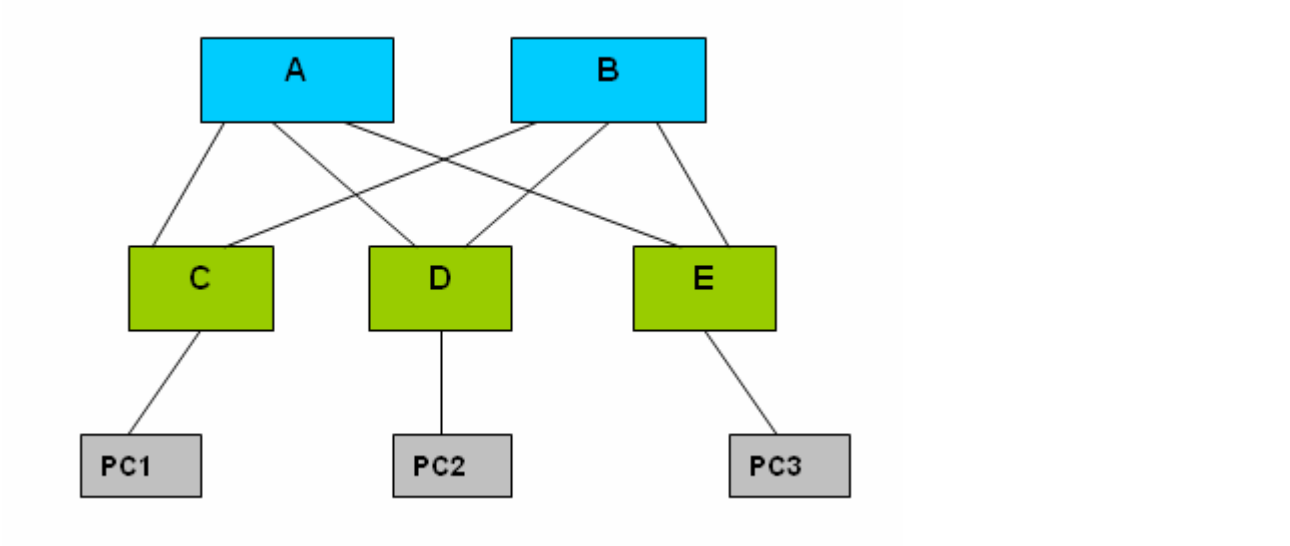


如上图的双核心拓扑，图中 A、B 为三层汇聚设备，C、D 为二层接入设备。A 为 MSTP 的根桥，各个网络设备的拓扑防护功能均开启。

三层汇聚设备 A 因遭受网络攻击造成 CPU 异常繁忙，从而导致 BPDU 报文不能正常发送。这时，拓扑防护功能检测到异常后，会向邻居设备发送异常通告报文，图中二层接入设备C、D的和三层汇聚设备B均接收到异常通告，这时，设备C、D 的和设备 B 会根据异常通告信息，进行相应的防振荡处理。

设备B因遭受大量报文攻击造成CPU异常繁忙，这时造成收发包不正常，检测到异常后，它会向所有的邻居设备发送异常通告。设备 A 收到异常报文后，根据来源，发现异常对其没有影响，不会进一步处理。而下游的二层接入设备 C、D 接收到异常报文后，发现异常会影响其拓扑的计算，因此做进一步的防御处理，从而保证网络拓扑保持稳定。

图 7-2



如上图，A、B 为三层汇聚设备，C、D 和 E 为二层接入设备。

三层汇聚设备 A、B 和二层接入设备 C、D 和 E 均开启 MSTP，同时两台三层汇聚设备开启 VRRP 协议。拓扑防护功能使 MSTP 和 VRRP 运行更加稳定，避免网络拓扑发生不必要的振荡。

对于三层汇聚设备 A、B 使能全局拓扑防护功能，同时使能各个端口的拓扑防护功能。对于各台二层接入设备 C、D 和 E 使能全局拓扑防护功能。

7.2 配置TPP

TPP 配置包括全局功能配置和端口功能配置。全局功能配置用于使能设备的拓扑防护功能，默认情况下，全局拓扑防护功能使能，这时它会检测本地和邻居设备的运行情况，对产生的异常情况进行处理。不过它不会向邻居设备通告本地的运行情况。端口功能配置用于使能端口的拓扑防护功能，端口的拓扑防护功能使能时，表示对端的邻居设备关心本地设备的运行情况，因此当本地设备发生异常时，将通告该端口的对端邻居设备。默认情况下，所有端口的拓扑防护功能关闭。

拓扑防护功能适用于点对点链路的网络，且相邻网络设备都必须使能拓扑防护功能。另外，部署 TPP 功能时，通常需要通过 cpu topology-limit 命令配置 cup 利用率检测的阀值，当设备的 cpu 利用率超过该值时，系统会产生拓扑防护通告。建议该值设置在一个中等偏上的位置比较合适，比如 50-70,这时 TPP 能够较为准确地对网络情况进行判断。如果该值太低，则可能导致网络拓扑该切换的时候由于 TPP 的报警而不切换，如果该值太高，则可能系统已经繁忙到无法产生 TPP 告警，导致 TPP 功能失效。

7.2.1 配置全局拓扑防护

全局拓扑防护功能默认是使能的。使用该命令的 **no** 选项禁止全局拓扑防护。

命令	作用
Ruijie# **config terminal**	进入全局配置模式
Ruijie(config)# **topology guard**	使能全局拓扑防护

使用 **no topology guard** 禁止设备的全局拓扑防护功能

7.2.2 配置端口拓扑防护

命令	作用
Ruijie# **config terminal**	进入全局配置模式
Ruijie(config)# **interface** *interface-id*	进入接口配置模式
Ruijie(config-if)# **tp-guard port enable**	使能端口拓扑防护功能

使用 **no tp-guard port enable** 禁止端口的拓扑防护，该命令只适用于二层交换口和路由口。不适用于 AP 成员口。

全局拓扑防护作为拓扑防护的全局开关，当全局拓扑防护使能时，设备会检测本设备的运行参数，同时监听各个邻居设备的运行参数，但当本地出现异常现象时，它不会向邻居设备发送异常通告报文进行通告。端口的拓扑防护功能使能时，当本地出现异常现象时，会向该端口对端的邻居设备发送异常通告报文进行异常通告。

7.2.3 查看设备的TTP配置及状态

命令	作用
Ruijie# **show tpp**	查看设备的 TPP 配置及状态。

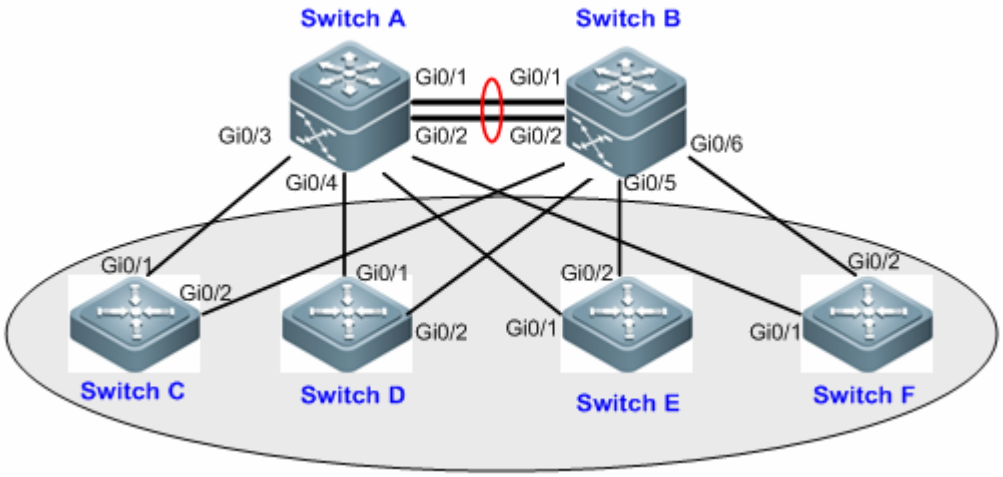
例：查看设备的 TTP 配置及状态

```
Ruijie #show tpp
tpp state          : enable
tpp local bridge   : 00d0.f822.35ad
```

7.3 配置举例

拓扑图

图 7-3 TPP 典型应用拓扑图



应用需求

如上图所示，某园区网络的核心层采用典型的 MSTP+VRPP 双核心拓扑结构。当网络中存在非法攻击时，可能造成网络设备的 CPU 利用率异常、帧通路堵塞等现象，很容易引起网络拓扑的振荡。

通过应用 TPP 功能，使 MSTP 和 VRRP 的运行能较为稳定，避免网络拓扑发生不必要的振荡。

配置要点

在三层核心设备（Switch A/B）和二层接入设备（Switch C/D/E/F）上配置以下功能：

- 使能全局拓扑防护功能。该功能默认开启。
- 使能连接设备的接口的拓扑防护功能，在本机出现异常时能及时通告邻居保持拓扑稳定。
- 在每台设备上配置 CPU 利用率检测的阈值，当设备的 CPU 利用率超过该值时，系统会产生拓扑防护通告。

> 建议该值设置在一个中等偏上的位置比较合适，比如 50-70，这时 TPP 能够较为准确地对网络情况进行判断。如果该值太低，则可能导致网络拓扑该切换的时候由于 TPP 的报警而不切换，如果该值太高，则可能系统已经繁忙到无法产生 TPP 告警，导致 TPP 功能失效。

配置步骤

以下仅列举设备上的 TPP 功能配置，对于 MSTP+VRPP 的相关配置说明可参见手册的《MSTP 配置》和《VRRP 配置》部分。

- Switch A/B 上的配置

第一步，全局拓扑防护功能功能默认开启。如果被关闭，可以使用以下命令开启。

```
Ruijie# config terminal
Ruijie(config)# topology guard
```

第二步，开启接口拓扑防护功能

！开启核心设备间 AP 口的拓扑防护功能

```
Ruijie(config)#interface aggregateport 1
Ruijie(config-if-AggregatePort 1)#tp-guard port enable
```

！开启下联设备接口的端口拓扑防护功能

```
Ruijie(config)#interface range gigabitEthernet 0/3-6
Ruijie(config-if-range)#tp-guard port enable
```

第三步，配置 CPU 利用率检测的阈值

！在设备 cpu 利用率超过百分之六十时，系统会产生拓扑防护通告

```
Ruijie(config)#cpu topology-limit 60
```

- Switch C/D/E/F 上的配置

第一步，全局拓扑防护功能功能默认开启。如果被关闭，可以使用以下命令开启。

```
Ruijie# config terminal
Ruijie(config)# topology guard
```

第二步，开启接口拓扑防护功能

```
Ruijie(config)#interface range gigabitEthernet 0/1-2
Ruijie(config-if-range)#tp-guard port enable
```

第三步，配置 CPU 利用率检测的阈值

！在设备 CPU 利用率超过百分之六十时，系统会产生拓扑防护通告

```
Ruijie(config)#cpu topology-limit 60
```

验证结果

- TPP 功能配置查看

以 Swtich A 为例，查看 TPP 的配置；关注点：TPP 状态，接口 TPP 信息。

```
Ruijie#show tpp
tpp state         : enable       //全局 TPP 功能默认开启
tpp local bridge  : 00d0.f822.33aa
----------------------------------
interface GigabitEthernet 0/3
port tpp state       : enable
interface GigabitEthernet 0/4
port tpp state       : enable
interface GigabitEthernet 0/5
port tpp state       : enable
interface GigabitEthernet 0/6
port tpp state       : enable
interface AggregatePort 1
port tpp state       : enable
```

- TPP 功能生效性验证

生成树拓扑稳定时，SwitchA 为根桥， Swtich C 的 Gi0/2 口处于 Block 状态。

第一步，为了模拟 Swtich C 由于受到下连非法用户的攻击。在验证中，将 Swtich B 的 Gi0/3 口配置 BPDU Filter 功能，使得 Swtich C 的 Gi0/2 口收不到 BPDU 报文；在未配置 TPP 的情况下，Swtich C 的 Gi0/2 口转变成 Forwarding 状态。拓扑改变。

```
Ruijie#show spanning-tree sum
Spanning tree enabled protocol mstp
MST 0 vlans map : 1-9, 11-19, 21-29, 31-39, 41-4094
  Root ID    Priority    4096
             Address     00d0.f834.56f0
             this bridge is root
```

```
            Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

  Bridge ID  Priority    32768
             Address     00d0.f822.33aa
             Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

Interface   Role   Sts   Cost    Prio   Type   OperEdge
---------   ----   ---   -----   ----   ----   --------
Gi0/2       Desg   FWD   20000   128    P2p    True
Gi0/1       Root   FWD   20000   128    P2p    False

MST 1 vlans map : 10, 20
  Region Root Priority   4096
             Address     00d0.f834.56f0
             this bridge is region root

  Bridge ID  Priority    32768
             Address     00d0.f822.33aa

Interface   Role   Sts   Cost    Prio   Type   OperEdge
---------   ----   ---   -----   ----   ----   --------
Gi0/2       Desg   FWD   20000   128    P2p    True
Gi0/1       Root   FWD   20000   128    P2p    False
```

第二步，在 Swtich C 按本例的配置步骤完成 TPP 的相关配置后，模拟 Swtich C 受到下连非法用户的攻击，向 Swtich C 发送大量 ARP 报文，导致 CPU 利用率超过限定值。此时再将 Swtich B 的 Gi0/3 口配置 BPDU Filter 功能，使得 Swtich C 的 Gi0/2 口收不到 BPDU 报文；查看 Swtich C 生成树接口的状态，发现接口仍然维持在 Block 状态。TPP 功能生效。

```
Ruijie#show spanning-tree summary
Spanning tree enabled protocol mstp
MST 0 vlans map : 1-9, 11-19, 21-29, 31-39, 41-4094
  Root ID    Priority    4096
             Address     00d0.f834.56f0
             this bridge is root
             Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

  Bridge ID  Priority    32768
             Address     00d0.f822.33aa
             Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

Interface   Role   Sts   Cost    Prio   Type   OperEdge
---------   ----   ---   -----   ----   ----   --------
Gi0/2       Altn   BLK   20000   128    P2p    False
Gi0/1       Root   FWD   20000   128    P2p    False

MST 1 vlans map : 10, 20
```

```
  Region Root Priority   4096
              Address    00d0.f834.56f0
              this bridge is region root

  Bridge ID  Priority    32768
              Address    00d0.f822.33aa

Interface   Role   Sts   Cost    Prio   Type   OperEdge
---------   ----   ---   -----   ----   ----   --------
Gi0/2       Altn   BLK   20000   128    P2p    False
Gi0/1       Root   FWD   20000   128    P
```

8 BFD

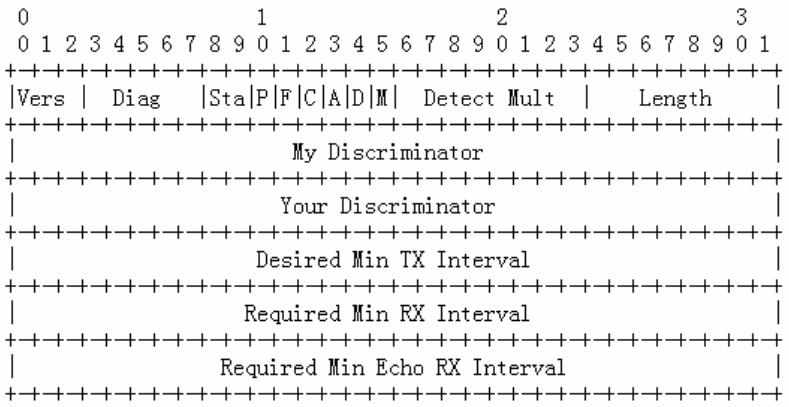
8.1 概述

BFD(Bidirectional Forwarding Detection，双向转发检测)协议提供一种轻负载、快速检测两台邻接路由器之间转发路径连通状态的方法。协议邻居通过该方式可以快速检测到转发路径的连通故障，加快启用备份转发路径，提升现有网络性能。

8.1.1 BFD报文格式

BFD 报文有两种类型分别是控制报文和回声报文。其中回声报文只有 BFD 会话本端系统关心，远端系统不关心，因此协议没有规定其具体格式。协议只规定了控制报文的格式。目前控制报文格式有两个版本(版本 0 和版本 1)，建立 BFD 会话时缺省采用版本 1，如果收到对端系统发送的是版本 0 的报文，将自动切换到版本 0。可以通过 **show bfd neighbors** 命令查看采用的版本。

图 8-1 BFD 控制报文（版本 1）格式



字段	说明
Vers	BFD 协议版本号，目前为 1。 支持版本 1 和版本 0 的报文格式，缺省情况下会话发送报文采用版本 1，如果收到对端发送的版本 0 的报文，将自动切换到版本 0 来建立会话。
Diag	给出本地最后一次从 UP 状态转到其他状态的原因，包括： 0—没有诊断信息 1—控制超时检测 2—回声功能失效 3—邻居通告会话 Down 4—转发面复位 5—通道失效 6—连接通道失效 7—管理 Down

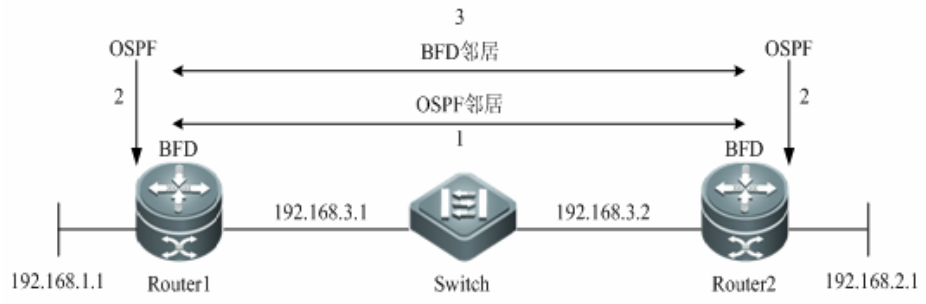
Sta	BFD 本地状态，包括： 0 代表 AdminDown 1 代表 Down 2 代表 Init 3 代表 Up
P	参数发生改变时，发送方在 BFD 报文中置该标志，接收方必须立即响应该报文。
F	响应 P 标志置位的回应报文中必须将 F 标志置位。
C	转发/控制分离标志，一旦置位，控制平面的变化不影响 BFD 检测，如：控制平面为 RIP，当 RIP 重启/GR 时，BFD 可以继续检测链路状态。
A	认证标识，置位代表会话需要进行验证。
D	查询请求，置位代表发送方期望采用查询模式对链路进行检测。
M	用于将来应用点到多点时使用，目前必须设置 0。
Detect Mult	检测超时倍数，用于检测方计算检测超时时间。
Length	报文长度。
My Discriminator	BFD 会话连接本端标识符。
Your Discriminator	BFD 会话连接远端标识符。
Desired Min Tx Interval	本地支持的最小 BFD 报文发送间隔。
Required Min RX Interval	本地支持的最小 BFD 报文接收间隔。
Required Min Echo RX Interval	本地支持的最小 Echo 报文接收间隔（如果本地不支持 Echo 功能，则设置 0）。
Auth Type	认证类型(可选)，包括： Simple Password Keyed MD5 Meticulous Keyed MD5 Keyed SHA1 Meticulous Keyed SHA1
Auth Length	认证数据长度。
Authentication Data	认证数据区。

8.1.2 BFD工作原理

BFD 提供的检测机制与所应用的接口介质类型、封装格式、以及关联的上层协议无关。BFD 在两台路由器之间建立会话，通过快速发送检测故障消息给正在运行的路由协议，以触发路由协议重新计算路由表，大大减少整个网络的收敛时间。BFD 本身没有发现邻居的能力，需要上层协议通知与哪个邻居建立会话。

如下图所示，两台路由器通过一台二层交换机相连，两台路由器同时运行 OSPF 和 BFD。

图 8-2 建立 BFD 会话



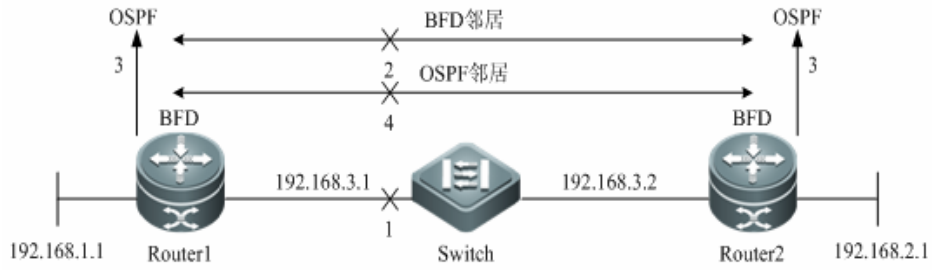
BFD 会话建立过程：

1) OSPF 发现邻居后并与邻居建立连接

2) OSPF 通知 BFD 与该邻居建立会话

3) BFD 与该邻居建立起会话

图 8-3 BFD 检测



BFD 会话检测到故障后的处理过程：

1) Router1 与 Switch 之间的链路通信发生故障

2) Router1 和 Router2 之间的 BFD 会话检测到故障

3) BFD 通知本地运行的 OSPF 到邻居的转发路径发生故障

4) OSPF 进行邻居 Down 过程的处理，如果存在备份转发路径那么将进行协议收敛，从而启用备份转发路径

8.1.3 相关协议规范

目前 BFD 的协议规范有：

- draft-ietf-bfd-base-09：Bidirectional Forwarding Detection
- draft-ietf-bfd-generic-05：Generic Application of BFD
- draft-ietf-bfd-mib-06：Bidirectional Forwarding Detection Management Information Base
- draft-ietf-bfd-v4v6-1hop-09：BFD for IPv4 and IPv6 (Single Hop)
- draft-ietf-bfd-multihop-07：BFD for IPv4 and IPv6 (Multihop)
- draft-ietf-bfd-mpls-07：BFD For MPLS LSPs

8.2 特性简介

8.2.1 建立BFD会话

以主动模式建立 BFD 会话：在建立会话前不管是否收到对端发来的建立 BFD 会话的控制报文，都会主动发送建立 BFD 会话的控制报文。

协商 BFD 会话参数

- 必须在两端接口上配置 BFD 会话参数(包括 Desired Min Tx Interval，Required Min RX Interval，Detect Mult)，否则 BFD 会话无法建立。
- 在建立 BFD 会话的过程中，两端接口会协商 BFD 会话参数，并依据此会话参数进行会话检测。
- 如果在建立 BFD 会话后修订 BFD 会话参数，则两端接口将重新发起协商。修订过程 BFD 会话保持 UP 状态。

8.2.2 BFD检测

以异步模式进行 BFD 检测：系统之间相互周期性地发送 BFD 控制报文，如果某个系统在检测时间内没有收到对端发来的 BFD 控制报文，就宣布会话为 Down。

8.2.3 BFD与动态路由协议联动

路由协议通过与BFD联动，可以利用BFD相对于协议自身的“HELLO”机制更快速检测故障的优点，提高协议的收敛性能。一般情况下，检测故障的时间可以缩短到 1 秒以内。

配置时需要确保 BFD 会话邻居都启用相应协议关联 BFD 会话，否则 BFD 会话将无法建立。但如果已经有动态路由协议或者其他应用通知 BFD 与相应邻居创建会话，那么该路由协议关联 BFD 会话也将建立。

8.2.4 BFD与静态路由联动

静态路由与 BFD 联动，可以避免在配置的静态路由不可达的情况下，路由选路不会选择该静态路由作为转发路径。如果存在备份路由转发路径，将可以快速地切换到该备份转发路径。

与动态路由协议不同，静态路由没有发现邻居的机制。因此，当配置 BFD 与静态路由关联，静态路由的下一跳可达性将依赖于 BFD 会话状态。如果 BFD 会话检测到故障，表示静态路由的下一跳不可达，则该静态路由将不安装到 RIB 中。配置时需要确保 BFD 会话邻居均启用静态路由关联 BFD 会话，否则 BFD 会话将无法建立。但如果已经有动态路由协议或者其他应用通知 BFD 与相应邻居创建会话，那么静态路由关联 BFD 会话也将使能。

如果 BFD 会话建立过程，远端系统删除 BFD 会话，将会造成 BFD 会话状态变为 Down，在这种情况下系统确保不影响静态路由的转发行为。

8.2.5 BFD与策略路由联动

策略路由与 BFD 联动，可以避免在配置的策略路由不可达的情况下，路由选路不会选择该策略路由作为转发路径。如果存在备份路由转发路径，将可以快速地切换到该备份转发路径。

与策略路由联动的方式等同于静态路由。通过 BFD 跟踪检测与指定邻居的转发路径，当会话检测到故障，将通知策略路由到达相应下一跳不可达，达到该下一跳的策略路由将不生效。

配置时需要确保 BFD 会话邻居都启用策略路由关联 BFD 会话，否则 BFD 会话将无法建立。但如果已经有动态路由协议或者其他应用通知 BFD 与相应邻居创建会话，那么策略路由关联 BFD 会话也将建立。

如果 BFD 会话建立过程，远端系统删除 BFD 会话，将会造成 BFD 会话状态变为 Down，在这种情况下系统确保不影响策略路由的转发行为。

8.2.6 BFD与VRRP联动

VRRP 与 BFD 联动可以替代 VRRP 自身的“HELLO”机制实现快速检测主备路由器的运行状态，加快了故障时主备路由器的切换，提高网络的性能。一般情况下，检测故障的时间可以缩短到 1 秒以内。

配置时需要确保 VRRP 两端的路由器都启用 VRRP 关联 BFD 会话，否则 BFD 会话将无法建立。但如果已经有动态路由协议或者其他应用通知 BFD 与相应邻居创建会话，那么 VRRP 关联 BFD 会话也将建立。

VRRP 还可以利用 BFD 来跟踪指定的邻居，如果 BFD 会话检测到与该邻居的转发路径发生故障，则自动降低 VRRP 优先级一定数额，触发主备路由器进行切换。该配置只有在动态路由协议或者其他应用通知 BFD 与相应邻居创建会话时，该会话才会创建。

8.2.7 BFD与VRRP+联动

VRRP+与 BFD 联动可以替代 VRRP+自身的 BVG 对 BVF 的检测，实现快速检测 BVF 的运行状态，加快了故障时转发实体的切换，提高网络的性能。一般情况下，检测故障的时间可以缩短到 1 秒以内。

VRRP+是基于 VRRP 协议的，所以在于 BFD 关联上，无须进行额外的配置，只需要确保两端的设备均已经开启 VRRP，并且正确的关联了 BFD 会话。

8.2.8 BFD支持VRF

BFD 支持 VRF（VPN Routing and Forwarding，VPN 路由转发），允许 BFD 检测 PE(provider edge)和 CE(customer edge)之间转发路径的连通状态。

8.3 配置BFD

BFD 只允许在 Routed Port 和 SVI 上配置，不支持在 L3 AP 上配置。如果 SVI 下的成员口为 L2AP，将无法在该成员口上建立 BFD 会话。

功能特性	缺省值

BFD 会话建立模式	主动模式，不可配置
BFD 检测模式	异步模式，不可配置
BFD 会话参数	没有缺省值，必须配置
BFD 支持与动态路由协议联动	关闭
BFD 支持与静态路由联动	关闭
BFD 支持与策略路由联动	关闭
BFD 支持与 VRRP 联动	关闭
BFD 支持与 VRRP+联动	关闭
BFD 支持 VRF	关闭

8.3.1 设置BFD会话参数

BFD 会话参数没有缺省值。必须配置 BFD 会话参数才能建立 BFD 会话。

命令	作用
Ruijie(config-if)# **bfd interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *interval-multiplier*	配置 BFD 参数在指定的接口。 interval *milliseconds*：最小发送间隔。单位毫秒。 min_rx *milliseconds*：最小接收间隔。单位毫秒。 multiplier interval-multiplier：检测超时倍数
Ruijie(config-if)# **no bfd interval**	删除 BFD 会话参数。

例：在 Routed Port 接口 FastEthernet 0/2 上配置 BFD 会话参数。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# interface fastEthernet 0/2
Ruijie(config-if)# bfd interval 100 min_rx 100 multiplier 3
```

建议 BFD 会话两端的参数配置一致，这样可以确保关联 BFD 应用协议同时生效，避免由于两端配置的抑制时间不同而出现转发路径单通的情况。

配置时设置的参数需要考虑不同接口传输上的带宽差异。如果设置最小发送间隔和最小接受间隔过小，可能导致 BFD 占用过大带宽而影响本身的数据传输。

8.3.2 设置BFD控制报文慢速定时器

命令	作用
Ruijie(config)# **bfd slow-timer** milliseconds	配置慢速定时器定时时间，缺省值为 1 秒。 取值范围：1000-30000，单位毫秒。
Ruijie(config)# **no bfd slow-time**	恢复慢速定时器的缺省值。

设置慢速定时器，以较慢的频率发送 BFD 控制报文。

例：配置慢速定时器时间为 1400 毫秒。

```
Ruijie# configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# bfd slow-timer 1400
```

8.3.3 设置BFD会话状态通告抑制时间

命令	作用
Ruijie(config)# **bfd up-dampening** *milliseconds*	配置 UP 状态稳定时间。
Ruijie(config)# **no bfd up-dampening**	恢复缺省值。

配置 BFD 会话状态通告抑制时间特性主要解决由于线路不稳定导致 BFD 会话在 DOWN 和 UP 状态之间频繁切换，从而引起关联的应用（比如静态路由）频繁的进行转发路径切换，影响业务的正常运行的问题。该特性允许用户配置通告给关联应用会话 UP 状态前所需 UP 状态稳定的时间。

例：配置为 BFD 会话状态抑制时间为 60，000 毫秒。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# interface fastEthernet 0/2
Ruijie(config-if)# bfd up-dampening 60000
```

8.3.4 启用BFD的保护策略

命令	作用
Ruijie(config)# **bfd cpp**	启用 BFD 的保护策略，缺省启用。
Ruijie(config)# **no bfd cpp**	关闭 BFD 的保护策略。

BFD 协议是非常敏感协议，如果所启用 BFD 功能的设备受到攻击（比如:大量 Ping 报文攻击设备）而发生 BFD 会话震荡，可以通过配置启用 BFD 的保护策略进行保护。但如果启用该设备 BFD 功能的同时打开该保护策略，会导致上一跳设备发出的 BFD 报文经过该设备时，该设备会将 BFD 报文丢弃，从而影响上一跳设备与其他设备的 BFD 会话建立。该功能及限制仅对交换机生效。

例：启用 BFD 的保护策略。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# bfd cpp
```

8.3.5 配置RIP与BFD联动

命令	作用
Ruijie(config-router)# **bfd all-interfaces**	所有接口允许 RIP 关联 BFD。
Ruijie(config-router)# **no bfd all-interfaces**	所有接口禁止 RIP 关联 BFD。
Ruijie(config-if)# **ip rip bfd**	指定接口允许 RIP 关联 BFD。
Ruijie(config-if)# **ip rip bfd disable**	指定接口禁止 RIP 关联 BFD。

RIP 协议周期性发送路由更新信息，当在指定时间内没有收到路由更新时，认为此条路由不再生效，这种方式不能快速响应链路故障。在 RIP 上启动 BFD 检测功能后，将会为 RIP 路由信息源(RIP 路由更新报文的源地址)建立 BFD 会话，一旦 BFD 检测到邻居失效，RIP 路由信息将直接进入失效状态，不再参与路由转发。收敛的时间可以从 180 秒(RIP 定时器的缺省配置情况下)降到 1 秒内。

使用 **show bfd neighbors** [**details**]命令检查 RIP 邻居之间建立了 BFD 会话，且与 RIP 联动。

例：配置 RIP 与 BFD 联动（允许除 FastEthernet 0/2 外所有接口）。

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# router rip
Ruijie(config-router)# bfd all-interfaces
Ruijie(config-router)# exit
Ruijie(config)# interface FastEthernet 0/2
Ruijie(config-if)# ip rip bfd disable
Ruijie(config-if)#end
```

- 运行 RIP 的两台设备的路由信息源(RIP 路由更新报文的源地址)必须在同一网段，才能在邻居之间建立 BFD 会话。
- 对于非 unnumbered 接口，如果邻居地址和本地地址不是直连地址，则无法建立 BFD 会话。
- 如果因 IP 选路而导致创建 BFD 会话时指定的接口和实际 BFD 报文出接口不一致，或创建 BFD 会话时指定的接口和实际 BFD 回来的报文入接口不一致，则无法建立 BFD 会话。
- 必须确保 BFD 会话参数已经配置，否则无法建立 BFD 会话。

8.3.6 配置静态路由与BFD联动

命令	作用
Ruijie(config)# **ip route static bfd** [**vrf** *vrf-name*] *interface-type interface-number gateway* [**souce** *ip-addess*]	配置 IPv4 静态路由与 BFD 联动。其中 *interface-type interface-number* 和 *gateway* 指邻居所在的接口及 IP。在多跳的情况下需要配置 **souce** *ip-addess* 作为会话的源 IP。
Ruijie(config)# **no ip route static bfd** [**vrf** *vrf-name*] *interface-type interface-number gateway* [**source** *ip-address*]	取消 IPv4 静态路由与 BFD 联动。

- 配置静态路由时，需要指定下一跳（或出接口）。配置静态路由与 BFD 联动时，也需要指定下一跳和出接口。必须确保两个命令中的下一跳和出接口一致，才能确保静态路由与 BFD 联动。

使用 **show bfd neighbors** [**details**] 命令检查静态路由出接口与下一跳之间建立了 BFD 会话，且与静态路由联动。

例：配置静态路由与 BFD 联动，通过 BFD 检测与 172.16.0.2 间的转发路径。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# interface FastEthernet 0/1
Ruijie(config-if)# no switchport
Ruijie(config-if)# ip address 172.16.0.1 255.255.255.0
```

```
Ruijie(config-if)# bfd interval 50 min_rx 50 multiplier 3
Ruijie(config-if)# ip route static bfd FastEthernet 0/1 172.16.0.2
Ruijie(config-if)# ip route 10.0.0.0 255.0.0.0 FastEthernet 0/1 172.16.0.2
Ruijie(config-if)# end
```

8.3.7 配置策略路由与BFD联动

命令	作用
Ruijie(config-route-map)# **set ip next-hop verify-availability** *next-hop-address* **bfd** [**vrf** *vrf-name*] *interface-type interface-number gateway*	配置策略路由与 BFD 联动，其中 *interface-type interface-number* 和 *gateway* 指邻居所在的接口及 IP。
Ruijie(config-route-map)# **no set ip next-hop verify-availability** [*next-hop-address* [**bfd** [**vrf** *vrf-name*] *interface-type interface-number gateway*]]	通过 **no** 命令删除该配置。

在配置 **set ip next-hop** 命令时携带 **verify-availability** 关键字，使通过此命令设置的策略路由与 BFD 联动。BFD 会话检测到故障，表示 **set ip next-hop** 命令指定的下一跳不可达。

使用 **show bfd neighbors** [**details**] 命令检查策略路由的出接口与下一跳之间建立了 BFD 会话，且与策略路由联动。

例：配置策略路由与 BFD 联动，通过 BFD 检测与 172.16.0.2 间的转发路径。

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# route-map Example1 permit 10
Ruijie(config-route-map)# match ip address 1
Ruijie(config-route-map)#set ip next-hop verify-availability 172.16.0.2 bfd FastEthernet 0/1 172.16.0.2
Ruijie(config-route-map)#end
Ruijie(config)#interface FastEthernet 0/1
Ruijie(config-if)#no switchport
Ruijie(config-if)#ip address 172.16.0.1 255.255.255.0
Ruijie(config-if)#bfd interval 50 min_rx 50 multiplier 3
Ruijie(config-if)#ip policy route-map Example1
Ruijie(config-if)#exit
```

8.3.8 配置VRRP与BFD联动

命令	作用
Ruijie(config-if)# **vrrp** *group-number* **bfd** *ip-address*	配置 VRRP 与 BFD 联动，ip-address 指定邻居 IP。
Ruijie(config-if)# **no vrrp** *group-number* **bfd**	关闭 VRRP 与 BFD 联动。
Ruijie(config-if)# **vrrp** *group-number* **track bfd** *interface-type interface-number ip-addess* [*priority*]	配置 VRRP 通过 BFD 跟踪指定邻居。
Ruijie(config-if)# **no vrrp** *group-number* **track bfd** *interface-type interface-number ip-addess*	通过 no 命令删除该配置。

使用 **show bfd neighbors** [**details**]命令检查 VRRP 成员口之间建立了 BFD 会话，且与 VRRP 联动。

VRRP+协议依赖于 VRRP。当配置完 VRRP 与 BFD 关联后，VRRP+也自动和 BFD 发生关联。

例：配置 VRRP 与 BFD 联动，通过 BFD 检测 VRRP 成员口是否活跃。

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#interface FastEthernet 0/1
Ruijie(config-if)#no switchport(路由器无需此配置)
Ruijie(config-if)#ip address 192.168.201.11 255.255.255.0
Ruijie(config-if)#bfd interval 50 min_rx 50 multiplier 3
Ruijie(config-if)#vrrp 1 priority 120
Ruijie(config-if)#vrrp 1 ip 192.168.201.1
Ruijie(config-if)#vrrp 1 bfd 192.168.201.12
Ruijie(config-if)#end
```

例：配置指定 VRRP 组通过 BFD 跟踪指定的邻居 192.168.1.3。

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#interface FastEthernet 0/1
Ruijie(config-if)#no switchport(路由器无需此配置)
Ruijie(config-if)#ip address 192.168.1.1 255.255.255.0
Ruijie(config-if)#bfd interval 50 min_rx 50 multiplier 3
Ruijie(config)#interface FastEthernet 0/2
Ruijie(config-if)#no switchport(路由器无需此配置)
Ruijie(config-if)#ip address 192.168.201.17 255.255.255.0
Ruijie(config-if)#vrrp 1 priority 120
Ruijie(config-if)#vrrp 1 ip 192.168.201.1
Ruijie(config-if)#vrrp 1 track bfd FastEthernet 0/1 192.168.1.3 30
Ruijie(config-if)#end
```

8.4 监视与维护

命令	作用
Ruijie# **show bfd neighbors** [**vrf** *vrf-name*] [**ipv4** *ip-addess* [**details**] | **client** { **rip** | **vrrp** | **vrrp-balance** | **static-route** | **pbr** } [**ipv4** *ip-addess* [**details**] | **ipv6** *ipv6-addess* [**details**] | **details**]]	显示 BFD 会话信息
Ruijie# **show vrrp**	显示 VRRP 与 BFD 联动信息
Ruijie# **show vrrp balance**	显示 VRRP+与 BFD 联动信息
Ruijie# **show route-map**	显示策略路由与 BFD 联动信息
Ruijie# **show ip route static bfd**	显示静态路由与 BFD 联动信息
Ruijie# **show ip rip peer**	显示 RIP 与 BFD 联动信息

8.5 配置举例

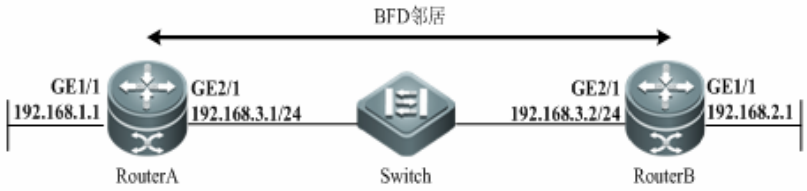
8.5.1 RIP与BFD联动

组网需求

Router A、Router B 通过二层交换机 switch 互连，在设备上运行 RIP 协议来建立路由，同时使能允许 RIP 在双方接口上关联 BFD 应用。在 Router B 和二层交换机 switch 之间的链路发生故障后，BFD 能够快速检测并通告 RIP 协议，触发协议快速收敛。

组网拓扑

图 8-4



配置要点

- 配置 RouterA

在 RouterA 配置 Routed Port 接口 ge2/1、接口 IP、接口的 BFD 会话参数

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# interface GigabitEthernet2/1
Ruijie(config-if)# no switchport(路由器无需此配置)
Ruijie(config-if)# ip address 192.168.3.1 255.255.255.0
Ruijie(config-if)# bfd interval 200 min_rx 200 multiplier 5
```

配置 Routed Port 接口 ge1/1

```
Ruijie(config-if)# exit
Ruijie(config)# interface GigabitEthernet1/1
Ruijie(config-if)# no switchport(路由器无需此配置)
Ruijie(config-if)# ip address 192.168.1.1 255.255.255.0
```

启用 RIP 协议并使能 RIP 协议关联 BFD 来检测 192.168.3.2 邻居

```
Ruijie(config-if)# exit
Ruijie(config)# router rip
Ruijie(config-router)# version 2
Ruijie(config-router)# network 192.168.3.0
```

```
Ruijie(config-router)# network 192.168.1.0
Ruijie(config-router)# passive-interface GigabitEthernet 2/1
Ruijie(config-router)# bfd all-interfaces
```

- 配置 RouterB

在 RouterB 配置 Routed Port 接口、接口 IP、接口的 BFD 会话参数

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# interface GigabitEthernet 2/1
Ruijie(config-if)# no switchport(路由器无需此配置)
Ruijie(config-if)# ip address 192.168.3.2 255.255.255.0
Ruijie(config-if)# bfd interval 50 min_rx 50 multiplier 3
```

配置 Routed Port 接口 ge1/1

```
Ruijie(config-if)# exit
Ruijie(config)# interface GigabitEthernet1/1
Ruijie(config-if)# no switchport(路由器无需此配置)
Ruijie(config-if)# ip address 192.168.2.1 255.255.255.0
```

启用 RIP 协议并使能 RIP 协议关联 BFD 来检测 192.168.3.1 邻居

```
Ruijie(config-if)# exit
Ruijie(config)# router rip
Ruijie(config-router)# version 2
Ruijie(config-router)# network 192.168.3.0
Ruijie(config-router)# network 192.168.2.0
Ruijie(config-router)# passive-interface GigabitEthernet 2/1
Ruijie(config-router)# bfd all-interfaces
Ruijie(config-router)# end
Ruijie#
```

显示验证

- 查看 RouterA BFD 会话建立情况

```
Ruijie# show bfd neighbors details
OurAddr        NeighAddr     LD/RD     RH/RS     Holdown(mult)      State     Int
192.168.3.1    192.168.3.2   1/2       Up        532 (3 )           Up        Ge2/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5
Received MinRxInt: 50000, Received Multiplier: 3
Holdown (hits): 600(22), Hello (hits): 200(84453)
Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332
Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196
Registered protocols: RIP
Uptime: 02:18:49
```

```
Last packet: Version: 1      - Diagnostic: 0
I Hear You bit: 1            - Demand bit: 0
Poll bit: 0                  - Final bit: 0
Multiplier: 3                - Length: 24
My Discr.: 2                 - Your Discr.: 1
Min tx interval: 50000       - Min rx interval: 50000
Min Echo interval: 0
```

字段	解释
OurAddr	会话本地的 IP 地址
NeighAddr	会话邻居的 IP 地址
LD/RD	会话本地和远端标识
RH/RS	会话对端当前状态
Holdown(mult)	会话本地未接收到 hello 报文的时间即会话超时检测次数
State	会话当前状态
Int	会话所在的接口号
Session state is UP and using echo function with 50 ms interval	会话是否采用 echo 模式以及 echo 的发帧时间间隔(该信息只有在工作在 Echo 情况下才会显示)
Local Diag	会话的诊断信息
Demand mode	会话查询模式是否激活
Poll bit	会话的配置是否修订
MinTxInt	会话本地配置的最小发送间隔
MinRxInt	会话本地配置的最小接收间隔
Multiplier	会话本地配置的超时检测次数
Received MinRxInt	会话远端配置的最小发送间隔
Received Multiplier	会话远端配置的超时检测次数
Holdown (hits)	会话检测时间及检测到超时的次数
Hello (hits)	会话协商后 hello 保文的接收最小间隔
Rx Count	会话本地接收到 BFD 报文的个数
Rx Interval (ms) min/max/avg	会话本地接收的最小间隔，最大间隔，平均间隔
Tx Count	会话本地发送到 BFD 报文的个数
Tx Interval (ms) min/max/avg	会话本地发送的最小间隔，最大间隔，平均间隔
Registered protocols	注册到该会话的应用协议类型
Uptime	会话保持 UP 的时间
Last packet	会话本地收到的最后一个 BFD 报文信息

- 查看 RouterB BFD 会话建立情况

```
Ruijie# show bfd neighbors details
OurAddr       NeighAddr     LD/RD     RH/RS     Holdown(mult)      State     Int
192.168.3.2   192.168.3.1   2/1       Up        532 (5 )           Up        Ge2/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3
Received MinRxInt: 200000, Received Multiplier: 5
Holdown (hits): 600(22), Hello (hits): 200(84453)
```

```
Rx Count: 49824, Rx Interval (ms) min/max/avg: 209/440/332
Tx Count: 84488, Tx Interval (ms) min/max/avg: 153/249/197
Registered protocols: RIP
Uptime: 02:18:49
Last packet: Version: 1      - Diagnostic: 0
I Hear You bit: 1            - Demand bit: 0
Poll bit: 0                  - Final bit: 0
Multiplier: 5                - Length: 24
My Discr.: 1                 - Your Discr.: 2
Min tx interval: 200000      - Min rx interval: 200000
Min Echo interval: 0
```

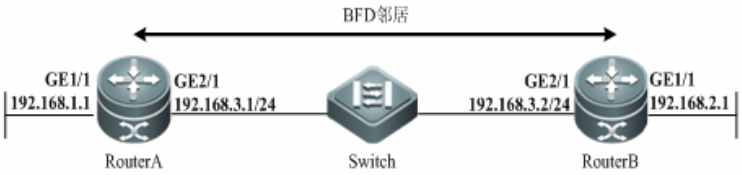
8.5.2 静态路由与BFD联动

组网需求

Router A、Router B 通过二层交换机 switch 互连，在设备上配置静态路由来建立转发，同时使能允许静态路由在双方接口上关联 BFD 应用。在 Router B 和二层交换机 switch 之间的链路发生故障后，BFD 能够快速检测并通告静态路由，触发系统将该静态路由从 RIB 中删除，从而避免选路错误。

组网拓扑

图 8-5



配置要点

- 配置 RouterA

#在 RouterA 配置 Routed Port 接口 ge2/1、接口 IP、接口的 BFD 会话参数

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# interface GigabitEthernet2/1
Ruijie(config-if)# no switchport(路由器无需此配置)
Ruijie(config-if)# ip address 192.168.3.1 255.255.255.0
Ruijie(config-if)# bfd interval 200 min_rx 200 multiplier 5
```

配置 Routed Port 接口 ge1/1

```
Ruijie(config-if)# exit
```

```
Ruijie(config)# interface GigabitEthernet1/1
Ruijie(config-if)# no switchport(路由器无需此配置)
Ruijie(config-if)# ip address 192.168.1.1 255.255.255.0
```

#配置静态路由并关联 BFD 来检测 192.168.3.2 邻居

```
Ruijie(config-if)# exit
Ruijie(config)# ip route static bfd GigabitEthernet 2/1 192.168.3.2
Ruijie(config)# ip route 192.168.2.0 255.255.255.0 GigabitEthernet 2/1 192.168.3.2
Ruijie(config)# end
Ruijie#
```

- 配置 RouterB

#在 RouterB 配置 Routed Port 接口、接口 IP、接口的 BFD 会话参数

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# interface GigabitEthernet 2/1
Ruijie(config-if)# no switchport(路由器无需此配置)
Ruijie(config-if)# ip address 192.168.3.2 255.255.255.0
Ruijie(config-if)# bfd interval 50 min_rx 50 multiplier 3
```

配置 Routed Port 接口 ge1/1

```
Ruijie(config-if)# exit
Ruijie(config)# interface GigabitEthernet1/1
Ruijie(config-if)# no switchport(路由器无需此配置)
Ruijie(config-if)# ip address 192.168.2.1 255.255.255.0
```

#配置静态路由并关联 BFD 来检测 192.168.3.1 邻居

```
Ruijie(config-if)# exit
Ruijie(config)# ip route static bfd GigabitEthernet 2/1 192.168.3.1
Ruijie(config)# ip route 192.168.1.0 255.255.255.0 GigabitEthernet 2/1 192.168.3.1
Ruijie(config)# end
Ruijie#
```

显示验证

- 查看 RouterA BFD 会话建立情况

```
Ruijie# show bfd neighbors details
OurAddr       NeighAddr     LD/RD     RH/RS     Holdown(mult)      State     Int
192.168.3.1   192.168.3.2   1/2       Up        532 (3 )           Up        Ge2/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5
Received MinRxInt: 50000, Received Multiplier: 3
Holdown (hits): 600(22), Hello (hits): 200(84453)
Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332
```

```
Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196
Registered protocols: STATIC ROUTE
Uptime: 02:18:49
Last packet: Version: 1     - Diagnostic: 0
I Hear You bit: 1           - Demand bit: 0
Poll bit: 0                 - Final bit: 0
Multiplier: 3               - Length: 24
My Discr.: 2                - Your Discr.: 1
Min tx interval: 50000      - Min rx interval: 50000
Min Echo interval: 0
```

- 查看 RouterB BFD 会话建立情况

```
Ruijie# show bfd neighbors details
OurAddr       NeighAddr     LD/RD    RH/RS    Holdown(mult)      State    Int
192.168.3.2   192.168.3.1   2/1      Up       532 (5 )           Up       Ge2/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3
Received MinRxInt: 200000, Received Multiplier: 5
Holdown (hits): 600(22), Hello (hits): 200(84453)
Rx Count: 49824, Rx Interval (ms) min/max/avg: 209/440/332 last: 66 ms ago
Tx Count: 84488, Tx Interval (ms) min/max/avg: 153/249/197 last: 190 ms ago
Registered protocols: STATIC ROUTE
Uptime: 02:18:49
Last packet: Version: 1     - Diagnostic: 0
I Hear You bit: 1           - Demand bit: 0
Poll bit: 0                 - Final bit: 0
Multiplier: 5               - Length: 24
My Discr.: 1                - Your Discr.: 2
Min tx interval: 200000     - Min rx interval: 200000
Min Echo interval: 0
```

8.5.3 策略路由与BFD联动

组网需求

Router A、Router B 通过二层交换机 switch 互连，在设备上配置策略路由来建立转发路径，同时使能允许策略路由在双方接口上关联 BFD 应用。在 Router B 和二层交换机 switch 之间的链路发生故障后，BFD 能够快速检测并通告策略路由，触发系统删除该策略路由，从而避免选路错误。

组网拓扑

图 8-6

配置要点

- 配置 RouterA

#在 RouterA 配置 Routed Port 接口 ge2/1、接口 IP、接口的 BFD 会话参数

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# interface GigabitEthernet2/1
Ruijie(config-if)# no switchport(路由器无需此配置)
Ruijie(config-if)# ip address 192.168.3.1 255.255.255.0
Ruijie(config-if)# bfd interval 200 min_rx 200 multiplier 5
```

配置 Routed Port 接口 ge1/1

```
Ruijie(config-if)# exit
Ruijie(config)# interface GigabitEthernet1/1
Ruijie(config-if)# no switchport(路由器无需此配置)
Ruijie(config-if)# ip address 192.168.1.1 255.255.255.0
```

#配置策略路由并关联 BFD 来检测 192.168.3.2 邻居

```
Ruijie(config)# ip access-list extended 100
Ruijie(config-ext-nacl)# permit ip any 192.168.2.0 0.0.0.255
Ruijie(config-ext-nacl)# deny ip any any
Ruijie(config-ext-nacl)# exit
Ruijie(config)# route-map Example1 permit 10
Ruijie(config-route-map)# match ip address 100
Ruijie(config-route-map)# set ip precedence priority
Ruijie(config-route-map)#set ip next-hop verify-availability 192.168.3.2 bfd GigabitEthernet 0/1 192.168.3.2
Ruijie(config)# end
Ruijie#
```

- 配置 RouterB

#在 RouterB 配置 Routed Port 接口、接口 IP、接口的 BFD 会话参数

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# interface GigabitEthernet 2/1
Ruijie(config-if)# no switchport(路由器无需此配置)
Ruijie(config-if)# ip address 192.168.3.2 255.255.255.0
Ruijie(config-if)# bfd interval 50 min_rx 50 multiplier 3
```

配置 Routed Port 接口 ge1/1

```
Ruijie(config-if)# exit
Ruijie(config)# interface GigabitEthernet1/1
Ruijie(config-if)# no switchport(路由器无需此配置)
Ruijie(config-if)# ip address 192.168.2.1 255.255.255.0
```

#配置策略路由并关联 BFD 来检测 192.168.3.1 邻居

```
Ruijie(config)# ip access-list extended 100
Ruijie(config-ext-nacl)# permit ip any 192.168.1.0 0.0.0.255
Ruijie(config-ext-nacl)# deny ip any any
Ruijie(config-ext-nacl)# exit
Ruijie(config)# route-map Example1 permit 10
Ruijie(config-route-map)# match ip address 100
Ruijie(config-route-map)# set ip precedence priority
Ruijie(config-route-map)#set ip next-hop verify-availability 192.168.3.1 bfd GigabitEthernet 2/1 192.168.3.1
Ruijie(config)# end
Ruijie#
```

显示验证

- 查看 RouterA BFD 会话建立情况

```
Ruijie# show bfd neighbors details
OurAddr       NeighAddr     LD/RD     RH/RS     Holdown(mult)      State     Int
192.168.3.1   192.168.3.2   1/2       Up        532 (3 )           Up        Ge2/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5
Received MinRxInt: 50000, Received Multiplier: 3
Holdown (hits): 600(22), Hello (hits): 200(84453)
Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332
Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196
Registered protocols: PBR
Uptime: 02:18:49
Last packet: Version: 1     - Diagnostic: 0
I Hear You bit: 1           - Demand bit: 0
Poll bit: 0                 - Final bit: 0
Multiplier: 3               - Length: 24
My Discr.: 2                - Your Discr.: 1
Min tx interval: 50000      - Min rx interval: 50000
Min Echo interval: 0
```

- 查看 RouterB BFD 会话建立情况

```
Ruijie# show bfd neighbors details
OurAddr       NeighAddr     LD/RD     RH/RS     Holdown(mult)      State     Int
192.168.3.2   192.168.3.1   2/1       Up        532 (5 )           Up        Ge2/1
```

```
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3
Received MinRxInt: 200000, Received Multiplier: 5
Holdown (hits): 600(22), Hello (hits): 200(84453)
Rx Count: 49824, Rx Interval (ms) min/max/avg: 209/440/332 last: 66 ms ago
Tx Count: 84488, Tx Interval (ms) min/max/avg: 153/249/197 last: 190 ms ago
Registered protocols: PBR
Uptime: 02:18:49
Last packet: Version: 1      - Diagnostic: 0
I Hear You bit: 1            - Demand bit: 0
Poll bit: 0                  - Final bit: 0
Multiplier: 5                - Length: 24
My Discr.: 1                 - Your Discr.: 2
Min tx interval: 200000      - Min rx interval: 200000
Min Echo interval: 0
```

8.5.4 VRRP与BFD联动

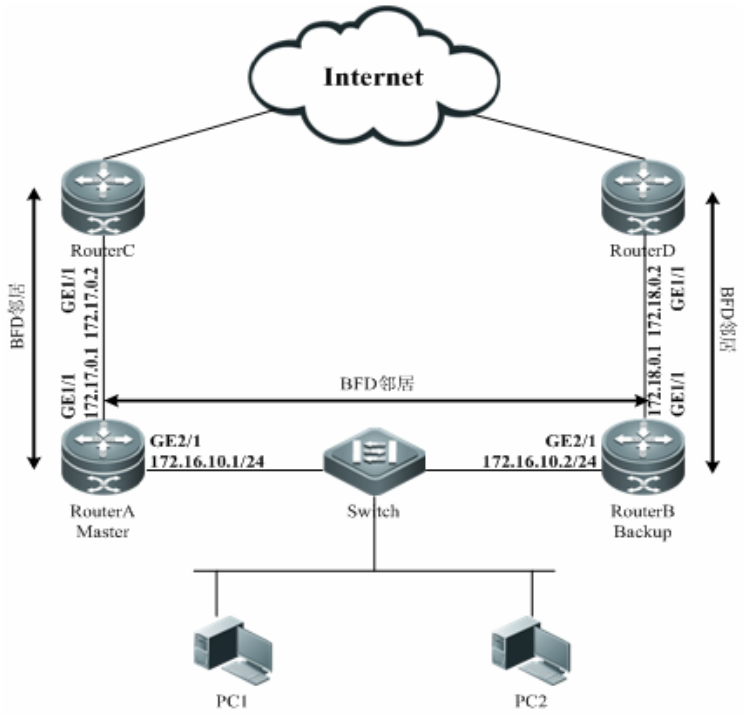
组网需求

Router A、Router B 通过二层交换机 switch 互连，在设备上配置 VRRP，同时使能允许 VRRP 在双方接口上关联 BFD 应用来检测主备路由器。在 Router A 和二层交换机 switch 之间的链路发生故障后，BFD 能够快速检测并通告 VRRP，触发 VRRP 主路由器降低优先级数额，引起主备切换，从而快速启用备份路由器。

Router A、Router B 分别通过 RouterC 和 RouterD 到达 Internet。RouterA 与 RouterC 之间以及 RouterB 与 RouterD 之间配置静态路由建立转发路径，同时也启用关联 BFD 来检测邻居。同时 Router A、Router B 设备上的 VRRP 还配置了通过与 BFD 联动来跟踪检测 RouterA 与 RouterC 和 RouterB 与 RouterD 之间转发路径，一旦检测失败将触发 VRRP 主路由器降低优先级数额，引起主备切换，从而快速启用备份路由器。

组网拓扑

图 8-7



配置要点

- 配置 RouterA

配置 Routed Port 接口、接口 IP、接口的 BFD 会话参数

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# interface GigabitEthernet2/1
Ruijie(config-if)# no switchport(路由器无需此配置)
Ruijie(config-if)# ip address 172.16.10.1 255.255.255.0
Ruijie(config-if)# bfd interval 200 min_rx 200 multiplier 5
```

配置 Routed Port 接口 ge1/1

```
Ruijie(config-if)# exit
Ruijie(config)# interface GigabitEthernet1/1
Ruijie(config-if)# no switchport(路由器无需此配置)
Ruijie(config-if)# ip address 172.17.0.1 255.255.255.0
Ruijie(config-if)# bfd interval 200 min_rx 200 multiplier 5
```

#启用 VRRP 协议并使能 VRRP 协议关联 BFD 来检测 172.16.10.2 邻居，同时启用 BFD 跟踪检测 172.17.0.2 邻居

```
Ruijie(config-if)# interface GigabitEthernet2/1
Ruijie(config-if)# vrrp 1 timers advertise 3
Ruijie(config-if)# vrrp 1 ip 172.16.10.3
Ruijie(config-if)# vrrp 1 priority 120
Ruijie(config-if)# vrrp 1 bfd 172.16.10.2
Ruijie(config-if)# vrrp 1 track bfd GigabitEthernet 1/1 172.17.0.2 30
```

#配置静态路由并关联 BFD 来检测 172.17.0.2 邻居

```
Ruijie(config-if)# exit
Ruijie(config)# ip route static bfd GigabitEthernet 1/1 172.17.0.2
Ruijie(config)# ip route 0.0.0.0 0.0.0.0 GigabitEthernet 1/1 172.17.0.2
Ruijie(config)# end
Ruijie#
```

- 配置 RouterB

#在 RouterB 配置 Routed Port 接口、接口 IP、接口的 BFD 会话参数

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# interface GigabitEthernet2/1
Ruijie(config-if)# no switchport(路由器无需此配置)
Ruijie(config-if)# ip address 172.16.10.2 255.255.255.0
Ruijie(config-if)# bfd interval 50 min_rx 50 multiplier 3
```

配置 Routed Port 接口 ge1/1

```
Ruijie(config-if)# exit
Ruijie(config)# interface GigabitEthernet1/1
Ruijie(config-if)# no switchport(路由器无需此配置)
Ruijie(config-if)# ip address 172.18.0.1 255.255.255.0
Ruijie(config-if)# bfd interval 200 min_rx 200 multiplier 5
```

#启用 VRRP 协议并使能 VRRP 协议关联 BFD 来检测 172.16.10.1 邻居，同时启用 BFD 跟踪检测 172.18.0.2 邻居

```
Ruijie(config-if)# interface GigabitEthernet2/1
Ruijie(config-if)# vrrp 1 timers advertise 3
Ruijie(config-if)# vrrp 1 ip 172.16.10.3
Ruijie(config-if)# vrrp 1 priority 90
Ruijie(config-if)# vrrp 1 bfd 172.16.10.1
Ruijie(config-if)# vrrp 1 track bfd GigabitEthernet 1/1 172.18.0.2 30
```

#配置静态路由并关联 BFD 来检测 172.18.0.2 邻居

```
Ruijie(config-if)# exit
Ruijie(config)# ip route static bfd GigabitEthernet 1/1 172.18.0.2
Ruijie(config)# ip route 0.0.0.0 0.0.0.0 GigabitEthernet 1/1 172.18.0.2
Ruijie(config)# end
Ruijie#
```

显示验证

- 查看 RouterA BFD 会话建立情况

```
Ruijie# show bfd neighbors details
OurAddr       NeighAddr     LD/RD     RH/RS     Holdown(mult)      State     Int
```

```
172.16.10.1   172.16.10.2   1/2      Up       532 (3 )          Up       Ge2/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5
Received MinRxInt: 50000, Received Multiplier: 3
Holdown (hits): 600(22), Hello (hits): 200(84453)
Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332
Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196
Registered protocols: VRRP
Uptime: 02:18:49
Last packet: Version: 1     - Diagnostic: 0
I Hear You bit: 1           - Demand bit: 0
Poll bit: 0                 - Final bit: 0
Multiplier: 3               - Length: 24
My Discr.: 2                - Your Discr.: 1
Min tx interval: 50000      - Min rx interval: 50000
Min Echo interval: 0

OurAddr       NeighAddr     LD/RD    RH   Holdown(mult)      State    Int
172.17.0.1    172.17.0.2    2/3      1    532 (3 )          Up       Ge2/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5
Received MinRxInt: 50000, Received Multiplier: 3
Holdown (hits): 600(22), Hello (hits): 200(84453)
Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332
Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196
Registered protocols: VRRP,STATIC ROUTE
Uptime: 02:18:49
Last packet: Version: 1     - Diagnostic: 0
I Hear You bit: 1           - Demand bit: 0
Poll bit: 0                 - Final bit: 0
Multiplier: 3               - Length: 24
My Discr.: 2                - Your Discr.: 1
Min tx interval: 50000      - Min rx interval: 50000
Min Echo interval: 0
```

查看 RouterB BFD 会话建立情况

```
Ruijie# show bfd neighbors details
OurAddr       NeighAddr     LD/RD    RH/RS    Holdown(mult)      State    Int
172.16.10.2   172.16.10.1   2/1      Up       532 (3 )          Up       Ge2/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3
Received MinRxInt: 200000, Received Multiplier: 5
Holdown (hits): 600(22), Hello (hits): 200(84453)
Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332 last: 68 ms ago
Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196 last: 192 ms ago
```

```
Registered protocols: VRRP
Uptime: 02:18:49
Last packet: Version: 1     - Diagnostic: 0
I Hear You bit: 1           - Demand bit: 0
Poll bit: 0                 - Final bit: 0
Multiplier: 3               - Length: 24
My Discr.: 1                - Your Discr.: 2
Min tx interval: 200000     - Min rx interval: 200000
Min Echo interval: 0

OurAddr       NeighAddr     LD/RD    RH/RS    Holdown(mult)      State    Int
172.18.0.1    172.18.0.2    1/3      Up       532 (3 )           Up       Ge2/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5
Received MinRxInt: 50000, Received Multiplier: 3
Holdown (hits): 600(22), Hello (hits): 200(84453)
Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332
Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196
Registered protocols: VRRP,STATIC ROUTE
Uptime: 02:18:49
Last packet: Version: 1     - Diagnostic: 0
I Hear You bit: 1           - Demand bit: 0
Poll bit: 0                 - Final bit: 0
Multiplier: 3               - Length: 24
My Discr.: 2                - Your Discr.: 1
Min tx interval: 50000      - Min rx interval: 50000
Min Echo interval: 0
```

9 Rns & track

9.1 概述

rns 是 ruijie network service 的缩写，rns 通过探测对端设备是否有响应报文发出，来监控端到端连接的完整性。利用 rns 的探测结果，用户可以对网络故障进行诊断和定位。目前锐捷实现了 icmp-echo 和 dns 两种探测类型。

为了提高通信的可靠性，一些应用模块需要及时跟踪接口链路状态或网络可达性。负责接口链路状态和网络可达性的监测模块与应用模块之间增加 track 模块，可以屏蔽不同监测模块的差异，简化应用模块的处理。一个 track 对象可以跟踪一个 IP 地址是否可达，也可以跟踪一个接口是否是 up 的。track 功能分离了要跟踪的对象和对这个对象状态感兴趣的模块，像 PBR(Policy Based Routing，策略路由)，VRRP(Virtual Router Redundancy Protocol，虚拟路由器冗余协议)。当 track 对象状态变化时，它们可以采取不同的动作。

9.2 配置rns

配置一个 rns 对象用来发送 icmp echo 报文。

命令	作用
Ruijie# **configure terminal**	进入全局配置模式
Ruijie(config)# **ip rns** *operation-number*	进入 ip rns 配置模式
Ruijie(config-ip-rns)# **icmp-echo** *destination-hostname* [**source-ipaddr** *ip-address*]	配置一个 ip rns 对象用来发送 icmp 报文

举例如下：

```
Ruijie> enable
Ruijie# configure terminal
Ruijie(config)# ip rns 1
Ruijie(config-ip-rns)# icmp-echo 10.1.1.1
```

显示 rns 对象的配置信息：

```
Ruijie# show ip rns configuration
Ip rns id:1
Type of operation to perform: icmp-echo
Target address/Source address:10.1.1.1/0.0.0.0
Operation timeout (milliseconds):1000
Vrf Name:
Operation frequency (milliseconds):1000
```

显示 rns 对象的统计信息：

```
Ruijie# show ip rns statistics
IP rns index    1
Number of successes:0
```

```
Number of failures:174
Round-trip min/avg/max = 0/0/0 ms
```

9.3 配置track

9.3.1 跟踪一个接口的链路状态

执行这个任务可以跟踪一个接口的链路状态。对于一个二层口，只要端口上电就认为是 up 的；对于三层口，只要三层口所包括的二层口有 up 的，就认为是 up；对于像 loopback 口这样的逻辑口，只要没有 shutdown 认为是 up 的。

配置步骤：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式
Ruijie(config)# **track** *object-number* **interface** *type number* **line-protocol**	跟踪一个接口的状态，并且进入 track 模式
Ruijie(config-track)# **delay** { **up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds* }	（可选）指定一段时间，当接口状态变化时，经过这段时间后才会改变 track 对象的状态，默认没有延迟。
Ruijie(config-track)# **show track** [*object-number*]	（可选）显示 track 对象的信息。可以使用这个命令来验证配置是否正确。

举例如下：

```
Ruijie> enable
Ruijie# configure terminal
Ruijie(config)# track 3 interface FastEthernet 1/0 line-protocol
Ruijie(config-track)# delay up 30
Ruijie(config-track)# show track 3
```

配置了一个 track 对象用来跟踪一个接口的状态，下面的例子显示了相关信息：

```
Ruijie# show track 3
Track 3
interface FastEthernet 1/0
The state is Up
1 change,current state last:11 secs
Delay up 10 secs,down 10 secs
```

9.3.2 跟踪一个rns对象的状态

我们用一个 track 对象来跟踪一个 rns 对象的状态，如果 rns 对象发送的报文有收到响应报文，则 track 对象状态为 up，相反 track 对象状态为 down。

> 当用 track 对象跟踪一个不存在的 rns 对象时，该 track 对象的状态是 up 的。

过程如下：

1) 配置一个 IP RNS 对象（略）

2) 配置一个 track 对象

3) 配置一个 route-map，应用上面的 track 对象

4) 在一个接口上应用策略路由

配置步骤：

命令	作用
Ruijie(config)# **track** *object-number* **rns** *entry-number*	跟踪一个 ip rns 对象的状态，并且进入 track 模式。
Ruijie(config-track)# **delay** { **up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds* }	（可选）指定一段时间，当 track 对象的状态变化时，经过这段时间后才会改变状态，默认没有延迟。
Ruijie(config-track)# **exit**	退到全局配置模式。
Ruijie(config)# **interface** *type number*	进入接口配置模式。
Ruijie(config-if)# **ip address** *ip-address* **mask** [*secondary*]	给接口配置一个 IP 地址。
Ruijie(config-if)# **ip policy route-map** *map-tag*	在这个接口上应用策略路由。
Ruijie(config-if)# **exit**	退到全局配置模式。
Ruijie(config)# **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]	配置一个 route-map。
Ruijie(config-route-map)# **set ip next-hop verify-availability** *next-hop-address* **track** *object*	设置下一跳，并使用 track 对象来跟踪。

举例如下：

```
Ruijie(config)# track 123 rns 1
Ruijie(config-track)# delay up 30
Ruijie(config-track)# exit
Ruijie(config)# interface ethernet 0
Ruijie(config-if)# ip address 10.1.1.11 255.0.0.0
Ruijie(config-if)# ip policy route-map alpha
Ruijie(config-if)# exit
Ruijie(config)# route-map alpha
Ruijie(config-route-map)# set ip next-hop verify-availability 10.1.1.1 10 track 123
```

显示 trackc 对象的状态：

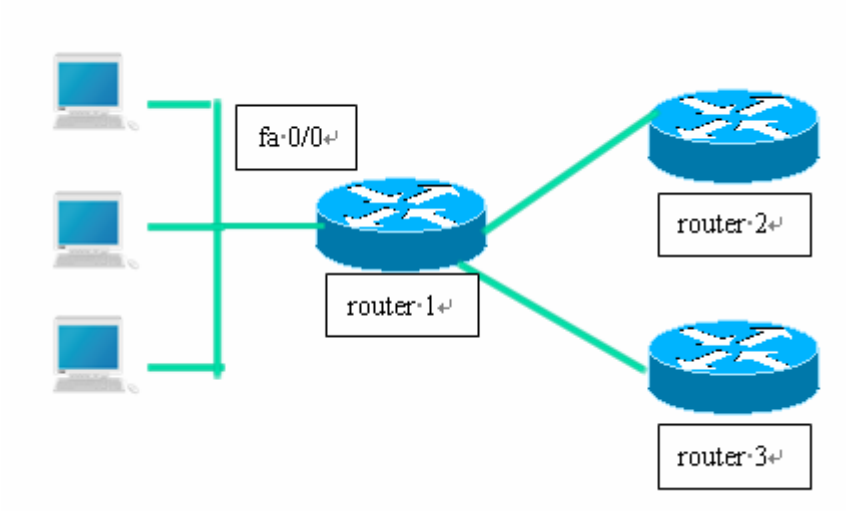
```
Track 2
Ruijie Network Service 1
The state is Down
1 change,current state last:7 secs
Delay up 30 secs,down 0 secs
```

9.4 配置举例

9.4.1 策略路由中的下一跳关联track对象

网络环境

图 9-1



实现策略路由：报文从 fa 0/0 口进来，当 IP 地址 10.1.1.1 可达时，报文的下一跳被设置为 10.1.1.1(router 2 的接口 IP 地址)。如果 10.1.1.1 不可达，报文的下一跳被设置为 10.2.2.2(router 3 的接口 IP 地址)。如果 10.2.2.2 也不可达,策略路由失败，根据查询核心路由表的结果,报文走普通路由。

配置要点

在策略路由中，配置策略路由中的下一跳关联一个 track 对象，当 track 对象状态为 down 时，该下一跳不生效。即策略路由不会用该下一跳来来设置报文的下一跳。

配置要点如下：

5) 配置 IP RNS 对象

6) 配置 track 对象

7) 配置 route-map，应用 track 对象。

8) 在接口上应用策略路由

配置步骤

Router1 的配置：

#定义两个 IP RNS 对象，用来跟踪远端的 IP 地址是否可达.

```
ip rns 1
icmp-echo 10.1.1.1
ip rns 2
icmp-echo 10.2.2.2
```

#定义 track 对象，用来跟踪 rns 对象的状态

```
track 123 rns 1
track 124 rns 2
```

#接口上应用策略路由

```
interface FastEthernet 0/0
ip address 10.4.4.4 255.255.255.0
ip policy route-map alpha
```

#10.1.1.1 是经过下面这个接口

```
interface fa 0/1
ip address 10.1.1.254 255.255.255.0
```

#10.2.2.2 是经过下面这个接口

```
interface fa 0/2
ip address 10.2.2.254 255.255.255.0
```

#定义一个 route-map，设置的下一跳是否可用，依赖于 track 对象的状态

```
route-map alpha
set ip next-hop verify-availability 10.1.1.1 track 123
set ip next-hop verify-availability 10.2.2.2 track 124
```

10 IP Event Dampening

10.1 概述

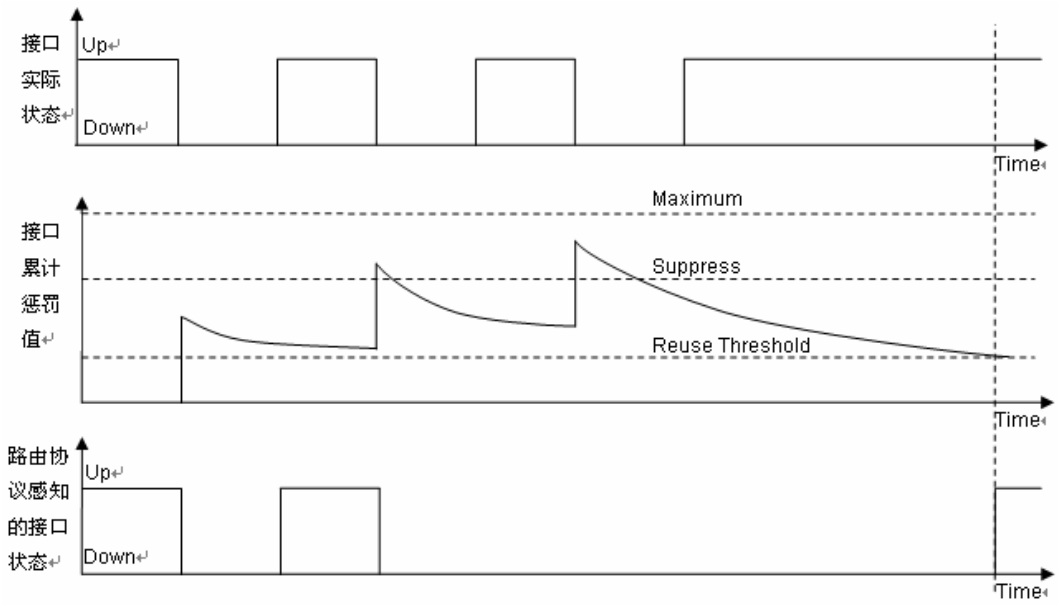
10.1.1 IP Event Dampening概述

对三层交换机，路由器来说，当三层网络接口状态频繁 UP/DOWN 变化时，会造成本设备上路由表的反复震荡。若配置了路由协议，那么路由协议还可能会将这一震荡扩散到整个网络中，造成路由协议的邻居反复的进行路由的更新和重新计算，不仅浪费网络的带宽，而且导致整个网络的不稳定。从设备本身的角度来说，反复的路由更新和计算需要消耗大量的 CPU 资源。这些都会影响客户网络的正常运行。

IP Event Dampening 功能提供了一种抑制接口震荡，避免上述带宽浪费和网络不稳定的方法。在三层接口上开启 IP Event Dampening 功能后，接口能够检测异常的 UP/DOWN 翻转，并自动的对接口状态频繁 UP/DOWN 进行抑制，使得从路由协议的角度看，这种异常行为的接口一直处于 DOWN 状态，从而使单点链路故障不会被路由协议扩散出去。当接口不再反复翻转恢复稳定后，抑制状态自动解除。通过配置 IP Event Dampening 功能，可以减少网络震荡，降低系统的 CPU 资源消耗，增强整网的稳定性。

10.1.2 接口状态变化事件

图 10-1 路由协议感知的接口状态事件



惩罚值（penalty）

IP Event Dampening 功能采用了一种对接口状态变化事件计算惩罚值的方式，对接口行为进行感知和控制。接口上每进行一次 up→down 翻转，惩罚值将会累加，接口稳定时，该惩罚值又会呈指数的递减。通过这种惩罚值计算，使得接口能智能的感知其自身的状态行为，进行相应的处理。

IP Event Dampening 采用的抑制算法核心与 RFC2439 所述的 BGP 路由翻转抑制算法一致。

抑制门限（Suppress Threshold）

为了识别接口震荡事件，为累计惩罚值设置一个门限，当累积惩罚值超过该门限时，认为该接口处于震荡状态，对接口实施抑制。

半衰期（Half-Life Period）

半衰期是指在接口稳定情况下惩罚值衰减到原来一半所需要的时间。它定义了惩罚值按指数衰减的速度，半衰期越短，衰减的越快，探测到接口稳定的速度越快，但震荡检测的灵敏度也越低。

解除抑制门限（Reuse Threshold）

当接口不再震荡，惩罚值衰减到一定程度（减少到抑制门限以下）时，可认为该接口恢复稳定状态，从而解除接口的抑制状态。

最大抑制时间（Maximum Suppress Time）

为避免接口长时间震荡后，惩罚值过大，导致过久不能恢复使用，算法定义了一个最大抑制时间，即无论接口震荡多久，接口被抑制的时间不会超过该最大抑制时间。

10.1.3 受影响的功能

当三层接口上未配置 dampening 功能，或配置了 dampening 功能但接口未被抑制时，路由协议或其他关心三层接口状态的协议都和正常情况下的行为一样。当接口上配置了 dampening 且接口被抑制时，上层协议认为接口状态为 down，这期间接口实质上的状态变化不会对路由表以及上层路由协议路由计算和通告造成影响，直到接口解除抑制为止。

10.2 配置IP Event Dampening

命令	作用
Ruijie(config-if)# **dampening** [*half-life-period* [*reuse-threshold suppress-threshold max-suppress* [**restart** [*restart-penalty*]]]]	在接口上开启 IP Event Dampening 功能。缺省关闭。 *half-life-period*，半衰期。缺省值 5 秒。 *reuse-threshold*，解除抑制门限。缺省值 1000。 *suppress-threshold*，抑制门限。缺省值 2000。 *max-suppress*，最大抑制时间。缺省值 20 秒。 **restart** *restart-penalty*，初始惩罚值。缺省值 2000。
Ruijie(config-if)# **no dampening**	在接口上关闭 IP Event Dampening 功能。

例：在交换机接口 FastEthernet 0/1 上开启 IP Event Dampening 功能，使用默认 dampening 参数。

```
Ruijie(config)# interface FastEthernet 0/1
Ruijie(config-if)# no switchport
Ruijie(config-if)# dampening
```

例：在交换机接口 FastEthernet 0/0 上开启 IP Event Dampening 功能，半衰期 30 秒，解除抑制门限 1500，开始抑制门限 10000，以及最长抑制时间为 120 秒。

```
Ruijie(config)# interface FastEthernet 0/0
Ruijie(config-if)# no switchport
Ruijie(config-if)# dampening 30 1500 10000 100
```

例：在交换机接口 FastEthernet 0/2 上开启 IP Event Dampening 功能，初始惩罚值为 500。

```
Ruijie(config)# interface FastEthernet 0/2
Ruijie(config-if)# no switchport
Ruijie(config-if)# dampening 5 500 1000 20 restart 500
```

10.3 监视与维护

命令	作用
Ruijie# **show dampening interface**	显示被 damening 的接口总的统计信息。
Ruijie# **show interfaces dampening**	显示所有接口的 dampening 详细信息。

例：显示接口抑制功能的概况。

```
Ruijie# show dampening interface
3 interfaces are configured with dampening.
No interface is being suppressed.
```

例：显示配置了 IP Event Dampening 功能的接口的 dampening 参数和状态信息。

```
Ruijie# show interfaces dampening
FastEthernet 0/1
Flaps  Penalty  Supp   ReuseTm  HalfL  ReuseV  SuppV  MaxSTm  MaxP   Restart
0      0        FALSE  0        5      1000    2000   20      16000  0
FastEthernet 0/2
Flaps  Penalty  Supp   ReuseTm  HalfL  ReuseV  SuppV  MaxSTm  MaxP   Restart
0      0        FALSE  0        5      1000    2000   20      16000  500
FastEthernet 0/3
Flaps  Penalty  Supp   ReuseTm  HalfL  ReuseV  SuppV  MaxSTm  MaxP   Restart

0      0        FALSE  0        5      1000    2000   20      16000  0
```

11 GRTD

11.1 概述

GRTD(Generic Real-Time Detections，通用实时检测)子系统提供一种实时故障检测功能。有了实时故障检测功能，用户可以在设备入网运行前或设备入网运行时检测设备是否存在硬件故障。

GRTD 提供四种硬件故障诊断方式：后台监控检测、系统启动自检、订制时间检测及 CLI 命令行检测。硬件检测功能主要检测系统管理链路及数据转发链路上各硬件组件是否正常，以确保系统在管理平面和数据转发平面无硬件故障。GRTD 的故障检测项分为影响系统正常运行的检测项及不影响系统正常运行的检测项：诸如端口环回测试、详尽的存储器测试等为影响系统正常运行的测试项；而 VSU 系统设备间通道测试等为不影响系统正常运行的检测项。

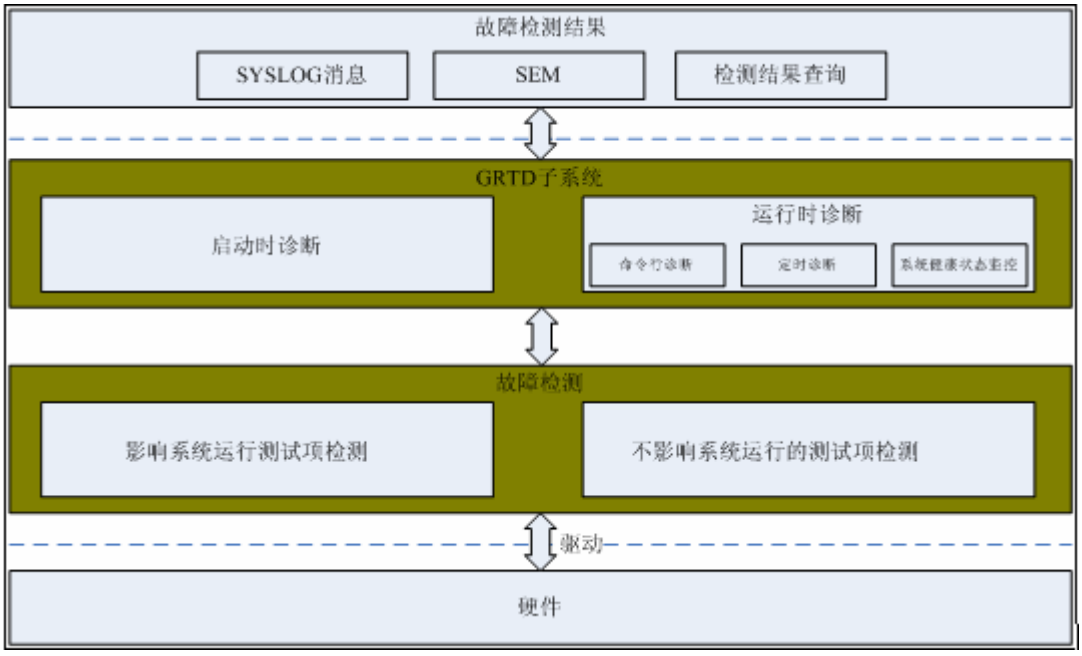
11.1.1 诊断范围

GRTD 可以检测以下几个方面问题：

- 各硬件组件
- 接口（以太网端口等）
- 连接器（VSU 系统设备间的连接器等）
- 存储器（内存、flash、芯片外挂存储器等）

11.1.2 工作原理

图 11-1 GRTD 框架图



由 GRTD 框架图中可以知道，GRTD 主要分三部分：

- 故障检测：根据设备硬件结构产生的具体检测项，主要分为影响系统正常运行检测项及不影响系统正常运行检测项。
- GRTD 子系统：检测功能核心模块，主要提供四种方式的检测功能。
- 故障检测结果：检测结果处理功能模块，主要用于故障检测结果的处理，包括产生 SYSLOG、与 SEM 模块的联动及结果查询。

GRTD 子系统提供四种检测方式：

- 启动时诊断：运行于系统初始化阶段，用于检测设备在使用前是否已经存在故障。
- 命令行诊断：利用 CLI 根据故障实行按需检测。
- 定时诊断：在用户指定时间进行检测项的检测。
- 监控检测：运行于系统后台，只有不影响系统正常运行的测试项能作为后台监控测试项。

实时诊断是网络高可靠性的要求之一，利用实时诊断降低设备异常给网络运行带来的一系列影响。网络高可靠性非常重要的一部分就是当设备在网络中运行时能实时检测硬件故障并根据硬件故障采取相应措施以降低硬件故障给网络带来的影响。GRTD 完成的就是这部分功能。

11.1.3 检测方式

GRTD 有以下四种检测方式。

启动自检

在设备初始化过程中对各硬件组件进行自检测试。启动自检分三个级别：最大限度自检测试、最小限度自检测试及不进行自检测试。最大限度自检测试与最小限度自检测试的区别在于参与启动自检测试的测试项数目不同，且最大限度自检测试包含最小限度自检测试。可以通过命令 **show diagnostic content** 命令查询哪些测试项参与最大限度自检测试，哪些测试项参与最小限度自检测试。比如执行 **show diagnostic content** 命令的现实结果如下：

```
PortLoopbackTest--------------->  MPDX*******  not config     N/A
MacSelfTest-------------------->  C*DX*******  not config     N/A
```

PortLoopbackTest 其中一个属性为 M，则表示它将参与最小限度启动自检测试；MacSelfTest 其中一个属性为 C，则表示它将参与最大限度启动自检测试。如果当前系统配置的启动自检测试等级为最大限度自检测试，则在系统初始化过程中会执行 PortLoopbackTest 和 MacSelfTest 两项检测；如果当前系统配置的启动自检测试等级为最小限度自检测试，则在系统初始化过程中只会执行 PortLoopbackTest 这一项检测。

命令行检测

命令行检测是指根据需要利用 CLI 对某一测试项进行测试。测试完后该测试项的检测结果需输入命令进行查询。

监控检测

监控检测运行于系统后台，所有不影响系统正常运行的测试项都可以作为监控测试项。监控测试项测试失败，可以设置产生 SYSLOG 消息。对于监控测试项，可以设置激活或禁止其监控测试，可以设置其监控时间间隔，可以设置该监控测试项持续测试失败的次数。

影响系统正常运行的测试不能作为监控测试，监控测试的最小时间间隔为 1 秒。

计划测试

计划测试指根据用户配置好的时间启动相应测试项的测试，支持三种测试时间配置：

- on: 某一明确时间点进行测试
- daily: 每天的某一时间点进行测试
- weekly: 每周中某一天的某一时间点进行测试

不能配置同一时间点的不同测试方式，如已经为某一测试项配置在某一天的 12:00 进行计划测试，则无法再为其设置 daily 12:00 测试计划表。

11.1.4 检测项

使用 **show diagnostic content** 命令查看 GRTD 支持的检测项。

支持的检测项如下。

```
******************************************************************
*Diagnostic test suite attributes:
M/C*/-Minimal bootup level test / Complete bootup level test / NA
P/V*/-Per port test / Per device test / NA
D/N*/-Disruptive test / Non-disruptive test / NA
  X*/-Not a health monitoring test / NA
  F*/-Fixed monitoring interval test / NA
  E*/-Always enabled monitoring test / NA
A/I*/-Monitoring in active / Monitoring in inactive / NA
Y/O*/-Key test / Non-key test / NA
  B*/-Basic ondemand test / NA
  R*/-Power-down line cards and need reload mainbord / NA
  K*/-Require resetting the line card after the test completed / NA
******************************************************************
                                          test interval  Thre-
ID   Test Name                    Attributes  day hh:mm:ss   shold
===  ============================  ==========  ============   ====
 1)  PortLoopbackTest------------->  MPDX*******  not config     N/A
 2)  MacSelfTest------------------->  C*DX*******  not config     N/A
 3)  TestCpld---------------------->  C*DX*******  not config     N/A
 4)  TestNandFlash----------------->  **DX*******  not config     N/A
 5)  TestNorFlash------------------->  **DX*******  not config     N/A
```

```
6)  TestI2C----------------------->  C*DX*******  not config     N/A
7)  TestPCI----------------------->  C*DX*******  not config     N/A
8)  TestDdr----------------------->  **DX****B**  not config     N/A
```

测试项属性	说明
M / C	参与最小限度启动自检测试 / 参与最大限度启动自检测试
P / V	端口级测试 / 设备级测试
D / N	影响系统正常运行的测试 / 不影响系统正常运行的测试
X	不能作为监控测试项
F	监控测试间隔固定的监控测试
E	监控检测状态总是激活的监控测试
A / I	监控检测状态为激活 / 监控检测状态为禁止
Y / O	关键测试 / 非关键测试
B	只用于命令行测试
R	检测项测试完后需要重启设备及 VSU 系统
K	检测项测试完后需要重启设备

下文将对各检测项进行详细说明。

端口环回帧交换测试(PortLoopbackTest)

端口环回帧交换测试是指对设备上端口先进行环回操作（自环头环回或设置芯片 MAC/PHY 环回），然后对该端口进行包交换测试。如果测试失败，需要检查相应的硬件是否存在故障。测试前需要先指定所要测试的端口 ID 及这些端口的环回模式，如果不指定，默认被测端口 ID 为该设备上的所有端口且这些端口都为 MAC 环回。

可先对端口进行自环头环回测试，如果测试成功则表明端口无硬件故障，如果测试失败，可设置端口为 PHY 环回再进行测试，此时如果测试通过，则说明 PHY 与 RJ45 间存在故障，如果测试失败，需要继续将端口设置为 MAC 环回进行测试，如果测试成功，则说明 MAC 与 PHY 间存在硬件故障，而如果测试还是失败，则 CPU 到 MAC 间的硬件链路存在故障。

主要应用场景举例：在实际使用设备过程中，如果出现端口不通故障，可以利用此检测功能初步判断端口是否存在硬件故障。

MAC 芯片自检测试(MacSelfTest)

MAC 芯片自检测试是指 MAC 芯片类型自检测试以及 MAC 芯片与 MAC 外置包缓存(如 SDRAM，SSRAM，TCAM)之间的通道是否正常，同时测试 MAC 外置包缓存是否正常。

主要应用场景举例：在实际使用设备过程中，可能出现数据包无法正常转发现象，这种情况下可以利用此功能初步检测是否 PCI 总线对 MAC 芯片读写存在故障及对于存在外扩存储器的 MAC 芯片其对外扩存储器的读写访问是否正常。

对于不带外扩存储器的 MAC 芯片自检测试不会影响设备的正常运行，但如果 MAC 芯片带有外扩存储器，则此测试会导致数据包无法正常转发。

CPLD 自检测试(TestCpld)

主要测试 CPU 与 CPLD 之间的通道是否正常，即测试 CPU 是否能正常访问 CPLD。如果测试失败，说明 CPU 与 CPLD 间通道异常，可能导致 CPU 与 CPLD 间无法正常交互，以致 CPLD 的功能无法正常实现，如指示灯显示异常等故障。

主要应用场景举例：在实际使用设备过程中，如果发现设备指示灯异常，设备无法正常重启等现象，可以利用此功能初步定位 CPLD 是否存在故障。

由于在对 CPLD 进行测试时，会对 CPLD 的寄存器进行读写操作，所以可能导致 CPLD 功能异常。

PCI/PCIE 总线自检测试(TestPCI)

用于检测 PCI 和 PCIE 总线上的故障。PCI/PCIE 总线自检测试失败，可能导致挂接在 PCI/PCIE 总线上的器件信息无法读取，带外、带内数据通道异常等。

主要应用场景举例：在实际使用设备过程中，如果出现总线扫描不到设备，总线奇偶检验错误、PCIE 没有办法 Link 等现象，可以利用此功能初步定位 PCI/PCIE 总线是否存在故障。

串行 flash 检测(TestNandFlash)

主要用于检测串行 flash 是否存在故障。flash 故障检测包含两个方面内容：一是 flash 数据线和地址线的检测；二是 flash 内部存储空间的扫描测试。一般在测试 flash 时会先进行数据线与地址线的测试。由于 flash 内部存储空间测试通常需要花费很长时间，目前实现不支持 flash 全部空间的扫描测试。

并行 flash 检测(TestNorFlash)

主要用于检测并行 flash 是否存在故障。

在执行并行 flash 测试时，不允许设备掉电，如果设备掉电，可能导致并行 flash 中保存的信息丢失。

I2C 自检测试(TestI2C)

用于检测 I2C 总线上的故障。I2C 如果测试失败，可能导致挂接在 I2C 上的器件信息无法正常读取，比如温度，光模块信息等无法正常读取。

主要应用场景举例：在实际使用设备过程中，如果出现温度无法读取，光模块信息无法获取，监控模块的信息无法获取等现象，可以利用此功能初步定位 I2C 总线是否存在故障。

对于 BOX 设备的 I2C 测试，在利用命令行进行检测时需要先确认扩展插槽上是否插有扩展模块，如果插槽上没有插扩展模块，测试将失败。

内存测试(TestDdr)

用于检测内存数据线及地址线、内存内部空间读写是否存在故障。

主要应用场景举例：设备无法启动或设备无故异常重启，需要排除是否由于内存硬件故障导致。

由于内存测试需要重启设备，故内存测试只能进行单独的 CLI 测试，如果将内存测试设置为计划测试或者与其余测试项一起进行 CLI 测试，内存测试将被略过，此时可以通过命令 `show diagnostic event` 查看。而且内存测试是在

BOOT 中执行的，在进行内存测试前需确认 BOOT 版本是否支持内存测试。如果 BOOT 版本不支持内存测试，该功能将失效，请将 BOOT 版本升级到支持内存测试的版本，而如果 BOOT 为双 BOOT，当内存测试重启时如果设备从从 BOOT 启动，也不进行内存测试。

```
Diagnostic events <storage for 500 events, 27 events recorded>
Event Type (ET): I - Info, W - Warning, E - Error
Time Stamp           ET  Slot  Event Message
-------------------  --  ----  --------------------------
2010-08-27 09:03:24  I   1/0   Diagnostic Pass
2010-08-27 09:49:02  I   1/0   PortLoopbackTest Pass
2010-08-27 09:49:02  I   1/0   MacSelfTest Pass
2010-08-27 09:49:02  E   1/0   TestCpld Fail
2010-08-27 09:49:02  I   1/0   TestNandFlash Pass
2010-08-27 09:49:04  I   1/0   TestNorFlash Pass
2010-08-27 09:49:04  I   1/0   TestI2C Pass
2010-08-27 09:49:04  I   1/0   TestPCI Pass
2010-08-27 09:49:04  I   1/0   TestDdr Escape
```

11.1.5 检测结果处理

GRTD 提供命令行查询所有测试项的检测结果。检测结果有以下三种处理方式：

- 如果测试项测试失败，产生 SYSLOG 消息。主要用于监控测试，可以配置是否需要产生该消息。
- 产生测试事件，总测试事件条数可配置。测试事件有三种类型：
  info：测试信息，通常为测试通过。
  warning：警告信息，测试执行超时及监控测试错误时产生警告信息。
  error：出错信息，除了监控测试项外的其余检测项测试错误时产生错误信息。

目前所有检测项都是针对硬件进行的检测，一旦检测到故障，说明某硬件组件存在问题，详细维修手段请咨询锐捷技术支持工程师。

- 检测项结果与 SEM 的联动
  severity-major 级别：目前支持的测试项检测到错误都为 severity-major 级别。
  severity-minor 级别：目前版本测试项暂无此错误级别。
  severity-normal 级别：目前版本测试项暂无此错误级别。

11.2 配置GRTD

本节命令中，仅在 VSU 系统下支持 slot 参数。

功能特性	缺省值
GRTD 启动自检测试等级	minimal: 最小限度自检测试
GRTD 计划测试时间配置	无
GRTD 监控测试激活配置	根据测试项不同默认值不同，目前 ping 测试为默认激活。

GRTD 监控时间间隔配置	根据测试项不同默认值不同，目前 ping 测试默认间隔为 30 秒。
GRTD 监控测试 SYSLOG 配置	默认监控测试失败产生 SYSLOG。
GRTD 监控测试失败持续次数配置	默认为 10 次
诊断事件记录条数	默认为 500 条

11.2.1 配置GRTD启动自检测试等级

GRTD 启动自检测试等级默认为 minimal，可以配置为 complete、minimal 及 bypass，complete 为执行最大限度的启动自检测试，minimal 为执行最小限度的启动自检测试，bypass 为不执行启动自检测试。配置步骤如下：

命令	作用
Ruijie# **configure terminal**	进入全局模式
Ruijie(config)# **diagnostic bootup level { complete | minimal | bypass }**	配置启动自检测试等级

如果要恢复 GRTD 默认启动自检测试等级，在全局模式下使用 **no diagnostic bootup level** 命令进行设置。

例：配置 GRTD 启动自检测试为最大限度自检测试。

```
Ruijie#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#diagnostic bootup level complete
```

配置完后可以通过命令 **show diagnostid bootup level** 命令查看配置结果，这个配置对系统上所有设备都起作用，且当前配置只能在系统下次复位启动时生效。由于该配置会被写进系统环境变量，因此在配置文件丢失情况下其默认值为环境变量中记录的值（并不是 minimal）

```
Ruijie#show diagnostic bootup level
Current bootup diagnostic level: complete
```

11.2.2 配置GRTD命令行测试

命令行诊断指利用 CLI 执行某个或某些测试项，由于部分测试项执行后会影响其它测试项的执行结果，故命令行检测需要注意测试项测试顺序问题，比如必须在存储器测试前进行通道测试。

命令行测试必须严格遵循如下测试顺序：

1) 先执行不影响系统正常运行的测试项，可以通过命令 **show diagnostic content** 获取测试项的属性。

2) 执行端口环回测试、通道测试等这一类测试，这一类测试项属于影响系统正常运行的测试项，但不会对其后续的测试项测试结果产生影响。

3) 执行 PCI/PCIE 等总线测试、CPLD 测试、MAC 自检测试等。

4) 最后执行详尽的存储器测试。

执行详尽存储器测试后，需要复位对应的设备。不能在没有进行复位操作后直接进行其余测试项的测试。

命令	作用

Ruijie# **diagnostic start** [**slot** *slot_id* [**sub_sysytem** *subsys_id*]] **test** { **all** | **range** *test_range* | *test_id* }	开始测试
Ruijie# **diagnostic stop** [**slot** slot_id [**sub_sysytem** *subsys_id*]]	结束测试
Ruijie# **show diagnostic result** [**slot** *slot_id* [**sub_sysytem** *subsys_id*]] [**test** { **all** | **range** *test_range* | *test_id* }]	查询测试结果

例：VSU 系统下，对设备 1 执行命令行测试

```
Ruijie# diagnostic start slot 1 test range 4,5  //开始测试
Ruijie# diagnostic stop slot 1  //结束测试
Ruijie# show diagnostic result slot 1 test all  //查询测试结果
Current bootup diagnostic level: complete
Overall Diagnostic Result for Module 1: PASS
Test result: (P = Pass, F = Fail, U = Untested)
Switch#sho dia re sl 1/0 t a
Current bootup diagnostic level: minimal
Overall Diagnostic Result for Module: PASS
Test result: (P = Pass, F = Fail, U = Untested)
 1) PortLoopbackTest(loop mode: Mac):
    slot 0 port    1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
                   P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P
                  26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48
                   P  P  P  P  P  P  P  P  P  P  P  P  P  P  U  P  P  P  P  U  U  U  U
 2) MacSelfTest-------------------------------------> U
 3) TestCpld----------------------------------------> U
 4) TestNandFlash-----------------------------------> U
 5) TestNorFlash------------------------------------> U
 6) TestI2C-----------------------------------------> U
 7) TestPCI-----------------------------------------> U
 8) TestDdr-----------------------------------------> U
```

11.2.3 配置GRTD计划测试

可以为测试项设置某一特定时间点、每天的某一特定时间点或每周某一天的某一特定时间点进行测试。配置步骤如下：

命令	作用
Ruijie# **configure terminal**	进入全局模式
Ruijie(config)# **diagnostic schedule** [**slot** *slot_id* [**sub_sysytem** *subsys_id*]] **test** { **all** | **range** *test_range* | *test_id* } { **daily** *hh:mm* | **on year** *month day_of_month hh:mm* | **weekly** *day_of_week hh:mm* }	配置计划测试时间。

如果需要删除已经配置的测试计划时间，在全局模式下使用 **no diagnostic schedule** 命令进行设置。

例：VSU 系统下，对设备 1 所有测试项配置在每天的 12:00 进行测试。

```
Ruijie#config terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#diagnostic schedule slot 1 test all daily 12:00
Scheduling test(s) [1 2 3 6 ] may disrupt normal system operation
```

配置完后可以利用 **show diagnostic schedule** 命令显示设置结果

```
Ruijie#*May  4 18:04:57: %SYS-5-CONFIG_I: Configured from console by console
Ruijie#show diagnostic schedule slot 1
Schedule #1:
    To be run on daily 12:0
    Test ID(s) to be executed : 1 2 3 4 5 6
```

删除测试项 1、2 在每天 12:00 的测试计划

```
Ruijie#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#no diagnostic schedule slot 1 test range 1,2 daily 12:00
```

显示设置结果

```
Ruijie#*May  4 18:04:57: %SYS-5-CONFIG_I: Configured from console by console
Ruijie#show diagnostic schedule slot 1
Schedule #1:
    To be run on daily 12:0
    Test ID(s) to be executed : 3 4 5 6
```

一旦已经配置了某一时间点的测试计划，就不能再配置同一时间点其它方式的测试计划，如:

```
Ruijie#show diagnostic schedule slot 1
Schedule #1:
To be run on daily 12:00
Test ID(s) to be executed : 3 4 5 6
Ruijie#
Ruijie#configure terminal
Ruijie(config)# diagnostic schedule slot 1 test all on 2010 5 20 12:00
Schedule time (12:00) is conflict
Ruijie(config)#
```

11.2.4 激活GRTD监控测试

对于某一监控测试项，可以激活或禁止其监控测试状态。

命令	作用
Ruijie# **configure terminal**	进入全局模式
Ruijie(config)# **diagnostic monitor active**	激活监控测试
Ruijie(config)# **diagnostic monitor active** [**slot** *slot_id* [**sub_sysytem** *subsys_id*]] **test** { **all** | **range** *test_range* | *test_id* }	激活某些监控测试项

如果需要禁止某些测试项的监控测试，在全局模式下使用 **no diagnostic monitor active** 命令进行设置。

例：VSU 系统下，激活设备 1 所有测试项的监控测试。

```
Ruijie#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#diagnostic monitor active slot 1 test all
The test[1] can not be used as health monitoring test
The test[2] can not be used as health monitoring test
The test[3] can not be used as health monitoring test
The test[6] can not be used as health monitoring test
```

测试项能否作为监控测试项，可以通过 **show diagnostic content** 命令查询。比如执行 **show diagnostic content** 命令的显示结果如下：

```
OutbandSelfTest--------->  M**D*********  not config     NA
InbandSelfTest---------->  C**D*********  not config     NA
InBandChannelTest------>  ***N*********  0    00:00:10   10
```

只要测试项带有属性 D，则表示该测试项为影响系统正常运行的测试项，不能作为监控测试项。而如果测试项其中一个属性为 N，则表示该测试项可以作为监控测试项。

11.2.5 配置GRTD监控测试时间间隔

配置监控测试时间间隔需要执行如下命令：

命令	作用
Ruijie# **configure terminal**	进入全局模式
Ruijie(config)# **diagnostic monitor interval**	进入设置监控测试时间间隔
Ruijie(config)# **diagnostic monitor interval** [**slot** *slot_id* [**sub_sysytem** *subsys_id*]] **test** { **all** | **range** *test_range* | *test_id* } *hh:mm:ss* ***day*** *day_count*	设置监控测试时间间隔

对于有默认监控时间间隔的测试项，如果需要恢复默认的监控间隔，可以在全局模式下使用 **no diagnostic monitor interval** 进行设置。

例：VSU 系统下，为设备 1 所有测试项设置监控测试时间间隔为 10 秒。

```
Ruijie#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#diagnostic monitor interval slot 1 test all 00:00:10 day 0
The test[1] can not be used as health monitoring test
The test[2] can not be used as health monitoring test
The test[3] can not be used as health monitoring test
The test[6] can not be used as health monitoring test
```

监控测试的监控时间间隔最小单位为秒，但可以设置监控间隔为 0，当监控测试项的监控间隔为 0 时，该测试项将无法进行监控测试。

11.2.6 配置GRTD监控测试最大持续失败次数

监控测试最大持续失败次数是指当某监控测试项测试失败次数达到这个最大值后，将不再进行监控测试。

命令	作用
Ruijie# **configure terminal**	进入全局模式
Ruijie(config)# **diagnostic monitor threshold**	进入设置监控测试最大持续测试失败次数
Ruijie(config)# **diagnostic monitor threshold** [**slot** *slot_id* [**sub_sysytem** *subsys_id*]] **test** { **all** | **range** *test_range* | *test_id* } **failure-count** *threshold_value*	设置监控测试最大持续测试失败次数

对于有默认监控测试最大持续测试失败次数的测试项，如果需要恢复默认的最大持续测试失败次数，可以在全局模式下使用 **no diagnostic monitor threshold** 进行设置。

例：VSU 系统下，为设备 1 所有测试项设置监控测试最大持续测试失败次数为 6 次。

```
Ruijie#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#diagnostic monitor threshold slot 1 test all failure-count 6
The test[1] can not be used as health monitoring test
The test[2] can not be used as health monitoring test
The test[3] can not be used as health monitoring test
The test[6] can not be used as health monitoring test
```

监控测试最大持续测试失败次数最小为 1，最大为 99。

11.2.7 配置GRTD监控测试SYSLOG

指当监控测试失败时是否产生 SYSLOG 信息。

命令	作用
Ruijie# **configure terminal**	进入全局模式
Ruijie(config)#**diagnostic monitor syslog**	设置监控测试失败时产生 SYSLOG 消息。

当需要取消该 SYSLOG 消息时，在全局模式下使用 **no diagnostic monitor syslog** 命令进行取消。

11.2.8 配置GRTD诊断事件记录条数

配置诊断事件记录条数。

命令	作用
Ruijie# **configure terminal**	进入全局模式
Ruijie(config)# **diagnostic event-log size** *size_value*	配置诊断记录条数，范围 1 到 1000。

当需要恢复默认诊断事件记录条数时，在全局模式下使用 **no diagnostic event-log size** 命令完成。

11.3 配置举例

11.3.1 启动自检测试等级举例

配置要点

配置后系统上所有启动自检测试等级都为配置的值。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# diagnostic bootup level complete
```

显示验证

```
Ruijie# show diagnostic bootup level
Current bootup diagnostic level: complete
```

11.3.2 配置监控测试举例

配置要点

如果需要开始某项监控测试，需先配置好该监控测试项的监控测试时间间隔和最大监控测试持续失败次数后激活该监控测试项。只有不影响系统正常运行的测试项能作为监控测试项。

1) VSU 系统下，显示设备 1 所有测试项信息，用以确认哪些测试项为不影响系统正常运行的测试项。

```
Ruijie# show diagnostic content slot 1
============================================================================
*Diagnostic test suite attributes:
M/C*/-Minimal bootup level test / Complete bootup level test / NA
P/V*/-Per port test / Per device test / NA
D/N*/-Disruptive test / Non-disruptive test / NA
  X*/-Not a health monitoring test / NA
  F*/-Fixed monitoring interval test / NA
  E*/-Always enabled monitoring test / NA
A/I*/-Monitoring in active / Monitoring in inactive / NA
Y/O*/-Key test / Non-key test / NA
  B*/-Basic ondemand test / NA
  R*/-Power-down line cards and need reload mainbord / NA
  K*/-Require resetting the line card after the test completed / NA
============================================================================
                                              test interval  Thre-
ID   Test Name                       Attributes  day hh:mm:ss   shold
```

```
===  ============================  ==========  ============   ====
 1)  InBandChannelTest------------>  **N*F*I****  0    00:00:30   10
 2)  OutBandChannelTest----------->  **N*F*I****  0    00:00:30   10
 3)  OutbandSelfTest-------------->  **DX*******  not config     N/A
 4)  InbandSelfTest--------------->  **DX*******  not config     N/A
 5)  MacSelfTest------------------->  C*DX*******  not config     N/A
 6)  TestCpld---------------------->  C*DX*******  not config     N/A
 7)  TestNandFlash----------------->  **DX*******  not config     N/A
 8)  TestNorFlash------------------>  **DX*******  not config     N/A
 9)  TestI2C----------------------->  C*DX*******  not config     N/A
10)  TestPCI----------------------->  C*DX*******  not config     N/A
11)  TestDdr----------------------->  **DX****B**  not config     N/A
```

2) 1 和 2 测试项为不影响系统正常运行的测试项，为 1、2 项设置监控测试时间间隔及最大持续失败次数（如果想更方便的操作，也可以为所有测试项设置监控测试时间间隔及最大持续失败次数，如果是影响系统运行的测试项，会提示这些测试项不能作为监控测试，当然也不会进行相应的设置）。

```
Ruijie(config)# diagnostic monitor interval slot 1 test range 1,2 00:00:20 day 0
The test[1] is used as fixed interval test
The test[2] is used as fixed interval test
Ruijie(config)# diagnostic monitor threshold slot 1 test range 1,2 failure-count 6
Ruijie(config)# diagnostic monitor active slot 1 test range 1,2
```

3) 配置监控测试失败时产生 SYSLOG。

```
Ruijie(config)# diagnostic monitor syslog
```

显示验证

```
Ruijie# show diagnostic content slot 1
=============================================================================
*Diagnostic test suite attributes:
M/C*/-Minimal bootup level test / Complete bootup level test / NA
P/V*/-Per port test / Per device test / NA
D/N*/-Disruptive test / Non-disruptive test / NA
  X*/-Not a health monitoring test / NA
  F*/-Fixed monitoring interval test / NA
  E*/-Always enabled monitoring test / NA
A/I*/-Monitoring in active / Monitoring in inactive / NA
Y/O*/-Key test / Non-key test / NA
  B*/-Basic ondemand test / NA
  R*/-Power-down line cards and need reload mainbord / NA
  K*/-Require resetting the line card after the test completed / NA
=============================================================================
                                              test interval  Thre-
ID   Test Name                       Attributes  day hh:mm:ss   shold
===  ============================  ==========  ============   ====
```

```
 1)  InBandChannelTest------------->  **N*F*I****  0   00:00:30   6
 2)  OutBandChannelTest------------>  **N*F*I****  0   00:00:30   6
 3)  OutbandSelfTest--------------->  **DX*******  not config    N/A
 4)  InbandSelfTest---------------->  **DX*******  not config    N/A
 5)  MacSelfTest------------------->  C*DX*******  not config    N/A
 6)  TestCpld---------------------->  C*DX*******  not config    N/A
 7)  TestNandFlash----------------->  **DX*******  not config    N/A
 8)  TestNorFlash------------------>  **DX*******  not config    N/A
 9)  TestI2C----------------------->  C*DX*******  not config    N/A
10)  TestPCI----------------------->  C*DX*******  not config    N/A
11)  TestDdr----------------------->  **DX****B**  not config    N/A
```

11.3.3 命令行测试举例

测试要点

需严格按照如下顺序进行命令行测试：

1) 进行命令行测试前先禁止所有后台监控测试及删除所有计划测试。

2) 先执行不影响系统正常运行的测试项，可以通过命令 **show diagnostic content** 获取所有测试项的属性。

3) 执行端口环回测试、通道测试等这一类测试，这一类测试项属于影响系统正常运行的测试项，但不会对其后续的测试项测试结果产生影响。

4) 执行 PCI/PCIE 等总线测试、CPLD 测试、MAC 自检测试等。

5) 最后执行详尽的存储器测试。

```
Ruijie#show diagnostic content
******************************************************************
*Diagnostic test suite attributes:
M/C*/-Minimal bootup level test / Complete bootup level test / NA
P/V*/-Per port test / Per device test / NA
D/N*/-Disruptive test / Non-disruptive test / NA
  X*/-Not a health monitoring test / NA
  F*/-Fixed monitoring interval test / NA
  E*/-Always enabled monitoring test / NA
A/I*/-Monitoring in active / Monitoring in inactive / NA
Y/O*/-Key test / Non-key test / NA
  B*/-Basic ondemand test / NA
  R*/-Power-down line cards and need reload mainbord / NA
  K*/-Require resetting the line card after the test completed / NA
******************************************************************
                                              test interval  Thre-
ID   Test Name                      Attributes  day hh:mm:ss   shold
===  ============================  ==========  ============   ====
```

```
1)  PortLoopbackTest-------------->  MPDX*******  not config     N/A
2)  MacSelfTest------------------->  C*DX*******  not config     N/A
3)  TestNandFlash----------------->  **DX*******  not config     N/A
4)  TestNorFlash------------------>  **DX*******  not config     N/A
5)  TestI2C----------------------->  C*DX*******  not config     N/A
6)  TestPCI----------------------->  C*DX*******  not config     N/A
7)  TestDdr----------------------->  **DX****B**  not config     N/A
```

先测试不影响系统正常运行的测试项

```
Ruijie#diagnostic start test all
Running test[7] may reload system
Running test(s) [1 2 3 4 5 6] may disrupt normal system operation
Do you want to continue? [no]:y
Ruijie#*Oct  8 12:53:34: %GRTD-6-TEST_RUNNING: Running PortLoopbackTest{ID=1}...
*Oct  8 12:53:35: %GRTD-6-TEST_OK:  PortLoopbackTest{ID=1} completed successfully.
*Oct  8 12:53:35: %GRTD-6-TEST_RUNNING: Running MacSelfTest{ID=2}...
*Oct  8 12:53:35: %GRTD-6-TEST_OK:  MacSelfTest{ID=2} completed successfully.
*Oct  8 12:53:35: %GRTD-6-TEST_RUNNING: Running TestNandFlash{ID=3}...
*Oct  8 12:53:35: %GRTD-6-TEST_OK:  TestNandFlash{ID=3} completed successfully.
*Oct  8 12:53:35: %GRTD-6-TEST_RUNNING: Running TestNorFlash{ID=4}...
*Oct  8 12:53:38: %GRTD-6-TEST_OK:  TestNorFlash{ID=4} completed successfully.
*Oct  8 12:53:38: %GRTD-6-TEST_RUNNING: Running TestI2C{ID=5}...
*Oct  8 12:53:38: %GRTD-3-TEST_ERR:  TestI2C{ID=5} completed error.
*Oct  8 12:53:38: %GRTD-6-TEST_RUNNING: Running TestPCI{ID=6}...
*Oct  8 12:53:38: %GRTD-6-TEST_OK:  TestPCI{ID=6} completed successfully.
*Oct  8 12:53:38: %GRTD-5-TEST_ESCAPE: Ddr test should be done alone.
```

显示验证

```
Ruijie#show diagnostic result test all
Current bootup diagnostic level: complete
Overall Diagnostic Result for Module: FAIL
Test result: (P = Pass, F = Fail, U = Untested)
 1) PortLoopbackTest(loop mode: Mac):
    slot 0 port    1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
                   P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P
                  25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48
                   P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P
 2) MacSelfTest------------------------------------> P
 3) TestNandFlash----------------------------------> P
 4) TestNorFlash-----------------------------------> P
 5) TestI2C----------------------------------------> F
 6) TestPCI----------------------------------------> P
 7) TestDdr----------------------------------------> U
```

对于较为耗时的检测，可以使用命令 **show diagnostic status** 查看当前系统的检测状态。

11.3.4 配置计划测试时间表举例

配置要点

一旦已经配置了某一时间点的测试计划，就不能再配置同一时间点其它方式的测试计划，因此需要注意测试计划时间是否冲突。如果是某一特定时间点的计划测试，还需要确认年月日是合法的。

- VSU 系统下，设备 1 所有测试项配置每天 12:00 进行计划测试。

```
Ruijie(config)#diagnostic schedule slot 1 test all daily 12:00
Scheduling test(s) [1 2 3 6] may disrupt normal system operation
Ruijie(config)#
```

- VSU 系统下，设备 1 所有测试项配置每周星期三 3:00 进行计划测试。

```
Ruijie(config)#diagnostic schedule slot 1 test all weekly  Wednesday 3:00
Scheduling test(s) [1 2 3 6] may disrupt normal system operation
```

- VSU 系统下，设备 1 所有测试项配置在 2010 年 8 月 1 号 00:00 进行计划测试

```
Ruijie(config)#diagnostic schedule slot 1 test all on 2010  August 1 00:00
Scheduling test(s) [1 2 3 6] may disrupt normal system operation
```

显示验证

```
Ruijie#show diagnostic schedule slot 1
Diagnostic for 1:
Schedule #1:
    To be run on daily 12:00
    Test ID(s) to be executed : 1 2 3 4 5 6
Schedule #2:
    To be run on August 1 2010 00:00
    Test ID(s) to be executed : 1 2 3 4 5 6
Schedule #3:
    To be run on Wednesday 03:00
    Test ID(s) to be executed : 1 2 3 4 5 6
```

12 SEM

12.1 概述

SEM(Smart Embedded Manager,智能嵌入管理器) 是一种网络管理工具。它内嵌于设备，可以独立部署，通过用户命令配置，而不依赖外部网管，这样使其非常容易部署。

传统的外部网络管理，必须通过网络连接到设备，再进行管理。一旦网络出现故障而影响到网络连接，则外部网管将失去作用。而 SEM 内嵌于设备，无论在任何情况下都可以直接对设备进行管理，对网络以及设备出现的各种故障进行及时的处理或者捕捉到关键信息。

SEM 实时检测用户配置的事件，当事件发生时，采取预先设定的行动，整个过程高度可定制。为用户提供故障检测与处理，自动化管理等手段，提高了设备及网络的可用性。

SEM 的事件种类丰富，可以是设备发生的关键事件，比如设备的关键告警 Syslog，关键 Trap，时间点。也可以是用户输入的操作，比如用户输入的 CLI 命令，用户的 SNMP 操作。还可以是设备的运行计数超过阈值，比如接口统计计数，snmp 对象值，系统资源统计。SEM 同样支持众多的行动，支持命令行执行所有的用户命令，支持发送日志，支持主动复位设备等。

12.1.1 基本概念

事件

用户关心的事件，由用户配置，附属于策略，可以是一个也可以是多个。每种事件都由特定的检测器负责检测。当事件条件符合时，由事件检测器触发事件。比如，用户需要检测到特权模式下包含 **shutdown** 的命令，需要使用命令 **event tag** *example* **cli pattern** *shutdown* **mode** *exec* 配置事件给命令行事件检测器。

行动

用户在事件发生以后所要采取的行动，由用户配置，附属于策略，可以是一个也可以是多个。每种行动都对应不同的行动配置。当策略的事件发生以后，策略依次运行行动。比如，用户在某事件发生以后，需要重新启动设备，需要使用命令 **action** *example* **reload**。

策略

组织事件与事件、事件与行动的关系。需要在配置好以后提交策略配置，当策略的事件符合预定规则时触发策略，并依次运行策略的行动。

事件检测器

嵌入到具体的业务中，按照用户的配置监控业务，并在业务运行至符合用户配置的时候触发事件。将事件消息通知给智能管理服务器。

智能管理服务器

接收事件检测器的事件通知，并根据事件发生情况判断是否触发策略运行。一旦策略被触发，由智能管理服务器运行策略管理中的策略。

策略管理器

管理 SEM 的策略信息，并在策略被智能管理服务器触发以后，运行策略中的行动。

SEM 环境变量

在 SEM 运行过程中被策略行动所使用的变量。SEM 中环境变量有三种：

- 全局变量
- 系统局部变量
- 用户局部变量

在策略中使用变量时，“$”符号往后直到第一个不是字母、数字或下划线的字符之间的单词符号作为要被置换的变量的名字。全局变量可以在所有策略中使用。系统局部变量和用户局部变量都是局部变量，只能在具体的策略中使用，系统局部变量是只读类型，不可以被改写。用户局部变量在策略运行过程中被策略中的行动定义。所以系统局部变量一般以“_”开头，防止与用户局部变量冲突。

SEM 特定应用事件

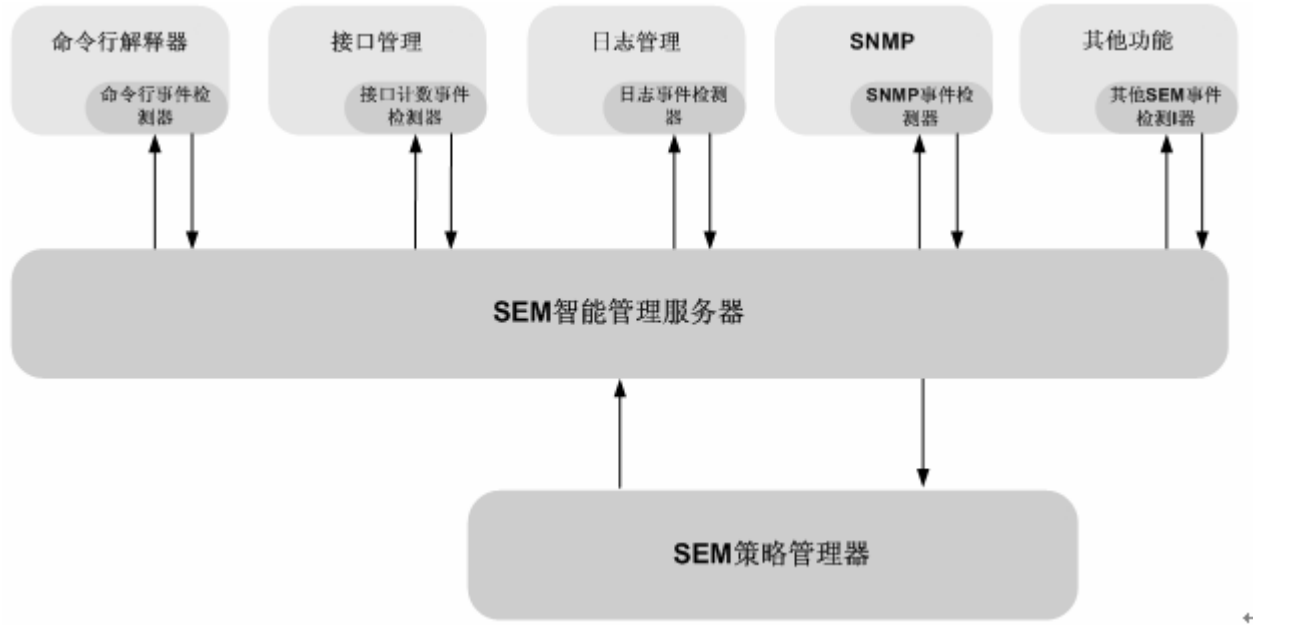
SEM 支持 SEM 系统内部使用特定应用事件，用于执行中的策略触发其他策略运行。为了方便区别不同的特定应用事件，使用子集和类型作为事件的标示。SEM 特定应用事件由特定应用事件检测器按照子集和类型进行检测，由策略运行中的特定应用事件行动项发布特定应用事件。当有策略行动发布了某子集和类型的特定应用事件时，正在检测的对应的子集和类型的事件被触发。举例见《SEM 典型配置举例章》中《SEM 检测特定应用事件》节。

SEM 命名计数器

SEM 支持一种 SEM 系统内部使用的命名计数器，由 SEM 计数事件检测器检测 SEM 命名计数器的变化，由策略运行中的 SEM 计数器行动项操作 SEM 命名计数器的值。SEM 命名计数器可以用于策略触发累计，数值统计等多种情况。举例见《SEM 典型配置举例章》中《SEM 检测计数器》节。

12.1.2 工作原理

图 12-1 SEM 结构图



SEM 提供了各种不同的事件检测器，这些事件检测器被嵌入到各种不同的业务中，实时的监控业务运行。检测器根据用户配置产生事件的条件与业务运行事件进行匹配，一旦匹配则事件检测器通知智能管理服务器事件发生。

智能管理服务器根据策略中的事件配置判断事件是否可以触发策略运行，当事件发生达到策略触发条件时，智能管理服务器运行策略管理器中的策略。

策略管理器中的策略按照用户的配置被依次运行预定的行动。

12.1.3 SEM支持的事件检测器

SEM 支持丰富的事件检测器，各种事件检测器嵌入到各个业务中。在业务运行过程中进行检测，决定事件是否发生。目前支持的检测器类型如下：

命令行事件检测器

命令行事件检测器检测用户的命令行输入。进行检测的用户命令行必须为通过命令行格式检查。将用户输入的命令的扩展形式进行正则匹配。一旦匹配通过，则触发命令行事件。命令行事件触发时支持两种等待模式：

- 同步模式：命令行事件被触发以后，命令行进入同步等待，等待策略运行结束。策略执行结束以后，由策略的执行结果决定用户输入的命令是否执行。
- 异步模式：命令行事件被触发后，不必等待策略运行结束。该模式下支持忽略命令执行的配置。当配置忽略时，命令行在触发完命令行事件以后，忽略对命令的执行。

计数事件检测器

计数事件检测器检测 SEM 内部的命名计数器，当命令计数器超过指定的阈值时触发计数器事件。当计数器事件被触发以后，该计数器事件检测将暂时失效，直到计数器达到其恢复阈值时其检测功能才可恢复。命名计数器的值由运行中的计数器行动改变，因此可以由其他策略将计数器的数值累加，当达到阈值后，计数器事件触发，计数器事件触发策略运行，在本策略运行过程中将计数器的值重置，以此达到循环的效果。

特定应用事件检测器

特定应用事件检测器检测 SEM 内部的特定应用事件，SEM 的内部事件由运行过程中的特定应用事件行动发布。当 SEM 发布的特定应用事件与当前特定应用事件的子集和类型相同，则特定应用事件触发。

接口计数事件检测器

接口计数事件检测器检测设备的接口统计计数。通过定期的采集和统计，判断接口的计数是否超过阈值，当接口统计超过阈值以后，接口计数事件被触发。当接口计数事件被触发以后，该接口计数事件检测将暂时失效，直到接口技术达到其恢复阈值时或者失效时间超过其恢复周期以后，其检测功能才能恢复。

空事件检测器

空事件检测器并非进行实际的检测，而是由 SEM 的 **smart manager run** 命令主动触发。该命令的参数为包含空事件的策略的名字。当该命令被执行成功以后，对应策略的空事件被触发。空事件被触发时支持两种等待模式：

- 同步模式：空事件被触发以后，命令行进入同步等待，待策略运行结束以后才能释放。
- 异步模式：空事件被触发以后直接释放，不进行等待。

热插拔事件检测器

在 VSU 系统下，热插拔事件检测器检测成员设备的插拔，当有成员设备插拔操作时热插拔事件触发。热插拔事件检测器支持两种事件种类：

- 插入
- 拔出

SNMP 事件检测器

SNMP 事件检测器分为以下 3 种类型：

- SNMP MIB 检测器：获取并统计检测设备的 SNMP MIB 对象值，当有 SNMP MIB 对象值超过事件设定阈值以后，SNMP MIB 事件被触发。当 SNMP MIB 事件被触发以后，该 SNMP MIB 事件检测器将暂时失效，直到 SNMP MIB 对象值达到其恢复阈值或者失效事件超过了事件的恢复周期以后，其检测功能才能恢复。
- SNMP Trap 检测器：检测 SNMP Trap 信息，当有 SNMP Trap 符合事件配置时，SNMP 事件触发。
- SNMP Object 检测器： 检测 SNMP 操作，当有 SNMP 操作符合事件配置时，SNMP 事件触发。SNMP Object 检测器支持同步和异步两种等待模式。并可以与 SNMP Object 行动配合完成自定义的 SNMP 回复。

Syslog 事件检测器

Syslog 事件检测器检测设备的日志信息，对设备发生的日志信息进行正则匹配，如果日志正则匹配通过，则 Syslog 事件触发。

定时器事件检测器

定时器事件检测器检测与时间有关的事件。主要有以下 4 种类型：

- 绝对时间定时器事件：定时器时间为未来某一时刻，当该时刻到达时，定时器事件触发。
- 倒计时定时器事件：定时器时间为从策略生效起的秒数，当到达该秒数时，定时器事件触发。
- 看门狗定时器事件：定时器时间为在策略生效起每经过设定的秒数，每当这些时刻到达时，就触发定时器事件一次。
- cron 定时器事件：cron (来源于希腊单词 chronos，意为“时间”)，广泛应用于 Unix 类操作系统中，用于设置周期性被执行的指令。SEM 支持 cron 方式的时间检测，当 cron 定时器事件 cron 串所描述的时间点到达时，定时器事件触发。

看门狗系统事件检测器

看门狗系统事件检测器检测设备的系统资源。当系统或任务的资源使用超过事件设定的阈值时，看门狗系统事件触发。目前支持的系统资源检测项目有如下：

- 设备的 CPU 资源
- 任务的 CPU 资源
- 设备的内存使用
- 设备的内存剩余
- 任务的内存使用

CPP 事件检测器

CPP 事件检测器检测检测 CPP（CPU Protect）功能的统计信息，当 CPP 的统计信息超过事件设定的阈值时，CPP 事件触发。CPP 事件检测器支持各种不同类型的报文检测：ARP，DHCP，IGMP，PIM，OSPF 等等。同时支持检测报文 pps，报文总数，报文丢弃数量。

GRTD 事件检测器

GRTD 事件检测器检测 GRTD（Generic Real-Time Diagnostics，通用实时诊断）发生的诊断结果，针对硬件相关组件以及组件间通信通道进行检测。当 GRTD 检测到的故障与事件设定的事件匹配时，GRTD 事件触发。

12.1.4 SEM支持的策略行动项

SEM 支持丰富的行动类型，在事件触发策略以后运行。可以执行收集信息和纠正设备或网络的问题，SEM 目前支持的行动项类型如下：

- 执行 CLI 命令：执行用户设定的命令。
- 发送 Syslog：发生指定的日志消息。
- 操作命名计数器：操作 SEM 内部的命名计数器。

- 切换至备份引擎：多设备进行主备倒换。
- 复位设备：将设备复位。
- 触发特定应用事件：发布 SEM 内部的特定应用事件。
- 使策略执行等待：使策略执行过程中等待一段时间。

12.1.5 SEM支持的环境变量

SEM 可以在策略中使用环境变量，SEM 支持如下类型的一下类型的环境变量：

- **全局变量**：定义以后可以在所有的策略中使用，由 **smart manager environment** 命令定义。在策略中只能读取全局变量的值。
- **局部变量**：策略运行过程中产生，分为系统局部变量和用户局部变量。系统局部变量由检测器创建，用于描述发生的事件，所以为只读类型，不可被改变。用户局部变量由策略的行动创建，运行过程中可以被修改。

在策略中局部变量的优先级大于全局变量的优先级。读取不存在的局部变量和全局变量或者修改只读局部变量将会产生错误。设置不存在的局部变量将会自动生成用户局部变量。

12.1.6 SEM智能管理服务器管理

SEM 智能管理服务器为用户提供管理接口，用户可以查看 SEM 运行信息，并做出管理。用户可以查看 SEM 的各种信息，主要包括：

- 查看目前支持的检测器的种类。
- 查看智能管理服务器的版本和各个事件检测器的版本。
- 查看用户配置并提交的策略。
- 查看正在执行的策略。
- 查看未被执行的策略。
- 查看历史产生的事件。
- 查看当前定义的计数器。
- 查看当前定义的 SEM 全局变量。

用户可以在 SEM 智能管理服务器运行过程中，对运行中的策略进行管理，可以做如下操作：

- 挂起和恢复整个 SEM 策略的调度的运行。
- 暂停和恢复特定的策略或者指定类别的策略。
- 调整指定类别的调度优先级。
- 强制中止特定策略，制定类别或者所有策略的执行。

12.2 配置SEM

在设备上使用 SEM 需要一定的前提，大部分前提都是因为策略行动的执行需要，如下：

- 配置 Syslog 行动项之前需要通过 **logging** 命令打开 Syslog 功能。
- 配置切换至备份引擎行动之前设备需要配备正常运行的备份引擎。

配置 SEM 可能涉及到各种检测器，各种行动和策略本身的配置。还有需要使用的环境变量。

12.2.1 创建策略

命令	作用
Ruijie# **configure terminal**	进入全局模式
Ruijie(config)# **smart manager applet** *applet-name* [**class** *class-options*]	创建策略并进入 SEM 配置模式，*applet-name* 参数制定策略的名字，class 参数指定策略的类别（默认为 default 类别）

如果要删除策略，在全局模式下使用 **no smart manager applet** *applet-name* 命令进行设置。

例：在设备上配置名为 policy_a 的策略，创建好策略以后，将进入 SEM 配置模式。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# smart manager applet policy_a
Ruijie(sem-applet)#
```

新创建和正在被修改的策略不会立即生效，需要在配置好事件和行动以后，由 **commit** 命令提交才能正式生效，未提交的策略配置可以通过 **rollback** 命令回退。

一个完整的策略包括事件和行动，如果策略没有配置事件，则提交过程中将会导致错误，提交不成功。如果策略没有配置行动，提交会成功，但是会给与提示，一旦策略被触发运行，则什么都不做，直接结束。

12.2.2 配置事件

命令	作用
Ruijie# **configure terminal**	进入全局模式
Ruijie(config)# **smart manager applet** *applet-name* [**class** *class-options*]	进入 SEM 配置模式，*applet-name* 参数制定策略的名字，class 参数指定策略的类别（默认为 default 类别）
Ruijie(sem-applet)# **event tag event-name** [**correlate** { **andnot | and | or** }] **syslog pattern** *regular-expression* [**priority** *priority-level*] [**occurs** *num-occurrences*] [**period** *period-value*] [**skip** { **yes | no** }]	每种事件检测都对应一个 event 命令，此处以 syslog 事件为例，介绍配置事件的方法。

如果要删除策略，在 SEM 配置模式下使用 **no event tag** *event-name* 命令进行设置。

例：为名为 policy_a 的策略配置名为 event_a 的 syslog 事件，检测内容包含“shutdown”的日志

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# smart manager applet policy_a
Ruijie(sem-applet)# event tag event_a syslog pattern "shutdown"
```

如果不配置事件就提交策略配置，则策略不会被注册，依然处于编辑状态。

一个策略中可以配置多个事件，事件的顺序按照策略的 tag 参数字符排序进行排列。

12.2.3 配置行动

命令	作用
Ruijie# **configure terminal**	进入全局模式
Ruijie(config)# **smart manager applet** *applet-name* [**class** *class-options*]	进入 SEM 配置模式，*applet-name* 参数制定策略的名字，class 参数指定策略的类别（默认为 default 类别）
Ruijie(sem-applet)# **action** *label* **syslog** [**priority** *priority-level*] **msg** *msg-text* **facility** *string*	每种行动都对应一个 action 命令，此处以 syslog 行动为例，介绍配置行动的方法。

如果要删除策略，在 SEM 配置模式下使用 **no action** *label* 命令进行设置。

例：为名为 policy_a 的策略配置名为 action_a 的 syslog 行动，发送级别为 6 的日志 action running。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# smart manager applet policy_a
Ruijie(sem-applet)# action label syslog priority 6 msg "action running"
```

如果不配置行动就提交策略配置，策略依然可以被注册，但是当策略被触发时将什么都不运行。

一个策略一般会配置多个行动，当策略被触发运行时，行动按照行动的 label 参数的字母排序顺序执行。

对于 cli 行动项，如果要保存命令的输入和输出，那么需要执行 **policy record** 命令，具体参见命令参考，相关的命令还包括 **smart manager policy record** 缺省情况下是不保存。

12.2.4 配置描述

命令	作用
Ruijie# **configure terminal**	进入全局模式
Ruijie(config)# **smart manager applet** *applet-name* [**class** *class-options*]	进入 SEM 配置模式，*applet-name* 参数制定策略的名字，class 参数指定策略的类别（默认为 default 类别）
Ruijie(sem-applet)# **description** *string*	设置描述信息

如果要删除策略描述信息，在 SEM 配置模式下使用 no **description** 命令进行设置。

例：为名为 policy_a 的策略配置描述信息，信息内容为“policy_for_test”。

```
Ruijie# configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# smart manager applet policy_a
Ruijie(sem-applet)# description "policy_for_test"
```

对描述信息的修改将立即生效，无须提交。

12.2.5 配置触发参数

命令	作用
Ruijie# **configure terminal**	进入全局模式
Ruijie(config)# **smart manager applet** *applet-name* [**class** *class-options*]	进入 SEM 配置模式，*applet-name* 参数制定策略的名字，class 参数指定策略的类别（默认为 default 类别）
Ruijie(sem-applet)# **trigger** [**occurs-value** *occurs-value*] [**occurs-period** *occurs-period-value*] [**correlate-start** *period-start-value*] [**correlate-period** *correlate-period-value*] [**delay** *delay-value*] [**maxrun** *maxruntime-number*]	设置策略触发参数

如果要恢复策略触发参数为默认，在 SEM 配置模式下使用 **no trigger** 命令进行设置。

例：为名为 policy_a 的策略配置触发参数，配置其触发以后延迟 5 秒运行，策略最大运行事件为 15 秒。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# smart manager applet policy_a
Ruijie(sem-applet)# trigger delay 5 maxrun 15
```

12.2.6 配置CLI行动项输出记录

命令	作用
Ruijie# **configure terminal**	进入全局模式
Ruijie(config)# **smart manager applet** *applet-name* [**class** *class-options*]	进入 SEM 配置模式，*applet-name* 参数制定策略的名字，class 参数指定策略的类别（默认为 default 类别）
Ruijie(sem-applet)# **policy record**	设计在 CLI 行动项运行时产生的输出记录到文件

如果要停止记录 CLI 行动项的输出记录，在 SEM 配置模式下使用 **no policy record** 命令进行设置。

例：为名为 policy_a 的策略配置 CLI 行动输出记录，单次策略运行产生的记录文件不大于 500K，policy_a 产生的所有记录文件不大于 2M。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# smart manager applet policy_a
Ruijie(sem-applet)# action action_1 cli command "enable"
Ruijie(sem-applet)# action action_2 cli command "show arp"
Ruijie(sem-applet)# policy record per-instance 500 per-policy 2000
```

12.2.7 显示当前策略配置

命令	作用
Ruijie# **configure terminal**	进入全局模式
Ruijie(config)# **smart manager applet** *applet-name* [**class** *class-options*]	进入 SEM 配置模式，*applet-name* 参数制定策略的名字，class 参数指定策略的类别（默认为 default 类别）
Ruijie(sem-applet)# **list-config**	显示当前策略配置

例：显示策略 policy_a 的策略配置。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# smart manager applet policy_a
Ruijie(sem-applet)# list-config
smart manager applet policy_a
 description "policy_for_test"
 event tag event_a syslog pattern "shutdown"
 trigger delay 5 maxrun 15
 action label syslog priority informational msg "action running"
Ruijie(sem-applet)#
```

当策略处于编辑状态而没有提交时，list-config 显示内容当前编辑中没有提交的配置，显示内容中不包含 commit 命令。当策略已经提交时，则显示提交策略的配置，显示内容中包含 commit 命令。

12.2.8 提交配置

命令	作用
Ruijie# **configure terminal**	进入全局模式
Ruijie(config)# **smart manager applet** *applet-name* [**class** *class-options*]	进入 SEM 配置模式，*applet-name* 参数制定策略的名字，class 参数指定策略的类别（默认为 default 类别）
Ruijie(sem-applet)# **commit**	提交策略配置

例：提交策略 policy_a 的策略配置。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# smart manager applet policy_a
Ruijie(sem-applet)# commit
```

提交过程中会进行策略配置合法性检查，如果检查不通过，则策略配置提交失败，策略不会被注册，依然处于编辑状态。比如策略没有配置事件，则提交检查不会通过。

可以被提交的策略分为两种：新创建的策略和被编辑的已经注册的策略。其他情况的策略，比如，已经注册的策略且没有被编辑，则不会被提交，会给出相应的提示信息。

以上两种可以提交的策略，在提交之前，如果用户希望放弃以做出的策略配置变化，通过 rollback 将策略配置回退。

12.2.9 查看注册策略

命令	作用
Ruijie# **show smart manager policy registered** [**policy** *policy-name*] [**event-type** *event-name*] [**class** *class-options*] [**time-ordered** | **name-ordered**]	显示已经注册的策略信息

例：提交策略 policy_a 的策略配置。

```
Ruijie# show smart manager policy registered
No.   Class    Event Type    Time Registered            Secu    Name
1     applet   syslog        Wed Mar 10 10:49:03 2010   none    policy_a
 event_a: syslog: pattern {shutdown}
 trigger delay 5.000
 maxrun 15.000
 action label syslog priority informational msg "action running"
```

12.2.10 回退配置

命令	作用
Ruijie# **configure terminal**	进入全局模式
Ruijie(config)# **smart manager applet** *applet-name* [**class** *class-options*]	进入 SEM 配置模式，*applet-name* 参数制定策略的名字，class 参数指定策略的类别（默认为 default 类别）
Ruijie(sem-applet)# **rollback**	回退策略配置

例：回退策略 policy_a 的策略配置。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# smart manager applet policy_a
Ruijie(sem-applet)# rollback
```

有两种情况下用户可以选择回退策略配置：新配置的策略，但尚未提交；配置了已经提交注册的策略，但尚未将变化提交。

以上两种情况用户可以通过 rollback 命令将未提交的策略配置回退掉。

12.2.11 配置多事件触发

命令	作用
Ruijie# **configure terminal**	进入全局模式
Ruijie(config)# **smart manager applet** *applet-name* [**class** *class-options*]	进入 SEM 配置模式，*applet-name* 参数制定策略的名字，class 参数指定策略的类别（默认为 default 类别）

Ruijie(sem-applet)# **event tag event-name** [**correlate** { **andnot** | **and** | **or** }] **syslog pattern** *regular-expression* [**priority** *priority-level*] [**occurs** *num-occurrences*] [**period** *period-value*] [**skip** { **yes** | **no** }]	配置首个事件
Ruijie(sem-applet)# **event tag event-name** [**correlate** { **andnot** | **and** | **or** }] **syslog pattern** *regular-expression* [**priority** *priority-level*] [**occurs** *num-occurrences*] [**period** *period-value*] [**skip** { **yes** | **no** }]	配置其他事件

例：配置策略 policy_a，并配置两个事件，首要事件检测日志中是否包含“need reload”，其他事件为是否有板卡插入。而且要求二者发生的间隔需要小于 180 秒。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# smart manager applet policy_a
Ruijie(sem-applet)# event tag event_a syslog pattern "need reload"
Ruijie(sem-applet)# event tag event_b correlate and oir type plugin "shutdown"
Ruijie(sem-applet)# trigger correlate-period 180
```

在配置多个事件的时候，SEM 会按照 tag 的字母排序自动为事件排序。建议对采用有排序规律的命名方法，如：01_cli ， 02_timer ， 03_counter ...。

事件之间的关系为：当前事件与其前边所有事件组合之间的关联系。只有首个事件被触发时，才检查策略是否触发。

除首个事件以外其他事件要配置并列关系，默认的并列关系为 and，首个事件配置的并列关系将被忽略。

12.2.12 配置和使用变量

命令	作用
Ruijie# **configure terminal**	进入全局模式
Ruijie# **smart manager environment** *variable-name string*	配置 SEM 全局变量
Ruijie(config)# **smart manager applet** *applet-name* [**class** *class-options*]	进入 SEM 配置模式，*applet-name* 参数制定策略的名字，class 参数指定策略的类别（默认为 default 类别）
Ruijie(sem-applet)# **action** *label* **set** *variable-name variable-value*	设置 SEM 局部变量
Ruijie(sem-applet)# **action** *label* **syslog** [**priority** *priority-level*] **msg** *msg-text* [**facility** *string*]	使用 SEM 变量 （多种行动中都支持使用变量，此处以 Syslog 为例）

例：配置 SEM 全局变量 var_g，配置策略 policy_a，配置 set 行动项设置 SEM 局部变量 var_l，并在配置 Syslog 行动，在行动中引用变量 var_g，var_l。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# smart manager environment var_g value_1
Ruijie(config)# smart manager applet policy_a
Ruijie(sem-applet)# action action_1 set var_l value_2
```

```
Ruijie(sem-applet)# action action_2 syslog msg "var_g = $var_g ; var_l = $var_l ; _event_type_string = $_event_type_string"
```

上例中，var_g 为全局变量，由 **smart manager environment** 命令设定。var_l 为用户局部变量，由 set 行动设定。_event_type_string 为系统局部变量，又 SEM 事件检测器设定。

系统局部变量为只读属性，不可以被更改，当行动试图更改的时候，策略执行将出现错误中止。局部变量的优先级高于全局变量，当设置了与全局变量重名的局部变量以后，以此名字引用变量时，被引用的变量为局部变量。

12.2.13 挂起/恢复调度器

命令	作用
Ruijie# **configure terminal**	进入全局模式
Ruijie(config)# **smart manager scheduler suspend**	将 SEM 策略调度器挂起

如果要恢复调度器运行，在全局配置模式下使用 **no smart manager scheduler suspend** 命令进行设置。

例：将 SEM 调度器挂起

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# smart manager scheduler suspend
```

将 SEM 调度器挂起仅为将调度功能挂起，已经被调度运行的线程不会因为调度器的挂起而停止运行。

12.2.14 暂停/恢复策略执行

命令	作用
Ruijie# **smart manager scheduler hold** { **all** | **policy** *job-id* | **class** *class-options* }	将执行中的策略暂停
Ruijie# **smart manager scheduler release** { **all** | **policy** *policy-id* | **class** *class-options* }	将暂停的策略恢复执行

例：将类别为 A 的的策略执行挂起

```
Ruijie# smart manager scheduler hold class a
```

例：将类别为 A 的的策略恢复执行

```
Ruijie# smart manager scheduler release class a
```

只有没有被调度器调度运行的线程可以被暂停，一旦被调度器调度运行，则无法被暂停。

暂停和恢复的参数中 class 和 all，是将指定的类别和所有类别暂停，类别的后续线程也将被暂停。而参数 policy 则只是将一个特定的类别暂停，类别中其他策略不受影响。

12.2.15 强制中止策略执行

命令	作用
Ruijie# **smart manager scheduler clear** { **all** | **policy** *job-id* | **class** *class-options*]	强制中止策略执行

例：强制中止策略运行 ID 为 150 的策略。

```
Ruijie# smart manager scheduler clear policy 150
```

12.2.16 显示SEM历史信息

命令	作用
Ruijie# **show smart manager history events**	显示 SEM 历史信息

例：显示 SEM 历史信息

```
Ruijie# show smart manager history events
No.   Job Id   Proc Status    Time of Event             Event Type   Name
1     1        Actv success   Tue Mar 9 00:00:00 2010   timer cron   applet: policy_a
```

12.2.17 显示SEM检测器信息

命令	作用
Ruijie# **show smart manager detector** [**all** | *detector-name*] [**detailed** | **statistics**]	显示 SEM 检测器信息

例：显示 SEM 检测器详细信息

```
Ruijie# show smart manager detector syslog detailed
No.   Name     Version
1     syslog   01.00
Applet Configuration Syntax:
event tag event-name [correlate {andnot | and | or }] syslog pattern regular-expression [occurs num-occurrences]
[period period-value] [priority priority-level]
Applet Built-in Environment Variables:
$_event_id
$_event_type
$_event_type_string
$_event_pub_time
$_event_pub_sec
$_event_pub_msec
$_syslog_msg
$_syslog_priority
```

例：显示 SEM 检测器统计信息

```
Ruijie# show smart manager detector syslog statistics
Syslog Detecotr Statistics:
Policy      Event     Detect   NoPri   PriPass   PriDeny   PatternPass   trigge
policy_a    event_a   1000     100     400       500       10            4
```

12.2.18 显示SEM版本信息

命令	作用
Ruijie# **show smart manager version**	显示 SEM 版本信息

例：显示 SEM 版本信息

```
Ruijie# show smart manager version
Smart Embedded Manager Version 1.0
Event Detectors:
name                 version
application          1.0
syslog               1.0
cli                  1.0
counter              1.0
cpp                  1.0
grtd                 1.0
interface            1.0
none                 1.0
oir                  1.0
snmp                 1.0
snmp-object          1.0
snmp-notification    1.0
sysmon               1.0
timer                1.0
```

12.3 配置举例

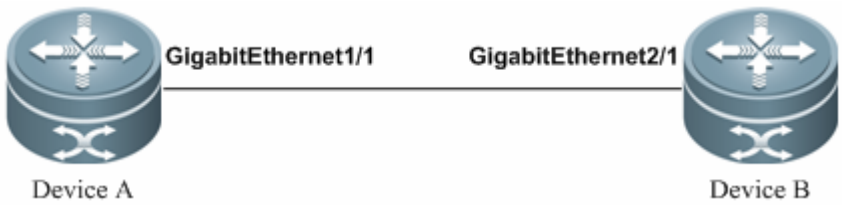
12.3.1 SEM检测接口计数

组网需求

Device A 和 Device B 直接相连，Device A 的 GigabitEthernet1/1 与 Device B 的 GigabitEthernet2/1 相连。因为线路或者 Device B 的问题，Device A 会经常突然接收到来自 Device B 的大量持续错帧，影响通信。将 Device A 的 GigabitEthernet1/1 shutdown 再恢复可以将问题修复。

组网拓扑

图 12-2 接口计数检测举例拓扑



配置要点

- 创建策略
- 配置接口事件
- 配置命令行行动
- 提交策略配置

配置步骤

配置 Device A

1) 给 Device A 配置策略取名为 policy_a。

2) 给 policy_a 配置名为 event_1 的事件，类型为 interface 类型。其具体的参数如下：
配置检测接口计数类型的参数“parameter input_errors_frame”，其含义为检测接口的输入错帧的数量；
配置被检测接口接口名字的参数“name GigabitEthernet 1/1”用于指定被检测的接口；
配置检测阈值的参数“entry-type value entry-op ge entry-val 2000”，其含义为检测计数的绝对值，当绝对值大于等于 2000 的时候为检测通过；
配置检测频率的参数“poll-interval 5”，其含义为检测接口计数的时间间隔为 5 秒钟一次；
计数检测通过以后恢复事件检测的条件参数为“exit-type value exit-op ge exit-val 2000 exit-time 60 exit-comb and”，其“exit-type value exit-op ge exit-val 2000”部分的选项与量值都与前边的检测阈值相同，即事件触发以后，量值检查立即满足恢复的条件，其“exit-time 60 exit-comb and”表示恢复时间与恢复检查为与关系，既然恢复检查在事件触发以后就立即满足，则一旦触发事件超过 60 秒，恢复的另一个条件恢复时间也得到满足，事件检测得到恢复。

3) 给 policy_a 配置多个行动，具体如下：
命令行进入 GigabitEthernet 1/1 的接口模式；
命令行将接口 shutdown；
命令行将接口 no shutdown；
命令行进入特权模式；
命令行清除接口 GigabitEthernet 1/1 的接口统计计数；

4) 保存 cli 行动项的输入命令和输出信息，通过配置 policy record 实现，缺省是不保存.

5) 将策略提交

6) 退出策略编辑

```
Ruijie# configure terminal
Ruijie(config)# smart manager applet policy_a
```

```
Ruijie(sem-applet)# event tag event_1 interface parameter input_errors_frame name GigabitEthernet 1/1 entry-type value entry-op ge entry-val 2000 poll-interval 5 exit-type value exit-op ge exit-val 2000 exit-time 60 exit-comb and
Ruijie(sem-applet)# action action_1 cli command "enable"
Ruijie(sem-applet)# action action_2 cli command "configure terminal"
Ruijie(sem-applet)# action action_3 cli command "interface GigabitEthernet 1/1"
Ruijie(sem-applet)# action action_4 cli command "shutdown"
Ruijie(sem-applet)# action action_5 cli command "no shutdown"
Ruijie(sem-applet)# action action_6 cli command "exit"
Ruijie(sem-applet)# action action_7 cli command "exit"
Ruijie(sem-applet)# action action_8 cli command "clear counters GigabitEthernet 1/1" pattern "y"
Ruijie(sem-applet)# policy record
Ruijie(sem-applet)# commit
Ruijie(sem-applet)# exit
Ruijie(config)#
```

显示验证

- 显示注册的 SEM 策略

```
Ruijie# show smart manager policy registered
No.   Class     Event Type          Time Registered           Secu   Name
1     applet    interface           Mon Mar 8 16:19:15 2010   none   policy_a
 event_1: interface: name GigabitEthernet 1/1 parameter input_errors_frame entry_op ge entry_val 2000 entry_type value exit_comb and exit_op ge exit_val 2000 exit_type value exit_time 60.000 poll_interval 5.000
 maxrun 20.000
 action action_1 cli command "enable"
 action action_2 cli command "configure terminal"
 action action_3 cli command "interface GigabitEthernet 1/1"
 action action_4 cli command "shutdown"
 action action_5 cli command "no shutdown"
 action action_6 cli command "exit"
 action action_7 cli command "exit"
 action action_8 cli command "clear counters GigabitEthernet 1/1" pattern "y"
```

- 在策略被执行之后，查看 CLI 行动输出记录

```
Ruijie# more /sem_record/policy_a/2010-05-08_16-21-15_1001.txt
                        SEM CLI RECORD FILE
SEM policy name: policy_a
SEM policy trigger id :1
SEM policy cli record time : Mon Mar 8 16:21:15 2010
================================================
Ruijie#enable
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
Ruijie(config)#interface GigabitEthernet 1/1
Ruijie(config-GigabitEthernet 1/1)#shutdown
Ruijie(config-GigabitEthernet 1/1)#no shutdown
Ruijie(config-GigabitEthernet 1/1)#exit
Ruijie(config)#exit
Ruijie#clear counters GigabitEthernet 1/1
Ruijie#
```

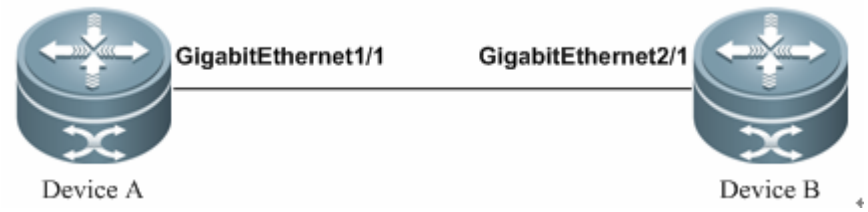
12.3.2 SEM检测特定应用事件

组网需求

Device A 和 Device B 直接相连，Device A 的 GigabitEthernet1/1 与 Device B 的 GigabitEthernet2/1 相连。因为线路或者 Device B 的问题，Device A 会经常突然接收到来自 Device B 的大量持续错帧，影响通信。将 Device A 的 GigabitEthernet1/1 shutdown 再恢复 可以将问题修复。而且 Device A 在执行事件过程中，如果一个小时内发生了五次，则需要发送日志和告警，以确定问题的时间分布。

组网拓扑

图 12-3 特定应用事件检测举例拓扑



配置要点

- 创建接口检测策略，配置接口计数事件，命令行行动，特定应用行动
- 创建特定应用事件检测策略，配置特定应用事件，Syslog 行动。

配置步骤

- 配置 Device A

1) 给 Device A 配置策略取名为 policy_a。

2) 给 policy_a 配置名为 event_1 的事件，类型为 interface 类型。其具体的参数如下：
配置检测接口计数类型的参数“parameter input_errors_frame”，其含义为检测接口的输入错帧的数量；
配置被检测接口接口名字的参数“name GigabitEthernet 1/1”用于指定被检测的接口；
配置检测阈值的参数“entry-type value entry-op ge entry-val 2000”，其含义为检测技术的绝对值，当绝对值大于等于 2000 的时候为检测通过；
配置检测频率的参数“poll-interval 5”，其含义为检测接口计数的时间间隔为 5 秒钟一次；

计数检测通过以后恢复事件检测的条件参数为“exit-type value exit-op ge exit-val 2000 exit-time 60 exit-comb and”，其“exit-type value exit-op ge exit-val 2000”部分的选项与量值都与前边的检测阈值相同，即事件触发以后，量值检查立即满足恢复的条件，其“exit-time 60 exit-comb and”表示恢复时间与恢复检查为与关系，既然恢复检查在事件触发以后就立即满足，则一旦触发事件超过 60 秒，恢复的另一个条件恢复时间也得到满足，事件检测得到恢复。

3) 给 policy_a 配置多个行动，具体如下：
命令行进入 GigabitEthernet 1/1 的接口模式；
命令行将接口 shutdown；
命令行将接口 no shutdown；
命令行进入特权模式；
命令行清除接口 GigabitEthernet 1/1 的接口统计计数；
发布 SEM 特定应用事件，其事件参数为：子集 100，类型 50

4) 将策略提交

5) 退出策略编辑

```
Ruijie# configure terminal
Ruijie(config)# smart manager applet policy_a
Ruijie(sem-applet)# event tag event_1 interface parameter input_errors_frame name GigabitEthernet 1/1 entry-type value entry-op ge entry-val 2000 poll-interval 5 exit-type value exit-op ge exit-val 2000 exit-time 60 exit-comb and
Ruijie(sem-applet)# action action_1 cli command "enable"
Ruijie(sem-applet)# action action_2 cli command "configure terminal"
Ruijie(sem-applet)# action action_3 cli command "interface GigabitEthernet 1/1"
Ruijie(sem-applet)# action action_4 cli command "shutdown"
Ruijie(sem-applet)# action action_5 cli command "no shutdown"
Ruijie(sem-applet)# action action_6 cli command "exit"
Ruijie(sem-applet)# action action_7 cli command "exit"
Ruijie(sem-applet)# action action_8 cli command "clear counters GigabitEthernet 1/1" pattern "y"
Ruijie(sem-applet)# action action_9 publish-event subset 100 type 50
Ruijie(sem-applet)# commit
Ruijie(sem-applet)# exit
Ruijie(config)#
```

■ 配置 Device A

1) 给 Device A 配置策略取名为 policy_b。

2) 给 Device A 配置名为 event_1 的事件(不同的策略中事件可以重名)，其类型为特定应用事件类型，子集和类型与上边 policy_a 中的 action_9 完全一致。检测 policy_a 中 action_9 发布的事件，当 policy_a 中 action_9 发布事件 100，50 以后，event_1 被触发。

3) 给 policy_b 配置行动发送日志

4) 将策略提交

5) 退出策略编辑

```
Ruijie# configure terminal
Ruijie(config)# smart manager applet policy_b
Ruijie(sem-applet)# event tag event_1 application subset 100 type 50
Ruijie(sem-applet)# action action_1 syslog msg "shutdown and no shutdown 5 times" priority 5
Ruijie(sem-applet)# trigger occurs 5 occurs-period 3600
Ruijie(sem-applet)# commit
Ruijie(sem-applet)# exit
Ruijie(config)#
```

显示验证

```
Ruijie# show smart manager policy registered
No.  Class    Event Type         Time Registered           Name
1    applet   interface          Mon Mar 8 21:07:21 2010   policy_a
 event_1: interface: name GigabitEthernet 1/1 parameter {input_errors_frame} entry_op ge entry_val 2000
entry_type value exit_comb and exit_op ge exit_val 2000 exit_type value exit_time 60.000 poll_interval 5.000
 maxrun 20.000
 action action_1 cli command "enable"
 action action_2 cli command "configure terminal"
 action action_3 cli command "interface GigabitEthernet 1/1"
 action action_4 cli command "shutdown"
 action action_5 cli command "no shutdown"
 action action_6 cli command "exit"
 action action_7 cli command "exit"
 action action_8 cli command "clear counters GigabitEthernet 1/1" pattern "y"
 action action_9 publish-event subset 100 type 50 arg1 "tmp"
2    applet   user application   Mon Mar 8 21:08:11 2010   policy_b
 event_1: application: sub_system 100 type 50
 trigger occurs 5 period 3600.000
 maxrun 20.000
 action action_1 syslog priority notifications msg "shutdown and no shutdown 5 times"
```

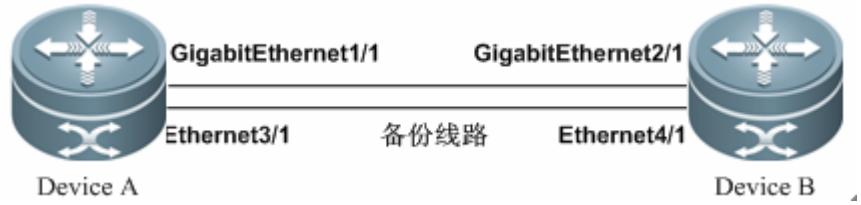
12.3.3 SEM检测计数器

组网需求

Device A 和 Device B 直接相连，Device A 的 GigabitEthernet1/1 与 Device B 的 GigabitEthernet2/1 相连。另外在 Device A 的 Ethernet3/1 到 Device B 的 Ethernet4/1 有两设备的低带宽备份线路。因为线路或者 Device B 的问题，Device A 在接口 GigabitEthernet1/1 会经常突然接收到来自 Device B 的大量持续错帧，影响通信。将 Device A 的 GigabitEthernet1/1 shutdown 再恢复 可以将问题修复。当事件被触发总数超过 50 次以后，永久 shutdonw 接口 GigabitEthernet1/1，使用备份线路。

组网拓扑

图 12-4 计数器事件检测举例拓扑



配置要点

- 创建接口检测策略，配置接口计数事件，命令行行动，计数器行动
- 创建特定应用事件检测策略，配置计数器事件，命令行行动。

配置步骤

- 配置 Device A

1) 给 Device A 配置策略取名为 policy_a。

2) 给 policy_a 配置名为 event_1 的事件，类型为 interface 类型。其具体的参数如下：
配置检测接口计数类型的参数“parameter input_errors_frame”，其含义为检测接口的输入错帧的数量；
配置被检测接口接口名字的参数“name GigabitEthernet 1/1”用于指定被检测的接口；
配置检测阈值的参数“entry-type value entry-op ge entry-val 2000”，其含义为检测技术的绝对值，当绝对值大于等于 2000 的时候为检测通过；
配置检测频率的参数“poll-interval 5”，其含义为检测接口计数的时间间隔为 5 秒钟一次；
计数检测通过以后恢复事件检测的条件参数为“exit-type value exit-op ge exit-val 2000 exit-time 60 exit-comb and”，其“exit-type value exit-op ge exit-val 2000”部分的选项与量值都与前边的检测阈值相同，即事件触发以后，量值检查立即满足恢复的条件，其“exit-time 60 exit-comb and”表示恢复时间与恢复检查为与关系，既然恢复检查在事件触发以后就立即满足，则一旦触发事件超过 60 秒，恢复的另一个条件恢复时间也得到满足，事件检测得到恢复。

3) 给 policy_a 配置多个行动，具体如下：
命令行进入 GigabitEthernet 1/1 的接口模式；
命令行将接口 shutdown；
命令行将接口 no shutdown；
命令行进入特权模式；
命令行清除接口 GigabitEthernet 1/1 的接口统计计数；
计数器行动，给名为 counter_a 的 SEM 命令计数器的值增加 1

4) 将策略提交

5) 退出策略编辑

```
Ruijie# configure terminal
Ruijie(config)# smart manager applet policy_a
Ruijie(sem-applet)# event tag event_1 interface parameter input_errors_frame name GigabitEthernet 1/1 entry-type value entry-op ge entry-val 2000 poll-interval 5 exit-type value exit-op ge exit-val 2000 exit-time 60 exit-comb and
```

```
Ruijie(sem-applet)# action action_1 cli command "enable"
Ruijie(sem-applet)# action action_2 cli command "configure terminal"
Ruijie(sem-applet)# action action_3 cli command "interface GigabitEthernet 1/1"
Ruijie(sem-applet)# action action_4 cli command "shutdown"
Ruijie(sem-applet)# action action_5 cli command "no shutdown"
Ruijie(sem-applet)# action action_6 cli command "exit"
Ruijie(sem-applet)# action action_7 cli command "exit"
Ruijie(sem-applet)# action action_8 cli command "clear counters GigabitEthernet 1/1" pattern "y"
Ruijie(sem-applet)# action action_9 counter name counter_a op inc value 1
Ruijie(sem-applet)# commit
Ruijie(sem-applet)# exit
Ruijie(config)#
```

■ 配置 Device A

1) 给 Device A 配置策略取名为 policy_b。

2) 给 Device A 配置名为 event_1 的事件(不同的策略中事件可以重名)，事件的类型为 SEM 计数器类型，具体参数如下：
检测的 SEM 计数器的名字为 counter_a，与策略 policy_a 中 action_9 操作的计数器名字相同；
计数器的检测参数为“entry-op ge entry-val 50”，其含义为当 SEM 计数器的值大于等于 50 的时候事件触发。
计数器的恢复参数为“exit-op ge exit-val 50”，其配置的类型与值都与检测参数相同，则表示计数器事件通过以后，立即恢复事件检测。

3) 给 policy_b 配置行动，具体如下：
命令行动进入 GigabitEthernet 1/1 的接口模式；
命令行动将接口永久 shutdown；

4) 将策略提交

5) 退出策略编辑

```
Ruijie# configure terminal
Ruijie(config)# smart manager applet policy_b
Ruijie(sem-applet)# event tag event_1 counter name counter_a entry-op ge entry-val 50 exit-op ge exit-val 50
Ruijie(sem-applet)# action action_1 cli command "enable"
Ruijie(sem-applet)# action action_2 cli command "configure terminal"
Ruijie(sem-applet)# action action_3 cli command "interface GigabitEthernet 1/1"
Ruijie(sem-applet)# action action_4 cli command "shutdown"
Ruijie(sem-applet)# action action_5 cli command "exit"
Ruijie(sem-applet)# commit
Ruijie(sem-applet)# exit
Ruijie(config)#
```

显示验证

```
Ruijie# show smart manager policy registered
No.   Class    Event Type     Time Registered           Name
1     applet   interface      Mon Mar 8 22:21:26 2010   policy_a
```

```
 event_1: interface: name GigabitEthernet 0/1 parameter input_errors_frame entry_op ge entry_val 2000 entry_type
value exit_comb and exit_op ge exit_val 2000 exit_type value exit_time 60.000 poll_interval 5.000
 maxrun 20.000
 action action_1 cli command "enable"
 action action_2 cli command "configure terminal"
 action action_3 cli command "interface GigabitEthernet 1/1"
 action action_4 cli command "shutdown"
 action action_5 cli command "no shutdown"
 action action_6 cli command "exit"
 action action_7 cli command "exit"
 action action_8 cli command "clear counters GigabitEthernet 1/1" pattern "y"
 action action_9 counter name counter_a value 1 op inc
2    applet   user counter   Mon Mar 8 22:23:26 2010   policy_b
 event_1: counter: name {counter_a} entry_val 50 entry_op ge exit_val 50 exit_op ge
 maxrun 20.000
 action action_1 cli command "enable"
 action action_2 cli command "configure terminal"
 action action_3 cli command "interface GigabitEthernet 1/1"
 action action_4 cli command "shutdown"
 action action_5 cli command "exit"
```

12.3.4 SEM检测热插拔

组网需求

VSU 系统在线状态插入新的成员设备后，由于软件故障，新插入的设备路由信息不完整，导致转发异常。通过命令 **clear ip route ***重新刷路由可以解决问题。

配置要点

- 创建策略
- 配置热插拔事件
- 配置行动
- 提交策略配置

配置步骤

配置 Device A

1) 给 Device A 配置策略取名为 policy_a。

2) 给 policy_a 配置名为 event_1 的事件，类型为热插拔事件类型，操作类型为插入。

3) 给 policy_a 配置多个行动，具体如下：
执行命令进入特权模式；
执行命令 **clear ip route ***刷新路由

4) 将策略提交

5) 退出策略编辑

```
Ruijie# configure terminal
Ruijie(config)# smart manager applet policy_a
Ruijie(sem-applet)# event tag event_1 oir type plugin
Ruijie(sem-applet)# action action_1 cli command "enable"
Ruijie(sem-applet)# action action_2 cli command "clear ip route *"
Ruijie(sem-applet)# delay 60
Ruijie(sem-applet)# commit
Ruijie(sem-applet)# exit
Ruijie(config)#
```

显示验证

```
Ruijie# show smart manager policy registered
No.   Class    Event Type          Time Registered           Secu   Name
1     applet   oir                 Mon Mar 8 16:45:17 2010   none   policy_a
 event_1: oir: type{plugin}
 maxrun 20.000
 delay 60.000
 action action_1 cli command "enable"
 action action_2 cli command "clear ip route *"
```

12.3.5 SEM定时器事件

组网需求

Device A 与 Tftp Server 相连，Devie A 需要每天零点自动将日志文件归档到 Tftp Server 上，并将原有日志文件删除。

组网拓扑

图 12-5 定时器检测举例拓扑

配置要点

- 创建策略
- 配置定时器事件
- 配置行动
- 提交策略配置

配置步骤

配置 Device A

1) 给 Device A 配置策略取名为 policy_a。

2) 给 policy_a 配置名为 event_1 的事件，类型为 cron 定时器类型，指示时间为每日的零点整。

3) 给 policy_a 配置多个行动，具体如下：
执行命令进入特权模式；
执行 **copy** 命令归档日志

4) 将策略提交

5) 退出策略编辑

```
Ruijie# configure terminal
Ruijie(config)# smart manager applet policy_a
Ruijie(sem-applet)# event tag event_1 timer cron cron-entry "0 0 * * *"
Ruijie(sem-applet)# action action_1 cli command "enable"
Ruijie(sem-applet)# action action_2 cli command "copy flash: logfile.txt
tftp://172.16.0.2/device_a/log_$_event_pub_time"
Ruijie(sem-applet)# action action_3 cli command "delete flash: logfile.txt"
Ruijie(sem-applet)# commit
Ruijie(sem-applet)# exit
Ruijie(config)#exit
```

显示验证

```
Ruijie# show smart manager policy registered
No.   Class    Event Type          Time Registered           Secu   Name
1    applet    timer cron          Mon Mar 8 17:25:47 2010   none   policy_a
 event_1: timer cron: cron entry “0 0 * * *”
 maxrun 20.000
 action action_1 cli command "enable"
 action action_2 cli command "copy flash:logfile.txt tftp://172.16.0.2/device_a/log_$_event_pub_time"
 action action_3 cli command "delete flash:logfile.txt"
```

12.3.6 SEM检测CPP计数

组网需求

Device A 与 用户相连，时而会有来自网络的不明攻击，导致设备 CPU 长期占用率高。如果能够发现攻击，并降低攻击报文的优先级，可缓解攻击造成的影响。

组网拓扑

图 12-6 CPP 计数检测举例拓扑

配置要点

- 准备工作
- 创建策略
- 配置 CPP 计数事件
- 配置行动
- 提交策略配置

配置步骤

配置 Device A

1) 将报文优先级小于1的都调整为1，这样发现有攻击类型的报文，就将其优先级设定为0，小于正常报文，保证设备正常工作。

2) 给 Device A 配置策略取名为 policy_a。

3) 给 policy_a 配置名为 event_1 的事件，类型为 cpp 类型，其参数如下：
配置检测所有类型的 CPP 报文，使用参数“parameter any”；
配置检测 CPP 报文的丢弃量“type drop op ge value 1000”，指示当指定类型的 CPP 报文丢弃量大于等于 1000 个时事件触发；
配置检测的时间检测“poll-interval 15”，指示检测的时间间隔为 15 秒

4) 给 policy_a 配置多个行动，具体如下：
执行命令进入全局模式；

执行命令**cpu-protect type $_type pri 0**将检测到攻击的CPP报文类型的优先级降低，其中“$_type”为环境变量，由 CPP 事件检测器设定。运行时被具体的 CPP 报文的类型所替换。

5) 将策略提交

6) 退出策略编辑

```
Ruijie# configure terminal
Ruijie(config)# cpu-protect type tp-guard pri 1
Ruijie(config)# cpu-protect type arp pri 1
Ruijie(config)# cpu-protect type dhcps pri 1
Ruijie(config)# cpu-protect type dot1x pri 1
Ruijie(config)# cpu-protect type gvrp pri 1
Ruijie(config)# cpu-protect type ipv6-mc pri 1
Ruijie(config)# cpu-protect type rip pri 1
Ruijie(config)# cpu-protect type unknow-ipmc pri 1
Ruijie(config)# cpu-protect type err-ttl pri 1
Ruijie(config)# cpu-protect type dhcp_relay_client pri 1
Ruijie(config)# cpu-protect type dhcp_realy_server pri 1
Ruijie(config)# cpu-protect type dhcp_option82 pri 1
Ruijie(config)# smart manager applet policy_a
Ruijie(sem-applet)# event tag event_1 cpp parameter any type drop op ge value 1000 poll-interval 15
Ruijie(sem-applet)# action action_1 cli command "enable"
Ruijie(sem-applet)# action action_2 cli command "configure terminal"
Ruijie(sem-applet)# action action_3 cli command "cpu-protect type $_type pri 0"
Ruijie(sem-applet)# commit
Ruijie(sem-applet)# exit
Ruijie(config)#
```

显示验证

```
Ruijie# show smart manager policy registered
No.  Class    Event Type          Time Registered           Name
1    applet   cli                 Mon Mar 8 19:30:00 2010   policy_a
 event_1: cpp: parameter any type drop op ge value 1000 poll-interval 15
 maxrun 20.000
 action action_1 cli command "enable"
 action action_2 cli command " configure terminal "
 action action_3 cli command " cpu-protect type $_type pri 0"
```

12.3.7 SEM检测命令行

组网需求

Device A 与 Tftp Server 相连，Devie A 每次执行 **copy running-config startup-config** 命令之前，都需要将旧配置备份到 Tftp Server。

组网拓扑

图 12-7 命令行检测举例拓扑

配置要点

- 创建策略
- 配置命令行事件
- 配置行动
- 提交策略配置

配置步骤

配置 Device A

1) 给 Device A 配置策略取名为 policy_a。

2) 给 policy_a 配置名为 event_1 的事件，类型为命令行类型，检测包含“copy running-config startup-config”内容的命令；并且执行策略使用同步方式，即使用参数“sync yes”

3) 给 policy_a 配置多个行动，具体如下：
执行命令进入特权模式；
执行 **copy** 命令归档配置文件；

4) 将策略提交

5) 退出策略编辑

```
Ruijie# configure terminal
Ruijie(config)# smart manager applet policy_a
Ruijie(sem-applet)# event tag event_1 cli pattern "copy running-config startup-config" sync yes
Ruijie(sem-applet)# action action_1 cli command "enable"
Ruijie(sem-applet)# action action_2 cli command "copy startup-config
tftp://172.16.0.2/device_a/conf_$_event_pub_time"
Ruijie(sem-applet)# action action_3 exit 1
Ruijie(sem-applet)# commit
Ruijie(sem-applet)# exit
```

```
Ruijie(config)#
```

显示验证

```
Ruijie# show smart manager policy registered
No.   Class    Event Type          Time Registered           Name
1     applet   cli                 Mon Mar 8 19:30:00 2010   policy_a
 event_1: cli: pattern “copy running-config startup-config” sync yes
 maxrun 20.000
 action action_1 cli command "enable"
 action action_2 cli command "copy startup-config tftp://172.16.0.2/device_a/conf_$_event_pub_time"
 action action_3 exit 1
```

12.3.8 SEM检测SNMP事件

组网需求

网管工作站通过以太网与 Device A 互联，Device A 上启用 SNMP 服务，网管工作站可以通过网络管理 Device A。出于兼容性考虑，get OID 1.3.6.1.2.1.2.1 的值的 SNMP 操作需要被阻止。

组网拓扑

图 12-8 SNMP 事件检测举例拓扑

配置要点

- 创建策略
- 配置 SNMP Object 事件
- 配置行动
- 提交策略配置

配置步骤

配置 Device A

1) 给 Device A 配置策略取名为 policy_a。

2) 给 policy_a 配置名为 event_1 的事件，类型为 SNMP Object 类型，参数如下：
检测 snmp 操作的 OID 参数“oid 1.3.6.1.2.1.2.1”；
OID 不可以是表类型参数“istable no”；
OID 的类型为 int 类型，使用参数“type int”；
触发策略的执行方式为异步方式，忽略 SNMP Object 操作，使用参数“skip yes”；

3) 给 policy_a 配置行动，记录到日志 snmp 操作被取消。

4) 将策略提交

5) 退出策略编辑

```
Ruijie# configure terminal
Ruijie(config)# smart manager applet policy_a
Ruijie(sem-applet)# event tag event_1 snmp-object oid 1.3.6.1.2.1.2.1 istable no type int skip yes
Ruijie(sem-applet)# action action_1 syslog msg "cancel snmp operate" priority 5
Ruijie(sem-applet)# commit
Ruijie(sem-applet)# exit
Ruijie(config)#
```

显示验证

```
Ruijie# show smart manager policy registered
No.   Class    Event Type          Time Registered           Secu   Name
1     applet   snmp-object         Tue Mar 9 17:46:01 2010   none   policy_a
 event_1: snmp-object: oid 1.3.6.1.2.1.2.1 type int skip yes istable no
 maxrun 20.000
 action action_1 syslog msg "cancel snmp operate"
```

12.3.9 SEM检测空事件

组网需求

Device A 安装调试过程中，需要反复的清理路由表，ARP 表，IPv6 路由表。需要一种简单的方法实现批量操作

配置要点

- 创建策略
- 配置空事件
- 配置行动
- 提交策略配置

配置步骤

配置 Device A

1) 给 Device A 配置策略取名为 policy_a。

2) 给 policy_a 配置名为 event_1 的事件，类型为空类型，通过命令行手动触发。

3) 给 policy_a 配置多个行动，具体如下：
执行命令进入特权模式；
执行 **clear arp-cache**，清除 ARP 缓存；
执行 **clear ip route ***，刷新 ipv4 路由；
执行 **clear ipv6 route ***，刷新 ipv6 路由；

4) 将策略提交

5) 退出策略编辑

```
Ruijie# configure terminal
Ruijie(config)# smart manager applet policy_a
Ruijie(sem-applet)# event tag event_1 none
Ruijie(sem-applet)# action action_1 cli command "enable"
Ruijie(sem-applet)# action action_2 cli command "clear arp-cache"
Ruijie(sem-applet)# action action_3 cli command "clear ip route *"
Ruijie(sem-applet)# action action_4 cli command "clear ipv6 route *"
Ruijie(sem-applet)# commit
Ruijie(sem-applet)# exit
Ruijie(config)#
```

显示验证

```
Ruijie# show smart manager policy registered
No.   Class    Event Type          Time Registered           Name
1     applet   none                Mon Mar 8 21:43:07 2010   policy_a
 event_1: none: policyname policy_a sync yes
 maxrun 20.000
 action action_1 cli command "enable"
 action action_2 cli command "clear arp-cache"
 action action_3 cli command "clear ip route *"
 action action_4 cli command "clear ipv6 route *"
```

12.3.10 SEM检测Syslog事件

组网需求

Device A 在发生内存不足的情况下会发送日志，发现该日志的时候需要对设备进行主备倒换操作。

配置要点

- 创建策略
- 配置 Syslog 事件
- 配置行动
- 配置策略触发参数
- 提交策略配置

配置步骤

配置 Device A

1) 给 Device A 配置策略取名为 policy_a。

2) 给 policy_a 配置名为 event_1 的事件，类型 Syslog 类型，检测级别为 2 内容包含“No-memory”的日志。

3) 给 policy_a 配置 switchover 行动。

4) 将策略提交

5) 退出策略编辑

```
Ruijie# configure terminal
Ruijie(config)# smart manager applet policy_a
Ruijie(sem-applet)# event tag event_1 syslog pattern "No-memory" priority critical
Ruijie(sem-applet)# action action_1 reload
Ruijie(sem-applet)# commit
Ruijie(sem-applet)# exit
Ruijie(config)#
```

显示验证

```
Ruijie# show smart manager policy registered
No.   Class    Event Type          Time Registered           Secu   Name
1     applet   syslog              Tue Mar 9 18:38:23 2010   none   policy_a
 event_1: syslog: pattern “No-memory” priority critical
maxrun 20.000
action action_1 switchover
```

12.3.11 SEM检测看门狗系统事件

组网需求

Device A 可能存在业务突发导致内存不足或者内存泄漏，当内存耗尽时设备出现故障。为了不因内存问题导致业务受影响，目前需要在内存使用量达到 95%时将设备主备倒换。

配置要点

- 创建策略
- 配置看门狗系统事件
- 配置行动
- 配置策略触发参数
- 提交策略配置

配置步骤

配置 Device A

1) 给 Device A 配置策略取名为 policy_a。
2) 给 policy_a 配置名为 event_1 的事件，类型为看门狗系统事件类型，检测的类型参数为“type memory scope system-use percent”，含义位检测系统内存使用百分比；检测的阈值参数为“entry-op ge entry-val 95”，含义位超过 95%是事件触发。
3) 给 policy_a 配置行动将设备主备倒换。
4) 将策略提交
5) 退出策略编辑

```
Ruijie# configure terminal
Ruijie(config)# smart manager applet policy_a
Ruijie(sem-applet)# event tag event_1 sysmon type memory scope system-use percent entry-op ge entry-val 95
Ruijie(sem-applet)# action action_1 switchover
Ruijie(sem-applet)# commit
Ruijie(sem-applet)# exit
Ruijie(config)#
```

显示验证

```
Ruijie# show smart manager policy registered
No.  Class    Event Type          Time Registered           Secu   Name
1    applet   sysmon              Tue Mar 9 18:38:23 2010   none   policy_a
 event_1: sysmon: type memory scope system-use percent entry-op ge entry-val 95
 maxrun 20.000
 action action_1 switchover
```

12.3.12 SEM检测GRTD事件

组网需求

Device A 的 GRTD 监控诊断发现严重问题时，为方式诊断出的问题影响业务正常运行，将设备主备倒换。

配置要点

- 创建策略
- 配置 GRTD 事件
- 配置行动
- 配置策略触发参数
- 提交策略配置

配置步骤

配置 Device A

1) 给 Device A 配置策略取名为 policy_a。
2) 给 policy_a 配置名为 event_1 的事件，类型为 GRTD 类型，检测所有槽位监控测试出严重问题，参数“slot all testing-type monitoring severity-major”；
3) 给 policy_a 配置行动将设备主备倒换
4) 将策略提交
5) 退出策略编辑

```
Ruijie# configure terminal
Ruijie(config)# smart manager applet policy_a
Ruijie(sem-applet)# event tag event_1 grtd slot all testing-type monitoring severity-major
Ruijie(sem-applet)# action action_1 switchover
Ruijie(sem-applet)# commit
Ruijie(sem-applet)# exit
Ruijie(config)#
```

显示验证

```
Ruijie# show smart manager policy registered
No.   Class    Event Type         Time Registered           Secu   Name
1     applet   grtd               Tue Mar 9 18:38:23 2010   none   policy_a
 event_1: grtd: slot all testing-type monitoring level severity-major
 maxrun 20.000
 action action_1 switchover
```

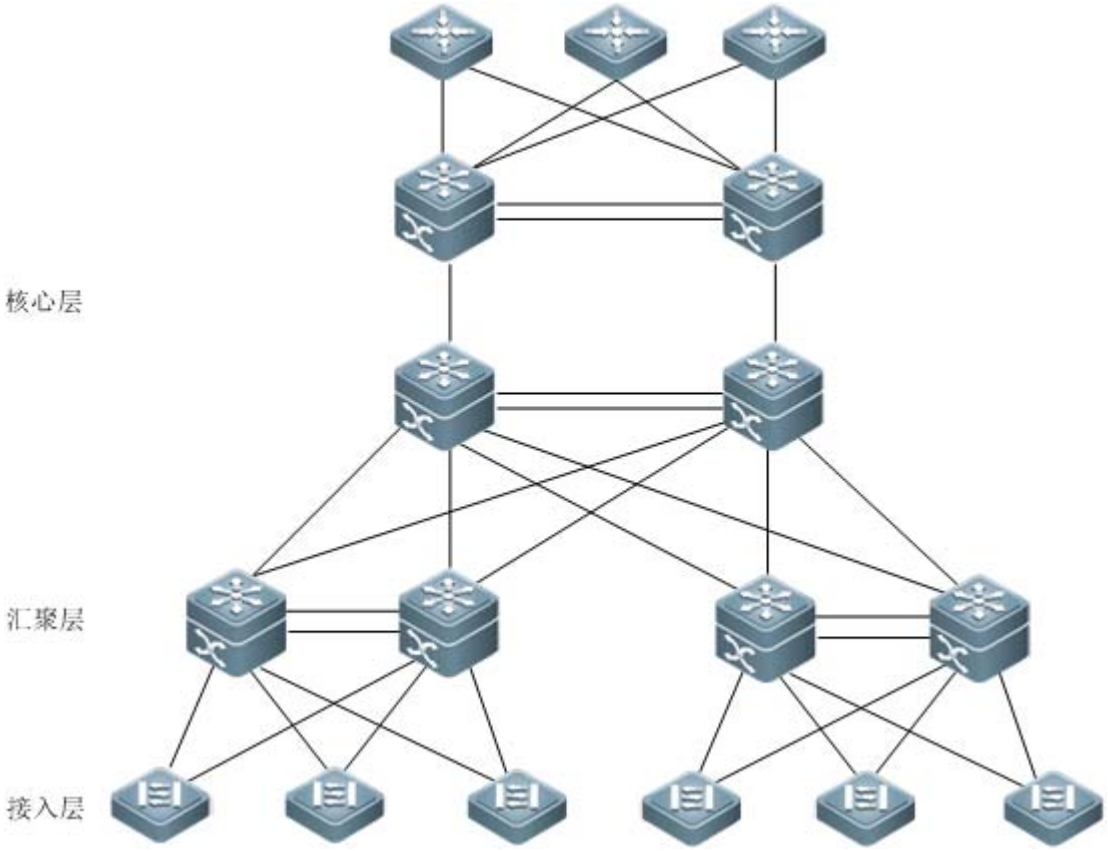
13 VSU

13.1 概述

13.1.1 简介

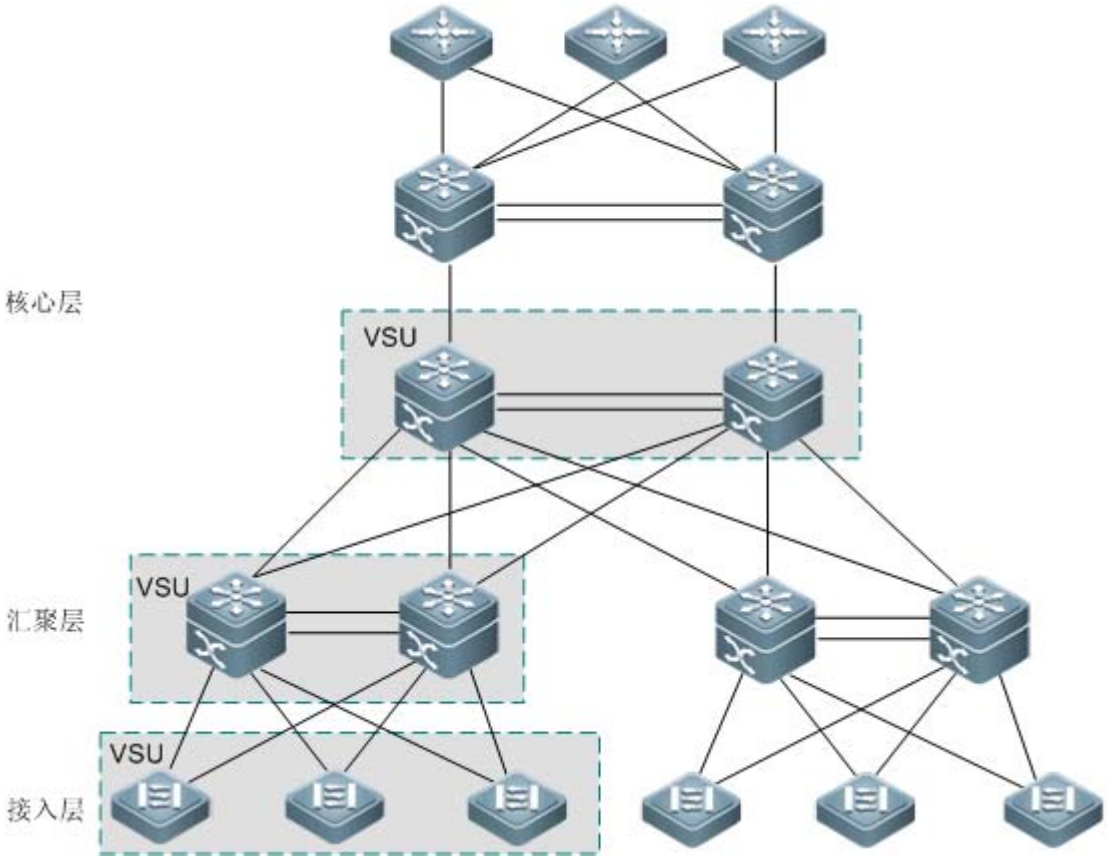
传统的网络中，为了提高网络的可靠性，一般在核心层或汇聚层将两台设备配置成双核心，起冗余备份作用，接入、汇聚设备分别连接两条链路到备份的双核心。下图显示的就是这样的一种典型的传统网络架构。冗余的网络架构增加了网络设计和操作的复杂性，同时大量的备份链路也降低了网络资源的利用率，减少了投资回报率。

图 13-1 传统网络结构



VSU(Virtual Switching Unit)是一种网络系统虚拟化技术，支持将多台设备组合成单一的虚拟设备。如图表 2 所示，接入、汇聚、核心层设备都可以组成VSU，形成整网端到端的VSU组网方案。和传统的组网方式相比，这种组网可以简化网络拓扑，降低网络的管理维护成本，缩短应用恢复的时间和业务中断的时间，提高网络资源的利用率。

图 13-2 端到端的 VSU 组网方案

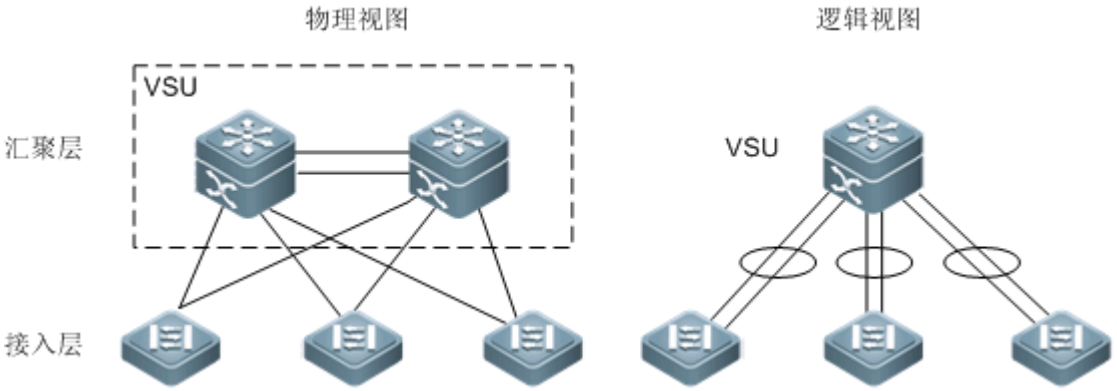


13.1.2 基本概念

VSU 系统

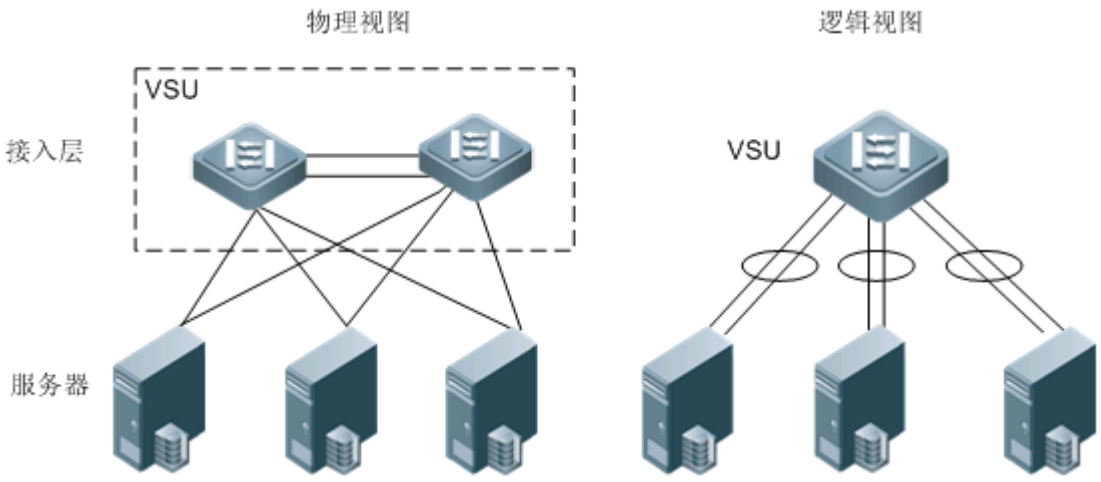
VSU 系统是由传统网络结构中的两台或多台设备组成的单一的逻辑实体，例如位于下图的汇聚层的VSU 系统可以看作单独的一台设备与核心层、接入层进行交互。

图 13-3 汇聚层的 VSU



上图的 VSU 网络结构中，成员之间通过内部的链路组成逻辑实体，接入层设备通过聚合链路与 VSU 建立连接。这样在接入层和汇聚层之间避免了二层环路，另外由于 VSU 减少了路由实体的数目，也简化了三层网络拓扑。

图 13-4 接入层的 VSU



除了核心、汇聚层设备外，接入层设备也可以组成 VSU 系统。对于接入可用性要求高的服务器，一般使用“单服务器多网卡绑定为 Aggregate Port 口(简称 AP 口)”技术来与接入层设备相连。由于 AP 要求只能接入在同一台接入设备上，所以单台设备故障的风险增加了。在这种情况下，可以应用 VSU 解决这个问题。在 VSU 模式下，服务器可以使用多网卡绑定为 AP 口，连接同一个 VSU 组内不同的成员设备，这样可以防止接入设备的单点失效，或是单条链路失效导致的网络中断。

VSU 与传统的盒式设备冷堆叠相比有以下优势:

1、 VSU 支持热插拔，也就是允许在系统运行过程中插入、移出、更换成员设备。

2、 对于组成环形拓扑的 VSU 系统，任何一台设备的失效或是 VSL 链路断开，并不会影响 VSU 系统运行，也就是系统不会重启或是数据断流。

VSU 域标识

VSU 域具有唯一标识 Domain ID。只有同一个域标识的设备才能组合在一起形成同一个 VSU 系统。

成员设备编号

VSU 系统的每个成员设备都拥有唯一的编号，即 Switch ID。这个编号用于管理成员设备，以及配置成员设备上的接口等用途。用户在将设备加入 VSU 系统时需要配置该编号，并且保证成员设备编号在同一个 VSU 系统中是唯一的。VSU 系统如果发现成员设备编号冲突，则将进行自动分配。

成员设备角色

VSU 系统由多台设备构成，在组建 VSU 系统时，多台设备通过一定的竞选协议选举出一台全局主设备，一台全局从设备，其余设备都是全局候选设备。

全局主设备负责控制整个 VSU 系统，运行控制面协议并参与数据转发；其余的设备，包括全局从设备、全局候选设备仅参与数据转发，并不运行控制面协议，所有接收到的控制面数据流都将转发给全局主设备进行处理。

全局从设备同时还实时同步接收全局主设备的状态。与全局主设备构成 1：1 热备份。在全局主设备失效后，全局从设备将切换成全局主角色，来管理整个 VSU 系统。

VSU 系统的主机选举方法为:

1、 VSU 系统的主机选举规则如下（如果根据上一次规则不能决定主机，则根据下一条规则继续判断）：a）主机优先选为主机（启机时所有设备都不是主机）。b）优先级高的成员设备选为主机。c）MAC 地址小的成员设备选为主机。

2、 选择从机的时候，优先选择与主机相近的设备为从机，这样可以尽量避免产生双主机，选择从机的条件排序为：最靠近主机/优先级/MAC 地址。

3、 VSU 系统支持设备的热加入。即使热加入设备的优先级比当前运行的 VSU 系统主机和从机优先级高，系统也不会进行主、从角色切换。

4、 成员设备的启机顺序可能会影响主机的选举。部分成员设备可能由于启机慢，而没有及时加入 VSU 系统。在这种情况下，该成员设备将做热加入处理，即使优先级比当前运行的 VSU 系统主机高，系统也不会发生角色切换。

13.1.3 硬件需求

盒式设备组成 VSU 系统有以下两种硬件方案。不同的产品可能同时支持这两种，或只支持其中一种方案：

堆叠模块：专用的堆叠模块可提供高带宽，低成本的连接方案；使用这种方案需要专用的堆叠模块与堆叠线缆，堆叠成员设备互连的距离受到堆叠线缆长度的约束。

普通端口：普通端口可提供成本低，长距离的连接方案；使用这种方案不需要专用的堆叠线缆，但带宽相对较低。

产品名称	堆叠模块	普通端口	线性拓扑	环形拓扑	成员设备最大数量
S5750-S 系列	不支持	支持	支持	支持	8

必须是同一系列的产品，才能组成 VSU 系统。

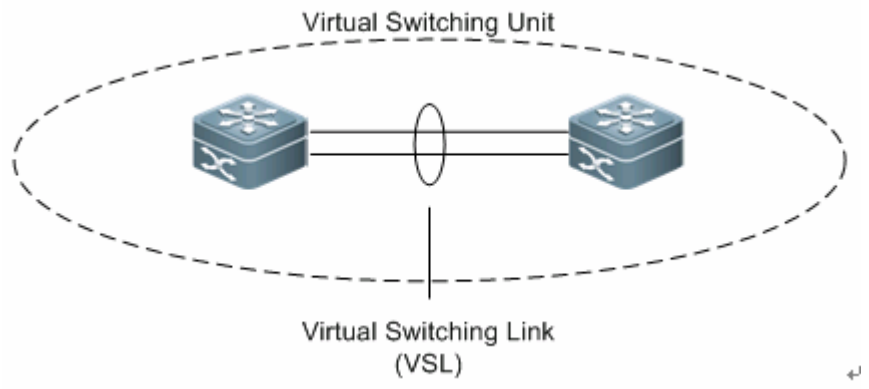
13.1.4 工作原理

13.1.4.1 虚拟交换链路

VSL 链路

由于 VSU 系统的多台设备作为一个网络实体，因此它们之间需要共享控制信息和部分数据流。虚拟交换链路(Virtual Switching Link，简称 VSL。为方便叙述，下文中出现的“虚拟交换链路”均以“VSL”表示)是 VSU 系统的设备间传输控制信息和数据流的特殊链路，目前支持在两台设备间通过万兆接口间建立 VSL。VSL 在 VSU 系统内的位置如下图所示：

图 13-5 虚拟交换链路



VSL 以聚合端口组的形式存在，由 VSL 传输的数据流根据流量平衡算法在聚合端口的各个成员之间就进行负载均衡。

VSL 链路流量

VSL 链路在设备间传输的控制流分为以下几种情况：

1) 成员设备接收到的协议报文，需要通过 VSL 链路转发到全局主设备进行处理。

2) 经过全局主设备处理的协议报文，需要通过 VSL 链路转发到其他成员设备的接口，由该接口发送该协议报文到对端设备。

VSL 链路在设备间传输的数据流分为以下几种情况：

1) VLAN 内泛洪的数据流。

2) 需要跨设备转发的数据流，需要通过 VSL 链路传输。

另外 VSL 链路上也传输 VSU 系统内部的管理类报文，例如热备份交换的协议信息，主机向其他成员设备下发配置信息的报文等等。

对于镜像(SPAN)功能，VSL 链路关联的接口既不能作为 SPAN 的源口，也不能作为 SPAN 的目的口。

VSL 链路故障

如果 VSL 聚合端口组的某一成员链路发生故障，VSU 将自动调整 VSL 聚合端口的配置，使得流量不再从故障的成员链接传输。

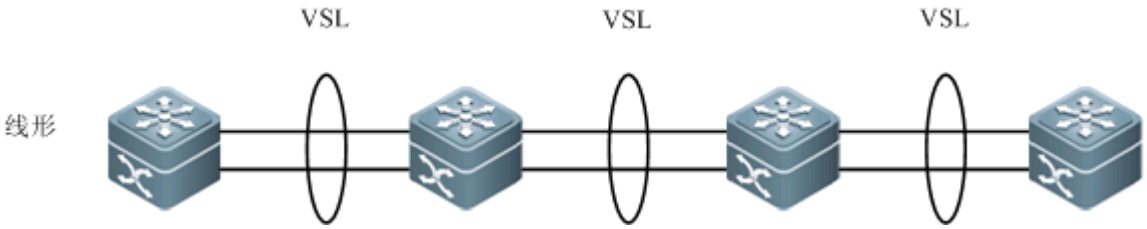
如果 VSL 聚合端口组的所有成员链路都断开，VSU 拓扑将会发生变化。如果原先是环形拓扑，那么将会发生“环转线”，具体情况请“参考拓扑”变化章节的拓扑环线互转部分。

VSL 端口必须和 VSL 端口相连，并且一个 VSL 聚合口只能连接一个 VSL 聚合口。如果 VSL 端口和普通端口相连，或者一个 VSL 聚合口连接多个 VSL 聚合口，就会影响 VSU 拓扑的可靠性。如果一个 VSL 聚合口连接到多个 VSL 聚合口，会导致部分 VSL 成员口被禁用；如果 VSL 成员口连接到非 VSL 成员口，也会导致 VSL 成员口被禁用。组网时要确保正确的连接 VSL 端口，否则会影响 VSU 拓扑的可靠性。对于因为连接错误而被禁用的 VSL 成员口，将其重新正确连接后即可恢复可用。

13.1.4.2 拓扑结构

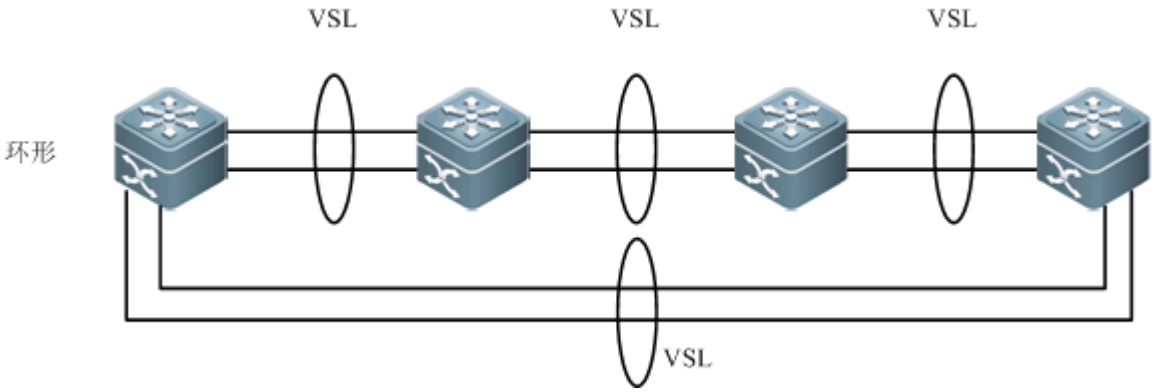
VSU 系统支持线形和环形两种拓扑结构。如下图所示，设备间通过 VSL 链路相连，形成一条线，所以称为线形拓扑。这种拓扑连接简单，使用较少的端口和线缆，但设备间只有一条通信链路，所以 VSL 链路的可靠性较低。

图 13-6 线形拓扑



除了线形拓扑外，如图所示，设备还可以组成环形拓扑，这样设备间的两条通信链路可以相互备份，形成链路冗余，提高 VSU 系统的可靠性。

图 13-7 环形拓扑



用户在选择 VSU 系统的拓扑时，应尽量选择环形拓扑，这样能保证任何单台设备失效、或是任何单条 VSL 链路失效都不会影响整个 VSU 系统的正常运行。

除了选择环形拓扑组网，建议每个 VSL-AP 中配置多根 VSL 链路，以提高单个 VSL-AP 的可靠性。

13.1.4.3 拓扑收敛

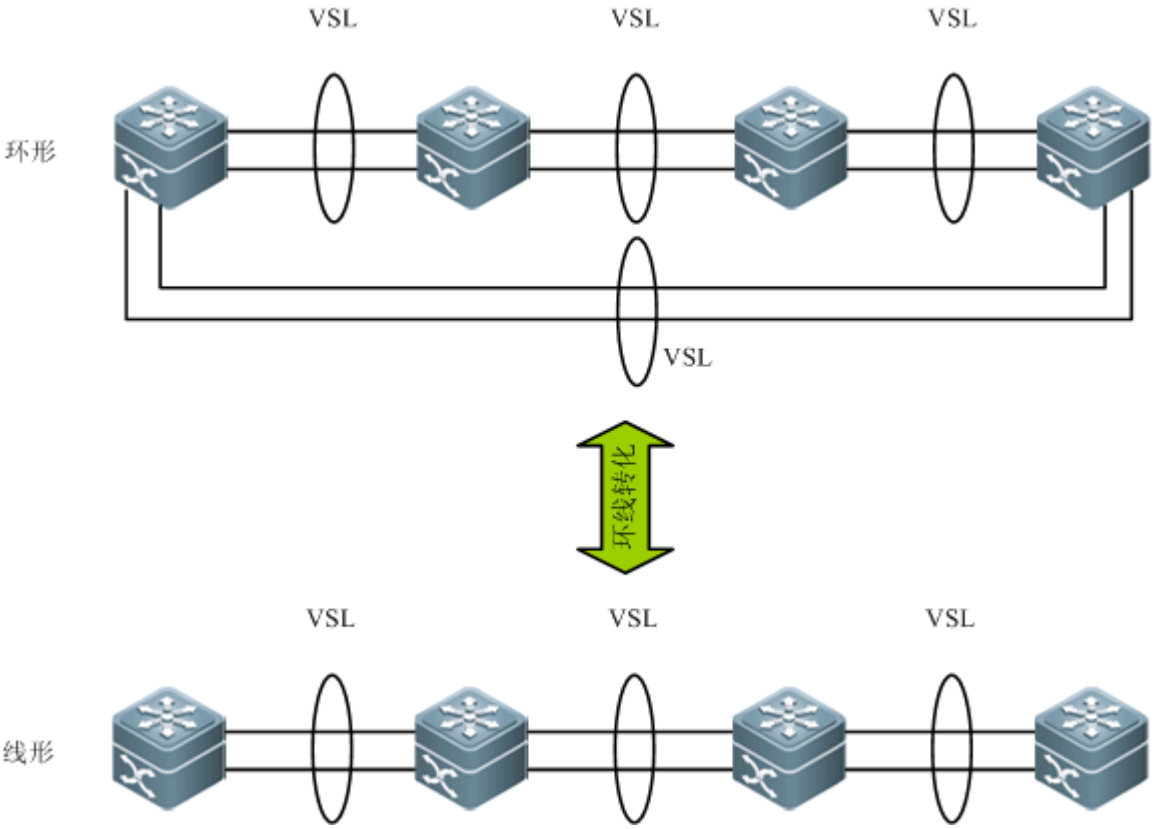
在 VSU 系统建立之前，成员设备间需要通过拓扑发现协议来发现邻居，最终确定 VSU 系统中有哪些设备，从而确定管理域的范围。然后选举出一台全局主设备来管理整个 VSU 系统，接着再选举出一台全局从设备作为主设备的备份。到此，整个 VSU 系统的拓扑已经收敛。由于不同的设备的启动时间有所不同，所以拓扑的首次收敛时间也有所不同。

13.1.4.4 拓扑变化

拓扑环线互转

对于环形拓扑，当其中一条 VSL-AP 链路断开时，拓扑将由环形转成线形。这时整个 VSU 系统仍然能够正常工作，不会造成网络的中断。但为了避免其他的 VSL-AP 链路失效、或节点失效，此时应该要及时去排查 VSL 链路故障，将 VSL 链路恢复。VSL-AP 链路恢复后，拓扑将由线形再转回到环形。

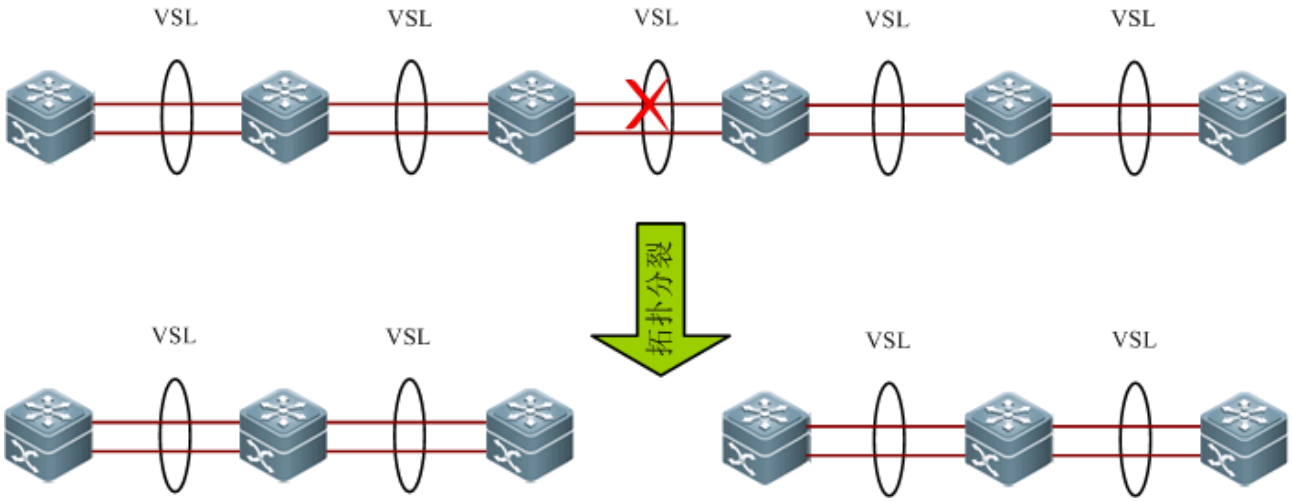
图 13-8 环转线、线转环



拓扑分裂

对于线形拓扑，如果 VSL-AP 链路断开时，拓扑将会发生分裂，如下图所示，一个 VSU 组分裂成两个 VSU 组。这种情况下，可能会导致网络中出现两台配置完全相同的设备，从而令网络无法正常工作。这种情况下需要通过部署双主机检测功能（详见 1.1.4.6 节双主机检测）来解决拓扑分裂问题。

图 13-9 拓扑分裂



拓扑合并

两个 VSU 组通过 VSL-AP 链路连接，将会发生拓扑合并。在拓扑合并过程中，会重启其中一个 VSU 组，然后热加入另一个 VSU 组。

拓扑合并的原则是：最大限度的降低拓扑合并时对业务所带来的影响。其合并规则如下(从第一条开始判断，如果本条无法选出最优拓扑，继续判断下一条）：

1) GM 的成员优先级高的 VSU 系统优先。

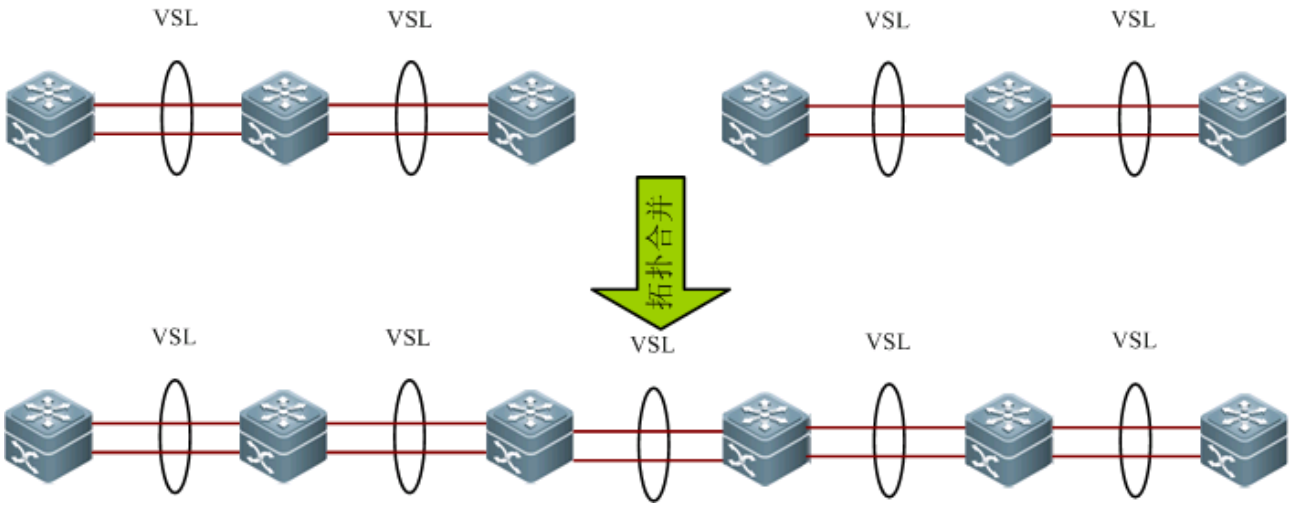
2) Up 端口的最高带宽(不计 VSL 口)高的 VSU 系统优先。比如一方 VSU 系统的 Up 端口的最高带宽为 40G，另外一方 VSU 系统的 Up 端口的最高带宽为 10G，则 40G 这一方优先。

3) Up 端口的最高带宽端口的数量(不计 VSL 口)多的 VSU 系统优先。比如两个 VSU 系统的 Up 端口的最高带宽都为 40G，则 40G 端口的 Up 数量多的 VSU 系统优先。

4) Up 端口的数量(不计 VSL 口) 多的 VSU 系统优先。

5) GM 的 MAC 地址小的 VSU 系统优先。

图 13-10 拓扑合并



当两个 VSU 组进行拓扑合并时，需要进行竞选，竞选失败的一方将逐一自动重启并热加入到另一个 VSU 组。

13.1.4.5 热备份

热备份原理

根据前面描述，VSU 系统的设备角色分为全局主设备、全局从设备以及全局候选设备，其中全局主设备负责整个VSU组的管理，全局主设备和全局从设备形成 1:1 热备份，全局候选设备，不参与热备。如果全局主设备失效，那么全局从设备就升级为主设备，接管整个 VSU 系统。要实现全局热备，就需要主、从设备进行以下同步：

- 状态同步：主设备将其运行状态实时同步至从设备，以使从设备能够在任意时刻接替主设备的管理功能。
- 配置同步：除了状态同步外，还需要同步配置。主要是同步 running-config 与 startup-config。

全局候选设备虽然不参与热备，但在主机上的全局配置文件 config.text 将会同步到其他所有成员设备。这样，即使主从设备都发生故障，将剩余设备进行重启，配置还能够恢复。

成员设备故障恢复

VSU 系统中的成员设备故障有以下几种情况：

1) 如果全局主设备发生故障，VSU 系统将进行热备份主从切换，原全局从设备升级成主设备，接管整个 VSU 组。故障的设备重启，将会重新热加入 VSU 系统。

2) 如果全局从设备发生故障，VSU 系统不会进行热备份主从切换，这时将从其余的全局候选设备中选举中新的全局从设备。故障的设备重启，将会重新热加入 VSU 系统。

3) 如果全局候选设备发生故障，VSU 系统不会进行热备份主从切换。故障的设备重启，将会重新热加入 VSU 系统。

VSU 系统中的设备故障还会对拓扑造成影响。

1) 对于线形拓扑，单台设备的失效将可能造成一个拓扑分裂成两个拓扑。具体情况请参考拓扑变化章节的拓扑分裂部分。

2) 对于环形拓扑，单台设备的失效将可能造成拓扑的“环转线”的变化。具体情况请参考拓扑变化章节的拓扑环线互转部分。

手动热备切换或重启

通过主设备的控制台界面，用户可以执行热备份切换及复位操作。

1) 通过执行 **reload** 命令，整个 VSU 系统将进行复位

2) 通过执行 **reload switch** [*switched*] 或 **redundancy reload shelf** [*switched*]对某台成员进行重启

3) 通过执行 **remove configuration switch** [*switched*] 命令清除某台设备配合，此时该设备自动重启

4) 通过执行 **redundancy reload peer** 命令，则仅仅复位全局从设备。

5) 通过执行 **redundancy forceswitch** 命令，VSU 系统将进行热备份主从切换。

如果当前 VSU 为线形拓扑，对某台设备执行重启命令的时，可能会导致其他设备一起重启。比如拓扑形状为：1-2-3-4，当对设备 3 进行设备重启时，设备 4 也会随之重启，此时会打印提示，等待用户确认后才执行。

13.1.4.6 双主机检测

当 VSL 断开时，从设备切换成主设备，如果原来的主设备还在运行，那么两台设备都是主角色，由于配置完全相同，在局域网中会引起 IP 地址冲突等一系列问题。在这种情况下，VSU 系统必须检测双主机，并且采取恢复措施。VSU 支持使用两种方式进行双主机检测：

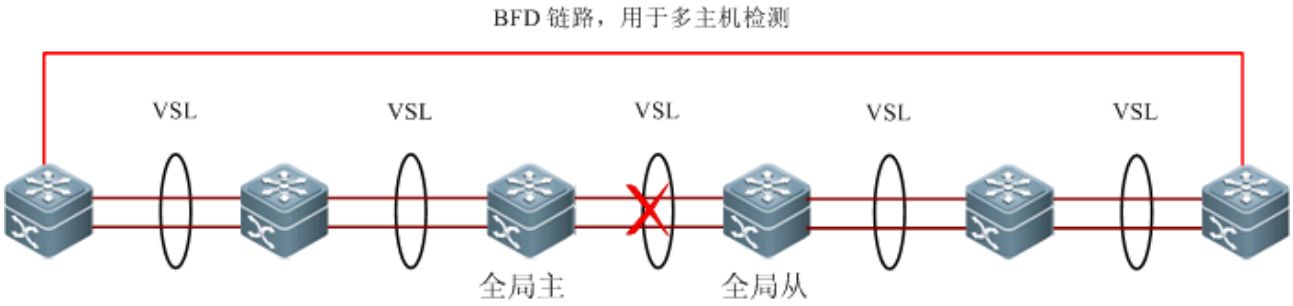
- 基于 BFD 检测
- 基于聚合口检测

基于 BFD 检测

VSU 支持使用 BFD(Bidirectional Forwarding Detection)检测多主机情况。其拓扑连接如图所示。两个边缘设备增加一条链路，专门用于多主机检测。当全局主和全局从之间的 VSL 链路断开，此时会产生两个主机，如果配置了 BFD 双主机检测功能，则两个主机之间通过 BFD 链路互相发送 BFD 双主机检测报文，从而检测到当前有相同的两个主机存在，最后通过一定的规则（同 1.1.4.4 拓扑合并规则）将其中一个主机所在的 VSU 系统关闭，使其进入 recovery 状态，避免网络异常。

基于 BFD 检测功能还专门针对 VSU 双机组网场景提供一种双机快速检测功能：当采用 VSU 双机组网并配置基于 BFD 检测时，一旦发生拓扑分裂，保留原来的主机，从机进入 recovery 状态。实际上，双机快速检测功能对 VSU 拓扑分裂时，原从机所在新拓扑只有 1 台设备，原主机所在新拓扑有 1 台或多台设备这一场景也适用。在符合双机快速检测的场景下，双机快速检测功能优先生效，如果双机快速检测功能失效则多主机检测功能生效。

图 13-11 基于 BFD 的多主机检测



一旦接口配置为 BFD 检测口，会关闭接口的 LLDP 功能。

只有一对 BFD 检测链路时建议将检测链路部署在拓扑的两端。

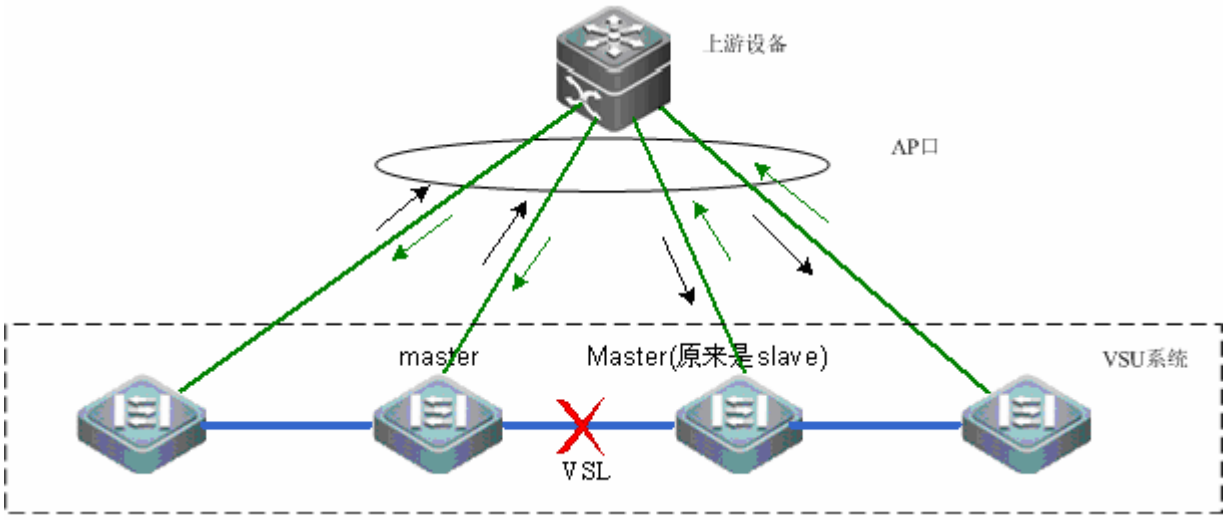
BFD 检测采用扩展 BFD，不能通过现有 BFD 的配置与显示命令配置双主机检测口。

基于聚合口检测

VSU 还支持使用聚合口检测双主机的机制， 其连接拓扑如下图所示。在 VSU 系统和上游设备上，都需要支持基于聚合口的双主机检测功能，当发生 VSL 端口断开后，产生两个主机，两个主机向聚合口的每个成员口发送私有协议报文，该报文通过上游设备进行中转，到另一个主机。如下图所示，聚合口共有四个成员口，每个成员口连接在 VSU 系统的四个不同设

备上，当发生分裂时，四个成员口都会发送和接受双主机检测报文，从而检测到当前有相同的两个主机存在，最后通过一定的规则（同 1.1.4.4 拓扑合并规则）将其中一个主机所在的 VSU 系统关闭，使其进入 recovery 状态，避免网络异常。

图 13-12 基于聚合口双主机检测



以上拓扑中，上游设备必须为锐捷设备，该设备需要支持双主机检测报文的转发。S5750-S 支持转发功能。

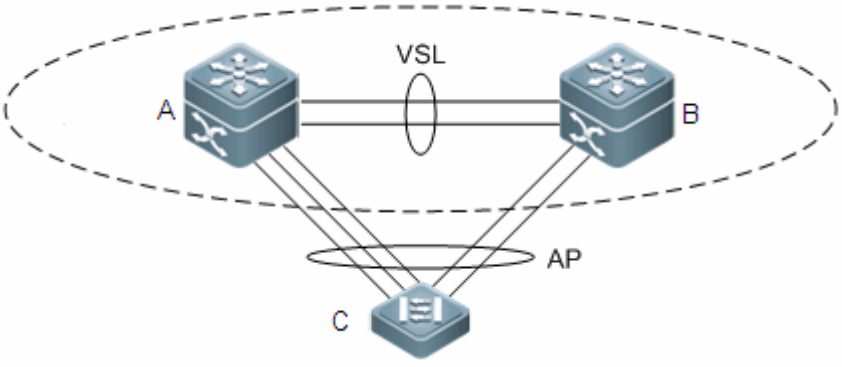
13.1.4.7 VSU设备外部连接

跨设备聚合端口组

AP 把多个物理链接捆绑在一起形成一个逻辑链接。VSU 系统支持跨成员设备的 AP。

如下图所示，设备 A、B 组成 VSU 组，外部的接入设备 C 以 AP 的形式链接到 VSU，对于 C 来说，图中的 AP 连接与普通的聚合端口组没有区别。

图 13-13 跨设备聚合端口



建议配置跨设备 AP 时，外围设备与 VSU 的每台设备之间均有物理链接。一方面，这可以保留 VSL 链路的带宽(跨机箱 AP 流量优先选择同一机箱的 AP 成员作为出口，避免不必要的流量通过 VSL 链路传输)；另一方面，可以提高网络的可靠性(如果某一机箱发生故障，属于正常设备的成员接口还可以正常工作)。

故障处理

以下描述跨设备 AP 可能的失败情形及导致的影响：

- 单条链路发生故障

如果跨设备 AP 的单条链路发生故障而其它链路仍然正常工作，则跨设备 AP 在剩余的正常链路之间重新分配流量。

- 全局主设备上的所有跨设备 AP 成员口链路发生故障

如果全局主设备上的所有跨设备 AP 成员口链路发生故障，则只有其它成员设备的成员口继续工作。由该 AP 进入 VSU 系统的数据流，如果数据流的转发出口在全局主设备上，则系统通过 VSL 链路转发到全局主设备对应的出口。

由于控制面协议仍然运行在全局主设备，所以进入 VSU 系统的协议报文通过 VSL 链路转发到全局主设备进行协议运算。

- 与其他成员设备的所有链路发生故障

如果跨设备 AP 与单台成员设备 A 的所有链路发生故障，则只有其它成员设备的成员口继续工作。由该 AP 进入 VSU 系统的数据流，如果数据流的转发出口在成员设备 A 上，则系统通过 VSL 链路转发到成员设备 A 对应的出口。

- 所有链路发生故障

如果跨设备 AP 的所有链路发生故障，与普通 AP 的处理相同，接口的状态变为 Link-Down。

- 全局主设备整机故障

如果主设备整机发生故障，将导致热备份切换，原来的从设备切换为主设备。同时，其它成员设备上的成员口继续工作。通过该 AP 与 VSU 相连的对端设备将检测到链路故障，调整流量平衡算法，将数据流分配到正常的链路。

- 其它成员设备整机故障

如果成员设备整机发生故障，连接在该成员设备的 AP 成员链路将断开，但其他成员链路照常工作。通过该 AP 与 VSU 相连的对端设备将检测到链路故障，调整流量平衡算法，将数据流转发路径分配到正常的链路。

13.1.4.8 系统管理

控制台访问

VSU 系统主设备的控制台同时管理系统内的多台设备。从设备、候选设备的控制台不支持命令行输入。但用户可以在主机上对指定成员设备进行 VSU 相关的配置，也可以通过从机的串口登录到主机的控制台。

接口命名

VSU 工作模式下，接口的命名方式为：设备编号/槽位号（盒式设备为 0）/端口号。例如：interface gigabitEthernet 1/0/2 表示设备 1 上的千兆端口 2。

访问文件系统

VSU 工作模式下，可以从主设备上访问其他成员设备上的文件系统。具体方式和访问本地文件系统相同。唯一不同的是使用不同的 URL 前缀。

系统升级

VSU 系统通常情况下要求成员设备主程序版本号一致,然而成员设备众多,按照单机模式逐一升级，不仅费时费力，而且容易出错。锐捷交换机提供了完善的系统升级方案,使您能够使用如下两种方法轻松完成系统升级。

- VSU 系统建立时：系统会自动匹配所有成员设备的主程序版本号。当发现主程序版本不一致时，其会选择主设备上的主程序同步到所有成员设备。
- VSU 系统建立后：可以通过 TFTP 下载的文件将自动的同步到所有成员设备。

SYSLOG

VSU 系统的所有成员设备都可以打印 SYSLOG。主机产生的 SYSLOG 直接在主机控制台上打印，且格式和单机情况下是完全一样的；其它成员设备的 SYSLOG 也在主机控制台上打印，但消息格式与单机不同，相比之下增加了设备编号信息。

例如：单机产生的SYSLOG信息是：“%VSU-5-DTM_TOPO_CVG: Node discovery done. Topology converged.”那么由编号为 3 的成员设备产生的 SYSLOG 信息应该就是：“%VSU-5-DTM_TOPO_CVG:(3) Node discovery done. Topology converged.”

13.1.5 典型应用

见简介章节的 VSU 系统部分说明。

13.2 配置VSU

缺省配置

功能特性	缺省值
交换机工作模式	单机模式(standalone)
VSU 模式下的交换机编号(Switch ID)	1
VSU 模式下的交换机优先级	100
VSU 模式下的 VSL 成员端口	无
机箱的备用配置	无

配置步骤

步骤	配置任务	说明
1	单机模式下配置 VSU 参数	必选
2	VSU 模式下配置 VSU 参数	可选
3	预配置成员设备	可选
4	手动热备切换	可选
5	复位设备	可选

13.2.1 单机模式下配置VSU参数

由于交换机默认工作在单机模式，因此在组建 VSU 系统前，用户可以将设备在单机模式下启动，配置 VSU 相关的参数。以下章节描述如何在单机模式下配置 VSU 参数。

13.2.1.1 配置VSU属性

用户需要在构建 VSU 系统的两台机箱上配置相同的域 ID(domain ID)，虚拟设备号取值范在局域网内域 ID 必须是唯一的。用户还需要配置每台机箱在虚拟设备中的编号。交换机缺省以单机模式启动，使用以下命令进行配置：

命令	作用
Ruijie(config)# **switch virtual domain** *domain_id*	配置域 ID，domain_id 范围为 1-255
Ruijie(config-vs-domain)# **switch** *sw_id*	配置交换机在虚拟设备中的编号，sw_id 的范围为 1-8，缺省值为 1。
Ruijie(config-vs-domain)# **switch** *sw_id* **priority** *priority_num*	*priority_num* 优先级取值范围是 1 到 255，缺省值是 100。数值越大，优先级越高。
Ruijie(config-vs-domain)#**switch** *sw_id* **description** *switch1*	配置设备的别名，最大为 32 个字符（可选）
Ruijie(config-vs-domain)# **exit**	退出虚拟设备配置模式

配置注意事项：

1、 配置优先级的命令只会修改优先级，不会修改交换机编号。所以在配置时必须正确输入当前设备的编号。例如，当前已经配置交换机编号为 1，如果输入 switch 2 priority 100，则优先级配置不生效。

2、 配置别名 description 的命令效果与优先级配置命令相同。

13.2.1.2 配置VSL链路

为了组成 VSU 系统，还需要配置哪些端口作为 VSL 成员端口。通过执行以下命令，可以配置交换机的 VSL 成员端口：

命令	作用
Ruijie(config)# **vsl-aggregateport** *ap-num*	VSL 以聚合口形式存在，首先进入 VSL-AP 聚合口的配置模式 ap_num 为 VSL-AP 聚合口的编号，一台设备可以配置 2 个 VSL-AP，取值只能为 1 和 2
Ruijie(config-vsl-ap-1)#[**no**] **port-member interface** *interface-name* [**copper** | **fiber**]	添加或移除 VSL-AP 链路的成员端口。接口模式表示进入 VSL-AP1 链路配置。*interface-name* 为单机模式下的二维端口名称，可以为万兆口，也可以为千兆口（千兆口可以为光电复用口，如果不指定介质类型，则默认为千兆电口）
Ruijie(config-vsl-ap-1)# **exit**	退出 VSL-AP 的配置模式

配置注意事项：

1、 单机模式下，VSL 成员端口的配置不能立即生效，需要转化为 VSU 模式重新启动后才能生效。

2、 属于同一个 VSL-AP 的各成员口的属性必须相同，比如万兆电口只能和万兆电口组成 VSL-AP，不能和千兆电口组成 VSL-AP，也不能和万兆光口组成 VSL-AP。

3、 对于光电复用口，在将其加入 VSL-AP 前，必须显示指定其光电属性。

4、 VSL 口不支持端口的速率自适应，只支持端口的最大能力速率生效。

13.2.1.3 查看和保存VSU参数

单机模式下，可通过以下命令查看当前 VSU 配置：

命令	作用
Ruijie# **show switch virtual config** [*sw_id*]	单机模式下查看当前交换机的 VSU 配置

配置说明：

1、 由于 VSU 相关的配置是针对单个物理设备的，因此 **show running config** 看不到 VSU 相关的配置信息，只能通过 **show switch virtual** config 来查看当前 VSU 的配置。

2、 单机模式下，VSU 运行信息全部空，用户敲入 **show switch virtual** 等命令时，则提示当前为单机模式，无 VSU 系统运行信息。

3、 用户修改设备的 VSU 配置参数后，为了使 VSU 配置参数在设备重启后可以生效，需要执行保存配置命令（write 命令），系统在用户执行保存配置命令后会将设备的 VSU 配置参数写入到设备文件系统根目录下的 VSU 配置文件 config_vsu.dat（如果 config_vsu.dat 文件不存在系统会自动创建）。

为保证VSU配置文件的正确存储与读取，请不要在设备文件系统根目录下创建与 config_vsu.dat 同名的其他文件或目录。如果存在同名的文件，保存 VSU 配置信息时系统将覆盖同名文件，这样可能导致用户创建的同名文件中内容丢失；如果存在同名的目录，会导致系统创建 VSU 配置文件失败。

以下例子显示如何在单机模式下配置和查看 VSU 参数：

```
Ruijie(config)#switch virtual domain 1
Ruijie(config-vs-domain)#switch 1
Ruijie(config-vs-domain)# switch 1 priority 200
Ruijie(config-vs-domain)# switch 1 description buildingA
Ruijie(config-vs-domain)#exit
Ruijie(config)#vsl-aggregateport 1
Ruijie(config-vsl-ap)# port-member interface GigabitEthernet 0/1
Ruijie(config-vsl-ap)# port-member interface GigabitEthernet 0/2
Ruijie(config-vsl-ap)# exit
Ruijie(config)# exit
Ruijie# show switch virtual config
switch_id: 1 (mac: 00d0.f810.3323)
!
switch virtual domain 1
!
switch 1
```

```
switch 1 priority 200
switch 1 description buildingA
!
vsl-aggregateport 1
port-member interface GigabitEthernet 0/1
port-member interface GigabitEthernet 0/2
!
Switch convert mode standalone
!
Ruijie#show switch virtual
Current system is running in “STANDALONE” mode.
```

13.2.1.4 单机模式切换到VSU模式

单机模式下，用户执行切换命令(**switch convert mode virtual**)后，软件自动进行以下动作：

1) 将单机模式下的全局配置文件“config.text”备份为“standalone.text”，以备后用；

2) 清除配置文件“config.text”的内容；

3) 把 VSU 相关的配置写到特殊配置文件“config_vsu.dat”中

如果交换机上存在”virtual_switch.text”文件，则提示用户是否将文件”virtual_switch.text”的内容覆盖到”config.text”(其中，”virtual_switch.text”文件是交换机从 VSU 模式切换到单机模式时对”config.text”的备份文件)，用户可选择”yes”或”no”。 最后交换机进行重启，读取“config_vsu.dat”中的 VSU 参数，以 VSU 模式进行启动。单机模式切换到 VSU 模式的命令如下：

命令	作用
Ruijie# **switch convert mode virtual**	把交换机从单机模式切换到虚拟交换模式，即 VSU 模式

如果当前交换机已经在 VSU 模式，则不允许再次切换到 VSU 模式，即以上命令无效。

以下是从单机模式切换到 VSU 模式的示例：

示例 1：

```
Ruijie# switch convert mode virtual
Do you want to convert switch to virtual mode[yes/no]：yes
Do you want to recover“config.text”from“virtual_switch.text”[yes/no]：yes
```

示例 2：

```
Ruijie# switch convert mode virtual
System is running in virtual mode, can’t convert to virtual mode again.
```

13.2.2 VSU模式下配置VSU参数

如果交换机已经工作在 VSU 模式，此时配置与单机模式下的 VSU 配置有所区别，以下章节描述如何在 VSU 模式下配置 VSU 参数。

- (可选)配置 VSU 属性
- (可选)配置 VSL 链路
- (可选)配置双主机检测
- (可选)配置流量负载均衡
- (可选)VSU 模式切换到单机模式

13.2.2.1 配置VSU属性

VSU 系统运行过程中，用户可以修改主机或从机的域 ID、交换机编号以及优先级，但用户只能登录到 VSU 系统的主机控制台上对以上参数进行修改，从机控制台禁止进入全局配置模式。以下命令显示 VSU 模式下如何修改主机或从机的 VSU 参数。

命令	作用
Ruijie (config)# **switch virtual domain** *domain_id*	进入 domian 配置模式，目前 VSU 系统运行的域 ID 为 *domain_id*
Ruijie(config-vs-domain)#**switch** *sw_id* **domain** *new_domain_id*	该命令将当前编号为 sw_id 的机箱，域 ID 修改为 *new_domain_id*
Ruijie(config-vs-domain)# **switch** *sw_id* **renumber** *new_sw_id*	该命令将当前编号为 sw_id 的交换机，修改其编号为 *new_sw_id*
Ruijie(config-vs-domain)# **switch** *sw_id* **priority** *new_priority_num*	将当前编号为 *sw_id* 的交换机优先级修改为 *new_priority_num*
Ruijie(config-vs-domain)#**switch** *sw_id* **description** *switch1*	配置设备的别名，最大为 32 个字符（可选）
Ruijie(config-vs-domain)# **exit**	退出虚拟设备配置模式
Ruijie# **write**	保存配置到文件
Ruijie# **show switch virtual** [**topology | config**]	显示当前运行的 VSU 信息，拓扑形状，或当前配置的 VSU 参数

命令说明:

1、 以上命令中，除了 **switch** *sw_id* **description** *swi*tch1 命令立即生效，其他配置命令只有在交换机重启后才能生效。

2、 show running config 看不到以上配置，只能通过 show switch virtual [config]查看 VSU 运行信息或配置参数

以下例子描述在 VSU 模式下如何配置和显示 VSU 相关状态和参数：

#1 VSU 模式下原有的运行信息和配置参数显示如下：

```
Ruijie#show switch virtual
Switch_id     Domain_id     Priority     Status     Role         Description
----------------------------------------------------------------------
1(1)          1(1)          100(100)      OK         ACTIVE       switch-1
2(2)          1(1)          100(100)      OK         CANDIDATE    switch-2
3(3)          1(1)          100(100)      OK         STANDBY      switch-3
```

显示内容说明:

1、 以上显示中，前面数值表示当前运行的参数值，括号中的数值为 config_vsu.dat 文件中配置参数。例如，200(200)表示当前运行的优先级和配置优先级都是 200。

2、 成员设备有两种状态：OK 和 recovery

#查看 VSU 组的拓扑信息

```
Ruijie # show switch virtual topology
Introduction: '[num]' means switch num, '(num/num)' means vsl-aggregateport num.

Ring Topology:
[1](1/2)---(2/1)[2](2/2)---(1/1)[1]

Switch[1]: ACTIVE, MAC: 00d0.f822.33d6, Description: Switch1
Switch[2]: STANDBY, MAC: 1234.5678.9003, Description: Switch2
```

上述显示的信息代表 1 号设备的 VSL-AP1 口连接 2 号设备的 VSL-AP1，VSL-AP2 连接 2 号设备的 VSL-AP1；如此类推。

#查看 VSU 配置信息

```
Ruijie#show switch virtual config
switch_id: 1 (mac: 00d0.f810.1111) → 每台交换机的出厂 mac 是不变的
!
switch virtual domain 1
!
switch 1
switch 1 priority 100
switch 1 description switch1
!
vsl-aggregateport 1
port-member interface GigabitEthernet 0/1
port-member interface GigabitEthernet 0/2
!
Switch convert mode virtual
!

switch_id: 2 (mac: 00d0.f810.2222)
!
switch virtual domain 1
!
switch 2
switch 2 priority 100
switch 2 description switch2
!
```

```
vsl-aggregateport 1
port-member interface GigabitEthernet 0/1
port-member interface GigabitEthernet 0/2
!
Switch convert mode virtual
!
switch_id: 3 (mac: 00d0.f810.3333)
!
switch virtual domain 1
!
switch 3
switch 3 priority 100
switch 3 description switch3
!
vsl-aggregateport 1
port-member interface GigabitEthernet 0/1
port-member interface GigabitEthernet 0/2
!
Switch convert mode virtual
!
switch_id: 4 (mac: 00d0.f810.4444)
!
switch virtual domain 1
!
switch 4
switch 4 priority 100
switch 4 description switch4
!
vsl-aggregateport 1
port-member interface GigabitEthernet 0/1
port-member interface GigabitEthernet 0/2
!
Switch convert mode virtual
!
```

#2 修改相关配置，重新进行显示：

```
Ruijie(config)#switch virtual domain 1
Ruijie(config-vs-domain)#switch 1 domain 5
Ruijie(config-vs-domain)#switch 1 renumber 2
Ruijie(config-vs-domain)#switch 1 priority 150
Ruijie(config-vs-domain)#switch 2 domain 6
Ruijie(config-vs-domain)#switch 2 renumber 1
Ruijie(config-vs-domain)#switch 2 priority 250
Ruijie(config-vs-domain)#exit
Ruijie#show switch virtual
```

```
Switch_id     Domain_id     Priority     Status     Role         Description
----------------------------------------------------------------------------
1(2)          1(5)          100(150)     OK         ACTIVE       switch-1
2(1)          1(6)          100(250)     OK         CANDIDATE    switch-2
3(3)          1(1)          100(100)     OK         STANDBY      switch-3

Ruijie#show switch virtual config
switch_id: 1 (mac: 00d0.f810.1111) → MAC 为 1111 的交换机，id 编号修改为 2
!
switch virtual domain 5 → domain id 修改为 5
!
switch 2
switch 2 priority 150 → priority 修改为 150
switch 2 description switch1
!
vsl-aggregateport 1
port-member interface GigabitEthernet 0/1
port-member interface GigabitEthernet 0/2
!
Switch convert mode virtual
!

switch_id: 2 (mac: 00d0.f810.2222) → MAC 为 2222 的交换机，id 编号修改为 1
!
switch virtual domain 6 → domain id 修改为 6
!
switch 1
switch 1 priority 250 → priority 修改为 250
switch 1 description switch2
!
vsl-aggregateport 1
port-member interface GigabitEthernet 0/1
port-member interface GigabitEthernet 0/2
!
Switch convert mode virtual
!
switch_id: 3 (mac: 00d0.f810.3333)
!
switch virtual domain 1
!
switch 3
switch 3 priority 100
switch 3 description switch3
!
vsl-aggregateport 1
```

```
port-member interface GigabitEthernet 0/1
port-member interface GigabitEthernet 0/2
!
Switch convert mode virtual
!
switch_id: 4 (mac: 00d0.f810.4444)
!
switch virtual domain 1
!
switch 4
switch 4 priority 100
switch 4 description switch4
!
vsl-aggregateport 1
port-member interface GigabitEthernet 0/1
port-member interface GigabitEthernet 0/2
!
Switch convert mode virtual
!
```

以上配置修改重启后，只有设备3和设备4 的domain_id为1，其他两台设备不能加入domain_id为1的VSU系统。

13.2.2.2 配置VSL链路

相关命令如下：

命令	作用
Ruijie(config)#**vsl-aggregateport** *sw_id/vsl_ap_num*	其中sw_id表示将要配置交换机的编号，vsl_ap_num表示VSL-AP聚合口的编号，范围为1-2
Ruijie(config-vsl-ap-1/1)#[**no**] **port-member interface** interface-name [**copper** | **fiber**]	添加或移除 VSL-AP 链路成员口。接口模式表示进入编号为1的交换机的VSL-AP1链路配置，interface-name也是二维端口名称。
Ruijie(config-vsl-ap-1/1)# **end**	退出VSL-AP的配置模式
Ruijie# **show switch virtual link** [**port**]	查看当前的VSL-AP运行信息

配置注意事项：

1、 属于同一个VSL-AP的各成员口的属性必须相同。

2、 VSU系统运行过程中，实时配置添加VSL成员端口不会立即生效，必须保存配置并重启配置添加的VSL成员口所在对应设备才能真正生效。在重启对应设备以前，为了防止对系统造成影响，系统会自动清除被配置添加的VSL成员端口对应的物理端口的配置信息并administratively shutdown这个物理端口。

3、 VSU系统运行过程中，实时配置删除VSL成员口不会立即生效，必须保存配置并重启配置删除的VSL成员口所在对应设备才能真正生效。在重启对应设备以前，为了防止对系统造成影响，系统会自动shutdown被配置删除的VSL成

员口对应的物理端口。用户删除已经连接起来的 VSL 成员口会对 VSU 拓扑造成影响，比如影响 VSL 带宽、造成拓扑环转线，甚至拓扑分裂。

4、 添加某个成员端口编号，必须是二维端口号。比如进入 VSL-AP-1/1 配置模式，执行 port-member interface GigabitEthernet 0/1 命令，则表示将全局三维端口 1/0/1 加入编号为 1 的交换机的 VSL-AP1 中。

5、 VSL 口不支持端口的速率自适应，只支持端口的最大能力速率生效。

配置举例：

#1 以下显示当前运行的 VSL-AP 的状态

```
Ruijie#show switch virtual link
VSL-AP    State     Peer-VSL    Rx                  Tx                  Uptime
-------------------------------------------------------------------------------------
1/1       UP        3/2         25398921            25398921            0d,0h,25m
1/2       UP        2/1         50797842            50797842            0d,0h,25m
3/1       UP        2/2         50031614            50031614            0d,0h,25m
3/2       UP        1/1         25015807            25015807            0d,0h,25m
2/1       UP        1/2         50071394            50071394            0d,0h,25m
2/2       UP        3/1         50071394            50071394            0d,0h,25m
```

#2 以下显示 VSL-AP 每个成员口的状态

```
Ruijie# show switch virtual link port
VSL-AP-1/1:
Port                    State     Peer-port               Rx            Tx        Uptime
-------------------------------------------------------------------------------------------------------
GigabitEthernet 1/0/21  OK        GigabitEthernet 2/0/22  171753        171753    0d,0h,25m

VSL-AP-1/2:
Port                    State     Peer-port               Rx            Tx        Uptime
-------------------------------------------------------------------------------------------------------
GigabitEthernet 1/0/22  OK        GigabitEthernet 2/0/21  171753        171753    0d,0h,25m

VSL-AP-2/1:
Port                    State     Peer-port               Rx            Tx        Uptime
-------------------------------------------------------------------------------------------------------
GigabitEthernet 2/0/21  OK        GigabitEthernet 1/0/22  170501        170501    0d,0h,25m

VSL-AP-2/2:
Port                    State     Peer-port               Rx            Tx        Uptime
-------------------------------------------------------------------------------------------------------
GigabitEthernet 2/0/22  OK        GigabitEthernet 1/0/21  170501        170501    0d,0h,25m
```

显示内容说明:

1、 Peer-VSL 表示与 VSL-AP 连接的对端 VSL-AP 的编号。Peer-port 表示与之连接的对端 VSL-AP 的成员口，

2、 VSL-AP 的 State 有两个值：DOWN 和 UP。“DOWN”表示 VSL-AP 当前的协议状态为 Down，VSL-AP 中不存在协议 Up 的成员口，“UP” 表示 VSL-AP 当前的协议状态为 Up，VSL-AP 中至少存在一个协议 Up 的成员口。

3、 Rx/Tx 表示该 VSL-AP/成员端口收发报文的统计值（包个数）

4、 成员端口有四种状态：“DOWN”，“DISABLE”，“UP”，“OK”，“AGED”。“DOWN”表示当前端口物理是 LINK DOWN；“DISABLE”表示当前端口物理连接错误，收发功能被禁用；“UP”表示当前端口物理是 LINK UP，但是还没有检测到对端是有效的 VSL-AP 成员口；“OK”表示端口不但物理上是 LINK UP，而且还检测到对端是一个有效的 VSL-AP 成员口；“AGED”表示端口在“OK”之后，检测心跳超时。

13.2.2.3 配置双主机检测

为了防止产生双主机，需要配置相关的检测机制。双主机检测只能在 VSU 模式下进行配置，单机模式下不允许配置双主机检测机制。

配置 BFD 双主机检测

基于 BFD 的双主机检测，要求在两台机箱之间建立一条直连链路，链路两端的端口必须是物理路由端口。通过以下命令可以配置基于 BFD 的双主机检测：

命令	作用
Ruijie(config)#**interface** *interface-name1*	进入检测接口 1 的接口配置模式
Ruijie(config-if)# **no switchport**	配置检测接口 1 为路由口
Ruijie (config-if)# **end**	退出检测接口 1 的接口配置模式
Ruijie(config)# **interface** *interface-name2*	进入检测接口 2 的接口配置模式
Ruijie(config-if)# **no switchport**	配置检测接口 2 为路由口
Ruijie(config-if)# **end**	退出检测接口 2 的接口配置模式
Ruijie(config)# **switch virtual domain number**	进入虚拟设备配置模式
Ruijie(config-vs-domain)# **dual-active detection bfd**	打开 BFD 双机检测开关，缺省情况下 BFD 双机检测开关是关闭的。
Ruijie(config-vs-domain)# **dual-active bfd interface** interface-name	配置 BFD 双机检测接口。
Ruijie (config-vs-domain)# **exit**	退出虚拟设备配置模式

配置说明：

1、 BFD 检测接口必须是直连的物理路由端口，检测端口必须在不同的设备上。

2、 配置的接口类型没有限制，由于双主机检测链路只用于传输 BFD 报文，流量不大，建议使用千兆口或百兆口作为双主机检测端口。

3、 当配置为双主机的三层路由口被转换为二层交换口(在该接口下执行switchport命令)后，BFD双主机配置将自动清除。

4、 BFD 检测的配置信息不能通过 BFD 的显示命令进行显示，只能通过双主机检测显示命令进行显示。

当 VSU 系统检测出双主机冲突并让其中一堆 VSU 进入 recovery 状态后，用户应该通过修复 VSL 故障方式来解决问题，而不能直接复位那堆进入 recovery 状态的 VSU，否则可能会引起网络上出现双主机冲突。

配置基于聚合口方式双主机检测

要配置基于聚合口检测方式，必须先配置一个 AP 聚合口，然后指定 AP 聚合口为检测口：

命令	作用
Ruijie(config-if)# **port-group** *ap-num*	将物理成员口加入到 AP 聚合口中
Ruijie(config)#**switch virtual domain** *domain_id*	进入 domain 配置模式
Ruijie(config-vs-domain)# **dual-active detection aggregateport**	打开聚合口方式检测开关，缺省情况下开关是关闭的
Ruijie(config-vs-domain)# **dual-active interface** *interface-name*	将聚合口配置为双主机检测口。
Ruijie(config-vs-domain)# **exit**	退出虚拟设备配置模式

要在上下游设备上打开双主机检测报文转发功能，通过以下命令：

命令	作用
Ruijie(config-if)# **dad relay enable**	打开上下游设备接口的双主机检测报文中转功能，该特性默认关闭。

配置说明：建议加入到聚合检测口的物理接口尽量分布在不同设备上。

配置 recovery 模式的例外端口列表

当检测到双主机，其中一台主机必须进入 recovery 模式。Recovery 模式下，需要将所有业务口进行关闭。为了某些特殊用途（如配置一个端口远程登陆管理交换机），用户可以将某些端口配置为在 recovery 模式不关闭的例外端口。配置命令如下：

命令	作用
Ruijie(config)#**switch virtual domain** *domain_id*	进入虚拟设备配置模式
Ruijie(config-vs-domain)#**dual-active exclude interface** interface-name	指定一个在恢复模式不关闭的例外端口。
Ruijie(config-vs-domain)# **exit**	退出虚拟设备配置模式

配置说明：

1、 例外端口必须是路由端口，不能是 VSL 端口。

2、 当例外端口由路由口被转换为交换口(在该接口下执行 switchport 命令)后，该接口关联的例外端口配置将被自动清除。

显示双主机配置与状态

通过以下命令显示当前的双主机配置与运行状态：

命令	作用
Ruijie# **show switch virtual dual-active** { **aggregateport** | **bfd** | **summary** }	查看当前双主机配置信息

以下是显示双主机检测的例子：

#当前双主机检测状态：

```
Ruijie# show switch virtual dual-active summary
BFD dual-active detection enabled: Yes
Aggregateport dual-active detection enabled: NO
Interfaces excluded from shutdown in recovery mode:
GigabitEthernet 1/0/3
GigabitEthernet 1/0/4
In dual-active recovery mode: NO
```

#BFD 双主机检测状态：

```
Ruijie# show switch virtual dual-active bfd
BFD dual-active detection enabled: Yes
BFD dual-active interface configured:
     gigabitEthernet 1/0/1: UP
     gigabitEthernet 2/0/1: UP
     gigabitEthernet 1/0/2: UP
     gigabitEthernet 2/0/2: UP
```

#查看基于聚合口双主机检测状态

```
Ruijie# show switch virtual dual-active aggregateport
Aggregateport dual-active detection enabled: Yes
Aggregateport dual-active interface configured:
     AggregatePort 1:  UP
          GigabitEthernet 1/0/1: UP
          GigabitEthernet 2/0/1: UP
          GigabitEthernet 1/0/2: UP
          GigabitEthernet 2/0/2: UP
DAD relay enable AP list:
     AggregatePort 1
```

所有双主机检测配置在主从机上立即生效，且属于全局配置，show running-config 可以查看。

13.2.2.4 配置流量均衡

配置 AP 本地转发优先模式

AP 成员口可以分布在 VSU 系统的两个机箱上。用户可以根据实际流量情况，使用以下命令配置 AP 的出口流量是否优先从本地成员口进行转发：

命令	作用
Ruijie(config)#**switch virtual domain** *domain_id*	进入虚拟设备配置模式
Ruijie(config-vs-domain)#[**no**] **switch virtual aggregateport-lff enable**	打开/ 关闭 AP 本地转发优先 LFF(Local Forward First)，如果使用 **no** 命令，则变为跨机箱的流量均衡模式。

Ruijie(config-vs-domain)# **exit**	退出虚拟设备配置模式

显示当前流量均衡配置模式

可通过以下命令显示 VSU 系统当前 AP/ECMP 的配置模式：

命令	作用
Ruijie#**show switch virtual balance**	查看当前 VSU 系统流量均衡模式

以下是显示当前流量均衡配置模式的例子：

```
Ruijie#show switch virtual balance
Aggregate port LFF：enable
```

配置说明：

1、 VSU 模式下，默认打开跨机箱 AP 本地转发优先模式。

2、 以上配置立即生效，属于全局配置模式，show running-config 可查看。

3、 三层设备若部署 VSU，建议用户配置基于 IP 的 AP 负载均衡模式（src-ip，dst-ip，src-dst-ip 等）。

13.2.2.5 VSU模式切换到单机模式

如果要将 VSU 系统转换成独立的设备，以单机模式进行工作，可以通过以下命令将 VSU 主机转换成单机模式：

命令	作用
Ruijie# **switch convert mode standalone** [*sw_id*]	sw_id 是将要被转成单机模式的交换机编号，sw_id 是可选的参数。如果不加这个参数，则是将本主机切换到单机模式

用户执行切换命令后，系统将给予提示：是否将配置文件恢复为之前备份的“standalone.text”。如果选“yes”，则将配置文件恢复；如果选“no”，则清除虚拟设备模式的配置。

设备恢复成单机模式后，如果用户在执行转化命令时，选择恢复原有的配置文件时选择了 no，单机模式启动后，还可以通过以下命令恢复 flash 中的单机模式的配置信息：

命令	作用
Ruijie# **copy flash:***standalone.text* **flash:config.text**	将之前保存的 standalone.text 恢复成配置文件
Ruijie# **reload**	重启交换机，重新应用参数文件

13.2.3 清除成员设备配置

用户可以通过 **remove configuration switch** [sw_id]命令清除某台设备的配置，该命令会引起设备重启。

命令	作用
Ruijie(config)# **remove configuration switch** *sw_id*	1. 如果指定的设备已经加入 VSU 系统，那么将从 VSU 系统中对应设备配置清除，并自动重启该设备 2. 删除指定设备的相关配置

13.2.4 手动热备切换

执行热备相关的命令可以指定复位从设备或者复位整个 VSU 组。

命令	作用
Ruijie# **redundancy forceswitch**	进行主从设备的热备切换；原主设备将进行重启，从设备升级为主设备

13.2.5 复位设备

用户还可以执行其它名来来复位指定的成员设备：

命令	作用
Ruijie# **reload switch** *sw_id*	对编号为 sw_id 的成员设备进行复位
Ruijie# **reload**	对整个 VSU 组都进行复位

执行热备相关的命令可以指定复位从设备或者复位某台 VSU 成员设备：

命令	作用
Ruijie# **redundancy reload** { **peer** | **shelf** *sw_id* }	peer 是仅复位从设备 shelf 是对编号为 sw_id 的设备进行复位重启 注：sw_id 只在 VSU 模式中才有

在 VSU 系统中，如果复位某台指定的设备，可能会导致拓扑分裂，对系统造成比较大的影响。为了避免这种风险，VSU 对复位某个特定的设备进行提醒。

1、 如果当前是环形拓扑，则可以自由复位任何一台设备，因为该不会导致拓扑分裂，只是从环形拓扑变为线性拓扑。

2、 如果当前为线性拓扑，如果复位处于拓扑边缘的设备，不会引起拓扑分裂。如果复位处于拓扑中间的设备，比如当前线形拓扑连接方式为：设备 1(主)--设备 2(备选)--设备 3(从)--设备 4(备选)，此时只能复位设备 1 或设备 4，如果复位设备 2 或设备 3，将会造成到主机设备 1 不可达的其他设备变为不可用，系统将会提示，用户确认后才进行复位。

可以导致某台设备复位的命令：

1、 **redundancy forceswitch**：手动进行热备切换

2、 **redundancy reload peer**：热备复位对端从设备

3、 **redundancy reload shelf** <*switch_id*>：热备指定复位某台设备

4、 **reload switch** <*switch_id*>：重启某台设备

5、 **remove configuration switch** <*switch_id*>：清除某台设备配置

13.2.6 版本升级

VSU 系统的版本升级方法同普通设备的升级方法相同，可以直接参考《系统升级》配置指南与命令参考手册。

VSU 版本升级注意事项：

1、 只有 copy tftp/xmodem 命令升级主设备的时候，才会自动同步到所有成员设备。如果使用其他命令将安装包拷贝到主设备上，必须先使用 upgrade system 命令手动同步到其他成员设备。否则，整机重启后，原先的主设备因为主从选举的优先级关系，可能变成从设备，导致该设备上升级的版本又会被新的主设备以自动同步的方式降回去。

2、 在使用 copy tftp 命令下载升级安装包时，在 tftp 下载过程和从设备升级过程中，只要一出现错误，整个升级过程立即停止，主设备上的主程序也不会被替换。因此，为了确保升级成功，在升级过程不要执行会导致设备复位的命令。在升级结束后，如果出现升级失败的提示，用户应该仔细观察升级过程中出现的错误提示，并按照提示进行人工干预处理，再重新执行 copy tftp 命令升级主程序。从设备升级过程常见错误：

1）提示内存不足。处理方式：减少配置，或重启一些应用，以恢复内存剩余量。

2）提示通信超时或通信出错。处理方式：检查 VSU 系统的连线，或通信错误的从设备是否存在故障。

3) 提示从设备文件系统空间不足。处理方式：使用跨设备文件系统访问命令删除从设备 flash 上的部分文件。

13.2.7 设备替换

VSU 支持对型号完全相同的设备进行在线替换。

用户在替换设备前，要确保新设备的 VSU 配置参数与被替换设备的 VSU 配置参数相同。如果 VSU 配置参数不同，可能会导致替换失败。

如果用来替换的新设备的设备型号与被替换的设备型号不完全相同，可能会导致正在运行的配置信息(**show running-config**)丢失。万一出现这种情况，可以尝试使用 **copy startup-config running-config** 命令来恢复丢失的配置。关于 **copy startup-config running-config** 命令的使用指导，详见《文件系统》对应的配置指南和命令参考手册。

13.3 监视与维护

命令	作用
Ruijie# **show switch virtual** [**topology** | **config**]	显示当前运行的 VSU 信息，拓扑形状，或当前配置的 VSU 参数
Ruijie#**show switch virtual dual-active** { **aggregateport** | **bfd** | **summary** }	查看当前双主机配置信息
Ruijie# **show switch virtual link** [**port**]	VSU 模式下查看当前的 VSL-AP 运行信息
Ruijie# **session** { **device** | **master**}	重定向到其他设备的控制台，以查看对应设备的运行状态

13.4 配置举例

13.4.1 VSU典型配置

组网需求

1) Switch 1 和 Switch 2 组成虚拟设备 VSU(domain ID 为 1)，Switch 1 的优先级是 200，Switch 2 的优先级是 150。Switch 1 的 Te1/1/1，Te1/1/2 与 Switch 2 的 Te2/1/1,Te2/1/2 分别建立链接，组成 Switch 1 和 Switch 2 之间的 VSL 链路。

2) Switch A 的端口 G0/1，G0/2，G0/3 和 G0/4 等 4 个端口分别与 Switch 1 的 G1/0/1 和 G1/0/2，以及 Switch 2 的 G2/0/1 和 G2/0/2 建立连接，并构成一个包含 4 个成员链路的聚合端口组，聚合端口组的 ID 是 1。

3) VSU 配置了三层接口 VLAN1，IP 地址是 1.1.1.1/24。

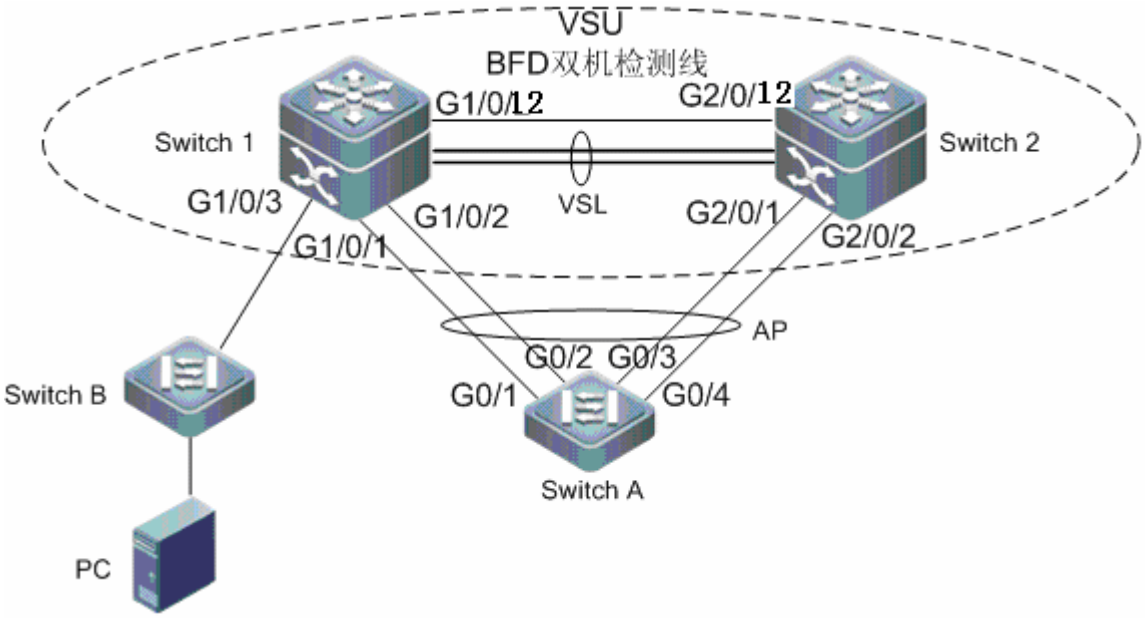
4) Switch A 配置了三层接口 VLAN2，IP 地址是 1.1.1.2/24。

5) 采用基于 BFD 或聚合口来检测双主机。

6) G1/0/2 和 G2/0/2 是一对 BFD 心跳接口，IP 地址分别是 2.1.1.1/32 和 2.1.2.1/32。

组网拓扑

图 13-14 VSU 组网拓扑



配置要点

1) 先正确配置设备的 VSU 参数，并依据配置正确连接 VSL 链路。

2) 设备上电后，系统组成 VSU。

3) 配置 VSU 系统的业务。

配置步骤

1) 配置 Switch1

#在 Switch1 配置 VSU 域标识，设备编号和优先级

```
Switch1# configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
Switch1(config)# switch virtual domain 1
Switch1(config-vs-domain)# switch 1
Switch1(config-vs-domain)# switch 1 priority 200
Switch1(config-vs-domain)# switch 1 description switch1
Switch1(config-vs-domain)# exit
Switch1(config)# vsl-aggregateport 1
Switch1(config-vsl-ap-1)# port-member interface TenGigabitEthernet 1/1
Switch1(config-vsl-ap-1)# port-member interface TenGigabitEthernet 1/2
Switch1(config-vsl-ap-1)# exit
Switch1(config)# exit
```

2) 配置 Switch2

#在 Switch2 配置 VSU 域标识，设备编号和优先级

```
Switch2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch2(config)# switch virtual domain 1
Switch2(config-vs-domain)# switch 2
Switch2(config-vs-domain)# switch 2 priority 150
Switch1(config-vs-domain)# switch 2 description switch2
Switch2(config-vs-domain)# exit
Switch1(config)# vsl-aggregateport 1
Switch1(config-vsl-ap-1)# port-member interface TenGigabitEthernet 1/1
Switch1(config-vsl-ap-1)# port-member interface TenGigabitEthernet 1/2
Switch1(config-vsl-ap-1)# exit
Switch2(config)# exit
```

3) 把 Switch1 和 Switch2 转换到 VSU 模式

```
Switch1# switch convert mode virtual
Switch2# switch convert mode virtual
```

4) 配置 VSU

#在 VSU 上配置端口聚合组 1

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# interface aggregateport 1
Ruijie(config-if)# interface GigabitEthernet 1/0/1
Ruijie(config-if)# port-group 1
Ruijie(config-if)# interface GigabitEthernet 1/0/2
Ruijie(config-if)# port-group 1
Ruijie(config-if)# interface GigabitEthernet 2/0/1
Ruijie(config-if)# port-group 1
Ruijie(config-if)# interface GigabitEthernet 2/0/2
Ruijie(config-if)# port-group 1
```

5) 配置 Switch A

```
SwitchA# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)# interface aggregateport 1
SwitchA(config-if)# interface range GigabitEthernet 0/1-4
SwitchA(config-if)# port-group 1
```

6) 配置 SVI

#在 VSU 上 SVI 1

```
Ruijie(config)# interface vlan 1
Ruijie(config-if)#ip address 1.1.1.1 255.255.255.0
```

#在 Switch A 上 SVI 1

```
SwitchA(config)# interface vlan 1
SwitchA(config-if)#ip address 1.1.1.2 255.255.255.0
```

7) 配置 BFD 双机检测接口

```
Ruijie(config)# interface GigabitEthernet 1/0/12
Ruijie(config-if)# no switchport
Ruijie(config)# interface GigabitEthernet 2/0/12
Ruijie(config-if)# no switchport
Ruijie(config-if)# switch virtual domain 1
Ruijie(config-if)# dual-active detection bfd
Ruijie(config-vs-domain)# dual-active bfd interface GigabitEthernet 1/0/12
Ruijie(config-vs-domain)# dual-active bfd interface GigabitEthernet 2/0/12
```

8) 配置基于聚合口方式双主机检测

#在 VSU 系统配置：

```
Ruijie(config)# switch virtual domain 1
Ruijie(config-vs-domain)# dual-active detection aggregateport
Ruijie(config-vs-domain)# dual-active interface aggregateport 1
Ruijie(config-vs-domain)# exit
```

#在 Switch A 上配置：

```
SwitchA(config)#interface aggregateport 1
SwitchA(config-if-AggregatePort 1)# dad relay enable
SwitchA(config-if-AggregatePort 1)# exit
```

显示验证

#查看 VSU 的基本信息

```
Ruijie#show switch virtual
Switch_id     Domain_id     Priority      Status     Role         Description
```

```
-------------------------------------------------------------------------------------------------
1(1)          1(1)          200(200)      OK          ACTIVE       switch1
2(2)          1(1)          150(150)      OK          STANDBY      switch2

Ruijie#show switch virtual config
switch_id: 1 (mac: 00d0.f810.1111)
!
switch virtual domain 1
!
switch 1
switch 1 priority 200
!
vsl-aggregateport 1
port-member interface TenGigabitEthernet 1/1
port-member interface TenGigabitEthernet 1/2
!
Switch convert mode virtual
!

switch_id: 2 (mac: 00d0.f810.2222)
!
switch virtual domain 1
!
switch 2
switch 2 priority 150
!
vsl-aggregateport 1
port-member interface TenGigabitEthernet 1/1
port-member interface TenGigabitEthernet 1/2
!
Switch convert mode virtual
!
```

#查看 VSL 状态信息

```
Ruijie#show switch virtual link
VSL-AP   State    Peer-VSL   Rx                  Tx                  Uptime
-------------------------------------------------------------------------------------------
1/1      UP       2/1        25398921            25398922            0d,0h,25m
2/1      UP       1/1        25398922            25398921            0d,0h,25m

Ruijie# show switch virtual link port
VSL-AP-1/1:
Port                        State    Peer-port                  Rx           Tx       Uptime
-------------------------------------------------------------------------------------------------------------
TenGigabitEthernet 1/1/1    OK       TenGigabitEthernet 2/1/1   1717531      1717532  0d,0h,25m
```

```
TenGigabitEthernet 1/1/2    OK       TenGigabitEthernet 2/1/2    1717531       1717531   0d,0h,25m

VSL-AP-2/1:
Port                        State    Peer-port                   Rx            Tx        Uptime
------------------------------------------------------------------------------------------------------------
TenGigabitEthernet 2/1/1    OK       TenGigabitEthernet 1/1/1    1717531       1717532   0d,0h,25m
TenGigabitEthernet 2/1/2    OK       TenGigabitEthernet 1/1/2    1717531       1717531   0d,0h,25m
```

#查看双主机箱配置状态

```
Ruijie# show switch virtual dual-active summary
BFD dual-active detection enabled: Yes
Aggregateport dual-active detection enabled: Yes
Interfaces excluded from shutdown in recovery mode:
In dual-active recovery mode: NO
```

#查看 BFD 双主机箱检测配置

```
Ruijie# show switch virtual dual-active bfd
BFD dual-active detection enabled: Yes
BFD dual-active interface configured:
     GigabitEthernet 1/0/12: UP
     GigabitEthernet 1/0/12: UP
```

#查看聚合口方式双主机箱检测配置

```
Ruijie# show switch virtual dual-active aggregateport
Aggregateport dual-active detection enabled: Yes
Aggregateport dual-active interface configured:
     AggregatePort 1:  UP
          GigabitEthernet 1/0/1: UP
          GigabitEthernet 1/0/2: UP
          GigabitEthernet 2/0/1: UP
          GigabitEthernet 2/0/2: UP
```

#查看流量均衡模式

```
Ruijie#show switch virtual balance
Aggregate port LFF：disable
```

#查看 VSU 组的拓扑信息

```
Ruijie# show switch virtual topology
Introduction: '[num]' means switch num, '(num/num)' means vsl-aggregateport num.

Chain Topology:
[1](1/1)---(2/2)[2]

Switch[1]: ACTIVE, MAC: 00d0.f822.33d6, Description: switch1
```

```
Switch[2]: STANDBY, MAC: 1234.5678.9003, Description: switch2
```

配置指南-网管和监控

本分册介绍网管和监控配置指南相关内容，包括以下章节：

1. SNMP
2. RMON
3. NTP
4. SNTP
5. SPAN
6. RSPAN
7. IPFIX

1 SNMP

1.1 SNMP相关知识

1.1.1 概述

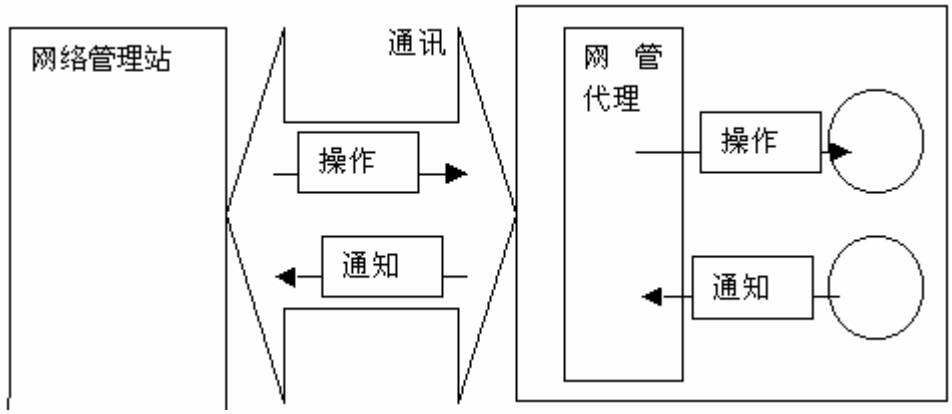
SNMP 是 Simple Network Management Protocol（简单网络管理协议）的缩写，在 1988 年 8 月就成为一个网络管理标准 RFC1157。到目前，因众多厂家对该协议的支持，SNMP 已成为事实上的网管标准，适合于在多厂家系统的互连环境中使用。利用 SNMP 协议，网络管理员可以对网络上的节点进行信息查询、网络配置、故障定位、容量规划，网络监控和管理是 SNMP 的基本功能。

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。

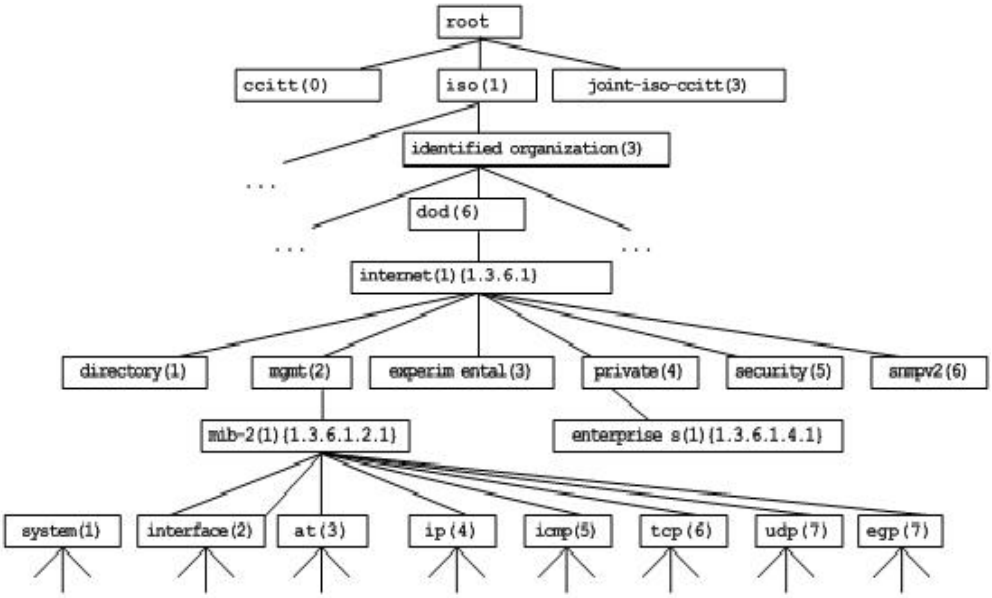
NMS 和 Agent 的关系可以用如下的图来表示：

图 1-1 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。

图 1-2 MIB 树形层次结构



1.1.2 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。

1.1.3 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。

4) Get-next-request 操作：NMS 从 Agent 提取一个或多个参数的下一个参数值。

5) Get-bulk 操作：NMS 从 Agent 提取批量的参数值；

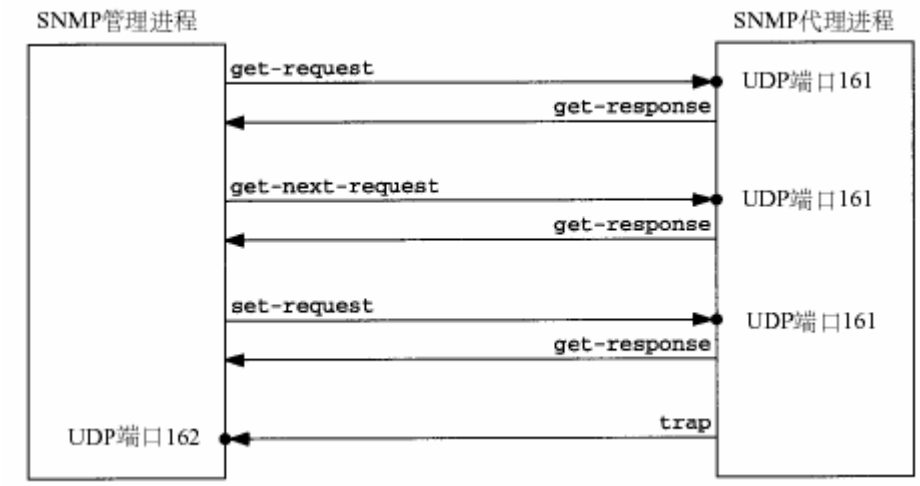
6) Set-request 操作：NMS 设置 Agent 的一个或多个参数值。

7) 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。

8) 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）。下图描述了这几种种操作。

图 1-3 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。

1.1.4 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

1.1.5 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 SnmpEngineID。

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。

1.2 SNMP的配置

SNMP 的配置工作在网络设备的全局配置模式下完成，在进行 SNMP 配置前，请先进入全局配置模式。

1.2.1 设置认证名及访问权限

SNMPv1/SNMPv2C 采用基于共同体（Community-based）的安全方案，SNMP 代理只接受来自相同认证名（Community-String）的管理操作，与网络设备的认证名不符的 SNMP 报文将不被响应，直接丢弃。认证名相当于 NMS 和 Agent 之间的密码。

可以设置访问列表关联，只有指定的 IP 地址的 NMS 可以管理；

可以设定该共同体的操作权限，是 ReadOnly（只读）还是 ReadWrite（读写）；

指定视图的名称，用于基于视图的管理。默认没有指定视图，即允许访问 所有 MIB 对象；

可以指明能够使用该认证名的管理者的 IP。 若不指明，则表示不限制使用该认证名的管理者的 IP 地址。缺省为不限制使用该认证名的管理者的 IP 地址；

要配置 SNMP 认证名，在全局配置模式下执行如下命令：

命令	作用
Ruijie(config)# **snmp-server community** [**0**|**7**] *string* [view *view-name*] **[ro | rw] [host** *host-ip*] [**ipv6** *ipv6-aclname*][*aclnum* | *aclname*]	设置认证名和权限。

可以配置一条或者多条指定，来指定多个不同的共同体名称，使得网络设备可以供不同的权限的 NMS 的管理，要删除共同体名称和权限，在全局配置模式下，执行 **no snmp-server community** [**0**|**7**] *string* 命令。

关键字“**0**”和“**7**”代表团体名字符串的加密类型。团体名字符串之前使用关键字“**0**”代表输入的团体名为明文，使用关键字“**7**” 代表输入的团体名为密文，不使用加密类型团体名默认为明文。配置 **service password-encryption** 命令后，团体名字符串（Community-String）将进行加密的显示和存放。此时取消 **service password-encryption** 配置后，团体字符串仍然以密文显示和存放，不会恢复为明文。

1.2.2 设置SNMP协议端口

SNMP 协议默认使用 161 UDP 端口接收 SNMP 报文；基于安全考虑，用户可自定义使用的 UDP 端口。

要配置 SNMP 协议端口号，在全局配置模式下执行如下命令：

命令	作用
Ruijie(config)# **snmp-server udp-port** *port-num*	设置 SNMP 协议接收报文的 UDP 端口号。

使用 **no snmp-server udp-port** 命令恢复使用默认端口。

1.2.3 配置MIB视图和组

可以使用基于视图的访问控制模型来判定一个操作关联的管理对象是否在视图允许之内或被排除在外，只有在视图允许之内的管理对象才被允许访问。在进行控制时，一般是将某些用户和一个组关联，再将某个组与某个视图关联。一个组内的用户具有相同的访问权限。

可以设置包含视图和排除视图；

可以为一组用户设置只读的视图和可写的视图；

如果是 SNMPv3 的用户，可以为其指定使用的安全级别，是否需要进行认证、是否需要进行加密；

要配置 MIB 视图和组，在全局配置模式下执行如下命令：

命令	作用
Ruijie(config)# **snmp-server view** *view-name oid-tree* {**include** | **exclude**}	创建一个 MIB 视图，包含或排除关联的 MIB 对象。

Ruijie(config)# **snmp-server group** *groupname* {**v1** | **v2c** |**v3** {**auth** | **noauth** | **priv**}} [**read** *readview*] [**write** *writeview*] [**access** {[**ipv6** *ipv6_aclname*] [*aclnum* | *aclname*] }]	创建一个组，并和视图关联。

使用 **no snmp-server view** *view-name* 命令来删除一个视图，或者使用 **no snmp-server view** *view-name oid-tree* 命令在一个视图中删除一棵子树。也可以使用 **no snmp-server group** *groupname* {**v1 | v2c | v3** }命令来删除一个组。

1.2.4 配置SNMP用户

可以使用基于用户的安全模型来进行安全管理，基于用户的管理必须事先配置用户的信息，NMS 只有使用合法的用户才能同代理进行通信。

对于 SNMPv3 用户，可以指定安全级别、认证算法（MD5 或 SHA）、认证口令、加密算法（目前只有 DES）和加密口令；

要配置 SNMP 用户，在全局配置模式下执行如下命令：

命令	作用
Ruijie(config)# **snmp-server user** *username roupname* {**v1 | v2c | v3 [encrypted] [auth { md5|sha }** *auth-password*] [**priv des56** *priv-password*] } [**access** {[**ipv6** *ipv6_aclname*] [*aclnum* | *aclname*] }]	设置用户信息。

通过 **no snmp-server user** *username groupname* {**v1 | v2c | v3** } 删除指定用户。

1.2.5 配置SNMP主机地址

Agent 在特定的情况下，也会主动的向 NMS 发送消息，要配置 Agent 主动发送消息的 NMS 主机地址，在全局配置模式下，执行如下指令：

命令	作用
Ruijie(config)# **snmp-server host** { *host-addr* | ipv6 *ipv6-addr* } [**vrf** *vrfname*] [**traps**] [**version** { **1 | 2c | 3** { **auth | noauth | priv** }] *community-string* [**udp-port** *port-num*] [*notification-type*]	设置 SNMP 主机地址，主机端口，vrf 选项，消息类型，认证名（在 SNMPv3 下是用户名）、安全级别（仅 SNMPv3 支持）等

1.2.6 设置SNMP代理参数

可以对 SNMP 的 Agent 的基本参数进行配置，设置设备的联系方式、设备位置、序列号的信息，NMS 通过访问设备的这些参数，便可以得知设备的联系人，设备所在的物理位置等信息。

要配置 SNMP 代理参数，在全局配置模式下，执行如下指令：

命令	作用
Ruijie(config)# **snmp-server contact** *text*	设置系统的联系方式
Ruijie(config)# **snmp-server location** *text*	设置系统的位置

Ruijie(config)# **snmp-server chassis-id** *number*	设置系统的序列码

1.2.7 定义SNMP代理最大数据报文长度

为了减少对网络带宽的影响，可以定义 SNMP 代理的数据包的最大长度。在全局配置模式下，执行如下指令：

命令	作用
Ruijie(config)# **snmp-server packetsize** *byte-count*	设置最大代理数据包大小

1.2.8 屏蔽SNMP代理

SNMP 代理服务是锐捷产品提供的一个服务，默认是启动的，在不需要代理服务的时候，可以通过如下方式屏蔽 snmp 代理功能以及相关配置信息；屏蔽 snmp 代理功能，在全局配置模式下，执行如下指令：

命令	作用
Ruijie(config)# **no snmp-server**	屏蔽 SNMP 代理服务

1.2.9 关闭SNMP代理

不同于屏蔽命令，锐捷产品提供了关闭 snmp 代理的命令，该命令会直接关闭 snmp 所有服务（相当于 snmp 代理功能被禁用了，不接收报文、不发送响应报文及 trap），但是不会屏蔽代理的配置信息；要关闭 SNMP 代理服务，在全局配置模式下，执行如下指令：

命令	作用
Ruijie(config)# **no enable service snmp-agent**	关闭 SNMP 代理服务

1.2.10 配置SNMP日志功能

SNMP 日志功能主要是记录 NMS 对 SNMP Agent 的 GET、GET-NEXT 和 SET 操作。缺省情况下，SNMP 日志开关处于关闭状态。要开启记录 get、set 操作的日志功能，get 开关控制 GET、GET-NEXT 操作记录，set 开关控制 SET 操作记录，在全局配置模式下，执行如下指令：

命令	作用
Ruijie(config)#**snmp-server logging { get-operation | set-operation }**	开启记录 get、set 操作的日志功能

1.2.11 配置Agent主动向NMS发送Trap消息

Trap 是 Agent 不经请求主动向 NMS 发送的消息，用于报告一些紧急而重要的事件的发生。缺省是不允许 Agent 主动发送 Trap 消息，如果要允许，在全局配置模式下，执行如下指令：

命令	作用
Ruijie(config)# **snmp-server enable traps** [*type*] [*option*]	允许 Agent 主动发送 Trap 消息

Ruijie(config)# **no snmp-server enable traps** [*type*] [*option*]	禁止 Agent 主动发送 Trap 消息

1.2.12 Link Trap策略配置

在设备中可以基于接口配置是否发送该接口的 LinkTrap，当功能打开时，如果接口发生 Link 状态变化，SNMP 将发出 LinkTrap，反之则不发。缺省情况下，该功能打开。

命令	作用
Ruijie(config)# **interface** *interface-id*	进入端口配置模式
Ruijie(config-if)# [**no**] **snmp trap link-status**	打开或者关闭发送该接口 link trap 的功能.

下面配置将配置接口为不发送 Link trap:

```
Ruijie(config)# interface gigabitEthernet 1/1
Ruijie(config-if)# no snmp trap link-status
```

1.2.13 配置发送消息操作的参数

可以指定 Agent 发送 Trap 消息的一些参数，执行如下指令来设置：

命令	作用
Ruijie(config)# **snmp-server trap-source** *interface*	指定发送 Trap 消息的源接口
Ruijie(config)# **snmp-server queue-length** *length*	指定每个 Trap 消息报文的队列长度
Ruijie(config)# **snmp-server trap-timeout** *seconds*	指定发送 Trap 消息的时间间隔

1.3 SNMP的监控与维护

1.3.1 查看当前的SNMP状态

为了监控 SNMP 状态和排除 SNMP 配置中的一些故障，锐捷产品提供了 SNMP 的监控指令，可以方便的查看当前网络设备的 SNMP 的状态，在特权用户模式下，执行 **show snmp** 来查看当前的 SNMP 状态。

```
Ruijie# show snmp
Chassis: 1234567890 0987654321
2381 SNMP packets input
5 Bad SNMP version errors
6 Unknown community name
0 Illegal operation for community name supplied
0 Encoding errors
9325 Number of requested variables
0 Number of altered variables
31 Get-request PDUs
2339 Get-next PDUs
```

```
0 Set-request PDUs
2406 SNMP packets output
0 Too big errors (Maximum packet size 1500)
4 No such name errors
0 Bad values errors
0 General errors
2370 Get-response PDUs
36 SNMP trap PDUs
SNMP global trap: disabled
SNMP logging: enabled
SNMP agent: enabled
```

.对于上述的统计报文信息的解释见下表：

显示信息	描述
Bad SNMP version errors	SNMP 版本不对
Unknown community name	不能识别的认证名称
Illegal operation for community name supplied	非法操作
Encoding errors	编码错误
Get-request PDUs	Get-request 报文
Get-next PDUs	Get-next 报文
Set-request PDUs	Set-request 报文
Too big errors (Maximum packet size 1500)	响应报文太大
No such name errors	不存在指定的管理单元
Bad values errors	设定值类型错误
General errors	一般性错误
Get-response PDUs	Get-response 报文
SNMP trap PDUs	SNMP trap 报文

1.3.2 查看当前SNMP代理支持的MIB对象

在特权用户模式下，执行 **show snmp mib** 来查看当前的代理支持的 MIB 对象。

```
Ruijie# show snmp mib
sysDescr
sysObjectID
sysUpTime
sysContact
sysName
sysLocation
sysServices
sysORLastChange
snmpInPkts
snmpOutPkts
…
```

1.3.3 查看SNMP用户

在特权用户模式下，执行 **show snmp user** 来查看当前代理上配置的 SNMP 用户。

```
Ruijie# show snmp user
User name: test
Engine ID: 800013110300000000000
storage-type: permanent     active
Security level: auth priv
Auth protocol: SHA
Priv protocol: DES
Group-name: g1
```

1.3.4 查看SNMP视图和组

在特权用户模式下，执行 **show snmp group** 来查看当前代理上配置的组。

```
Ruijie# show snmp group
groupname: g1
securityModel: v3
securityLevel:authPriv
readview: default
writeview: default
notifyview:
groupname: public
securityModel: v1
securityLevel:noAuthNoPriv
readview: default
writeview: default
notifyview:
groupname: public
securityModel: v2c
securityLevel:noAuthNoPriv
readview: default
writeview: default
notifyview:
```

在特权用户模式下，执行 show snmp view 来查看当前代理上配置的视图。

```
Ruijie# show snmp view
default(include) 1.3.6.1
test-view(include) 1.3.6.1.2.1
```

1.3.5 查看用户配置的主机信息

在特权用户模式下，执行 **show snmp host** 来查看当前代理上用户配置的主机信息。

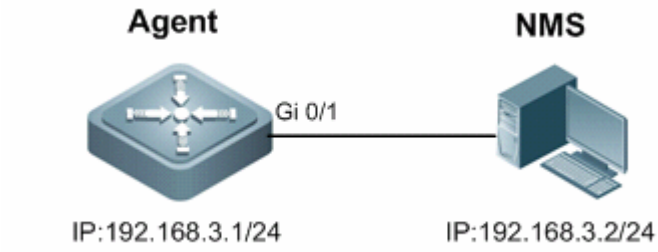
```
Ruijie# show snmp host
Notification host: 192.168.64.221
udp-port: 162   type: trap
user: public    security model: v1
Notification host: 2000:1234::64
udp-port: 162   type: trap
user: public    security model: v1
```

1.4 SNMP典型配置用例

1.4.1 SNMP v1/v2 配置用例

拓扑图

图 1-4 SNMP v1/2 应用拓扑



应用需求

1) 网管工作站（NMS）基于共同体认证模式对网络设备（Agent）进行管理，网络设备能够控制共同体访问指定 MIB 对象的操作权限（可读或可写），例如：某共同体“user1”只能读写 System（1.3.6.1.2.1.1）节点下的对象。

9) 网络设备仅允许特定 IP（例如：192.168.3.2/24）的网管工作站对网络设备进行管理。

10) 网络设备能够主动向网管工作站发送消息。

11) 网管工作站能够获取设备的基本系统信息，如系统的联系方式、位置、序列码。

配置要点

1) 通过创建 MIB 视图，并关联设置认证名（Community）及访问权限（Read 或 Write），即可实现第一个应用需求。

12) 在设置认证名及访问权限的同时，设置访问控制列表关联或指明使用该认证名的管理者的 IP，即可实现第二个应用需求（本例采用关联访问控制列表）。

13) 配置 SNMP 主机地址，并使能 Agent 主动发送 Trap 消息的功能。

14) 配置 SNMP 代理的参数信息。

配置步骤

第一步，配置 MIB 视图和访问控制列表。

！创建一个 MIB 视图名“v1”，包含关联的 MIB 对象（1.3.6.1.2.1.1）。

```
Ruijie(config)#snmp-server view v1 1.3.6.1.2.1.1 include
```

！创建访问控制列表名“a1”，允许 IP 地址为 192.168.3.2/24。

```
Ruijie(config)#ip access-list standard a1
Ruijie(config-std-nacl)#permit host 192.168.3.2
Ruijie(config-std-nacl)#exit
```

第二步，配置认证名及访问权限。

！配置 Community 为“user1”，关联 MIB 视图“v1”可写，以及关联访问控制列表“a1”。

```
Ruijie(config)#snmp-server community user1 view v1 rw a1
```

第三步，配置 Agent 主动向 NMS 发送消息。

！配置 SNMP 主机地址为 192.168.3.2，消息格式为 Version 2c，认证名为“user1”。

```
Ruijie(config)#snmp-server host 192.168.3.2 traps version 2c user1
```

！使能 Agent 主动发送 Trap 消息。

```
Ruijie(config)#snmp-server enable traps
```

第四步，配置 SNMP 代理参数。

！配置系统所处的位置。

```
Ruijie(config)#snmp-server location fuzhou
```

！配置系统的联系方式。

```
Ruijie(config)#snmp-server contact ruijie.com.cn
```

！配置系统的序列码。

```
Ruijie(config)#snmp-server chassis-id 1234567890
```

第五步，配置 Agent 的 IP 地址。

！配置 Gi 0/1 的接口地址为 192.168.3.1/24。

```
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-gigabitEthernet 0/1)#ip address 192.168.3.1 255.255.255.0
Ruijie(config-if-gigabitEthernet 0/1)#exit
```

验证结果

第一步，查看设备的配置信息。

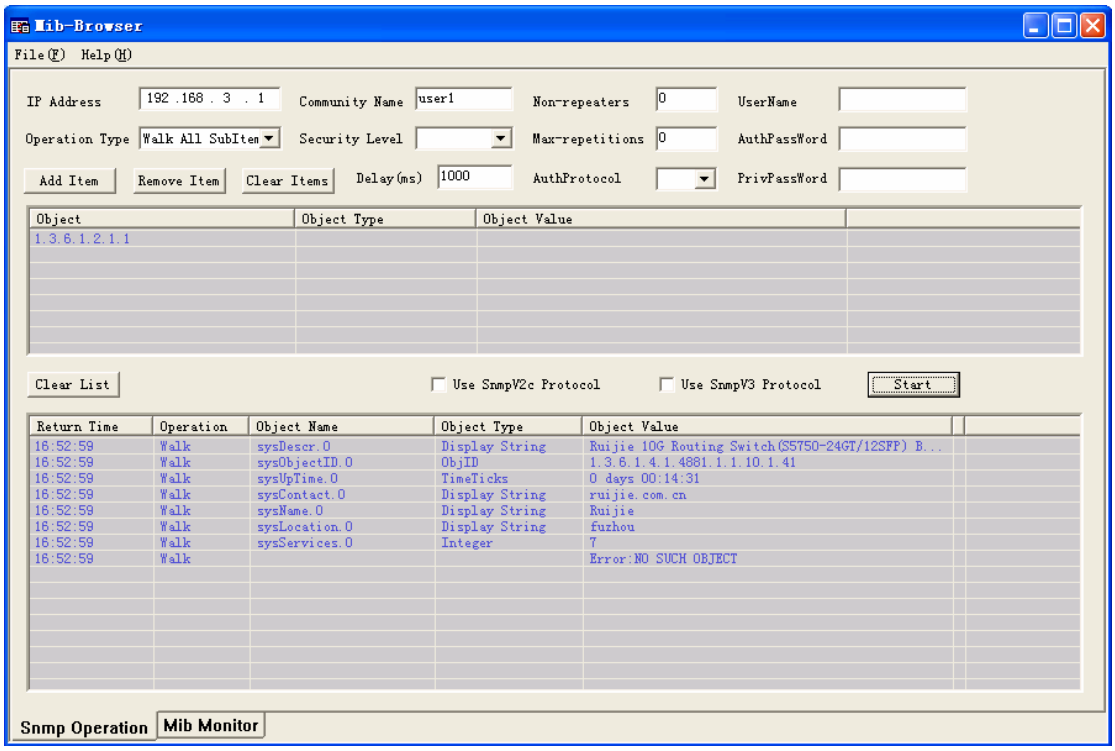
```
Ruijie# show running-config
!
ip access-list standard a1
 10 permit host 192.168.3.2
!
interface gigabitEthernet 0/1
 no ip proxy-arp
 ip address 192.168.3.1 255.255.255.0
!
snmp-server view v1 1.3.6.1.2.1.1 include
snmp-server location fuzhou
snmp-server host 192.168.3.2 traps version 2c user1
snmp-server enable traps
snmp-server contact ruijie.com.cn
snmp-server community user1 view v1 rw a1
snmp-server chassis-id 1234567890
```

第二步，查看 SNMP 视图和组的信息。

```
Ruijie#show snmp view
v1(include) 1.3.6.1.2.1.1                    //自定义 MIB 对象“v1”
default(include) 1.3.6.1                     //系统缺省定义 MIB 对象
Ruijie#show snmp group
groupname: user1                        //配置 Community 默认为 SNMP 组
securityModel: v1
securityLevel:noAuthNoPriv
readview: v1
writeview: v1
notifyview:
groupname: user1
securityModel: v2c
securityLevel:noAuthNoPriv
readview: v1
writeview: v1
notifyview:
```

第三步，安装 MIB-Browser，在 IP Address 中输入设备的 IP 地址：192.168.3.1，在 Community Name 中输入“user1”，点击 add item 按钮，选择要查询的 MIB 的具体管理单元，比如下图的 System。点击 Start 按钮，便开始对网络设备进行 MIB 的查询了，具体的查询结果见对话框的最下面的窗口：

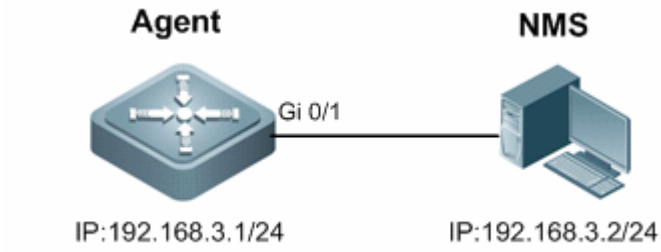
图 1-5



1.4.2 SNMP v3 配置用例

拓扑图

图 1-6 SNMPv3 应用拓扑



应用需求

1) 网络工作站（NMS）基于用户的认证加密模式对网络设备（Agent）进行管理。例如：使用用户名“user1”，认证方式为 MD5，认证密码为 123，加密算法为 DES56，加密密码为 321。

15) 网络设备能够控制用户访问 MIB 对象的操作权限。例如：用户“user1”可以对 System（1.3.6.1.2.1.1）节点下的 MIB 对象进行读操作，其中只能对 SysContact（1.3.6.1.2.1.1.4.0）节点下的 MIB 对象进行写操作。

16) 网络设备能够主动向网管工作站发送验证加密的消息。

配置要点

- 创建 MIB 视图，并指定包含或排除的 MIB 对象。
- 创建 SNMP 组，设置该组的版本号为“v3”，并指定该组使用的安全级别，同时需要设置该组对相应视图的读写权限。
- 创建用户名，同时关联对应的 SNMP 组名，即可以设置用户访问 MIB 对象的操作权限，同时需要配置版本号为“v3”，以及相应的认证方式、认证密码、加密算法、加密密码。
- 配置 SNMP 主机地址，同时需要配置版本号为“3”，并设置使用的安全级别。

配置步骤

第一步，配置 MIB 视图和组。

！创建一个 MIB 视图 “view1”，包含关联的 MIB 对象（1.3.6.1.2.1.1）；再创建一个 MIB 视图“view2”，包含关联的 MIB 对象（1.3.6.1.2.1.1.4.0）。

```
Ruijie(config)#snmp-server view view1 1.3.6.1.2.1.1 include
Ruijie(config)#snmp-server view view2 1.3.6.1.2.1.1.4.0 include
```

！创建一个组“g1”，选择版本号为“v3”，配置安全级别为认证加密模式“priv”，并可读视图“view1”，可写视图“view2”。

```
Ruijie(config)#snmp-server group g1 v3 priv read view1 write view2
```

第二步，配置 SNMP 用户。

！创建用户名“user1”，属于组“g1”，选择版本号为“v3”，配置认证方式为“md5”，认证密码为“123”，加密方式为“DES56”，加密密码为“321”。

```
Ruijie(config)#snmp-server user user1 g1 v3 auth md5 123 priv des56 321
```

第三步，配置 SNMP 主机地址。

！配置主机地址为 192.168.3.2，选择版本号为“3”，配置安全级别为认证加密模式“priv”，关联对应的用户名“user1”。

```
Ruijie(config)#snmp-server host 192.168.3.2 traps version 3 priv user1
```

！使能 Agent 主动向 NMS 发送 Trap 消息。

```
Ruijie(config)#snmp-server enable traps
```

第四步，配置 Agent 的 IP 地址。

！配置 Gi0/1 的接口地址为 192.168.3.1/24。

```
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-gigabitEthernet 0/1)#ip address 192.168.3.1 255.255.255.0
Ruijie(config-if-gigabitEthernet 0/1)#exit
```

验证结果

第一步，查看设备的配置信息。

```
Ruijie# show running-config
!
```

```
interface gigabitEthernet 0/1
 no ip proxy-arp
 ip address 192.168.3.1 255.255.255.0
!
snmp-server view view1 1.3.6.1.2.1.1 include
snmp-server view view2 1.3.6.1.2.1.1.4.0 include
snmp-server user user1 g1 v3 encrypted auth md5 7EBD6A1287D3548E4E52CF8349CBC93D priv des56
D5CEC4884360373ABBF30AB170E42D03
snmp-server group g1 v3 priv read view1 write view2
snmp-server host 192.168.3.2 traps version 3 priv user1
snmp-server enable traps
```

第二步，查看 SNMP 用户

```
Ruijie# show snmp user
User name: user1
Engine ID: 800013110300d0f8221120
storage-type: permanent     active
Security level: auth priv
Auth protocol: MD5
Priv protocol: DES
Group-name: g1
```

第三步，查看 SNMP 视图

```
Ruijie#show snmp view
view1(include) 1.3.6.1.2.1.1
view2(include) 1.3.6.1.2.1.1.4.0
default(include) 1.3.6.1
```

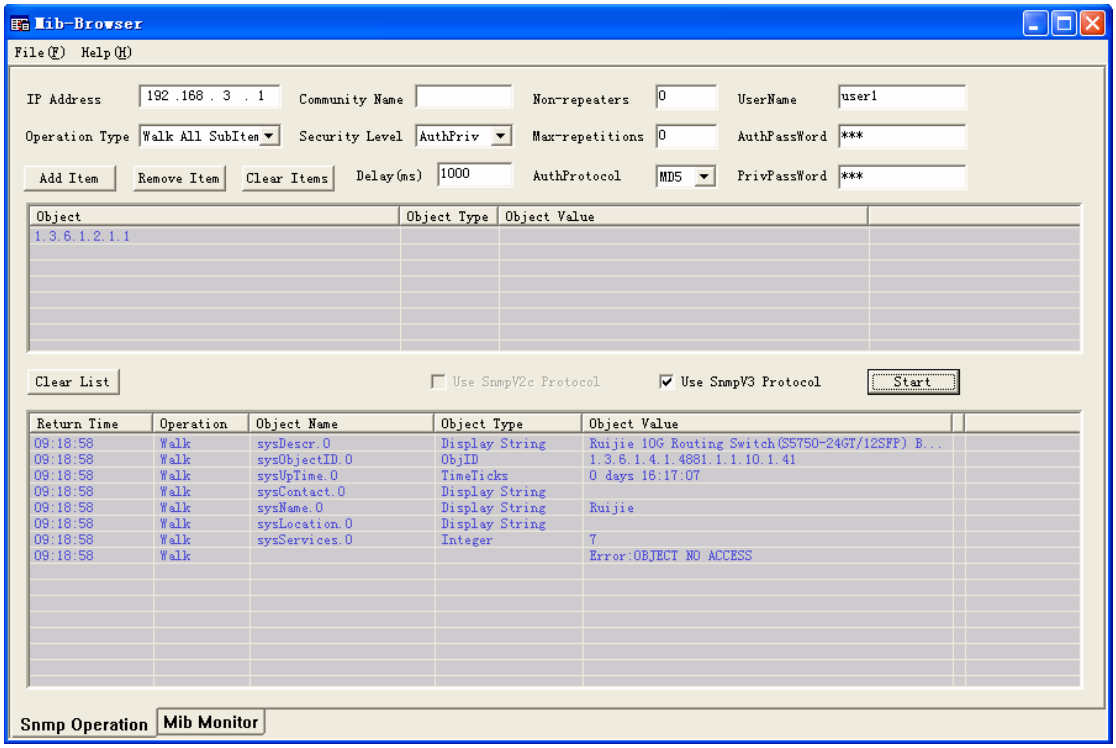
第四步，查看 SNMP 组

```
Ruijie# show snmp group
groupname: g1
securityModel: v3
securityLevel:authPriv
readview: view1
writeview: view2
notifyview:
```

第五步，查看用户配置的主机信息

```
Ruijie#show snmp host
Notification host: 192.168.3.2
udp-port: 162
type: trap
user: user1
security model: v3 authPriv
```

第六步，安装 MIB-Browser，在 IP Address 中输入设备的 IP 地址：192.168.3.1，在 UserName 中输入“user1”，在 Security Level 中选择“AuthPriv”，在 AuthPassWord 中输入“123”，在 AuthProtocol 中选择“MD5”，在 PrivPassWord 中输入“321”。点击 add item 按钮，选择要查询的 MIB 的具体管理单元，比如下图的 System。点击 Start 按钮，便开始对网络设备进行 MIB 的查询了，具体的查询结果见对话框的最下面的窗口：



2 RMON

2.1 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。

交换机实现其中的第 1，2，3，9 组的内容：统计组、历史组、警告组、事件组。

2.1.1 统计组

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。

2.1.2 历史组

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。

2.1.3 警告组

警报组（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。

2.1.4 事件组

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。

2.2 配置RMON

2.2.1 配置统计组

您可以使用如下命令添加一个统计表项。

命令	作用
Ruijie(config-if)# **rmon collection stats** *index* [**owner** *ownername*]	添加一个统计项
Ruijie(config-if)# **no rmon collection stats** *index*	删除一个统计项

☑ 我司产品当前版本只支持以太网接口的统计。

索引值应该是一个 1-65535 之间的整数，目前可最多同时配置 100 条统计项。

2.2.2 配置历史控制组

你可以使用如下命令添加一条历史控制表项：

命令	作用
Ruijie(config-if)# **rmon collection history** *index* [**owner** *ownername*] [**buckets** *bucket-number*] [**interval** *seconds*]	添加一个历史控制表项
Ruijie(config-if)# **no rmon collection history** *index*	删除一个历史控制表项

☑ 我司产品当前版本只支持以太网的记录。

索引值应该在 1-65535 之间，最多可以配置 10 条控制表项。

Bucket-number：控制项指定了采用的数据源、时间间隔。每个采样区间，都进行一次采样。采样的结果保存下来，Bucket-number 指定了保存采样的最大数目，当采样纪录达到最大值时，则新纪录覆盖最早的纪录。Bucket-number 取值范围是 1-65535，默认值是 10。

Interval：采样的时间间隔。默认值是 1800 秒，取值在 1-3600 之间。

2.2.3 配置警告组和事件组

你可以使用如下命令配置警告表：

命令	作用
Ruijie(config)# **rmon alarm** *number variable interval* {**absolute** | **delta**} **rising-threshold** *value* [*event-number*] **falling-threshold** *value* [*event-number*] [**owner** *ownername*]	添加一个历史控制表项

Ruijie(config)# **rmon event** *number* [**log**] [**trap** *community*] [**description** *description-string*] [**owner** *ownername*]	添加一个事件组表项
Ruijie(config)# **no rmon alarm** *number*	删除一个警告组
Ruijie(config)# **no rmon event** *number*	删除一个事件组

number：警告表（事件表）的索引，范围 1-65535。

variable：警告表监控的变量。变量必须是整数类型。

interval：采样的时间间隔。范围<1-4294967295>

关键字 Absolute 表示拿每次采样得到的值和上限、下限比较，关键字 Delta 表示利用和上次采样的差值和上限、下限比较。

value 定义了上限、下限的值。

event-number：当超过了上限或者下限的时候，触发事件组索引为 Event-number 的事件。

关键字 Log 表示事件触发的动作是：纪录事件

关键字 Trap 表示事件触发后的动作是：发送 Trap 消息到管理站。

community：发送 Trap 时的认证名。

description-string：事件的描述。

ownername：警告组或事件组的所有者。

2.2.4 显示RMON状态

命令	作用
show rmon alarm	显示警告组
show rmon event	显示事件组
show rmon history	显示历史组
show rmon statistics	显示统计组

2.3 RMON配置实例

2.3.1 配置统计组实例

如果您希望统计以太端口 3，使用如下命令：

```
Ruijie(config)# interface gigabitEthernet 0/3
Ruijie(config-if)# rmon collection stats 1 owner zhangsan
```

2.3.2 配置历史组实例

如果您希望每隔 10 分钟统计以太网端口 3 的历史信息，使用如下命令：

```
Ruijie(config)# interface gigabitEthernet 0/3
Ruijie(config-if)# rmon collection history 1 owner zhangsan interval 600
```

2.3.3 配置警告组和事件组实例

如果您希望配置对一个可统计的 MIB 变量的报警功能。下面的例子说明了对 MIB-II 中 IfEntry 表中实例 ifInNUcastPkts.6（端口 6 上收到的非单播帧的个数，实例的标识符为 1.3.6.1.2.1.2.2.1.12.6）设置报警功能。具体功能为：交换机每隔 30 秒检查端口 6 上收到的非单播帧的个数的变化，如果收到的非单播帧的个数比上次检查时（30 秒前）增加了 20 个或 20 个以上，或者比上次只增加 10 个或 10 以下，则警报被触发，同时警报将触发事件 1 进行相应的操作（记录到日志中，并发送认证名为”rmon”的 Trap，事件的描述为“ifInNUcastPkts is too much”）。警报和事件表项的拥有者均为 zhangsan。

```
Ruijie(config)# rmon alarm 10 1.3.6.1.2.1.2.2.1.12.6 30 delta rising-threshold 20 1 falling-threshold 10 1 owner zhangsan
Ruijie(config)# rmon event 1 log trap rmon description "ifInNUcastPkts is too much " owner zhangsan
```

2.3.4 显示rmon状态实例

show rmon alarm

```
Ruijie# show rmon alarm
rmon alarm table:
                    index: 10,
                    interval: 30,
                    oid = 1.3.6.1.2.1.2.2.1.12.6
                    sampleType: 2,
                    alarmValue: 0,
                    startupAlarm: 3,
                    risingThreshold: 20,
                    fallingThreshold: 10,
                    risingEventIndex: 1,
                    fallingEventIndex: 1,
                    owner: zhangesan,
                    stats: 1,
```

show rmon event

```
Ruijie# show rmon event
rmon event table:
                    index = 1
                    description = ifInNUcastPkts
                    type = 4
                    community = rmon
                    lastTimeSent = 0 d:0 h:0 m:0 s
                    owner = zhangsan
                    status = 1
```

show rmon history

```
Ruijie# show rmon history
rmon history control table:
                    index = 1
                    interface = FastEthernet 0/1
                    bucketsRequested = 10
                    bucketsGranted = 10
                    interval = 1800
                    owner = zhangsan
                    stats = 1

rmon history table:
                    index = 1
                    sampleIndex = 198
                    intervalStart = 0d:14h:0m:47s
                    dropEvents = 0
                    octets = 67988
                    pkts = 726
                    broadcastPkts = 502
                    multiPkts = 189
                    crcAllignErrors = 0
                    underSizePkts = 0
                    overSizePkts = 0
                    fragments = 0
                    jabbers = 0
                    collisions = 0
                    utilization = 0
```

show rmon statistics

```
Ruijie#  show rmon statistics
ether statistic table:
                    index = 1
                    interface = FastEthernet 0/1
                    owner = zhangsan
                    status = 0
                    dropEvents = 0
                    octets = 1884085
                    pkts = 3096
                    broadcastPkts = 161
                    multiPkts = 97
                    crcAllignErrors = 0
                    underSizePkts = 0
                    overSizePkts = 1200
                    fragments = 0
```

```
                jabbers = 0
                collisions = 0
                packets640ctets = 128
                packets65To1270ctets = 336
                packets128To2550ctets = 229
                packets256To5110ctets = 3
                packets512To10230ctets = 0
                packets1024To15180ctets = 1200
```

3 NTP

3.1 理解NTP

Network Time Protocol（NTP）是用来使网络设备时间同步化的一种协议，它可以使网络设备对其服务器或时钟源做同步化，它可以提供高精准度的时间校正（LAN 上与标准时间差小于 1 毫秒，WAN 上几十毫秒），且可使用加密确认的方式来防止攻击。

NTP 提供准确时间，首先要有准确的时间来源，这一时间应该是国际标准时间 UTC。 NTP 获得 UTC 的时间来源可以是原子钟、天文台、卫星，也可以从 Internet 上获取。这样就有了准确而可靠的时间源。

为防止对时间服务器的恶意破坏，NTP 使用了识别（Authentication）机制，检查时间同步信息是否是真正来自所宣称的服务器并检查资料的返回路径，以提供对抗干扰的保护机制。

目前我司设备支持 NTP 的客户端与服务器功能，即设备既可以从时间服务器上同步时间，也能够作为时间服务器对其他设备进行时间同步。在作为服务器工作时设备仅支持单播 Server 模式。

3.2 配置NTP

3.2.1 配置NTP全局安全识别机制

锐捷的 NTP 客户端支持与服务器进行加密通信，加密方式为密钥加密机制。

配置 NTP 客户端通过加密方式与服务器通信分两步：第一，对 NTP 客户端进行全局安全识别以及全局密钥相关设置；第二，设置通信服务器的信任密钥；NTP 全局安全设置机制属于第一个设置步骤，但是要真正发起与服务器之间的加密通信，还要对对应的服务器设置认证密钥。

在缺省情况下，客户端不使用全局安全识别机制。如果未使用安全识别机制则不对通信进行加密处理。但是仅仅设置了全局安全标志，并不代表一定采用了加密方式完成服务器与客户端的通信，还必须完成其他全局密钥配置并设置服务器加密密钥才可能发起和服务器的加密通信。

要配置全局安全识别机制，在全局配置模式中执行以下命令：

命令	作用
Ruijie(config)#**ntp authenticate**	配置 NTP 全局安全识别机制。
Ruijie(config)#**no ntp authenticate**	关闭 NTP 全局安全识别机制。

报文的验证是通过 **ntp authentication-key**、**ntp trusted-key** 指定的信任密钥进行验证的。

3.2.2 配置NTP全局认证密钥

进行 NTP 安全认证全局配置，接下来的配置就是设置全局认证密钥。

配置全局认证密钥，每个密钥有一个唯一的 key-id 标识，客户可以用 **ntp trusted-key** 将该 key-id 对应的密钥设置为全局信任密钥。

要配置全局认证密钥，在全局配置模式中执行以下命令：

命令	作用
Ruijie(config)#**ntp authentication-key** *key-id* **md5** *key-string* [*enc-type*]	配置 NTP 全局认证密钥。 key-id：1-4294967295 key-string：长度范围任意 enc-type：有 0 和 7 两种类型。
Ruijie(config)#**no ntp authentication-key** *key-id*	删除 NTP 全局认证密钥。

配置了全局认证密钥并不说明该密钥一定有效，在使用该密钥之前必须将该密钥配置成为全局信任密钥。

☑ 锐捷目前的版本只支持最大 1024 认证密钥，每个服务器允许设置唯一一个密钥进行安全通信。

3.2.3 配置NTP全局信任密钥ID

进行全局安全认证配置的最后一个阶段，就是将一个全局密钥配置成全局信任密钥。通过该信任密钥，用户才可以发送加密数据并检验收到数据报文的合法性。

要指定全局信任密钥，在全局配置模式中执行以下命令：

命令	作用
Ruijie(config)#**ntp trusted-key** *key-id*	配置 NTP 全局信任密钥 ID。
Ruijie(config)#**no ntp trusted-key** *key-id*	删除 NTP 全局信任密钥 ID。

以上三步设置仅仅是完成安全认证机制的第一个步骤，真正发起与客户服务器的加密通信必须对相应的服务器设置信任密钥。

直接删除全局认证密钥，则该密钥对应的信任信息也会被删除。

3.2.4 配置NTP服务器

在缺省情况下，没有配置 NTP 服务器。锐捷的客户端系统支持最多同时与 20 个 NTP 服务器交互，（在全局认证以及密钥相关设置完成后）可以为每一个服务器设置一个认证密钥，发起与服务器的加密通信。

与服务器的默认通信版本为 NTP 版本 3，同时可以配置发送 NTP 报文的源接口，并只在发送接口上接收对应服务器的 NTP 报文。

配置一个 NTP 服务器，在全局配置模式下执行以下命令：

命令	作用

Ruijie(config)#**ntp server [vrf** *vrf-name*] *ip-addr* [**version** *version*][**source** *if-name number*][**key** *keyid*][**prefer**]	配置 NTP 服务器 vrf-name：参考时钟源绑定 VRF 的名称 version（NTP 版本号）：1-3 if-name（接口类型）：包括 AggregatePort、Dialer GigabitEthernet、Loopback、Multilink、Null、Tunnel、Virtual-ppp、Virtual-template、Vlan 类型。 keyid：1-4294967295
Ruijie(config)#**no ntp server** *ip-addr*	删除 NTP 服务器

只有完成了全局安全识别以及密钥设置机制，这时候设置服务器通信的信任密钥，才能发起与服务器的加密通信，而加密通信的完成需要服务器端信任相同的密钥。

3.2.5 关闭接口接收NTP报文

该命令的功能是关闭对应接口上接收 NTP 报文。

在缺省情况下，任意接口上接收的 NTP 报文都可以提供给客户端进行时钟调整，通过设置这个功能，可以屏蔽对应接口上收到的 NTP 报文。

能够进行该功能命令配置的接口肯定是能够配置 IP 收发报文的接口，在其他接口上没有该命令。

在接口配置模式下执行以下命令，配置关闭接口接收 NTP 报文：

命令	作用
Ruijie(config-if)#**interface** *interface-type number*	进入接口配置模式
Ruijie(config-if)#**ntp disable**	关闭接口接收 NTP 报文的功能。

要打开接口接收 NTP 报文的功能，在接口模式下使用 **no ntp disable** 命令。

3.2.6 NTP功能开关

no ntp 命令的功能是关闭 NTP 同步服务，停止时间同步，同时清空相关的 NTP 配置信息。

在缺省情况下，NTP 功能是关闭的，但只要配置了 NTP 服务器或 NTP 安全识别机制，NTP 功能就会被打开。

要关闭 NTP，在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)#**ntp authenticate** 或 **ntp server** *ip-addr* [**version** *version*][**source** *if-name number*][**key** *keyid*][**prefer**]	打开 NTP 功能
Ruijie(config)#**no ntp**	关闭 NTP 功能。

3.2.7 配置NTP更新硬件时钟

使用此功能可以让 NTP 客户端使用从外部时钟源同步得来的时钟值更新设备的硬件时钟。

在全局配置模式下执行以下命令配置更新硬件时钟：

命令	作用
Ruijie(config)#**ntp update-calendar**	配置更新硬件时钟
Ruijie(config)#**no ntp update-calendar**	取消配置更新硬件时钟

在缺省情况下没有配置 NTP 更新硬件时钟。配置之后，NTP 客户端会在每次与外部时钟源同步成功时也同时更新设备的硬件时钟。一般情况下建议启用此功能，使设备的硬件时钟也能同时保持精准。

3.2.8 设置NTP主时钟

该功能用来设置本地时钟作为 NTP 主时钟（本地时钟参考源可靠），为其它设备提供同步时间。

在通常情况下，本地系统都会直接或间接地与外部的时钟源进行同步。但若由于网络连接故障等原因而导致本地系统无法与外部时钟源同步时，可以通过该命令设置本地时钟参考源可靠，为其他设备提供同步时间。

一旦进行了此设置，系统便不会与比其时钟层数数值更高的时钟源进行同步。

NTP 使用“层数（stratum）”的概念来描述设备距离权威时钟源的“跳数（hops）”。一个层数为 1 的时间服务器应当有个直连的原子钟或电波钟；层数为 2 的时间服务器就从层数为 1 的服务器获取时间；层数为 3 的服务器就从层数为 2 的获取时间……如此递推。因此时钟层数数值更低的时钟源即被认为拥有更高的时钟精度。

在全局配置模式下执行以下命令配置 NTP 主时钟功能：

命令	作用
Ruijie(config)#**ntp master** [*stratum*]	设置本地时钟作为 NTP 主时钟并指定相应时钟层数。时钟层数取值范围为 1～15；若不指定该参数则默认值为 8。
Ruijie(config)#**no ntp master**	取消 NTP 主时钟设置

如下可以设置本地时钟参考源可靠，并设置其时钟层数为 12。

```
Ruijie(config)# ntp master 12
```

使用此命令时必须特别小心。将本地时钟设置为主时钟（尤其是指定了较低的时钟层数值时）很有可能将真正的有效时钟源覆盖。如果对同一网络中的多个设备都使用了该命令，则可能由于设备之间的时钟差异导致网络的时钟同步不稳定。

另外，使用该命令前若系统从未与外部时钟源同步过，则有可能需要手动校准系统时钟以保证其不会有过大的偏差（关于如何手动校准系统时钟请参考《交换机基础管理配置指南》中的系统时间配置部分）

3.2.9 配置NTP服务的访问控制权限

NTP 服务的访问控制功能提供了一种最小限度的安全措施（更安全的方法是使用 NTP 身份验证机制）。系统在缺省情况下未配置任何 NTP 访问控制规则。

在全局配置模式下执行以下命令配置 NTP 服务的访问控制权限：

命令	作用
Ruijie(config)#**ntp access-group { peer | serve | serve-only | query-only }** *access-list-number* | *access-list-name*	设置对本地服务的访问控制权限
Ruijie(config)#**no ntp access-group { peer | serve | serve-only | query-only }** *access-list-number* | *access-list-name*	取消对本地服务的访问控制权限的设置

其中：

- **peer**：既允许对本地 NTP 服务进行时间请求和控制查询，也允许本地设备与远程系统同步时间（完全访问权限）。
- **serve**：允许对本地 NTP 服务进行时间请求和控制查询，但不允许本地设备与远程系统同步时间。
- **serve-only**：仅允许对本地 NTP 服务进行时间请求。
- **query-only**：仅允许对本地 NTP 服务进行控制查询。
- *access-list-number*：IP 访问控制列表标号；范围为 1～99 和 1300～1999。关于如何创建 IP 访问控制列表请参考《访问控制列表配置指南》中的相关描述。
- *access-list-name*：IP 访问控制列表名。关于如何创建 IP 访问控制列表请参考《访问控制列表配置指南》中的相关描述。

当一个访问请求到达时，NTP 服务按照从最小访问限制到最大访问限制的顺序依次匹配规则，以第一个匹配到的规则为准。匹配顺序为 peer、serve、serve-only、query-only。

目前系统暂未支持控制查询功能（用于通过网络管理设备对 NTP 服务器进行控制，如设置闰秒标记或监控其工作状态等）。虽然是按照上述顺序进行规则匹配，但涉及到与控制查询相关的请求都无法支持。

如果未配置任何访问控制规则，则所有访问都是允许的。但一旦配置了访问控制规则，则仅有规则中所允许的访问才能进行。

可以如下配置以允许第 1 号访问列表中的对端设备对本地设备进行时间请求、查询控制和时间同步；并限制第 2 号访问列表中的对端设备仅能对本地设备进行时间请求：

```
Ruijie(config)# ntp access-group peer 1
Ruijie(config)# ntp access-group serve-only 2
```

3.3 显示NTP信息

3.3.1 调试NTP

要进行 NTP 功能调试，可以通过该命令输出必要的调试信息，进行故障诊断和排除。

调试 NTP 功能，在特权模式下执行以下命令：

命令	作用
debug ntp	打开调试功能。

no debug ntp	关闭调试功能。

3.3.2 显示NTP信息

在特权模式下，您可以使用 **show ntp status** 命令来显示当前的 NTP 信息。

显示 NTP 状态信息，在特权模式下执行以下命令：

命令	作用
show ntp status	显示当前的 NTP 信息

只有在配置了相关的通信服务器之后该命令才能打印出显示信息。

```
Ruijie# show ntp status
Clock is synchronized,stratum 9,reference is 192.168.217.100
nominal freq is 250.0000 Hz,actual freq is 250.0000 Hz,precision is 2**18
reference time is AF3CF6AE.3BF8CB56(20:55:10.000 UTC Mon Mar 1 1993)
clock offset is 32.97540 sec,root delay is 0.00000 sec
root dispersion is 0.00003 msec,peer dispersion is 0.00003 msec
```

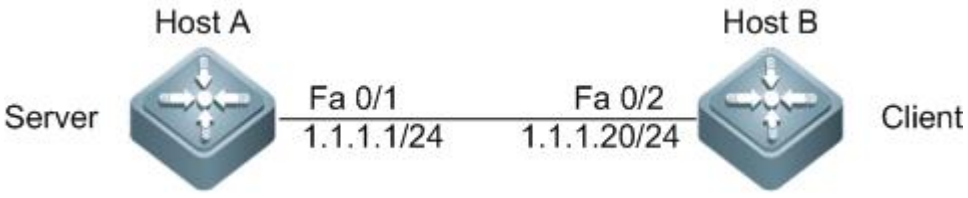
stratum 代表当前时钟的等级，reference 为同步服务器的地址，frep 当前系统时钟频率，precision 为当前系统时钟精度，reference time 为同步服务器参考时钟的 UTC 时间值，clock offset 为当前时钟偏移， root delay 为当前时钟延迟，root dispersion 为顶级服务器精度，peer dispersion 为同步服务器精度。

3.4 NTP典型配置举例

3.4.1 配置NTP客户端/服务器模式

拓扑图

图 3-1 NTP 客户端/服务器模型



应用需求

- Host A 设置本地时钟作为 NTP 主时钟，其时钟层数为 12
- Host B 配置为 NTP 客户端，指定 Host A 为 NTP 服务器
- Host B 的硬件时钟也能保持同步

配置要点

1) NTP 服务器

- 在通常情况下，本地系统都会直接或间接地与外部的时钟源进行同步。但若由于网络连接故障等原因而导致本地系统无法与外部时钟源同步时，可以通过 **ntp master** 命令设置本地时钟作为 NTP 主时钟，为其他设备提供同步时间。

17) NTP 客户端

- 配置指定的 NTP 服务器
- 通过配置 NTP 的硬件时钟更新功能，让 NTP 客户端使用从外部时钟源同步得来的时钟值更新设备的硬件时钟，使设备的硬件时钟也能同时保持精准

配置步骤

- NTP 服务器端的配置

！设置 NTP 主时钟。将本地时钟作为可信基准时钟源，时钟层数为 12

```
HostA(config)# ntp master 12
```

- NTP 客户端的配置

！设置 Host A 为 NTP 服务器

```
HostB(config)# ntp server 1.1.1.1
```

！配置 NTP 硬件时钟更新功能

```
HostB(config)# ntp update-calendar
```

配置验证

- 配置 NTP 同步之前，查看时间

！查看基准时钟源的时间

```
HostA# show clock
17:12:48 UTC Tue, Sep 8, 2009
```

！查看未同步前客户端的时间

```
HostB# show clock
12:01:10 UTC Sat, Jan 1, 2000
```

！查看未同步前客户端 NTP 状态

```
HostB(config)# show ntp status
Clock is unsynchronized, stratum 16, no reference clock
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**0
```

```
reference time is 0.0 (00:00:00.000 UTC Thu, Jan 1, 1970)
clock offset is 0.00000 sec, root delay is 0.00000 sec
root dispersion is 0.00000 msec, peer dispersion is 0.00000 msec
```

由以上显示可以看出，此时未同步；

- 配置 NTP 同步之后，查看 NTP 配置。关注点：NTP 服务器地址、层数。

CLI 界面打印如下日志信息：

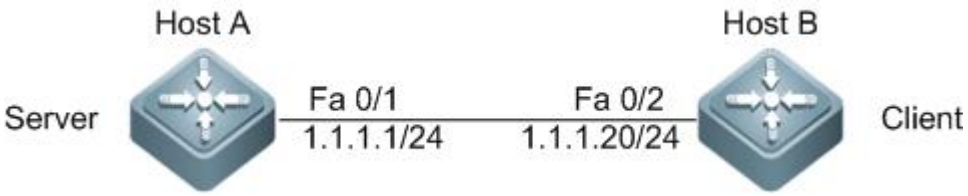
```
*Sep  8 18:10:37: %SYS-6-CLOCKUPDATE: System clock has been updated to 18:10:37 UTC Tue Sep  8 2009.
HostB# show ntp status
Clock is synchronized, stratum 13, reference is 1.1.1.1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**24
reference time is CE511CC9.37EB5B2D (18:11:21.000 UTC Tue, Sep 8, 2009)
clock offset is -0.00107 sec, root delay is 0.00000 sec
root dispersion is 0.00002 msec, peer dispersion is 0.00002 msec
```

由以上显示信息可以看出，NTP 客户端同服务器建立了连接，Host B 与 Host A 时间同步，且比 Host A 层数大 1，为 13。

3.4.2 配置带身份认证的NTP客户端/服务器模式

拓扑图

图 3-2 NTP 客户端/服务器模型



应用需求

- Host A 设置本地时钟作为 NTP 主时钟，其时钟层数为 12
- Host B 配置为 NTP 客户端，指定 Host A 为 NTP 服务器
- 启用身份认证机制，防止非法用户对时间服务器的恶意破坏

配置要点

配置 NTP 服务器/客户端的身份认证功能包括以下几个步骤：

- 使能 NTP 全局安全识别机制
- 配置 NTP 全局认证密钥及其对应的密钥 ID
- 指定 NTP 全局信任密钥 ID

NTP 客户端同指定 NTP 服务器之间的通信认证密钥及对应密钥的 ID 值一致。

配置步骤

■ NTP 服务器端的配置

第一步，设置本地 NTP 主时钟。将本地时钟作为可信基准时钟源，层数为 12

```
HostA(config)# ntp master 12
```

第二步，配置 NTP 身份认证

！使能 NTP 全局安全识别机制

```
HostA(config)# ntp authenticate
```

！配置 NTP 全局认证密钥为“helloworld”，其对应的密钥 ID 为“6”

```
HostA(config)# ntp authentication-key 6 md5 helloworld
```

！指定“6”为 NTP 全局信任密钥 ID

```
HostA(config)# ntp trusted-key 6
```

■ NTP 客户端的配置

第一步，配置 NTP 身份认证

！使能 NTP 全局安全识别机制

```
HostB(config)# ntp authenticate
```

！配置 NTP 全局认证密钥为“helloworld”，其对应的密钥 ID 为“6”

```
HostB(config)# ntp authentication-key 6 md5 helloworld
```

！指定“6”为 NTP 全局信任密钥 ID

```
HostB(config)# ntp trusted-key 6
```

！设置 Host A 为 NTP 服务器，并设置同该服务器通信的密钥 ID 为“6”

```
HostB(config)# ntp server 1.1.1.1 key 6
```

配置验证

■ 查看 NTP 服务器端的配置信息。关注点：NTP 主时钟设置、NTP 服务器 IP 地址、认证相关功能配置。

```
HostA#show run
!
interface fastEthernet 0/1
ip address 1.1.1.1 255.255.255.0
!
ntp authentication-key 6 md5 07360623191d300a004609 7
ntp authenticate
```

```
ntp trusted-key 6
ntp master 12
!
```

■ 查看 NTP 客户端的配置信息。关注点：指定 NTP 服务器的 IP 地址及密钥 ID、认证相关功能配置。

```
HostB #show run
!
interface fastEthernet 0/2
ip address 1.1.1.20 255.255.255.0
!
ntp authentication-key 6 md5 141a4f012d1d3c23174905 7
ntp authenticate
ntp trusted-key 6
ntp server 1.1.1.1 key 6
!
```

正确配置后，CLI 打印如下日志信息：

```
*Sep  9 11:31:29: %SYS-6-CLOCKUPDATE: System clock has been updated to 11:31:29 UTC Wed Sep  9 2009.
```

以上日志信息说明 NTP 客户端 HostB 的时钟已经被更新。

■ 查看 NTP 服务器端的 NTP 状态信息

```
HostA #show ntp status
Clock is synchronized, stratum 12, reference is 127.127.1.1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**24
reference time is CE521261.E52DECA2 (11:39:13.000 UTC Wed, Sep 9, 2009)
clock offset is 0.00000 sec, root delay is 0.00000 sec
root dispersion is 0.00002 msec, peer dispersion is 0.00002 msec
```

■ 查看 NTP 客户端的 NTP 状态信息；关注点：NTP 服务器地址、层数。

```
HostB# show ntp status
Clock is synchronized, stratum 13, reference is 1.1.1.1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**24
reference time is CE5212A1.E5D712A0 (11:40:17.000 UTC Wed, Sep 9, 2009)
clock offset is -0.00005 sec, root delay is 0.00000 sec
root dispersion is 0.00002 msec, peer dispersion is 0.00002 msec
```

由以上显示信息可以看出，NTP 客户端同服务器成功建立了连接，Host B 与 Host A 时间同步，且比 Host A 层数大 1，为 13。

4 SNTP

4.1 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。

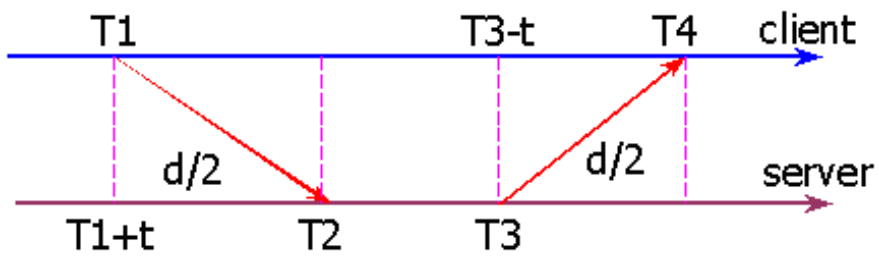
SNTP（简单网络时间协议）是 NTP 的简化版本，在实现时，计算时间用了简单的算法，性能较高。而精确度一般也能达到 1 秒左右，也能基本满足绝大多数场合的需要。

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。

4.2 SNTP原理

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。

图 4-1



Originate Timestamp	T1	time request sent by client
Receive Timestamp	T2	time request received at server
Transmit Timestamp	T3	time reply sent by server
Destination Timestamp	T4	time reply received at client

T1：客户机发送查询请求时间（以客户机时间系统为参照），标记为 Originate Timestamp；

T2：服务器收到查询请求时间（以服务器时间系统为参照），标记为 Receive Timestamp；

T3：服务器回复时间信息包时间（以服务器时间系统为参照），标记为 Transmit Timestamp；

T4：客户机收到时间信息包时间（以客户机时间系统为参照），标记为 Destination Timestamp；

T：服务器和客户机之间的时间偏差；

d：两者之间的往返时间；

时间求解过程：

因为

T2 = T1 + t + d / 2；

所以

T2 - T1 = t + d / 2；

又因为

T4 = T3 – t + d / 2；

所以

T3 - T4 = t – d / 2；

求得

d = （T4 - T1） - （T3 - T2）；

t = （（T2 - T1） + （T3 - T4）） / 2；

求出了 t 和 d，SNTP Client 就可据此算出当前的时间。

即，当前时间为 T4 + t

4.3 配置SNTP

4.3.1 缺省的SNTP设置

缺省情况下，SNTP 的配置如下：

功能特性	缺省值
SNTP 状态	Disable，关闭 SNTP 服务
NTP Server 的 IP 地址	0
SNTP 的同步时间的间隔	1800s
本地时区	+8，即东八区

4.3.2 打开SNTP

进入特权模式，按以下步骤打开 SNTP：

1) 进入全局配置模式。

```
Ruijie# config
```

18) 打开 SNTP，即时同步一次时钟。后续如果输入这个命令， 都会“即时同步”时钟，不必等待定时同步。（为了避免频繁地同步时间，每两次的“即时同步”时间间隔请勿小于 5 秒）。

```
Ruijie(config)# sntp enable
```

19) 退回到特权模式

```
Ruijie(config)# End
```

20) 显示当前配置

```
Ruijie# show running-config
```

21) 保存配置。

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

您如果要关闭 SNTP，可以用 **no sntp enable** 全局配置命令来关闭 SNTP。

4.3.3 配置SNTP Server的地址

由于 SNTP 的报文和 NTP 的报文是完全一致的，所以 SNTP Client 能完全兼容 NTP Server。网络上存在着较多的 NTP Server，您可以选择一个网络延迟较少的一个作为设备上的 SNTP Server。

具体的 NTP server 地址可以登录 http://www.time.edu.cn/或 http://www.ntp.org/上获取。

如 192.43.244.18（time.nist.gov）。

进入特权模式，按以下步骤配置 SNTP Server IP 地址：

1) 进入全局配置模式。

```
Ruijie# config
```

22) 设置 SNTP Server 的 IP 地址。

```
Ruijie(config)# sntp server <ip-addr>
```

23) 退回到特权模式

```
Ruijie(config)# End
```

24) 显示当前配置

```
Ruijie# show running-config
```

25) 保存配置。

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

4.3.4 配置SNTP同步时钟的间隔

SNTP Client 需要设置一定的时间间隔定期访问 NTP Server，以便定时校正时钟。以下步骤将配置设备和 NTP Server 同步时钟的间隔：

1) 进入全局配置模式。

```
Ruijie# config
```

2) 设置定时同步时钟的间隔，单位为秒。范围为 60 秒-65535 秒，缺省值为 1800 秒。

```
Ruijie(config)# sntp interval <seconds>
```

3) 退回到特权模式

```
Ruijie(config)# End
```

4) 显示当前配置

```
Ruijie# show running-config
```

5) 保存配置。

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

这里设置的时间间隔不会立即生效，如果要立即生效，请配置完时间间隔后执行 sntp enable 命令。

4.3.5 配置本地时区

通过 SNTP 协议通讯后获取的时间都是格林威治标准时间 （GMT），为了准确的获取本地时间，需要设置本地时区来对标准时间进行调正。

1) 进入全局配置模式。

```
Ruijie# config
```

26) 配置时区，范围为-23 至 23，负数表示西区，正数表示东区。如 8 表示东八区，-8 表示西 8 区，0 表示格林威治标准时间。默认时区名为“UTC”，缺省值为 0。

```
Ruijie(config)# clock timezone <time-zone>
```

27) 退回到特权模式

```
Ruijie(config)# end
```

28) 显示当前配置

```
Ruijie# show running-config
```

29) 保存配置

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

您可以通过 **no clock timezone** 来恢复缺省值。

4.4 显示SNTP

步骤如下：

1) 查看 SNTP 的相关参数

```
Ruijie# show sntp
```

30) 使用 **show sntp** 查看 SNTP 的配置参数：

```
Ruijie# show sntp
SNTP state                  : ENABLE                                    //SNTP 是否打开
SNTP server                 : 192.168.4.12                               //SNTP Server
SNTP sync interval          : 60                                       //定时同步的时间间隔
Time zone                   : +8                                                 //本地时区
```

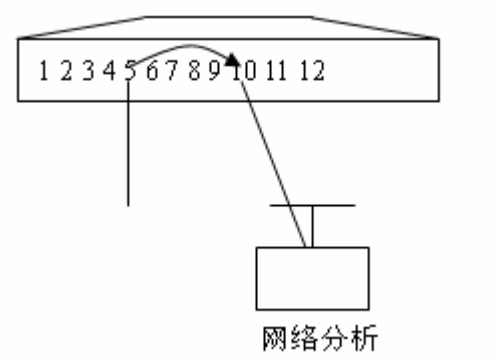
5 SPAN

5.1 SPAN概述

用户可以利用端口镜像(SPAN)提供的功能，将指定端口的报文复制到交换机上另一个连接有网络监测设备的端口，进行网络监控与故障排除。

通过 SPAN 可以监控所有进入和从源端口输出的报文。例如，在图 1 中，端口 5 上的所有报文都被映射到了端口 10，连接在端口 10 上的的网络分析仪虽然没有和端口 5 直接相连，但是可以接收通过端口 5 上的所有报文。

图 5-1 SPAN 配置实例



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

5.2 SPAN基本概念

5.2.1 SPAN会话

SPAN 会话是镜像源端口与目的端口之间的数据流，可以监控单个或多个端口的输入、输出、双向的报文。Switched port、Routed port 和 AP 等类型的端口都可以配置为 SPAN 会话的源端口和目的端口。端口加入 SPAN 会话后并不影响交换机的正常操作。

用户可以在处于关闭状态的端口上配置 SPAN 会话，但是该 SPAN 会话是非活动的，只有相关的端口被打开后，SPAN 会话才会变为活动状态。另外，SPAN 会话在交换机上电后并不立即生效，直到目的端口处于可操作状态后，SPAN 会话才处于活动状态。用户可以通过 **show monitor** [**session** *session_num*]命令查看 SPAN 会话的操作状态。

5.2.2 镜像数据流

数据流方向

SPAN 会话包含以下三种方向的数据流：

- 输入数据流：所有源端口上接收到的报文都将被复制一份到目的端口。在一个 SPAN 会话中，用户可以监控一个或多个源端口的输入报文。由于某些原因（如端口安全），从源端口输入的报文可能被丢弃，但这不影响 SPAN 功能，该报文仍然会镜像到目的端口。
- 输出数据流：所有从源端口发送的报文都将复制一份到目的端口。在一个 SPAN 会话中，用户可以监控一个或多个源端口的输出报文。若由于某些原因，从别的端口发送到源端口的报文可能被丢弃，同样，该报文也不会发送到目的端口。由于某些原因从源端口输出的报文的格式可能改变，例如源端口输出经过路由之后的报文，报文的源 MAC、目的 MAC、VLAN ID 以及 TTL 发生变化，同样，拷贝到目的端口的报文的格式也会变化。
- 双向数据流：包括上面所说的两种数据流。在一个 SPAN 会话中，用户可监控一个或多个源端口的输入和输出方向的数据流。

SPAN Traffic

使用 SPAN 可以监控所有网络通讯，包括多播帧，BPDU 帧等。

5.2.3 源端口

源端口也被称为被监控口，在 SPAN 会话中，源端口上的数据流被监控，用于网络分析或故障排除。在单个 SPAN 会话中，用户可以监控输入、输出和双向数据流，且源端口的最大个数没有限制。

源端口具有以下特性：

- 源端口可以是 switched port，routed port 或 AP。
- 源端口不能同时作为目的端口。
- 源端口和目的端口可以属于同一 VLAN，也可以属于不同 VLAN。

5.2.4 目的端口

SPAN 会话有一个目的端口（也被称为监控口），用于接收源端口的报文拷贝。

目的端口具有以下特性：

- 目的端口可以是 switched port、routed port 或 AP。
- 目的端口不能同时作为源端口。

☑ 交换机目的端口不支持 AP 口。

5.2.5 SPAN和其他功能的关系

SPAN 和以下功能交互：

- Spanning Tree Protocol（STP）

SPAN 的目的端口参与 STP 协议计算。

5.3 配置SPAN

5.3.1 SPAN缺省状态

功能特性	缺省值
SPAN 状态	关闭

5.3.2 创建SPAN会话并指定目的端口和源端口

用户可以按照以下步骤创建 SPAN 会话并指定目的端口（监控口）和源端口（被监控口）：

命令	作用
Ruijie(config)# **monitor session** *session_num* **source interface** *interface-id* [**,** **|** **-**] {**both | rx | tx**}	指定源端口。对于 *interface-id*，请指定相应的接口号。
Ruijie(config)# **monitor session** *session_num* **destination interface** *interface-id* [**switch**]	指定目的端口。对于 *interface-id*，请指定相应的接口号，添加 switch 参数将支持镜像目的端口交换功能。

想要删除 SPAN 会话，可以使用 **no monitor session** *session_num* 全局配置命令。想要删除所有 SPAN 会话，可以使用 **no monitor session all** 全局配置命令。使用 **no monitor session** *session_num* **source interface** *interface-id* 全局配置命令或 **no monitor session** *session_num* **destination interface** *interface-id* 可删除源端口或目的端口。

下面这个例子说明如何创建一个 SPAN 会话：会话 1。首先，将当前会话 1 的配置清除掉，然后设置端口 gigabitEthernet 3/1 的报文镜像到端口 gigabitEthernet 3/8。**Show monitor session** 特权命令用于确认配置是否成功。

```
Ruijie(config)# no monitor session 1
Ruijie(config)# monitor session 1 source interface
gigabitEthernet 3/1 both
Ruijie(config)# monitor session 1 destination interface
gigabitEthernet 3/8
Ruijie(config)# end
Ruijie# show monitor session 1
sess-num: 1
src-intf:
GigabitEthernet 3/1 frame-type Both
dest-intf:
GigabitEthernet 3/8
```

session 1 是用来支持全局跨线卡端口镜像，要配置跨线卡 SPAN 只能使用 session 1。

5.3.3 从SPAN会话中删除一个口

用户可以按照以下步骤从一个 SPAN 会话中删除源端口。

命令	作用

Ruijie(config)# **no monitor session** *session_num* **source interface** *interface-id* [，| -] [**both	rx	tx**]	指定需删除的源端口。对于 interface-id，请指定相应的接口号。

使用 **no monitor session** *session_num* **source interface** *interface-id* 全局配置命令可以从一个 SPAN 会话中删除源端口。下面这个例子显示如何将端口 gigabitEthernet 1/1 从会话 1 中删除并确认配置是否成功。

```
Ruijie(config)# no monitor session 1 source interface
gigabitethernet 1/1 both
Ruijie(config)# end
Ruijie# show monitor session 1
sess-num: 1
dest-intf:
GigabitEthernet 3/8
```

5.3.4 配置基于流的镜像

在全局配置模式下，按照以下步骤可以设置基于流的镜像。

命令	作用
Ruijie(config)# [**no**] **monitor session** *session_num* **source interface** *interface-id* **rx acl** *name*	设定需要镜像的流所匹配的 acl name，以及镜像源端口和目的端口

☑ 只支持入口镜像。

5.3.5 配置一对多镜像

如果用户需要将同一源端口的数据流镜像到多个目的端口，请按照以下步骤进行配置：

- 配置一个 RSPAN 会话(参见 RSPAN 配置指南)，该 RSPAN 的源口为一对多镜像源端口，转发口为非一个多镜像目的的其它以太网口。
- 在 RSPAN 转发口的接口模式下配置 MAC 自环功能。

命令	作用
Ruijie(config-if)# **mac-loopback**	设置接口 MAC 自环

将转发口和一对多镜像的目的端口以 Access 模式加入 RSPAN VLAN。

RSPAN 转发口最好不要有其它配置，也不要接插网线。

请不要配置 RSPAN 转发端口参与交换。

一对多镜像的无法镜像到 BPDU 等只送 CPU 不转发的报文。

5.3.6 其他注意事项

1) 请将网络分析仪连接到监控口。

31) 当 SPAN 处于使能状态，配置的变更有以下结果：

- 如果改变了源端口的 VLAN 配置，配置将马上生效。
- 如果改变了目的端口的 VLAN 配置，配置马上生效。
- 如果禁用了源端口或目的端口，SPAN 将不起作用。
- 如果将源端口或目的端口加入 AP，源端口或目的端口将退出 SPAN 会话。

5.4 显示SPAN状态

使用 **show monitor** 特权命令可显示当前 SPAN 配置的状态，下面这个例子说明了如何通过 **show monitor** 特权命令显示 SPAN 会话 1 的当前状态

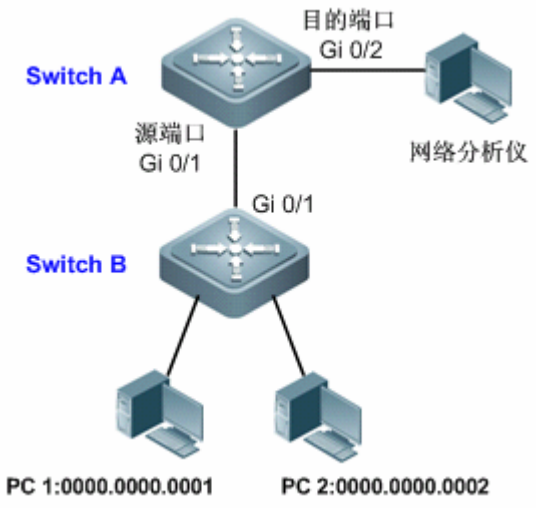
```
Ruijie# show monitor session 1
sess-num: 1
src-intf:
GigabitEthernet 3/1 frame-type Both
dest-intf:
GigabitEthernet 3/8
```

5.5 SPAN典型配置用例

5.5.1 基于流的镜像配置用例

拓扑图

图 5-2 SPAN 简单应用拓扑



应用需求

网络分析仪能够监控 Switch A 转发给 Switch B 的所有数据流，监控来自 Switch B 的特定数据流（如来自 PC1 和 PC2 的数据流）。

配置要点

1、在连接网络分析仪的设备上（本例为 Switch A）配置 SPAN 功能，将连接 Switch B 的端口（本例为 Gi 0/1）设置 SPAN 的源端口，将直连网络分析仪的端口（本例为 Gi 0/2）设置为 SPAN 的目的端口。

2、配置 SPAN 源端口（本例为 Gi 0/1）基于流的镜像（仅允许 PC1 和 PC2 的数据流）

配置步骤

第一步，配置互联设备的连接口。

！配置 Switch A 的端口 Gi 0/1 为 Trunk Port。

```
SwitchA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)#interface gigabitEthernet 0/1
SwitchA(config-if-GigabitEthernet 0/1)#switchport mode trunk
SwitchA(config-if-GigabitEthernet 0/1)#exit
```

第二步，配置 ACL。

！在 Switch A 上创建 MAC 扩展访问列表“ruijie”，允许源 MAC 为 0000.0000.0001 和 0000.0000.0002。

```
SwitchA(config)#mac access-list extended ruijie
SwitchA(config-mac-nacl)#permit host 0000.0000.0001 any
SwitchA(config-mac-nacl)#permit host 0000.0000.0002 any
SwitchA(config-mac-nacl)#exit
```

第三步，创建 SPAN 会话，并指定源端口和目的端口。

！在 Switch A 上，创建 Session 1，并指定 Gi 0/1 为源端口，镜像双向数据流，并配置基于流的入口镜像。

```
SwitchA(config)#monitor session 1 source interface gigabitEthernet 0/1 tx
SwitchA(config)#monitor session 1 source interface gigabitEthernet 0/1 rx acl ruijie
```

！在 Switch A 指定端口 Gi 0/2 为 Session 1 的镜像目的端口

```
SwitchA(config)#monitor session 1 destination interface gigabitEthernet 0/2
```

验证结果

第一步，查看设备的配置信息。

```
SwitchA#show running-config
!
```

```
mac access-list extended ruijie
 10 permit host 0000.0000.0001 any etype-any
 20 permit host 0000.0000.0002 any etype-any
!
interface GigabitEthernet 0/1
 switchport mode trunk
!
monitor session 1 destination interface GigabitEthernet 0/2
monitor session 1 source interface GigabitEthernet 0/1 tx
monitor session 1 source interface GigabitEthernet 0/1 rx acl ruijie
!
```

第二步，查看设备的 SPAN 状态。

```
SwitchA#show monitor session 1
sess-num: 1                              //SPAN Session
span-type: LOCAL_SPAN                   //本地镜像
src-intf:                                 //SPAN 源端口信息
GigabitEthernet 0/1         frame-type Both
rx acl id 2900                          //基于流的镜像
acl name ruijie
dest-intf:                               //SPAN 目的端口信息
GigabitEthernet 0/2
```

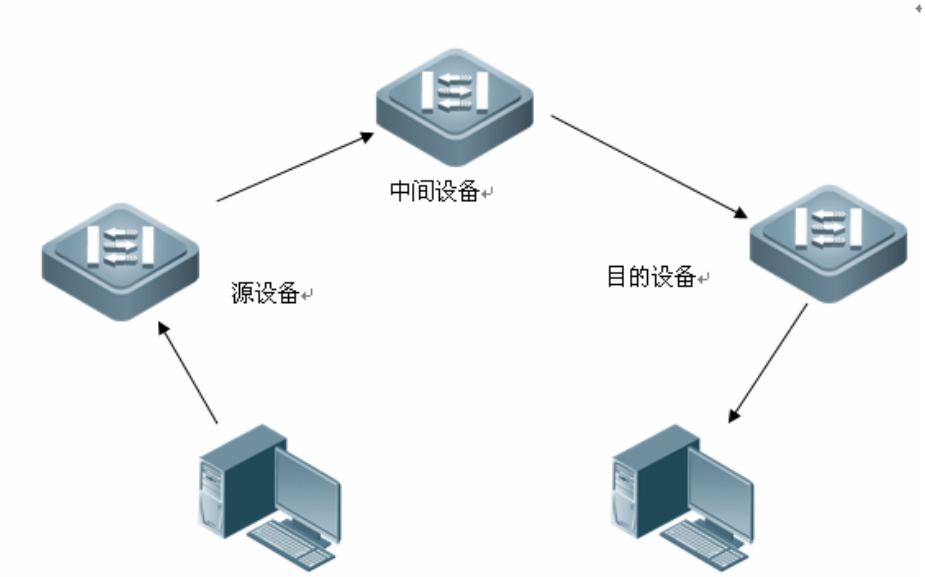
6 RSPAN

6.1 概述

远程端口镜像（RSPAN）是本地端口镜像（SPAN）的扩展，远程端口镜像突破了源端口和目的端口必须在同一台设备上的限制，使源端口和目的端口之间可以跨越多个网络设备。这样网络管理员就可以坐在中心机房通过分析仪观测远端被镜像端口的数据报文。

RSPAN 实现的功能是将所有的被镜像报文通过一个特殊的 RSPAN VLAN（称为 Remote VLAN）传递到远端镜像设备的目的端口，典型应用拓扑如下所示：

图 6-1 RSPAN 典型应用拓扑图



图中各设备的角色分为三种：

- 源交换机：远程镜像源端口所在的交换机，负责将源端口的报文复制一份从源交换机的输出端口输出，通过 Remote VLAN 进行转发，传输给中间交换机或目的交换机。
- 中间交换机：网络中处于源交换机和目的交换机之间的交换机，通过 Remote VLAN 把镜像报文传输给下一个中间交换机或目的交换机。如果源交换机与目的交换机直接相连，则不存在中间交换机。
- 目的交换机：远程镜像目的端口所在的交换机，将从 Remote VLAN 接收到的镜像报文通过镜像目的端口转发给监控设备。

各个交换机上参与 RSPAN 的端口如下所示。

交换机	参与镜像的端口	作用
源交换机	源端口（Source Port）	被监测的用户端口，通过本地端口镜像把用户数据报文复制到指定的输出端口，源端口可以有多个
	输出端口	将镜像报文发送到中间交换机或者目的交换机

中间交换机	普通端口	将镜像报文发送到目的交换机。 建议中间交换机上配置两个 Trunk 端口，和两侧的设备相连
目的交换机	源端口	接收远程镜像报文
	镜像目的端口（Destination port）	远程镜像报文的监控端口

为了实现远程端口镜像功能，需要定义一个特殊的 VLAN，称之为 Remote VLAN。这个 VLAN 只传输镜像报文，不能用来承载正常的业务数据。所有被镜像的报文通过该 VLAN 从源交换机传递到目的交换机的指定端口，实现在目的交换机上对源交换机的远程端口的报文进行监控的功能。

- 在源交换机、中间交换机和目的交换机上，RSPAN 与本地 SPAN 功能可以共存，互不冲突。
- 远程镜像 Remote VLAN 内的报文不影响设备的 CPU 利用率
- 支持指定镜像目的口允许或不允许对外通讯，默认不允许对外通讯。
- 建议将镜像源端口设置于不同 VLAN 内。
- Remote VLAN 不能是 VLAN 1，也不能是 Private VLAN。
- Remote VLAN 不参与 GVRP。

6.2 配置RSPAN

- 配置准备
- 源交换机上的配置
- 中间交换机上的配置
- 目的交换机上的配置
- 基于流的 RSPAN 配置
- 配置举例

6.2.1 配置准备

- 确定源交换机、中间交换机、目的交换机
- 确定镜像源端口、镜像目的端口、Remote VLAN
- 通过配置保证 Remote VLAN 内从源交换机到目的交换机的二层互通性
- 确定被监控报文的方向
- 启用 Remote VLAN

6.2.2 源交换机上的配置

- RSPAN 会话

- 源端口
- 输出端口
- Remote VLAN
- VSPAN 配置
- 配置步骤

RSPAN 会话

RSPAN 会话具有本地 SPAN 会话相同的特性，具体见 SPAN 配置指南。

源端口

源端口也被称为被监控口，在 RSPAN 会话中，源端口上的数据流被监控，用于网络分析或故障排查。在单个 RSPAN 会话中，用户可以监控输入、输出或双向数据流，且源端口的个数没有限制。

源端口具有以下特性：

- 源端口可以是 switched port，routed port 或 AP（Aggregate Port）；
- 支持将源设备上的多个源端口镜像到指定的输出端口；
- 源端口与输出端口不能为同一端口；
- 当镜像源端口为三层接口时，监控的报文包括二层报文和三层报文；
- 在双向监控多个端口的情况下，一份报文由一个端口进入，从另外一个端口输出，只要有监控到一份报文视为正确；
- 当启用 STP 的端口处于 block 状态时，该端口输入、输出的报文能够被监控到；
- 源端口和目的端口可以属于同一 VLAN，也可以属于不同 VLAN。

输出端口

RSPAN 镜像数据流从源设备的输出端口向中间设备广播出去，输出端口具有以下特性：

- 输出端口可以是 switched port，routed port 或 AP（Aggregate Port）。
- 输出端口只能属于一个 RSPAN 会话。

☑ S5750S 系列产品不支持 AP(Aggregate Port)口作为输出端口。

Remote VLAN

RSPAN 镜像的数据流通过 Remote VLAN 进行广播，这个 VLAN 只传输镜像报文，不能用来承载正常的业务数据。所有被镜像的报文通过该 VLAN 从源交换机传递到目的交换机的指定端口，实现在目的交换机上对源交换机的远程端口的报文进行监控的功能。

Remote VLAN 具有以下特性：

- Remote VLAN 不能是 VLAN 1，也不能是 Private VLAN。

- 一个 Remote VLAN 对应一个 RSPAN session。

VSPAN 配置

VSPAN 是 VLAN SPAN 的简称，是指将某些 VLAN 的数据流作为数据源镜像到目的设备的目的端口。

VSPAN 具有以下特性：

- 可以指定某个 VLAN 作为镜像的数据源，这个 VLAN 不能是 Remote VLAN。配置命令为 **monitor session** *session-num* **source vlan** *vlan-id* [rx | tx | both]。
- 可以指定某些 VLAN 作为镜像的数据源，这些 VLAN 不能是 Remote VLAN。配置命令为 **monitor session** *session-num* **filter vlan** *vlan-id-list*。

源交换机上的配置步骤

源设备的配置步骤如下所示：

命令	作用
Ruijie# **configure**	进入全局配置模式
Ruijie(config)# **vlan** *vlan-id*	进入 Vlan 配置模式
Ruijie(config-Vlan)# **remote-span**	设置 Vlan 为 remote-span Vlan
Ruijie(config-Vlan)# **exit**	退到全局配置模式
Ruijie(config)# **monitor session** *session_num* **remote-source**	配置远程源镜像
Ruijie(config)# **monitor session** *session-num* **source interface** *interface-name*[**rx | tx | both**]	配置远程镜像源端口（源口的 rx，tx 可以配置到同一个目的口，也可以配置到不同的目的口，但每一个只能配置到一个目的口）
Ruijie(config)#**monitor session** *session_num* **destination remote vlan** *remote_vlan-id* **interface** *interface-name* [**switch**]	**switch** 关键字表示目的口参与交换
Ruijie(config)# **monitor session** *session_number* **source interface** *interface-id* **rx acl** *name*	设定需要镜像的流所匹配的 **acl** *name*

建议不要将普通端口加入 Remote VLAN。

不要在与中间交换机或目的交换机相连的端口上配置镜像源端口，否则可能引起网络内的流量混乱。

6.2.3 中间交换机上的配置

RSPAN 会话的中间设备确保远程镜像 VLAN 内的报文的透传，配置过程如下：

命令	作用
Ruijie# **configure**	进入全局配置模式
Ruijie(config)# **vlan** *vlan-id*	进入 vlan 配置模式
Ruijie(config-vlan)# **remote-span**	设置 vlan 为 remote-span Vlan
Ruijie(config-vlan)# **exit**	退到全局配置模式

6.2.4 目的交换机上的配置

目的端口

RSPAN 远程设备将 Remote VLAN 接收到的镜像报文通过目的端口转发给监控设备。目的端口具有如下特性：

目的端口可以是 switched port，routed port 或 AP（Aggregate Port）。

用户可以指定镜像目的端口允许或不允许对外通讯，默认状态是不允许对外通讯。目的端口处于不允许通讯状态下时，既不允许转发其他端口的数据报文，也不允许转发 CPU 发出的报文。

☑ S5750S 系列产品不支持 AP(Aggregate Port)口作为目的端口。

配置步骤

命令	作用
Ruijie# **configure**	进入全局配置模式
Ruijie(config)# **vlan** *vlan-id*	进入 vlan 配置模式
Ruijie(config-vlan)# **remote-span**	设置 vlan 为 remote-span vlan
Ruijie(config-vlan)# **exit**	退到全局配置模式
Ruijie(config)# **monitor session** *session_num* **remote-destination**	配置远程目的镜像
Ruijie(config)# **monitor session** *session-num* **destination remote** vlan *vlan-id* **interface** *interface-name* [**switch**]	配置 Remote VLAN 和远程镜像目的端口 **switch** 关键字表示目的口参与交换
Ruijie(config)# **interface** *interface-name*	进入远程镜像目的端口
Ruijie(config-if)# **switchport access vlan** *vid* | **switchport trunk native vlan** *vid*	vid 表示 remote-span vlan 的 vid 如果目的口是 access 口，则把它加入 remote-span vlan 如果目的口是 trunk 口，则把它加入 remote-span vlan，并且将 remote-span vlan 设置成它的 native vlan

6.2.5 基于流的RSPAN配置

RSPAN 是对本地 SPAN 的扩展，因此 RSPAN 同样也支持基于流的镜像（具体配置见镜像的配置指南）。

基于流的 RSPAN 不影响正常通讯。

用户可以在 RSPAN 源设备上配置源端口的 in 方向的 ACL，支持标准 ACL、扩展 ACL、MAC ACL、自定义 ACL。

用户可以在 RSPAN 源设备上配置源端口的 in 方向的端口 ACL，可以在 RSPAN 目的设备上配置目的端口 out 方向的端口 ACL。

用户可以在 RSPAN 源交换机上基于 Remote VLAN 应用 out 方向的 ACL，在 RSPAN 目的交换机上基于 Remote VLAN 应用 in 方向的 ACL。

6.2.6 显示RSPAN会话

命令	作用
show monitor	显示镜像

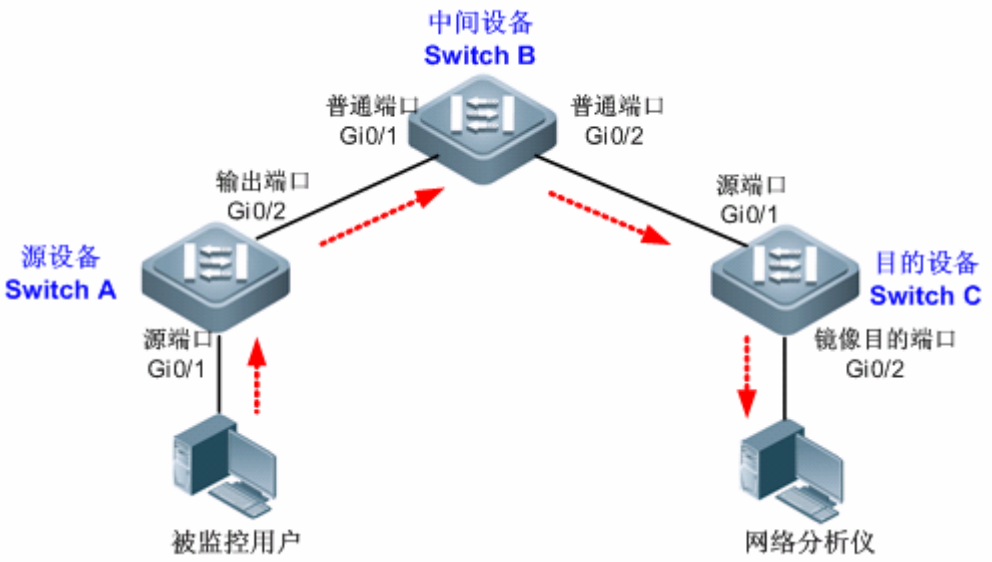
示例：

```
Ruijie# show monitor
sess-num: 1
src-intf:
GigabitEthernet 0/4 frame-type Both
dest-intf:
GigabitEthernet 0/6
remote vlan 3
```

6.3 RSPAN典型配置用例

拓扑图

图 6-2 RSPAN 的应用拓扑



应用需求

- 网络分析仪可以通过远程镜像监控用户。
- 设备之间均能正常交换数据。

配置要点

- 在源设备（本例为 Switch A）、中间设备（本例为 Switch B）、目的设备（本例为 Switch C）上配置 Remote VLAN。
- 在源设备上，配置直连用户的端口（本例为 Gi 0/1）为源端口，与中间设备相连的端口（本例为 Gi 0/2）为输出端口，并配置输出端口可交换功能。
- 在中间设备上，与源设备、目的设备相连的端口（本例为 Gi 0/1 和 Gi 0/2）仅需配置为普通端口。
- 在目的设备上，与中间设备相连的端口（本例为 Gi 0/1）作为源端口，仅需配置为普通端口，与网络分析仪相连的端口（本例为 Gi 0/2）配置为镜像目的端口，并配置镜像目的端口可交换功能。

通过源设备的输出端口转发的镜像数据流，可以在 Remote VLAN 中广播，则除源设备外的任意设备端口加入 Remote VLAN，便可对源端口进行监控，实现一对多远程镜像。如果在目的设备上指定一个镜像目的端口，则镜像数据流仅转发到该目的端口。

配置步骤

第一步，配置 Remote VLAN。

！在 Switch A 上创建 VLAN 7，设置为 Remote VLAN。

```
SwitchA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)#vlan 7
SwitchA(config-vlan)#remote-span
SwitchA(config-vlan)#exit
```

！在 Switch B、C 上配置同上。

第二步，配置 RSPAN 源设备。

！在 Switch A 上，配置端口 Gi 0/2 为 Trunk Port，用于连接 Switch B。

```
SwitchA(config)#interface gigabitEthernet 0/2
SwitchA(config-if-GigabitEthernet 0/2)#switchport mode trunk
SwitchA(config-if-GigabitEthernet 0/2)#exit
```

！在 Switch A 上，创建 RSPAN Session 1，设置为源设备，并设置端口 Gi 0/1 为源端口，端口 Gi 0/2 为输出端口。

```
SwitchA(config)#monitor session 1 remote-source
SwitchA(config)#monitor session 1 source interface gigabitEthernet 0/1 both
SwitchA(config)#monitor session 1 destination remote vlan 7 interface gigabitEthernet 0/2 switch
```

第三步，配置 RSPAN 中间设备

！在 Switch B 上，配置端口 Gi 0/1 和 Gi 0/2 为 Trunk Port。

```
SwitchB(config)#interface range gigabitEthernet 0/1-2
SwitchB(config-if-range)#switchport mode trunk
```

第四步，配置 RSPAN 目的设备

！在 Switch C 上，配置端口 Gi 0/1 为 Trunk Port，用于连接 Switch B 作为源端口。

```
SwitchC(config)#interface gigabitEthernet 0/1
SwitchC(config-if-GigabitEthernet 0/1)#switchport mode trunk
```

！在 Switch C 上，创建 RSPAN Session，设置为目的设备，并设置端口 Gi 0/2 为镜像目的端口。

```
SwitchC(config)#monitor session 1 remote-destination
SwitchC(config)#monitor session 1 destination remote vlan 7 interface gigabitEthernet 0/2 switch
```

验证结果

第一步，查看设备配置信息。

！Switch A 的配置

```
SwitchA#show running-config
!
vlan 7
 remote-span
!
interface GigabitEthernet 0/2
 switchport mode trunk
!
monitor session 1 remote-source
monitor session 1 destination remote vlan 7 interface GigabitEthernet 0/2 switch
monitor session 1 source interface GigabitEthernet 0/1 both
!
```

！Switch B 的配置

```
SwitchB#show running-config
!
vlan 7
 remote-span
!
interface GigabitEthernet 0/1
 switchport mode trunk
!
interface GigabitEthernet 0/2
 switchport mode trunk
```

！Switch C 的配置

```
SwitchC#show running-config
!
vlan 7
 remote-span
!
interface GigabitEthernet 0/1
 switchport mode trunk
```

```
!
monitor session 1 remote-destination
monitor session 1 destination remote vlan 7 interface GigabitEthernet 0/2 switch
```

第二步，查看设备的 RSPAN 信息

！查看 Switch A

```
SwitchA#show monitor
sess-num: 1                                          //RSPAN Session
span-type: SOURCE_SPAN                               //RSPAN 源设备
src-intf:                                            //RSPAN 源端口信息
GigabitEthernet 0/1         frame-type Both
dest-intf:                                           //RPSAN 输出端口信息
GigabitEthernet 0/2
remote vlan 7
mtp_switch on                                  //允许输出端口正常交换数据
```

！查看 Switch C

```
SwitchC#show monitor
sess-num: 1                                          //RSPAN Session
span-type: DEST_SPAN                                 //RSPAN 目的设备
dest-intf:                                           //RSPAN 目的端口信息
GigabitEthernet 0/2
remote vlan 7
mtp_switch on                                  //允许目的端口正常交换数据
```

7 IPFIX

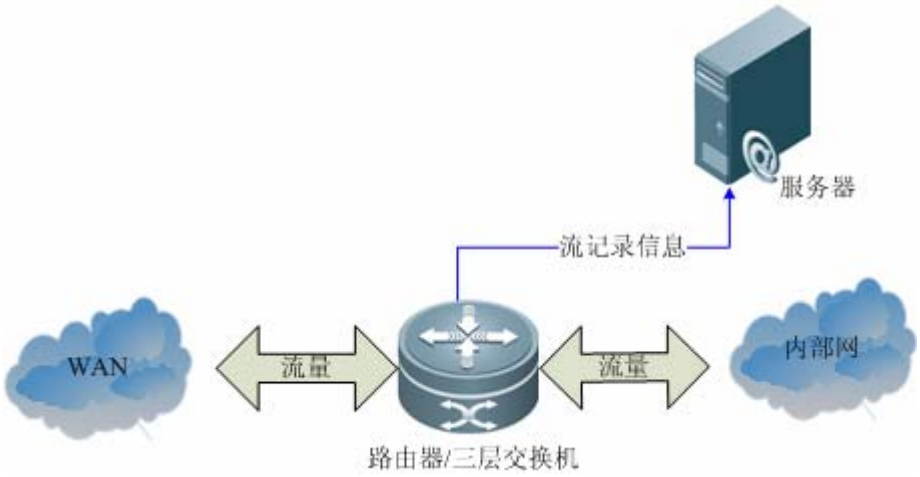
7.1 概述

随着网络的高速发展，为用户提供了更高的带宽和可预测的 QoS，同时用户也需要对网络进行更细致的管理和计费，为此就需要支持这种需求的相应技术，IPFIX 技术就是应这些需求产生。

为了完整记录网络数据传输状况，网络设备以七个关键域来表示每股网络流量：源 IP 地址、目的地 IP 地址、应用层源端口、应用层目的端口、三层协议类型、服务类型（Type-of-service）字节、输入接口号。如果不同的 IP 报文中所有的七个关键域都相同，那么所有这些 IP 报文都将被视为属于同一股流量。通过记录网络中这些流量的特征，如流量持续时间（开始和结束时间）、流的报文个数、字节数、流量中报文平均长度等，用户可以了解到当前网络的应用情况，根据这些信息对网络进行优化，安全检测，流量计费。

如下图所示：启用 IPFIX 功能的路由器/三层交换机会以流记录的方式统计网络传输的每一个 IP 报文，定时或在流结束时把流记录信息传输给服务器，服务器保存该流记录信息；服务器采用可视化的界面，根据用户的要求，分析和统计这些流信息，产生用户需要的统计信息，比如统计某个 IP 占用的带宽、或者某种应用占用的带宽。

图 7-1



IPFIX 全称为 IP Flow Information eXport，即 IP 流信息输出，它是由 IETF 公布的用于网络中的流信息测量的标准协议，它使网络中流量统计信息的格式标准化，使不同厂家的网络设备和服务器可以互通。

7.1.1 IPFIX应用

如上图所示，使能 IPFIX 流统计功能的路由器/交换机对报文中很多信息进行统计，包括三层协议类型、输入/输出接口号、源/目的 IP 地址、服务类型、字节数、报文数等，并且把这些信息输出给服务器，服务器可以对这些信息进行分析，广泛应用到诸如用户检测、网络分析与计划、安全分析、流量计费、网络流量工程等应用。

网络应用和用户检测

服务器软件可以分析 IPFIX 网络设备输出的流记录，获得详细、实时、基于应用的当前网络使用情况。例如，网络管理员可以查看 Web、文件传输协议（FTP）、VOIP、视频、Telnet 和其它著名的应用所占通信量的百分比。网络管理者可以根据这些信息来规划和分配网络和应用资源以满足用户需求。

服务器软件可以分析 IPFIX 流统计功能输出的流记录，获得用户利用网络和应用资源的详细情况，进而用于高效地规划和分配资源，并保障网络的安全运营。

网络规划

IPFIX 流统计功能可以检测长时间的网络流信息，使用户跟踪网络的变化规律，根据这些历史数据，对网络的变化进行有效的预测。同时设备采集的流记录数据可以用来对各种网络的升级计划进行有效的优化。它也可以在最小化网络花费同时最大化网络性能、容量及稳定性。IPFIX 功能还可以检测到用户不希望的广域网流量、不希望的带宽花费及不合适 QoS（Quality of Service，服务质量）的使用。IPFIX 流统计功能提供的信息可以有效地减少网络花费。例如当 WAN 链路上的流量增加时，用户一般会增加投资，进行链路升级，但这可能是某些用户的非法使用网络（使用 BT 下载）而导致的，有了 IPFIX 的流统计功能，用户就可以查找造成网络流量增加的真正原因，修改网络的使用策略，便可以解决这个问题，从而避免不必要的网络升级。

安全分析和攻击检测

服务器软件可以分析 IPFIX 流统计功能输出的流记录来实时识别 DoS 攻击、网络病毒、网络蠕虫等不安全因素。网络中不规则的变化都可以通过输出的流记录清楚地反映出来。例如 DoS 袭击的特征是向网络中发送大量报文，这些 IP 数据报文通常不同于普通的 IP 报文，一般从不可信源地址发往同一个目的地址，通过 IPFIX 能收集这些报文的源地址、目的地址、协议号、端口号及报文大小，然后将这些信息发往服务器，由网络安全专家或者安全软件进行分析，再结合其它网络控制（ACL，QoS），即可有效抑止恶意的网络攻击。

流量计费

IPFIX 流统计功能提供对网络中流量详细地测量，包括数据流的源/目的 IP 地址，报文数量、字节总数、时间标签、服务质量、应用层端口等，服务器软件可以利用这些信息进行基于时间、基于带宽、基于应用、基于网络服务质量的收费。

7.1.2 基本概念

IPFIX 采样

网络设备从一个接口接收报文，把报文从另一个接口发送出去，IPFIX 要对报文进行分析，需要指定对哪个接口流入或者流出的报文进行统计，这就是采样；锐捷设备可以指定对某个接口进行输入或者输出方向的采样，也可以两个方向同时采样。

IPFIX 流

网络转发设备根据报文的目的地址一个接一个转发报文，对于转发设备而言都是根据目的地址转发，没有必要知道这些报文的关联性，但是实际上这些报文是有一定的关联性，比如属于同一个 TCP Session。

一个报文由一系列的属性构成（比如 IP 地址，TCP 端口号），不同报文，有些报文的属性相同，在一段时间内流经某一探测点的具有某些相同属性的一系列连续报文，称之为一个报文流，这些用于决定报文是否属于相同流的报文属性称之为流的

关键属性，如果报文关键属性相同，那么这些报文属于同一个流。这些属性可以为 IP 报文头部的某些字段如 IP 源地址、Tos 字段以及这些字段的任意组合。在我司设备的实现中，一个流由如下关键字段的组合来确定：

- 源 IP 地址
- 目的 IP 地址
- 源端口号
- 目的端口号
- 三层协议类型
- Tos
- 输入/输出逻辑接口

这七个关键字段确定唯一的流，这七个字段都相同的报文属于同一个流，如果一个报文只要有一个关键字段不同于另一报文，则它们就属于不同的流。一个流还包括其它统计字段，如报文个数、下一跳 IP、流总字节数等。锐捷设备流信息还包括如下流量统计信息：

- 流开始时间
- 流结束时间
- 报文总数
- 字节总数

这里描述的 IPFIX 流，又称 IPFIX 基本流，或称主模式流，便于区分如下描述的聚合和聚合流。

IPFIX 流表

流表用来存储测量的 IP 流信息，对于一个 IP 报文，首先根据其流关键字段在主缓存中查找相应的流记录，不存在就创建一个新的流记录，记录流信息，若已存在该流记录，则更新流记录中的流统计信息，如报文个数、流字节数等。锐捷 IPFIX 流表中流的信息在 IPFIX 流章节中描述。

例如设备按顺序收到如下报文：

第 1 个报文

源 IP 地址	192.168.196.3
目的 IP 地址	218.30.66.101
源端口号	1000
目的端口号	80
三层协议类型	TCP
Tos	0x0
输入逻辑接口	Gi 1/0
……	
Bytes	100
Time:	2009/4/8 11:21:13

由于流表为空，为该报文建立新流表项，并且记录流信息：

Input ifx	Gi 1/0	
Src ip	192.168.196.3	
Dst ip	218.30.66.101	
Pro	TCP	
src port	1000	
Dst port	80	
Tos	0	
Start time	2009/4/8 11:21:13	
Stop time	2009/4/8 11:21:13	
packet	1	
bytes	100	

第 2 个报文

源 IP 地址	192.168.196.3
目的 IP 地址	218.30.66.101
源端口号	2000
目的端口号	80
三层协议类型	TCP
Tos	0x0
输入逻辑接口	Gi 1/0
……	
Bytes	100
Time:	2009/4/8 11:21:14

第 2 个报文由于源接口同第 1 个报文不一样，也是一个新的流，因此为该报文建立新流表项，并且记录流信息：

Input ifx	Gi 1/0	Gi 1/0
Src ip	192.168.196.3	192.168.196.3
Dst ip	218.30.66.101	218.30.66.101
Pro	TCP	TCP
src port	1000	2000
Dst port	80	80
Tos	0	0
Start time	2009/4/8 11:21:13	2009/4/8 11:21:14
Stop time	2009/4/8 11:21:13	2009/4/8 11:21:14
packet	1	1
bytes	100	100

第 3 个报文

源 IP 地址	192.168.196.3
目的 IP 地址	218.30.66.101
源端口号	1000
目的端口号	80

三层协议类型	TCP
Tos	0x0
输入逻辑接口	Gi 1/0
……	
Bytes	100
Time:	2009/4/8 11:21:15

第 3 个报文同第 1 个报文一样，属于第 1 个流表项中的流，统计第 1 个流信息

Input ifx	Gi 1/0	Gi 1/0
Src ip	192.168.196.3	192.168.196.3
Dst ip	218.30.66.101	218.30.66.101
Pro	TCP	TCP
src port	1000	2000
Dst port	80	80
Tos	0	0
Start time	2009/4/8 11:21:13	2009/4/8 11:21:14
Stop time	2009/4/8 11:21:15	2009/4/8 11:21:14
packet	2	1
bytes	200	100

这里描述的 IPFIX 流表，又称 IPFIX 基本流表，或称主模式流表，用于保存基本流，便于区分如下描述的聚合流和聚合流表。

IPFIX 基本功能

IPFIX 设备基本功能如下：

- 统计流信息：从传输的报文中获取报文属性，根据 7 个关键字段查找流表，如果不存在，该报文是新的流，创建流表项，并且统计流信息，如果不是新的流，更新流统计信息。
- 输出流信息给服务器：在适当的时机把流的统计信息发送给服务器，让服务器进行分析。

IPFIX 规范中，只定义 IPFIX 设备如何输出流记录，至于流记录的保存以及分析（IPFIX 服务器）不属于 IPFIX 规定的范畴

7.1.3 工作原理

IPFIX 流统计

网络设备 IPFIX 流统计流程如下：

32) 网络设备作正常转发，一个报文从一个接口输入，经过转发从另外一个接口输出。

33) 网络设备硬件在设备入口处查询流记录信息，如果存在对应的流记录，则更新流信息（比如 packet 数目，byte 数目），本次 IPFIX 统计完成；如果不存在对应的流记录，则将报文拷贝一份送到 CPU，继续步骤 3。

34) IPFIX 功能模块对采样到的报文进行分析，生成流记录，同时为该流记录加上时间戳，加入时间目的是为了记录流开始和结束的时间以及持续的时间。

35) IPFIX 功能模块将生成的流记录安装到硬件中，从而后续对该流记录对应的报文进行流量统计。

36) 在特定的时刻，流记录被删除，并且流记录信息被输出到 IPFIX 服务器。

IPFIX 流老化

流表中的流记录在一定情况下需要从流表中删除，并且把删除之前的统计信息输出给服务器，称之为流老化，这样就可以保证 IPFIX 服务器可以得到流的统计信息， IPFIX 流在以下情况下会老化流记录。

- 当在一定时间内（非活跃时间）没有检测到属于该流的报文，则这个流已经老化，应该输出。
- 当某个流持续太长时间，不能无限地记录它的信息，用户设定一个时间（活跃时间），当超过这个时间，它也应该被老化。
- 当进行 IPFIX 的相关配置时，流记录会被老化。

如果一个流表项被老化删除后，马上又接收到和该老化流七个关键字段一样的报文时，由于流表中不存在该流表项，该报文作为新的流处理，重新创建流表项。

IPFIX 流输出

流老化后流记录需要输出给服务器，当某个流记录需要输出时，该流记录的信息按照 IPFIX 定义的格式封装为 UDP 或者 TCP 报文，发往配置好的服务器，由服务器上的收集器进行处理。收集器是专门对流记录进行处理的软件工具，它可以根据接收的流记录信息可视化地显示当前网络中状态，分析网络流量等。

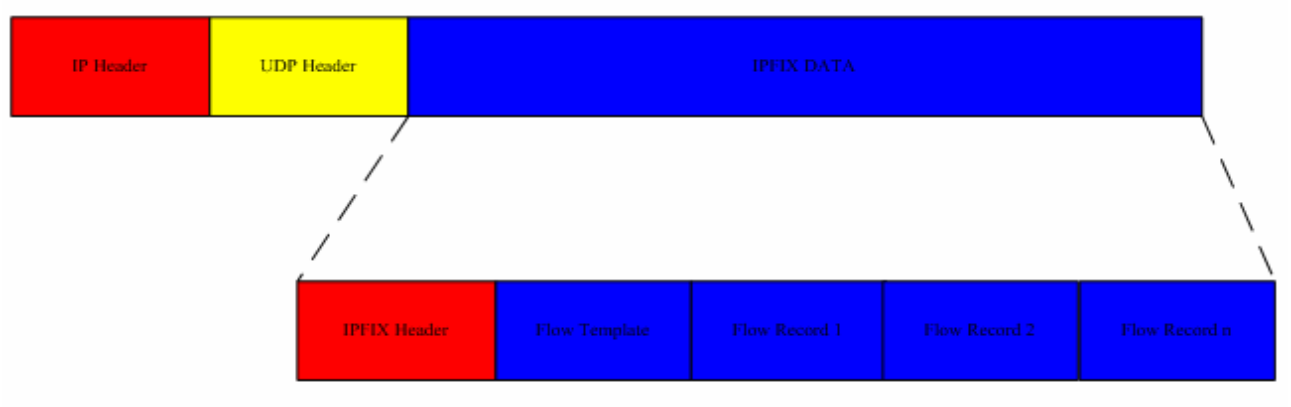
IPFIX 采用模板的方式来传输流记录，在发送流记录时，应首先创建该数据记录格式的模板，并且把模板发送给服务器，模板定义了数据记录中字段的属性、长度， IPFIX 定义的字段的属性非常多，有几百个，每个属性对应一个标识，用于标识属性的含义，例如标为 8 表示源 IP 地址；服务收到模板之后，根据模板就可以知道后续流记录的格式，并且按照模板定义流记录的格式来解释后续的 IPFIX 流记录。模板和流记录信息可以同时存在一个报文中，也可以一个报文附带多个流记录或者模板。

IPFIX 设备可以只发送流的重要属性，而服务端软件也可以从流记录只提起认为有用的流属性，其它的流属性可以忽略，例如有些锐捷设备认为 TCP Flag 可以用于分析网络安全，因此在流的输出信息中包含 TCP FLAG，但是有些服务端软件只用于流量分析，没有网络分析功能，它可以忽略设备发出的 TCP FLAG，设备和服务端不存在兼容性问题。

同样当网络设备在数据记录中扩展新的字段时（流的属性），网络设备只需重新创建对应的数据模板即可，服务器就可以根据新的模板解释流记录信息，而不需要对服务器软件进行升级，极大提高了可扩展性。

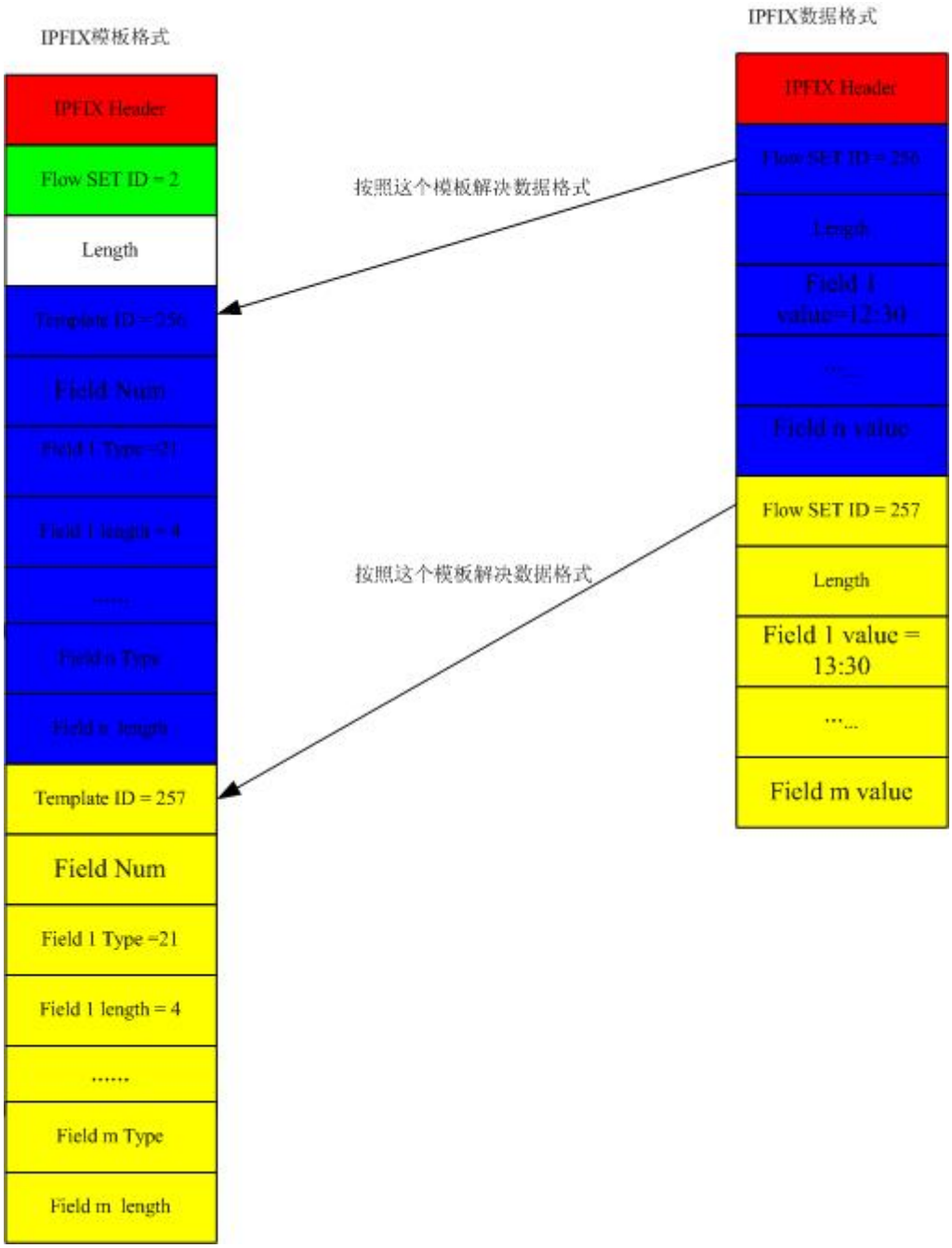
下面以 UDP 为例描述 IPFIX 的模板和数据。

图 7-2 IPFIX 报文格式



如图：IPFIX 报文包含：模板和流记录，IPFIX 报文前面会加一个 IPFIX 报文头，并且以 UDP 的方式传输。

图 7-3 IPFIX 模板和数据的对应关系



IPFIX 模板格式说明：

Flow Set ID = 2 表示后续内容是模板，用于描述某几个流记录格式。

Length:表示模板的长度。

Template ID = 256：表示后续描述的某一类流记录的格式，类型为 256

Field Num：表示该流记录格式由多少项组成。

Field n type：表示该流记录第 N 个项的含义，每个值代表的含义在 IPFIX 规范中有详细定义,比如 Field 1 type = 21 ，它定义流记录的第一项表示流开始的时间。

Field n length：表示该流记录第 N 项目的字节数，比如 Field 1 length = 4，它定义流记录第一项表示流开始的时间，并且该时间占用 4 个字节。

通过模板可以描述某个流记录的格式，包括由多少项组成，每个项的含义以及数据位宽。

IPFIX 数据格式说明：

Flow Set ID = 256 表示后续内容是流记录，并且按照模板 256 来解释后续的数据。

Length：表示数据的长度。

Field n Value：表示该流记录第 N 个项的的值，比如 Field 1 Value = 12:30 ,表示流开始的时间为 12:30,它占用 4 个字节（含义和位宽在模板中已经定义）。

IPFIX 流聚合

流聚合模式类似于上述描述的基本流模式，它也是对网络中的流信息进行统计，唯一不同的是二者流记录的关键字不同，基本流模式的关键字由七个元素构成（具体参见 1.1.2 节），而聚合模式依据其定义从基本流模式的七个元素中选出部分作为关键字，因此聚合模式下单条流的粒度较粗，可以有效的节省表项资源。

用户可以根据不同的需要，选择相应的聚合模式，从而产生出用户需要的流记录信息。例如用户只关心指定服务器上应用的分布情况，这时用户就可以选择使用 IP、三层协议号、端口号作为聚合关键字段的聚合模式，获得用户想要的流信息。

流聚合模式同基本流模式一样，有自己的流记录格式，它也有对应的老化机制，定时检查流聚合记录是否已经老化，一旦老化，也需要对其进行输出。

支持 4 种流聚合：

聚合模式	分类依据的关键字段
目的前缀聚合（destination-prefix）	目的地址掩码长度、目的前缀、接口索引（根据 IPFIX 的开启方向决定是接口方向，输入 IPFIX 功能对应的是入口，输出 IPFIX 功能对应的是出口）
源前缀聚合（source-prefix）	源地址掩码长度、源前缀、接口索引（根据 IPFIX 的开启方向决定是接口方向，输入 IPFIX 功能对应的是入口，输出 IPFIX 功能对应的是出口）
目的前缀—协议－目的端口聚合（destination-prefix-protocol- destination port）	源掩码长度、源前缀、协议号、四层源端口、接口索引（根据 IPFIX 的开启方向决定是接口方向，输入 IPFIX 功能对应的是入口，输出 IPFIX 功能对应的是出口）
源前缀—协议－源端口聚合（Source prefix-protocol-Source port）	源掩码长度、源前缀、协议号、四层源端口、接口索引（根据 IPFIX 的开启方向决定是接口方向，输入 IPFIX 功能对应的是入口，输出 IPFIX 功能对应的是出口）

除了关键字段外，每种聚合流还输出：

- 流开始时间
- 流结束时间
- 报文总数
- 字节总数

7.1.4 协议规范

文档	概述	备注
RFC 5470	Architecture for IP Flow Information Export	IPFIX 协议体系结构。总述了 IPFIX 的各个组成部分
RFC 5472	IP Flow Information Export (IPFIX) Applicability	描述了 IPFIX 能服务于哪些典型应用。对那几类典型应用做了细化及实现说明
RFC 5103	Bidirectional Flow Export Using IP Flow Information Export (IPFIX)	双向流的 IPFIX 输出。
RFC 5153	IP Flow Information Export (IPFIX) Implementation Guidelines	IPFIX 实现指导。概述了 IPFIX 中的几个知识要点的及关联。协助实现者找到实现方向。
RFC 5102	Information Model for IP Flow Information Export	IPFIX 各种元素、选项的定义及具体要求。
RFC 5101	Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information	IPFIX 协议交互细节。最主要的协议实现文档。描述了输出者和收集者的交互约定。报文格式的具体说明。
RFC 5473	Reducing Redundancy in IP Flow Information Export (IPFIX) and Packet Sampling (PSAMP) Reports	描述了 IPFIX 输出中一个带宽节省的方法。
RFC 3917	Requirements for IP Flow Information Export	IPFIX 的需求，简述了该协议的需求来源、简单协议原理。
RFC 5471	Guidelines for IP Flow Information Export (IPFIX) Testing	PFIX 的测试建议。
RFC 3954	Cisco Systems NetFlow Services Export Version 9	Cisco netflow V9

对于流输出技术，比较著名的还有 Cisco 的 NetFlow，Juniper 的 JFlow 等等，Cisco 的 Netflow 有 V1、V5、V7、V8、V9 多个版本，锐捷产品同时兼容 Cisco Netflow v9 和 IPFIX

7.2 配置IPv4 IPFIX

以下章节描述如何配置 IPv4 IPFIX 的基本特性

7.2.1 缺省配置

这里列出了 IPv4 IPFIX 的缺省配置：

功能特性	缺省值
IPv4 IPFIX 功能	禁止
输出目的地址 ip、端口号	无配置
源地址	无配置
报文格式	IETF(V10)
模板刷新率/重传时间间隔	20 个报文/10 分钟
选项数据刷新率/重传时间间隔	20 个报文/10 分钟

流记录表项数目	聚合模式与基本模式相同。 物理口上输入方向 1500 条流每 24 口，输出方向 500 条每 24 口，VSU 环境下容量可叠加； AP 口视其成员口分布情况而定： 对于有 48 个口的设备， 1. 若 AP 口的成员口全都分布在同一台设备的前 24 口或后 24 口，则 AP 口上支持的流记录容量情况与物理口相同； 2. 单机下若 AP 口的成员口同时分布在一台设备的前 24 口以及后 24 口，则该 AP 口上支持的留记录容量为整机输入方向 1500 条，输出方向 500 条； 3. VSU 环境下，若 AP 口的成员口分布在多台设备，其容量不能叠加，AP 口上流记录容量与单机情况相同。
流活跃老化时间	30 分钟
流非活跃老化时间	15 秒
聚合表项活跃老化时间	30 分钟
聚合表项非活跃老化时间	15 秒
流聚合模式下，源或目的地址的前缀掩码	默认值为 0，即无 mask 设置

IPFIX 功能与其它的安全相关应用（比如 ACL、安全通道等）共用硬件资源，IPFIX 功能的优先级低于其它安全相关应用，因此上述的流表项记录数目指的是最大容量，如果配置了大量的安全相关应用，IPFIX 的流记录容量会相应的减少。

7.2.2 配置采样

开启 IPFIX 采样后，报文会被硬件捕获到 CPU 进行软件分析，并依据相应的 IPFIX 模式生成流记录，最终将流记录安装到硬件中进行流量统计。

可通过如下命令来配置 IPFIX 采样：

命令	作用
Ruijie> **enable**	进入特权命令模式
Ruijie# **config terminal**	进入全局配置模式
Ruijie(config)# **interface** *interface-name*	进入物理端口配置模式
Ruijie(config-if)# **ip flow** { **ingress** | **egress** }	打开接口的 IPFIX 采样功能
Ruijie(config-if)# **end**	退回特权命令模式
Ruijie# **copy running-config startup-config**	保存配置。

由于需要将报文捕获到 CPU 进行分析，出于对 CPU 保护的考虑，对报文采样的速率进行了限制，因此不能线速建流，具体的建流速率取决于 CPP 功能限制的报文速率。

在输出方向无法将报文送 CPU，因此只能依据输入方向采样到的报文建流，若输入方向 IPFIX 采样功能开启，则依据采样到的报文关键字生成输入方向的 IPFIX 流记录，同时若输出 IPFIX 功能开启，由于通信是双向的，因此依据采样到的报文关键字可以预期相应的输出 IPFIX 流记录的关键字，从而生成输出 IPFIX 流记录。

在基本流模式下不支持输出方向的 IPFIX 采样。

7.2.3 配置监控范围

通过配置监控范围可以大大减少设备的 IPFIX 流表消耗，设备只为在监控范围内的流建立 IPFIX 流表，但不对统计进行控制。

命令	作用
Ruijie> **enable**	进入特权命令模式
Ruijie# **config terminal**	进入全局配置模式
Ruijie(config)# **interface** *interface-name*	进入物理端口配置模式
Ruijie(config-if)# **ip flow filter** *acl-name* { **ingress** | **egress** }	配置输入或输出 IPFIX 的监控范围，基于接口配置
Ruijie(config-if)# **ip flow** { **ingress** | **egress** }	打开接口的 IPFIX 功能
Ruijie(config-if)# **end**	退回特权命令模式
Ruijie# **copy running-config startup-config**	保存配置。

在接口上使能了 IPFIX 功能后，不能进行监控范围的变更(包括监控范围的解除、监控范围所关联的 ACL 变动等操作)。

监控范围仅用于控制建流的范围，而不对报文统计进行控制；比如监控范围设置的内容为 permit host 1.1.1.1，而若此时的聚合模式为源 IP 聚合，且掩码长度为 24；此时只会为源 IP 为 1.1.1.1 的报文建流，不会为其它源 IP 的报文建流；建流后生成的统计表项为源 IP 为 1.1.1.0/24，该表项会统计所有符合 1.1.1.0/24 的报文。

7.2.4 配置主模式流记录输出

当主缓存中的流记录老化时，软件使用输出机制将这些老化的流记录封装成相应格式的 UDP 报文，发送到配置的服务器。同时为了防止使用 UDP 协议发送流记录的数据模板不可靠而造成模板丢失，因此需要定时重传模板，以保证数据模板被正确接收。

在入口或出口的一个方向上，主模式与聚合模式只能二者选其一；

主模式下与聚合模式下均可配置 IPFIX 输出相关参数，相关模式下配置的输出参数只针对相应模式下生成的流记录生效；

7.2.4.1 配置输出目的IP地址和目的端口

锐捷产品可以配置最多两个输出服务器，配置命令如下：

命令	作用
Ruijie> **enable**	进入特权命令模式
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **ip flow-export destination** { { *ip-address* | *hostname*} *udp-port* }	配置输出目标的目的地址和目的端口。
重复上面步骤	配置多个输出目标的目的地址和目的端口，本系统可配置两个输出目标

Ruijie(config)# **end**	退回特权命令模式
Ruijie# **copy running-config startup-config**	保存配置。

使用 **no ip flow-export destination** { { **ipv6** *ipv6-address* | *ip-address* | *hostname* } *udp-port* } 删除某个输出目标

例如：

```
Ruijie# config terminal
Ruijie(config)#ip flow-export destination 192.168.217.76 1111
Ruijie(config)#ip flow-export destination ipv6 2222::2222 2222
Ruijie(config)#ip flow-export destination 192.168.217.76 3333
%Exceeded maximum export destinations
Ruijie(config)# end
```

上面配置第三个输出目标时将提示错误。

默认情况下，系统中没有配置任何输出目标，此时，流记录不会被输出，只是将信息记录在本设备中，以备查看；

输出的 IPFIX 报文的源地址，自动取本机和目的地址最匹配的地址。

7.2.4.2 配置输出的报文格式

用户可以设置输出报文格式为 Netflow V9 或 IETF(目前其版本号为 0x0A)。缺省为 IETF 格式。具体配置命令如下：

命令	作用
Ruijie> **enable**	进入特权命令模式
Ruijie# **config terminal**	进入全局配置模式
Ruijie(config)# **ip flow-export version** { **9	10** }	配置输出格式为 Netflow V9 或者 V10
Ruijie(config)# **end**	退回特权命令模式
Ruijie# **copy running-config startup-config**	保存配置。

例如：

```
Ruijie# config terminal
Ruijie(config)# ip flow-export version 9
Ruijie(config)# end
```

7.2.4.3 配置输出模板的相关参数

系统在输出网络流数据之前，应首先将对应的数据模板发送给服务器。UDP 协议作为一个不可靠的协议，可能造成数据模板的丢失，使服务器无法正确地解析流数据，因此为了保证可靠性，对数据模板的发送采用重传机制。RGNOS 重传数据模板的机制有两种，一种以报文数量为计量单位，每发送 n 个数据报文，重传一次数据模板；另一种使用时间为单位，每隔一段时间重传数据模板。具体配置命令如下：

命令	作用
Ruijie> **enable**	进入特权命令模式
Ruijie# **config terminal**	进入全局配置模式

Ruijie(config)# **ip flow-export template refresh-rate** *packets*	设定重传的报文间隔，单位为报文个数，默认值为 20 个报文，配置范围为 1－600
Or: Ruijie(config)# **ip flow-export template timeout-rate** *minutes*	设定重传的时间间隔,单位为分钟，默认值为 10 分钟，配置范围为 1－3600
Or: Ruijie(config)# **ip flow-export template options export-stats**	使能输出选项数据报文，内容包括：IPFIX 输出报文总个数；IPFIX 输出流记录总数
Or: Ruijie(config)# **ip flow-export template options refresh-rate** *packets*	设定选项数据重传的报文间隔，单位为报文个数，默认值为 20 个报文，配置范围为 1－600
Or: Ruijie(config)# **ip flow-export template options timeout-rate** *minutes*	设定选项数据重传的时间间隔,单位为分钟，默认值为 10 分钟，配置范围为 1－3600
Ruijie(config)# **end**	退回特权命令模式
Ruijie# **copy running-config startup-config**	保存配置。

举例如下：

```
Ruijie# config terminal
Ruijie(config)# ip flow-export template refresh-rate 30
Ruijie(config)# ip flow-export template timeout-rate 40
Ruijie(config)# end
```

上面的例子设定发送数据模板报文间隔为 30 个报文，40 分钟；即每 30 个报文重传一次数据模板，每 40 分钟重传一次数据模板。

默认情况下，重传的报文间隔为 20，时间间隔为 10 分钟

聚合模式的输出模板相关参数需要在对应的聚合模式下进行配置才能生效。

7.2.5 配置主模式缓存

- 主模式缓存用来保存“IPFIX 流”章节定义的流的信息，每个流记录表项的大小是固定的，系统为每个活跃的流创建一个流记录表项，记录该流的特征信息及统计信息。系统会定时检查缓存中的所有记录表项，看是否已经老化，需要输出。具体的老化由以下条件判断：流变为非活跃，默认情况下，若一个流记录 15 秒内没有更新，则表示该流非活跃，应该老化该流，把流信息输出给服务器；
- 流持续活跃太长时间，默认情况下，一个流持续活跃 30 分钟，应该老化该流，把流信息输出给服务器；
- 当进行 IPFIX 的相关配置时，流记录会被老化。
- 当配置其它与 IPFIX 共用硬件资源的安全相关应用（如 ACL、安全通道等）时，如果硬件资源不足，会将 IPFIX 流老化掉，优先保证其它安全相关应用对硬件资源的需求。

7.2.5.1 配置缓存中流表项老化参数

使用下列命令来配置缓存中流记录表项的老化参数：

命令	作用
Ruijie> **enable**	进入特权命令模式
Ruijie# **config terminal**	进入全局配置模式
Ruijie(config)# **ip flow-cache timeout active** *minutes*	配置活跃老化时间，范围为 1－60 分钟
Or: Ruijie(config)# **ip flow-cache timeout inactive** *seconds*	配置非活跃老化时间，范围为 10－600 秒
Ruijie(config)# **end**	退回特权命令模式
Ruijie# **copy running-config startup-config**	保存配置。

活跃老化时间默认值为 30 分钟，非活跃老化时间默认值为 15 秒，使用 **no ip flow-cache timeout active** 和 **no ip flow-cache timeout inactive** 恢复它们的默认值。

举例如下：

```
Ruijie# config terminal
Ruijie(config)# ip flow-cache timeout active 20
Ruijie(config)# ip flow-cache timeout inactive 20
Ruijie(config)# end
```

7.2.6 配置流聚合模式

7.2.6.1 流聚合模式简介

一个流聚合模式，就是通过其定义的特定关键字段，对主模式的流进行重新的聚合产生新的流。系统为这些聚合模式保留一定的缓存，类似于主缓存，这里称作流聚合缓存。当一个流记录从主缓存老化后，它包含的流信息将用于对每个使能的流聚合缓存中相应的流聚合记录进行更新。用户可以单独地配置每个聚合模式的聚合表项老化参数、输出目的 ip 地址及输出目的 UDP 接口。同时，流聚合模式下的缓存表项老化机制与主模式下的老化机制相同。

本系统中支持以下流聚合模式：

- Destination Prefix 聚合模式
- Source Prefix 聚合模式
- destination-prefix-protocol- destination port 聚合模式
- Source prefix-protocol- Source port 聚合模式

聚合模式	分类依据的关键字段
目的前缀聚合（destination-prefix）	目的地址掩码长度、目的前缀、接口索引（根据 IPFIX 的开启方向决定是接口方向，输入 IPFIX 功能对应的是入口，输出 IPFIX 功能对应的是出口）

源前缀聚合（source-prefix）	源地址掩码长度、源前缀、接口索引（根据 IPFIX 的开启方向决定是接口方向，输入 IPFIX 功能对应的是入口，输出 IPFIX 功能对应的是出口）
目的前缀—协议－目的端口聚合（destination-prefix-protocol- destination port）	源掩码长度、源前缀、协议号、四层源端口、接口索引（根据 IPFIX 的开启方向决定是接口方向，输入 IPFIX 功能对应的是入口，输出 IPFIX 功能对应的是出口）
源前缀—协议－源端口聚合（Source prefix-protocol- Source port）	源掩码长度、源前缀、协议号、四层源端口、接口索引（根据 IPFIX 的开启方向决定是接口方向，输入 IPFIX 功能对应的是入口，输出 IPFIX 功能对应的是出口）

7.2.6.2 配置流聚合模式

命令	作用
Ruijie> **enable**	进入特权命令模式
Ruijie# **config terminal**	进入全局配置模式
Ruijie(config)# **ip flow-aggregation cache** { **destination-prefix** | **source-prefix** | **source-prefix-protocol-source-port** | **destination-prefix-protocol-destination-port** } [**ingress | egress**] 例如： Ruijie(config)# **ip flow-aggregation cache destination-prefix ingress**	进入相应的流聚合模式
Ruijie(config-flow-cache)# **cache timeout active** *minutes* 例如： Ruijie(config-flow-cache)# **cache timeout active** *15*	（配置可选）配置缓存中记录表项的活跃老化时间 • minutes 为配置的活跃老化时间，范围从 1 到 60 分钟。默认值为 30 分钟。
Ruijie(config-flow-cache)# **cache timeout inactive** *seconds* 例如： Ruijie(config-flow-cache)# **cache timeout inactive** *300*	（配置可选）配置缓存中记录表项的非活跃老化时间 • seconds 为设置的非活跃老化时间，范围从 10 到 600 秒。默认值为 15 秒。
Ruijie(config-flow-cache)# **export destination** { { *ip-address* | *hostname* } **udp-port** } 例如： Ruijie(config-flow-cache)# **export destination** *172.30.0.1 991*	（配置可选）使能流聚合记录输出 •ip-address | hostname 为输出目的 IP 地址或主机名字 •port 为目的 UDP 端口号
重复前一步骤，配置第二个输出目的	（配置可选）可以为每个聚合模式配置最多两个输出目标。
Ruijie(config-flow-cache)# **export version** [**9 | 10**] 例如： Ruijie(config-flow-cache)# **export version 9**	设置报文输出版本格式。Version 9 是按 Netflow V9 的标准，version 10 是按 IETF 的标准
Ruijie(config-flow-cache)# **enabled** 例如： Ruijie(config-flow-cache)# **enabled**	使能该聚合模式 只有使用该命令，该聚合模式才真正使能，默认情况下，所有聚合模式是 disable 的

Ruijie(config-flow-cache)# **exit** 例如： Ruijie(config-flow-cache)# **exit**	退出流聚合配置模式，进入全局配置模式
Ruijie(config)# **end** 例如： Ruijie(config)# **end**	退出全局配置模式至特权命令模式

- 主模式和各个聚合模式的配置相互独立，例如输出服务器地址、老化时间、输出版本格式等，主模式和各个聚合模式配置相互独立，他们的配置只对本模式起作用
- 入口/出口每个方向只能使能一种聚合模式，不能同时使能多个聚合模式，最后使能的聚合模式生效;
- 一旦在某个方向使能了聚合模式，相应方向的基本模式自动失效；聚合模式禁止掉之后，自动恢复为基本模式;

7.2.6.3 配置源或目的地址的前缀掩码

在 ipv4 流聚合配置模式下，使用 **mask** 命令设置源或目的地址的前缀掩码。

命令	作用
Ruijie(config-flow-cache)# **mask** { [**destination | source**] **minimum** *value* }	设置源或目的地址的前缀掩码。
Ruijie(config-flow-cache)# **no mask** { [**destination | source**] **minimum** }	恢复默认值。

前缀掩码聚合模式可以对流按其 IPV4 地址进行相应的流聚合，在进行聚合时，源地址或目的地址（有流聚合模式决定）与地址掩码进行相与操作，相与的结果作为关键字决定报文应该属于的流。用户可以根据自己相应的地址掩码：希望一个比较详细的统计信息，就选择一个大的掩码值，若只是想要一个大致的统计信息，则可选一个较小的掩码值。

只能在以下几种聚合模式才允许进行对地址掩码进行配置：

Destination Prefix 聚合模式 （只有目的地址掩码可以配置）

Source prefix 聚合模式 （只允许源地址掩码配置）

Source Prefix-protocol- Source port 聚合模式 （只允许源地址掩码配置）

Destination Prefix-protocol- Destination port 聚合模式 （只有目的地址掩码可以配置）

例如：

下面的例子显示如何配置 source-prefix 聚合模式的源地址掩码:

```
Ruijie(config)# ip flow-aggregation cache source-prefix
Ruijie(config-flow-cache)# mask source minimum 16
```

下面的例子显示如何配置 destination-prefix 聚合模式的目的地址掩码:

```
Ruijie(config)# ip flow-aggregation cache destination-prefix
Ruijie(config-flow-cache)# mask destination minimum 16
```

7.3 监视与维护

7.3.1.1 显示主模式输出配置信息

使用命令 **show ip flow export** 显示 ipv4 IPFIX 当前配置的输出信息，包括输出使能、输出目的，流记录输出报文格式等情况。

```
Ruijie(config)#show ip flow export
IPV4 cache for source-prefix-protocol-port aggregation ingress:
        Exporting flows to 192.168.196.14 (9996)
        Exporting using source IP address 1.1.1.1
        Version 10 flow records
        IPV4 Template ID = 256
                Template timeout = 1 Minute(s)
                Template refresh rate = 600
        0 flows exported in 0 udp datagrams
        0 flows failed to export
        0 messages failed to export
```

主模式和聚合模式下配置的输出信息都可以使用该命令来查看，只有相应模式被使能，并且配置了输出服务器地址，并且该服务器地址是可达的才显示相应的输出信息。

7.3.1.2 显示主缓存信息

使用命令 **show ip flow cache [sort-by { packet | byte }]**显示 ipv4 IPFIX 当前主模式下的报文流统计信息，包括报文大小分布，缓存表项使用情况等

由于 IPFIX 与其它安全相关应用共用硬件资源，因此无法得知准确的剩余表项，因此剩余表项数目显示为“-”。

7.3.1.3 显示流聚合配置信息

配置命令如下：

show ip flow cache aggregation { destination-prefix | source-prefix | destination-prefix-protocol- destination port | source prefix-protocol- Source port} [sort-by {packet | byte }]

显示 ipv4 IPFIX 各个聚合模式的缓存信息，包括该聚合模式的有效流记录个数，每条聚合流的等统计信息。

例如：

```
Ruijie(config)# show ip flow cache aggregation source-prefix-protocol-source-port ingress

        IPV4 Flow Switching Cache, 96 bytes

        1 active, - inactive, 1 added

        0 flow alloc failures
```

```
        Exporting flows to 192.168.196.14 (9996)

        4 ipv4 flows exported in 4 udp datagrams, 0 failed

        Last clearing of statistics 0 Days 00:10:50


SrcIf                       DstIf                       SrcIPAddress      pr  port  Pkts       B/Pk
Active
GigabitEthernet 0/1         -                           192.168.64.0      1   0     2339       68
257
Ruijie(config)#
```

7.3.1.4 清除流统计信息

在特权模式下，使用命令：**clear ip flow stats**

7.4 配置举例

7.4.1 配置IPv4 IPFIX

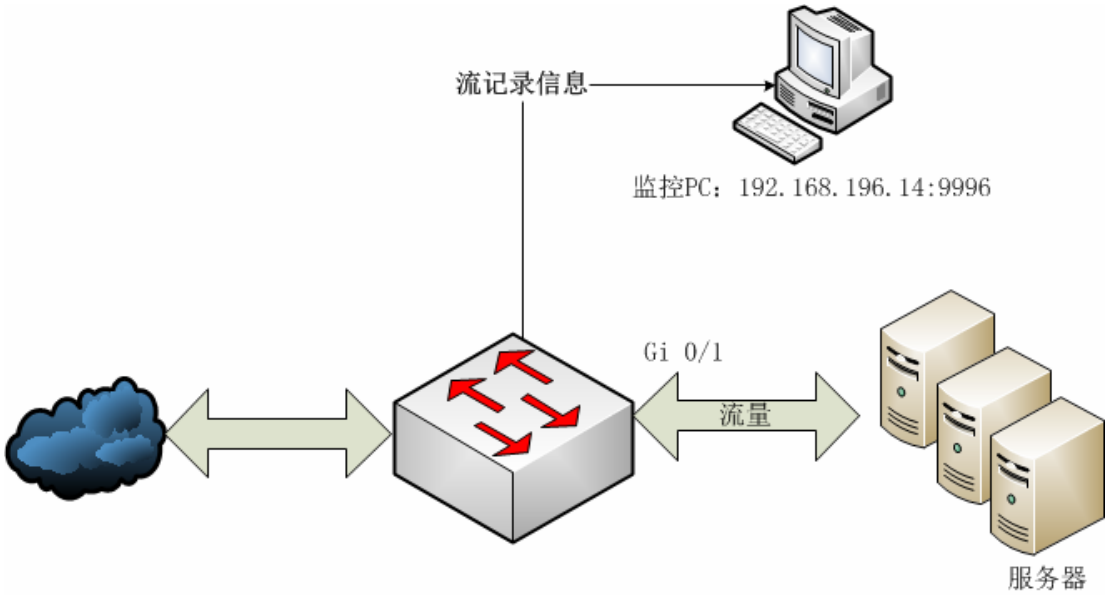
组网需求

某大学服务器接入交换机的 0/1 接口连接到服务器，需要对该台服务器的业务流量进行监控和分析，从而判断该服务器是否过载，从而作为是否应该进行服务器升级的判断依据；IPFIX 服务器软件采用 netflow analyzer,该软件支持 IPFIX V10,服务器的地址为 192.168.196.14，服务端口号为 9996，不给，要求只要流持续超过 10 分钟，就要把流统计信息发送给服务器，或者流空闲时间超过 10 秒，也要把流统计信息发送给服务器，综合用户需求，配置需求如下：

- 在交换机上运行 ipv4 IPFIX 功能。
- 配置输入和输出 IPFIX 模式为聚合模式，分别为：输入 Source prefix-protocol- Source port 聚合模式，输出 destination-prefix-protocol- destination port 聚合模式。
- 对接口 0/1 使能 ipv4 IPFIX 输入和输出采样功能。
- 接收服务器的 ip 地址为 192.168.196.14，端口号 9996。
- 报文格式为 IPFIX V10。
- active 和 inactive 老化时间为：10 分钟和 10 秒。
- 模板刷新频率是：每隔 600 个报文发送一次模板，并且定时 1 分钟发送一次模板。

组网拓扑

图 7-4 ipv4 IPFIX 组网图



配置步骤

- 配置输入聚合模式

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# ip flow-aggregation cache source-prefix-protocol-source-port ingress
Ruijie(config-flow-cache)# mask source minimum 32
Ruijie(config-flow-cache)#cache timeout active 10
Ruijie(config-flow-cache)#cache timeout inactive 10
Ruijie(config-flow-cache)#export destination 192.168.196.14 9996
Ruijie(config-flow-cache)# export template timeout-rate 1
Ruijie(config-flow-cache)# export template refresh-rate 600
Ruijie(config-flow-cache)# enabled
Ruijie(config-flow-cache)# exit
Ruijie(config)#
```

- 配置输出聚合模式

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# ip flow-aggregation cache destination-prefix-protocol-destination-port egress
Ruijie(config-flow-cache)# mask destination minimum 32
Ruijie(config-flow-cache)#cache timeout active 10
Ruijie(config-flow-cache)#cache timeout inactive 10
Ruijie(config-flow-cache)#export destination 192.168.196.14 9996
Ruijie(config-flow-cache)# export template timeout-rate 1
Ruijie(config-flow-cache)# export template refresh-rate 600
Ruijie(config-flow-cache)# enabled
Ruijie(config-flow-cache)# exit
```

```
Ruijie(config)#
```

■ 验证输出地址是否可达

```
Ruijie#ping 192.168.196.14
Sending 5, 100-byte ICMP Echoes to 192.168.196.14, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/10 ms
Ruijie#
```

■ 配置采样

```
Ruijie(config)#int g0/1
Ruijie(config-if-GigabitEthernet 0/1)#ip flow ingress
Ruijie(config-if-GigabitEthernet 0/1)#ip flow egress
Ruijie(config-if-GigabitEthernet 0/1)#exit
Ruijie#write
```

■ 验证 IPFIX

```
Ruijie#show ip flow export
IPV4 cache for source-prefix-protocol-port aggregation ingress:
        Exporting flows to 192.168.196.14 (9996)
        Exporting using source IP address 1.1.1.1
        Version 10 flow records
        IPV4 Template ID = 256
                Template timeout = 1 Minute(s)
                Template refresh rate = 600
        23 flows exported in 23 udp datagrams
        0 flows failed to export
        0 messages failed to export

IPV4 cache for destination-prefix-protocol-port aggregation egress:
        Exporting flows to 192.168.196.14 (9996)
        Exporting using source IP address 1.1.1.1
        Version 10 flow records
        IPV4 Template ID = 260
                Template timeout = 1 Minute(s)
                Template refresh rate = 600
        0 flows exported in 0 udp datagrams
        0 flows failed to export
        0 messages failed to export
Ruijie#

Ruijie#show ip flow interface
GigabitEthernet 0/1
  ip flow ingress
```

```
  ip flow egress
Ruijie#

Ruijie#show ip flow cache aggregation source-prefix-protocol-source-port ingress
        IPV4 Flow Switching Cache, 96 bytes
        1 active, - inactive, 7 added
        0 flow alloc failures
        Exporting flows to 192.168.196.14 (9996)
        25 ipv4 flows exported in 25 udp datagrams, 0 failed
        Last clearing of statistics 0 Days 00:26:31

SrcIf                DstIf                SrcIPAddress      pr  port  Pkts       B/Pk    Active
GigabitEthernet 0/1  -                    192.168.64.1      1   0     1382       68      150
Ruijie#

Ruijie#show ip flow cache aggregation destination-prefix-protocol-destination-port egress
        IPV4 Flow Switching Cache, 96 bytes
        1 active, - inactive, 15 added
        0 flow alloc failures
        Exporting flows to 192.168.196.14 (9996)
        2 ipv4 flows exported in 2 udp datagrams, 0 failed
        Last clearing of statistics 0 Days 16:52:48

SrcIf                DstIf                DstIPAddress      pr  port  Pkts       B/Pk    Active
-                    GigabitEthernet 0/1  192.168.64.1      1   0     0          0       0
Ruijie#
```