



配置手册

RG-S5750-28GT-S 交换机

RGOS 10.4(2b12)p2

文档版本号：V1.1

版权声明

锐捷网络©2014

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。

、、、、
®、®、®、®、
®、®、®、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 (2b12)p2

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>。
- 锐捷网络远程技术支持中心：<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://support.ruijie.com.cn>
- 锐捷网络技术支持与反馈信箱：service@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. 配置命令行界面
2. 配置基础管理
3. HTTP 服务
4. 配置 LINE 模式
5. 配置系统升级
6. 配置文件系统
7. 配置系统管理
8. 系统内存状态查看
9. 配置系统日志
10. 配置 USB 使用
11. 配置系统升级维护
12. 配置堆叠管理
13. 配置门限
14. 配置节能管理
15. 配置设备管理

1 配置命令行界面

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

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。	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#	要进入特权模式，输入 enable 命令。 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。 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。	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 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

1.3 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**

1.4 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。

1.5 理解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。

1.6 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。

1.7 使用编辑特性

1.7.1 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。
删除输入的字符。	Ctrl-A	光标移到命令行的首部。
	Ctrl-E	光标移到命令行的尾部。
	Backspace 键	删除光标左边的一个字符。
输出时屏幕滚动一行或一页。	Delete 键	删除光标所在的字符。
	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。

1.7.2 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 **mac-address-table static** 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。

```
mac-address-table static 00d0.f800.0c0c vlan 1
interface
$static 00d0.f800.0c0c vlan 1 interface fastEthernet
$static 00d0.f800.0c0c vlan 1 interface fastEthernet 0/1
```

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：

```
-address-table static 00d0.f800.0c0c vlan 1 interface $
```



注意

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。

1.8 CLI输出信息的过滤和查找

1.8.1 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
Step 1	<code>Ruijie# show any-command begin regular-expression</code>	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。



注意

- 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
Step 1	<code>Ruijie# show any-command exclude regular-expression</code>	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。
Step 2	<code>Ruijie# show any-command include regular-expression</code>	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。



注意

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。

1.9 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 0.0.0.0 192.1.1.1”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。

1.10 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（Outband）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 配置基础管理

2.1 概述



说明

有关本节引用的 CLI 命令的详细使用信息及说明，请参照《设备管理命令参考》。

2.1.1 通过命令的授权控制用户访问

2.1.1.1 概述

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。

2.1.1.2 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。

2.1.1.3 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
Step 1	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。
Step 2	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。
Step 3	Ruijie(config)# service password-encryption	设置是否对相关口令进行加密。
Step 4	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。

2.1.1.4 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。

2.1.1.4.1 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
Step 1	Ruijie# configure terminal	进入全局配置模式
Step 2	Ruijie(config)# privilege mode [all] {level level reset} command-string	设置命令的级别划分。 mode：一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。

2.1.1.4.2 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.
```

2.1.1.5 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
Step 1	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；
Step 2	Ruijie(config-line)# login	启用 line 线路口令保护

说明

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。

2.1.1.6 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。

2.1.1.6.1 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
Step 1	Ruijie(config)# password policy min-size length	设置口令最小长度 length：口令最小长度
Step 2	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。

2.1.1.6.2 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。强口令需要同时包含数字、小写字母、大写字母和特殊符号。

	命令	作用
Step 1	Ruijie(config)# password policy strong	设置强口令检查
Step 2	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。

说明

特殊字符是指除了数字、小写字母、大写字母以外的可见字符。空格符和“?”不能作为口令的特殊字符。

2.1.1.6.3 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 times** 配置。

	命令	作用
Step 1	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 <i>times</i> : 最近几次已配置过的口令
Step 2	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。

2.1.1.6.4 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
Step 1	Ruijie(config)# password policy life-cycle days	配置口令生存周期 <i>days</i> : 口令生存周期，单位：天
Step 2	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。

2.1.1.7 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，系统自动解锁。

	命令	作用
Step 1	Ruijie(config-line)# lockable	启用锁住 line 终端的功能
Step 2	Ruijie# lock	锁住当前 line 终端

2.1.2 登录认证控制

2.1.2.1 概述

前面一节我们描述了如何通过配置本地保存的口令来控制对网络设备的访问。除了线路口令保护和本地认证外，如果启用了 **AAA** 模式，则在用户登录网络设备进行管理时，在登录时我们还可以通过一些服务器来根据用户名和密码进行用户的管理权限的认证，目前我们还支持利用 **RADIUS** 服务器根据用户登录时的用户名和密码控制用户对网络设备的管理权限。

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

2.1.2.2 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
Step 1	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
Step 2	Ruijie(config)# username name [privilege level]	为用户设置权限级别（可选）

2.1.2.3 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
Step 1	<code>Ruijie(config)#username name permission oper-mode filename</code>	设置用户对指定文件操作权限
Step 2	<code>Ruijie(config)#no username name permission oper-mode filename</code>	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：`n`：无权限；`r`：读权限；`w`：写权限；`x`：执行权限，对于 `rw` 权限可进行组合设置，如 `rw` 代表读、写权限；`rx` 代表读、执行权限；`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 rw /`

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。

2.1.2.4 限制用户账号进行远程登录

锐捷产品支持限制本地用户账号进行远程登录。为了兼容以前的用户账号，在未配置限制本地用户进行远程登录的情况下，本地用户账号均允许进行远程访问。

要限制本地用户账号进行远程登录，请在全局配置模式下，根据需求执行以下命令：

	命令	作用
Step 1	<code>Ruijie(config)#username name reject rlogin</code>	限制本地用户账号进行远程登录
Step 2	<code>Ruijie(config)#no username name reject rlogin</code>	取消本地用户账号进行远程登录的限制

在配置了限制本地用户账号进行远程登录的时候，用户将不能使用该本地用户账号登录到设备。

2.1.2.5 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
Step 1	<code>Ruijie(config-line)# login local</code>	AAA 认证模式关闭时，设置线路登录进行本地认证
Step 2	<code>Ruijie(config-line)# login authentication {default list-name}</code>	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。

说明

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。

2.1.3 系统时间配置

2.1.3.1 概述

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，当第一次使用时你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，你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。

2.1.3.2 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
Step 1	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
```

2.1.3.3 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
```

2.1.3.4 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
Step 1	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
```

2.1.4 定时重启

2.1.4.1 概述

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。**modifiers** 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。

 说明

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,否则有可能会设置失效，比如将系统时间调到重启时间之后。

2.1.4.2 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
Step 1	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

2.1.4.3 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
Step 1	Ruijie# reload in mmm [reload-reason]	指定系统 <i>mmm</i> 分钟后 reload ， reload 的原因是 <i>reload-reason</i> (如果有输入的话)
Step 2	Ruijie# reload in hhh:mm [reload-reason]	指定系统 <i>hhh</i> 小时 <i>mm</i> 分钟后 reload ， reload 的原因是 <i>reload-reason</i> (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.
```

2.1.4.4 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。

2.1.4.5 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
Step 1	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。

2.1.5 系统名称和命令提示符

2.1.5.1 概述

为了管理的方便，你可以为一台网络设备配置系统名称(System Name)来标识它。同时如果你还没有为 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”。

2.1.5.2 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
Step 1	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 个字符。

你可以在全局配置模式下使用 **no hostname** 来将系统名称恢复位缺省值。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
```

2.1.5.3 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。你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
Step 1	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。

你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。

2.1.6 标题配置

2.1.6.1 概述

当用户登录网络设备时，你可能需要告诉用户一些必要的信息。你可以通过设置标题来达到这个目的。你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，你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。

2.1.6.2 配置每日通知

你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。您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
Step 1	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，现在你可以开始输入文本，你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。

你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)#
```

2.1.6.3 配置登录标题

您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
Step 1	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，现在你可以开始输入文本，你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)#
```

2.1.6.4 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。

2.1.7 查看系统信息

2.1.7.1 概述

你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。

2.1.7.2 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
Step 1	Ruijie# show version	显示系统、版本信息

说明

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。

说明

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。

2.1.7.3 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
Step 1	Ruijie# show version devices	显示网络设备当前的设备信息

2.1.8 控制台速率配置

2.1.8.1 概述

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。您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。

2.1.8.2 设置控制台速率

在线路配置模式下，您可以使用以下命令来设置控制台的速率：

	命令	作用
Step 1	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
  
```

```

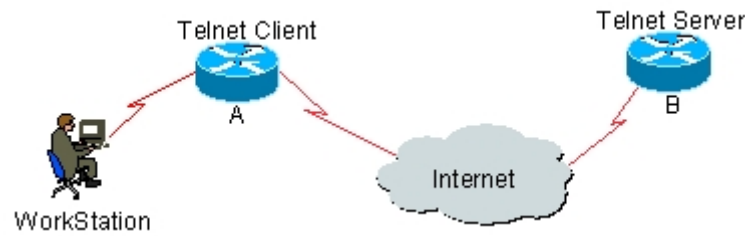
              never          never
History is enabled, history size is 10.
Total input: 22 bytes
Total output: 115 bytes
Data overflow: 0 bytes
stop rx interrupt: 0 times
Modem: READY

```

2.1.9 在网络设备上使用telnet

2.1.9.1 概述

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，并对其配置管理。



2.1.9.2 使用Telnet Client

您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
Step 1	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 IPV4 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:

```

2.1.9.3 使用Telnet Server

您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
Step 1	Ruijie# enable service telnet-server	打开 Telnet Server 服务；该命令同时打开 IPV4 服务；

2.1.10 连接超时设置

2.1.10.1 概述

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。

2.1.10.2 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
Step 1 Ruijie(config-line)# exec-timeout <i>minutes</i> [<i>seconds</i>]	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。 <i>minutes</i> : 指定的超时时间的分钟数； <i>seconds</i> : 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
```

2.1.10.3 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
Step 1 Ruijie(config-line)# session-timeout <i>minutes</i> [<i>output</i>]	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。 <i>minutes</i> : 指定的超时时间的分钟数； <i>output</i> : 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 exec-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
```

2.1.11 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

Step 1	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 vty 1 16
Ruijie(config-line)# transport input all
Ruijie(config-line)# no exec
Ruijie(config-line)# end
```



说明

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。

2.1.12 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
Step 1	Ruijie(Config)# enable service snmp-agent	打开 SNMP Server
Step 2	Ruijie(Config)# enable service ssh-sesrver	打开 SSH Server
Step 3	Ruijie(Config)# enable service telnet-server	打开 Telnet Server
Step 4	Ruijie(Config)# enable service web-server	打开 Http 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
```

2.1.13 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
Step 1	Ruijie(Config)# ip http port number	指定 HTTP 服务端口，默认是 80

Step 2	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。以下例子在交换机上打开 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 //打开 Web 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
```

3 HTTP服务

3.1 概述

3.1.1 HTTP协议简介

HTTP 是 Hypertext Transfer Protocol(超文本传输协议)的简称。它用来在 Internet 上传递 Web 页面信息。HTTP 位于 TCP/IP 协议栈的应用层，传输层采用面向连接的 TCP。

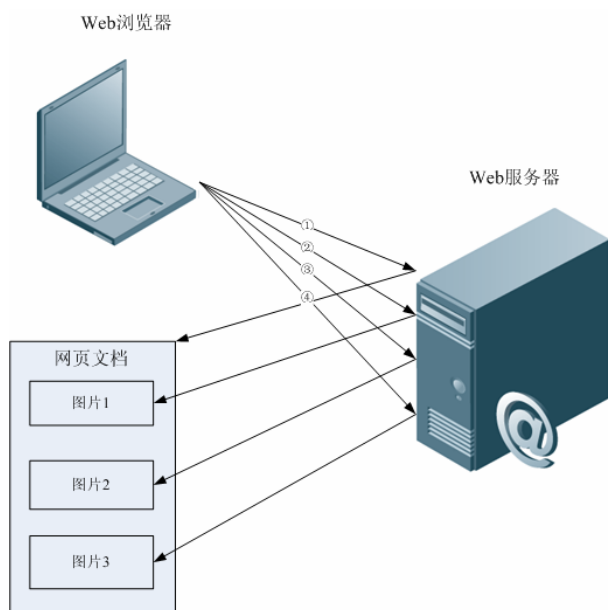
HTTPS (Hypertext Transfer Protocol Secure) 是支持 SSL (Secure Sockets Layer, 安全套接层) 协议的 HTTP 协议。主要思想是在不安全的网路上创建一个安全的通道，保证信息很难被监听以及对中间人攻击提供一定的合理保护。HTTPS 目前已被广泛用于互联网上安全敏感的通讯，如电子交易支付等。

3.1.2 基本概念

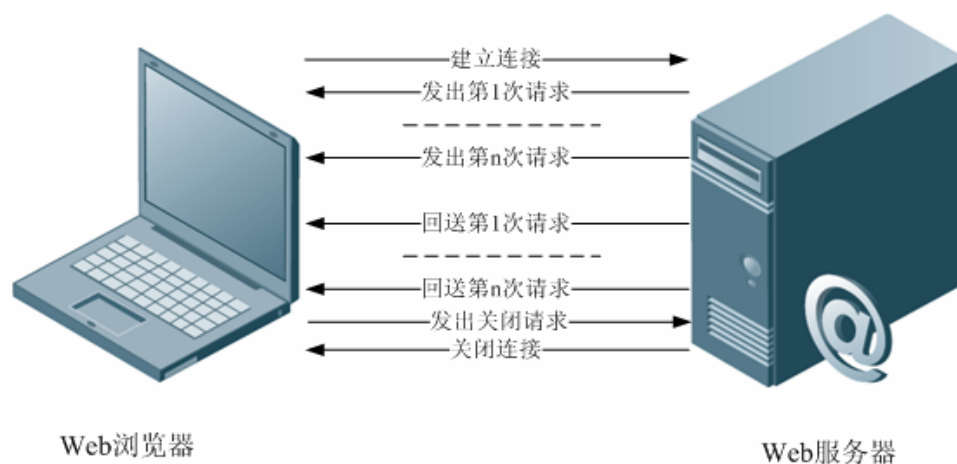
HTTP 服务

HTTP 服务是指在 Internet 上利用 HTTP 协议传递 Web 页面信息。HTTP/1.0 是目前业界使用最广泛的 HTTP 协议版本，由于一个 Web 服务器每天可能有上万甚至上百万的访问量，为了便于连接管理，HTTP/1.0 采用短连接方式。一个请求创建一个 TCP 连接，请求完成后释放连接，服务器不需要记录和跟踪过去的请求。HTTP/1.0 虽然简化了连接管理，但是却引入了性能缺陷。

例如一个网页中可能需要很多图片，网页中包括的不是真正的图片内容，而是它们的 URL 连接地址，这样浏览器在访问过程中会发出多次请求，每次请求都要建立一个单独的连接，每次连接都是完全隔离的。建立和释放连接是一个相对费劲的过程，从而严重影响了客户机和服务器的性能，如图所示。



HTTP/1.1 克服了这个缺陷。该版本支持持久连接，即一个连接可以传输多个请求和响应，这样客户机可以不用等待上一次请求完成就可以发送第二个请求，减少了网络时延，提高性能，如图所示。



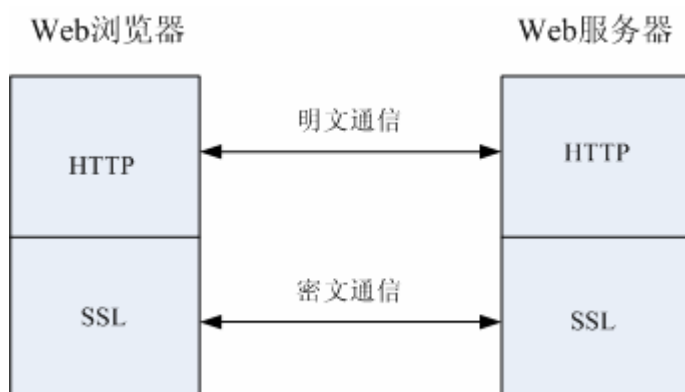
目前，锐捷交换机支持 HTTP/1.0 和 HTTP/1.1 两种协议版本。

交换机使用哪种协议版本由 Web 浏览器决定。

HTTPS 服务

HTTPS 服务就是在 HTTP 基础上加入 SSL 层，其安全基础是 SSL。要使协议能够正常运行，服务器必需有 PKI（公钥基础设施）证书，而客户端则不一定，SSL 协议提供的服务主要有：

- 认证用户和服务器，确保数据发送到正确的客户机和服务器；
- 加密数据以防止数据中途被窃取
- 维护数据的完整性，确保数据在传输过程中不被改变。



HTTP 升级服务

HTTP 升级包括 HTTP 本地升级和 HTTP 远程升级两种方式。

- 本地升级时，设备作为 HTTP 服务器，用户通过 Web 浏览器登录到设备，将需要升级的文件上传到设备，实现设备上文件的升级。
- 远程升级时设备作为客户端连接到远程 HTTP 服务器上，通过获取服务器上的文件来实现本地文件的升级。

3.1.3 工作原理

HTTP 工作过程

HTTP 是为 Web 管理提供服务。用户通过 Web 界面登陆到设备中进行配置与管理。Web 管理包括 Web 客户端和 Web 服务器，同理 HTTP 服务也采用客户端/服务器模式。HTTP 客户端内嵌在 Web 管理客户端的 Web 浏览器中，能够发送 HTTP 报文和接收处理 HTTP 响应报文。而 Web 服务器(即 HTTP 服务器)则内嵌于设备中。客户端和服务器之间的信息交互过程如下：

- 在客户端与服务器之间建立 TCP 连接，HTTP 服务默认端口号是 80，HTTPS 服务默认端口号是 443

- 客户端向服务器发送请求消息
- 服务器处理客户请求后，回复响应消息给客户端
- HTTP 服务处理完一次请求后，直接关闭客户端与服务器之间的 TCP 连接；HTTPS 可以处理多个请求，直到客户端发送关闭请求或者服务器超时关闭连接。

HTTP 远程升级服务的工作过程可以归纳：

- 连接服务器。连接时，优先连接用户配置的服务器地址，如果无法连接，则尝试连接本地升级记录文件中的服务器地址。
- 发送本机各程序的版本号到服务器
- 服务器解析后，给出下载文件列表
- 设备根据列表连接到文件服务器，并下载需要升级的文件。下载不同的文件又可连接不同的服务器
- 设备升级文件。

3.1.4 相关协议规范

RFC1945 - Hypertext Transfer Protocol -- HTTP/1.0

RFC2616 - Hypertext Transfer Protocol -- HTTP/1.1

RFC2818 - Hypertext Transfer Protocol Over TLS -- HTTPS

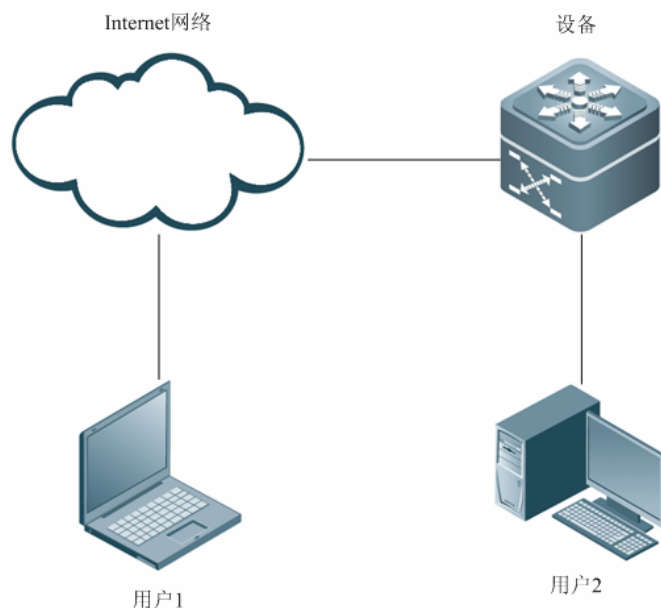
3.1.5 典型应用

HTTP 应用服务

目前 Web 网管仍然是用户进行设备管理维护的主要方式之一，锐捷网络设备也提供了 Web 管理功能。设备开启 HTTP 服务后，用户只需在 PC 机浏览器中输入 `http: //+`设备的 IP 地址，认证通过后就可以登录到 Web 管理界面。在 Web 界面中，用户可以进行设备状态信息监控、配置设备、上传和下载文件等操作。

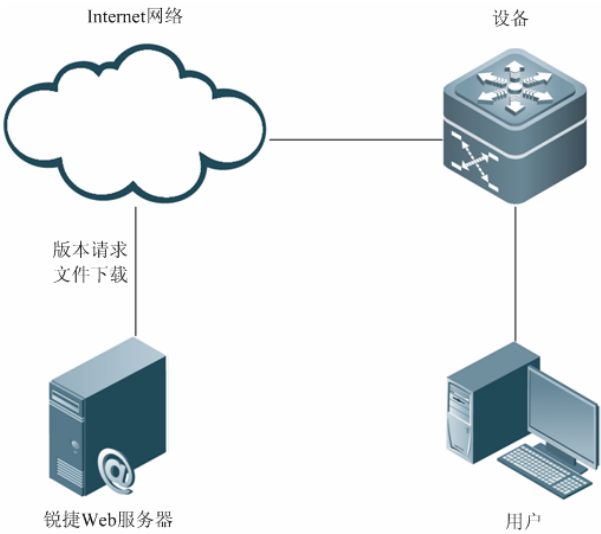
普通的 HTTP 服务是不安全的通信方式，对于比较敏感的通讯，锐捷设备还提供了更安全的 HTTPS 服务，使得用户和设备之间的通信是加密的，第三方无法通过监听获取和篡改通信内容。用户只需要在浏览器中输入 `https: //+`设备的 IP 地址，认证成功后就可以进行 Web 管理。

描绘了用户进行 Web 管理的典型应用场景，用户可以通过 Internet 进行远程访问设备，也可以在本地局域网中通过登录 Web 服务器对设备进行配置管理。用户可以根据实际情况，选择在设备上单独启用 HTTPS 服务或者 HTTP 服务，也可以同时启用 HTTPS 和 HTTP 服务。用户还可以再浏览器上设置使用 HTTP/1.0 还是 HTTP/1.1 协议来访问设备的 HTTP 服务。



HTTP 远程升级服务

HTTP 远程升级是指设备作为客户端连接到远程 HTTP 服务器上，通过获取服务器上的文件来实现本地文件的升级。锐捷提供的 Web 服务器域名默认是 rgos.ruijie.com.cn。典型应用场景如图所示。



3.2 配置HTTP

缺省配置

功能特性	缺省值
使能 HTTP 服务	默认是关闭的
HTTP 认证方式	默认普通 HTTP 服务的认证方式是 enable
HTTP 服务端口	默认普通 HTTP 服务默认端口是 80，HTTPS 服务端口是 443
HTTP 升级服务器	默认服务器地址是 0.0.0.0，端口是 80
HTTP 升级模式	默认是手动升级模式
HTTP 升级自动检测时间	默认是随机的

配置前提

如果用户配置普通 HTTP 服务的认证方式是 **enable**，要求用户配置 **enable secret** 或者 **enable password** 口令，权限级别为 15。

如果用户配置普通 HTTP 服务的认证方式 **local**，要求用户通过 **username** 配置本地数据库的身份信息，权限级别是 15。

在配置 HTTP 升级服务器域名之前，要求用户开启设备的 DNS 功能，并配置 DNS 服务器地址。

配置步骤

步骤	配置任务	说明
1	使能 HTTP 服务	“必选”
2	配置 HTTP 认证信息	“可选”；用户需要改变认证方式时配置
3	配置 HTTP 服务端口	“可选”；用户需要改变 HTTP 服务端口时配置
4	配置 HTTP 升级服务器	“可选”；用户需要指定服务器地址时配置
5	配置 HTTP 升级模式	“可选”；用户需要改变升级模式时配置
6	配置 HTTP 升级自动检测时间	“可选”；用户需要改变自动检测时间时配置
7	HTTP 手动升级文件	“必选”

3.2.1 使能HTTP服务

HTTP 服务包括普通 HTTP 和 HTTPS 两种。HTTPS 是在 HTTP 协议基础上增加 SSL，提高信息安全性。

要打开 HTTP 服务，请在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)# enable service web-server http	“必选”；打开普通 HTTP 服务。
Ruijie(config)# enable service web-server https	“必选”；打开 HTTPS 服务。
Ruijie(config)# enable service web-server [all]	“必选”；同时打开 HTTP 和 HTTPS 服务

配置举例：

例 1：配置在 Ruijie 设备中同时打开 HTTP 和 HTTPS 服务。

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# enable service web-server
```

3.2.2 配置HTTP认证信息

在使用 HTTP 服务的时候，需要进行登录认证才能进入 Web 页面。锐捷提供两种认证设置方式。

使用 **webmaster level** 命令配置

命令	作用
Ruijie# configure terminal	进入全局配置模式
Ruijie(config)# webmaster level privilege-level username name password { password [0 7] encrypted-password }	“必选”；配置登陆认证方式，缺省没有配置。

 用户名和密码有三个权限等级；每个权限等级最多可以配置 20 个用户名和密码。

配置举例：

例 1：配置在 Ruijie 设备中使用用户名 admin，明文密码 ruijie，级别 1 进行 Web 认证。

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# webmaster level 1 username admin password ruijie
```

3.2.3 配置HTTP服务端口

通过配置端口号，可以减少非法用户对 HTTP 服务的攻击。锐捷设备支持 HTTP、HTTPS 两种服务方式。

■ 配置 HTTP 端口号

命令	作用
Ruijie# configure terminal	进入全局配置模式
Ruijie(config)# ip http port port-number	“可选”；配置 HTTP 服务端口号，默认是 80

配置举例：

例 1：配置设备 Ruijie 的 HTTP 服务端口号是 8080

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# ip http port 8080
```

■ 配置 HTTPS 端口号

命令	作用
Ruijie# configure terminal	进入全局配置模式
Ruijie(config)# ip http secure-port port-number	“可选”；配置 HTTPS 服务端口号，默认是 443

配置举例：

例 1：配置设备 Ruijie 的 HTTPS 服务端口号是 4430

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# ip http secure-port 4430
```


3.2.4 配置HTTP升级服务器

缺省情况下，HTTP 远程升级配置的服务器地址是 0.0.0.0，端口号是 80，如果需要服务器地址，按以下步骤进行操作：

命令	作用
Ruijie# configure terminal	进入全局配置模式
Ruijie(config)# http update server { host-name ip-address } [port port-number]	“可选”；配置升级服务器地址



服务器地址可不配置，因为本地升级记录文件中记录了可能的升级服务器地址。



如果配置服务器域名，需要开启设备的 DNS 功能，并配置 DNS 服务器地址。



服务器地址不支持 IPV6。

配置举例：

例 1：配置 Ruijie 设备的 HTTP 升级服务器域名为 rgos.ruijie.com.cn，端口号是 85

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# http update server rgos.ruijie.com.cn port 85
```

3.2.5 配置HTTP升级模式

HTTP 默认是手动升级模式。用户如果需要 HTTP 能自动检测服务器中可升级的文件信息，可以改变升级模式。进入配置模式，按以下步骤进行操作：

命令	作用
Ruijie# configure terminal	进入全局配置模式
Ruijie(config)# http update mode auto-detect	“可选”；配置 HTTP 升级模式为自动检测模式；如果没有配置或者执行 no 形式，则系统默认是手动模式。

自动检测模式下，设备在升级时间内对服务器上的文件进行检测，用户可以通过 Web 界面查看有哪些 Web 版本可以升级。

配置举例：

例 1：配置 Ruijie 设备的 HTTP 升级模式为自动升级模式。

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# http update mode auto-detect
```

3.2.6 配置HTTP升级自动检测时间

在自动检测模式下，HTTP 远程自动检测时间是随机的。如果需要修改自动检测时间，进入配置模式，按以下步骤进行操作：

命令	作用
Ruijie# configure terminal	进入全局配置模式
Ruijie(config)# http update time daily hh:mm	“可选”；配置 HTTP 自动检测时间；默认是随机的



只能配置为每天的某一个时间，精确度为分钟。



只有 HTTP 升级模式为自动检测，该配置命令才会生效。

配置举例：

例 1：配置 Ruijie 设备的 HTTP 自动检测时间为每天的凌晨三点。

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# http update time daily 03:00
```

3.2.7 HTTP手动升级文件

■ 远程升级

缺省情况下，HTTP 只提供远程自动检测，系统不会自动升级。如果需要升级，进入特权模式，按以下步骤进行操作：

命令	作用
Ruijie# http check-version	“可选”；检测升级版本
Ruijie# http update web [version string]	需要升级 Web 包的版本信息。

配置举例：

例 1：手动对 Ruijie 设备进行 HTTP 远程升级文件。

```
Ruijie# http check-version
app name:web
sn          version          filename
-----
0           1.2.1(82381)          web1.2.1(145680).upd
1           1.2.1(82380)          web1.2.1(145680).upd
2           1.2.1(82379)          web1.2.1(145680).upd
3           1.2.1(82378)          web1.2.1(145680).upd
```

■ 本地升级

用户可以通过 **copy tftp** 将最新的 Web 文件下载到设备中，在按以下步骤进行操作：

命令	作用
Ruijie# http web-file update	更新 Web 包。

 要使新的 Web 包生效，用户还需要重新认证登陆 Web 界面。

例 1：本地对 Ruijie 设备进行 Web 包升级

```
Ruijie#copy tftp://10.10.10.13/web_management_pack.upd flash:web_management_pack.upd
Ruijie#http web-file update
```

3.3 监视与维护

3.3.1 显示HTTP配置信息

命令	作用
show web-server status	要查 Web 服务配置信息和状态。

配置举例：

例 1：显示 Ruijie 设备的 HTTP 配置信息

```
Ruijie# show web-server status
http server status : enabled
http server port : 80
https server status: enabled
https server port: 443
http(s) use memory block: 768, create task num: 0
```

3.4 配置举例

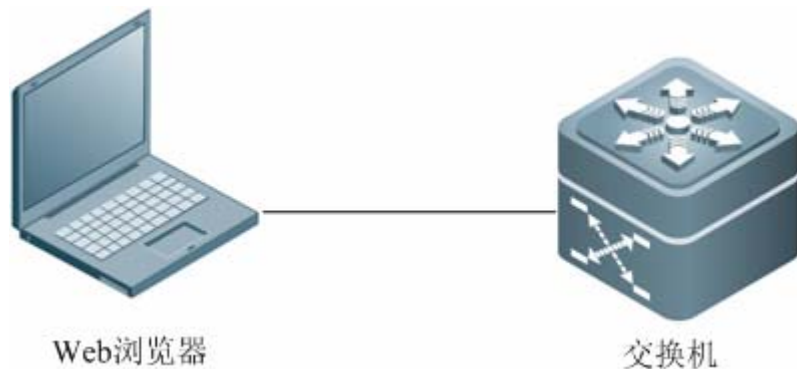
3.4.1 HTTP服务配置举例

组网需求

网络管理员希望使用 Web 管理一台交换机设备；通过 Web 浏览器登录到交换机中进行相关功能的配置。

- 使用本地数据库的身份进行认证
- 为了提高安全性，要求 Web 浏览器即可以通过 HTTP 协议访问，也可以通过 HTTPS 协议访问
- 要求自己配置 HTTP 服务端口，减少非法用户对 HTTP 的攻击。

组网拓扑



配置要点

要满足客户要求，配置要点如下：

- 要使用本地数据库的身份进行认证，需要通过 `username` 配置数据库信息
- 需要同时打开 HTTP 和 HTTPS 服务，以满足客户的安全性要求
- 可以配置 HTTP 服务端口号为 8080；HTTPS 服务端口号为 4430

配置步骤

- 1) 配置本地数据库的身份认证信息，用户名为 `admin`，明文密码为 `ruijie`，15 级权限

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#username admin password ruijie
Ruijie(config)#username admin privilege 15
```

- 2) 打开 HTTP 和 HTTPS 服务

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#enable service web-server
```

- 3) 配置 HTTP 服务认证方式为 `local`

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#ip http authentication local
```

- 4) 配置 HTTP 服务端口为 8080

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#ip http port 8080
```

- 5) 配置 HTTPS 服务端口为 4430

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#ip http secure-port 4430
```

显示验证

- 6) 查看 HTTP 配置信息

```
Ruijie#show web-server status
http server status : enabled
http server port : 8080
https server status: enabled
https server port: 4430
http(s) use memory block: 768, create task num: 0
```

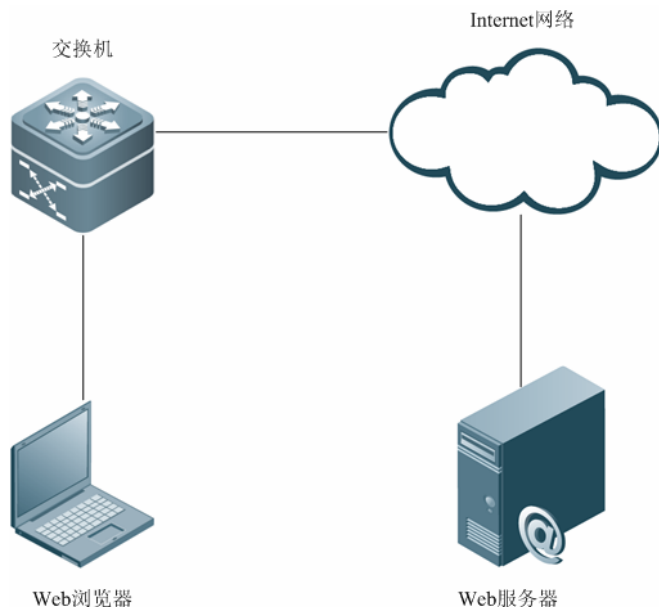
3.4.2 HTTP远程升级配置举例

组网需求

一个企业购买了锐捷产品，希望能使用 HTTP 升级功能进行文件升级。

- 设备每天能定时远程获取锐捷服务器中可升级的文件信息
- 可以查看当前可升级的文件信息
- 从锐捷提供的服务器中下载最新文件，并更新升级设备

组网拓扑



配置要点

要实现客户需求，要点如下：

- 配置设备每天定时在凌晨 2 点远程获取最新文件信息

配置步骤

1) 配置 DNS 信息

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#ip domain-lookup //打开设备的 DNS 域名解析功能
Ruijie(config)#ip name-server 192.168.5.134 //配置的 DNS 服务器地址
```

2) 配置升级服务器地址

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# http update server rgos.ruijie.com.cn
```

3) 开启自动检测模式，配置设备的定时远程监测时间为凌晨 2 点

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#http update mode auto-detect
Ruijie(config)#http update time daily 02:00
```

4) 获取远程服务器中可更新升级的文件信息

```
Ruijie#http check-version
app name:web
sn          version          filename
-----
0           1.2.1(82381)       web1.2.1(145680).upd
1           1.2.1(82380)       web1.2.1(145680).upd
2           1.2.1(82379)       web1.2.1(145680).upd
3           1.2.1(82378)       web1.2.1(145680).upd
```

5) 从服务器中下载文件并更新

```
Ruijie#http update web
```

显示验证

在 Web 在线升级界面可查看服务器版本信息。

3.4.3 HTTP本地升级配置举例

组网需求

- 用户通过官网获取到最新的 Web 包，希望设备运行最新的 Web 包。

组网拓扑



配置要点

要实现客户需求，要点如下：

- 与本地 PC 机相连，PC 机的 IP 地址是 10.10.10.13；给设备配置一个同网段的 IP 地址 10.10.10.131
- 将最新的 Web 包下载到设备中
- 更新设备运行的 Web 包

配置步骤

创建 VLAN1，并给设备配置一个 IP 地址

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#vlan 1
Ruijie(config-vlan)#exit
Ruijie(config)#interface vlan 1
Ruijie(config-VLAN 1)#ip address 10.10.10.131 255.255.255.0
```

在 PC 中打开 tftp 服务器，并在设备中执行 copy tftp 下载 Web 包

```
Ruijie#copy tftp://10.10.10.13/web_management_pack.upd flash:web_management_pack.upd
```

更新设备的 Web 包

```
Ruijie#http web-file update
```

显示验证

在 PC 机中，重新进行 Web 认证登陆，验证是否显示最新的 Web 页面

4 配置 LINE 模式

4.1 概述

本章描述对 LINE 的一些操作：

- 进入 LINE 模式
- 增加/减少 LINE VTY 数目
- 配置 LINE 下可以通讯的协议
- 配置 LINE 下的访问控制列表

4.2 LINE模式配置

4.2.1 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

4.2.2 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

4.2.3 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 line number	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

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

5 配置系统升级

5.1 理解系统中的程序映像

系统映像包含了 RGOS 的软件。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。

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。在路由器设备中，只有 Bootloader 和主程序两个程序映像。Bootloader 具有 BOOT 和 CTRL 的所有功能。

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。通常情况下，要得到产品的新特性，需要更新设备的主程序。为了保持设备的 BOOT、CTRL 和主程序的兼容性以及管理板主程序的兼容性，升级功能提供了自动的兼容保障。即针对不兼容的部分将进行自动化的更新，而无需单独下载映像进行更新。在升级过程中，会自动将设备上和新版本软件不兼容的映像升级。因此升级过程将明确的看到这些映像的更新信息。

5.1.1 升级功能概述

5.1.2 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。

5.1.3 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。

对于堆叠设备升级来说，当发现成员设备之间存在主程序版本不一致时，也会产生自动安装过程。主设备上的 RGOS 程序映像会被同步到版本不一致的从设备上，并且在这些从设备上安装。安装后，整堆设备将被复位。当所有的设备进入就绪状态后，它们都将运行相同的主程序版本。

用户在系统升级时，自动安装的流程是：

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。

说明

10.4(2)这个版本在升级功能上进行了许多的优化和改进。主要包括：更安全可靠的升级过程、更少的设备复位次数和业务间断、更易理解的升级界面。因此以 10.4(2) 版本作为分水岭，在升级界面也存在大量的差异。但是升级本身的操作步骤是兼容的。

5.2 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

说明

- (1) 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。

5.2.1 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：

- 确认文件下载方法
- 确认文件系统空间
- 备份配置文件

 注意

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。

5.2.1.1 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。首先确认服务器上已经运行了 TFTP server 软件（工作在 **server** 模式）。然后指定下载文件的目录，这个目录中需要保存着要下载的 RGOS 程序映像。最后确认 TFTP server 的地址，确保设备端能够访问该 TFTP server。

 说明

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** 命令单独覆盖从板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。

 注意

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。

 注意

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。

 注意

该方法拷贝升级文件时不会进行合法性检查。

5.2.1.2 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。

 **注意**

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。

 **注意**

即使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。

5.2.1.3 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。

5.2.2 升级典型过程举例

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

5.2.2.1.1 升级到 10.4(2)或更高版本

将新版本软件拷贝到设备上：

```
Ruijie#copy tftp://192.168.201.98/S8600_V10.4(2)_R64047.bin flash:rgos.bin
Accessing tftp://192.168.201.98/ S8600_V10.4(2)_R64047.bin...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Other members are not present, quit synchronize...
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 10.4 (2) 以及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。只在极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...eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee [ok]
Writing flash ##### [OK - 1,215,488 bytes]
*Apr 10 07:32:44: %UPGRADE-5-LOCAL_FIN: New software image installed in flash.

```



注意

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。

5.2.2.1.2 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/s26_64047_install_10_4_1.bin
flash:rgos.bin
Accessing tftp://192.168.201.98/s26_64047_install_10_4_1.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。

5.2.2.2 堆叠设备的升级

堆叠设备会在两种情况下产生升级动作:

- 对整堆设备进行升级

这种情况适用于设备已经完成了堆叠，此时需要对整堆设备进行升级。升级的步骤与盒式设备相同。

- 堆叠过程中产生的升级

参与堆叠的设备要求具有相同的软件版本。如果不一致，那么将在堆叠的过程中，系统将自主决策（以主设备为准或者以最高版本为准）自动对版本不一致的从设备进行升级。

堆叠设备自动安装的过程中，界面提示除了主设备的安装内容外，还有从设备的安装提示，如：

```
*Jan 2 00:01:39:%STACK-5-INST: (Device 2): Install CTRL.
```

```
*Jan 2 00:03:39:%STACK-5-INST: (Device 2): Install SYSINFO.
```

```
*Jan 2 00:06:40:%STACK-5-FINISH: All software images installed.
```

当系统提示“All software images installed.”的日志时，表示整堆设备的安装已经结束。系统业务可以开展。

5.2.3 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** 版本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。

说明

通过 **show version** 命令显示早于 10.4（2）之前的映像版本号时，无法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。

5.3 升级常见问题

5.3.1 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.
```

5.3.2 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。

5.3.3 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。

5.3.4 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。

5.3.5 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：

1. 确认待升级板卡是否被拔插或者复位；
2. 确认待升级板卡是否系统繁忙（CPU 利用率高）；
3. 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。

6 配置文件系统

6.1 理解文件系统

6.1.1 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，RGOS 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。

6.1.2 基本特性

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

6.1.2.1 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

6.1.2.1.1 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：

 注意

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。

6.1.2.1.2 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。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。

 说明

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:

 注意

当使用 **prefix** 指定本地文件时，“:”后的路径必须是绝对路径

6.1.2.1.3 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。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：

Ruijie#copy ?

 说明

WORD	Copy from current file system
flash:	Copy from flash: file system
running-config	Copy from current system configuration
slave:	Copy from slave: file system
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

 说明

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。

6.1.2.2 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:
	-	-	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。

 注意

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。

6.1.2.3 管理本地设备上的文件

本地文件是指保持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 **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。

注意

在 **flash** 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。

注意

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。

注意

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!
```



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。

6.1.2.4 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:
```

6.2 典型配置举例

6.2.1 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\ 目录上下载一个文件到设备上：

(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:
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.
```

6.2.2 上传文件到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
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

6.2.3 使用xmodem下载文件

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

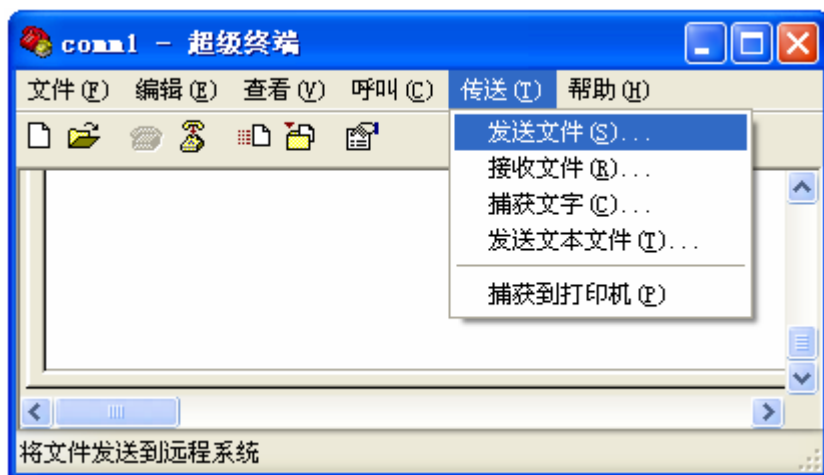
(1) 首先用串口线将 PC 的串口和设备的串口连接起来。

(2) 打开 Windows 的超级终端, 连接到设备控制台

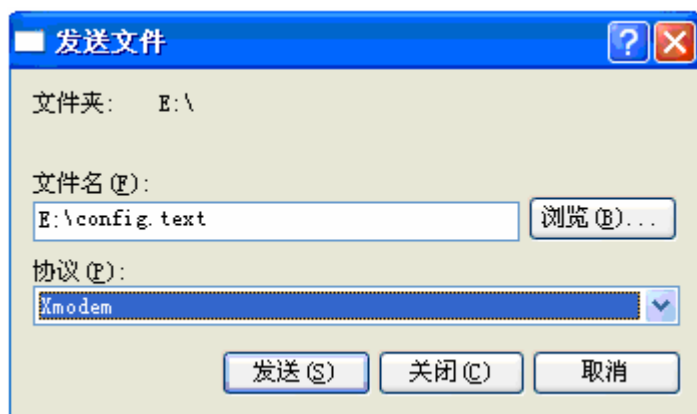
(3) 在特权模式下使用以下命令下载文件

```
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:



(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。



(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.
```

6.2.4 使用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：

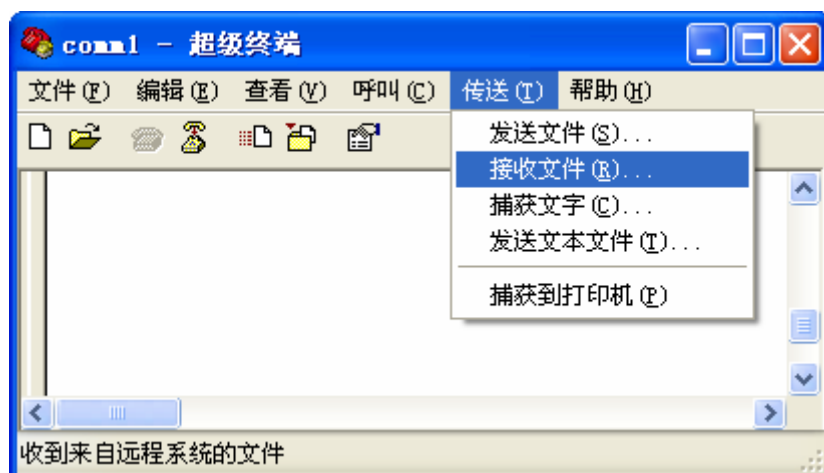
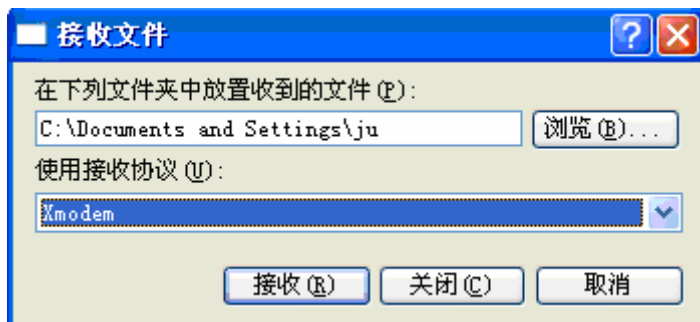


图 3

(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：



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

6.2.5 目录的删除

以下例子说明如何删除一个非空的 aaa 目录：

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

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
```

aaa 目录不是空目录，必须将文件先删除才能删除目录

```
Ruijie# delete aaa/backup.txt
```

删除空目录

```
Ruijie# rmdir aaa
```

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, 9563693 bytes (9MB) available
```

7 配置系统管理

7.1 基本系统管理

7.1.1 配置任务列表

7.1.1.1 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
Step 1	Ruijie# show cpu	查看系统 CPU 利用率信息

缺省情况下，交换机的名称为 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_rcv_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_rcv
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%	dhcpcd_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_rcv_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。

7.1.1.2 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。

Step 1	命令	作用
	<code>cpu-log log-limit low_num high_num</code>	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:CPU utilization in one minute:
95% , Using most cpu's task is ktimer : 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:CPU utilization in one
minute:68% , Using most cpu's task is ktimer : 60%
Oct 20 15:47:01 %SYSCHECK-5-CPU_USING_RATE:The CPU using rate has down!
```

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

- 显示系统总的内存使用情况

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
Ruijie# show memory	查看系统内存使用情况

缺省情况下，交换机的名称为 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
Systrem 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 配置系统日志

9.1 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。

9.1.1 日志报文格式

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
Step 1	Ruijie(config)# logging on	打开日志开关
Step 2	Ruijie(config)# no logging on	关闭日志开关

注意

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
Step 1	Ruijie(config)# logging buffered [buffer-size level]	将日志记录到内存缓冲区
Step 2	Ruijie# terminal monitor	允许日志信息显示在 VTY 窗口上
Step 3	Ruijie(config)# logging server host	将日志信息发送给网络上的 Syslog Sever
Step 4	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。

注意

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
Step 1	Ruijie(config)# service timestamps message-type [uptime datetime]	启用日志信息中的时间戳
Step 2	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做为日志信息时间戳，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做为日志信息时间戳。

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
Step 1	Ruijie(config)# no service sysname	在日志报文中取消系统名。
Step 2	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
Step 1	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。
Step 2	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
Step 1	Ruijie(config)# no service sequence-numbers	在日志报文中取消序列号。
Step 2	Ruijie(config)# service sequence-numbers	在日志报文中添加序列号。

 **注意**

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
Step 1	Ruijie(config-line)# logging synchronous	设置用户输入与日志信息输出同步；

Step 2	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
Step 1	Ruijie(config)# logging rate-limit number	设置对日志信息进行速率控制
Step 2	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
Step 1	Ruijie(config)# logging console level	设置允许在控制台上显示的日志信息级别
Step 2	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
Step 3	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
Step 4	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
Step 5	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
Step 1	Ruijie(config)# logging facility facility-type	设置日志信息的设备值
Step 2	Ruijie(config)# no logging facility facility-type	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 IP 地址为发送报文接口的 IP 地址，可以通过命令来固定所有日志报文的源 IP 地址。

可以直接设定日志报文的源 IP 地址，倘若设备上未配置该 IP 地址，则日志报文源 IP 地址仍为发送报文接口的 IP 地址；也可以设定日志报文的源接口，倘若设备上未配置该源接口或源接口上未配置 IP 地址，则日志报文源 IP 地址也仍为发送报文接口的 IP 地址。

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
Step 1	Ruijie(config)# logging source interface <i>interface-type interface-number</i>	设置日志信息的源端口
Step 2	Ruijie(config)# logging source {ip <i>ip-address</i> }	设置日志报文的源 ip 地址



注意

如果配置了日志报文的源接口，不管该接口是否处于 shutdown 状态，都使用源接口上配置的 IP 地址作为日志报文的源 IP 地址。

9.2.12 设置发送用户LOG信息

	命令	作用
Step 1	Ruijie(config)# logging userinfo	设置用户登录/退出的 LOG 信息；
Step 2	Ruijie(config)# logging userinfo 日志监控 command-log	设置执行配置命令时，发送 LOG 信息

9.3 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
Step 1	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
Step 2	Ruijie# show logging count	查看系统中各模块日志信息统计情况
Step 3	Ruijie# clear logging	清除内存缓冲区中的日志报文
Step 4	Ruijie# more flash:filename	查看扩展 FLASH 中的日志文件



注意

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。

9.3.1 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 配置 USB 使用

10.1 概述

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**卡的上文件可以使用 **URL** 进行定位和访问。如 `usb0:/abc/1.txt`



注意

10.4（2）及以上的版本才支持使用 **URL** 访问 **U 盘**卡。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。

10.2 插入并识别存储设备

直接将 **USB** 存储器插入 **USB** 插槽。系统找到设备并加载驱动时，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。

提示信息	说明
USB Mass Storage Device	找到的设备的名称
usb0	第 1 个 USB 设备
size : 1050673152B(1002MB)	分区的大小 (RGOS 只自动加载第一个分区)

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 **u 盘**分区的根目录下。

Ruijie# **copy a.txt usb0:/b.txt**

这时执行 `dir` 命令就可以看到 **USB** 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。

 注意

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。

 注意

10.4（2）及以上的版本才支持使用 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:/mnt/usb0/a.txt flash:/a.txt

10.2.2 显示 USB信息

	命令	作用
Step 1	Ruijie# 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
Step 1	Ruijie# usb remove <i>Device_ID</i>	卸载设备号为 <i>Device_ID</i> 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!

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

10.3 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 配置系统升级维护

11.1 概述

系统升级维护指的是在命令行界面下进行主程序或者 CTRL 程序的升级或者文件的上传和下载，通常有两种手段：一种是使用 TFTP 协议通过网口进行升级，另一种是使用 Xmodem 协议通过串口进行升级。

11.2 升级维护方法

11.2.1 通过TFTP协议传输文件

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	下载主机端的 URL 指定的文件 <i>filename</i> 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 <i>filename</i> 到主机端的 URL 指定的目录下，可重设文件名。



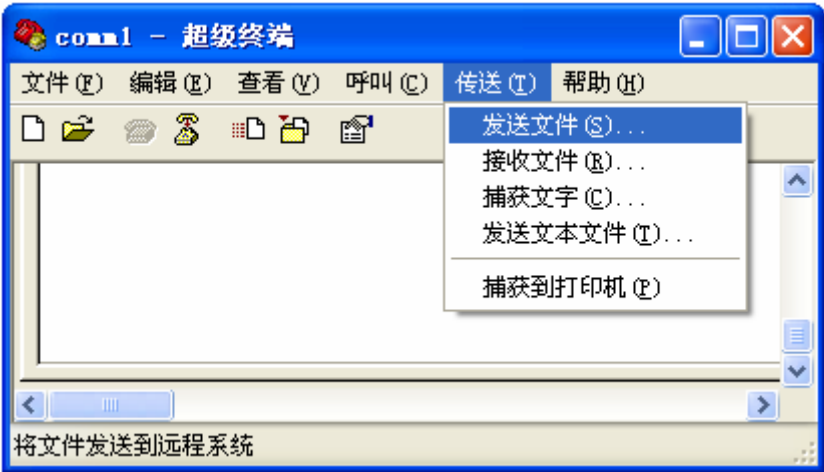
如果源文件的文件名中有空格，则需要给 tftp 链接加上引号，如下：
copy tftp:"//localtion/filename" flash:filename
 同样的，如果目标的文件名中有空格，也需要将文件名加上引号，如下：
copy tftp://localtion/filename flash:"filename"

11.2.2 通过XMODEM协议传输文件

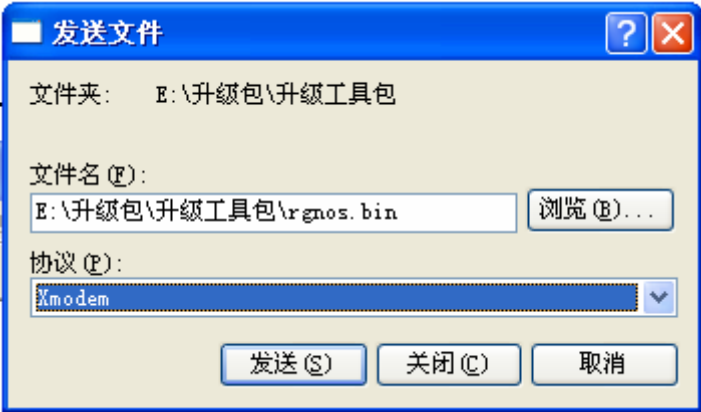
一种是从主机端下载文件到设备，另一种是从设备上传文件到主机端。

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：



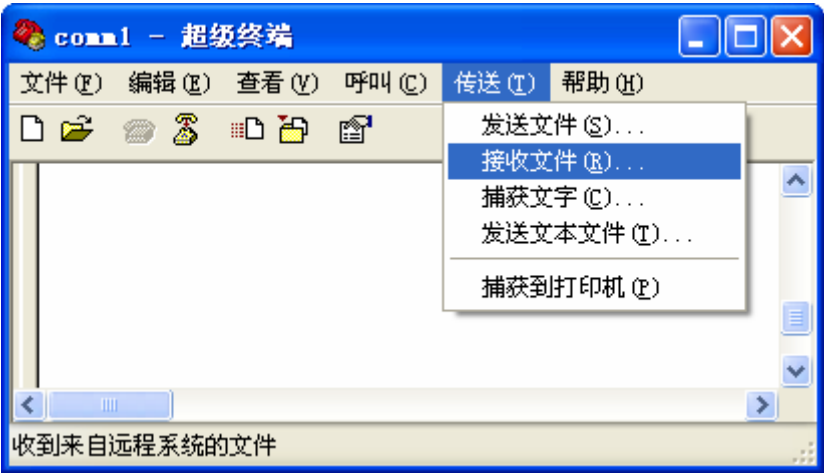
在弹出的对话框的文件名选择本地主机要下载的文件，协议选择“Xmodem”，点击“发送”，则 Windows 超级终端显示发送的进度以及数据包。如图所示：



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 <i>filename</i> 。

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：



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：



命令	作用
Ruijie# copy flash:filename xmodem	从设备端上传文件 <i>filename</i> 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

11.2.3 升级系统

使用上述的 **ttftp** 或者 **xmodem** 将升级文件传输到设备上。传输成功后，重新启动设备，升级文件就会自动完成当前系统的检测和升级，这个过程不需要人工干预和介入。

盒式设备的升级只完成自己单板系统的升级操作，升级完毕，系统自动复位，机器再次启动正常运行。

- 1. 确认要载入的升级文件的文件名为 **rgos.bin**；
- 2. 使用上述 **copy** 命令，将此文件下载到设备上；
- 3. 如果设备上存在从管理板，需要等待主从管理板的主程序升级成功，成功时将有如下提示：
Upgrade Slave CM MAIN successful!!
Upgrade CM MAIN successful!!
- 4. 执行整机复位操作；
- 5. 系统再次启动后，升级文件会开始运行，将会看到类似如下提示：

```
Installing is in process .....  
Do not restart your machine before finish !!!!!!  
.....
```

- 6. 在升级操作完成后，将会看到类似如下提示：
Installing process finished
Restart machine operation is permitted now !!!!!!
- 7. 升级文件运行完毕后系统会自动复位，出现如下提示：
System restarting, for reason 'Upgrade product !'.
然后系统自行复位后就会正常运行了。

12 配置堆叠管理

12.1 理解堆叠

12.1.1 概述

堆叠技术是一种集中管理和端口扩展技术。用户可以使用堆叠端口和堆叠连接线将多台独立的交换机连接在一起构成统一堆叠系统，具有以下优点：

灵活扩展端口密度。堆叠系统的端口数是由堆叠中所有成员设备的端口相加得到的，用户可以根据网络规模灵活的增加或减少端口数量，而不需要废弃先前采购的设备，从而保护了用户投资。

方便用户管理操作。堆叠系统在逻辑上是一台设备，在网络中是一个节点，其通过一个 IP 地址来管理，减少 IP 地址的占用并方便网络管理。

12.1.2 硬件结构

组成堆叠系统一般来说需要特殊的堆叠端口和堆叠线缆，锐捷交换机提供多种硬件方案供用户选择：

堆叠模块：专用的堆叠模块可提供高带宽，低成本的堆叠方案；使用这种方案需要专用的堆叠线缆，堆叠成员设备互连的距离受到堆叠线缆长度的约束。

普通模块：普通模块可提供高带宽，长距离的堆叠方案；使用这种方案不需要专用的堆叠线缆，成本高是这种方案的缺点。

固定端口：固定端口可提供成本低，长距离的堆叠方案；使用这种方案不需要专用的堆叠线缆，带宽低是这种方案的缺点。

☺各产品支持情况

交换机堆叠系统支持 8 台成员设备，使用堆叠模块或堆叠线缆建立堆叠系统，堆叠的安装参见具体产品的硬件说明书。
本产品不支持混堆。

12.1.3 堆叠的启动和停止

在启动阶段如果交换机的插槽内未插堆叠模块，则工作在单机模式下；如果交换机的插槽内插有堆叠模块，它将会检测堆叠链路是否连通，若堆叠链路能够正常连通，则工作在堆叠模式下，若交换机在经过一段时间的检测发现堆叠链路仍无法正常连通，则工作在单机模式下。

在堆叠环境中，若堆叠电缆连接中断，对堆叠的管理操作将会失败，系统将会发送相应的日志信息提示用户：

```
STACKMODULE-LINKSTATUS-CHANGED:Link loss is detected in the stack loop.  
Device [2] loss has been detected, system will reset.
```

如果在 3 秒钟内堆叠电缆恢复连接，则堆叠环境可以恢复正常工作,系统将会发送相应的日志信息提示用户：

```
STACKMODULE-LINKSTATUS-CHANGED:Link recover is detected in the stack loop.
```

如果连接中断超过 3 秒，堆叠无法正常工作，堆叠系统会重新启动，重新建立堆叠。

在网络流量过大的情况下，对堆叠的管理操作将会失败，此时不必重新启动交换机，待网络流量减小后，堆叠环境中的交换机又都可恢复正常工作。

堆叠不支持热插拔，也就是不能在堆叠运行过程中插入、移出、更换成员设备。如果这么做，则堆叠系统会重新启动，重新建立堆叠。在稳定工作的堆叠环境中，如果任何一台交换机下电并重新上电，堆叠中的所有其他交换机将自动复位并重新竞选，构建新的堆叠。

注意

在堆叠运行过程中插入、移出、更换成员设备，则导致堆叠复位，重新竞选，构建新的堆叠。

12.2 配置堆叠

12.2.1 缺省配置

设备的堆叠属性缺省配置如下表所示：

功能特性	缺省值
堆叠口	堆叠模块
设备优先级	1
设备描述	SWITCH

12.2.2 如何根据设备号确认堆叠成员设备

堆叠系统中的主机是根据成员设备的优先级属性选举出来的，优先级值最大的为主机，当成员设备的优先级值一样的时候，则根据 MAC 地址进行选举，MAC 地址最小的为主机。配置完设备优先级后需要重启才能生效。

当堆叠建立之后，只有通过主机串口才能执行带外管理，所以建议您在建立堆叠之前先选择一台主机，在单机模式下将其优先级修改为较高优先级，保证其在堆叠中为主机。设备优先级从低到高为 1-10，出厂缺省设置为 1，详细设置方法参见配置设备优先级。堆叠启动用 **show member** 命令显示堆叠成员信息中，您可以根据堆叠成员 MAC 地址信息来确定堆叠中的设备以及排列顺序。

建议您将需要堆叠的设备从设备 1 到设备 N 依序摆好后根据上述规则连接堆叠线以方便管理。

注意

堆叠中只有主机串口能执行带外管理，所以在建立堆叠之前最好先选择一台主机，将其优先级在单机模式下设置为较高，然后建立堆叠，确保该设备在堆叠中为主机。

12.2.3 配置设备优先级

在全局模式下,请使用如下命令配置：

命令	作用
Step 1 Ruijie(config)# device-priority [<i>member</i>] <i>priority</i>	<i>member</i> 取值 1-MAX，配置的成员设备； <i>priority</i> 取值 1-10，指定设备的优先级； 默认情况下配置的成员设备为 1。

配置实例：指定成员设备 2 的优先级为 8

```
Ruijie(config)# device-priority 2 8
```



注意

配置完成后，需要执行 **write** 命令保存，在堆叠复位后重新建立堆叠系统时新的优先级才能生效。

12.2.4 配置设备别名

为了方便记忆，您可以给堆叠成员设备配置别名。在全局配置模式下，请使用如下命令配置：

	命令	作用
Step 1	Ruijie(config)# device-description [member member] description	<i>member</i> 取值 1-MAX，配置的成员设备； <i>description</i> 字符长度为 31，指设备的别名； 默认情况下配置的成员设备为 1。

配置实例：指定成员设备 2 的别名为 red-giant

```
Ruijie(config)# device-description member 2 red-giant
```

12.2.5 配置堆叠端口

在接口配置模式下，请使用如下命令配置：

	命令	作用
Step 1	Ruijie(config-if)# stack on	使能设备的堆叠口，可以使用 no 参数取消。

配置实例：使能交换机的 GigabitEthernet 0/28 口的堆叠功能

```
Ruijie(config)# int GigabitEthernet 0/28  
Ruijie(config-if)# stack on
```



注意

对于本产品，需要将指定端口配置为堆叠口后，才可以使用特定的堆叠模块通过该端口进行堆叠。对于本产品，其 GigabitEthernet 0/27，GigabitEthernet 0/28 可以被配置为堆叠口，后续版本将支持 GigabitEthernet 0/25 - 0/28 都可配置为堆叠口。

12.2.6 参数保存

通过以下配置命令配置的堆叠信息将保存在所配置的成员设备中：

device-priority [member] priority

device-description [member member] description

stack on

这些配置信息随成员设备移动而移动，其余的系统配置信息只保存在主机中，随主机移动而移动。

12.2.7 配置EntPhysicalEntry表中的MIB节点entPhysicalIndex的访问权限

在全局配置模式下，用户可以修改 EntPhysicalEntry 表中的 MIB 节点 entPhysicalIndex 的最大访问权限：

命令	作用

Step 1

```
Ruijie(config)# ent-physical-entry mib
ent-physical-index max-access mode
read-only
```

修改 EntPhysicalEntry 表中的 MIB 节点 entPhysicalIndex 的最大访问权限为“只读”模式。配置该命令后，MIB 节点 entPhysicalIndex 支持通过 SNMP 软件进行读取操作。

如果用户需要将 MIB 节点 entPhysicalIndex 的最大访问权限恢复到缺省的“禁止访问”模式，只需输入 **no ent-physical-entry mib ent-physical-index max-access mode** 命令即可。

12.3 显示堆叠信息

在特权模式下，您可以使用如下命名显示堆叠信息

	命令	作用
Step 1	Ruijie# show version devices	显示系统设备信息
Step 2	Ruijie# show version	显示堆叠系统的版本信息
Step 3	Ruijie# show member [<i>member</i>]	显示成员设备堆叠信息 <i>member</i> 取值 1-MAX，指定的成员设备



说明

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。

实例：显示堆叠系统的各种信息

```
Ruijie# show version devices
```

```
Device Slots Description
-----
1        3      RG-S5750-24GT/12SFP
2        3      RG-S5750-48GT/4SFP
3        3      RG-S5750-24GT/12SFP
4        3      RG-S5750-24GT/12SFP
5        3      RG-S5750-24GT/12SFP
6        3      RG-S5750-24GT/12SFP
7        3      RG-S5750-24GT/12SFP
8        3      RG-S5750-48GT/4SFP
```

```
Ruijie# show version
```

```
System description : Red-Giant 10G Routing
Switch(RG-S5750-24GT/12SFP) By Ruijie Network
System start time   : 2007-4-23 17:39:11
System hardware version : 1.0
System software version : RGOS 10.1.00(2), Release(12889)
System BOOT version   : 10.1.11330
System CTRL version   : 10.1.11330
System Serial Number  : 1234942570002
Device information:
Device-1
Hardware version : 1.0
Software version : RGOS 10.1.00(2), Release(12889)
BOOT version     : 10.1.11330
CTRL version     : 10.1.11330
Serial Number    : 1234942570002
Device-2
Hardware version : 1.0
Software version : RGOS 10.1.00(2), Release(12889)
```



```

BOOT version      : 10.1.11330
CTRL version      : 10.1.11330
Serial Number     : 1234942570001
Device-3
Hardware version  : 1.0
Software version  : RGOS 10.1.00(2), Release(12889)
BOOT version      : 10.1.11330
CTRL version      : 10.1.11330
Serial Number     : 1234942570003
Device-4
Hardware version  : 1.0
Software version  : RGOS 10.1.00(2), Release(12889)
BOOT version      : 10.1.11330
CTRL version      : 10.1.11330
Serial Number     : 1234942570004
Device-5
Hardware version  : 1.0
Software version  : RGOS 10.1.00(2), Release(12889)
BOOT version      : 10.1.11330
CTRL version      : 10.1.11330
Serial Number     : 1234942570005
Device-6
Hardware version  : 1.0
Software version  : RGOS 10.1.00(2), Release(12889)
BOOT version      : 10.1.11330
CTRL version      : 10.1.11330
Serial Number     : 1234942570006
Device-7
Hardware version  : 1.0
Software version  : RGOS 10.1.00(2), Release(12889)
BOOT version      : 10.1.11330
CTRL version      : 10.1.11330
Serial Number     : 1234942570007
Device-8
Hardware version  : 1.0
Software version  : RGOS 10.1.00(2), Release(12889)
BOOT version      : 10.1.11330
CTRL version      : 10.1.11330
Serial Number     : 1234942570008

```

Ruijie#**show member**

Member	Mac Address	Priority	Software Version
Hardware	Version	Description	
1	00d0.f810.3323	1	RGOS 10.1.00(2), Release(12889) 1.0
2	00d0.f822.33aa	1	RGOS 10.1.00(2), Release(12889) 1.0
3	00d0.f822.33ae	1	RGOS 10.1.00(2), Release(12889) 1.0
4	00d0.f822.33b0	1	RGOS 10.1.00(2), Release(12889) 1.0
5	00d0.f822.33b2	1	RGOS 10.1.00(2), Release(12889) 1.0
6	00d0.f824.23b4	1	RGOS 10.1.00(2), Release(12889) 1.0
7	00d0.f833.44b4	1	RGOS 10.1.00(2), Release(12889) 1.0
8	00d0.f855.33ae	1	RGOS 10.1.00(2), Release(12889) 1.0

13 配置门限

13.1 理解门限

13.1.1 门限概述

门限（Threshold）是用来了解系统状态的特殊值。门限分三类，分别为 CPU 利用率门限、内存利用率门限、温度门限。每类都有两级的门限，第一级门限为告警门限，第二级门限为严重告警门限。门限除了可以使用 CLI 进行设置和读取以外，还可以使用 MIB 进行设置和读取。

13.1.2 门限基本概念

13.1.2.1 CPU利用率门限

CPU 利用率门限用来指示当前 CPU 的使用状况。可供 MIB 软件读取，没有相关的 log。

13.1.2.2 内存利用率门限

内存利用率门限用来指示当前内存的使用状况。可供 MIB 软件读取，没有相关的 log。

13.1.2.3 温度门限

温度门限用来指示当前设备的温度状况。

当设备温度低于告警门限时，系统温度处于正常状态（normal condition）。当设备温度高于告警门限但低于严重告警门限时，系统温度处于警告状态（warning condition）。当温度高于严重告警门限时，系统温度处于警报状态（alert condition）。

当设备温度状态有变动时，会打印相关的 log，每次变动只打印一次 log，不会重复一直打。

当设备温度从正常状态或警报状态进入警告状态时，会打印如下 log

%SYS-1-TEMP_STATE: System detected temperature is in warning condition.

当系统温度从正常状态或警告状态进入警报状态时，会打印如下 log

%SYS-1-TEMP_STATE: System detected temperature is in alert condition.

当系统温度从警告状态或警报状态恢复到正常状态后，会打印如下 log

%SYS-1-TEMP_STATE: System detected temperature is in normal condition.

13.2 缺省配置

下表用来描述门限的缺省配置。

功能特性	缺省值
CPU 利用率门限	告警门限为 90，严重告警门限为 100
内存利用率门限	告警门限为 90，严重告警门限为 100
温度门限	告警门限为 90，严重告警门限为 100

部分产品有的门限缺省值，下表给出了已定缺省值的产品及其缺省值。

产品系列	缺省值
S78 系列	温度告警门限为 60，严重告警门限为 70

13.3 配置门限

13.3.1 配置CPU利用率门限

	命令	作用
Step 1	Ruijie# configure terminal	进入全局配置模式。
Step 2	Ruijie(config)# threshold set cpu <i>warning_value critical_value</i>	配置指定设备的 CPU 利用率告警门限和严重告警门限，范围为 1~100。

如果要恢复到缺省值，可用 **no threshold set cpu** 配置命令恢复配置。

13.3.2 配置内存利用率门限

	命令	作用
Step 1	Ruijie# configure terminal	进入全局配置模式。
Step 2	Ruijie(config)# threshold set memory <i>warning_value critical_value</i>	配置指定设备的内存利用率告警门限和严重告警门限，范围为 1~100。

如果要恢复到缺省值，可用 **no threshold set memory** 配置命令恢复配置。

13.3.3 配置温度门限

	命令	作用
Step 1	Ruijie# configure terminal	进入全局配置模式。
Step 2	Ruijie(config)# threshold set temperature <i>warning_value critical_value</i>	配置指定设备的温度告警门限和严重告警门限，范围为 0 ~ 2147483647。

如果要恢复到缺省值，可用 **no threshold set temperature** 配置命令恢复配置。

13.3.4 查看配置

门限提供了如下的显示命令用于查看各类门限值，各命令的功能说明如：

命令	作用
show threshold cpu	显示设备的 CPU 利用率门限
show threshold memory	显示设备的内存利用率门限
show threshold temperature	显示设备的温度利用率门限



以上显示命令均能在除用户模式外的任何模式配置。

13.4 门限典型配置举例

13.4.1 配置步骤

使用如下命令将 CPU 利用率的两级门限设置为 80 和 90，温度的两级门限设置为 50 和 80。

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#threshold set cpu member 1 80 90
Ruijie(config)#threshold set temperature member 1 60 80
```

13.4.2 显示验证

使用 show threshold 查看各个门限的值

```
Ruijie#show threshold cpu
Device      Warning    Critical
Member 1:   80        90
Ruijie#show threshold memory
Device      Warning    Critical
Member 1:   90        100
Ruijie#show threshold temperature
Device      Warning    Critical
Member 1:   60        80
```

由上述信息可以看出，CPU 利用率门限和温度门限已被设置为指定值，而内存利用率门限依然为缺省值。

14 配置节能管理

14.1 理解EEE

14.1.1 概述

EEE(Energy Efficient Ethernet)，高效能以太网，是一种节省能源的以太网方案。EEE 是在以太网网连接闲置时间，使端口进入低功耗节能模式来达到节省能源的目的。

LPI(Low Power Idle) 模式，即低功耗节能模式，端口进入该模式后，会大幅减小端口发送的信号，仅发送维持端口链路连接的信号来达到节能的目的。

14.1.2 工作原理

100M 及 100M 以上接口的固有以太网标准规格具备闲置状态 (Active Idle State)，若要维持在连接状态，不受数据传输的限制，则需使用大量的电能。因此，无论链路上有没有数据，耗电量都很大。即使没有数据传输，为了保持连接状态，端口也会一直发送 IDLE 信号来维持端口链路的连接状态。

EEE 通过控制交换机端口，将端口进入 LPI (Low Power Idle) 模式来达到节省能源的目的。LPI 低功耗模式在链路利用率低的阶段耗电量低。EEE 技术也可以使端口从 LPI 状态快速转换成正常状态，提供高性能数据传输。

端口使能 EEE 节能功能后，如果在连续一段时间内端口状态始终为 up 且没有收发任何报文，则端口自动进入节能模式；当端口需要收发报文时，端口又自动恢复工作模式，从而达到节能的效果。EEE 功能要生效，达到节能效果，需要对端端口也支持 EEE 功能。

14.1.3 协议规范

参见 IEEE 802.3az 标准。

14.2 配置EEE

14.2.1 缺省配置

功能特性	缺省值
端口 EEE 节能模式	关闭

14.2.2 配置端口EEE节能功能

以下是配置端口 EEE 节能功能的命令。

	命令	作用
Step 1	Ruijie# configure	进入全局配置模式
Step 2	Ruijie(config)# interface gigabitEthernet interface-id	进入接口配置模式，指定要配置的物理端口

Step 3	Ruijie(config-if)# eee enable no eee enable	使能/关闭端口的 EEE 节能功能

例：打开/关闭端口 1 的 EEE 节能功能。

```
Ruijie# configure
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# eee enable
Ruijie(config-if)# no eee enable
Ruijie(config-if)# end
```

☺各产品支持情况

仅 S5750-28GT-S V2.0 设备支持 EEE 功能。

⚡ 注意

- 1、仅工作在 100M 和 1000M 速率模式的电口支持 EEE 功能。
- 2、EEE 功能仅在端口开启自协商能力时生效。

14.2.3 显示端口EEE状态

用户可以在特权模式下通过 show 命令可来查看接口状态。

命令	作用
Ruijie# show eee interface [gigabitEthernet interface-id]	显示指定端口的 EEE 节能状态
Ruijie# show eee interfaces status	显示所有端口 EEE 节能状态

例如：显示单个端口 gigabitEthernet 0/1 的 EEE 状态：

```
Ruijie#show eee interface gigabitEthernet 0/1
Interface           : Gi0/1
EEE Support         : YES
Admin Status        : enable
Oper Status         : disable
Remote Status       : disable
Trouble Cause       : Remote disable
```

显示的信息的含义是：

显示项	说明
Interface	接口编号。
EEE Support	端口是否支持 EEE 功能。
Admin Status	端口 EEE 管理配置状态。
Oper Status	端口 EEE 实际工作状态。
Remote Status	对端端口 EEE 状态。
Trouble Cause	故障原因，None 表示不存在故障。

Trouble cause 表示端口 EEE 状态不正常的原因，具体如下：

ID	Port trouble cause	说明

0	None	正常
1	Link down	端口 link down。
2	Speed not supported EEE	端口速率模式不支持 EEE。
3	Auto-negotiation was off	端口的自协商关闭。
4	Remote disable	对端端口关闭或不支持 EEE。

用户还可以不输入端口号，通过 **show eee interfaces status** 命令来显示全部端口的 EEE 节能状态。

显示所有端口的节能状态：

```
ruijie#show eee int st
```

Interface	EEE Support	Admin Status	Oper Status	Remote Status	Trouble Cause

Gi0/1	YES	enable	disable	unknown	1
Gi0/2	YES	enable	disable	unknown	1
Gi0/3	YES	enable	enable	enable	0
Gi0/4	YES	enable	enable	enable	0
Gi0/5	YES	enable	enable	enable	0
Gi0/6	YES	enable	enable	enable	0
Gi0/7	YES	enable	enable	enable	0
Gi0/8	YES	enable	enable	enable	0
Gi0/9	YES	enable	enable	enable	0
Gi0/10	YES	enable	enable	enable	0
Gi0/11	YES	enable	enable	enable	0
Gi0/12	YES	enable	enable	enable	0
Gi0/13	YES	enable	enable	enable	0
Gi0/14	YES	enable	enable	enable	0
Gi0/15	YES	enable	enable	enable	0
Gi0/16	YES	enable	enable	enable	0
Gi0/17	YES	enable	enable	enable	0
Gi0/18	YES	enable	enable	enable	0
Gi0/19	YES	enable	enable	enable	0
Gi0/20	YES	enable	enable	enable	0
Gi0/21	YES	enable	enable	enable	0
Gi0/22	YES	enable	enable	enable	0
Gi0/23	YES	enable	enable	enable	0
Gi0/24	YES	enable	enable	enable	0
Gi0/25	NO	-	-	-	-
Gi0/26	NO	-	-	-	-
Gi0/27	NO	-	-	-	-
Gi0/28	NO	-	-	-	-

15 配置设备管理

15.1.1 简介

设备管理主要包括：智能温控、资产管理两部分内容。

智能温控提供了一种系统的温度调控机制以及过温保护功能，在正常情况时通过智能控制风扇转速，保持系统在不过温的情况下实现降噪、节能以及提高风扇寿命的目的；在温度异常情况时提供过温保护功能，保护系统板卡上的器件安全。同时，提供对智能风扇模式的配置。

资产管理提供了对在线资产信息的查看，实现高效、快捷的资产信息的查看与管理。

15.1.2 基本概念

15.1.2.1 智能温控

智能温控系统由智能风扇以及设备过温保护两个功能构成。

缺省情况下使能智能温控，不支持关闭智能温控配置。各温度门限的默认值如下表所示(注：该温度值是指当前机箱内部温度)：

门限	门限值描述	温度门限值	
		S5750-28GT-S 1.X 设备	S5750-28GT-S 2.X 设备
最大工作温度门限	系统正常工作的最高温度	87℃	83℃
过温门限	超过这个温度，系统不能正常工作	94℃	88℃

智能风扇

风扇支持三种调速模式：自动模式和强制开启模式、强制关闭模式。

自动模式：根据设备机箱内的运行温度动态的控制智能风扇以适当的转速运行，从而实现：

- 降低设备工作噪声
- 降低风扇工作能耗
- 提高风扇工作寿命

强制开启模式：强制风扇转动，此模式的下的风扇一直处于高速运转状态，从而保证设备一直处于很低的工作温度下，有效的保护设备的正常工作。

强制关闭模式：强制风扇转动，此模式下的风扇在保护温度下会处于不转状态，从而达到设备静音效果。



使用风扇的强制模式会提高设备的噪声、功耗，而且会降低风扇的使用寿命，请慎重此模式。

过温保护

过温保护功能，是当运行的设备机箱内温度升高，并超过设备的最大工作温度的情况下，设备会将所有端口都关闭，POE 供电也会停止。从而有效的降低设备的温度，在设备机箱内温度降低到正常工作温度以下后，再将所有的端口打开，同时 POE 也开始供电。

15.1.2.2 资产管理

资产管理主要实现在线资产软件版本、硬件版本、产品序列号等信息的查看，方便用户对设备的资产信息进行查看。

15.1.3 工作原理

智能风扇，通过独立的软件进行控制，根据实时采集的温度，实时的调整风扇的转速，从而达到降低设备的工作温度等目的。智能风扇缺省情况下的工作模式为自动模式。

过温保护，通过独立的软件进行控制，每 2 秒采集一次设备的工作温度，取连续 5 次的采样数据中的最小值作为比较温度，与系统的最大工作温度和正常共组温度进行对比，进而进行对应的控制。

15.2 配置风扇

15.2.1 缺省配置

功能特性	缺省值
工作模式	Auto

15.3 监视与维护

15.3.1 查看风扇

命令	作用
Ruijie# show fans	查看风扇的运行状态、工作模式和转速等信息。

例：查看风扇的工作模式。

```
Ruijie#show fans
```

```
Device   Fan    State   Mode                               Speed(rpm)
-----
1        1      Normal  Disable                           N/A
```

15.3.2 查看设备温度状态和温度值

命令	作用
Ruijie# show temperature	查看当前设备温度状态和温度值。

例：查看在线资产的信息。

```
Ruijie#show temperature
Device  Temperature Slot  State      Current(C)
-----  -
1        0                normal      46
Ruijie#
```



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. 配置接口
2. 配置 MAC 地址
3. 配置 Aggregate Port
4. 配置 VLAN
5. 配置 Super-vlan
6. 配置 Protocol VLAN
7. 配置 Private VLAN
8. 配置 Voice VLAN
9. 配置 MSTP
10. 配置协议帧透传
11. 配置 GVRP
12. 配置 LLDP
13. 配置 QINQ

1 配置接口

1.1 接口类型概述

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) (三层设备支持)

1.1.1 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

1.1.1.1 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。

1.1.1.1.1 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

Untagged 帧

Access Port 接收不带 TAG 标志的帧，并为无 TAG 帧添加缺省 VLAN 的 TAG。发送前，去掉添加的 TAG，再发送。

Tagged 帧

Access 端口接收到的数据帧带有 TAG 时，将按照以下条件进行处理：

当 TAG 的 VID (VLAN ID) 与缺省 VLAN ID 相同时，接收该数据帧，并在发送时去掉 TAG 标志后发送。

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。

1.1.1.1.2 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。



注意

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。

Untagged 帧

若 Trunk port 接收到的帧不带 IEEE802.1Q TAG,那么帧将在这个接口的 Native VLAN 中传输。

Tagged 帧

若 Trunk port 接收到帧是带 TAG 的，将按照以下条件进行处理：

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。



说明

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。

1.1.1.1.3 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。

1.1.1.2 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。

1.1.2 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

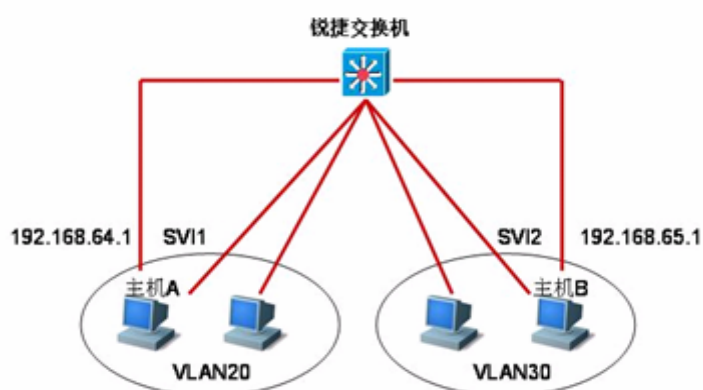
L3 Aggregate Port

1.1.2.1 SVI(Switch virtual interface)

SVI 是交换虚拟接口, 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



1.1.2.2 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。



注意

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。

1.1.2.3 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。

1.2 配置接口

本节描述接口的缺省配置，配置指南，配置步骤，配置实例

1.2.1 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。



注意

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。

1.2.2 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 接口 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。

1.2.3 使用interface range命令

1.2.3.1 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;

Fastethernet slot/{第一个 port} - {最后一个 port};

Gigabitethernet slot/{第一个 port} - {最后一个 port};

TenGigabitethernet 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 fastethernet 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 fastethernet 1/1-5, 1/7-8
Ruijie(config-if-range)# no shutdown
Ruijie(config-if-range)#
```

1.2.3.2 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

Step 1	Ruijie(config)# define interface-range <i>macro_name interface-range</i>	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。
Step 2	Ruijie(config)# interface range macro <i>macro_name</i>	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代表接口范围的字符串。

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;
- **fastethernet slot**{第一个 *port*} - {最后一个 *port*};
- **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 fastethernet1/1-4 的宏定义：

```
Ruijie# configure terminal
Ruijie(config)# define interface-range resource
fastethernet 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
fastethernet 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
```

1.2.4 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。

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。

命令	作用
Ruijie(config-if)# medium-type { 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# config 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
```

1.2.5 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# config 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
```



R2700 交换卡(NM2-24ESW/NM2-16ESW)端口在 **shutdown** 时，相连的本端和对端端口的 Link 灯不会灭，对端端口发包时，Link 灯会闪，但是本端端口不会转发任何报文。

1.2.6 配置接口的速率、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、流控和自协商模式。

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 和 Routed Port 有效。

	命令	作用
Step 1	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; 设备的光口速率强制为 1000M。
Step 2	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。
Step 3	Ruijie(config-if)# flowcontrol {auto on off}	设置接口的流控模式。 注意: 当接口的速率、双工和流控都设为非 auto 模式时, 该接口关闭自协商过程
Step 4	Ruijie(config-if)# negotiation mode { on off }	设置接口的自协商模式为 on 状态或者 off 状态。
 说明 10.4(2b12)及其之前版本, 自协商模式默认为 on 状态。10.4(2b12)p1 及其之后版本自协商模式默认为 off 状态。		

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、关闭流控, 并且设置接口的自协商模式为 on 状态:

```
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
```

 注意

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、流控和接口的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** 的，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** 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。

speed	duplex	flowcontrol	negotiation mode	自协商工作状态
auto	full/half	on/off	off	开启
10/100/1000	auto	on/off	off	开启
10/100/1000	full/half	auto	off	开启
10/100/1000	full/half	on/off	on	开启
10/100/1000	full/half	on/off	off	关闭

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。

1.2.7 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# config 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
```

1.2.8 配置二层接口

下表显示了二层接口的缺省配置，有关 **VLAN** 及端口的配置请参照“配置 **VLAN**”和“配置基于端口的流量控制”。

二层接口的缺省配置如下表：

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
Aggregate port	无
风暴控制	关闭
保护端口	关闭
端口安全	关闭

1.2.8.1 配置Switch Port

1.2.8.1.1 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 <i>vlan-id</i>	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
```

1.2.8.1.2 配置Hybrid端口

您可以通过以下步骤配置 Hybrid 端口：

	命令	作用
Step 1	configure terminal	进入配置模式
Step 2	interface <interface>	进入接口配置模式 百兆,千兆, 万兆
Step 3	switchport mode hybrid	配置为端口为 hybrid 口
	no switchport mode	删除端口模式
Step 4	switchport hybrid native vlan <i>id</i>	设置 hybrid 口的默认 VLAN

Step 5	switchport hybrid allowed vlan [[add] [tagged untagged]] [remove] vlist	设置端口的输出规则

```
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
```

1.2.8.2 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”。

1.2.8.3 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 Aggregate 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 interface 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 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
```

1.2.9 配置三层接口

配置三层接口：

	命令	作用
Step 1	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 Aggregate port。
Step 2	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
```

1.2.9.1 配置SVI

本节主要描述如何创建 SVI 及和 SVI 的一些相关配置。

您可通过 **interface vlan vlan-id** 创建一个 SVI 或修改一个已经存在的 SVI。

SVI 的配置：

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
```

1.2.9.2 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
Step 1	Ruijie(config-if)# no switchport	将该接口 Shut Down 并转换成三层模式
Step 2	Ruijie(config-if)# ip address ip_address subnet_mask	配置 IP 地址和子网掩码。



注意

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
```

1.2.9.3 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
Step 1	Ruijie(config-if)# no switchport	将该接口 Shut Down 并转换成三层模式
Step 2	Ruijie(config-if)# ip address <i>ip_address</i> <i>subnet_mask</i>	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 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** 命令可来看查看接口状态。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 [<i>interface-id</i>]	显示指定接口的全部状态和配置信息。
Ruijie# show interfaces <i>interface-id</i> status	显示接口的状态。
Ruijie# show interfaces [<i>interface-id</i>] switchport	显示可交换接口（非路由接口）的 administrative 和 operational 状态信息。
Ruijie# show interfaces [<i>interface-id</i>] description	显示指定接口的描述配置和接口状态。
Ruijie# show interfaces [<i>interface-id</i>] 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。

以下例子为显示接口 GigabitEthernet 1/1 的接口状态：

```
Ruijie# show interfaces gigabitethernet 1/1
GigabitEthernet : Gi 1/1
Description    : user A
AdminStatus    : up
OperStatus     : down
Hardware       : 1000BASE-TX
Mtu            : 1500
PhysAddress    :
LastChange     : 0:0h:0m:0s
AdminDuplex    : Auto
OperDuplex     : Unknown
AdminSpeed     : 1000M
OperSpeed      : Unknown
FlowControlAdminStatus : Enabled
FlowControlOperStatus : Disabled
Priority        : 1
```

以下例子为显示接口 SVI 5 的接口状态和配置信息：

```
Ruijie# show interfaces vlan 5
VLAN : V5
```

```

Description          : SVI 5
AdminStatus          : up
OperStatus           : down
Primary Internet address : 192.168.65.230/24
Broadcast address      : 192.168.65.255
PhysAddress           : 00d0.f800.0001
LastChange            : 0:0h:0m:5s

```

以下例子为显示接口 Aggregate Port 3 的接口状态:

```

Ruijie# show interfaces aggregateport 3
Interface   : AggregatePort 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 1/2 description
Interface      Status      Administrative  Description
-----
gigabitEthernet 2/1      down        down           Gi 2/1

```

以下例子为显示端口统计值

```

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

```

1.4 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) : 1310
Transfer Distance:
  SMF fiber
    -- 10km
  EBW 50/125 um fiber
    -- 300m
  50/125 um fiber
    -- 100m
  62.5/125 um fiber
    -- 33m
Digital Diagnostic Monitoring : YES
```

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
gigabitEthernet 5/4 transceiver current alarm information:
RX loss of signal
```

下表是 SFP 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
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

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:
Temp(°C)   Voltage(V)   Bias(mA)   RX power(dBM)   TX power(dBM)
36(OK)     3.31(OK)     6.13(OK)   -35.64(warning) -5.19(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

注意

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。
光模块故障告警和诊断参数测量需要光模块支持 **Digital Diagnostic Monitoring** 功能才能显示。

1.5 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
Step 1	configure terminal	进入配置模式
Step 2	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
```

1.6 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。

此命令可以在接口模式下和特权模式下执行。

在接口模式下使用如下命令执行线缆检测：

	命令	作用
Step 1	configure terminal	进入配置模式
Step 2	Ruijie(config)# interface interface	进入接口模式
Step 3	Ruijie(config-if)# line-detect [detail]	执行线缆检测

在特权模式下使用如下命令执行线缆检测：

命令	作用
show interface interface line-detect [detail]	执行线缆检测



注意

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-diagnoses end! this is result:
cable-state: Ok   length(meters): NA
```

显示项解释：

显示项	解释
cable-state	线缆的全局状态，共有四个值：OK（正常），Short（短路），Open（断路），Fail（检测失败）。
length	线缆的全局长度，单位为米。只有 cable-state 全局状态为 Short 或 Open 的长度才有效。其它状态下长度无效，显示为 NA。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。

```
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#line-detect detail
Interface: GigabitEthernet 0/1
start cable-diagnoses, please wait...
cable-daignoses end! this is result:
pair state      length(meters)
-----
A   Ok          1
-----
B   Ok          2
-----
C   Short       1
-----
D   Short       1
```

显示项解释：

显示项	解释
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，共有五个值：OK（正常），Short（短路），Open（断路），Crosstalk（若即若离），Unknown（检测失败）。
length	线缆的线对长度，单位为米。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。

1.7 LinkTrap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。

1.7.1 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.

1.7.2 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 配置 MAC 地址

以太网交换机利用 MAC 地址表的信息在数据链路层对报文进行快速寻址转发，本章对 MAC 地址的配置方法进行描述。

2.1 理解MAC地址表

2.1.1 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：

状态	VLAN	MAC地址	端口

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。

说明

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》。

2.1.2 动态地址学习

2.1.2.1 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。

2.1.2.2 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。

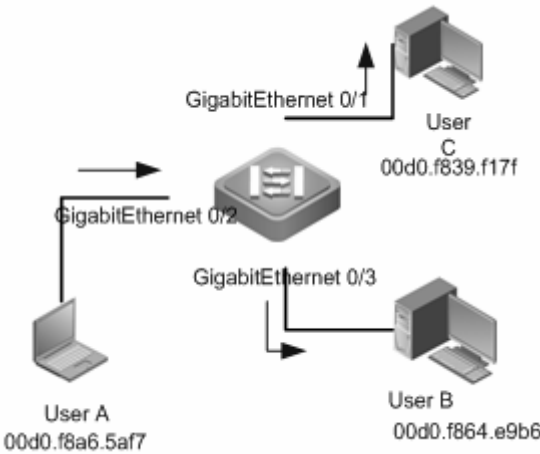


图 2-2 动态地址学习步骤一

Status	VLAN	MAC地址	端口
动态	1	00d0.f8a6.5af7	GigabitEthernet 0/2

图 2-3 以太网交换 MAC 地址表一

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。

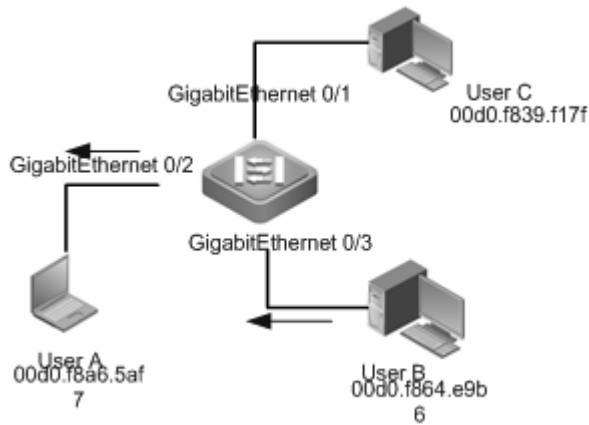


图 2-4 动态地址学习步骤二

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

图 2-5 以太网交换机 MAC 地址表二

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。

注意

堆叠系统下各成员设备的地址表是不同步的堆叠下各成员的地址表是不同步的。举例说明如下:

假如设备 A 和设备 B 堆叠,设备 A 为主机;往设备 A 发送广播报文,那么设备 A 的收帧端口会学习到该地址—mac1,地址表中记录设备 A 的收帧端口学习到地址 mac1;由于报文会通过堆叠口广播到设备 B,因此设备 B 上的堆叠口实际上也会学习到该地址,但不会记录到地址表中。

删除设备 A 收帧端口学习到的地址,那么地址表中的 mac1 被删除,但是设备 B 的堆叠口依然学习到了该地址,这就造成了主从机硬件地址表不一致。此时往设备 A 的其它端口发送目的 mac 为 mac1 的报文,那么该报文将不会在设备 B 上广播,因为该地址已经被设备 B 的堆叠口学习到了,该地址老化之后,报文广播到设备 B 的端口上。

由于堆叠下各成员设备的地址表可能是不同步的,再加上 hash 存在冲突的可能,在某些极端情况下,地址表记录会多出,而且地址表中的某些记录可能会老化不掉。举例说明如下:

假设设备 A 和设备 B 堆叠,设备 A 为主机。设备 B 的端口 Bport 接终端设备(如 PC)发送广播报文。假设这时,设备 A 和设备 B 都学满地址,由于各成员设备的地址表是不同步的,此时就可能出现设备 B 上有一个 mac1+vid1+Bport 的地址,而在设备 A 上没有。但这个地址也会记录到地址记录中,这样就导致地址表记录多出来了。

这时用户将 mac1 的终端设备(如 pc)从设备 B 的 Bport 移到设备 A 的 Aport 时,重新进行 mac1+vid1 的地址学习时,由于设备 A 的地址已经学满,而且原先不存在 mac1+vid1 的地址,所以无法学到该地址,报文通过堆叠口广播到设备 B,设备 B 发现该 mac1+vid1 的地址已经存在,于是设备 B 用 mac1+vid1+Aport 的地址覆盖掉 mac1+vid1+Bport 的地址。由于实现限制地址记录中 mac1+vid1+Bport 的地址记录并没有被删除掉,但此时设备 B 学到的是 mac1+vid1+Aport 的地址,因此,即使过了老化时间,地址记录中的 mac1+vid1+Bport 也不会被老化掉。这时就要手动清空地址表,命令为 clear mac-address-table dynamic。

2.1.2.3 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计时，在达到老化计时前，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，则该地址在达到老化时间后会从 MAC 地址表中删除。

2.1.3 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。

2.1.4 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。

2.1.5 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。

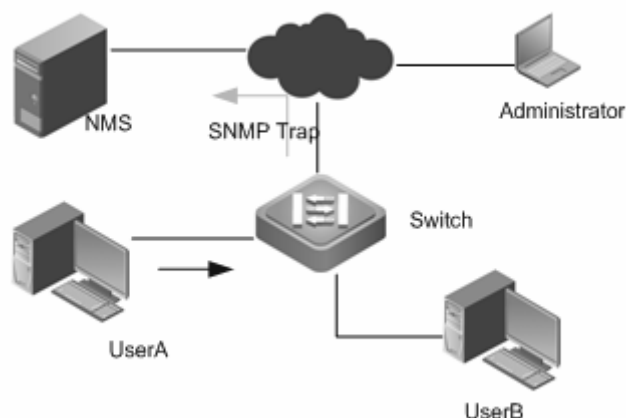


图 2-6 地址变化通告

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。

说明

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。

2.1.6 IP和MAC地址绑定

2.1.6.1 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。

2.1.6.2 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

2.1.6.3 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。

 说明

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。

2.1.7 工作原理

无

2.1.8 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》

2.2 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
动态地址学习模式	dispersive
动态地址同步功能	关闭
VLAN 动态地址数目限制	关闭
MAC 地址变化通知功能	关闭
地址绑定模式	compatible

2.3 配置动态地址

2.3.1 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。

2.3.2 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 <i>mac-address</i> vlan <i>vlan-id</i>	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 <i>interface-id</i> [vlan <i>vlan-id</i>]	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 <i>vlan-id</i>	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 中的所有动态地址。

```
Ruijie#clear mac-address-table dynamic interface GigabitEthernet 0/1 vlan 1
```

2.3.3 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 count interface g0/1
Dynamic Address Count : 10
Static Address Count : 0
Filter Address Count : 0
Total Mac Addresses : 10
```

2.4 配置动态地址老化时间

2.4.1 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)# on 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
```

2.4.2 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
```

2.5 配置静态地址

2.5.1 管理静态地址

命令	作用
Ruijie(config)# mac-address-table static <i>mac-address</i> vlan <i>vlan-id</i> interface <i>interface-id</i>	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 <i>mac-address</i> vlan <i>vlan-id</i> interface <i>interface-id</i>	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
```

2.5.2 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

2.6 配置过滤地址

2.6.1 管理过滤地址

命令	作用
Ruijie(config)# mac-address-table filtering <i>mac-address</i> vlan <i>vlan-id</i>	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 <i>vlan-id</i> 指定的 VLAN 上接收到以 <i>mac-address</i> 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 <i>mac-address</i> vlan <i>vlan-id</i>	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一个过滤地址 00d0.f800.073c，当在 VLAN 4 中接受到源地址或目的地址为该地址的报文时，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 filtering 00d0.f800.073c vlan 4
```

2.6.2 查看配置

命令	作用
Ruijie#show mac-address-table filtering	查看所有的过滤地址信息

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

2.7 配置MAC地址变化通知

2.7.1 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
Step 1	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。
Step 2	Ruijie (config)#snmp-server enable traps	使能设备发送 trap 功能。
Step 3	Ruijie(config)#mac-address-table notification	打开 MAC 地址通知功能开关。
Step 4	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。
Step 5	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

```

2.7.2 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

```

2.8 配置IP地址和MAC地址绑定

2.8.1 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
Step 1	Ruijie(config)# address-bind <i>ip-address</i> <i>mac-address</i>	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
Step 2	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
```

 注意

-
- 问题缺陷：由于地址绑定的存在，堆叠交换机中的某一台交换机，如果收到不符合地址绑定的 ip 报文时进行地址学习，这个地址只会被收到报文的交换机的芯片学习到，堆叠中的其他交换机芯片不会学习到。
现象：使用不符合地址绑定的 IP 报文进行 MAC 地址学习时，在堆叠情况下会出现在“show mac”地址表中存在该表项，而报文仍然会在堆叠中的其他交换机上被广播，使用 ARP 等非 IP 报文或使用符合地址绑定的 IP 报文时可正常进行地址学习。
 - 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。

2.8.2 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:

注意

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。 1: IPV6 兼容模式与端口安全/DOT1X 认证共用时,所有安全地址的 IPV6 报文都可以通行。 2: 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。

2.8.3 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
```

2.8.4 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
```

2.9 典型配置举例

2.9.1 网络配置

某信息系统组网如下：

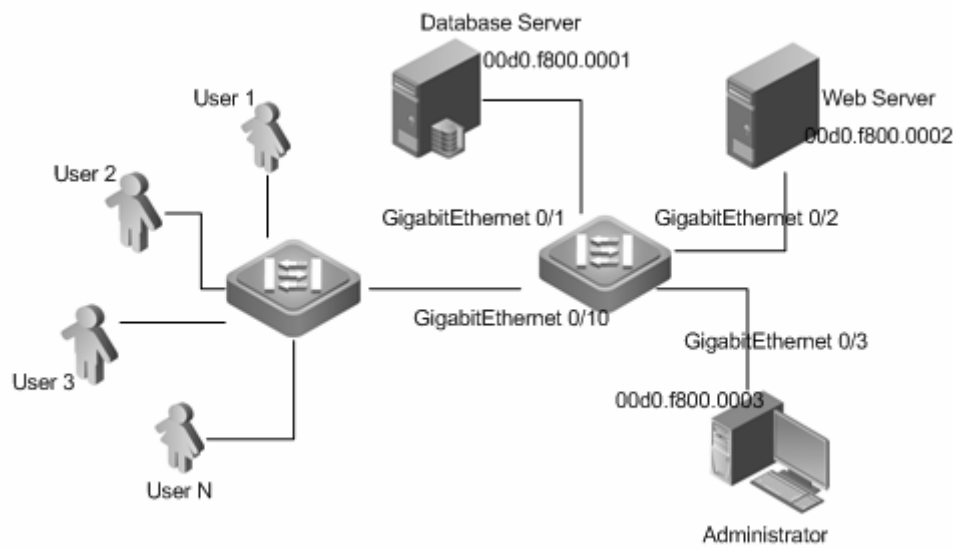


图 2-7 典型应用模型

数据库服务器通过 GigabitEthernet0/1 接到以太网交换机，WEB 服务服务器通 GigabitEthernet 0/2 接到以太网交换机，服务器管理员通过 GigabitEthernet 0/3 接到以太网交换机，其他的一般用户通过以太网交换机的 GigabitEthernet 0/10 接入访问 WEB 服务器，所有的数据均在 VLAN 1 中转发。

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的数据转发采用单播方式，管理员与服务器之间的数据转发也采用单播方式，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。

2.9.2 设备配置

设备配置过程

```
Ruijie#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Ruijie(config)#mac-address-table static 00d0.f800.0001 vlan 1 interface  
GigabitEthernet 0/1
```

```
Ruijie(config)#mac-address-table static 00d0.f800.0002 vlan 1 interface  
GigabitEthernet 0/2
```

```
Ruijie(config)#mac-address-table static 00d0.f800.0003 vlan 1 interface  
GigabitEthernet 0/3
```

查看设备配置

```
Ruijie#show mac-address-table static
```

Vlan	MAC Address	Type	Interface
1	00d0.f800.0001	STATIC	GigabitEthernet 0/1
1	00d0.f800.0002	STATIC	GigabitEthernet 0/2
1	00d0.f800.0003	STATIC	GigabitEthernet 0/3

3 配置Aggregate Port

本章描述如何在锐捷设备的上配置 Aggregate Port。

3.1 概述

3.1.1 理解Aggregate Port

我们可以把多个物理链接捆绑在一起形成一个逻辑链接，这个逻辑链接我们称之为 **Aggregate Port**（以下简称 **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去。**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。

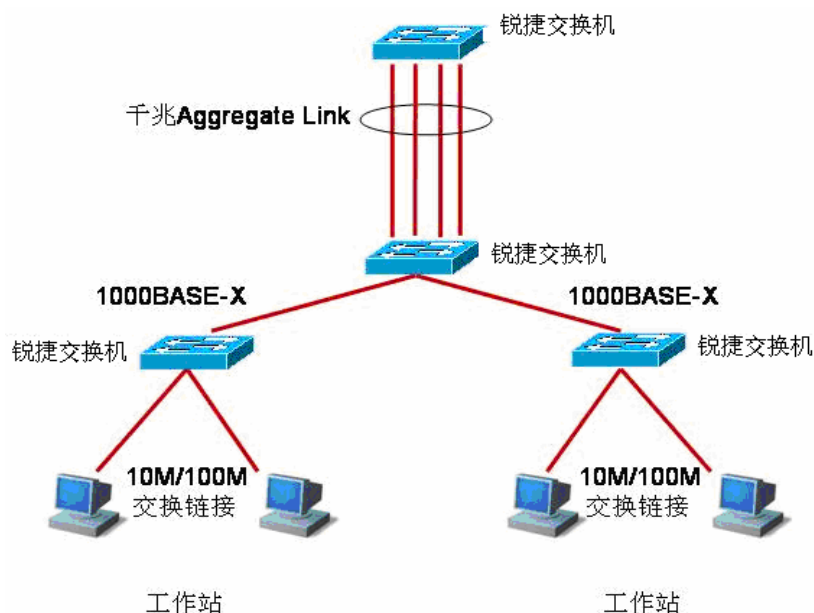


图 3-1 典型的 AP 配置

交换机各产品系列的每个 **AP** 口最多包含的成员口数量都为 8 个，各系列支持最大 **AP** 数量则如下表所示：

3.1.2 理解流量平衡

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，一，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。

我们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。

说明

1. 流量平衡模式设置为源 IP、目的 IP、源 IP+目的 IP 时对 2 层报文采用设备的默认模式进行流量平衡。默认模式可在设备未配置 **aggregateport load-balance** 参数时通过 **show aggregateport load-balance** 命令获得。

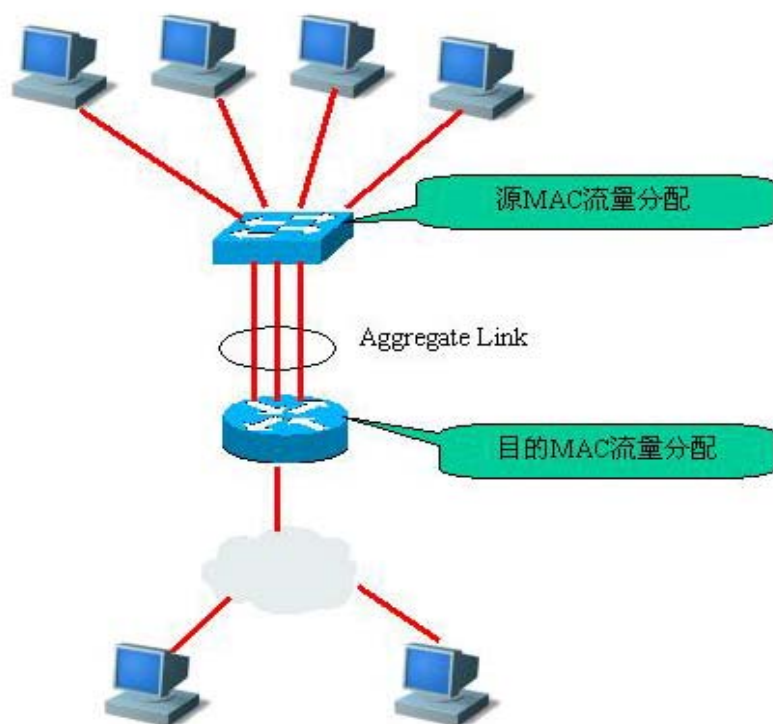


图 3-2 AP 流量平衡示意图

3.2 配置Aggregate Port

3.2.1 缺省的Aggregate Port配置

AP 的缺省配置如下表所示：

功能特性	缺省值
二层 AP 接口	无
三层 AP 接口	无
流量平衡	根据源 MAC 和目的 MAC 地址进行流量分配。

3.2.2 Aggregate Port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其加入 AP 前的属性。

**注意**

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Aggregate Port

在接口配置模式下，请按如下步骤将端口加入 AP：

命令	作用
Ruijie(config-if-range)# port-group port-group-number	将该接口加入一个 AP(如果这个 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** 命令将一个物理端口退出 AP。

下面的例子是将二层的以太网接口 0/1 配置成二层 AP 5 成员：

```
Ruijie# configure terminal
Ruijie(config)# interface range gigabitEthernet 0/1
Ruijie(config-if-range)# port-group 5
Ruijie(config-if-range)# end
```

您可以在全局配置模式下使用命令 Ruijie(config)# **interface aggregateport n** (n 为 AP 号)来直接创建一个 AP(如果 AP n 不存在)。

**注意**

- 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 配置三层Aggregate Port

缺省情况下，一个 Aggregate Port 是一个二层的 AP，如果您要配置一个三层 AP，您需要进行如下操作。

下面的例子是如何配置一个三层 AP 接口（AP 3），并且给它配置 IP 地址（192.168.1.1）：

```
Ruijie# configure terminal
Ruijie(config)# interface aggregateport 3
Ruijie(config-if)# no switchport
Ruijie(config-if)# ip address 192.168.1.1 255.255.255.0
Ruijie(config-if)# end
```

**注意**

- 三层 AP 是三层交换机才支持的功能，所有二层交换机均不支持。
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，所以，您必须先创建该三层 AP 接口，再将各三层接口加入。

创建了一个三层的 AP 接口以后，您就可以往该 AP 口添加成员口了，如下例，将 gigabitEthernet 0/1-3 加入三层 AP 2：

```
Ruijie# configure terminal
Ruijie(config)# interface range aggregateport 1-3
Ruijie(config-if)# no switchport
Ruijie(config-if)# port-group 2
```

3.2.5 配置Aggregate Port的流量平衡

在配置模式下，请按如下步骤配置 AP 的流量平衡算法：

命令	作用
Ruijie(config)# aggregateport load-balance { dst-mac src-mac src-dst-mac dst-ip src-ip src-dst-ip }	设置 AP 的流量平衡，选择使用的算法： 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。

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。

3.3 显示Aggregate Port

在特权模式下，请按如下步骤显示 AP 设置：

命令	作用
Ruijie# show aggregateport [<i>port-number</i>] { oad-balance summary }	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 配置 VLAN

本章描述如何配置 IEEE802.1Q VLAN

4.1 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。

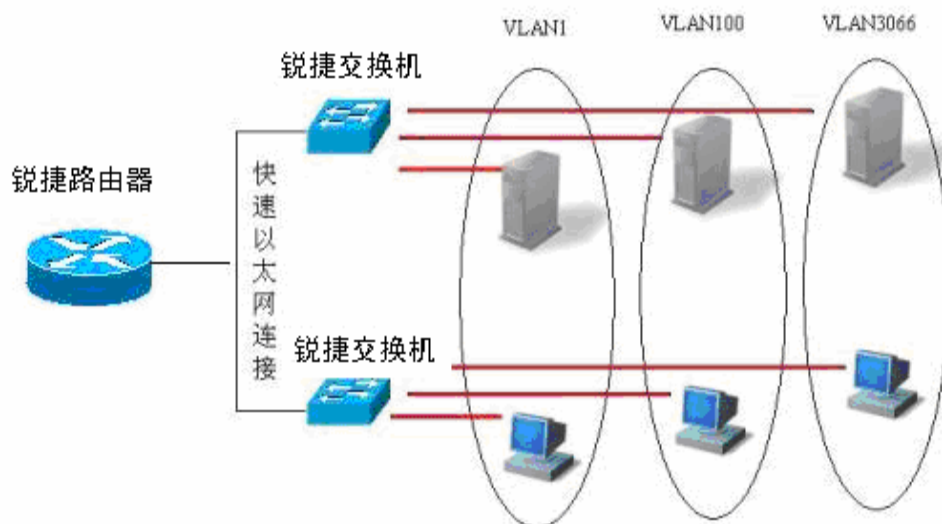


图 4-1

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。

4.1.1 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。

注意

- 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。

4.1.2 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
Step 1	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。
Step 2	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。

4.2 配置VLAN

一个 VLAN 是以 VLAN ID 来标识的。在设备中，您可以添加、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。

4.2.1 VLAN 配置信息的保存

当您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。

4.2.2 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

4.2.3 创建、修改一个 VLAN

在全局配置模式下，您可以创建或者修改一个 VLAN：

	命令	作用
Step 1	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。
Step 2	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。

如果您想把 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
```

4.2.4 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
Step 1	Ruijie(config)# no vlan vlan-id	输入一个 VLAN ID，删除它。

4.2.5 向 VLAN 分配 Access 口

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
Step 1	Ruijie(config-if)# switchport mode access	定义该接口的 VLAN 成员类型（二层 ACCESS 口）
Step 2	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 FastEthernet 1/10 作为 Access 口加入了 VLAN20：

```
Ruijie# configure terminal
Ruijie(config)# interface fastethernet 1/10
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# sh int gi 0/1 switchport
Interface      Switchport Mode    Access Native Protected VLAN lists
-----
GigabitEthernet 0/1  enabled  ACCESS  1    1    Disabled ALL
```



注意

在路由器的交换卡上，接口在 trunk 模式下依然可以配置 access vlan，但该 access vlan 配置不生效，接口依然工作在 trunk 模式下，只有 native vlan 和 allowed vlan list 配置生效。

4.2.6 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
Step 1	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。

4.3 配置VLAN Trunks

4.3.1 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（如路由器或交换机）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。

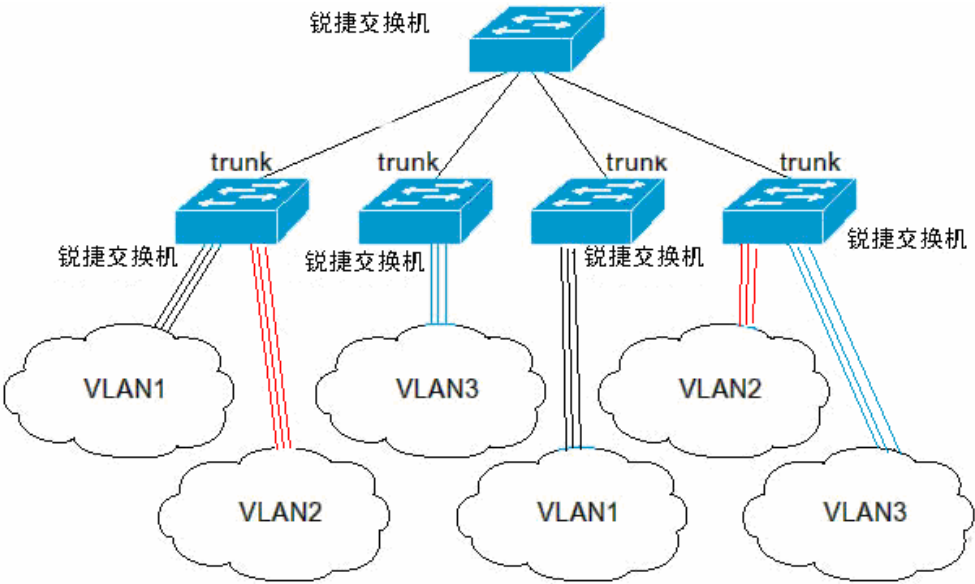


图 4-2

您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
Step 1	Ruijie(config-if)# switchport mode access	将一个接口设置成为 Access 模式
Step 2	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。

4.3.2 配置一个 Trunk 口

4.3.2.1 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
Step 1	Ruijie(config-if)# switchport mode trunk	定义该接口的类型为二层 Trunk 口

Step 2	Ruijie(config-if)# switchport trunk native vlan <i>vlan-id</i>	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。

4.3.3 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，您也可以通过设置 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
Step 1	Ruijie(config-if)# switchport trunk allowed vlan {all [add remove except] } <i>vlan-list</i>	（可选）配置这个 Trunk 口的许可 VLAN 列表。参数 <i>vlan-list</i> 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
```

4.3.4 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
Step 1	Ruijie(config-if)# switchport trunk native vlan <i>vlan-id</i>	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。

4.4 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
Step 1	<code>show vlan [id vlan-id]</code>	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
```

4.5 配置举例

4.5.1 组网拓扑

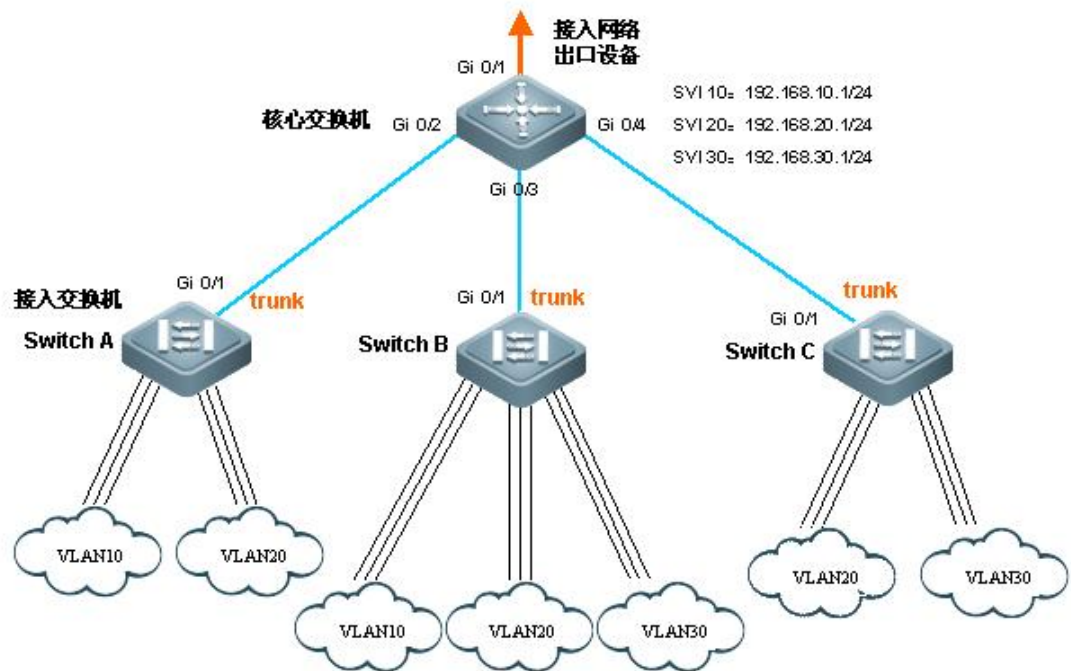


图 4-3

4.5.2 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。

4.5.3 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。

4.5.4 配置步骤

4.5.4.1 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
```

4.5.4.2 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
```

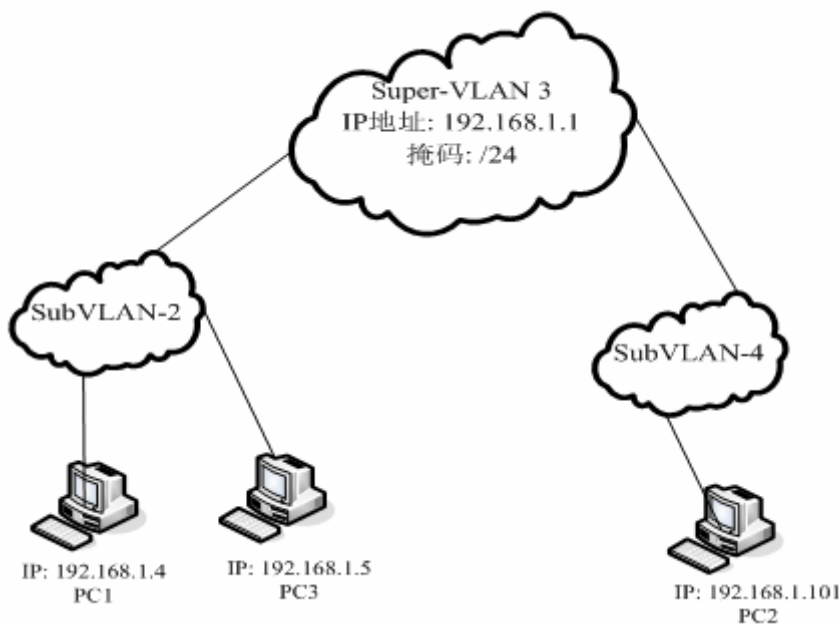
5 配置 Super VLAN

本章描述锐捷设备的 Super VLAN 配置

5.1 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。



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。

5.2 配置Super VLAN

可以使用下面的命令来设置 Super VLAN。

	命令	作用
Step 1	Ruijie# configure terminal	进入全局配置模式
Step 2	Ruijie(config)# vlan vlan-id	进入 VLAN 配置模式
Step 3	Ruijie(config-vlan)# supervlan	打开 SuperVLAN 的功能
Step 4	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。

5.3 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。



注意

可能由于资源不足导致设置 SubVLAN 失败

	命令	作用
Step 1	Ruijie# configure terminal	进入配置模式
Step 2	Ruijie(config)# vlan vlan-id	进入 VLAN 配置模式
Step 3	Ruijie(config-vlan)# supervlan	设置该 vlan 为 SuperVLAN
Step 4	Ruijie(config-vlan)# subvlan vlan-id-list	指定若干个 sub vlan 并把它们加入 supervlan 中。
Step 5	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。



注意

不能使用 **no vlan** 命令删除 SubVLAN，必须先转成普通 VLAN 才能删除。

5.4 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
Step 1	Ruijie# configure terminal	进入配置模式
Step 2	Ruijie(config)# vlan vlan-id	进入 vlan 配置模式
Step 3	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
Step 4	Ruijie(config-vlan)# end	回到特权模式
Step 5	Ruijie# show running-config	验证前面各步骤的配置



注意

用户可以通过执行 no subvlan-address-range 删除之前配置

5.5 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
Step 1	Ruijie# configure terminal	进入配置模式
Step 2	Ruijie(config)# interface vlan vlan-id	进入 SVI 模式
Step 3	Ruijie(config-vlan)# ip address ip mask	设置虚拟接口的 IP 地址
Step 4	Ruijie(config-vlan)# end	回到特权模式
Step 5	Ruijie# show running-config	验证前面各步骤的配置

5.6 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
Step 1	Ruijie# configure terminal	进入配置模式

Step 2	Ruijie(config)# vlan vlan-id	进入 VLAN 模式
Step 3	Ruijie(config-vlan)# proxy-arp	打开 VLAN 的 ARP 代理功能
Step 4	Ruijie(config-vlan)# end	回到特权模式
Step 5	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。

5.7 显示supervlan设置

可以使用下面的命令来显示设置 SuperVLAN 的配置

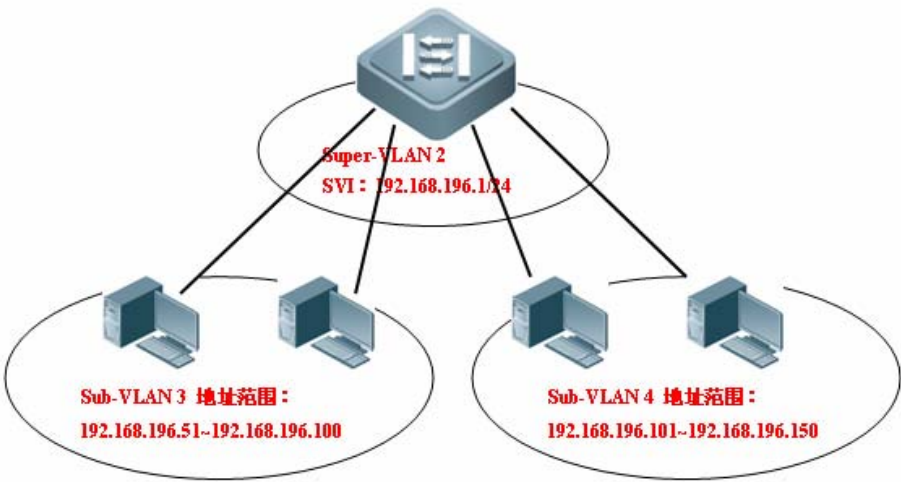
命令	作用
show supervlan	显示 supervlan 配置

5.8 Super VLAN配置用例

5.8.1 组网需求

创建一个 Super-VLAN 为 VLAN 2，并配置与它关联的 Sub-VLAN 为 VLAN 3 和 VLAN ；
Sub-VLAN 3 的地址范围为 192.168.196.51~192.168.196.100，Sub-VLAN 4 的地址范围为
192.168.196.101~192.168.196.150；
设置 Super-VLAN 的虚拟接口的 IP 地址为 192.168.196.1，子网掩码为 255.255.255.0；
设置 VLAN 的 ARP 代理功能。

5.8.2 组网拓扑



5.8.3 配置步骤

```
# 进入交换机的配置模式
Ruijie# configure terminal
# 创建 VLAN 2，并进入该 VLAN 的配置模式
```

```
Ruijie(config)# vlan 2
# 设置 VLAN 2 为 Super VLAN
Ruijie(config-vlan)# supervlan
# 退出到全局模式
Ruijie(config-vlan)# exit
# 创建 VLAN 3
Ruijie(config)# vlan 3
# 退出到全局模式
Ruijie(config-vlan)# exit
# 创建 VLAN 4
Ruijie(config)# vlan 4
# 退出到全局模式
Ruijie(config-vlan)# exit
# 进入 VLAN 2 的配置模式，并设置 VLAN 3 和 VLAN 4 为 Super VLAN 2 的 Sub-VLAN
Ruijie(config)# vlan
Ruijie(config-vlan)# subvlan 3,4
# 退出到全局模式，进入 VLAN 3 的配置模式，配置 VLAN 3 的地址范围为了
192.168.196.51~192.168.196.100
Ruijie(config-vlan)# exit
Ruijie(config)# vlan 3
Ruijie(config-vlan)# subvlan-address-range 192.168.196.51 192.168.196.100
# 退出到全局模式，进入 VLAN 4 的配置模式，配置 VLAN 4 的地址范围为了
192.168.196.101~192.168.196.150
Ruijie(config-vlan)# exit
Ruijie(config)# vlan 4
Ruijie(config-vlan)# subvlan-address-range 192.168.196.101 192.168.196.150
# 退出到全局模式
Ruijie(config-vlan)# exit
# 进入 SVI 模式
Ruijie(config)# interface vlan 2
# 为 VLAN 2 虚拟接口配置 IP 地址为 192.168.96.1，子网掩码为 255.255.255.0
Ruijie(config-if)# ip address 192.168.196.1 255.255.255.0
# 退出到全局模式，进入 VLAN 2 的配置模式，开启 ARP 代理功能（默认是开启的）
Ruijie(config-if)# exit
Ruijie(config)# vlan 2
Ruijie(config-vlan)# proxy-arp
# 退出到特权模式
Ruijie(config-vlan)# end
Ruijie# show supervlan
supervlan id  supervlan arp-proxy  subvlan id  subvlan arp-proxy  subvlan ip
range
-----
2              ON                    3        ON  192.168.196.51 - 192.168.196.100
              4        ON  192.168.196.101 - 192.168.196.150
```

6 配置Protocol VLAN

6.1 Protocol VLAN技术

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：

1. 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。
2. 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。
3. 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。

我司产品支持全局的基于 IP 地址的 VLAN 分类和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。

基于 IP 地址的 VLAN 分类是全局配置，如果您配置了基于 IP 地址的 VLAN 分类的话，其将应用到所有的 Trunk 口和 Hybrid 口上。

1. 如果输入报文为空 VLAN ID 报文,且输入报文的 IP 地址匹配您配置的 IP 地址的话，该报文将被划分到您配置的 VLAN 内。
2. 如果输入报文为空 VLAN ID 报文,且输入报文的报文类型和以太网类型匹配您配置在输入端口上的报文类型和以太网类型的话，该报文将被划分到您配置的 VLAN 内。

基于 IP 地址的 VLAN 分类优先级高于基于报文类型和以太网类型的 VLAN 分类，所以如果您同时配置了基于 IP 地址以及基于报文类型和以太网类型的 VLAN 分类，且输入报文同时符合两者的话，将是基于 IP 地址的 VLAN 分配起作用。

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。

6.2 配置 Protocol VLAN

6.2.1 缺省 Protocol VLAN

缺省情况下，没有 Protocol VLAN 的配置。

6.2.2 配置基于 IP 地址的 VLAN 分类

配置方法如下命令：

	命令	作用
Step 1	Ruijie# configure terminal	进入全局配置模式
Step 2	Ruijie(config)# protocol-vlan ipv4 address mask address vlan vid	配置 IP 地址、子网掩码以及 VLAN 分类
	Ruijie(config)# no protocol-vlan ipv4 address mask address	取消 IP 地址配置
	Ruijie(config)# no protocol-vlan ipv4	取消所有的 IP 地址配置
Step 3	Ruijie(config)# interface interface-id	进入接口配置模式
	Ruijie(config-if)# protocol vlan ipv4	在接口上使能基于 IP 地址的 VLAN 分类
	Ruijie(config-if)# no protocol vlan ipv4	在接口上取消使能基于 IP 地址的 VLAN 分类
Step 4	Ruijie(config-vlan)# show protocol-vlan ipv4	显示 IP 地址配置

说明

请以 x.x.x.x 的方式指定 IP 地址和子网掩码。
可用的 VLAN ID 不同的产品可能会有所区别。

以下命令配置 IP 为 192.168.100.3，掩码为 255.255.255.0 的 VLAN 分类为 VLAN 100：

```
Ruijie# configure terminal
Ruijie(config)# protocol-vlan ipv4 192.168.100.3 mask 255.255.255.0 vlan 100
Ruijie(config-vlan)# show protocol-vlan ipv4
ip            mask            vlan
-----
192.168.100.3 255.255.255.0 100
```

6.2.3 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
Step 1	Ruijie# configure terminal	进入全局配置模式
Step 2	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
Step 3	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
ETHER_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      ETHER_AARP      NULL|NULL
2                SNAP        ETHER_APPLETALK NULL|NULL
```

说明

1. Profile 应用到端口上之后，配置才能生效；
2. 在更新某个 Profile 配置时，必须先删除该 Profile，再重新配置该 Profile；

6.2.4 应用profile

您可以通过下面的设置步骤来完成:

	命令	作用
Step 1	Ruijie# configure terminal	进入全局配置模式
Step 2	Ruijie(config)# interface interface-id	进入接口配置模式
Step 3	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
Step 5	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      ETHER_AARP      gi3/1|101
2                SNAP        ETHER_APPLETALK gi3/1|102
```

说明

- 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

6.3 Protocol VLAN的显示

您可以通过以下步骤显示 Protocol VLAN 内容：

命令	作用
Ruijie# 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 配置 Private VLAN

7.1 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。

隔离端口(Isolated Port)， 隔离 VLAN 中的端口，只能与混杂口通讯。

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。

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。

7.2 Private VLAN配置

7.2.1 缺省Private VLAN设置

缺省情况下，没有 Private VLAN 的配置

7.2.2 配置VLAN作为私有VLAN

配置方法如下命令

	命令	作用
Step 1	Ruijie# configure terminal	进入配置模式
Step 2	Ruijie(config)# vlan vid	进入 VLAN 配置模式
Step 3	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
Step 4	Ruijie(config-vlan)# end	退出 VLAN 模式

Step 5	Ruijie# show vlan private-vlan [type]	显示私有 VLAN

说明

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, 一对 Private VLAN 处于 ACTIVE 状态必须满足以下条件:

1. 具有 Primary 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
```

7.2.3 关联 Secondary VLAN 和 Primary VLAN

按如下方式关联 Secondary VLAN 和 Primary VLAN:

	命令	作用
Step 1	Ruijie# configure terminal	进入配置模式
Step 2	Ruijie(config)# vlan vid	进入 VLAN 配置模式
Step 3	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
Step 5	Ruijie(config-vlan)# end	退出 VLAN 模式
Step 6	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

说明

该操作在声明为 Primary VLAN 的 VLAN 配置模式进行。

7.2.4 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	作用
Step 1	Ruijie# configure terminal	进入配置模式
Step 2	Ruijie(config)# interface vlan p_vid	进入 Primary VLAN 的接口模式
Step 3	Ruijie(config-if-VLAN id)# private-vlan mapping {svlist add svlist remove svlist}	映射 Secondary VLAN 到 Primary VLAN 的 SVI 三层交换。
Step 4	Ruijie(config-if-VLAN id)# 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
Ruijie#
```

说明

操作中的 Primary VLAN 和 Secondary VLAN 是相关联的。

7.2.5 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	作用
Step 1	Ruijie# configure terminal	进入配置模式
Step 2	Ruijie(config-if)# interface <interface>	进入接口配置模式 <i>fastethernet, gigabitethernet, tengigabitethernet</i>
Step 3	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

Step 4	Ruijie(config-if)# switchport private-vlan host-association <i>p_vid s_vid</i>	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
Ruijie#
```

说明

操作中的 Primary VLAN 和 Secondary VLAN 是相关联的

7.2.6 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	作用
Step 1	Ruijie# configure terminal	进入配置模式
Step 2	Ruijie(config-if)# interface <interface>	进入接口配置模式 百兆,千兆, 万兆
Step 3	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
Step 4	Ruijie(config-if)# switchport private-vlan mapping <i>p_vid</i> { <i>svlist</i> add <i>svlist</i> remove <i>svlist</i> }	私有 VLAN 混杂端口选择所在 VLAN，及混杂的 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
Ruijie#
```

说明

操作中的 Primary VLAN 和 Secondary VLAN 是相关联的

7.3 Private VLAN显示

7.3.1 显示private VLAN

您可以通过以下步骤显示 Private VLAN 内容：

命令	作用
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
```

7.4 Private VLAN典型用例

7.4.1 多台交换机上的Private VLAN配置

7.4.1.1 组网需求

在两台设备上实现 Private VLAN 的配置应用，创建一个 Primary VLAN，一个 Community VLAN，一个 Isolated VLAN，同一个 Community VLAN 内的主机可以进行二层通讯，Isoated VLAN 内的主机与其它主机互不通讯，但 Private VLAN 内的主机均能与路由器通讯。

7.4.1.2 组网拓扑

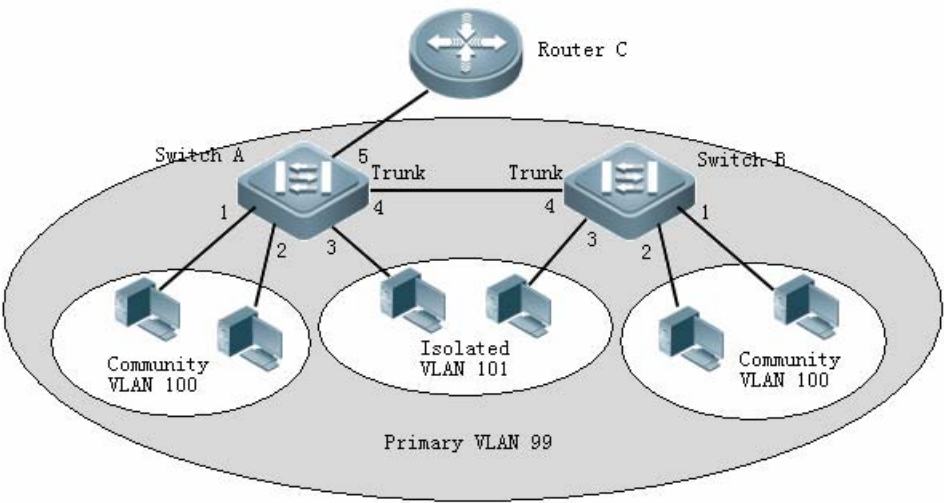


图 7-1

7.4.1.3 配置步骤

创建 VLAN 99 为 Primary VLAN，创建 VLAN 100 为 Community VLAN，创建 VLAN 101 为 Isolated VLAN，并关联主次 VLAN。

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#vlan 99
Ruijie(config-vlan)#private-vlan primary
Ruijie(config-vlan)#exit
Ruijie(config)#vlan 100
Ruijie(config-vlan)#private-vlan community
Ruijie(config-vlan)#exit
Ruijie(config)#vlan 101
Ruijie(config-vlan)#private-vlan isolated
Ruijie(config-vlan)#exit
Ruijie(config)#vlan 99
Ruijie(config-vlan)#private-vlan association 100,101
Ruijie(config-vlan)#exit
```

配置端口 0 / 1 和 0 / 2 属于 Community VLAN 100，端口 0/3 属于 Isolated VLAN 101，端口 0/4 为 Promiscuous Port。

```
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if)#switchport mode private-vlan host
Ruijie(config-if)#switchport private-vlan host-association 99 100
Ruijie(config-if)#exit
Ruijie(config)#interface gigabitEthernet 0/2
Ruijie(config-if)#switchport mode private-vlan host
Ruijie(config-if)#switchport private-vlan host-association 99 100
Ruijie(config-if)#exit
Ruijie(config)#interface gigabitEthernet 0/3
Ruijie(config-if)#switchport mode private-vlan host
Ruijie(config-if)#switchport private-vlan host-association 99 101
Ruijie(config-if)#exit
Ruijie(config)#interface gigabitEthernet 0/4
Ruijie(config-if)#switchport mode trunk
Ruijie(config-if)#exit
Ruijie(config)#interface gigabitEthernet 0/5
Ruijie(config-if)#switchport mode private-vlan promiscuous
Ruijie(config-if)#switchport private-vlan mapping 99 add 100-101
Ruijie(config-if)#show vlan private-vlan
```

VLAN	Type	Status	Routed	Ports	Associated VLANs
99	primary	active	Disabled	Gi0/4, Gi0/5	100-101
100	community	active	Disabled	Gi0/1, Gi0/2, Gi0/4	99
101	isolated	active	Disabled	Gi0/3, Gi0/4	99

7.4.2 单台三层交换机上的Private VLAN配置

7.4.2.1 组网需求

在支持 Private VLAN 的三层交换机上，可以为 Private VLAN 配置一个 SVI，一个 Private VLAN 下的所有 VLAN（包括 Primary VLAN 与的有的 Secondary VLAN）可以在同一个 SVI 内，只需在上个用例配置的基础上，为 Primary VLAN 配置一个 IP 地址，对于特定需要使用路由的 Secondary VLAN 只要在 Primary VLAN 配置相应的三层映射即可。

7.4.2.2 组网拓扑

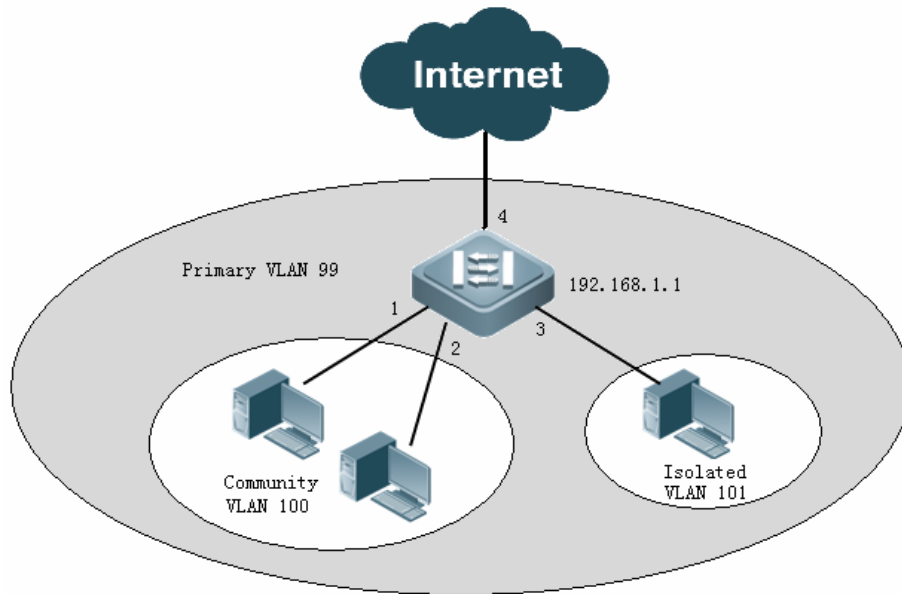


图 7-2

7.4.2.3 配置步骤

类似上一个用例，创建 VLAN 99 为 Primary VLAN，创建 VLAN 100 为 Community VLAN，创建 VLAN 101 为 Isolated VLAN，并关联主次 VLAN。

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#vlan 100
Ruijie(config-vlan)#private-vlan community
Ruijie(config-vlan)#exit
Ruijie(config)#vlan 101
Ruijie(config-vlan)#private-vlan isolated
Ruijie(config-vlan)#exit
Ruijie(config)#vlan 99
Ruijie(config-vlan)#private-vlan primary
Ruijie(config-vlan)#private-vlan association 100,101
Ruijie(config-vlan)#exit
```

配置端口 0 / 1 和 0 / 2 属于 Community VLAN 100，端口 0/3 属于 Isolated VLAN 101，端口 0/4 为 Promiscuous Port。

```
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if)#switchport mode private-vlan host
Ruijie(config-if)#switchport private-vlan host-association 99 100
Ruijie(config-if)#exit
Ruijie(config)#interface gigabitEthernet 0/2
Ruijie(config-if)#switchport mode private-vlan host
Ruijie(config-if)#switchport private-vlan host-association 99 100
Ruijie(config-if)#exit
Ruijie(config)#interface gigabitEthernet 0/3
Ruijie(config-if)#switchport mode private-vlan host
Ruijie(config-if)#switchport private-vlan host-association 99 101
Ruijie(config-if)#exit
Ruijie(config)#interface gigabitEthernet 0/4
Ruijie(config-if)#switchport mode private-vlan promiscuous
Ruijie(config-if)#switchport private-vlan mapping 99 add 100-101
Ruijie(config-if)#exit
```

为 Primary VLAN 配置一个 SVI (192.168.1.1)，以及映射 Secondary VLAN 和 Primary VLAN 的三层接口。

```
Ruijie(config)#interface vlan 99
```

```
Ruijie(config-if)#ip address 192.168.1.1 255.255.255.0
```

```
Ruijie(config-if)#private-vlan mapping 100-101
```

```
Ruijie(config-if)#show vlan private-vlan
```

VLAN	Type	Status	Routed	Ports	Associated VLANs
99	primary	active	Enabled	Gi0/4	100-101
100	community	active	Enabled	Gi0/1, Gi0/2	99
101	isolated	active	Enabled	Gi0/3	99

8 配置 Voice VLAN

8.1 理解Voice VLAN

8.1.1 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：

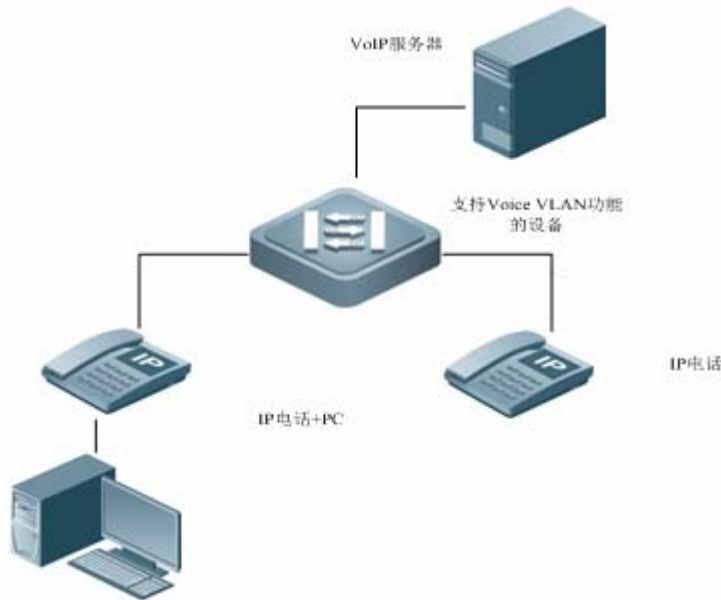


图 8-1Voice VLAN 基本组网图

IP 电话和 Voice VLAN 的连接常用的有 2 种（参见上图）：

- 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 进行数据业务的场合。
- 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

表 1 Voice VLAN 基本组网角色功能表

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。

 说明

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。

8.1.2 Voice VLAN 基本概念

8.1.2.1 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，所发出的报文经支持 Voice VLAN 的设备时，设备通过识别该报文的源 MAC 地址，匹配设备上所配置的 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，并使用老化机制对 Voice VLAN 内的端口进行维护。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。

■ 手动模式

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。用户 IP 电话通讯过程中，设备通过识别报文的源 MAC 地址，匹配设备上所配置的 OUI 地址，OUI 地址匹配成功后，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。

自动模式适用于 PC--IP 电话串联接入端口，可以同时传输语音数据和普通业务数据的组网方式。

手工模式适用于 IP 电话单独接入交换机，端口仅传输语音报文的组网方式，这种组网的方式可以使该端口专用于传输语音数据，避免业务数据对语音数据传输的影响。

8.1.2.2 Voice VLAN 端口与 IP 电话的配合工作

按照是否自动获取 IP 地址与 Voice 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。

IP 电话的工作原理

与其他网络设备一样，IP 电话也需要 IP 地址才能在网络中正常通信。IP 电话获取 IP 地址的方式有两种：

- 通过 DHCP 自动获取。
- 通过用户手工配置。

在自动获取 IP 地址时，IP 电话还可以向 DHCP 服务器同时请求 Voice VLAN 信息，如果 DHCP 服务器返回了 Voice VLAN 信息，IP 电话就可以直接发送携带有 Voice VLAN Tag 的语音流；如果 DHCP 服务器没有返回 Voice VLAN 信息，IP 电话就只能发送不带 VLAN Tag 的语音流。如果 IP 电话支持手动设置 IP 地址和 Voice VLAN 编号，用户也可以在 IP 电话上手工设置 IP 地址，设置 Voice VLAN 信息，IP 电话将根据用户的配置发出 Tagged、Untagged 语音流。

Voice VLAN 端口与发送 Tagged 语音流的 IP 电话

IP 电话发送 Tagged 语音流时，IP 电话必须已经通过自动获取或手工配置的方式得到了 Voice VLAN 信息，这种情况下，不同类型的端口需要进行相应的配置，才能使语音报文能够在 Voice VLAN 中正常传输，同时不影响交换机对普通业务数据的转发处理。与自动获取 Voice VLAN 信息的 IP 电话不同，手工配置 Voice VLAN 的 IP 电话将始终发送、接收带有 Voice VLAN Tag 的语音流。

Voice VLAN 端口与发送 Untagged 语音流的 IP 电话

IP 电话在以下两种情况下会发送、接收 Untagged 语音流：

- 自动获取 IP 地址，但没有获取到 Voice VLAN 信息。
- 手工配置 IP 地址，但没有配置 Voice VLAN 信息。

IP 电话发送 Untagged 语音流的情况下，用户需要配置接收端口的缺省 VLAN 且允许缺省 VLAN 通过，又必须将端口的缺省 VLAN 配置为 Voice VLAN，才能使语音流在 Voice VLAN 中传输，此时端口的 Voice VLAN 工作模式只能为手工模式。

 具体 IP 电话的支持情况、获取 IP 地址和 Voice VLAN 的过程，不同厂商的 IP 电话产品，其工作原理可能与上述的描述不同，具体情况请参见 IP 电话的用户手册。

Voice VLAN 工作模式、IP 电话类型、端口类型能够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
		Private VLAN 主机口	不支持
		Private VLAN 混杂口	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

手动模式	Untagged 语音流	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
		Access Port	不支持
		Private VLAN 主机口	不支持
		Private VLAN 混杂口	不支持
		Trunk Port	不支持
		Hybrid Port	不支持
		Uplink 口	不支持
	Tagged 语音流	Access Port	不支持
		Private VLAN 主机口	不支持
		Private VLAN 混杂口	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
		Private VLAN 主机口	支持, Voice VLAN 必须配置成该端口所对应的 Isolated VLAN 或 Community VLAN
		Private VLAN 混杂口	支持, Voice VLAN 必须配置成 Primary VLAN
		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 VoiceVLAN，且在接入端口允许通过的 untagged VLAN 列表中
	Uplink 口	不支持

表 2 端口模式与 IP 电话语音流类型匹配关系表

 注意	1) Voice VLAN 与接入控制的 802.1x、Web 认证功能共用时，需要配置安全通道，将 Voice VLAN 对应的 OUI 地址设为允许通过的报文，从而使得 VoIP 电话无需认证即可通信。 2) 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。 3) 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。 4) 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。

8.1.2.3 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，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。

 说明	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。
 注意	1) 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。

8.1.3 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。

8.1.4 协议规范

无

8.2 Voice VLAN的缺省配置

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

8.3 配置Voice VLAN基本特性

8.3.1 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
Step 1	Ruijie# configure terminal	进入全局配置模式。
Step 2	Ruijie(config)# vlan vlan-id	创建 Voice VLAN。
Step 3	Ruijie(config-vlan)# exit	退出 VLAN 配置模式。
Step 4	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
```

说明

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。

注意

- 1) 配置 Voice VLAN 之前，须先创建对应的 VLAN。
- 2) VLAN 1 是默认 VLAN，无需创建，但 VLAN 1 不能被设置为 Voice VLAN。
- 3) 不允许将某个 VLAN 同时设置为 Voice VLAN 与 Super VLAN。
- 4) 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。
- 5) 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。

8.3.2 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
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，可使能 Voice VLAN 的端口为物理端口。
Step 3	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
```

说明

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。

注意

- 1) Voice VLAN 仅支持二层物理口（Access Port/Trunk Port/Hybrid Port/Uplink Port/Private VLAN 端口等），不支持在 AP 口与 Routed Port 上打开 Voice VLAN 功能。
- 2) 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。

8.3.3 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
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)# 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
```

说明

- 1) 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。
- 2) 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。

注意

- 1) 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。
- 2) 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。
- 3) 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。

8.3.4 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
Step 1	Ruijie# configure terminal	进入全局配置模式。
Step 2	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
```

8.3.5 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
Step 1	Ruijie# configure terminal	进入全局配置模式。
Step 2	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
Step 2	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
```

说明

Voice VLAN OUI 地址不能是组播地址，所配置的掩码需连续。

8.3.6 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
Step 1	Ruijie# configure terminal	进入全局配置模式。
Step 2	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
```

8.3.7 配置Voice VLAN的语音流优先级

设备通过修改 Voice VLAN 的语音流的 CoS 与 DSCP 值来提高语音流的优先级，保证通话质量。关于 CoS 与 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
Step 1	Ruijie# configure terminal	进入全局配置模式。
Step 2	Ruijie(config)# voice vlan cos cos-value	设置 Voice VLAN 语音流的 CoS 值。 缺省情况下，CoS 为 6。
Step 3	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 CoS 与 DSCP 值恢复为缺省值，可使用 **no voice vlan cos** 或 **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，CoS 为 5，DSCP 为 40。

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# voice vlan cos 5
Ruijie(config)# voice vlan dscp 40
```

8.3.8 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。

8.4 Voice VLAN典型配置举例

8.4.1 Voice VLAN自动模式配置举例

8.4.1.1 组网需求

假设 Voice VLAN 自动模式配置有以下需求：

- 1) Voice VLAN 为 VLAN 2，端口老化时间为 1000 分钟，为保证通话质量，需要将语音数据在专用的 Voice VLAN 中传输，并且这个 Voice VLAN 中不能传输非语音数据。
- 2) 部署的 IP 电话支持自动获取 IP 地址和 Voice VLAN 信息，发送 Tagged 的语音流，MAC 地址为 0012.3456.7890，OUI 地址为 0012.3400.0000。

3) 接入端口 Fa0/1 下连的 PC 需要使用 802.1x 认证。

8.4.1.2 组网拓扑

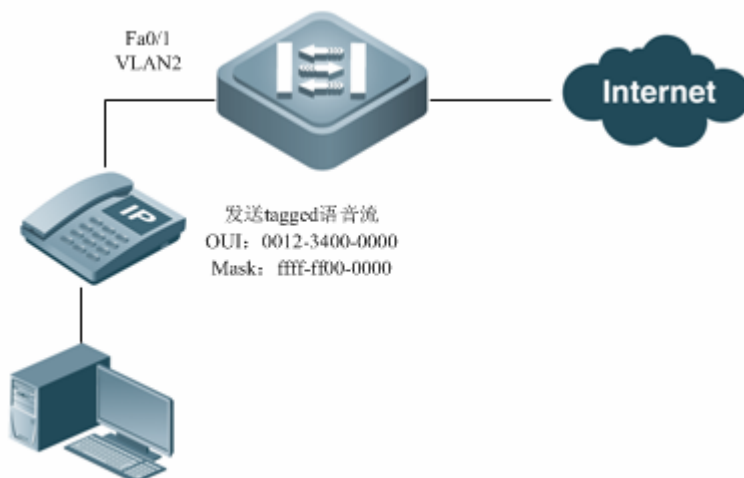


图 8-2 Voice VLAN 自动模式配置组网图

8.4.1.3 配置要点

Fa 0/1 接入的是自动获取 IP 地址的 IP 电话，IP 电话在 Voice Vlan 内获取 IP 地址以后，就可以正常使用了。组网要求 Fa 0/1 端口同时转发并且隔离语音流和数据流，端口可配置为 Trunk 口，Native Vlan 转发数据流，Voice Vlan 转发语音流。

PC 发出的是 Untagged 的报文，因此会在端口的 Native VLAN 内传输，我们将 Native Vlan 设置为 5，用来传输 PC 发出的数据流。

PC 使用 802.1X 认证，接入端口 Fa 0/1 需打开 802.1x 功能，我们希望 PC 使用网络通过 1x 认证，而 IP 电话不受影响，此时需手动配置安全通道命令，将 Voice Vlan 对应的 OUI 地址设为允许通过的报文，使得 IP 电话可以绕过接入控制的检查，使符合 Voice Vlan OUI 设置的 IP 电话无需认证即可使用 Voice Vlan 通信。

组网要求隔离语音流和数据流，当配置端口为 Trunk Port，Voice VLAN 模式为自动模式时，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，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(VLAN 2)从 Fa0/1 的 VLAN 许可列表中移出。

8.4.1.4 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。

配置专家级 ACL, 允许 OUI 地址通过

```
Ruijie(config)# expert access-list extended safe_channel
```

```
Ruijie(config-exp-nacl)# permit ip any 0012.3400.0000 0000.00ff.ffff any any
```

配置安全通道

```
Ruijie(config)# security global access-group safe_channel
```

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

8.4.1.5 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: 1000minutes
```

```
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
```

```
0012.3400.0000 ffff.ff00.0000
```

8.4.2 Voice VLAN手动模式配置举例

8.4.2.1 组网需求

- 1) Voice VLAN 为 VLAN 2，为保证通话质量，需要将语音数据在专用的 Voice VLAN 中传输，并且这个 Voice VLAN 中不能传输非语音数据。
- 2) 部署的 IP 电话，自动获取 IP 地址，发送 Untagged 语音流，MAC 地址为 0012.3456.7890，OUI 地址为 0012.3400.0000，掩码是 ffff.ff00.0000。

8.4.2.2 组网拓扑

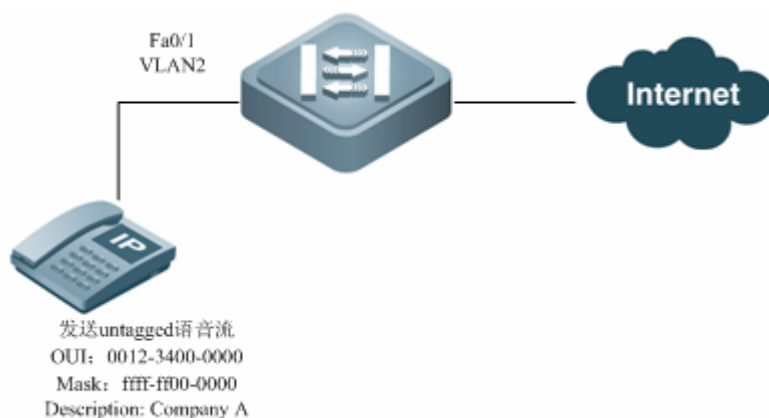


图 1 Voice VLAN 自动模式配置组网图

8.4.2.3 配置要点

由于 Fa0/1 下连的是发出 Untagged 的语音流 IP 电话，而且只有语音流，由于不带 Tag 的语音流不支持自动模式，所以端口只能配置为手动模式，同时配置 Fa0/1 为 Hybrid Port，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。

8.4.2.4 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 Ruijie。

设置 Voice VLAN OUI 地址

```
Ruijie(config)# voice vlan mac-address 0012.3400.0000 mask ffff.ff00.0000
description Company A
```

- 4) 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, 工作于手动模式
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# no voice vlan mode auto
Ruijie(config-if)# voice vlan enable

```

8.4.2.5 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
0012.3400.0000   ffff.ff00.0000   Company A

```

9 配置 MSTP

9.1 MSTP概述

9.1.1 STP、RSTP

9.1.1.1 STP、RSTP 总述

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扑结构。

- 发现故障并随之进行恢复，自动更新网络拓扑结构，使在任何时候都选择了可能的最佳树型结构。

局域网的拓扑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扑树。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，一旦网络拓扑改变而要重新生成拓扑树只需要不超过 1 秒的时间（传统的 STP 需要大约 50 秒）。

9.1.1.2 Bridge Protocol Data Units(简称为BPDU)：

要生成一个稳定的树型拓扑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扑结构所需要的信息。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扑变化、本端口状态的标志位。

当网桥的一个端口收到高优先级的 BPDUs（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 BPDUs，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—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

9.1.1.3 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

9.1.1.4 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 BPDUs 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。

9.1.1.5 Port Roles and Port States

每个端口都在网络中有扮演一个角色（Port Role），用来体现在网络拓扑中的不同作用。

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。

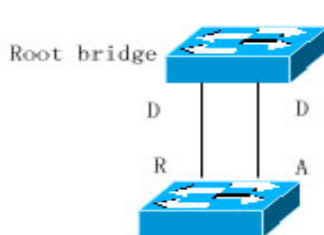


图 9-1

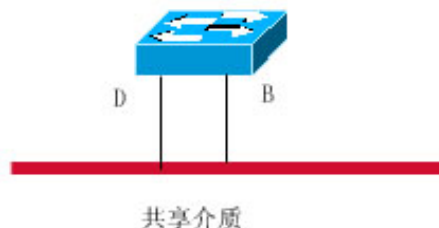


图 9-2

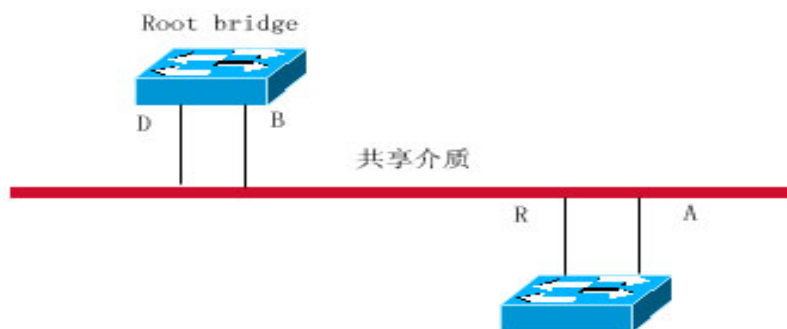


图 9-3

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扑结构。

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扑，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。

9.1.1.6 网络拓扑树的生成（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路拓扑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 间为百兆链路，B 和 C 间为十兆链路。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。

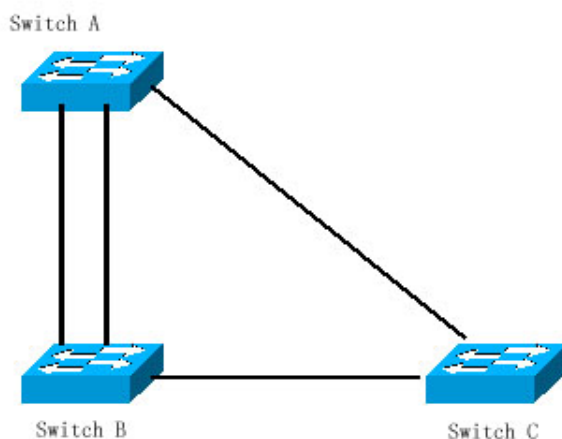


图 9-4

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。

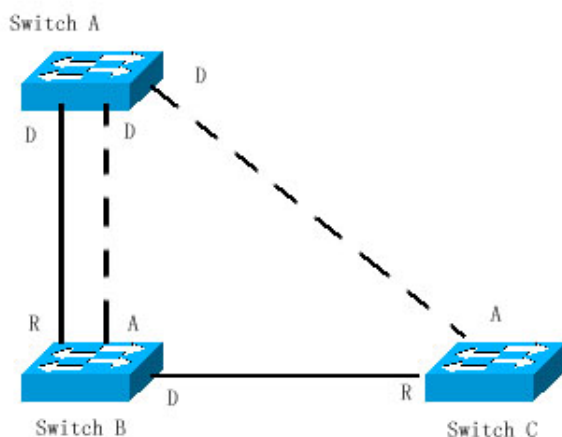


图 9-5

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。

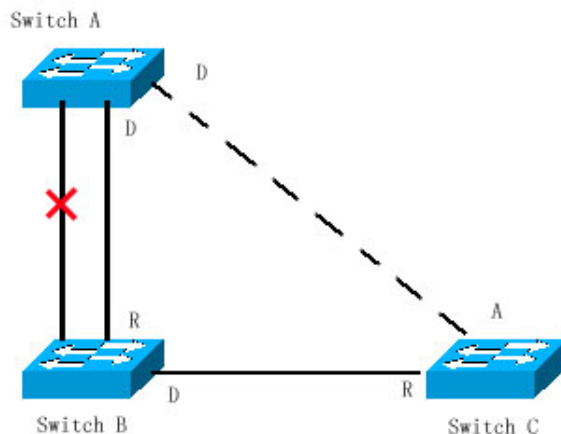


图 9-6

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。

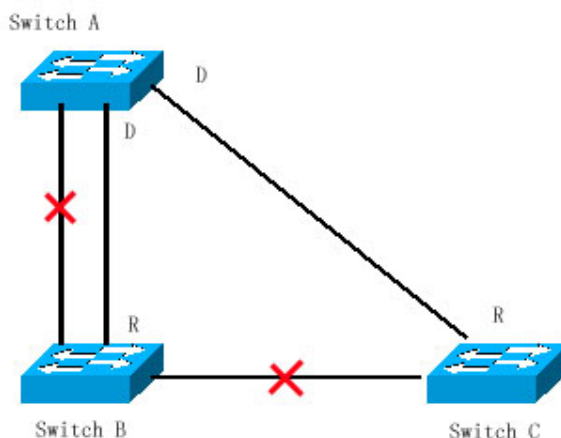


图 9-7

9.1.1.7 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, 而且每当拓扑发生变化后, 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扑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 是能够在网络拓扑发生变化的一瞬间恢复网络树型结构, 达到快速收敛。

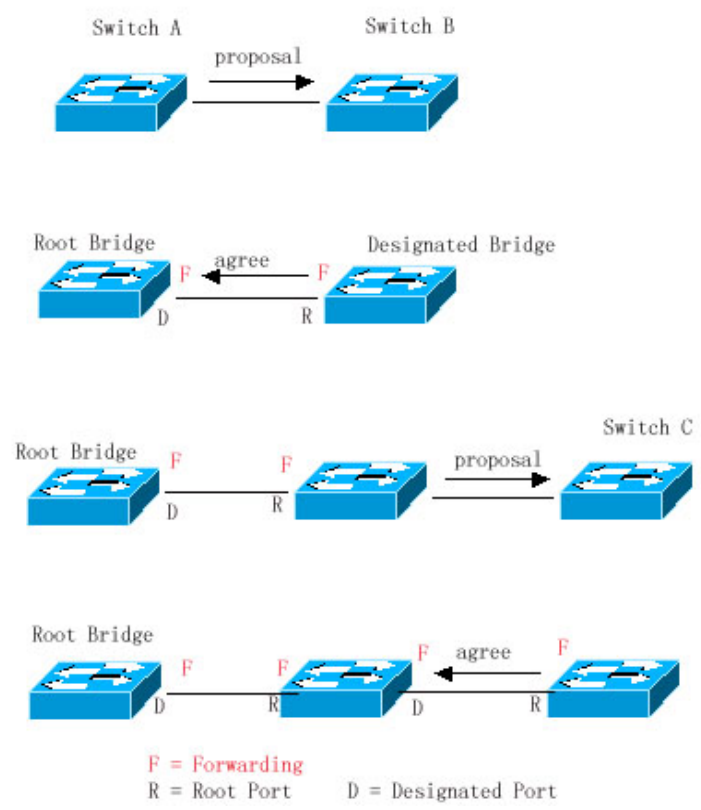


图 9-8

注意

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：

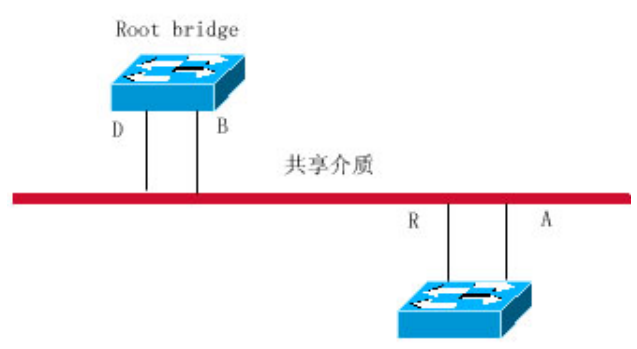


图 9-9

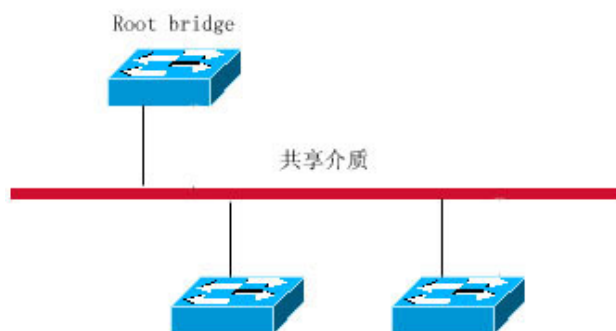


图 9-10

另外、下图为“点对点”连接，请用户注意区分

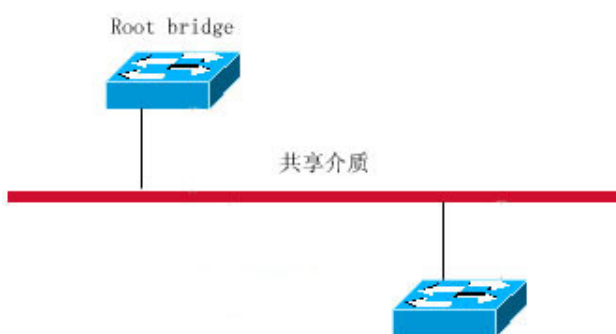


图 9-11

9.1.1.8 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。

Protocol Migration

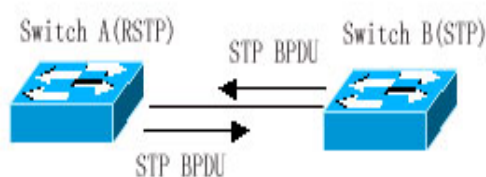


图 9-12

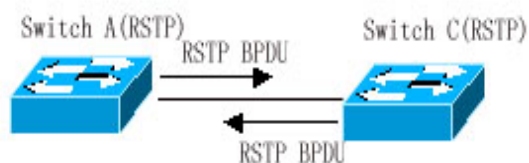


图 9-13

9.1.2 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，因此在特定网络拓扑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。

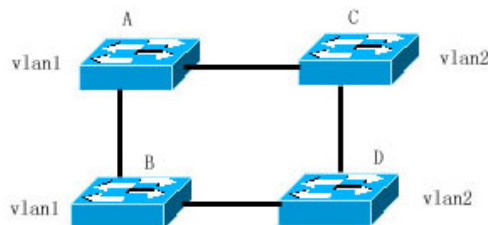


图 9-14

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。

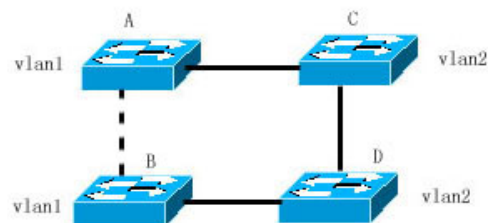


图 9-15

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 的拓扑：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。

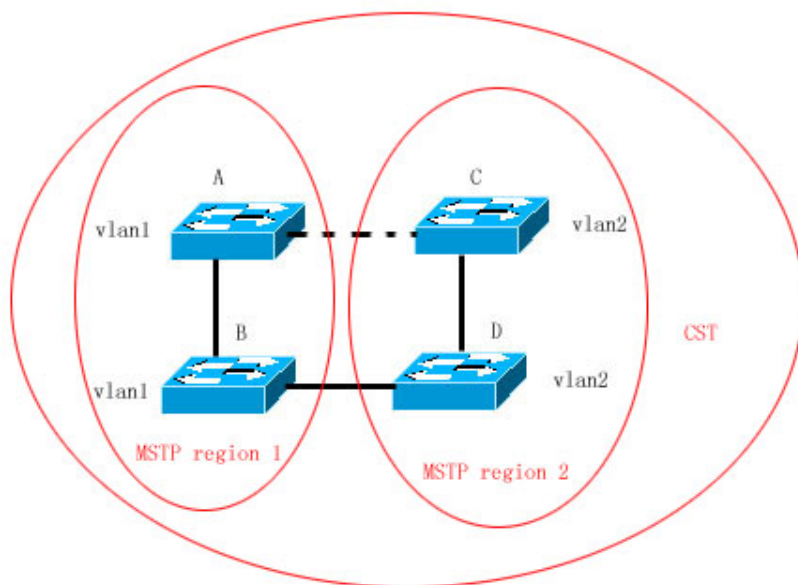


图 9-16

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。

9.1.2.1 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。

说明

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，以保证网络拓扑的稳定和收敛。

9.1.2.2 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 CIST 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、不含环路的网络拓扑。

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。

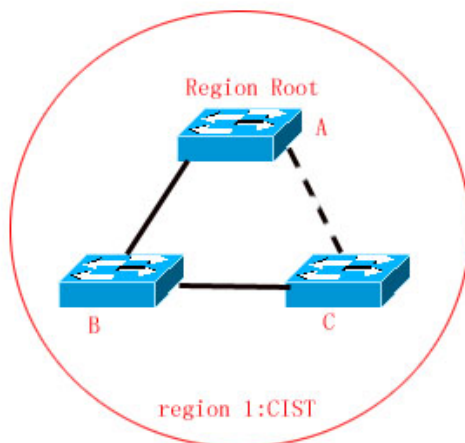


图 9-17

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。

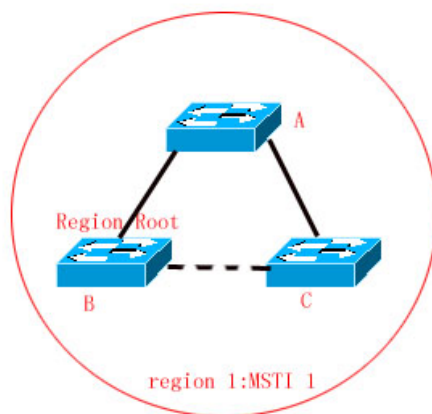


图 9-18

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。

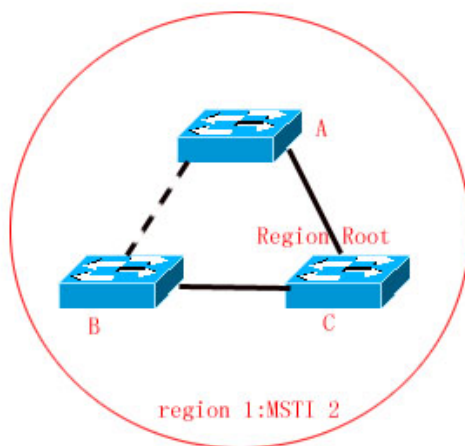


图 9-19

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。

9.1.2.3 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扑树，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。1

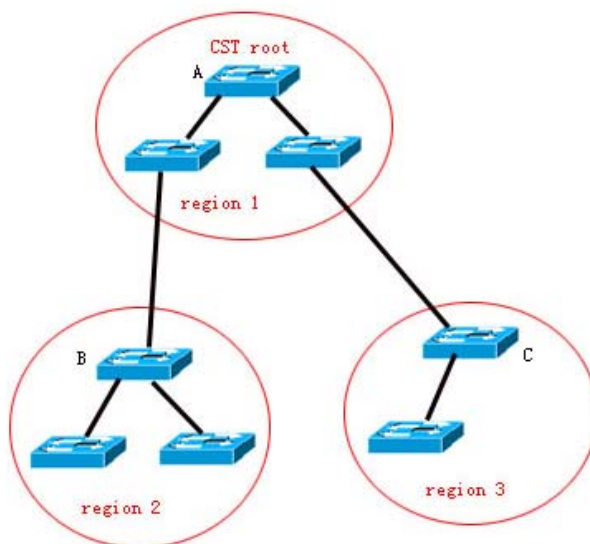


图 9-20

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。为了使拓扑更稳定，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！

9.1.2.4 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。

9.1.2.5 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。

9.2 MSTP可选特性概述

9.2.1 理解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。

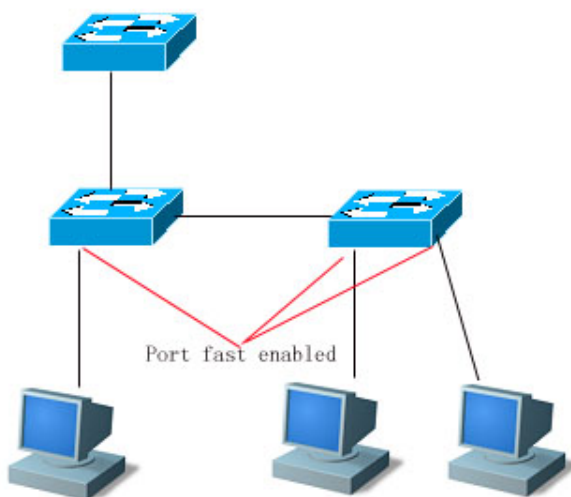


图 9-21

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。

9.2.2 理解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, 使网络拓扑发生改变。

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。

9.2.3 理解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 bpdupfilter 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 bpdupfilter 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。

9.2.4 理解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。

9.2.5 理解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。

注意

- 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。

理解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。

**注意**

TC 过滤功能缺省关闭。

9.2.6 理解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。

9.2.7 理解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。

9.2.8 理解边缘口的自动识别

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。

**注意**

- 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。

9.2.9 理解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）。

注意

- 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。

9.2.10 理解 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。

注意

- 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。

9.3 配置 MSTP

9.3.1 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)。

9.3.2 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
Step 1	Ruijie# configure terminal	进入全局配置模式。
Step 2	Ruijie(config)# spanning-tree	打开 Spanning Tree 协议。
Step 3	Ruijie(config)# end	退回到特权模式。
Step 4	Ruijie# show spanning-tree	核对配置条目。
Step 5	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。

9.3.3 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。



注意

从 MSTP 模式切换到 RSTP 或 STP 模式时，有关 MSTP Region 的所有信息将被清空。

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
Step 1	Ruijie# configure terminal	进入全局配置模式。
Step 2	Ruijie(config)# spanning-tree mode mstp / rstp / stp	切换 Spanning Tree 模式。
Step 3	Ruijie(config)# end	退回到特权模式。
Step 4	Ruijie# show spanning-tree	核对配置条目。
Step 5	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。

9.3.4 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扑结构。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
Step 1	Ruijie# configure terminal	进入全局配置模式。
Step 2	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。 <i>instance-id</i> ，范围为 0—64 <i>priority</i> ，取值范围为 0 到 61440，按 4096 的倍数递增，缺省值为 32768。
Step 3	Ruijie(config)# end	退回到特权模式。
Step 4	Ruijie# show running-config	核对配置条目。
Step 5	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。

9.3.5 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，设备会选择了一个高优先级（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
Step 1	Ruijie# configure terminal	进入全局配置模式。
Step 2	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。
Step 3	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。 <i>instance-id</i> ，范围为 0—64 <i>priority</i> ，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
Step 4	Ruijie(config-if)# end	退回到特权模式。

Step 5	Ruijie# show spanning-tree [mst instance-id] interface interface-id	核对配置条目。
Step 6	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。

9.3.6 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
Step 1	Ruijie# configure terminal	进入全局配置模式。
Step 2	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。
Step 3	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。 <i>instance-id</i> ，范围为 0—64 <i>cost</i> ，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。
Step 4	Ruijie(config-if)# end	退回到特权模式。
Step 5	Ruijie# show spanning-tree [mst instance-id] interface interface-id	核对配置条目。
Step 6	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。

9.3.7 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 和 IEEE 802.1t 对相同的链路速率规定了不同 Path Cost 值，802.1d 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)。请管理员一定要统一好整个网络内 Path Cost 的标准。缺省模式为长整型模式 (IEEE 802.1t 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)
10M	普通端口	100	2000000
	Aggregate Link	95	1900000
100M	普通端口	19	200000
	Aggregate Link	18	190000

1000M	普通端口	4	20000
	Aggregate Link	3	19000

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
Step 1	Ruijie# configure terminal	进入全局配置模式。
Step 2	Ruijie(config)# spanning-tree pathcost method long/short	配置端口路径花费的缺省计算方法，设置值为长整型（long）或短整型（short），缺省值为长整型（long）。
Step 3	Ruijie(config)# end	退回到特权模式。
Step 4	Ruijie# show running-config	核对配置条目。
Step 5	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。

9.3.8 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
Step 1	Ruijie# configure terminal	进入全局配置模式。
Step 2	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。
Step 3	Ruijie(config)# end	退回到特权模式。
Step 4	Ruijie# show running-config	核对配置条目。
Step 5	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。

9.3.9 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
Step 1	Ruijie# configure terminal	进入全局配置模式。
Step 2	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。
Step 3	Ruijie(config)# end	退回到特权模式。
Step 4	Ruijie# show running-config	核对配置条目。
Step 5	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。

9.3.10 配置Max-Age Time

	命令	作用
Step 1	Ruijie# configure terminal	进入全局配置模式。
Step 2	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。
Step 3	Ruijie(config)# end	退回到特权模式。
Step 4	Ruijie# show running-config	核对配置条目。
Step 5	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： $2 * (\text{Hello Time} + 1.0 \text{ seconds}) \leq \text{Max-Age Time} \leq 2 * (\text{Forward-Delay} - 1.0 \text{ seconds})$ 。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。

9.3.11 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
Step 1	Ruijie# configure terminal	进入全局配置模式。
Step 2	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。
Step 3	Ruijie(config)# end	退回到特权模式。
Step 4	Ruijie# show running-config	核对配置条目。
Step 5	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。

9.3.12 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
Step 1	Ruijie# configure terminal	进入全局配置模式。
Step 2	Ruijie(config)# interface interface-id	进入接口配置模式

Step 3	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。
Step 4	Ruijie(config-if)# end	退回到特权模式。
Step 5	Ruijie# show running-config	核对配置条目。
Step 6	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。

9.3.13 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
Step 1	Ruijie# clear spanning-tree detected-protocols	对所有端口强制版本检查
Step 2	Ruijie# clear spanning-tree detected-protocols interface interface-id	针对一个端口进行版本检查

9.3.14 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，以保证网络拓扑的稳定和收敛。

进入特权模式，按以下步骤配置 MSTP Region：

	命令	作用
Step 1	Ruijie# configure terminal	进入全局配置模式。
Step 2	Ruijie(config)# spanning-tree mst configuration	进入 MST 配置模式。
Step 3	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。
Step 4	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。

Step 5	Ruijie(config-mst)# revision version	指定 MST revision number，范围为 0—65535。缺省值为 0
Step 6	Ruijie(config-mst)# show	核对 MST 的配置条目。
Step 7	Ruijie(config-mst)# end	退回到特权模式。
Step 8	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。您也可以使用 **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
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)#
```



注意

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。

9.3.15 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
Step 1	Ruijie# configure terminal	进入全局配置模式。
Step 2	Ruijie(config)# spanning-tree max-hops hop-count	配置 Maximum-Hop Count，范围为 1—40，缺省值为 20
Step 3	Ruijie(config)# end	退回到特权模式。
Step 4	Ruijie# show running-config	核对配置条目。
Step 5	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。

9.3.16 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，按以下步骤配置接口的兼容性模式：

	命令	作用
Step 1	Ruijie# configure terminal	进入全局配置模式。
Step 2	Ruijie(config)# interface interface-id	进入接口配置模式
Step 3	Ruijie(config-if)# spanning-tree compatible enable	打开接口的兼容性模式
Step 4	Ruijie(config-if)# end	退回到特权模式。
Step 5	Ruijie# show running-config	核对配置条目。
Step 6	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。

9.3.17 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
Step 1	Ruijie# clear spanning-tree counters	清除所有端口的收发包统计信息
Step 2	Ruijie# clear spanning-tree counters interface interface-id	清除指定端口的收发包统计信息
Step 3	Ruijie# show spanning-tree counters	显示 STP 端口的收发包统计信息

9.4 配置MSTP可选特性

9.4.1 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外缺省都是关闭的。

9.4.2 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
Step 1	Ruijie# configure terminal	进入全局配置模式。
Step 2	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。
Step 3	Ruijie(config-if)# spanning-tree portfast	打开该 interface 的 portfast。
Step 4	Ruijie(config-if)# end	退回到特权模式。
Step 5	Ruijie# show spanning-tree interface interface-id portfast	核对配置条目。

Step 6	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。

9.4.3 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
Step 1	Ruijie# configure terminal	进入全局配置模式。
Step 2	Ruijie(config)# spanning-tree portfast bpduguard default	全局的打开 BPDU guard
Step 3	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。
Step 4	Ruijie(config-if)# spanning-tree portfast	打开该 interface 的 portfast。全局的 BPDU guard 配置才生效。
Step 5	Ruijie(config-if)# end	退回到特权模式。
Step 6	Ruijie# show running-config	核对配置条目。
Step 7	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。

9.4.4 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
Step 1	Ruijie# configure terminal	进入全局配置模式。
Step 2	Ruijie(config)# spanning-tree portfast bpduguard default	全局的打开 BPDU filter
Step 3	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。
Step 4	Ruijie(config-if)# spanning-tree portfast	打开该 interface 的 portfast。全局的 BPDU filter 配置才生效。
Step 5	Ruijie(config-if)# end	退回到特权模式。
Step 6	Ruijie# show running-config	核对配置条目。
Step 7	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。

9.4.5 打开Tc_Protection

进入特权模式，按以下步骤配置 Tc_Protection：

	命令	作用
Step 1	Ruijie# configure terminal	进入全局配置模式。
Step 2	Ruijie(config)# spanning-tree tc-protection	打开 tc-protection
Step 3	Ruijie(config)# end	退回到特权模式。
Step 4	Ruijie# show running-config	核对配置条目。
Step 5	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。

9.4.6 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
Step 1	Ruijie# configure terminal	进入全局配置模式。
Step 2	Ruijie(config)# spanning-tree tc-protection tc-guard	打开全局的 TC Guard
Step 3	Ruijie(config)# end	退回到特权模式。
Step 4	Ruijie# show running-config	核对配置条目。
Step 5	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
Step 1	Ruijie# configure terminal	进入全局配置模式。
Step 2	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。
Step 3	Ruijie(config-if)# spanning-tree tc-guard	打开该 interface 的 TC Guard。
Step 4	Ruijie(config-if)# end	退回到特权模式。
Step 5	Ruijie# show running-config	核对配置条目。
Step 6	Ruijie# copy running-config startup-config	保存配置。

9.4.7 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
Step 1	Ruijie# configure terminal	进入全局配置模式
Step 2	Ruijie(config)# interface <i>Interface-id</i>	进入该 interface 的配置模式，合法的 interface 包括物理端口和 Aggregate Link
Step 3	Ruijie(config-if)# spanning-tree ignore tc	打开该 interface 的 TC 过滤
Step 4	Ruijie(config-if)# end	退回到特权模式
Step 5	Ruijie# show running-config	核对配置条目
Step 6	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。

9.4.8 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
Step 1	Ruijie# configure terminal	进入全局配置模式。
Step 2	Ruijie(config)# interface <i>Interface-id</i>	进入该 interface 的配置模式，合法的 interface 包括物理端口和 Aggregate Link。
Step 3	Ruijie(config-if)# bpdu src-mac-check <i>H.H.H</i>	打开 bpdu 源 mac 检查。
Step 4	Ruijie(config-if)# end	退回到特权模式。
Step 5	Ruijie# show running-config	核对配置条目。
Step 6	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。

9.4.9 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
Step 1	Ruijie# configure terminal	进入全局配置模式。
Step 2	Ruijie(config)# interface <i>interface-id</i>	进入该 interface 的配置模式，合法的 interface 包括物理端口和 Aggregate Link。
Step 3	Ruijie(config-if)# spanning-tree autoedge	打开该 interface 的 autoedge。
Step 4	Ruijie(config-if)# end	退回到特权模式。
Step 5	Ruijie# show spanning-tree interface <i>interface-id</i>	核对配置条目。

Step 6	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。

9.4.10 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
Step 1	Ruijie# configure terminal	进入全局配置模式。
Step 2	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。
Step 3	Ruijie(config-if)# spanning-tree guard root	打开接口的 ROOT Guard 特性
Step 4	Ruijie(config-if)# end	退回到特权模式。
Step 5	Ruijie# show running-config	核对配置条目。
Step 6	Ruijie# copy running-config startup-config	保存配置。

9.4.11 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
Step 1	Ruijie# configure terminal	进入全局配置模式。
Step 2	Ruijie(config)# spanning-tree Loopguard default	打开全局的 LOOP Guard。
Step 3	Ruijie(config)# end	退回到特权模式。
Step 4	Ruijie# show running-config	核对配置条目。
Step 5	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
Step 1	Ruijie# configure terminal	进入全局配置模式。
Step 2	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。
Step 3	Ruijie(config-if)# spanning-tree guard loop	打开该 interface 的 Loop Guard。
Step 4	Ruijie(config-if)# end	退回到特权模式。
Step 5	Ruijie# show running-config	核对配置条目。
Step 6	Ruijie# copy running-config startup-config	保存配置。

9.4.12 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
Step 1	Ruijie# configure terminal	进入全局配置模式。
Step 2	Ruijie(config)# interface <i>Interface-id</i>	进入该 interface 的配置模式，合法的 interface 包括物理端口和 Aggregate Link。
Step 3	Ruijie(config-if)# spanning-tree guard none	关闭接口的 guard 功能
Step 4	Ruijie(config-if)# end	退回到特权模式。
Step 5	Ruijie# show running-config	核对配置条目。
Step 6	Ruijie# copy running-config startup-config	保存配置。

9.5 显示MSTP配置和状态

MSTP 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
Step 1	Ruijie# show spanning-tree	显示 MSTP 的各项参数信息及生成树的拓扑信息
Step 2	Ruijie# show spanning-tree summary	显示 MSTP 的各 instance 的信息及其端口转发状态信息
Step 3	Ruijie# show spanning-tree inconsistentports	显示因根保护或环路保护而 block 的端口
Step 4	Ruijie# show spanning-tree mst configuration	显示 MST 域的配置信息
Step 5	Ruijie# show spanning-tree mst <i>instance-id</i>	显示该 instance 的 MSTP 信息
Step 6	Ruijie# show spanning-tree mst <i>instance-id</i> interface <i>interface-id</i>	显示指定 interface 的对应 instance 的 MSTP 信息
Step 7	Ruijie# show spanning-tree interface <i>interface-id</i>	显示指定 interface 的所有 instance 的 MSTP 信息
Step 8	Ruijie# show spanning-tree forward-time	显示 forward-time
Step 9	Ruijie# show spanning-tree Hello time	显示 Hello time
Step10	Ruijie# show spanning-tree max-hops	显示 max-hops
Step11	Ruijie# show spanning-tree tx-hold-count	显示 tx-hold-count
Step12	Ruijie# show spanning-tree pathcost method	显示 pathcost method
Step13	Ruijie# show spanning-tree counters [interface <i>interface-id</i>]	显示 STP 的收发包统计信息

10 配置协议帧透传

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。

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
保留组播协议帧透传	开启
PVST 协议帧透传	开启

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
Step 1	Ruijie# configure	进入全局配置模式

Step 2	Ruijie(config)# bridge-frame forwarding protocol bpdu	开启 BPDU 协议帧透传功能
Step 3	Ruijie(config-if)# end	退回到特权模式

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
Step 1	Ruijie# configure	进入全局配置模式
Step 2	Ruijie(config)# bridge-frame forwarding protocol gvrp	开启 GVRP 协议帧透传功能
Step 3	Ruijie(config-if)# end	退回到特权模式

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
Step 1	Ruijie# configure	进入全局配置模式
Step 2	Ruijie(config)# bridge-frame forwarding protocol 802.1x	开启 802.1X 协议帧透传功能
Step 3	Ruijie(config-if)# end	退回到特权模式

保留组播协议帧透传配置

在全局配置模式下，执行如下命令可以在设备上开启保留组播协议帧透传功能：

	命令	作用
Step 1	Ruijie# configure	进入全局配置模式
Step 2	Ruijie(config)# bridge-frame forwarding protocol reserved-multicast	开启保留组播协议帧透传功能
Step 3	Ruijie(config-if)# end	退回到特权模式

PVST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 CISCO PVST 协议帧透传功能：

	命令	作用
Step 1	Ruijie# configure	进入全局配置模式
Step 2	Ruijie(config)# bridge-frame forwarding protocol cisco-pvst	开启 CISCO PVST 协议帧透传功能
Step 3	Ruijie(config-if)# end	退回到特权模式

配置举例

配置举例

10.1.1.1 组网拓扑

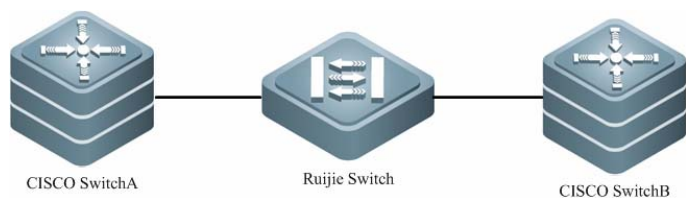


图 10-1 PVST 协议透传简单配置

10.1.1.2 配置要点

在该拓扑环境中，锐捷交换设备同 CISCO 设备一同使用，而 CISCO 产品开启了自己的私有 STP 协议（即 PVST 协议），而在锐捷交换设备上开启了组播功能，要保证 CISCO 的私有协议报文可以正常运行。

10.1.1.3 配置步骤

在 Ruijie Switch 上配置 PVST 协议帧透传配置

```
SwitchA# configure terminal
SwitchA(config)# bridge-frame forwarding protocol cisco-pvst
SwitchA(config)# end
```

11 配置 GVRP

11.1 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。通过在网内自动通告 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

11.2 配置 GVRP

11.2.1 GVRP 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

11.2.2 GVRP 配置指导

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。

11.2.3 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
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# gvrp enable
Ruijie(config)# end
```

11.2.4 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 dynamic-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
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# gvrp dynamic-vlan-creation enable
Ruijie(config)# end
```

11.2.5 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。

11.2.6 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
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
```

11.2.7 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
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
```

11.2.8 设置GVRP定时器

GVRP 中使用了三个定时器:

1. 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。

2. 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。

3. 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 ($\text{Leave} \geq \text{Join} * 3$)，同时 Leaveall 必须大于 Leave ($\text{Leaveall} > \text{Leave}$)。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。

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
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# gvrp timer join 1000
Ruijie(config)# end
```

11.3 显示GVRP的配置和状态

11.3.1 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

清除端口上 GVRP 统计值的示例：

```
Ruijie# clear gvrp statistics gigabitethernet 1/1
```

11.3.2 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

```

11.3.3 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
```

12 配置 LLDP

12.1 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。

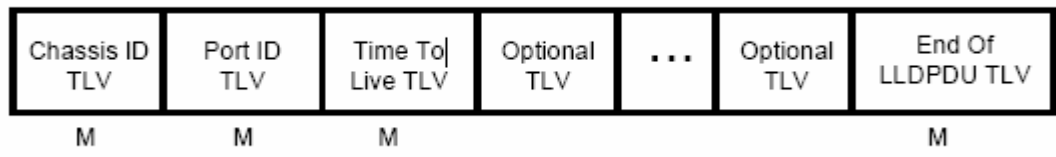
通过 LLDP，网络管理系统可以掌握拓扑的连接情况，比如设备的哪些端口与其它设备相连接，链路连接两端的端口的速率、双工是否匹配等，管理员可以根据这些信息快速地定位及排查故障。

12.1.1 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 12-1 LLDPDU 格式



其中：

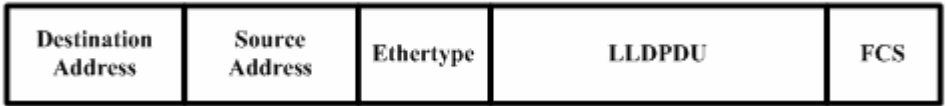
- M 表示是固定的 TLV。
- 在 LLDPDU 中，Chassis ID TLV、Port ID TLV、Time To Live TLV 和 End Of LLDPDU TLV 是必须携带的，而其它类型的 TLV 是可选携带。

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 12-2 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 12-3 SNAP 格式封装的 LLDP 报文

Destination Address	Source Address	SNAP-encoded Ethertype	LLDPDU	FCS

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。

1) 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。

2) 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：

3) 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。

4) 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。

5) 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。

12.1.2 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。

12.1.3 协议规范

LLDP 相关的协议规范和标准有：

- IEEE 802.1AB 2005: Station and Media Access Control Connectivity Discovery
- ANSI/TIA-1057: Link Layer Discovery Protocol for Media Endpoint Devices

12.2 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

12.2.1 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

12.2.2 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
```

12.2.3 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在工作模式修改为 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
```

12.2.4 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 <i>interface-name</i>	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 [<i>vlan-id</i>] vlan-name [<i>vlan-id</i>] } dot3-tlv { all link-aggregation mac-physic max-frame-size power } med-tlv { all capability inventory location { civic-location elin } identifier <i>id</i> network-policy profile [<i>profile-num</i>] power-over-ethernet } }	缺省情况下，端口上不允许发布 IEEE 802.3 TLV 及 LLDP-MED TLV。
Ruijie(config-if)# show lldp tlv-config interface <i>interface-name</i>	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 LLDP-MED TLV 时，必须配置允许发布 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，由 IP 电话修改语音流 tag 和 QOS，此时可以不用 **voice vlan** 功能，但需要把连接 IP 电话的端口配置为 QOS 信任口；若 IP 电话不支持 LLDP-MED，则必须配置 **voice vlan**，并将话机 MAC 地址手动配置到 **voice vlan OUI** 列表中

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

12.2.5 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 <i>interface-name</i>	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 <i>[ip-address]</i>	配置 LLDP 报文中发布的管理地址
Ruijie(config-if)# show lldp local-information interface <i>interface-name</i>	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
```

12.2.6 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
```

12.2.7 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

```

12.2.8 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

```

12.2.9 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

```

12.2.10 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 <i>interface-name</i>	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 <i>interface-name</i>	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

```

12.2.11 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 <i>interface-name</i>	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
```

12.2.12 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。

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
```

12.2.13 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
```

12.2.14 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
```

12.2.15 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。

12.3 LLDP典型配置举例

12.3.1 利用LLDP查看拓扑连接情况

组网需求

■ 设备需求

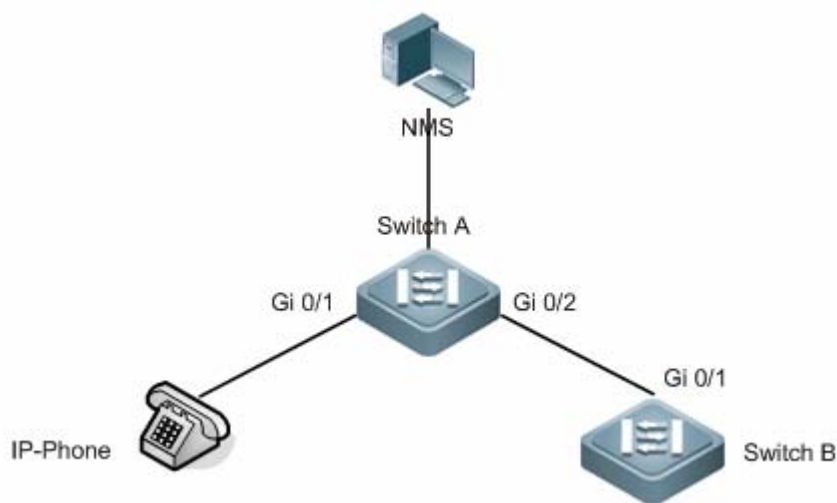
以太网交换机二台（分别以 Switch A 和 Switch B 表示）、MED 设备一台（以 IP Phone 为例）、NMS（Network Management System，网络管理系统）一台。

■ 配置需求

LLDP 功能默认打开，不需要再行配置。

组网拓扑

图 12-4 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   :

```

12.3.2 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 12-5 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。

13 配置 QinQ

13.1 QinQ概述

对于 QinQ, 业界有多种不同的称呼, 比如 dot1q-tunneling、Tag in Tag、VLAN VPN、Stack VLAN, 其标准出自 IEEE 802.1ad。它的出现主要是因为: IEEE 802.1Q 中定义的 VLAN Tag 域只有 12 个比特用于表示 VLAN ID, 所以设备最多可以支持 4094 个 VLAN。在实际应用中, 尤其是在城域网中, 需要大量的 VLAN 来隔离用户, 4094 个 VLAN 远远不能满足需求。它实现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 (即服务提供商网络的 VLAN Tag) 传播, 当用户报文离开服务提供商网络时, 剥去公服务提供商网络的 VLAN Tag, 报文在用户网络中, 根据私网 VLAN Tag 传播。

如图 1 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。

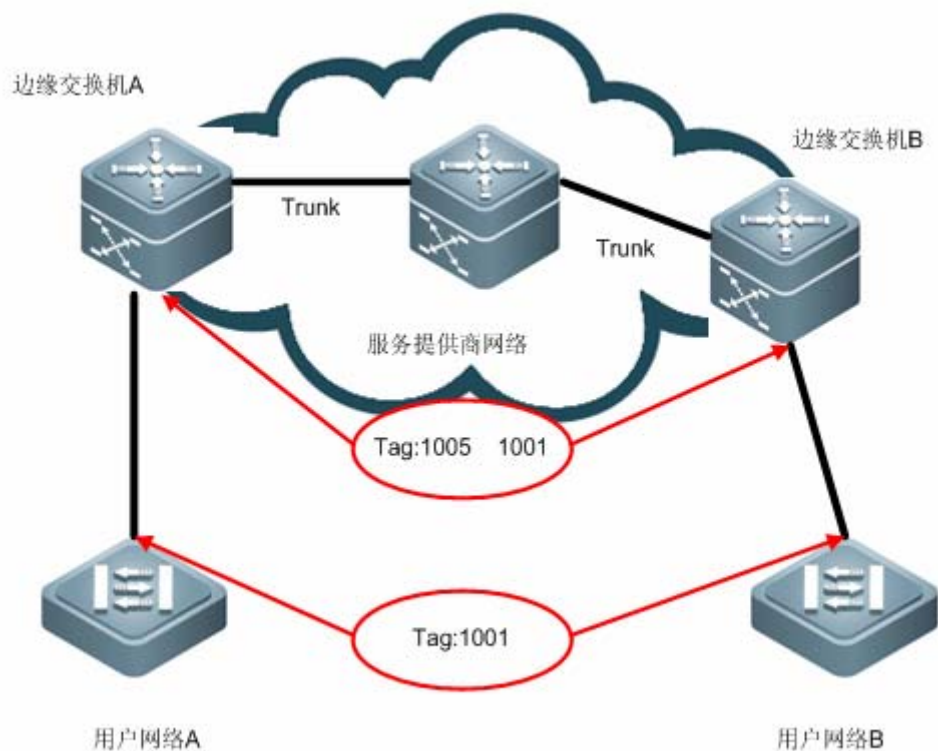


图 13-1 QinQ 示意图

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。

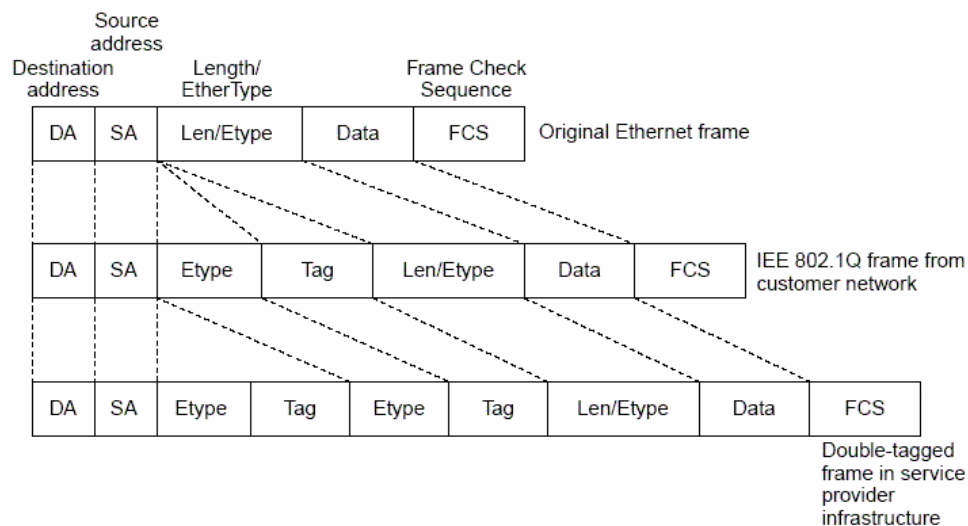


图 13-2 双 Tag 报文的结构

13.1.1 基本 QinQ

基本 QinQ 是基于端口方式实现的。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。

13.1.2 灵活 QinQ

灵活 QinQ 是一种灵活的实现，它可以为不同的流打上不同的外层 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。借助上述流分类方法，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；

13.1.3 其他功能

13.1.3.1 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。

13.1.3.2 MAC地址复制

由于采用基于流的灵活 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。

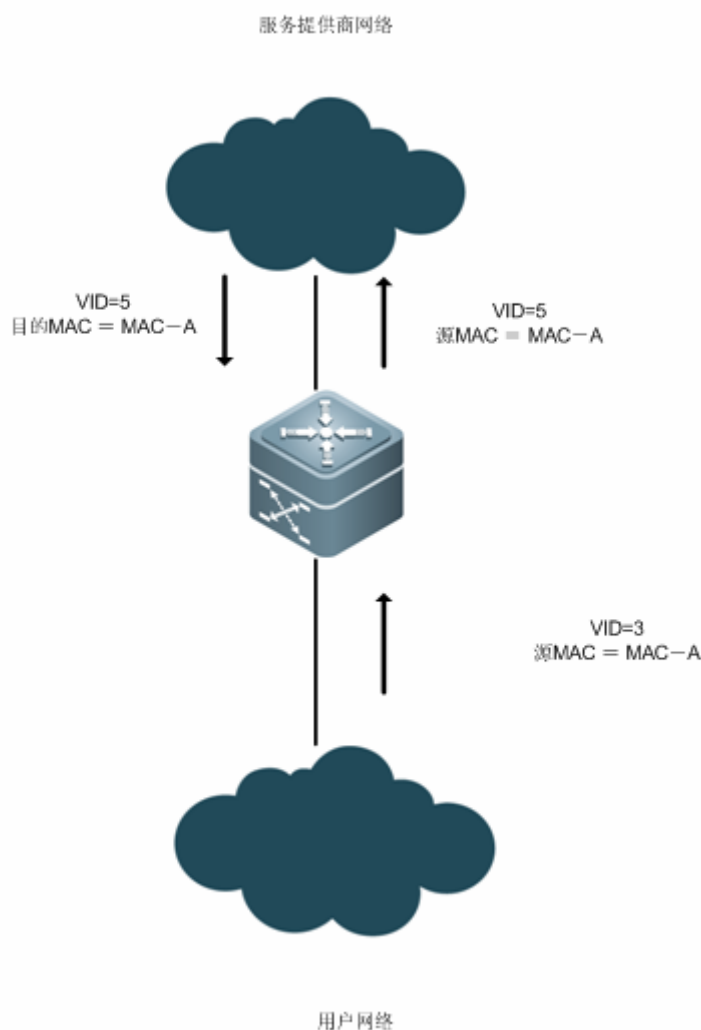


图 13-3 灵活 QinQ 报文的 MAC 地址学习示意图

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，对 vlan 3 的报文封装外层 Tag 为 vlan 5。当交换机收到用户网络 vlan 3 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。

13.1.3.3 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。

13.1.3.4 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。

13.2 配置QinQ

13.2.1 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。

13.2.2 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。

建议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。

QinQ 不支持热备。

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。

13.2.3 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
Step 1	configure terminal	进入全局配置模式
Step 2	interface <interface>	进入接口配置模式
Step 3	switchport mode dot1q-tunnel	接口设置成 dot1q-tunnel port

Step 4	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
Step 5	switchport dot1q-tunnel allowed vlan remove v_list	删除 dot1q-tunnel 口的许可 vlan
Step 6	switchport dot1q-tunnel native vlan VID	设置 dot1q-tunnel 口的缺省 vlan
Step 7	end	退出接口模式
Step 8	show running-config	查看全局配置

 说明

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)# end
```

13.2.4 配置灵活QinQ

13.2.4.1 配置基于协议的vid变更策略表

13.2.4.1.1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
Step 1	configure terminal	进入配置模式
Step 2	interface intf-id	进入接口模式
Step 3	switchport mode dot1q-tunnel	接口配置为 dot1q-tunnel 口
Step 4	dot1q outer-vid VID register inner-vid v_list	配置基于协议添加外部 Tag 的 VID 策略
Step 5	no dot1q outer-vid VID register inner-vid v_list	取消基于协议添加外部 Tag 的 VID 策略
Step 6	end	退出接口模式
Step 7	show registration-table	查看该配置。

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

```
Ruijie# configure
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
```

13.2.4.1.2 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
Step 1	configure terminal	进入配置模式
Step 2	interface intf-id	进入接口模式
Step 3	switchport mode port-type	配置为 Access、Trunk、Uplink 或 Hybrid 口
Step 4	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
Step 5	no dot1q relay-vid VID translate local-vid v_list	取消基于外部 Tag 修改外部 Tag 的 VID 策略
Step 6	end	退出接口模式
Step 7	show translation-table	查看该配置。

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
```

13.2.4.2 配置基于流的vid变更策略表

13.2.4.2.1 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
Step 1	configure terminal	进入配置模式
Step 2	interface intf-id	进入接口模式
Step 3	switchport mode dot1q-tunnel	接口配置为 dot1q-tunnel 口

Step 4	traffic-redirect access-group acl nested-vlan VID in	配置基于报文流添加外部 Tag 的 VID 策略
Step 5	no traffic-redirect access-group acl nested-vlan	取消基于报文流添加外部 Tag 的 VID 策略
Step 6	end	退出接口模式
Step 7	show traffic-redirect	查看该配置。

说明

- 基于流的 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，无法采用基于流的匹配规则来添加 Tag。
- 若某个报文同时匹配两个或两个以上流策略的规则，且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 1.1.1.3 输入报文添加 VID 为 9

```
Ruijie# configure
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
```

13.2.4.2.2 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
Step 1	configure terminal	进入配置模式
Step 2	interface intf-id	进入接口模式
Step 3	switchport mode trunk	配置为 Access, Trunk 或 Hybrid 口
Step 4	traffic-redirect access-group acl outer-vlan VID in	配置基于报文流修改外部 Tag 的 VID 策略
Step 5	no traffic-redirect access-group acl outer-vlan	取消基于报文流修改外部 Tag 的 VID 策略
Step 6	end	退出接口模式
Step 7	show traffic-redirect	查看该配置。

 说明

- 基于流的外部 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流策略的规则，且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
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
```

13.2.5 配置 QinQ 其他功能

13.2.5.1 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
Step 1	configure terminal	进入全局配置模式
Step 2	interface <interface>	进入接口配置模式
Step 3	switchport mode uplink	配置端口为 Uplink 口
Step 4	end	退出接口模式
Step 5	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
```

13.2.5.2 配置服务商 Tag 中的 TPID 值

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配置：

	命令	作用
Step 1	configure terminal	进入配置模式
Step 2	interface <interface>	进入接口配置模式
Step 3	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。该功能需要在出口配置才能生效。

Step 4	end	退出接口模式
Step 5	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)# interface gigabitethernet 0/1
Ruijie(config-if)# frame-tag tpid 9100
Ruijie(config)# end
Ruijie# show frame-tag tpid interface gigabitethernet 0/1
Port    tpid
-----
Gi0/1   0x9100
```

☹各产品支持情况

- 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)。

13.2.5.3 配置优先级复制

实现在 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
Step 1	configure terminal	进入配置模式
Step 2	interface <interface>	进入接口配置模式
Step 3	mls qos trust cos	配置端口信任模式为 trust CoS。
Step 4	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)。
Step 5	end	退出接口模式
Step 6	show inner-priority-trust	查看复制的配置。

📖 说明

- 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
```

13.2.5.4 配置优先级映射

在 tunnel 口上，实现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
Step 1	configure terminal	进入配置模式
Step 2	interface <interface>	进入接口配置模式
Step 3	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)。
Step 4	end	退出接口模式
Step 5	show interface intf-name remark	查看优先级映射的配置。

说明

- 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个接口上同时打开。
- 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
```

13.2.5.5 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
Step 1	configure terminal	进入配置模式
Step 2	interface <interface>	进入接口配置模式
Step 3	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。
Step 4	end	退出接口模式
Step 5	show interface intf-name mac-address-mapping x	查看地址复制的配置。

说明

- 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)# switchport mode trunk
Ruijie(config-if)#mac-address-mapping destination-vlan5 source-vlan 1-3
Ruijie(config)# end
Ruijie# show interface mac-address-mapping
Ports      destination-VID      Source-VID-list
-----
Gi0/1      5                     1-3
```

13.2.5.6 配置二层协议透传功能

13.2.5.6.1STP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
Step 1	configure terminal	进入配置模式
Step 2	l2protocol-tunnel stp	配置全局使能 STP 协议报文透传功能
Step 3	interface interface-name	进入接口模式
Step 4	l2protocol-tunnel stp enable	在接口上使能 STP 协议报文透传功能
Step 5	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
Ruijie(config)# l2protocol-tunnel stp
Ruijie(config)# interface fa 0/1
Ruijie(config-if)# l2protocol-tunnel stp enable
```

13.2.5.6.2 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
Step 1	configure terminal	进入配置模式
Step 2	l2protocol-tunnel gvrp	配置全局使能 GVRP 协议报文透传功能
Step 3	interface interface-name	进入接口模式
Step 4	l2protocol-tunnel gvrp enable	在接口上使能 GVRP 协议报文透传功能
Step 5	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
Ruijie(config)# l2protocol-tunnel gvrp
Ruijie(config)# interface fa 0/1
Ruijie(config-if)# l2protocol-tunnel gvrp enable
```

说明

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。

13.2.5.6.3 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
Step 1	configure terminal	进入配置模式
Step 2	l2protocol-tunnel { STP GVRP } tunnel-dmac mac-address	配置相应协议的透传地址
Step 3	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
Ruijie(config)# l2protocol-tunnel stp tunnel-dmac 011AA9 000005
```

说明

- 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)。

13.3 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

Step 1	Ruijie# show dot1q-tunnel	显示接口的 dot1q-tunnel 是否打开
Step 2	Ruijie#show interface [intf-id]dot1q-tunnel	显示 dot1q-tunnel 口配置
Step 3	Ruijie# show registration-table [interface intf-id]	显示基于协议的 dot1q-tunnel 端口 vid 添加策略表
Step 4	Ruijie# show translation-table [interface intf-id]	显示基于协议 access,trunk,hybrid 端口 vid 修改策略表
Step 5	Ruijie# show traffic-redirect [interface intf-id]	显示基于流的 vid 变更或添加策略表
Step 6	Ruijie# show frame-tag tpid interface [intf-id]	显示接口 tpid 的配置
Step 7	Ruijie# show inner-priority-trust	显示优先级复制配置
Step 8	Ruijie# show interface intf-name remark	显示优先级映射的配置
Step 9	Ruijie# show mac-address-mapping	显示 MAC 地址复制配置
Step10	Ruijie# show l2protocol-tunnel { gvrp stp }	显示二层透传配置



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. 配置 IP 地址与服务
2. 配置 DHCP Server & Client
3. 配置 DHCP Relay Agent
4. 配置 UDP-Helper
5. 配置 DNS
6. 配置 FTP Server
7. 配置 FTP CLIENT
8. 网络连通性测试工具
9. 配置 IPV4 快速转发

1 配置 IP 地址与服务

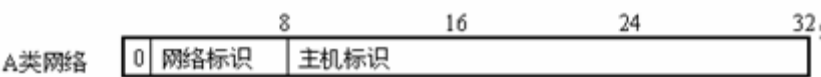
1.1 IP地址配置

1.1.1 IP地址简介

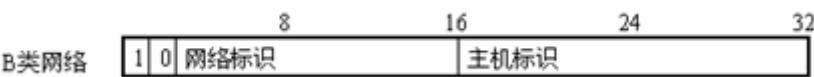
IP 地址由 32 位二进制组成，为了书写和描述方便，一般用十进制表示。十进制表示时，分为四组，每组 8 位，范围从 0~255，组之间用 “.” 号隔开，比如 “192.168.1.1” 就是用十进制表示的 IP 地址。

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。

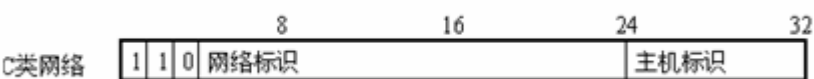
A 类地址，最高比特位为 “0”，有 7 个比特位表示网络号，24 个比特位表示本地地址。这样总共有 128 个 A 类网络。



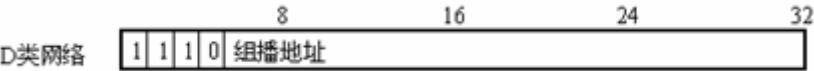
B 类地址，前两个最高比特位为 “10”，有 14 个比特位表示网络号，16 个比特位表示本地地址。这样总共有 16,384 个 B 类网络。



C 类地址，前三个最高比特位为 “110”，有 22 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。



D 类地址，前四个最高比特位为 “1110”，其余比特位为组播地址。



说明

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 IP地址配置任务列表

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。

- 接口 IP 地址配置（要求）
- 地址解析协议（ARP）配置（可选）

- 关闭 IP 路由（可选）
- 广播包处理配置（可选）

1.1.2.1 接口IP地址配置

一个设备只有配置了 IP 地址，才可以接收和发送 IP 数据报，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
Step 1	Ruijie(config-if)# ip address <i>ip-address mask</i>	设置一个接口的 IP 地址
Step 2	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 地址比特位就是为网络部分，值为“0”的比特对应的 IP 地址比特位就是为主机地址部分。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，子网划分就是将一个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。

说明

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。锐捷产品只支持从网络部分开始的从左到右连续的子网掩码。

子网掩码还可以用从左到右连续为 1 的比特位数来表示，因此地址配置还有另外两种形式：

	命令	作用
Step 1	Ruijie(config-if)# ip address <i>ip-address/mask-length</i>	设置一个接口的 IP 地址
Step 2	Ruijie(config-if)# no ip address	取消一个接口的 IP 地址配置

或

	命令	作用
Step 1	Ruijie(config-if)# ip address <i>ip-address mask-length</i>	设置一个接口的 IP 地址
Step 2	Ruijie(config-if)# no ip address	取消一个接口的 IP 地址配置

与接口 IP 地址相关的特性配置见下列任务列表，以下任务作为可选配置，可以根据实际情况决定是否需要进行配置：

1.1.2.1.1 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。

说明

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
Step 1	Ruijie(config-if)# ip address ip-address mask secondary	设置接口次 IP 地址
Step 2	Ruijie(config-if)# no ip address ip-address mask secondary	取消接口次 IP 地址配置

1.1.2.2 地址解析协议 (ARP) 配置

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 文当中描述。

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 通常应用在没有盘的工作站上。

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。除非有特殊情况，否则不需要额外配置，锐捷产品还能通过以下配置来管理地址解析：

1.1.2.2.1 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
Step 1	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。
Step 2	Ruijie(config)# no arp ip-address	取消静态 ARP



对于 s3750/s3250 堆叠，配置完静态 arp 后，交换机必须在学习到该静态 arp 对应的 mac 后才能进行正常的三层路由。

1.1.2.2.2 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。

1.1.2.2.3 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

Step 1	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
Step 2	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。

1.1.2.2.4 配置可信任ARP功能

防 ARP 欺骗。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
Step 1	Ruijie(config)# service trustedarp	启用可信任 ARP 功能
Step 2	Ruijie(config)# no service trustedarp	关闭可信任 ARP 功能

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
Step 1	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
Step 1	Ruijie(config)# clear arp trusted [ip [mask]]	查看交换机上的可信任 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
Step 1	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
Step 1	Ruijie(config)# arp trusted number	调整可信任 ARP 的容量为 <i>number</i> 。

1.1.2.3 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
Step 1	Ruijie(config)# no ip routing	关闭 IP 路由功能
Step 2	Ruijie(config)# ip routing	启动 IP 路由功能

1.1.2.4 广播包处理配置

广播包是指目标地址为某个物理网络上所有的主机。锐捷产品支持两种类型广播包：1) 定向广播，是指数据报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，是指数据报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。

如何对广播包进行处理，按照以下任务任务表，根据网络实际的需求进行配置。

1.1.2.4.1 定向网络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
Step 1	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
Step 2	Ruijie(config-if)# no ip directed-broadcast	取消转换

1.1.2.4.2 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
Step 1	Ruijie(config-if)# ip broadcast-address ip-address	创建新的广播地址
Step 2	Ruijie(config-if)# no ip broadcast-address	取消新的广播地址

1.1.3 监视和维护IP地址

要监视和维护网络，根据以下任务描述，根据实际需要进行操作。

- 清除缓冲和表内容
- 显示系统和网络状态

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
Step 1	Ruijie# clear arp-cache	清除 ARP 缓冲
Step 2	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那条路径发送。

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：

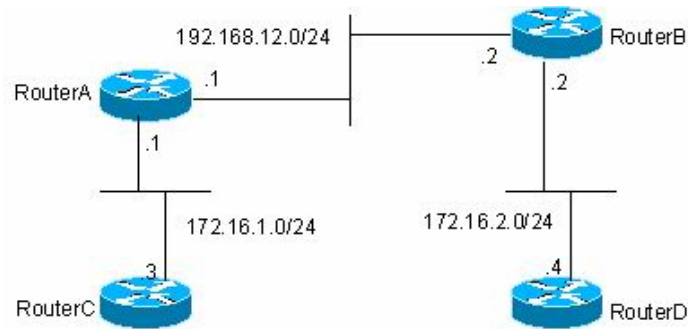
	命令	作用
Step 1	Ruijie# show arp [[ip [mask] mac-address] static complete incomplete]	显示 ARP 缓冲表，其中 complete / incomplete 关键字是用来分别显示动态 ARP 中已解析 / 未解析的表项。
Step 2	Ruijie# show ip arp	显示 IP ARP 缓冲表
Step 3	Ruijie# show ip interface [interface-type interface-number]	显示接口 IP 信息
Step 4	Ruijie# show ip route [network [mask]]	显示路由表
Step 5	Ruijie# show ip route	显示路由表摘要
Step 6	Ruijie# ping ip-address [length bytes] [ntimes times] [timeout seconds]	测试网络可达性

1.1.4 IP地址配置范例

1.1.4.1 次IP地址配置范例

■ 配置要求

IP 地址分配和网络设备连接图见图 1。



次 IP 地址配置范例

要求配置 RIP 路由协议，但只允许将版本设定为 RIPv1，在路由器 C 上可以看到 172.16.2.0/24 的路由，在路由器 D 上可以看到 172.16.1.0/24 的路由。

■ 路由器具体配置

RIPv1 路由协议是不支持无类路由的，即在路由通告中不携带掩码信息，172.16.1.0/24 和 172.16.2.0/24 两个同网络的子网又被 C 类网络 192.168.12.0/24 分割开，按照通常配置，路由器 C 和路由器 D 上是不可能学到对方网络的详细路由。但是 RIP 路由协议有个特性，如果接口网络与接收的路由同属一个网络，该路由的网络掩码与该接口网络掩码将设为一致。根据这个特性，可以通过配置路由器 A 和路由器 B，在 192.168.12.0/24 网络上构建一个次网络 172.16.3.0/24，这样两个被分割的子网就连接起来了。以下只写出路由器 A 和路由器 B 的配置。

路由器 A 的配置：

```
interface FastEthernet 0/0
ip address 172.16.3.1 255.255.255.0 secondary
ip address 192.168.12.1 255.255.255.0
!
interface FastEthernet 0/1
ip address 172.16.1.1 255.255.255.0
!
router rip
network 172.16.0.0
network 192.168.12.0
```

路由器 B 的配置：

```
interface FastEthernet 0/0
ip address 172.16.3.2 255.255.255.0 secondary
ip address 192.168.12.2 255.255.255.0
!
interface FastEthernet 0/1
ip address 172.16.2.1 255.255.255.0
!
router rip
network 172.16.0.0
```

```
network 192.168.12.0
```

1.2 IP服务配置

1.2.1 IP服务配置任务列表

IP 服务配置，包括以下配置任务，以下任务都是可选任务，您可以根据实际需要选择执行：

1.2.1.1 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。

1.2.1.1.1 启用ICMP目标不可达消息

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
Step 1	Ruijie(config-if)# ip unreachable	启用 ICMP 协议不可达和主机不可达消息
Step 2	Ruijie(config-if)# no ip unreachable	关闭 ICMP 协议不可达和主机不可达消息

1.2.1.1.2 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
Step 1	Ruijie(config-if)# ip redirects	启用 ICMP 重定向消息，缺省启用
Step 2	Ruijie(config-if)# no ip redirects	关闭 ICMP 重定向消息

1.2.1.1.3 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
Step 1	Ruijie(config-if)# ip mask-reply	启用掩码应答消息
Step 2	Ruijie(config-if)# no ip mask-reply	关闭掩码应答消息

1.2.1.1.4 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
Step 1	Ruijie(config-if)# ip mtu bytes	设置 MTU 值，范围 68~1500
Step 2	Ruijie(config-if)# no ip mtu	恢复缺省值

1.2.1.1.5 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
Step 1	Ruijie(config)# ip source-route	启用 IP 源路由
Step 2	Ruijie(config)# no ip source-route	关闭 IP 源路由

2 配置 DHCP Server & Client

2.1 DHCP介绍

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。

2.2 DHCP服务器简介

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



DHCP 基本工作流程

DHCP 请求 IP 地址的过程如下:

- 1) 主机发送 DHCPDISCOVER 广播包在网络上寻找 DHCP 服务器;

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

说明

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。另外，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，应用我司产品 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。

2.3 DHCP客户端简介

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。

注意

我司产品目前版本支持以太网接口以及 FR、PPP、HDLC 接口上的 DHCP 客户端。

2.4 DHCP中继代理简介

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。

2.5 DHCP配置

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）
- DHCP 排斥地址配置（要求）
- DHCP 地址池配置（要求）
- 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）
- 以太网接口 DHCP 客户端配置（可选）
- PPP 封装链路上的 DHCP 客户端配置（可选）
- FR 封装链路上的 DHCP 客户端配置（可选）
- HDLC 封装链路上的 DHCP 客户端配置（可选）

2.5.1 启用DHCP服务器与中继代理

要启用 DHCP 服务器、中继代理，全局配置模式中执行以下命令：

命令	作用
Ruijie(config)# service dhcp	启用 DHCP 服务器和 DHCP 中继代理功能
Ruijie(config)# no service dhcp	关闭 DHCP 服务器和中继代理功能

 说明

我司产品 10.1 及以后版本缺省情况下, 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。

在我司 10.1 之前的产品上 (不包括 10.1), 服务器和中继并不是全部支持的, 因此在这些系统上 **service dhcp** 这条命令就退化成打开当前产品支持的中继或者服务器。

在我司 10.1 及以后版本的部分产品上, 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, 请参考具体的产品的提示信息。

2.5.2 DHCP排斥地址配置

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 <i>low-ip-address</i> [<i>high-ip-address</i>]	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 <i>low-ip-address</i> [<i>high-ip-address</i>]	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: 1) 不会发生地址冲突; 2) DHCP 分配地址时, 减少了检测时间, 从而提高 DHCP 分配效率。

2.5.3 DHCP地址池配置

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。我司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）
- 配置地址池子网及其掩码（要求）
- 配置客户端缺省网关（要求）
- 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）

2.5.3.1 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，在全局配置模式中执行以下命令：

命令	作用
Ruijie(config)# ip dhcp pool <i>dhcp-pool</i>	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)#”。

2.5.3.2 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 <i>filename</i>	配置客户端启动文件名

2.5.3.3 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 <i>address</i> [<i>address2...address8</i>]	配置缺省网关

2.5.3.4 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 { <i>days</i> [<i>hours</i>] [<i>minutes</i>] infinite }	配置地址租期

2.5.3.5 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 <i>domain</i>	配置域名

2.5.3.6 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 <i>address</i> [<i>address2...address8</i>]	配置 DNS 服务器

2.5.3.7 配置 NetBIOS WINS 服务器

WINS 是微软 TCP/IP 网络解析 NetBIOS 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 <i>address [address2...address8]</i>	配置 DNS 服务器

2.5.3.8 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 <i>type</i>	配置 NetBIOS 节点类型

2.5.3.9 配置DHCP地址池的网络号和掩码

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 <i>network-number</i> <i>mask</i>	配置 DHCP 地址池的网络号和掩码

 注意

我司产品的 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;如果客户端和服务端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。

2.5.4 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
Step 1	Ruijie(config)# ip dhcp pool name	定义地址池名,进入 DHCP 配置模式
Step 2	Ruijie(dhcp-config)# host address	定义客户端 IP 地址
	Or: Ruijie(dhcp-config)# client-identifier unique-identifier	定义客户端硬件地址,如 aabb.bbbb.bb88 定义客户端的标识,如 01aa.bbbb.bbbb.88
Step 3	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

2.5.5 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 <i>number</i>	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。

2.5.6 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 <i>milliseconds</i>	配置 DHCP 服务器 Ping 包超时时间，缺省为 500ms。

2.5.7 以太网接口DHCP客户端配置

我司产品支持以太网端口通过 DHCP 获得动态分配的 IP 地址。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

2.5.8 PPP封装链路路上的DHCP客户端配置

我司产品支持 ppp 封装的端口通过 DHCP 获得动态分配的 IP 地址。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

2.5.9 FR封装链路路上的DHCP客户端配置

我司产品支持 FR 封装的端口通过 DHCP 获得动态分配的 IP 地址。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

2.5.10 HDLC封装链路上的DHCP客户端配置

我司产品支持 HDLC 封装的端口通过 DHCP 获得动态分配的 IP 地址。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

说明

在我司 10.1 的部分产品上，客户端支持在通过 PPP、HDLC、FR 封装的点对点链路上以 dhcp 方式获得 IP。

2.6 监视和维护信息

2.6.1 监视和维护DHCP服务器

监视和维护 DHCP 服务器有三类命令：

- 1) 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；
- 2) 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；
- 3) 显示命令，显示 DHCP 相关信息。

我司产品提供了三条清除命令，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

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

Ruijie# show ip dhcp binding [address]	显示 DHCP 地址绑定信息
Ruijie# show ip dhcp conflict	显示 DHCP 地址冲突信息
Ruijie# show ip dhcp server statistics	显示 DHCP 服务器统计信息

2.6.2 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
Ruijie# show dhcp lease	显示 DHCP 租约信息

2.7 配置范例

2.7.1 地址池配置例子

在以下配置中，定义了一个地址池 **net172**，地址池网段为 **172.16.1.0/24**，缺省网关为 **172.16.16.254**，域名为 **rg.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 **30** 天。该地址池中除了 **172.16.1.2~172.16.1.100** 地址外，其余地址均为可分配地址。

```
ip dhcp excluded-address 172.16.1.2 172.16.1.100
!
ip dhcp pool net172
network 172.16.1.0 255.255.255.0
default-router 172.16.1.254
domain-name rg.com
dns-server 172.16.1.253
netbios-name-server 172.16.1.252
netbios-node-type h-node
lease 30
```

2.7.2 手工绑定配置

在以下配置中，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 Billy.rg.com，缺省网关为 172.16.1.254，WINS 服务器为 172.16.1.252，NetBIOS 节点类型为复合型。

```
ip dhcp pool Billy
host 172.16.1.101 255.255.255.0
hardware-address 00d0.df34.32a3 ethernet
client-name Billy
default-router 172.16.1.254
domain-name rg.com
dns-server 172.16.1.253
netbios-name-server 172.16.1.252
netbios-node-type h-node
```

2.7.3 DHCP客户端配置

以下配置中，为设备接口 FastEthernet 0/0 配置 DHCP 自动分配地址。

```
interface FastEthernet0/0
ip address dhcp
```


3 配置 DHCP Relay Agent

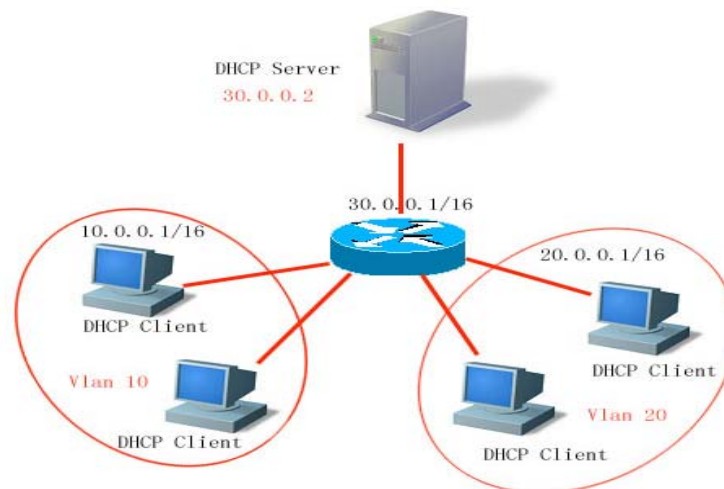
3.1 概述

3.1.1 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。DHCP 客户端发出 DISCOVER 广播报文给 DHCP 服务器。DHCP 服务器收到后 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 理解DHCP Relay Agent

DHCP 请求报文的目的 IP 地址为 255.255.255.255，这种类型报文的转发局限于子网内。为了实现跨网段的动态 IP 地址分配，DHCP 中继就产生了。DHCP 中继将收到的 DHCP 请求报文以单播方式转发给 DHCP 服务器，同时将收到的 DHCP 响应报文转发给 DHCP 客户端。DHCP 中继相当于一个转发站，负责沟通位于不同网段的 DHCP 客户端和 DHCP 服务器。这样就实现了只要安装一个 DHCP 服务器，就可以实现对多个网段的动态 IP 管理，即 Client—Relay—Server 模式的 DHCP 动态 IP 管理。如下图所示：

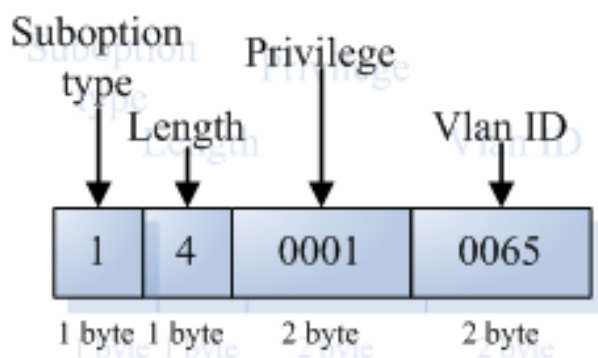


VLAN 10 和 VLAN 20 分别对应 10.0.0.1/16 和 20.0.0.1/16 的网络，而 DHCP 服务器在 30.0.0.1/16 的网络上，30.0.0.2 的 DHCP 服务器要对 10.0.0.1/16 和 20.0.0.1/16 的网络进行动态 IP 管理，只要在作为网关的设备上打开 DHCP 中继功能，并配置 30.0.0.2 为 DHCP 服务器的 IP 地址。

3.1.3 理解DHCP Relay Agent Information(option 82)

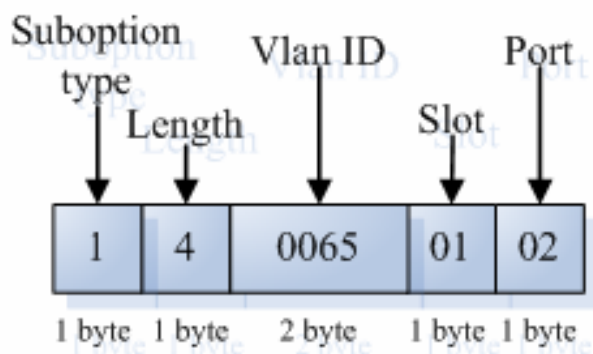
根据 RFC3046 的定义，中继设备进行 DHCP relay 时，可以通过添加 option 的方式来详细的标明 DHCP 客户端的一些网络信息，从而使服务器可以根据更精确的信息给用户分配不同权限的 IP，根据 RFC3046 的定义，所使用 option 选项的选项号为 82，故也被称作 option 82。锐捷网络实现的 relay agent information 目前存在三种应用方案，下面分别对三种应用方案进行说明：

1、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：

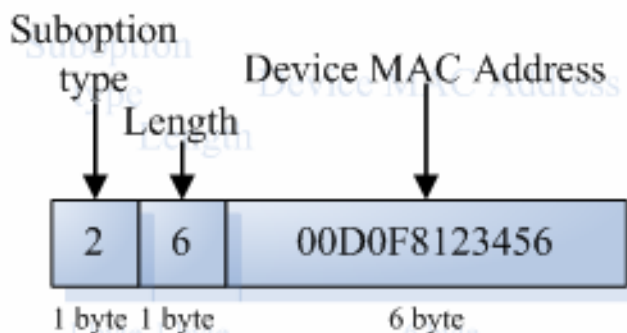


2、relay agent information option82：此种 option 的应用不需要结合其他协议模块的运行。DHCP 中继根据接收 DHCP 请求报文的实体端口，以及设备自身的物理地址信息，组合构成 option82 选项。选项格式如下图 **Agent Circuit ID** 和 **Agent Remote ID** 所示：

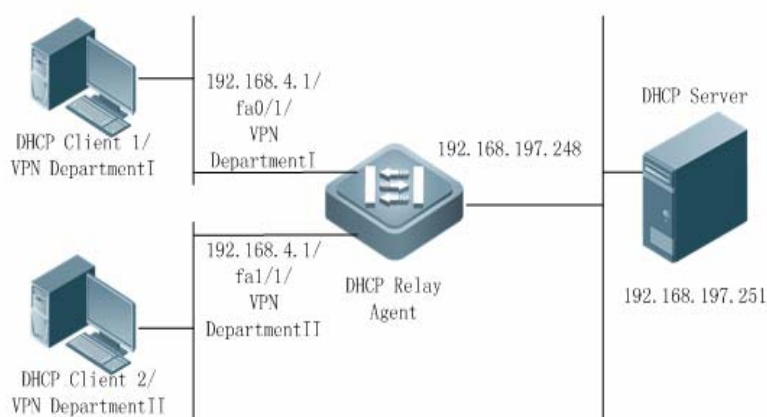
Agent Circuit ID



Agent Remote ID



3、relay agent information option vpn: 此种 option 的应用需要结合 MPLS VPN 相关功能。



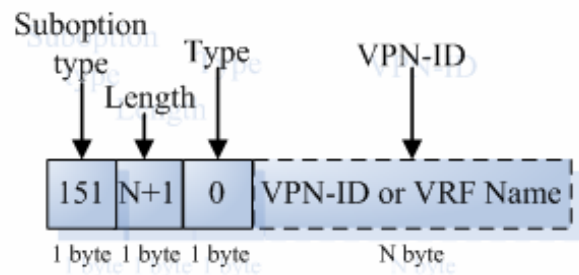
如上图所示，在 MPLS VPN 环境中，DHCP Client 1 和 DHCP 中继上的 fa0/1 口相连，DHCP Client 2 和 DHCP 中继上的 fa1/1 相连，接口 fa0/1 和接口 fa1/1 分别属于不同的 VRF，DHCP Client 1 和 DHCP Client 2 通过 DHCP 获取地址。按照网络规划，VPN Department I 和 VPN Department II 使用重叠网段 192.168.4.0/24，在该应用环境下，传统的 DHCP 应用根本无法支持该部署。为了实现在 MPLS VPN 环境下对 DHCP 中继的支持，在 DHCP 中继中引入了 option vpn 选项，该选项包括 VPN-ID、Subnet-Selection 以及 Server-Identifier-Override 三个子选项，简单说明一下这三个子选项的意义：

1)、VPN-ID: 在接收到 DHCP 请求报文时，将 DHCP 客户端所属的 VPN 信息，以选项形式加入 DHCP 请求报文中。DHCP 服务器发送响应报文时，将该选项信息原样保留，DHCP 中继根据该选项，将 DHCP 响应报文转发到正确的 VRF 中。选项格式如图 **VPN-ID** 所示：

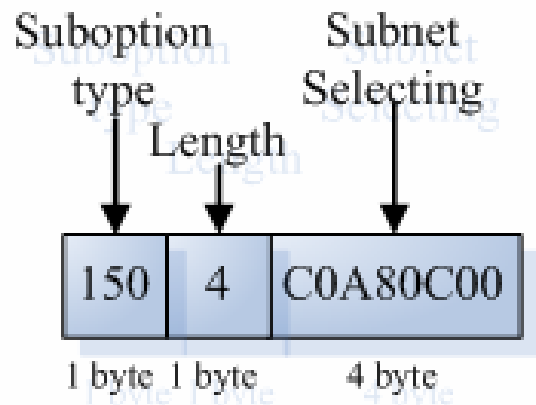
2)、Subnet-Selection: 在传统的 DHCP 中继环境中，通过 gateway address[giaddr]字段表示客户端所在的网络信息以及 DHCP 服务器与 DHCP 中继的通讯地址。在 MPLS VPN 环境中，将 giaddr 修改为 DHCP 中继连接 DHCP 服务器的接口 IP，使 DHCP 服务器可以与 DHCP 中继直接通讯。但是客户端的子网信息必须通过新的选项 Subnet-Selection 来表示。选项格式如图 **Subnet-Selecting** 所示：

3)、**Server-Identifier-Override**: 在 MPLS VPN 环境下, DHCP 客户端后续的请求报文都无法直接发送到 DHCP 服务器。DHCP 中继使用该选项携带 DHCP 中继与 DHCP 客户端直连的接口地址信息, DHCP 服务器发送响应报文的时候, 用该选项覆盖 **Server-identifier** 选项信息。从而使 DHCP 客户端在与 DHCP 服务器交互的过程中, 能够将报文送往 DHCP 中继, 然后由 DHCP 中继将报文转发到 DHCP 服务器。选项格式如图 **Server-id-Overriden** 所示:

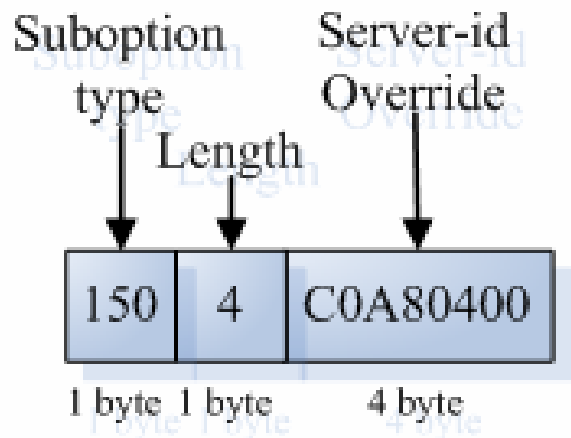
VPN-ID:



Subnet-Selecting:



Server-id-Overriden:



3.1.4 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 Relay Agent

3.2.1 配置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
Step 1	Ruijie (config)# service dhcp	启用 DHCP 代理
Step 2	Ruijie(config)# no service dhcp	关闭 DHCP 代理。

3.2.2 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。

配置 DHCP 服务器地址请按如下方式进行：

	命令	作用
Step 1	Ruijie(config)# ip helper-address [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
Step 2	Ruijie(config-if)# ip helper-address [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；

Step 3	Ruijie(config)# no ip helper-address [global] A.B.C.D	删除一个全局的 DHCP 服务器地址
Step 4	Ruijie(config-if)# no ip helper-address [global] A.B.C.D	删除一个接口的 DHCP 服务器地址

3.2.3 配置DHCP manage-vlan

用户在配置 DHCP RELAY 下联接口的时候为每一个接口配置一个地址及掩码，这样通过 RELAY 去分配地址时，DHCP 服务器会分配一个和该客户端连接的 RELAY 下联接口同一网段的地址，但如果 DHCP RELAY 开启了 option82 功能，DHCP 服务器在为客户端分配地址的时候使用 option82 中的信息来确认使用哪一类 IP 地址，所以当我们使用 option82 功能时，接口配置的地址及掩码实际上在分配地址过程中是没有被使用到的，但是如果不配置，报文由于源接口上无地址，无法上送到 DHCP RELAY 应用模块进行处理。特别对于 S29 这种弱三层设备来说，客户更多的是当二层设备来使用，所以用户一般情况下只需要配置一个管理 VLAN 地址，而这个地址是配置在某一个 VLAN 创建的 SVI 接口上。这时我们可以把所有的 DHCP RELAY 下联接口的源接口指定为管理 VLAN，这样报文成功送到 DHCP RELAY 应用模块，最终成功完成 DHCP 代理功能。

以上功能是在 DHCP RELAY 启用了 option82 功能的情况下使用的，可能有多 VLAN 接口作为 DHCP RELAY 的下联接口，在未开启这个功能情况下需要为每一个下联 VLAN 接口创建一个 SVI 并配置 IP 地址；开启这个功能后，我们不需要为下联 VLAN 接口创建 SVI，只需要通过这条命令把所有客户端上行的报文指定源接口为管理 VLAN 接口即可，这样不但简化了配置，同时也节省了地址的使用。

在全局配置模式下，请按如下步骤配置 DHCP manage-vlan，

	命令	作用
Step 1	Ruijie(config)# ip dhcp relay information manage-vlan vlanid	启用 DHCP manage-vlan 功能，同时指定来源接口为 vlan vlanid
Step 2	Ruijie(config)# no ip dhcp relay information manage-vlan	关闭 DHCP manage-vlan 功能。
Step 3	Ruijie(config)# default ip dhcp relay information manage-vlan	配置指定来源接口为默认的 vlan 1。

3.2.4 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
Step 1	Ruijie(config)# ip dhcp relay information option dot1x	启用 DHCP option dot1x 功能
Step 2	Ruijie(config)# no ip dhcp relay information option dot1x	关闭 DHCP option dot1x 功能。

3.2.5 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 DenyAccessEachOtherOfUnauthorize` 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
Step 1	Ruijie(config)# ip dhcp relay information option dot1x access-group <i>acl-name</i>	应用 DHCP option dot1x acl
Step 2	Ruijie(config)# no ip dhcp relay information option dot1x access-group <i>acl-name</i>	取消 DHCP option dot1x acl 的应用。

3.2.6 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
Step 1	Ruijie(config)# ip dhcp relay information option82	启用 DHCP option82 功能
Step 2	Ruijie(config)# no ip dhcp relay information option82	关闭 DHCP option82 功能。

3.2.7 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
Step 1	Ruijie(config)# ip dhcp relay check server-id	启用 DHCP relay check server-id 功能
Step 2	Ruijie(config)# no ip dhcp relay check server-id	关闭 DHCP relay check server-id 功能。

3.2.8 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
Step 1	Ruijie(config-if)# ip dhcp relay Suppresson	启用 DHCP relay suppresson 功能
Step 2	Ruijie(config-if)# no ip dhcp relay Suppresson	关闭 DHCP relay suppresson 功能。

3.2.9 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 option vpn 功能
Ruijie(config)# ip dhcp relayinformation option vpn
//添加全局服务器地址
Ruijie(config)# ip helper-address 192.18.100.1
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)# ip helper-address 192.18.200.1
Ruijie(config-if)# ip helper-address 192.18.200.2
Ruijie(config-if)# end

```

3.3 配置DHCP Relay Agent的其他注意事项

对于二层的网络设备来说，需要实现跨管理 vlan 的 DHCP 中继功能时，必须打开 **option dot1x**、**动态地址绑定**或者 **option82** 功能中的一个功能，否则在二层设备上只能实现管理 vlan 的 relay 功能。

3.3.1 配置DHCP option dot1x需要的注意事项

- 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 动态绑定功能不能同时启用。

3.3.2 配置DHCP option82 需要的注意事项

DHCP option82 功能于 **dhcp option dot1x** 功能互斥，不能同时使用。

3.4 显示配置

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
```

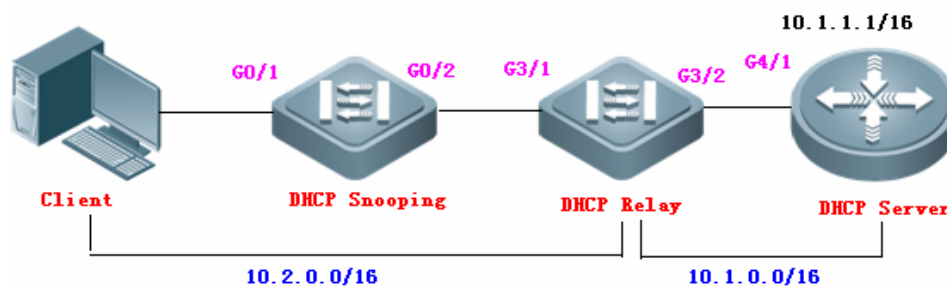
3.5 配置用例

3.5.1 跨网段的用户申请IP上网

配置要求

- 1)、要求用户跨网段可以获取 IP 地址进行正常上网；
- 2)、防止非法的用户私自设置 IP 地址进行上网。

拓扑图



分析

DHCP Snooping 交换机与 DHCP Relay 相连的交换机端口是普通 access 口，要求 Client 可以跨网段自动获取 IP 地址进行上网，这就需要 DHCP Relay 设备来实现。防止非法用户私自设置 IP 地址上网有两种做法：一种是在全局模式下开启 DAI（动态 ARP 检测功能），另一种是在接口模式下配置端口地址绑定，并结合 arp-check 功能来防止非法用户上网。该用例采用第一种做法。

配置过程

按上述拓扑图搭建环境，按下述配置步骤进行配置：

■ DHCP Snooping 的配置：

开启 DHCP Snooping 功能

```
Ruijie(config)# ip dhcp snooping
# 配置与服务器相连的 Gi0/2 为可信任口
Ruijie(config)# interface gigabitEthernet 0/2
Ruijie(config-if)# ip dhcp snooping trust
# 配置 Gi0/2 为 ARP 检测信任口
Ruijie(config-if)# ip arp inspection trust
Ruijie(config-if)# exit
# 启用指定 VLAN 的 DAI 报文检查功能
Ruijie(config)# ip arp inspection vlan 1
# 配置设备的 IP 地址 (SVI1)
Ruijie(config)# interface vlan 1
Ruijie(config-if)# ip address 10.2.0.1 255.255.0.0
# 配置到另一个网段 (10.1.0.0/16) 的静态路由
Ruijie(config)# ip route 10.1.0.0 255.255.0.0 10.2.1.1
```

■ DHCP Relay 的配置

```
# 启用 DHCP 中继代理
Ruijie(config)# server dhcp
# 添加一个全局的 DHCP 服务器的地址
Ruijie(config)# ip helper-address 10.1.1.1
# 配置与 Snooping 设备连接的端口的 IP 地址
Ruijie(config)# interface gigabitEthernet 3/1
Ruijie(config-if)# no switchport
Ruijie(config-if)# ip address 10.2.1.1 255.255.0.0
# 配置与 Server 设备连接的端口的 IP 地址
Ruijie(config)# interface gigabitEthernet 3/2
Ruijie(config-if)# no switchport
Ruijie(config-if)# ip address 10.1.0.1 255.255.0.0
```

■ DHCP Server 上的配置:

```
# 为连接 Relay 设备的端口配置 IP 地址
Ruijie(config)# interface gigabitEthernet 4/1
Ruijie(config-if)# no switchport
Ruijie(config-if)# ip address 10.1.1.1 255.255.0.0
# 启用 DHCP 服务器
Ruijie(config)# service dhcp
```

配置 DHCP 排斥地址，这些地址不会被分配给客户端

```
Ruijie(config)# ip dhcp excluded-address 10.1.1.1 10.1.1.10
```

配置地址池名并进入地址池配置模式

```
Ruijie(config)# ip dhcp pool linwei
```

配置客户端缺省网关

```
Ruijie(dhcp-config)# default-router 10.2.1.1
```

配置 DHCP 地址池的网络号和掩码

```
Ruijie(dhcp-config)# network 10.2.0.0 255.255.0.0
```

配置到另一个网段（10.2.0.0/16）的静态路由

```
Ruijie(config)# ip route 10.2.0.0 255.255.0.0 10.1.0.1
```

4 配置 UDP-Helper

4.1 UDP-Helper配置

4.1.1 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。

4.2 配置UDP-Helper

4.2.1 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

4.2.2 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。

说明

1. 缺省情况下中继转发功能处于关闭状态。
2. 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。
3. 当关闭 DUP 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。

4.2.3 配置中继转发的目的服务器

命令	作用
Ruijie(config-if)# ip helper-address <i>IP-Address</i>	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。

说明

1. 一个接口最多对应 20 个目的服务器
2. 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。

4.2.4 配置需要中继转发的UDP端口

命令	作用
Ruijie(config)# ip forward-protocol udp <i>ID</i>	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。

 说明

- 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。

5 配置 DNS

5.1 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。

5.2 配置域名解析

5.2.1 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

5.2.2 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
Step 1	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
```

5.2.3 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
Step 1	Ruijie(config)# ip name-server { <i>ip-address</i> <i>ipv6-address</i> }	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。

5.2.4 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
Step 1	Ruijie(config)# ip host <i>host-name</i> <i>ip-address</i>	手工配置主机名和 IP 地址映射
Step 2	Ruijie(config)# ipv6 host <i>host-name</i> <i>ipv6-address</i>	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。

5.2.5 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
Step 1	Ruijie# clear host [<i>word</i>]	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。

5.2.6 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
Step 1	Ruijie# show hosts [hostname]	查看 DNS 的相关参数
<pre>Ruijie# show hosts DNS name server : 192.168.5.134 static host type address www.163.com static 192.168.5.243 www.ruijie.com dynamic 192.168.5.123</pre>		

5.2.7 应用举例

Ping 指定域名的主机：

```
Ruijie# ping www.ietf.org
Resolving host[www.ietf.org].....
Sending 5,100-byte ICMP Echos to 192.168.5.123,
timeout is 2000 milliseconds.
!!!!!
Success rate is 100 percent(5/5)
Minimum = 1ms Maximum = 1ms, Average = 1ms
```

6 配置 FTP Server

6.1 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。

6.1.1 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	rhel	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。

6.2 配置FTP服务器

我们将从以下几个章节描述如何配置 FTP 服务器：

6.2.1 启用或关闭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

注意

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。

6.2.2 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。

6.2.3 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。

注意

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。

6.2.4 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] <i>password</i>	指定的 FTP 用户名相关联的缺省口令
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。

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
```

6.2.5 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
```

6.2.6 配置范例

下面展示如何完整地配置一个 FTP 服务器:

步骤 1: 配置登录用户名为 “admin”、密码为 “letmein”

```
Ruijie(config)# ftp-server username admin
Ruijie(config)# ftp-server password letmein
```

步骤 2: 配置会话空闲时限为 5 分钟

```
Ruijie(config)# ftp-server timeout 5
```

步骤 3: 配置服务器顶层目录为 “/syslog”

```
Ruijie(config)# ftp-server topdir /syslog
```

步骤 4: 启动 FTP 服务器

```
Ruijie(config)# ftp-server enable
```


7 配置 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。

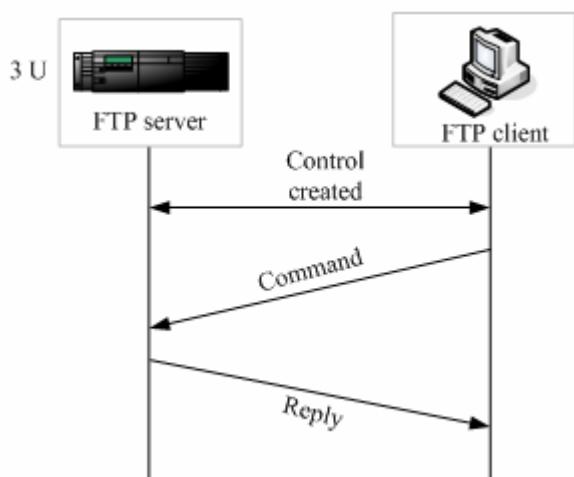
7.1 FTP概述

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 客户端和服务端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。

7.1.1 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。

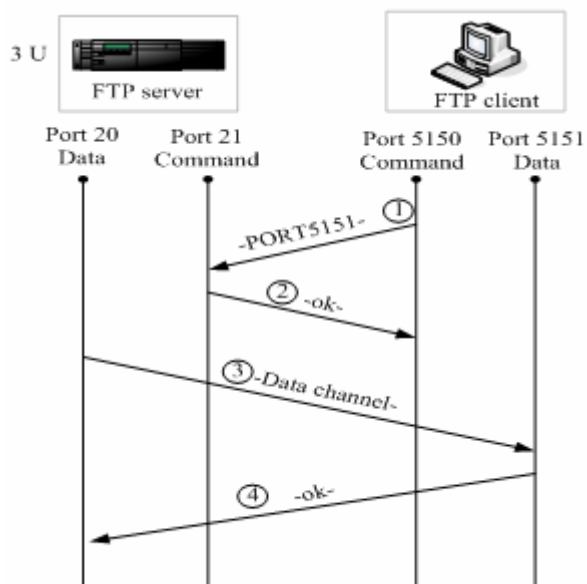
- 控制连接：对于一些比较简单的连接只需要建立控制连接，客户端向服务器发送命令，服务器接收到命令则进行命令响应，其过程如下：



- 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。

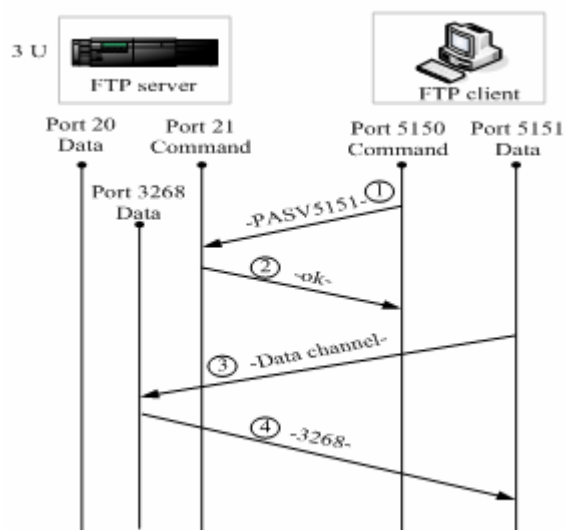
7.1.1.1 主动方式



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

7.1.1.2 被动方式



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。

7.1.2 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。

7.1.2.1 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`。

7.1.2.2 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。

7.1.3 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。

7.2 配置FTP Client

7.2.1 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 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 port	设置 FTP 为被动连接模式

7.2.2 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 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 ascii	设置 FTP 为二进制传输模式

7.2.3 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-clientsource-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 source-address	删除客户端源 ip 地址绑定

7.2.4 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	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

7.2.5 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 e flash:[local-directory]local-file	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。

 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。

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
```

7.2.6 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	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。

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
```

8 网络通信检测工具

8.1 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, 1000-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
```

8.2 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, 1000-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
```


8.3 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 [protocol] [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。

1. 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。

2. 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。

8.4 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] [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。

1. 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。

2. 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。

9 配置 IPv4 快转

9.1 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：

1. Express Forwarding 对报文解封装；
2. 用 Prefix Tree 来检索其报文路由所要输出的邻接节点；
3. 匹配到输出邻接节点后，再根据邻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。

9.2 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。

要监控和维护快转表，目前提供如下命令：

9.2.1 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
Ruijie# show ip ref	显示当前快转中的统计信息

9.2.2 邻接表信息

快转表中，一类重要的数据结构就是邻接表。我们可以通过以下命令来查看当前的邻接信息：

命令	作用
Ruijie# 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

1. 直连路由，如：1.1.0.0/16 vlan1
2. 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
3. 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

9.2.3 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像，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
Ruijie# 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，包括路由、默认路由与普通的网关路由。

9.2.4 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。硬件哈希桶冲突现在没办法解决。

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发生哈希桶冲突时,会以日志的形式打印该事件,其格式为: EFHW-4-(TBL_NO_RESOURCE): DESCRIPTION.

9.3 交换机快转ECMP/WCMP策略配置

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. 配置协议无关
2. 配置 RIP 路由协议
3. 配置 OSPF2 路由协议

1 配置协议无关

1.1 开启IP路由功能

缺省情况下，IP 路由功能开启。

命令	作用
Ruijie(config)# ip routing	开启 IPv4 路由功能

配置对应的 **no** 命令，可以关闭 IP 路由功能。

1.2 静态路由配置

静态路由就是手工配置的路由，使得数据包能够按照预定的路径传送到指定的目标网络。当不能通过动态路由协议学到一些目标网络的路由时，配置静态路由就会显得十分重要。通常可以给没有确切路由的数据包静态配置缺省路由。

要配置静态路由，在全局配置模式中执行以下命令：

命令	作用
Ruijie(config)# ip route network net-mask { ip-address interface [ip-address] } [distance] [tag tag] [permanent] [weight number] [disable enable]	配置 IPv4 静态路由
Ruijie(config)# ip static route-limit number	指定 IPv4 静态路由数的上限

如果没有执行删除动作，我司产品将永久保留静态路由。但是您可以用动态路由协议学到得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。以下为我司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
OSPF 路由	110
ISIS 路由	115
RIP 路由	120
不可达路由	255

 说明

对于静态路由，如果需要由 RIP、OSPF 等动态路由协议通告，需要对动态路由协议配置重分布静态路由。

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，当我公司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。

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。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
```

如果配置的静态路由数已经超过了指定的上限，则新配置的静态路由添加不进来。

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。

1.3 缺省路由配置

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手工配置。

缺省路由的产生有两种方法：1）手工配置缺省静态路由，具体配置参见上节“静态路由配置”；2）手工配置缺省网络。

多数的内部网关路由协议，都有一个将缺省路由传播到整个路由域的机制。要传播缺省路由的设备必须具有缺省路由。本节缺省路由的传播只适合 RIP 路由协议，RIP 向 RIP 路由域通告的缺省路由永远为“0.0.0.0”网络。OSPF 路由协议如何产生和传播缺省路由请参见“OSPF 路由协议配置指南”相关章节。

要产生缺省路由，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

说明

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。

同样的条件下，RIP 也可以传播缺省路由，但是 RIP 传播缺省路由还有另外一个办法，那就是配置缺省静态路由，或者通过其它路由协议学到了 0.0.0.0/0 的路由。

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”。

1.4 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，提供给路由协议使用。在路由协议中，用于路由信息的过滤和修改。

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	配置缺省网络
Ruijie(config)# no route-map route-map-name { [permit deny] sequence }	删除缺省网络

一个路由图规则配置中，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。

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 metric <i>Metric</i>	匹配路由的量度值 <i>Metric</i> : 0-4294967295
Ruijie(config-route-map)# match route-type { local internal external [type-1 type-2] }	匹配路由的类型
Ruijie(config-route-map)# match tag tag	匹配路由的标记值 <i>tag</i> : 0-4294967295

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 level { stub-area backbone }	设置输入路由的区域
Ruijie(config-route-map)# set metric metric	设置重分布路由的量度值
Ruijie(config-route-map)# set metric [+ <i>metric-value</i> - <i>metric-value</i> <i>metric-value</i>]	设置重分布路由的类型
Ruijie(config-route-map)# set metric-type { type-1 type-2 external internal }	设置重分布路由的类型
Ruijie(config-route-map)# set next-hop <i>next-hop</i>	设置重分布路由的下一跳 <i>next-hop</i> : 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

路由图的 **match** 命令与 **set** 命令对路由图不同应用的支持情况不同，为了方便用户了解 **match** 命令、**set** 命令是否适用于当前应用，我们将在如下情况下给予用户提示信息：

- 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。

1.5 路由重分布配置

为了支持本设备能够运行多个路由协议进程，我司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。比如您可以将 OSPF 路由域的路由重新分布后通告到 RIP 路由域中，也可以将 RIP 路由域的路由重新分布后通告到 OSPF 路由域中。路由的相互重分布可以在所有的 IP 路由协议之间进行。

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。

要把路由从一个路由域分布到另一个路由域，并且进行控制路由重分布，在路由进程配置模式中执行以下命令：

	命令	作用
Step 1	Ruijie(config-router)# redistribute <i>protocol</i> [<i>process-id</i>] [metric <i>metric</i>] [metric-type <i>metric-type</i>] [match internal external type nssa-external type] [tag <i>tag</i>] [route-map <i>route-map-name</i>] [subnets]	进行重分布路由 <i>protocol</i> （协议类型）： connected、rip、ospf、static
Step 2	Ruijie(config-router)# default-metric <i>metric</i>	给所有重分布路由设置缺省量度值 <i>metric</i>

路由重分布很容易造成路由环路，在使用时应该谨慎。

说明

OSPF 路由进程中配置路由重分布时，缺省情况下，赋予重分布路由的量度值为 20，类型为 Type-2，该类型路由属于 OSPF 最不可信的路由。

1.6 缺省路由分发配置

为了通告缺省路由，路由协议需要将缺省路由引入进程，或者强制生成一条缺省路由。

要对缺省路由进行分发设置，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 <i>metric</i>] [metric-type <i>type</i>] [route-map <i>map-name</i>]	将缺省路由引入路由协议进程并进行通告。 always(可选) ：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(可选) ：对引入的缺省路由的 <i>metric</i> 值进行设置 metric-type(可选) ：设置 OSPF 引入的缺省路由类型 route-map(可选) ：对引入缺省路由进行过滤和设置
Ruijie(config-router)# no default-information originate [always] [metric <i>metric</i>] [metric-type <i>type</i>] [route-map <i>map-name</i>]	取消将缺省路由引入路由协议进程并进行通告。

1.7 路由过滤配置

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 {[<i>access-list-number</i> <i>access-list-name</i>] prefix <i>prefix-list-name</i> } out [<i>interface-type</i> <i>interface-number</i>]	根据访问列表规则，允许或拒绝某些路由被分发出去。 prefix: 本关键字表明用前缀列表来过滤路由；前缀列表需要另外通过 ip prefix-list 配置。
Ruijie(config-router)# no distribute-list {[<i>access-list-number</i> <i>access-list-name</i>] prefix <i>prefix-list-name</i> } out [<i>interface-type</i> <i>interface-number</i> <i>protocol</i>]	取消遏制路由更新通告

说明

配置 OSPF 时，不能指定接口，而且该特性只适用于 OSPF 路由域的外部路由。

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。该特性不适用于 OSPF 路由协议。

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 {[<i>access-list-number</i> <i>access-list-name</i>] prefix <i>prefix-list-name</i> [gateway <i>prefix-list-name</i>]} gateway <i>prefix-list-name</i> } in [<i>interface-type</i> <i>interface-number</i>]	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: 本关键字表明用前缀列表来过滤路由；前缀列表需要另外通过 ip prefix-list 配置。 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 {[<i>access-list-number</i> <i>name</i>] prefix <i>prefix-list-name</i> [gateway <i>prefix-list-name</i>] gateway <i>prefix-list-name</i> } in [<i>interface-type</i> <i>interface-number</i>]	取消控制路由更新处理

1.8 配置密钥链

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 <i>key-chain-name</i>	配置密钥链
Ruijie(config-keychain)# key <i>key-id</i>	配置密钥
Ruijie(config-keychain-key)# key-string [0 7] <i>text</i>	配置认证串
Ruijie(config-keychain-key)# accept-lifetime <i>start-time</i> {infinite <i>end-time</i> duration <i>seconds</i> }	配置接收方向生存期
Ruijie(config-keychain-key)# send-lifetime <i>start-time</i> {infinite <i>end-time</i> duration <i>seconds</i> }	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(config)# show key chain	显示密钥链信息

1.9 配置范例

1.9.1 路由图应用

以下的配置例子，是 OSPF 路由协议重分布 RIP 路由，要求只重分布跳数为 4 的 RIP 路由，在 OSPF 路由域中，该路由的类型为外部路由 type-1，初始量度值为 40，路由标记值设为 40。

配置 OSPF

```
Ruijie(config)# router ospf 1
Ruijie(config-router)# redistribute rip subnets route-map redrip
Ruijie(config-router)# network 192.168.12.0 0.0.0.255 area 0
```

配置访问控制列表

```
Ruijie(config)# access-list 20 permit 200.168.23.0
```

配置路由图

```
Ruijie(config)# route-map redrip permit 10
Ruijie(config-route-map)# match metric 4
Ruijie(config-route-map)# set metric 40
```

```
Ruijie(config-route-map)# set metric-type type-1
Ruijie(config-route-map)# set tag 40
```

以下配置例子，是 RIP 路由协议重分布 OSPF 路由，要求只重分布标记为 10 的 OSPF 路由，初始量度值设为 10。

配置 RIP

```
Ruijie(config)# router rip
Ruijie(config-router)# version 2
Ruijie(config-router)# redistribute ospf 1 route-map redospf
Ruijie(config-router)# network 200.168.23.0
```

配置路由图

```
Ruijie(config)# route-map redospf permit 10
Ruijie(config-route-map)# match tag 10
Ruijie(config-route-map)# set metric 10
```

1.9.2 静态路由重分布

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。

这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 配置 RIP 路由协议

2.1 RIP简介

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 RIP配置任务列表

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）

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
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

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

Step 1	Ruijie(config)# router rip	创建 RIP 路由进程
Step 2	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。

说明

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 RIP报单播配置

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
Step 1	Ruijie(conf-router)# neighbor ip-address	配置 RIP 报单播通告

配合该命令的使用，您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。

说明

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 水平分割配置

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。

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

Step 1	Ruijie(config-if)# no ip rip split-horizon	关闭水平分割
Step 2	Ruijie(config-if)# ip rip split-horizon	打开水平分割

所有接口的默认行为设置为开启水平分割。

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、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。您可以通过配置，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
Step 1	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
Step 1	Ruijie(config-if)# ip rip send version 1	指定只发送 RIPv1 数据包
Step 2	Ruijie(config-if)# ip rip send version 2	指定只发送 RIPv2 数据包
Step 3	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
Step 1	Ruijie(config-if)# ip rip receive version 1	指定只接收 RIPv1 数据包
Step 2	Ruijie(config-if)# ip rip receive version 2	指定只接收 RIPv2 数据包
Step 3	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
Step 1	Ruijie(config-router)# no auto-summary	关闭路由自动汇聚
Step 2	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
Step 1	Ruijie(config-if)# ip rip summary-address <i>ip-address ip-network-mask</i>	配置接口级路由汇聚
Step 2	Ruijie(config-if)# no ip rip summary-address <i>ip-address ip-network-mask</i>	取消接口级路由汇聚

2.2.6 RIP认证配置

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，或者关联了密钥串但密钥串实际未配置，此时并不会认证行为发生。同样，如果采用 MD5 认证，但未配置关联密钥串，或者关联了密钥串但密钥串实际未配置，也不会有认证行为发生。

要配置 RIP 认证，在接口配置模式中执行以下命令：

	命令	作用
Step 1	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。
Step 2	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。
Step 3	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 RIP时钟调整

RIP 提供了时钟调整的功能，您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
Step 2	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。



说明

连接在同一网络上的设备，RIP 时钟值一定要一致。

2.2.8 RIP路由源地址验证配置

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
Step 1	Ruijie(config-router)# no validate-update-source	关闭源地址验证
Step 2	Ruijie(config-router)# validate-update-source	启动源地址验证

2.2.9 RIP 接口状态控制

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

Step 1	Ruijie(config-router)# passive-interface {default interface-type interface-num}	配置被动接口
Step 2	Ruijie(config-router)# no passive-interface {default interface-type interface-num}	取消被动接口

**注意**

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
Step 1	Ruijie(config-if)# no ip rip receive enable	禁止接口接收 RIP 报文
Step 2	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接收 RIP 报文，在接口配置模式中执行以下命令

	命令	作用
Step 1	Ruijie(config-if)# no ip rip send enable	禁止接口发送 RIP 报文
Step 2	Ruijie(config-if)# ip rip send enable	允许接口发送 RIP 报文

2.2.10 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
Step 1	Ruijie(config-if)# ip rip default-information originate [metric metric-value]	通告默认路由，也通告其它路由
Step 2	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
Step 1	Ruijie(config-if)# ip rip default-information only [metric metric-value]	通告默认路由，不通告其它路由
Step 2	Ruijie(config-if)# no ip rip default-information	取消接口通告默认路由

**说明**

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 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
Step 1	Ruijie(config-router)# no ip rip send supernet-routes	禁止接口通告超网路由
Step 2	Ruijie(config-router)# ip rip send supernet-routes	允许接口通告超网路由

 说明

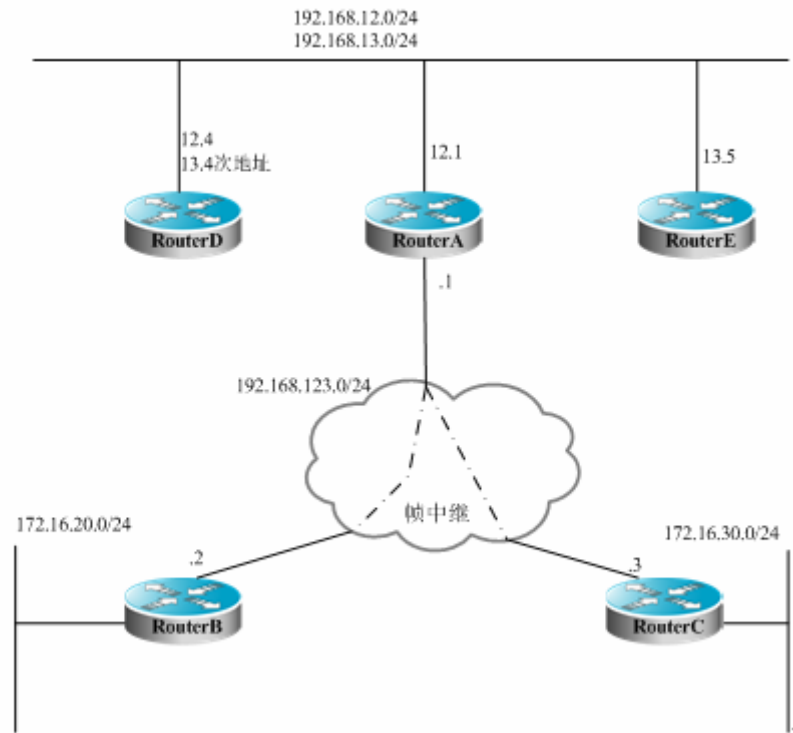
- 1) 接口上只接收 RIPv1 报文时，不接收 RIPv2 报文，也就不会接收超网路由；
- 2) 接口上能够接收 RIPv2 报文时，支持接收超网路由；
- 3) 接口上发送 RIPv1 报文时，不发送超网路由；
- 4) 接口上发送 RIPv2 报文时，缺省支持发送超网路由。
- 5) 通过接口模式命令 “no ip rip send supernet-routes” 控制不发送超网路由。
 - 自动汇聚(auto-summary)：对超网路由无效，即超网路由不会被汇聚。
 - 接口配置汇聚路由(ip summary rip)：不支持配置超网路由。

2.3 RIP配置范例

2.3.1 RIP水平分割配置例子

2.3.1.1 配置要求

有五台设备，其中 RouterA、RouterD、RouterE 三台设备通过以太网连接，RouterA、RouterB、RouterC 三台设备通过帧中继连接。IP 地址分配及设备连接图见下图，其中 RouterD 配置了次地址。



RIP 水平分割配置例子

通过配置设备需要达到以下要求：

- 所有设备运行 RIP 路由协议；
- RouterB、RouterC 能够相互学到对方通告的网段路由；3) RouterE 能够学到 192.168.12.0/24 的网段路由。

2.3.1.2 设备具体配置

在该范例配置中，为了达到配置要求，RouterA 和 RouterD 一定要关闭水平分割功能，否则 RouterA 将不会将 RouterB 通告的路由通告给 RouterC，RouterD 也不会将 192.168.12.0 网段通告给 RouterE。以下为每台设备的具体配置。

设备 A 的配置：

```
# 配置以太网端口
interface FastEthernet0/0
ip address 192.168.12.1 255.255.255.0

# 配置广域网端口
interface Serial1/0
ip address 192.168.123.1 255.255.255.0
encapsulation frame-relay
no ip rip split-horizon

# 配置 RIP 路由协议
```



```
router rip
version 2
network 192.168.12.0
network 192.168.123.0
```

设备 B 的配置:

```
# 配置以太网端口
interface FastEthernet0/0
ip address 172.16.20.1 255.255.255.0

# 配置广域网端口
interface Serial1/0
ip address 192.168.123.2 255.255.255.0
encapsulation frame-relay
```

配置 RIP 路由协议

```
router rip
version 2
network 172.16.0.0
network 192.168.123.0
no auto-summary
```

设备 C 的配置

```
# 配置以太网端口
interface FastEthernet0/0
ip address 172.16.30.1 255.255.255.0

# 配置广域网端口
interface Serial1/0
ip address 192.168.123.3 255.255.255.0
encapsulation frame-relay
```

配置 RIP 路由协议

```
router rip
version 2
network 172.16.0.0
network 192.168.123.0
no auto-summary
```

设备 D 的配置

```
# 配置以太网端口
interface FastEthernet0/0
ip address 192.168.12.4 255.255.255.0
ip address 192.168.13.4 255.255.255.0 secondary
no ip rip split-horizon
```

```
# 配置 RIP 路由协议
```

```
router rip
version 2
network 192.168.12.0
network 192.168.13.0
```

设备 E 的配置

```
# 配置以太网端口
```

```
interface FastEthernet0/0
ip address 192.168.13.5 255.255.255.0
```

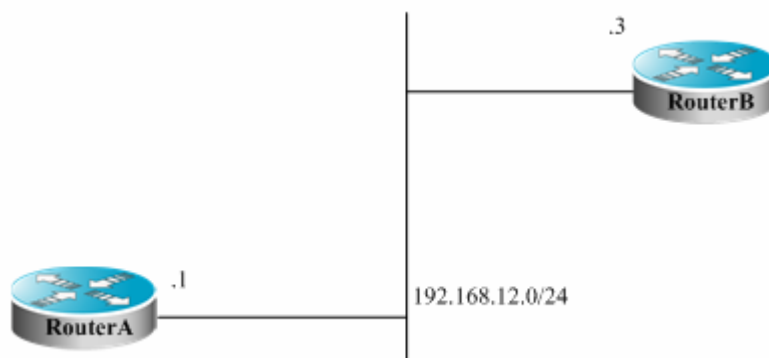
```
# 配置 RIP 路由协议
```

```
router rip
version 2
network 192.168.13.0
```

2.3.2 RIP认证配置例子

2.3.2.1 配置要求

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。设备之间连接图以及 IP 地址分配见下图。



RIP 认证配置例子

要求 Router A 发送 RIP 包的认证密钥为 Keya，可接收认证密钥为 Keya、Keyb 的 RIP 包；Router B 发送 RIP 包的认证密钥为 Keyb，可接收认证密钥为 Keya、Keyb 的 RIP 包。

2.3.2.2 设备具体配置

设备 A 的配置：

```
# 密钥串配置
```

```
key chain ripkey
key 1
key-string keya
key 2
key-string keyb

# 配置以太网端口

interface FastEthernet0/0
ip address 192.168.12.1 255.255.255.0
ip rip authentication mode md5
ip rip authentication key-chain ripkey

# 配置 RIP 路由协议

router rip
version 2
network 192.168.12.0
```

设备 B 的配置:

```
# 密钥串配置

key chain ripkey
key 1
key-string keyb
key 2
key-string keya

# 配置以太网端口

interface FastEthernet0/0
ip address 192.168.12.2 255.255.255.0
ip rip authentication mode md5
ip rip authentication key-chain ripkey

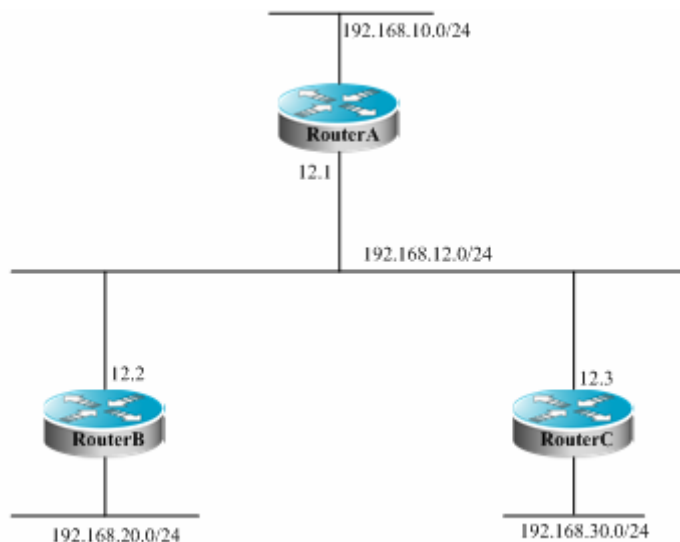
# 配置 RIP 路由协议

router rip
version 2
network 192.168.12.0
```

2.3.3 RIP报文单播配置例子

2.3.3.1 配置要求

三台设备全部连接在局域网上，并且全部运行 RIP 路由协议。设备 IP 地址分配和设备连接图见下图。



RIP 报文单播配置例子

通过 RIP 报文单播配置，要求实现以下目标：

- Router A 可以学到 Router C 通告的路由；
- Router C 学不到 Router A 通告的路由。

2.3.3.2 设备具体配置

为了实现以上配置要求，需要在设备 A 配置 RIP 报文单播。

设备 A 的配置：

配置以太网端口

```
interface FastEthernet0/0
ip address 192.168.12.1 255.255.255.0
```

配置回环端口

```
interface Loopback0
ip address 192.168.10.1 255.255.255.0
```

配置 RIP 路由协议

```
router rip
version 2
network 192.168.12.0
network 192.168.10.0
passive-interface FastEthernet0/0
neighbor 192.168.12.2
```

设备 B 的配置：

配置以太网端口

```
interface FastEthernet0/0
ip address 192.168.12.2 255.255.255.0

# 配置回环端口

interface Loopback0
ip address 192.168.20.1 255.255.255.0

# 配置 RIP 路由协议

router rip
version 2
network 192.168.12.0
network 192.168.20.0
```

设备 C 的配置:

```
# 配置以太网端口

interface FastEthernet0/0
ip address 192.168.12.3 255.255.255.0

# 配置回环端口

interface Loopback0
ip address 192.168.30.1 255.255.255.0

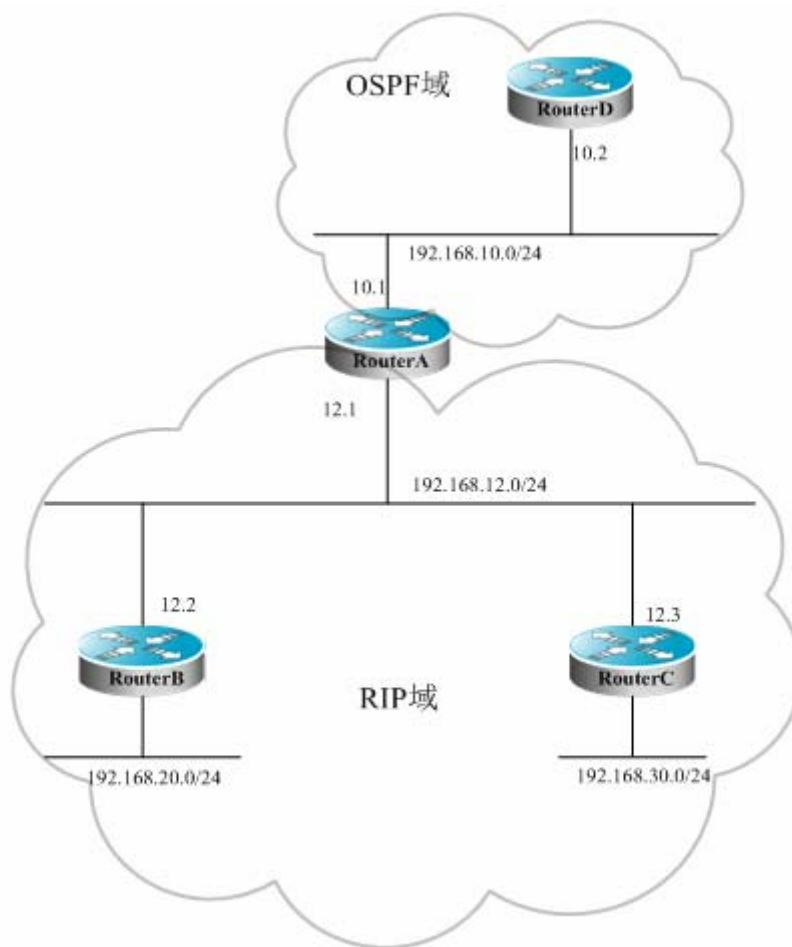
# 配置 RIP 路由协议

router rip
version 2
network 192.168.12.0
network 192.168.30.0
```

2.3.4 RIP重分发和缺省路由配置例子

2.3.4.1 配置要求

RouterA、RouterB、RouterC 连接在同一网段，运行 RIP 路由协议；RouterA 和 RouterD 连接在同一网段，运行 OSPF 路由协议。设备 IP 地址分配和设备连接图见下图。



RIP 重分发和缺省路由配置例子

分别配置四台设备，要求实现以下目标：

- Router A 可以学到 Router D 通告的 OSPF 路由；
- Router A 将 OSPF 路由重分发到 RIP
- Router A 向 Router B 和 Router C 通告重分发的路由
- Router C 向 Router A 和 Router B 通告缺省路由

2.3.4.2 设备具体配置

设备 A 的配置：

```
# 配置以太网端口
interface FastEthernet0/0
ip address 192.168.12.1 255.255.255.0
interface FastEthernet0/1
ip address 192.168.10.1 255.255.255.0

# 配置 RIP 路由协议
router rip
```

```
version 2
network 192.168.12.0
redistribute ospf 10 metric 3

# 配置 OSPF 路由协议

router ospf 10
network 192.168.10.0 0.0.0.255 area 0
```

设备 B 的配置:

```
# 配置以太网端口

interface FastEthernet0/0
ip address 192.168.12.2 255.255.255.0

# 配置回环端口

interface Loopback0
ip address 192.168.20.1 255.255.255.0
```

配置 RIP 路由协议

```
router rip
version 2
network 192.168.12.0
network 192.168.20.0
```

设备 C 的配置:

```
# 配置以太网端口

interface FastEthernet0/0
ip address 192.168.12.3 255.255.255.0
ip rip default-information originate metric 5

# 配置回环端口

interface Loopback0
ip address 192.168.30.1 255.255.255.0
```

配置 RIP 路由协议

```
router rip
version 2
network 192.168.12.0
network 192.168.30.0
```

设备 D 的配置:

```
# 配置以太网端口

interface FastEthernet0/0
ip address 192.168.10.2 255.255.255.0

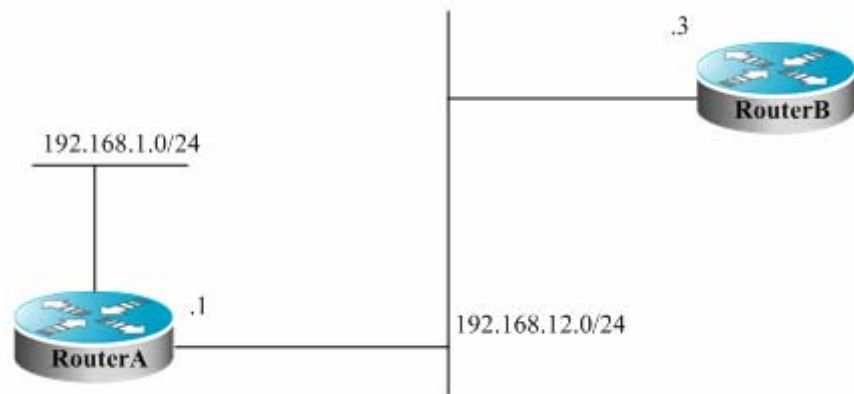
# 配置 OSPF 路由协议
```

```
router ospf 10
network 192.168.10.0 0.0.0.255 area 0
```

2.3.5 RIP超网路由配置例子

2.3.5.1 配置要求

两台设备通过以太网互连，Router A 运行 RIPv2，Router B 为只支持 RIPv1 协议的路由设备，无法支持超网路由的学习。设备之间连接图以及 IP 地址分配见 下图。



RIP 超网路由配置例子

要求：

- 在 Router 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；
- 将以上静态路由重分发到 RIP；
- 在 Router A 禁止通告超网路由。

2.3.5.2 设备具体配置

该配置范例中，Router 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，Router 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。为了避免这种情况的发生，需要在 Router A 上禁止通告超网路由。

设备 A 的配置：

配置以太网端口

```
interface FastEthernet0/0
ip address 192.168.12.1 255.255.255.0
no ip rip send supernet-routes
```

配置回环端口


```
interface loopback 1
ip address 192.168.1.1 255.255.255.0

# 配置静态路由

ip route 80.0.0.0 252.0.0.0 loopback 1

# 配置 RIP 路由协议

router rip
version 2
network 192.168.12.0
redistribute static
```

设备 B 的配置(只支持 RIPv1):

```
# 配置以太网端口

interface FastEthernet0/0
ip address 192.168.12.2 255.255.255.0

# 配置 RIP 路由协议

router rip
network 192.168.12.0
```

3 配置 OSPF 路由协议

3.1 OSPF简介

OSPF (Open Shortest Path First) 为 IETF OSPF 工作组开发的一种基于链路状态的内部网关路由协议。OSPF 是专为 IP 开发的路由协议，直接运行在 IP 层上面，协议号为 89，采用组播方式进行 OSPF 包交换，组播地址为 224.0.0.5（全部 OSPF 设备）和 224.0.0.6（指定设备）。

链路状态算法是一种与哈夫曼向量算法（距离向量算法）完全不同的算法，应用哈夫曼向量算法的传统路由协议为 RIP，而 OSPF 路由协议是链路状态算法的典型实现。与 RIP 路由协议对比，OSPF 除了算法上的不同，还引入了路由更新认证、VLSMs(可变长子网掩码)、路由汇聚等新概念。即使 RIPv2 做了很大的改善，可以支持路由更新认证、可变长子网掩码等特性，但是 RIP 协议还是存在两个致命弱点：1) 收敛速度慢；2) 网络规模受限制，最大跳数不超过 16 跳。OSPF 的出现克服了 RIP 的弱点，使得 IGP 协议也可以胜任中大型、较复杂的网络环境。

OSPF 路由协议利用链路状态算法建立和计算到每个目标网络的最短路径，该算法本身较复杂，以下简单地、概括性地描述了链路状态算法工作的总体过程：

- 初始化阶段，设备将产生链路状态通告，该链路状态通告包含了该设备全部链路状态；
- 所有设备通过组播的方式交换链路状态信息，每台设备接收到链路状态更新报文时，将拷贝一份到本地数据库，然后再传播给其它设备；
- 当每台设备都有一份完整的链路状态数据库时，设备应用 Dijkstra 算法针对所有目标网络计算最短路径树，结果内容包括：目标网络、下一跳地址、花费，是 IP 路由表的关键部分。

如果没有链路花费、网络增删变化，OSPF 将会十分安静，如果网络发生了任何变化，OSPF 通过链路状态进行通告，但只通告变化的链路状态，变化涉及到的设备将重新运行 Dijkstra 算法，生成新的最短路径树。

一组运行 OSPF 路由协议的设备，组成了 OSPF 路由域的自治域系统。一个自治域系统是指由一个组织机构控制管理的所有设备，自治域系统内部只运行一种 IGP 路由协议，自治域系统之间通常采用 BGP 路由协议进行路由信息交换。不同的自治域系统可以选择相同的 IGP 路由协议，如果要连接到互联网，每个自治域系统都需要向相关组织申请自治域系统编号。

当 OSPF 路由域规模较大时，一般采用分层结构，即将 OSPF 路由域分割成几个区域(AREA)，区域之间通过一个骨干区域互联，每个非骨干区域都需要直接与骨干区域连接。

在 OSPF 路由域中，根据设备的部署位置，有三种设备角色：

- 1) 区域内部设备，该设备的所有接口网络都属于一个区域；
- 2) 区域边界设备，也称为 ABR (Area Border Routers)，该设备的接口网络至少属于两个区域，其中一个必须为骨干区域；
- 3) 自治域边界设备，也称为 ASBR (Autonomous System Boundary Routers)，是 OSPF 路由域与外部路由域进行路由交换的必经之路。

锐捷产品对 OSPF 的实现完全遵循了 RFC 2328 中定义的 OSPF v2，以下列出了锐捷产品实现的 OSPF 的主要特性：

- 支持 OSPF 多进程，最多可以支持 64 个 OSPF 进程同时运行；
- 残域——完全支持残域的定义；
- 认证——支持邻居之间明文或者 MD5 的认证；
- 虚链路——支持虚链路；
- 可变长子网掩码 VLSMs 的支持；
- 区域的划分；
- NSSA（Not So Stubby Area），RFC 3101 定义；

3.2 OSPF配置任务列表

OSPF 的配置需要在各设备（包括内部设备、区域边界设备和自治系统边界设备等）之间相互协作。在未作任何配置的情况下，设备的各参数使用缺省值，此时，发送和接收报文都无须进行验证，接口也不属于任何一个自治系统的分区。在改变缺省参数的过程中，请务必保证各设备之间的配置相互一致。

为了配置 OSPF，需要完成的工作如下所列。其中，创建 OSPF 路由进程是必需的，其他选项可选，但也可能为特定的应用所必需。以下为 OSPF 路由协议的配置步骤：

- 创建 OSPF 路由进程(必须)
- 配置 OSPF 接口参数（可选）
- 配置 OSPF 以适应不同物理网络（可选）
- 配置 OSPF 区域参数（可选）
- 配置 OSPF NSSA（可选）
- 配置 OSPF 路由汇聚（可选）
- 创建虚拟链接（可选）
- 产生缺省路由（可选）
- 用 Loopback 地址做路由标识符（可选）
- 更改 OSPF 缺省管理距离（可选）
- 配置路由计算计时器（可选）
- 状态更新信息调整时间（可选）
- 配置 OSPF 接口度量（可选）
- 配置接口接收数据库描述报文时是否校验 MTU 值（可选）
- 配置禁止接口发送 OSPF 报文（可选）
- 配置 OSPF 容量保护（可选）
- 配置 OSPF 网管功能（可选）
- 监视和维护 OSPF

以下为 OSPF 的缺省配置：

功能特性	缺省值
网络接口	接口代价：不预设接口代价； LSA 重传间隔：5 秒； LSA 发送延迟：1 秒； hello 报文发送间隔：10 秒(对于非广播网络为 30 秒)； 邻接设备失效的时间：hello 报文发送间隔的四倍； 优先级：1； 认证类型：0 (无认证)； 认证密码：无。
区间	认证类型：0(无认证)； 进入 Stub 或 NSSA 区域的汇聚路由的缺省代价：1； 区间路由汇聚范围：未定义； 存根区间(STUB)：未定义； 不完全存根区间(NSSA)：未定义。
虚拟连接	未定义虚拟连接。 有关虚拟连接参数的缺省值： LSA 重传间隔：5 秒； LSA 发送延迟：1 秒； hello 报文发送间隔：10 秒； 邻接设备失效的时间：hello 报文发送间隔的四倍； 认证类型：无认证； 认证密码：无；
自动代价计算	打开； 缺省的自动代价参考是 100 Mbps；
缺省路由产生	关闭； 如果打开则缺省使用的 metric 是 1，类型是 type-2
缺省 metric (Default metric)	重分发其他路由协议所使用的缺省 metric；
管理距离	区间内路由信息：110 区间间路由信息：110 外部路由信息：110
数据库过滤	关闭，所有接口都可以接收状态更新信息 LSA
邻居变化日志记录	打开

邻居 (neighbor)	无
邻居数据库过滤	关闭, 输出的 LSA 发送到所有邻居;
区间网络范围 (network area)	无
设备 ID	未定义,缺省 ospf 协议没有运行
外部路由汇聚 (summary-address)	未定义
状态更新信息调整时间	240 秒
最短路径优先算法定时器	收到拓扑改变信息到下一次开始调用 SPF 算法计算的延迟时间: 1000 毫秒; 两次 SPF 计算之间的最小时间间隔: 5000 毫秒; 两次 SPF 计算之间的最大时间间隔: 10000 毫秒
计算外部路由时采用的最优路径的规则	采用 RFC1583 中的规则
内存不足情况下 OSPF 行为	进入 OVERFLOW 状态
OSPFv2 MIB 绑定	进程号最小的 OSPFv2 进程
OSPFv2 TRAP 发送	关闭

3.2.1 创建 OSPF 路由进程

创建 OSPF 路由进程, 并定义与该 OSPF 路由进程关联的 IP 地址范围, 以及该范围 IP 地址所属的 OSPF 区域。OSPF 路由进程只在属于该 IP 地址范围的接口发送、接收 OSPF 报文, 并且对外通告该接口的链路状态。目前我们支持 64 个 OSPF 路由进程。

要创建 OSPF 路由进程, 可以按照如下步骤进行 :

	命令	作用
Step 1	Ruijie # configure terminal	进入全局配置模式。
Step 2	Ruijie (config)# ip routing	启用路由功能(如果为关闭的话)
Step 3	Ruijie (config)# router ospf process_id	打开 OSPF, 进入 OSPF 配置模式
Step 4	Ruijie (config-router)# network address wildcard-mask area area-id	定义属于一个区间的地址范围;
Step 5	Ruijie (config-router)# end	退回到特权模式。
Step 6	Ruijie # show ip protocols	显示当前运行的路由协议。
Step 7	Ruijie # write	保存配置。

 说明

Network 命令中 32 个“比特通配符”与掩码的取值相反，取“1”代表不比较该比特位，“0”代表比较该比特位。不过用掩码的方式来定义，锐捷产品也会自动翻译成比特通配符。只有接口地址与 **network** 命令定义的 IP 地址范围相匹配，该接口才属于指定的区域。当接口地址同时与多个 OSPF 进程 **network** 命令定义的 IP 地址范围相匹配时，按照最优匹配方式，确定接口参与的 OSPF 进程。

使用命令 **no router ospf process-id** 关闭 OSPF 协议。以下为打开 OSPF 协议的示例：

```
Ruijie(config)# router ospf 1
Ruijie(config-router)# network 192.168.0.0 0.0.0.255 area 0
Ruijie(config-router)# end
```

3.2.2 配置 OSPF 接口参数

OSPF 允许用户更改某些特定的接口参数，用户可以根据实际应用的需要设置这些参数。应该注意的是，一些参数的设置必须保证与该接口相邻接的设备的相应参数一致，这些参数通过 **ip ospf hello-interval**，**ip ospf dead-interval**，**ip ospf authentication**，**ip ospf authentication-key** 和 **ip ospf message-digest-key** 五个接口参数进行设置，当使用这些命令时应该注意邻居设备也有同样的配置。

要配置 OSPF 接口参数，在接口配置模式中进行执行以下命令：

	命令	作用
Step 1	Ruijie# configure terminal	进入全局配置模式。
Step 2	Ruijie(config)# ip routing	启用路由功能(如果为关闭的话)
Step 3	Ruijie(config)# interface interface-id	进入接口配置模式。
Step 4	Ruijie(config-if)# ip ospf cost cost-value	(可选) 定义接口费用，
Step 5	Ruijie(config-if)# ip ospf retransmit-interval seconds	(可选) 设置链路状态重传间隔；
Step 6	Ruijie(config-if)# ip ospf transmit-delay seconds	(可选) 设置链路状态更新报文传输过程的估计时间；
Step 7	Ruijie(config-if)# ip ospf hello-interval seconds	(可选) 设置 hello 报文发送间隔，对于整个网络的节点，该值要相同；
Step 8	Ruijie(config-if)# ip ospf dead-interval seconds	(可选) 设置相邻设备失效间隔，对于整个网络的节点，该值必须相同；
Step 9	Ruijie(config-if)# ip ospf priority number	(可选) 优先级，用于选举指派设备 (DR) 和备份指派设备 (BDR)
Step10	Ruijie(config-if)# ip ospf authentication [message-digest null]	(可选) 设置接口的认证方式

Step11	Ruijie(config-if)# ip ospf authentication-key [0/7] key	(可选) 配置接口文本认证的密码,
Step12	Ruijie(config-if)# ip ospf message-digest-key keyid md5 [0/7] key	(可选) 配置接口的 MD5 加密认证的密码
Step13	Ruijie (config-if)# ip ospf database-filter all out	(可选) 阻止接口泛洪链路状态更新报文; 缺省情况下, OSPF 将接收的 LSA 信息从属于同一区间的所有接口上泛洪出去, 除了接收该 LSA 信息的接口;
Step14	Ruijie (config-if)# end	退回到特权模式。
Step15	Ruijie # show ip ospf [process-id]interface [interface-id]	显示当前运行的路由协议。
Step16	Ruijie # write	(可选) 保存配置。

使用以上命令的 **no** 模式, 可以取消原来的设置或者恢复缺省值。

3.2.3 配置OSPF以适应不同物理网络

根据不同的媒介的传输性质, OSPF 将网络分为三种类型:

- 广播网络 (以太网, 令牌环, FDDI)
- 非广播网络 (帧中继, X.25)
- 点到点网络 (HDLC, PPP, SLIP)

其中非广播网络, 根据 OSPF 的操作模式不同又分为两种子类型:

- 非广播多路访问网络(NBMA)类型。NBMA 要求所有互联的设备必须能够直接通讯, 只有全网状的连接才能达到该要求, 如果采用 SVC (比如 X.25) 连接没问题, 但是采用 PVC (如帧中继) 组网将有一定难度。OSPF 在 NBMA 网络上操作与广播网络上类似, 需要选举指定设备 (Designated Router), 并由指定设备通告 NBMA 网络的链路状态。
- 点到多点网络类型。如果网络拓扑结构不是全网状的非广播网络, OSPF 需要将该接口网络类型设置成点到多点网络类型。在点到多点网络类型中, OSPF 将所有的设备之间的连接看作点到点的链路, 所以没有指定设备的选举。

不管接口的缺省网络类型是什么, 都可以设置为广播网络类型。比如可以将非广播多路访问网络 (帧中继, X.25) 设置成广播网络, 这样在 OSPF 路由进程配置时, 省去了要配置邻居的步骤。通过 X.25 map 和 Frame-relay map 命令, 可以让 X.25 和帧中继网络具有广播的能力, 这样 OSPF 可以把 X.25 和帧中继这样的网络看作广播网络。

点到多点网络的接口可以看作是有一个或多个邻居的标识的点到点接口, 当 OSPF 配置成点到多点网络类型时, 会生成多个主机路由。点到多点网络类型与 NBMA 网络类型相比有以下好处:

- 容易配置, 不需要配置邻居, 也没有指定设备的竞选;
- 代价小, 不要求全网状拓扑。

要配置网络类型，在接口配置模式中执行以下命令：

	命令	作用
Step 1	Ruijie(config-if)# ip ospf network {broadcast non-broadcast point-to-point {point-to-multipoint [non-broadcast]}}	配置 OSPF 网络类型

对应于不同的链路封装类型,缺省情况下的网络类型如下：

■ 点到点网络类型

PPP、SLIP、帧中继点到点子接口、X.25 点到点子接口封装

■ NBMA 网络类型(non-broadcast)

帧中继、X.25 封装（点到点子接口除外）

■ 广播网络类型

以太网封装

■ 缺省类型没有为点到多点网络类型

配置时需要注意两端网络类型必须一致，否则可能出现邻居 FULL，但是路由计算错误的异常情况；

3.2.3.1 配置点到多点广播网络

当设备通过 X.25、帧中继网络互联时，不是全网状拓扑结构或者不想进行指定设备的选举时，就可以将 OSPF 接口网络类型设置为点到多点类型，由于点到多点网络类型将链路看作多个点到点链路，因此将产生多个主机路由。另外由于在点到多点网络中，所有的邻居花费都是一样的，如果要求每个邻居的花费不同，可以通过 neighbor 命令进行设置。

要设置点到多点网络类型，在接口配置模式中执行以下命令：

	命令	作用
Step 1	Ruijie(config-if)# ip ospf network point-to-multipoint	配置一个接口为点到多点广播网络类型
Step 2	Ruijie(config-if)# exit	退出到全局配置模式
Step 3	Ruijie(config)# router ospf 1	进入路由进程配置模式
Step 4	Ruijie(config-router)# neighbor ip-address cost cost	可选，指定邻居的花费

 说明

OSPF 点到多点类型网络虽然属于非广播网络，但是通过帧中继、X.25 映射手工配置或者自动学习，可以让非广播网络具有广播的能力。所以在配置点到多点网络类型时，可以不要指定邻居。

3.2.3.2 配置非广播网络

当 **ospf** 工作在非广播网络上时既可以配置成 **NBMA** 也可以配置成点到多点非广播类型。因为不具备广播能力所以无法动态的发现邻居，因此 **ospf** 工作于非广播网络上时必须手工为其配置邻居。

考虑到以下情况时，可以配置 **NBMA** 网络类型：

- 当一个非广播类型网络具有全网状拓扑结构；
- 可以将一个广播类型的网络设置成 **NBMA** 网络类型，这样可以减少广播报文的产生，节约网络带宽，也可以在一定的程度上避免随便的接收和发布路由。配置 **NBMA** 网络必须要指定邻居，由于有指定设备的选择，你可能需要明确哪台设备作为指定设备，这就需要配置优先级了，优先值越大就越有可能成为指定设备。

要配置 **NBMA** 网络类型，在接口配置模式中执行以下命令：

	命令	作用
Step 1	Ruijie (config-if)# ip ospf network non-broadcast	指定该接口的网络类型为 NBMA 类型
Step 2	Ruijie (config-if)# exit	退出到全局配置模式
Step 3	Ruijie (config)# router ospf 1	进入路由进程配置模式
Step 4	Ruijie(config-router)# neighbor ip-address [priority number] [poll-interval seconds]	指定邻居，并且指定它的优先级和 hello 的轮询间隔

当在一个非广播网络中，不能保证任意两台设备之间都是直接可达的话，更好的解决方法是将 **ospf** 的网络类型设置为点到多点非广播网络类型。

无论在点到多点广播或者非广播网络中，由于所有的邻居花费都是一样的，使用的花费都是使用 **ip ospf cost** 所配置的值.而实际上可能到每个邻居的带宽是不同的,因此花费也应该不同。因此可以通过 **neighbor** 命令为每个邻居指定所要的花费,这一点只适合点到多点类型（广播或者非广播）的接口。

在一个非广播网络中，如果要将接口配置成点到多点类型，在接口配置模式中执行以下命令：

	命令	作用
Step 1	Ruijie (config-if)# ip ospf network point-to-multipoint non-broadcast	指定该接口的网络类型为点到多点非广播 类型
Step 2	Ruijie (config-if)# exit	退出到全局配置模式
Step 3	Ruijie (config)# router ospf 1	进入路由进程配置模式
Step 4	Ruijie(config-router)# neighbor ip-address [cost number]	指定邻居，并且指定到该邻居的花费。

注意步骤 4，如果没有邻居指定花费，那么将使用接口配置模式下的 **ip ospf cost** 命令所参考的代价。

3.2.3.3 配置广播网络类型

OSPF 广播类型网络，需要选举指定设备（DR, Designated Router）和备份指定设备（BDR, Backup Designated Router），由指定设备对外通告该网络的链路状态。所有的设备之间都保持邻居关系，但是所有设备只与指定设备和备份指定设备之间保持邻接关系，也就是说每台设备只与指定设备和备份指定设备交换链路状态数据包，然后由指定设备通告给所有的设备，从而每台设备能够保持一致的链路状态数据库。

你可以通过 OSPF 优先级参数设置来控制指定设备的选举结果。但是参数设置并不能马上产生作用，影响当前的指定设备，只有在新一轮的选举中，设置的参数才会起作用。进行新一轮指定设备选举的唯一条件是：OSPF 邻居在一定时间内没有接收到指定设备的 HELLO 报文，认为指定设备宕机了。

要配置广播网络类型，在接口配置模式中执行以下命令

	命令	作用
Step 1	Ruijie(config-if)# ip ospf network broadcast	指定该接口的类型为广播网络类型
Step 2	Ruijie(config-if)# ip ospf priority priority	可选，指定该接口的优先级

3.2.4 配置OSPF区域参数

当你需要配置区域认证、残域、缺省汇聚路由花费时，就需要通过配置区域命令来实现。

配置区域认证是为了防止学到非认证、无效路由，以及避免通告有效路由到非认证设备，在广播类型网络中，区域认证还可以避免非认证设备成为指定设备的可能性，保证了路由系统的稳定性和抗入侵性。

当一个区域为 OSPF 路由域的叶区域，即该区域不作为过渡区域，也不会向 OSPF 路由域注入外部路由时，可以考虑将该区域配置为残域（Stub Area）。残域设备只能学到三种路由：1）残域内部路由；2）其它区域路由；3）残域边界设备通告的缺省路由。由于没有大量的外部路由，所以残域设备的路由表将很小，可以节约设备的资源，因此残域的设备可以为中低端设备。为了进一步减少发送到 Stub 区域中的链路状态广播（LSA）的数量可以将区域配置为全残域(配置 no-summary 选项)，全残域设备就只能学到两种路由：1）残域内部路由；2）残域边界设备通告的缺省路由。全残域的配置，使得 OSPF 占用设备资源最小化，提高了网络传输效率。

如果残域设备可以学到多条缺省路由，就需要对缺省路由的花费进行设置(通过 area default-cost 配置)，这样就可以控制残域设备优先使用指定的缺省路由。

配置 STUB 区域要注意以下几点：

- 骨干区域不能配置成 STUB 区域，不能将 STUB 区域作为虚拟连接的传输区域。
- Stub 区域内不能存在 ASBR，即自治系统外部的路由不能在本区域内传播。
- 如果想将一个区域配置成 STUB 区域，则该区域中的所有设备必须都要配置该属性。

用户可以使用 **no area area-id** 清除指定 OSPF 区域的配置并删除该区域，包括清除 **area authentication**、**area default-cost**、**area filter-list**、**area stub**、**area nssa** 等基于区域的配置命令。但在如下情况下，用户无法清除 OSPF 区域的配置：

- 1) 要清除主干区域的所有配置，但存在虚链路的配置。此时必须先清除虚链路配置，才能删除主干区域。
- 2) 任何一个区域，存在对应的 **network area** 命令。此时必须先清除所有加入该区域的网段命令，才能删除该区域。

配置 OSPF 区域参数，在路由进程配置模式下执行以下命令：

	命令	作用
Step 1	Ruijie (config-router)#area area-id authentication	区域认证方式设置为明文认证
Step 2	Ruijie (config-router)#area area-id authentication message-digest	区域认证方式设置为 MD5 认证
Step 3	Ruijie (config-router)#area area-id stub [no-summary]	将区域配置成残域 no-summary: 将该区域配置成全残域，阻止 Stub 区间上的 ABR 发送 summary-LSAs 信息进入 stub 区间
Step 4	Ruijie (config-router)#area area-id default-cost cost	配置发送到 STUB 区域的缺省路由的花费

 说明

认证的配置还需要在接口进行认证参数的配置，参见本章“配置 OSPF 接口参数”部分。残域的配置需要在该区域所有设备上配置；如果要配置成全残域，在残域基础配置上，只要在残域边界设备上配置全残域参数就行了，其它设备不要更改配置。

3.2.5 配置OSPF NSSA

NSSA(Not-So-Stubby Area)是 OSPF STUB 区域的一个扩展,NSSA 也通过阻止第 5 类 LSA(AS-external-LSA)向 NSSA 的泛洪来降低设备的资源的消耗,但是和 STUB 不同的是 NSSA 可以注入一定数量的自治系统外部的路由信息到 OSPF 的路由选择域。

通过重分发，NSSA 允许输入类型 7 的自治系统外部路由到 NSSA 区域,这些类型 7 的外部 LSA 在 NSSA 的区域边界设备上将被转换成类型 5 的 LSA 并且泛洪到整个自治系统，在转换过程中可以实现对外部路由的汇聚和过滤。

配置 NSSA 时要注意以下几点：

- 骨干区域不能配置成 NSSA，不能将 NSSA 作为虚拟连接的传输区域。
- 如果想将一个区域配置成 NSSA，所有连接到 NSSA 区域的设备必须使用 **area nssa** 命令将该区域配置成 NSSA 属性。

要配置区域成为一个 NSSA 区域，在路由进程配置模式中执行以下命令：

命令	作用

Step 1	Ruijie (config-router)# area area-id nssa [no-redistribution] [no-summary] [default-information-originate[metric metric][metric-type [1 2]]]	(可选) 定义一个 NSSA 区间;
Step 2	Ruijie (config-router)# area area-id default-cost cost	配置发送到 NSSA 区域的缺省路由的花费

参数 **default-information-originate** 用来产生默认的 Type-7 LSA, 该选项在 **nssa** 的 ABR 和 ASBR 上有些差别, 在 ABR 上无论路由表中是否存在缺省路由, 都会产生 Type-7 LSA 缺省路由, 在 ASBR 上(同时也不是 ABR)当路由表中存在缺省路由, 才会产生 Type-7 LSA 缺省路由。

参数 **no-redistribution** 在 ASBR 上使得 OSPF 通过 **redistribute** 命令引入的其它外部路由不发布到 NSSA 区。该选项通常用于 NSSA 的设备既是 ASBR 又是 ABR 的时候, 它可以阻止外部路由信息进入 **nssa**。

为了进一步减少发送到 NSSA 区域中的链路状态广播 (LSA) 的数量, 可以在 ABR 上配置 **no-summary** 属性, 禁止 ABR 向 NSSA 区域内发送 **summary LSAs** (Type-3 LSA)。

另外 **area default-cost** 用在连接该 NSSA 区域的边界设备 ABR 上。该命令配置区域边界设备发送到 NSSA 区域的缺省路由的花费值。缺省情况下, 发送到 NSSA 区域缺省路由的花费值为 1。

3.2.6 配置OSPF路由汇聚

3.2.6.1 配置区间路由汇聚

区域边界设备(Area Border Routers)至少有两个接口属于不同的区域, 而且其中一个区域一定为骨干区域。区域边界设备在 OSPF 路由域中起着枢纽作用, 可以将一个区域的路由通告到其它区域, 如果该区域的路由网络地址是连续的, 则区域边界设备可以只通告一个汇聚路由到其它区域。区域之间的路由汇聚大大缩减了路由表的规模, 提高了网络工作效率。

要配置区域之间路由汇聚, 在路由进程配置模式中执行以下命令:

	命令	作用
Step 1	Ruijie (config-router)# area area-id range ip-address mask [advertise not-advertise] [cost cost]	配置区间路由汇聚



如果配置了路由汇聚, 落在该范围的详细路由将不再被区域边界设备通告到其它区域。

3.2.6.2 配置外部路由汇聚

当路由从其它路由进程重新分布，注入 OSPF 路由进程时，每条路由均分别单独以一个外部链路状态的方式通告给 OSPF 设备。如果注入的路由是一个连续的地址空间，自治域边界设备也可以只通告一个汇聚路由，从而大大减小路由表的规模。

要配置外部路由汇聚，在路由进程配置模式中执行以下命令：

	命令	作用
Step 1	Ruijie (config-router)# summary-address <i>ip-address mask {not-advertise tag tag-id}</i>	配置外部汇聚路由

3.2.6.3 配置汇聚路由表项添加到核心路由表的控制

在路由汇聚时，汇聚后的范围有可能超出路由表中实际的网络范围，如果数据发往汇聚范围内不存在的网络，将有可能发生路由环路或加重路由设备的处理负担。为阻止这种情况的发生，需要在 ABR 或 ASBR 添加一条 discard 路由到路由表。

要允许或禁止 discard 路由添加到路由表，在路由进程配置模式中执行以下命令：

	命令	作用
Step 1	Ruijie (config-router)# discard-route {internal external}	允许 discard 路由添加到路由表
Step 2	Ruijie (config-router)# no discard-route {internal external}	禁止 discard 路由添加到路由表

缺省情况下，允许 discard 路由添加到路由表。

3.2.7 创建虚拟链接

在 OSPF 路由域中，非骨干区域之间的 OSPF 路由更新是通过骨干区域来交换完成的，所有的区域都必须与骨干域连接，如果骨干域断接，就需要配置虚拟链接将骨干域接续起来，否则网络通讯将出现问题。如果由于网络拓扑结构的限制可能无法保证物理上连通，也可以通过创建虚连接来满足这一要求。

虚拟链接需要在两个区域边界设备 (ABR) 之间创建，两个 ABR 共同所属的区域成为过渡区域。残域 (Stub Area) 和 NSSA 区域是不能作为过渡区域的。虚连接可以看成是在两台 ABR 之间通过传输区域建立的一条逻辑上的连接通道，它的两端必须是 ABR，而且必须在两端同时配置方可生效。虚连接由对端设备的 router-id 号来标识。为虚连接两端提供一条非骨干区域内部路由的区域称为传输区域 (Transit Area)，其区域号也必须在配置时指明。

虚连接要在传输区域内的路由计算出来后(到达对方设备的路由算出来)才会被激活，可以看成是一条点到点的连接，在这个连接上，和物理接口一样可以配置接口的多数参数，如 hello-interval, dead-interval 等。

“逻辑通道”是指两台 ABR 之间的多台运行 OSPF 的设备，只是起到一个转发报文的作用（由于协议报文的目的地址不是这些设备，所以这些报文对于他们而言是透明的，只是当作普通的 IP 报文来转发），两台 ABR 之间直接传递路由信息。这里的路由信息是指由 ABR 生成的 type3 的 LSA，区域内的设备同步方式没有因此改变。

要建立虚拟链接，在路由进程配置模式中执行以下命令：

	命令	作用
Step 1	Ruijie (config-router)# area area-id virtual-link router-id <i>[[hello-interval seconds]]</i> <i>[retransmit-interval seconds] [[transmit-delay seconds]]</i> <i>[[dead-interval seconds]]</i> <i>[authentication [message-digest null]]</i> <i>[[[authentication-key [0 7] key message-digest-key keyid md5 [0 7] key]]]</i>	创建一个虚拟连接

注意

如果自治系统被划分成一个以上的区域，则必须有一个区域是骨干区域，并且保证其它区域与骨干区域直接相连或逻辑上相连，且骨干区域自身也必须是连通的。

说明

router-id 为 OSPF 邻居设备标识符，如果不确定 router-id 的值，请用 **show ip ospf** 命令进行确认或通过 **show ip ospf neighbor** 命令查看邻居的 router-id。如何手工配置 router-id，请参考本章“用 Loopback 地址做路由标识符”部分内容。

3.2.8 产生缺省路由

一个自治域系统边界设备(ASBR)，可以强迫其产生一条缺省路由注入到 OSPF 路由域中。如果一个设备强制产生缺省路由，该设备就自动成为 ASBR。但是 ASBR 不会自动产生缺省路由的。

要强制 ASBR 产生缺省路由，在路由进程配置模式下执行以下命令：

	命令	作用
Step 1	Ruijie (config-router)# default-information originate <i>[always] [metric metric-value]</i> <i>[metric-type type-value] [route-map map-name]</i>	配置产生缺省路由

说明

当配置残域时，区域边界设备将自动产生缺省路由，然后通告到残域中的所有设备。

3.2.9 用Loopback地址做路由标识符

OSPF 路由进程总是用最大的接口 IP 地址作为设备标识符，如果该接口关闭或者该 IP 地址不存在了，OSPF 路由进程必须重新计算路由标识符并发送所有的路由信息给邻居。

如果配置了 Loopback（本地环路地址），则路由进程会选择 Loopback 接口的 IP 地址作为设备标识符。如果有多个 Loopback 接口，则选择 IP 地址最大的地址作为设备标识符。由于 Loopback 地址会永久存在，增强了路由表的稳定性。

要配置 Loopback 地址，在全局配置模式下，执行以下命令：

	命令	作用
Step 1	Ruijie (config)# interface loopback 1	创建 Loopback 接口
Step 2	Ruijie (config-if)# ip address ip-address mask	配置 Loopback IP 地址

说明

若 OSPF 路由进程已经选举了普通接口的 IP 地址为路由标识符时，此时配置 loopback 口不会导致 OSPF 进程重新选举标识符。

3.2.10 更改OSPF缺省管理距离

路由管理距离，代表着该路由来源的可信度。管理距离是一个 0~255 之间的数值，管理距离值越大，说明该路由来源可信度越低。

我司产品的 OSPF 有三大类路由，管理距离缺省值均为 110：区域内部，区域之间，外部。属于一个区域的路由称为区域内部路由，到另一个区域的路由称为区域之间路由，到其它路由域（通过重新分布学到）的路由称为外部路由。

要更改 OSPF 管理距离，在路由进程配置模式下执行以下命令：

	命令	作用
Step 1	Ruijie(config-router)# distance {distance ospf { intra-area distance inter-area distance external distance }}	更改 OSPF 管理距离值

3.2.11 配置路由计算计时器

在 OSPF 路由进程接收到网络拓扑变化的通知后，会延迟一段时间，然后运行 SPF 进行路由运算。该延时是可以配置的，另外还可以配置两次 SPF 运算之间最小的时间间隔、最大时间间隔。

要配置 OSPF 路由计算的计时器，在路由进程配置模式下执行以下命令：

命令	作用

Step 1	Ruijie (config-router)# timers throttle spf <i>spf-delay spf-holdtime spf-max-waittime</i>	配置路由计算计时器

说明

spf-delay 表示从拓扑发生变化到 SPF 开始计算，至少需要延迟的时间。第一次触发 SPF 计算到第二次触发 SPF 计算的最小时间间隔为 **spf-holdtime**，此后，连续触发 SPF 计算的时间间隔至少为上一次时间间隔的两倍，当时间间隔达到 **spf-max-waittime** 之后，将不再增加。如果两次 SPF 计算的时间间隔已经超过了要求的最小值，那么 SPF 计算时间间隔将重新从 **spf-holdtime** 开始计算。

在正常情况，只是链路偶尔动荡时，减少 **spf-delay** 和 **spf-holdtime** 值，可以加快 OSPF 收敛速度；**spf-max-waittime** 设置为较大值，可以防止链路连续动荡导致的 OSPF 消耗大量 CPU 的情况。

举例配置值为（**timers throttle spf 1000 5,000 100,000**）：

若拓扑连续变化，则 SPF 计算时间分别为(SPF 计算时间间隔以二进制指数退避算法递增，但最大不超过 **max-wait-time**)：

1s, 6s, 16s, 36s, 76s, 156s, 256s, 256+100, ...

如果只需要配置 OSPF 路由计算的延迟时间和保持时间，可以在路由进程配置模式下执行以下命令：

	命令	作用
Step 1	Ruijie (config-router)# timers spf <i>spf-delay</i> <i>spf-holdtime</i>	配置路由计算计时器，此命令以秒为单位

注意

timers spf 与 **timers throttle spf** 两个配置命令会互相覆盖，后配置的命令生效，当两个命令都未配置时，此时系统的缺省行为是 **timers throttle spf** 的缺省值。

timers throttle spf 命令功能已经包含了 **timers spf** 命令的功能，并且更加强大；建议用户使用 **timer throttle spf** 命令。

3.2.12 状态更新信息调整时间

每个 LSA 都有自己的更新和老化的时间(LSA age)，如果对每个 LSA 都独立进行 LSA 的更新和老化计算，将消耗 CPU 大量的资源。为了有效利用 CPU 资源，将设备内 LSA 进行统一的更新和老化操作。

更新老化操作的缺省设置为 4 分钟，可以通过本命令修改该缺省值。该参数并不需要经常调整。最佳的时间是与路由设备有多少 LSA 需要计算成反比的。比如，数据库中有 10000 条 LSA，降低步调间隔将使你受益；如果只有 40~100 条，则调整到 10~20 分钟可能会更好。

在路由进程配置模式下执行以下命令：

	命令	作用
Step 1	Ruijie # configure terminal	进入全局配置模式
Step 2	Ruijie (config)# router ospf 1	打开 OSPF，进入 OSPF 配置模式

Step 3	Ruijie (config-router)# timers lsa-group-pacing seconds	(可选) 改变步调时间
Step 4	Ruijie (config-router)# end	退回到特权模式。
Step 5	Ruijie # show running-config	验证设置内容是否正确
Step 6	Ruijie # write	(可选) 保存配置。

使用 `no timers lsa-group-pacing` 命令将取消设置使其恢复使用缺省值。

3.2.13 配置OSPF接口度量

OSPF 利用度量 (Cost) 计算目的路径, Cost 最小者即为最短路径。缺省的路由度量是基于网络带宽的。在配置 OSPF 设备时还可根据实际情况, 如链路带宽、时延或经济上的费用, 设置链路度量大小。度量越小, 则该链路被选为路由的可能性越大。如果发生路由汇聚, 则使用汇聚的所有链路的度量最大值作为整个汇聚信息的度量。

路由选择的配置有两个部分。首先可以设置带宽产生度量的参考值, 该值与接口带宽值一起计算生成缺省度量。其次, 可以通过接口配置命令 `ip ospf cost` 设置每个接口各自的度量值, 此时缺省度量对该接口就不产生作用了。比如, 缺省的参考值为 100Mbps, 一个以太网接口带宽为 10Mbps, 则该接口缺省的度量为 $100/10 + 0.5 \approx 10$ 。

在协议内部是这样选择接口代价的, 用户设置的接口的代价优先级最高, 如果用户设置了接口的代价, 则选取该值作为接口代价, 如果没有设置而自动代价功能是打开的则将根据自动代价计算出来的值作为接口的代价, 如果自动代价功能也关闭了则将使用缺省值 10 作为接口的代价。

配置过程如下:

	命令	作用
Step 1	Ruijie # configure terminal	进入全局配置模式。
Step 2	Ruijie (config)# router ospf 1	打开 OSPF, 进入 OSPF 配置模式
Step 3	Ruijie(config-router)# auto-cost reference-bandwidth ref-bw	(可选) 根据接口带宽设置缺省度量, 度量值根据 ref-bw 确定;
Step 4	Ruijie (config-router)# end	退回到特权模式。
Step 5	Ruijie # show ip protocols	显示当前运行的路由协议。
Step 6	Ruijie # write	(可选) 保存配置。

使用命令 `no auto-cost` 与 `no ip ospf cost` 取消设置内容。

3.2.14 配置接口接收数据库描述报文时是否校验MTU值

OSPF 在收到数据库描述报文时会校验邻居的接口的 MTU 和自己接口的 MTU 是否相同, 如果收到的数据库描述报文中指示的接口的 MTU 大于接收接口的 MTU, 那么邻接关系将不能被建立, 此

时可以通过关闭 MTU 的校验来解决。要关闭某个接口的 MTU 校验可以在接口模式下执行如下命令：

	命令	作用
Step 1	Ruijie (config-if)# ip ospf mtu-ignore	关闭该接口在收到数据库描述报文时对 MTU 进行校验

缺省情况下，接口的 MTU 校验功能是打开的。

3.2.15 配置禁止接口发送 OSPF 报文

为了防止网络中的其他设备动态的学习到本设备的路由信息，可以将本设备的指定网络接口设为被动接口，通过使用 **passive-interface** 命令来禁止在此接口上发送 OSPF 报文。

在特权模式下，用户可以按如下步骤进行被动口的配置：

	命令	作用
Step 1	Ruijie# configure terminal	进入全局配置模式。
Step 2	Ruijie(config)# router ospf 1	进入路由协议配置模式
Step 3	Ruijie(config-router)# passive-interface interface-name	(可选)将指定的网络接口设为被动。
Step 4	Ruijie(config-router)# passive-interface default	(可选)设置所有的网络接口为被动
Step 5	Ruijie(config-router)# end	退回到特权模式。
Step 6	Ruijie# write	保存配置

缺省情况下，允许所有接口收发 OSPF 报文。如果要想网络接口重新发送路由信息，则可以使用 **no passive-interface interface-id** 命令进行设置。如果使用参数 **default** 则是对所有的接口进行设置。

3.2.16 配置 OSPF 容量保护

内存不足情况下，允许 OSPF 进入 OVERFLOW 状态。OVERFLOW 状态是指在该状态下，OSPF 协议将触发如下行为：

- 对于学习到的 LSA：对于表示区内区间拓扑的 LSA，需要接收；对于外部 LSA，如果 LSA 所表示的路由目的地址为已经学习到的某条非缺省路由的精细路由，则接收；其他情况，LSA 不接收。
- 对于自身成的外部 LSA：清除除表示缺省路由外的其他外部 LSA。
- 由于路由学习和通告的不完整性，可能会引起网络出现路由环路的现象，为了减少出现这种现象的产生，OSPF 会生成一条指向 NULL 口的缺省路由，该路由在 OVERFLOW 状态下将一直存在。

设置内存不足时 OSPF 进入 OVERFLOW 状态的配置步骤如下：

	命令	作用
Step 1	Ruijie(config)# router ospf process-id	进入 OSPF 配置模式
Step 2	Ruijie(config-router)# overflow memory-lack	设置内存不足时 OSPF 进入 OVERFLOW 状态
说明 缺省情况下，内存不足将自动进入 OVERFLOW 状态，如果用户不希望进入 OVERFLOW 状态，可以使用 no overflow memory-lack 命令关闭该功能。		
注意 在进入 OVERFLOW 状态后，目前 OSPF 协议只支持使用 clear ip ospf process 命令，或者关闭再重新启动 OSPF 协议的方式退出 OVERFLOW 状态。		

3.2.17 配置 OSPF 网管功能

3.2.17.1 配置 OSPFv2 MIB 绑定

由于 OSPFv2 MIB 本身没有 OSPFv2 进程信息，所以用户通过 SNMP 操作 OSPFv2 进程，只能操作唯一的进程。缺省情况下，OSPFv2 MIB 绑定在进程号最小的 OSPFv2 进程上，用户的操作都对该进程生效。

如果用户希望能够通过 SNMP 操作指定的 OSPFv2 进程，可以通过手工配置的方式将 OSPFv2 MIB 绑定该进程上。

在路由进程配置模式下执行以下命令：

	命令	作用
Step 1	Ruijie# configure terminal	进入全局配置模式。
Step 2	Ruijie(config)# router ospf 1	进入路由协议配置模式。
Step 3	Ruijie(config-router)# enable mib-binding	(可选) 配置将 OSPFv2 MIB 绑定到指定的 OSPFv2 进程上。
Step 4	Ruijie(config-router)# end	退回到特权模式。
Step 5	Ruijie# write	保存配置。

3.2.17.2 配置 OSPFv2 TRAP 绑定

OSPFv2 协议定义了多种类型的 TRAP 信息，用于报告 OSPFv2 协议内部发生的各类事件。OSPFv2 TRAP 信息的发送不受 OSPFv2 进程绑定 MIB 的限制，允许不同进程同时打开 TRAP 开关。

在全局配置模式下，按照如下步骤执行：

	命令	作用
Step 1	Ruijie# configure terminal	进入全局配置模式。
Step 2	Ruijie(config)# snmp-server enable traps ospf	(可选) 打开 OSPF TRAP 发送开关。
Step 3	Ruijie(config)# router ospf 1	进入路由协议配置模式
Step 4	Ruijie(config-router)# enable traps [error [IfAuthFailure IfConfigError IfRxBadPacket VrtIfAuthFailure VrtIfConfigError VrtIfRxBadPacket] lsa [LsdbApproachOverflow LsdbOverflow MaxAgeLsa OriginateLsa] retransmit [IfTxRetransmit VrtIfTxRetransmit] state-change [IfStateChange NbrRestartHelperStatusChange NbrStateChange RestartStatusChange VrtIfStateChange VrtNbrRestartHelperStatusChange VrtNbrStateChange]]	(可选) 配置打开指定的 OSPF TRAP 开关
Step 5	Ruijie(config-router)# end	退回到特权模式。
Step	Ruijie# write	保存配置

3.2.18 监视和维护 OSPF

可以显示 OSPF 的路由表，缓存，数据库等数据。下表列出了部分具体可以显示的内容供参考。

	命令	作用
Step 1	Ruijie# show ip ospf [process-id]	显示相应进程 OSPF 协议的一般信息，未指定进程号则显示所有进程。
Step 2	Ruijie# show ip ospf [process-id area-id] database [adv-router ip-address {asbr-summary external network nssa-external opaque-area opaque-as opaque-link router summary} [link-state-id] [{adv-router ip-address self-originate}] database-summary max-age self-originate]	OSPF 数据库的信息 可以看指定进程每种 LSA 类型的信息。
Step 3	Ruijie# show ip ospf [process-id] border-routers	查看指定进程到达 ABR 与 ASBR 路由信息
Step 4	Ruijie# show ip ospf interface [interface-name]	查看参与 ospf 路由的接口信息

Step 5	Ruijie# show ip ospf [process-id] neighbor [interface-name] [neighbor-id] [detail]	接口相邻设备的信息 interface-name: 与该 neighbor 相连的本地接口。 neighbor-id: neighbor 的设备 ID
Step 6	Ruijie# show ip ospf [process-id] virtual-links ip-address	查看指定进程虚拟连接信息
Step 7	Ruijie# show ip ospf [process-id] route [count]	显示 OSPF 路由表路由

具体的命令解释，请参见 OSPF 命令参考中对各条命令的解释。常用的监视和维护命令有以下几个：

1) 显示 OSPF 邻居状态

使用 **show ip ospf [process-id] neighbor** 显示 OSPF 进程的所有邻居信息，包括邻居的状态、角色、设备标识、IP 地址、BFD 状态等。

Ruijie # **show ip ospf neighbor**

OSPF process 1:

Neighbor ID Address	Pri	State Interface	BFD State	Dead Time
10.10.10.50	1	Full/DR	Up	00:00:38
10.10.10.50		eth0/0		

OSPF process 100:

Neighbor ID Address	Pri	State Interface	BFD State	Dead Time
10.10.11.50	1	Full/Backup	Down	00:00:31
10.10.11.50		eth0/1		

Ruijie # **show ip ospf 1 neighbor**

OSPF process 1:

Neighbor ID Address	Pri	State Interface	BFD State	Dead Time
10.10.10.50	1	Full/DR	Up	00:00:38
10.10.10.50		eth0		

Ruijie # **show ip ospf 100 neighbor**

OSPF process 100:

Neighbor ID Address	Pri	State Interface	BFD State	Dead Time
10.10.11.50	1	Full/Backup	Down	00:00:31
10.10.11.50		eth1		

2) 显示 OSPF 接口状态

以下显示表明 F0/1 端口属于 OSPF 的区域 0，设备标识符为 172.16.120.1，网络类型为“BROADCAST”—广播类型。要特别注意 Area、Network Type、Hello、Dead 等参数，如果这些参数与邻居不一致，将不会建立邻居关系。

```
Ruijie#sh ip ospf interface fastEthernet 1/0
FastEthernet 1/0 is up, line protocol is up
Internet Address 192.168.1.1/24, Ifindex: 2 Area 0.0.0.0, MTU 1500
Matching network config: 192.168.1.0/24
Process ID 1, Router ID 192.168.1.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 192.168.1.1, Interface Address 192.168.1.1
Backup Designated Router (ID) 192.168.1.2, Interface Address 192.168.1.2
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:04
Neighbor Count is 1, Adjacent neighbor count is 1
Crypt Sequence Number is 30
Hello received 972 sent 990, DD received 3 sent 4
LS-Req received 1 sent 1, LS-Upd received 10 sent 26
LS-Ack received 25 sent 7, Discarded 0
```

3) 显示 OSPF 路由进程信息

以下命令可以显示路由标识符，设备类型，区域的信息，区域汇聚的信息等。

```
Ruijie# show ip ospf
Routing Process "ospf 1" with ID 1.1.1.1
Process uptime is 4 minutes
Process bound to VRF default
Conforms to RFC2328, and RFC1583Compatibility flag is enabled
Supports only single TOS(TOS0) routes
Supports opaque LSA
This router is an ASBR (injecting external routing information)
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
LsaGroupPacing: 240 secs
Number of incoming current DD exchange neighbors 0/5
Number of outgoing current DD exchange neighbors 0/5
Number of external LSA 4. Checksum 0x0278E0
Number of opaque AS LSA 0. Checksum 0x000000
Number of non-default external LSA 4
External LSA database is unlimited.
Number of LSA originated 6
Number of LSA received 2
Log Neighbor Adjency Changes : Enabled
Graceful-restart disabled
Graceful-restart helper support enabled
Number of areas attached to this router: 1
Area 0 (BACKBONE)
Number of interfaces in this area is 1(1)
Number of fully adjacent neighbors in this area is 1
```

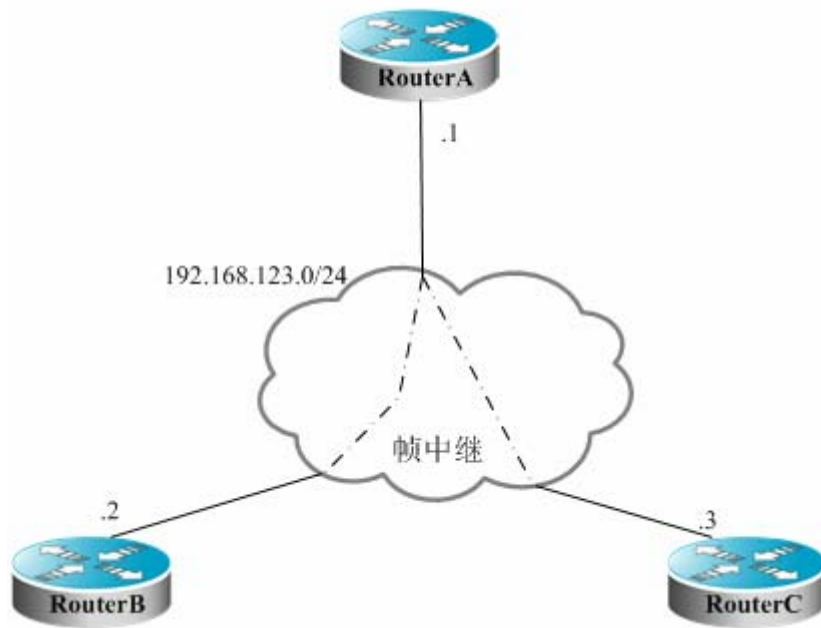
```
Area has no authentication
SPF algorithm last executed 00:01:26.640 ago
SPF algorithm executed 4 times
Number of LSA 3. Checksum 0x0204bf
Routing Process "ospf 20" with ID 2.2.2.2
Process uptime is 4 minutes
Process bound to VRF default
Conforms to RFC2328, and RFC1583Compatibility flag is enabled
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
LsaGroupPacing: 240 secs
Number of incoming current DD exchange neighbors 0/5
Number of outgoing current DD exchange neighbors 0/5
Number of external LSA 0. Checksum 0x000000
Number of opaque AS LSA 0. Checksum 0x000000
Number of non-default external LSA 0
External LSA database is unlimited.
Number of LSA originated 0
Number of LSA received 0
Log Neighbor Adjacency Changes : Enabled
Number of areas attached to this router: 0
```

3.3 OSPF配置范例

3.3.1 OSPF NBMA网络类型配置例子

3.3.1.1 配置要求

三台设备要通过帧中继网络实现网状全连接，每台设备只有一条帧中继线路，线路带宽和 PVC 速率全部一样。IP 地址分配和设备连接图见下图。



OSPF NBMA 网络类型配置例子

要求：

- 设备 A、B、C 之间配置 NBMA 类型网络；
- 设备 A 为指定设备，设备 B 为备份指定设备；
- 全部网络都在一个区域内；
- 加快拓扑收敛。

3.3.1.2 设备具体配置

由于 OSPF 没有特殊配置，将采用组播方式自动发现邻居，如果接口配置了 NBMA 网络类型，该接口就不会发 OSPF 组播报文，因此需要指定邻居的 IP 地址。可以通过设置较短的 SPF 计算等待时间来加快拓扑收敛。

设备 A 的配置：

配置广域网端口

```
interface Serial 1/0
ip address 192.168.123.1 255.255.255.0
encapsulation frame-relay
ip ospf network non-broadcast
ip ospf priority 10
```

配置 OSPF 路由协议，到设备 B 的花费更小

```
router ospf 1
network 192.168.123.0 0.0.0.255 area 0
neighbor 192.168.123.2 priority 5
neighbor 192.168.123.3
```



```
timers throttle spf 500 1000 10000
```

设备 B 的配置:

配置广域网端口

```
interface Serial 1/0
ip address 192.168.123.2 255.255.255.0
encapsulation frame-relay
ip ospf network non-broadcast
ip ospf priority 5
```

配置 OSPF 路由协议

```
router ospf 1
network 192.168.123.0 0.0.0.255 area 0
neighbor 192.168.123.1 priority 10
neighbor 192.168.123.3
timers throttle spf 500 1000 10000
```

设备 C 的配置:

配置广域网端口

```
interface Serial 1/0
ip address 192.168.123.3 255.255.255.0
encapsulation frame-relay
ip ospf network non-broadcast
```

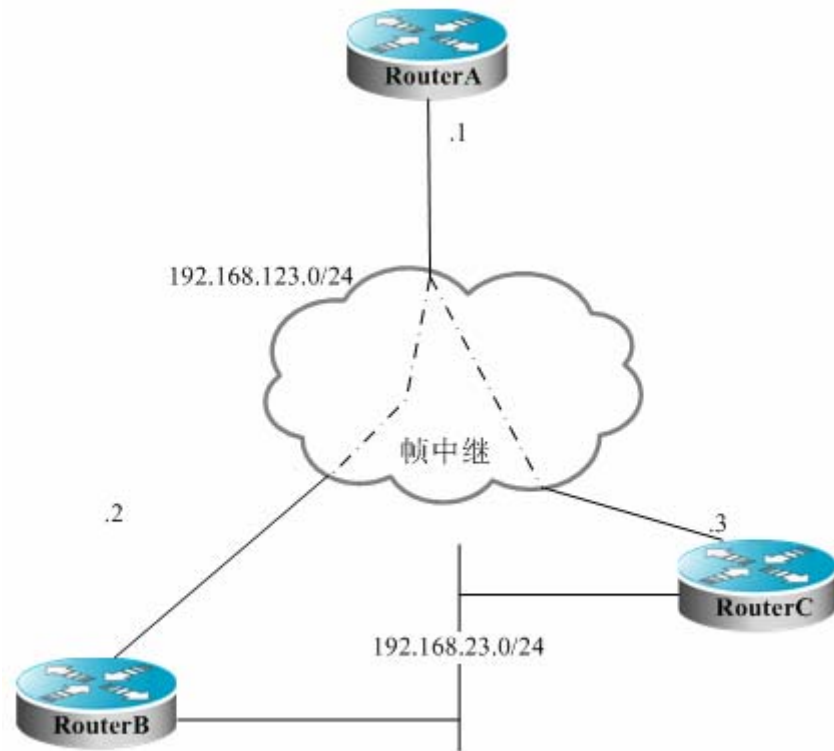
配置 OSPF 路由协议

```
router ospf 1
network 192.168.123.0 0.0.0.255 area 0
neighbor 192.168.123.1 10
neighbor 192.168.123.2 5
timers throttle spf 500 1000 10000
```

3.3.2 OSPF点到多点广播网络类型配置例子

3.3.2.1 配置要求

三台设备要通过帧中继网络实现互联，每台设备只有一条帧中继线路，线路带宽和 PVC 速率全部一样。IP 地址分配和设备连接图见下图。



OSPF 点到多点网络类型配置例子

要求：

- 设备 A 与 B、C 之间配置点到多点类型网络。

3.3.2.2 设备具体配置

如果接口配置了点到多点网络类型，点到多点网络类型没有竞选指定设备的过程，OSPF 操作与点到点网络类型的行为很类似。

设备 A 的配置：

配置以太网端口

```
interface FastEthernet 0/0
ip address 192.168.12.1 255.255.255.0
```

配置广域网端口

```
interface Serial 1/0
ip address 192.168.123.1 255.255.255.0
encapsulation frame-relay
ip ospf network point-to-multipoint
```

配置 OSPF 路由协议

```
router ospf 1
network 192.168.12.0 0.0.0.255 area 0
```

```
network 192.168.123.0 0.0.0.255 area 0
```

设备 B 的配置:

配置以太网端口

```
interface FastEthernet 0/0  
ip address 192.168.23.2 255.255.255.0
```

配置广域网端口

```
interface Serial 1/0  
ip address 192.168.123.2 255.255.255.0  
encapsulation frame-relay  
ip ospf network point-to-multipoint
```

配置 OSPF 路由协议

```
router ospf 1  
network 192.168.23.0 0.0.0.255 area 0  
network 192.168.123.0 0.0.0.255 area 0
```

设备 C 的配置:

配置以太网端口

```
interface FastEthernet 0/0  
ip address 192.168.23.3 255.255.255.0
```

配置广域网端口

```
interface Serial 1/0  
ip address 192.168.123.3 255.255.255.0  
encapsulation frame-relay  
ip ospf network point-to-multipoint
```

配置 OSPF 路由协议

```
router ospf 1  
network 192.168.23.0 0.0.0.255 area 0  
network 192.168.123.0 0.0.0.255 area 0
```

在上图的配置中假设还有一个需求是:

设备 A 到 192.168.23.0/24 目标网络将优先选择设备 B; 要达到优先选路的要求, 必须在配置邻居时设置该邻居的花费.

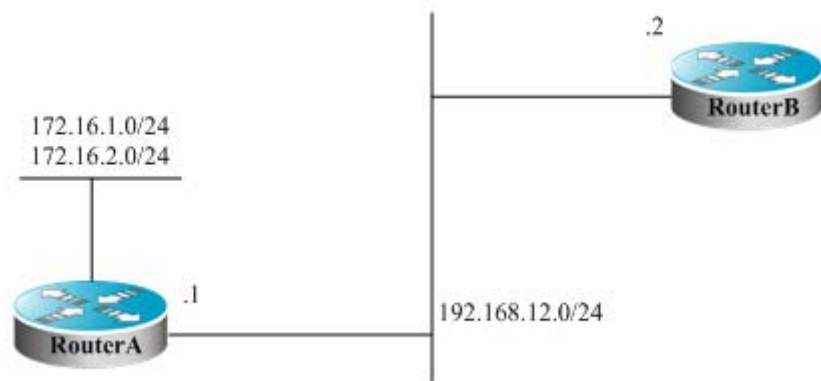
可以在设备 A 中配置如下命令:

```
router ospf 1  
neighbor 192.168.123.2 cost 100  
neighbor 192.168.123.3 cost 200
```

3.3.3 OSPF认证配置例子

3.3.3.1 配置要求

两台设备通过以太网互连，运行 OSPF 路由协议，采用 MD5 认证方式。设备之间连接图以及 IP 地址分配见下图。



OSPF 认证配置例子

3.3.3.2 设备具体配置

OSPF 的认证配置有两个地方：

- 1) 路由配置模式中，指定区域的认证方式；
- 2) 在接口中配置认证的方式和密钥。

如果区域认证方式和接口认证方式都配置了则以接口的认证方式为准

设备 A 的配置：

配置以太网端口

```
interface FastEthernet0/0
ip address 192.168.12.1 255.255.255.0
ip ospf message-digest-key 1 md5 hello
```

配置 OSPF 路由协议

```
router ospf 1
network 192.168.12.0 0.0.0.255 area 0
area 0 authentication message-digest
```

设备 B 的配置：

配置以太网端口

```
interface FastEthernet0/0
ip address 192.168.12.2 255.255.255.0
```

```

ip ospf message-digest-key 1 md5 hello

# 配置 OSPF 路由协议

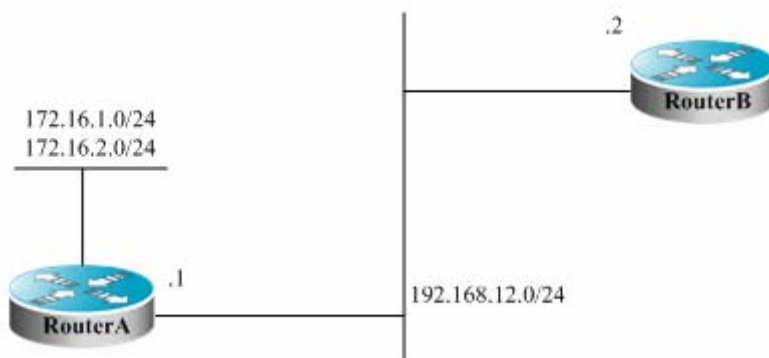
router ospf 1
network 192.168.12.0 0.0.0.255 area 0
area 0 authentication message-digest

```

3.3.4 OSPF路由汇聚配置例子

3.3.4.1 配置要求

两台设备通过以太网连接，IP 地址分配和设备连接图见下图。



OSPF 路由汇聚配置例子

要求：

- 两台设备均运行 OSPF 路由协议，网络 192.168.12.0/24 属于区域 0，网络 172.16.1.0/24 和 172.16.2.0/24 属于区域 10；
- 通过配置 Router A，使得路由 A 只通告 172.16.0.0/22 路由，而不通告 172.16.1.0/24、172.16.2.0/24 的路由。
- 通过配置 Router A，使得设备 A 通告的汇聚路由的度量值为 20，并且不向路由表添加 discard 路由。

3.3.4.2 设备具体配置

需要在 Router A 上配置 OSPF 区域路由汇聚，注意区域路由汇聚只能在区域边界设备上配置。

设备 A 的配置：

```

# 配置以太网端口

interface FastEthernet0/0
ip address 192.168.12.1 255.255.255.0

```

```
# 配置以太网卡上的 2 个端口

interface FastEthernet1/0
ip address 172.16.1.1 255.255.255.0
interface FastEthernet1/1
ip address 172.16.2.1 255.255.255.0

# 配置 OSPF 路由协议

router ospf 1
network 192.168.12.0 0.0.0.255 area 0
network 172.16.1.0 0.0.0.255 area 10
network 172.16.2.0 0.0.0.255 area 10
no discard-route internal
area 10 range 172.16.0.0 255.255.252.0 cost 20
```

设备 B 的配置:

```
# 配置以太网端口

interface FastEthernet0/0
ip address 192.168.12.2 255.255.255.0

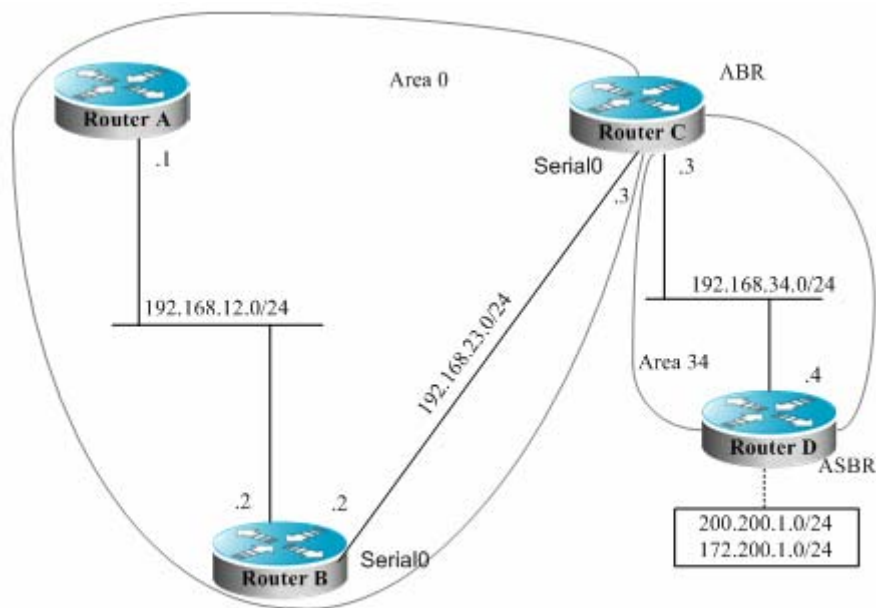
# 配置 OSPF 路由协议

router ospf 1
network 192.168.12.0 0.0.0.255 area 0
```

3.3.5 OSPF ABR、ASBR配置例子

3.3.5.1 配置要求

有四台设备组成了一个 OSPF 路由域，网络 192.168.12.0/24、192.168.23.0/24 属于区域 0，网络 192.168.34.0/24 属于区域 34。具体 IP 地址分配和设备连接图见下图。



OSPF ABR、ASBR 配置例子

如图所示，设备 A、B 为区域内部设备，设备 C 为区域边界设备，设备 D 为自治域边界设备。200.200.1.0/24、172.200.1.0/24 为 OSPF 路由域外的网络。通过配置各设备，使得所有 OSPF 设备学到外部路由，要求外部路由携带“34”标记以及类型为外部路由 I 型。

3.3.5.2 设备具体配置

OSPF 重分布其它来源的路由时，缺省类型为 II 型，而且不携带任何标记。

设备 A 的配置：

```
# 配置以太网端口
interface FastEthernet0/0
ip address 192.168.12.1 255.255.255.0

# 配置 OSPF 路由协议
router ospf 1
network 192.168.12.0 0.0.0.255 area 0
```

设备 B 的配置：

```
# 配置以太网端口
interface FastEthernet0/0
ip address 192.168.12.2 255.255.255.0

# 配置广域网端口
interface Serial 1/0
ip address 192.168.23.2 255.255.255.0
```

配置 OSPF 路由协议

```
router ospf 1
network 192.168.12.0 0.0.0.255 area 0
network 192.168.23.0 0.0.0.255 area 0
```

设备 C 的配置:

配置以太网端口

```
interface FastEthernet 0/0
ip address 192.168.34.3 255.255.255.0
```

配置广域网端口

```
interface Serial 1/0
ip address 192.168.23.3 255.255.255.0
```

#配置 OSPF 路由协议

```
router ospf 1
network 192.168.23.0 0.0.0.255 area 0
network 192.168.34.0 0.0.0.255 area 34
```

设备 D 的配置:

配置以太网端口

```
interface FastEthernet 0/0
ip address 192.168.34.4 255.255.255.0
```

配置以太网卡上的端口

```
interface FastEthernet 1/0
ip address 200.200.1.1 255.255.255.0
interface FastEthernet 1/1
ip address 172.200.1.1 255.255.255.0
```

配置 OSPF 路由协议, 重分布 RIP 路由

```
router ospf 1
network 192.168.34.0 0.0.0.255 area 34
redistribute rip metric-type 1 subnets tag 34
```

配置 RIP 路由协议

```
router rip
network 200.200.1.0
network 172.200.0.0
```

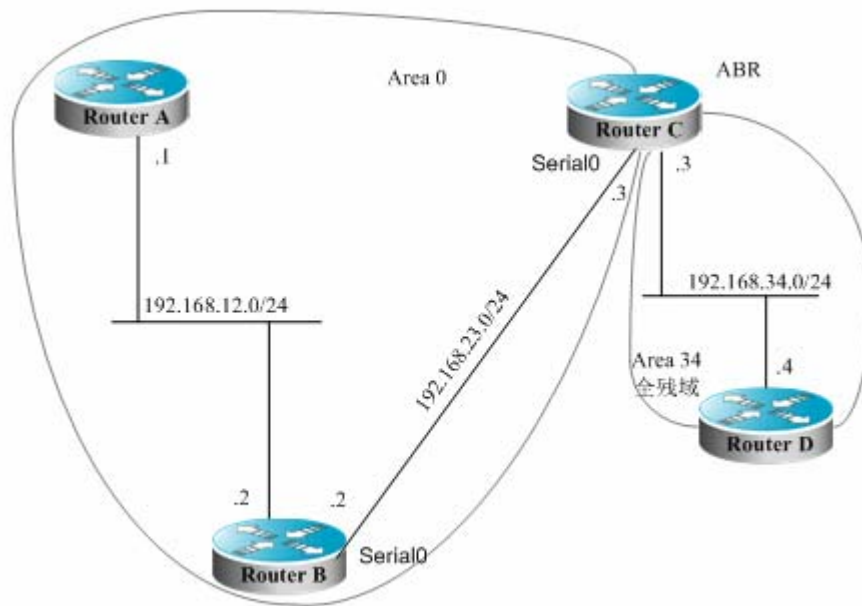
在设备 B 上看到 **ospf** 生成的路由如下, 注意外部路由类型变为“E1”了。

```
0 E1 200.200.1.0/24 [110/85] via 192.168.23.3,00:00:33,Serial1/0
0 IA 192.168.34.0/24 [110/65] via 192.168.23.3,00:00:33,Serial1/0
0 E1 172.200.1.0 [110/85] via 192.168.23.3,00:00:33,Serial1/0
```


3.3.6 OSPF 残域的配置例子

3.3.6.1 配置要求

有四台设备组成了一个 OSPF 路由域，网络 192.168.12.0/24、192.168.23.0/24 属于区域 0，网络 192.168.34.0/24 属于区域 34。具体 IP 地址分配和设备连接图见下图。



OSPF 残域配置例子

要求经过配置 RouterD 的路由表中将只能看到 OSPF 缺省路由和本区域网络路由。

3.3.6.2 设备具体配置

只有在全残域中的设备，路由表才能达到最简化，没有到外部和区域间的路由。残域的配置需要在该区域的所有路由上配置。为了在设备 D 上可以看到区域间路由，设备 C 还通告了一个 192.168.30.0/24 的网络。

设备 A 的配置：

配置以太网端口

```
interface FastEthernet0/0
ip address 192.168.12.1 255.255.255.0
```

配置 OSPF 路由协议

```
router ospf 1
network 192.168.12.0 0.0.0.255 area 0
```

设备 B 的配置：

```
# 配置以太网端口
interface FastEthernet0/0
ip address 192.168.12.2 255.255.255.0

# 配置广域网端口
interface Serial1/0
ip address 192.168.23.2 255.255.255.0

# 配置 OSPF 路由协议
router ospf 1
network 192.168.12.0 0.0.0.255 area 0
network 192.168.23.0 0.0.0.255 area 0
```

设备 C 的配置:

```
# 配置以太网端口
interface FastEthernet0/0
ip address 192.168.34.3 255.255.255.0

# 配置广域网端口
interface Serial1/0
ip address 192.168.23.3 255.255.255.0

# 增加一个网络
interface Dialer10
ip address 192.168.30.1 255.255.255.0
```

配置 OSPF 路由协议

```
router ospf 1
network 192.168.23.0 0.0.0.255 area 0
network 192.168.34.0 0.0.0.255 area 34
network 192.168.30.0 0.0.0.255 area 34
area 34 stub no-summary
```

设备 D 的配置:

```
# 配置以太网端口
interface FastEthernet0/0
ip address 192.168.34.4 255.255.255.0

# 配置 OSPF 路由协议
router ospf 1
network 192.168.34.0 0.0.0.255 area 34
area 34 stub
```

设备 D 上看到的 ospf 生成 的路由如下:

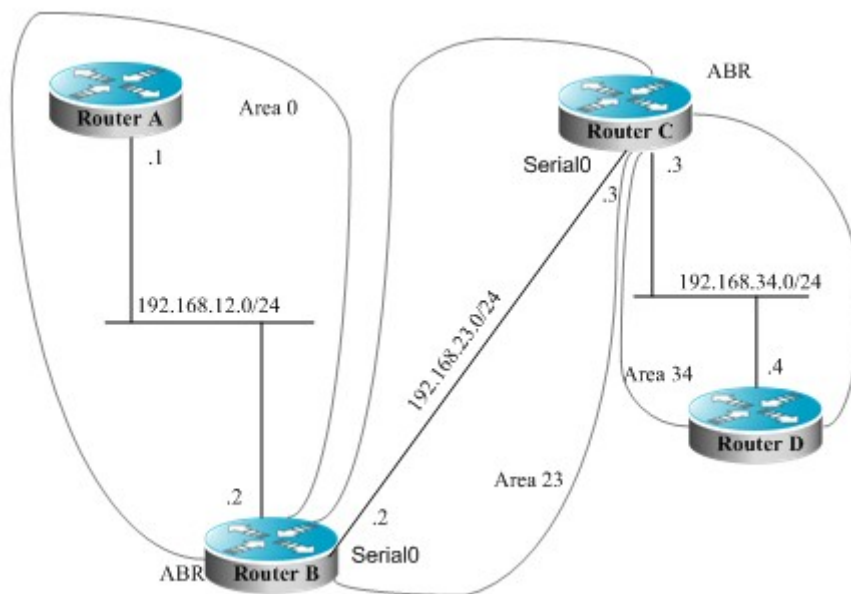
```
0 192.168.30.0/24 [110/1786] via 192.168.34.3, 00:00:03, FastEthernet0/0
```

```
0*IA 0.0.0.0/0 [110/2] via 192.168.34.3, 00:00:03, FastEthernet0/0
```

3.3.7 OSPF 虚拟链接配置例子

3.3.7.1 配置要求

有四台设备组成了一个 OSPF 路由域，网络 192.168.12.0/24 属于区域 0，网络 192.168.23.0/24 属于区域 23，网络 192.168.34.0/24 属于区域 34。具体 IP 地址分配和设备连接图见下图。



OSPF 虚拟链接配置例子

通过配置使得设备 D 能够学到 192.168.12.0/24、192.168.23.0/24 的路由。

3.3.7.2 设备具体配置

OSPF 路由域由多个区域组成时，每个区域必须域骨干域（area 0）直接连接，如果没有直接连接，则必须创建虚拟链接，使得在逻辑上跟骨干域是直接相连的，否则区域间将不能连通。虚拟链接必须在 ABR 上进行配置。

设备 A 的配置：

配置以太网端口

```
interface FastEthernet0/0
ip address 192.168.12.1 255.255.255.0
```

配置 OSPF 路由协议

```
router ospf 1
network 192.168.12.0 0.0.0.255 area 0
```

设备 B 的配置:

```
# 配置以太网端口
interface FastEthernet0/0
ip address 192.168.12.2 255.255.255.0

# 配置广域网端口
interface Serial1/0
ip address 192.168.23.2 255.255.255.0

# 增加回环 IP 地址作为 OSPF 设备标识符
interface Loopback2
ip address 2.2.2.2 255.255.255.0

# 配置 OSPF 路由协议
router ospf 1
network 192.168.12.0 0.0.0.255 area 0
network 192.168.23.0 0.0.0.255 area 23
area 23 virtual-link 3.3.3.3
```

设备 C 的配置:

```
# 配置以太网端口
interface FastEthernet0/0
ip address 192.168.34.3 255.255.255.0

# 配置广域网端口
interface Serial1/0
ip address 192.168.23.3 255.255.255.0

# 增加回环 IP 地址作为 OSPF 设备标识符
interface Loopback2
ip address 3.3.3.3 255.255.255.0

# 配置 OSPF 路由协议
router ospf 1
network 192.168.23.0 0.0.0.255 area 23
network 192.168.34.0 0.0.0.255 area 34
area 23 virtual-link 2.2.2.2
```

设备 D 的配置:

```
# 配置以太网端口
interface FastEthernet0/0
ip address 192.168.34.4 255.255.255.0

# 配置 OSPF 路由协议
router ospf 1
```

```
network 192.168.34.0 0.0.0.255 area 34
```

设备 D 上看到的 **ospf** 生成的路由如下：

```
0 IA 192.168.12.0/24[110/66]via 192.168.34.3,00:00:10, FastEthernet0/0
```

```
0 IA 192.168.23.0/24[110/65]via 192.168.34.3,00:00:25, FastEthernet0/0
```



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. 配置 IGMP Snooping

1 配置 IGMP Snooping

1.1 概述

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。

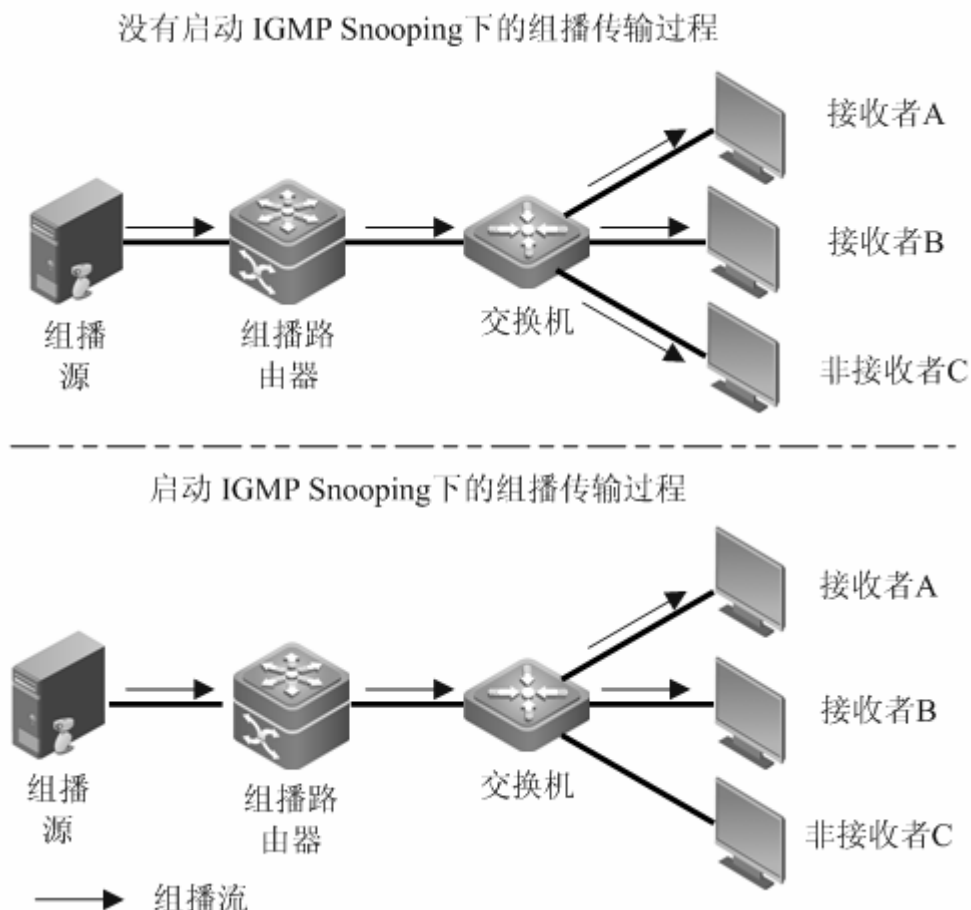


图 1. VLAN 上运行 IGMP Snooping 前后的对比

锐捷推出的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。

1.1.1 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）。

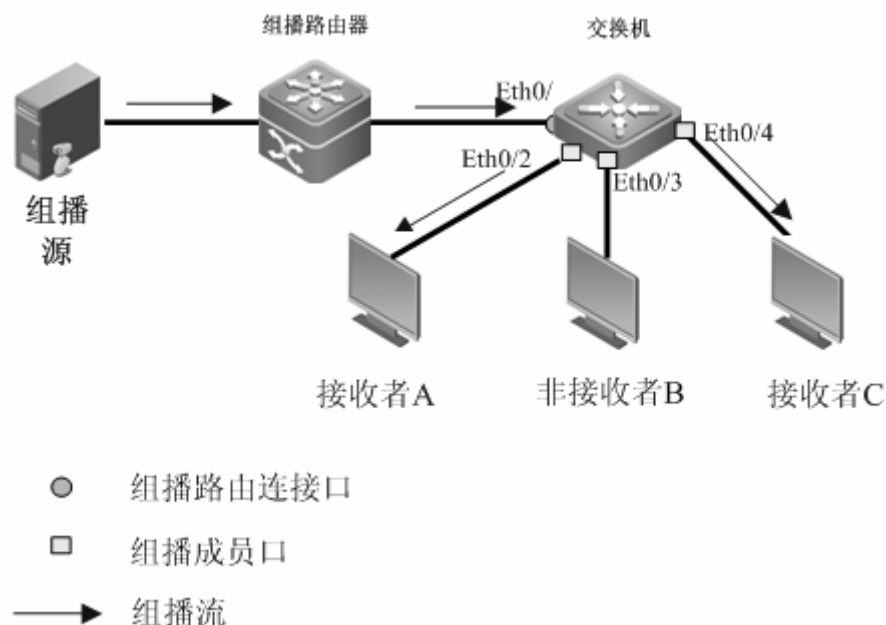


图 2. IGMP Snooping 的两类端口

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，又称侦听器端口 (Listener Port)，表示交换机上连接 IP 组播组成员侧的端口，如 Switch A 的 Eth0/2、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。

1.1.2 IGMP Snooping 的工作原理

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，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。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。

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

1.1.3 IGMP Snooping 的工作模式

- **DISABLE 模式**：在该模式下，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 工作模式(Independent VLAN Group Learning)**：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。

1.2 配置 IGMP Snooping

1.2.1 使能 IGMP Snooping

必须使能 IGMP Snooping。其他配置可选。



注意

如果二层组播设备工作在 private vlan 模式下，则不支持 IGMP snooping。

如果 VLAN 配置为 Remote VLAN 时，VLAN 上的 IGMP Snooping 功能状态为 Disable，和该 VLAN 相关的 IGMP Snooping 配置（如基于 VLAN 配置路由连接口或配置成员口）仍然可以进行配置，但是不生效。

全局打开/关闭 IGMP Snooping

使用如下命令，全局打开/关闭 IGMP Snooping 的 IVGL 模式。

	命令	作用
Step 1	Ruijie(config)# ip igmp snooping ivgl	打开并设置 IGMP Snooping 为 IVGL 模式，缺省情况下，IGMP Snooping 处于关闭状态。
Step 2	Ruijie(config)# show ip igmp snooping	确认配置是否生效。
Step 3	Ruijie(config)# no ip igmp snooping	全局关闭 IGMP Snooping 功能。

以下例子是打开并设置 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
```

以下例子是关闭 IGMP Snooping:

```
Ruijie# configure terminal
Ruijie(config)# no ip igmp snooping ivgl
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
```

基于 VLAN 关闭/启动 IGMP Snooping

默认情况下，当全局打开 IGMP Snooping，所有 VLAN 也将自动打开 IGMP Snooping 功能。如果需要在特定 VLAN 上关闭 IGMP Snooping 功能，可以采用下面的命令。

命令	作用
Ruijie(config)# no ip igmp snooping vlan num	关闭 VLAN num 的 IGMP Snooping，缺省情况下，VLAN num 的 IGMP Snooping 处于打开状态。
Ruijie(config)# ip igmp snooping vlan num	将 VLAN num 的 IGMP Snooping 功能打开。

以下例子是关闭 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
```



说明

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，必须在该 VLAN 上也启用 MLD Snooping。

1.2.2 配置动态路由连接口的老化定时器

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。

在全局模式下，按如下步骤配置动态端口的老化定时器：

命令	作用
Ruijie(config)# ip igmp snooping dyn-mr-aging-time time	配置动态路由连接口老化时间， <i>time</i> : <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，默认值为 300s。

以下是配置动态路由连接口老化时间为 100s 的实例：

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping dyn-mr-aging-time 100
```

 说明

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。

该命令非即配即用，即在下一次定时器更新时，才启用该配置值。

1.2.3 配置对 IGMP 查询报文的最长响应时间

- 在收到 IGMP 的普遍组查询报文后，运行二层组播功能的设备会对所有的成员端口启动各自的老化定时器，定时器时间为最长响应时间，当定时器的值减为 0 时，则认为该端口不再有成员接收组播流，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，当定时器的值减为 0 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。
- 对于 IGMP 的特定组源查询报文，不做定时器的更新处理。

命令	作用
Ruijie(config)# ip igmp snooping query-max-response-time time	配置 IGMP 普遍组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 普遍组查询报文的最长响应时间为缺省值，缺省值为 10s。

以下是配置 IGMP 查询报文的最长响应时间为 15s 的实例：

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping query-max-response-time 15
```

1.2.4 配置 IGMP Profiles

IGMP Profiles 实际上是一些组过滤器，供其它功能引用。

在全局模式下，按如下步骤设置一个 Profile：

命令	作用

Step 1	Ruijie(config)# ip igmp profile <i>profile-number</i>	进入 IGMP 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。
Step 2	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。
Step 3	Ruijie(config-profile)# range <i>low-address high_address</i>	添加组播地址范围，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），同时还可以配置多个 range 范围。
Step 4	Ruijie(config)# end	退回到特权模式。

如果要删除其中一个 IGMP 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。

以下有个例子是表示 Profile 的配置过程：

```
Ruijie(config)# ip igmp profile 1
Ruijie(config-profile)# permit
Ruijie(config-profile)# range 224.0.1.0 239.255.255.255
Ruijie(config-profile)# end
Ruijie# show ip igmp profile 1
Profile      1
    Permit
    range 224.0.1.0,    239.255.255.255
```

按以上配置，这个 IGMP Profile 的规则就是 permit 224.0.1.0 到 239.255.255.255 的组播地址，其他的组播地址都被 deny。

1.2.5 配置路由连接口

缺省的情况下，VLAN 内将进行动态路由连接口的学习，您可以配置关闭组播设备动态路由连接口的学习的功能，用相应的 no 选项命令关闭动态学习，并清空所有动态学习到的路由连接口。

另外可以通过命令将交换机上的端口配置为静态路由连接口。

	命令	作用
Step 1	Ruijie(config)# ip igmp snooping vlan <i>vlan-id</i> mrouter interface <i>interface-id</i>	设置接口为静态路由连接口。

Step 2	Ruijie(config)# no ip igmp snooping vlan <i>vlan-id</i> mrouter interface <i>interface-id</i>	取消接口为静态路由连接口。
	Ruijie(config)# ip igmp snooping vlan <i>vlan-id</i> mrouter learn pim-dvmrp	设置 VLAN 上路由连接口的动态学习功能；缺省是启动动态学习功能。
	Ruijie(config)# no ip igmp snooping vlan <i>vlan-id</i> 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。

以下例子是设置以太网接口 1/1 为 VLAN1 的静态路由连接口，并启动 VLAN1 自动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
```

1.2.6 配置静态成员端口

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。

	命令	作用
Step 1	Ruijie(config)# ip igmp snooping ivgl	打开并设置 IGMP Snooping 为 IVGL 模式。
Step 2	Ruijie(config)# ip igmp snooping vlan <i>vlan-id</i> static <i>ip-addr</i> interface <i>interface-id</i>	静态配置一个端口接收某个组播流。 • <i>vlan-id</i> : 组播流的 vid • <i>ip-addr</i> : 组播地址 • <i>interface-id</i> : 端口号

Step 3

```
Ruijie(config)# no ip igmp snooping vlan
vlan-id static ip-addr interface interface-id
```

删除一个静态成员端口。

- **vlan-id**: 组播流的 vid
- **ip-addr**: 组播地址
- **interface-id**: 端口号

您可以用 **no ip igmp snooping vlan vlan-id static ip-addr interface interface-id** 删除组播成员的静态配置。

以下为配置 IGMP snooping 静态成员端口的实例：

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping vlan 1 static 233.3.3.4 interface
GigabitEthernet 0/7
Ruijie(config)# end
Ruijie(config)# 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)
```

1.2.7 配置端口快速离开

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。该功能运用在相关端口下只存在一个点播者的情况。

在全局模式下，按如下步骤设置 **IGMP snooping** 的端口快速离开：

命令	作用
Ruijie(config)# ip igmp snooping fast-leave enable	打开二层组播的快速离开功能，缺省情况下是关闭的。
Ruijie(config)# no ip igmp snooping fast-leave enable	关闭端口快速离开功能。

使用 **no ip igmp snooping fast-leave enable** 命令关闭端口快速离开功能。

以下例子是打开端口快速离开功能：

```
Ruijie# configure terminal
```



```
Ruijie(config)# ip igmp snooping fast-leave enable
```

1.2.8 配置 IGMP Snooping 成员关系报告报文的响应抑制

当 VLAN 内的相应端口收到来自某 IP 组播组成员的 IGMP 成员关系报告报文时，会将该报文转发给路由接口。这样，当相同 VLAN 上的其它端口也将收到属于相同 IP 组播组的 Report 报文时，路由接口上会收到多份相同 IGMP 成员关系报告报文。

当使能了 IGMP 成员关系报告报文抑制功能后，在一个查询间隔内同一 VLAN 内只会把收到的某 IP 组播组内的第一个 IGMP 成员关系报告报文转发给路由接口，而不继续向三层设备转发来自同一组播组的其它 IGMP 成员关系报告报文，这样可以减少网络中的报文数量。

在全局模式下，按如下步骤设置 IGMP snooping suppression:

命令	作用
Ruijie(config)# ip igmp snooping suppression enable	打开二层组播 Report 报文抑制功能，缺省情况下是不打开响应抑制功能的。
Ruijie(config)# no ip igmp snooping suppression enable	关闭二层组播 Report 报文抑制功能。

以下例子是打开 Suppression 功能:

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping suppression enable
```

1.2.9 配置 IGMP Filtering

在某些情况下，您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。

您可以把某一个 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。

您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。

	命令	作用
Step 1	Ruijie(config)# interface interface-id	进入配置接口。

Step 2	Ruijie(config-if)# ip igmp snooping filter <i>profile-number</i>	(可选) 应用 Profile 于该端口, <i>profile number</i> 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	(可选) 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 <i>number</i>	(可选) 允许最多几个组动态的加入该端口, 参数范围为 0 – 1024。缺省情况下, 无限制。

以下是配置 IGMP Filtering 的实例:

```
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

1.3 监视与维护

1.3.1 查看 IGMP Snooping 工作模式

在特权模式下使用如下命令查看 IGMP Snooping 当前的工作模式及全局配置:

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。

以下例子使用 **show ip igmp snooping** 命令查看 IGMP Snooping 配置信息:

```
Ruijie# show ip igmp snooping
IGMP-snooping mode      : IVGL
SVGL vlan-id            : 1
SVGL profile number     : 0
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Disable
```

IGMP Report suppress: Disable

1.3.2 查看和清除 IGMP Snooping 的统计值

在特权模式下使用如下命令查看和清除 IGMP Snooping 的统计值信息：

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

以下例子使用 **show ip igmp snooping statistics** 命令查看 IGMP Snooping 的路由连接口信息：

```
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 report time	Last reporter	Report pkts	Leave pkts
233.3.3.3	gi1/1	00:02:40	1.1.1.1	3	1

1.3.3 查看路由连接口信息

在特权模式下使用如下命令查看 IGMP Snooping 的路由连接口信息：

命令	作用
Ruijie# show ip igmp snooping mrouter	查看 IGMP Snooping 的路由连接口信息。

以下例子使用 **show ip igmp snooping** 命令查看 IGMP Snooping 的路由连接口信息：

```
Ruijie# show ip igmp snooping mrouter
Vlan    Interface      State      IGMP profile number
----    -
1  GigabitEthernet 0/7    static      1
1  GigabitEthernet 0/12   dynamic     0
```

1.3.4 查看转发表

在特权模式下使用如下命令查看各端口在组播组中的转发规则，即查看组目的地址 GDA（Group Destination Address）表：

命令	作用
Ruijie# show ip igmp snooping gda-table	查看各端口在组播组中的转发规则表。

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 ip igmp snooping gda-table
```

```
Abbr: M - mrouter
```

```
      D - dynamic
```

```
      S - static
```

```
VLAN  Address                Member ports
-----
1      233.3.3.3              GigabitEthernet 0/7(S)
```

1.3.5 清除动态转发表信息

在特权模式下使用如下命令查看各端口在组播组中的转发规则，即查看组目的地址 GDA（Group Destination Address）表：

命令	作用
Ruijie# clear ip igmp snooping gda-table	清除转发表中动态学习到的组信息。

以下例子是清除 GDA 表的动态组播组信息：

```
Ruijie# clear ip igmp snooping gda-table
```

1.3.6 清除转发表节点的统计信息

在特权模式下使用如下命令查看各端口在组播组中的转发规则，即查看组目的地址 GDA（Group Destination Address）表：

命令	作用
Ruijie# clear ip igmp snooping statistics	清除转发表中表项节点的动态统计信息。

以下例子是清除 GDA 表的动态组播组统计信息：

```
Ruijie# clear ip igmp snooping statistics
```

1.3.7 查看 IGMP Profile

在特权模式下使用如下命令查看 IGMP Profile 信息：

命令	作用
Ruijie# show ip igmp profile <i>profile-number</i>	查看 IGMP Profile 信息。

以下为查看 IGMP Profile 的信息：

```
Ruijie# show ip igmp profile 1
Profile      1
    Permit
    range 224.0.1.0,    239.255.255.255
```

1.3.8 查看 IGMP Filtering

在特权模式下使用如下命令查看 IGMP Filtering 的配置信息：

命令	作用
Ruijie# show ip igmp snooping interface <i>interface-id</i>	查看 IGMP Filtering 的配置信息。

以下为查看 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
```



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. 配置 AAA
2. 配置 802.1X
3. SSH 终端服务
4. 配置基于端口的流控制
5. 配置 CPU 保护
6. 配置 DOS 保护
7. 配置 DHCP Snooping
8. 配置动态 ARP 检测
9. 配置 IP Source Guard
10. 配置防网关 ARP
11. 配置 NFPP
12. 锐捷交换机安全功能兼容模式配置

1 配置 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。



说明

部分产品的 AAA 仅提供认证功能。所有涉及产品规格的问题，可以通过向福建星网锐捷网络有限公司市场人员或技术支援人员咨询得到。

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。

注意

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。



典型的 AAA 网络配置图

上图说明了一个典型的 AAA 网络配置，它包含两台安全服务器：R1 和 R2 是 RADIUS 服务器。

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。

注意

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。

说明

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 AAA配置基本步骤

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，使用全局配置层命令 **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，请参见安全配置命令参考中的相关章节。

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
Step 1	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
Step 1	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

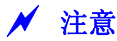
身份认证是在允许用户使用网络资源以前对其进行识别，在大多数情况下，身份认证是通过 AAA 安全特性来实现的。我们建议，在可能的情况下，最好使用 AAA 来实现身份认证。

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
Step 1	configure terminal	进入全局配置模式
Step 2	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
Step 1	configure terminal	进入全局配置模式
Step 2	aaa new-model	打开 AAA 开关
Step 3	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。
Step 4	line vty 2	进入线路 2 配置层
Step 5	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。

**注意**

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

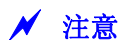
要配置 AAA 身份认证，都必须执行以下任务：

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。

**注意**

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：

**注意**

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：

Step 1

命令	作用
configure	terminal

Step 2	aaa new-model	启用 AAA。
Step 3	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。
Step 4	line vty line-num	进入您需要应用 AAA 身份认证的线路。
Step 5	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**

注意

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
Step 1	local	使用本地用户名数据库进行身份认证
Step 2	none	不进行身份认证
Step 3	group radius	使用 RADIUS 服务器组进行身份认证
Step 4	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。

1.3.5.1 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
Step 1	configure terminal	进入全局配置模式
Step 2	username name [password password]	建立本地用户，设置口令
Step 3	end	退出到特权模式
Step 4	show running-config	确认配置

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
Step 1	configure terminal	进入全局配置模式
Step 2	aaa new-model	打开 AAA 开关

Step 3	aaa authentication login {default list-name} local	定义使用本地认证方法
Step 4	end	退出到特权模式
Step 5	show aaa method-list	确认配置的方法列表
Step 6	configure terminal	进入全局配置模式
Step 7	line vty line-num	进入线路配置模式
Step 8	login authentication {default list-name}	应用方法列表
Step 9	end	退出到特权模式
Step10	show running-config	确认配置

1.3.5.2 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
Step 1	configure terminal	进入全局配置模式
Step 2	aaa new-model	打开 AAA 开关
Step 3	radius-server host ip-address [auth-port port] [acct-port port]	配置 RADIUS 服务器
Step 4	end	退出到特权模式
Step 5	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
Step 1	configure terminal	进入全局配置模式
Step 2	aaa new-model	打开 AAA 开关
Step 3	aaa authentication login {default list-name} group radius	定义使用 RADIUS 认证方法
Step 4	end	退出到特权模式
Step 5	show aaa method-list	确认配置的方法列表
Step 6	configure terminal	进入全局配置模式
Step 7	line vty line-num	进入线路配置模式
Step 8	login authentication {default list-name}	应用方法列表
Step 9	end	退出到特权模式
Step10	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
Step 1	configure terminal	进入全局配置模式
Step 2	aaa new-model	启用 AAA。
Step 3	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。

 注意

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。

 注意

(可选)表示需读者留心关注的重要信息，用“注意栏”的形式提醒读者认真对待此部分内容，严格遵照其中的要求操作或使用。若读者忽略此内容，可能会因误操作而导致不良后果或无法成功操作。如产品限制信息，包括芯片差异导致的功能缺陷、功能之间的互斥信息、实现上的缺陷等等都需用“注意栏”的形式来描述。

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。

1.3.6.1 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
Step 1	configure terminal	进入全局配置模式
Step 2	username name [password password]	建立本地用户，设置口令
Step 3	username name [privilege level]	为用户设置权限级别（可选）
Step 4	end	退出到特权模式
Step 5	show running-config	确认配置

定义本地 Enable 认证方法列表，可使用以下命令：

	命令	作用
Step 1	configure terminal	进入全局配置模式
Step 2	aaa new-model	打开 AAA 开关
Step 3	aaa authentication enable default local	定义使用本地认证方法
Step 4	end	退出到特权模式
Step 5	show aaa method-list	确认配置的方法列表
Step 6	show running-config	确认配置

1.3.6.2 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
Step 1	configure terminal	进入全局配置模式
Step 2	aaa new-model	打开 AAA 开关
Step 3	aaa authentication enable default group radius	定义使用 RADIUS 认证方法
Step 4	end	退出到特权模式
Step 5	show aaa method-list	确认配置的方法列表
Step 6	show running-config	确认配置

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
Step 1	configure terminal	进入全局配置模式
Step 2	aaa new-model	启用 AAA。
Step 3	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。
Step 4	interface interface-type interface-number	进入需要应用 AAA 身份认证的异步或 ISDN 接口。
Step 5	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 提供点对点的接入，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
Step 1	configure terminal	进入全局配置模式
Step 2	aaa new-model	启用 AAA。
Step 3	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。
Step 4	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“802.1x 配置”中相关章节。

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。



说明

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
Step 1	configure terminal	进入全局配置模式

Step 2	aaa new-model	打开 AAA 开关
Step 3	aaa authorization exec {default list-name} method1 [method2 ...]	定义 AAA Exec 授权方法
Step 4	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
Step 1	configure terminal	进入全局配置模式
Step 2	aaa new-model	启用 AAA。
Step 3	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。
Step 4	line vty line-num	进入您需要应用 AAA Exec 授权的线路。
Step 5	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
Step 1	local	使用本地用户名数据库进行 Exec 授权
Step 2	none	不进行 Exec 授权
Step 3	group radius	使用 RADIUS 服务器组进行 Exec 授权
Step 4	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。

注意

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。

1.4.4.1 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
Step 1	configure terminal	进入全局配置模式
Step 2	username name [password password]	建立本地用户，设置口令
Step 3	username name [privilege level]	为用户设置权限级别（可选）
Step 4	end	退出到特权模式
Step 5	show running-config	确认配置

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
Step 1	configure terminal	进入全局配置模式
Step 2	aaa new-model	打开 AAA 开关
Step 3	aaa authorization exec {default list-name} local	定义使用本地认证方法
Step 4	end	退出到特权模式
Step 5	show aaa method-list	确认配置的方法列表
Step 6	configure terminal	进入全局配置模式
Step 7	line vty line-num	进入线路配置模式
Step 8	authorization exec {default list-name}	应用方法列表
Step 9	end	退出到特权模式
Step10	show running-config	确认配置

1.4.4.2 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“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
Step 1	configure terminal	进入全局配置模式
Step 2	aaa new-model	打开 AAA 开关
Step 3	aaa authorization exec {default list-name} group radius	定义使用 RADIUS 认证方法
Step 4	end	退出到特权模式
Step 5	show aaa method-list	确认配置的方法列表

Step 6	configure terminal	进入全局配置模式
Step 7	line vty line-num	进入线路配置模式
Step 8	authorization exec {default list-name}	应用方法列表
Step 9	end	退出到特权模式
Step10	show running-config	确认配置

1.4.4.3 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。



注意

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
Step 1	configure terminal	进入全局配置模式
Step 2	aaa new-model	启用 AAA。
Step 3	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。

1.4.5.1 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
Step 1	configure terminal	进入全局配置模式
Step 2	aaa new-model	打开 AAA 开关
Step 3	aaa authorization network {default list-name} group radius	定义使用 RADIUS 授权方法。

1.4.5.2 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；而网络记账针对的是与网络连接上的用户会话有关的信息。



说明

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。



注意

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
Step 1	configure terminal	进入全局配置模式
Step 2	aaa new-model	启用 AAA。
Step 3	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。
Step 4	line vty line-num	进入您需要应用 AAA Exec 记账的线路。
Step 5	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。

说明

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。

1.5.3.1 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”。

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
Step 1	configure terminal	进入全局配置模式
Step 2	aaa new-model	打开 AAA 开关
Step 3	aaa accounting exec {default list-name} start-stop group radius	定义使用 RADIUS 记账方法。
Step 4	end	退出到特权模式
Step 5	show aaa method-list	确认配置的方法列表
Step 6	configure terminal	进入全局配置模式
Step 7	line vty line-num	进入线路配置模式
Step 8	accounting exec {default list-name}	应用方法列表
Step 9	end	退出到特权模式
Step10	show running-config	确认配置

1.5.3.2 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。



说明

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
Step 1	configure terminal	进入全局配置模式
Step 2	aaa new-model	启用 AAA。
Step 3	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。

1.5.4.1 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
Step 1	configure terminal	进入全局配置模式
Step 2	aaa new-model	打开 AAA 开关
Step 3	aaa accounting network {default list-name} start-stop group radius	定义使用 RADIUS 记账方法。

1.5.4.2 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

要查看当前登录用户的信息，请在特权用户模式下执行命令：

	命令	作用
Step 1	show aaa user { id all }	查看当前 AAA 用户信息

1.7 配置Login的用户认证失败锁定

Login 登录交换机，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
Step 1	configure terminal	进入全局配置模式
Step 2	aaa new-model	打开 AAA 开关
Step 3	aaa local authentication attempts <1-2147483647>	配置 login 登录，用户尝试失败次数
Step 4	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）
Step 5	show aaa user lockout {all user-name <word>}	显示当前被锁定的用户列表
Step 6	clear aaa local user lockout {all user-name <word>}	清除被锁定的用户列表
Step 7	end	



说明

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。

配置基于域名的 AAA 服务

基于域名的 AAA 服务的配置相关内容，本节包含如下内容：

- 概述
- 基于域名的 AAA 服务配置任务
- 配置基于域名的 AAA 服务配置注意事项

 注意

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“802.1x 配置”中相关章节。

概述

在多域环境下，同一台 NAS（Network Access Switch）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。

 说明

本产品支持以下几种形式的用户名

1. userid@domain-name
2. domain-name\userid
3. userid.domain-name
4. userid

对于第 4 种不带 domain-name 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

 说明

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：

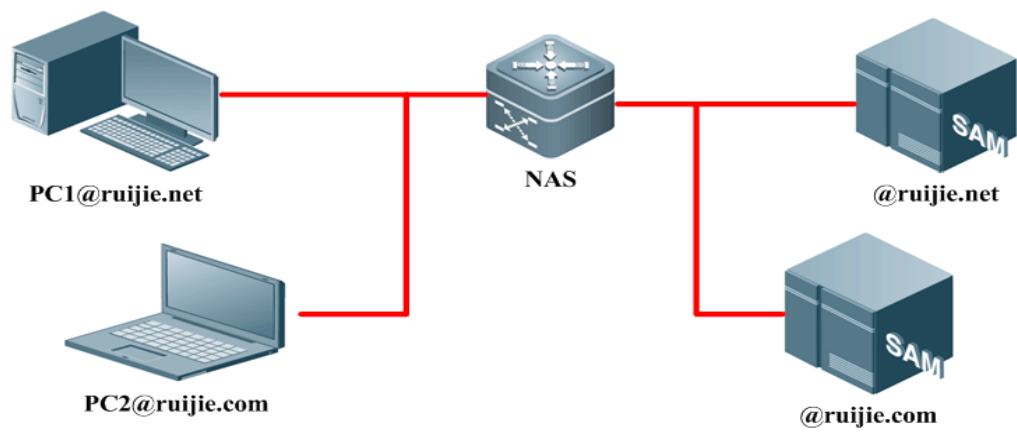


图 2 典型多个域网络图

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

 **说明** 系统最多支持配置 32 个域。

1.7.1.1 启用AAA

	命令	作用
Step 1	configure terminal	进入全局配置模式
Step 2	aaa new-model	打开 AAA 开关

具体命令说明请参见“启用 AAA” 章节。

1.7.1.2 定义AAA服务的方法列表

	命令	作用
Step 1	configure terminal	进入全局配置模式
Step 2	aaa authentication dot1x {default list-name} method1 [method2...]	定义一个 IEEE802.1x 认证方法列表
Step 3	aaa accounting network {default list-name} start-stop method1 [method2...]	定义一个 Network 记账方法列表

Step 4	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。

1.7.1.3 打开基于域名的AAA服务开关

	命令	作用
Step 1	configure terminal	进入全局配置模式
Step 2	aaa domain enable	打开基于域名的 AAA 服务开关

1.7.1.4 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
Step 1	configure terminal	进入全局配置模式
Step 2	aaa domain domain-name	创建域名为 <i>domain-name</i> 的域，并进入域配置模式

说明

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。

1.7.1.5 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
Step 1	authentication dot1x {default list-name}	在域配置模式下，选择认证方法列表
Step 2	accounting network {default list-name}	在域配置模式下，选择记账方法列表

Step 3	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
Step 1	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
Step 1	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
Step 1	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）

说明

1. 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；
2. 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；
3. 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；

1.7.1.6 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
Step 1	show aaa domain [domain-name]	显示当前基于域名的 AAA 服务域信息

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。

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:
```

```
authentic
```

2 配置 802.1x

2.1 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。

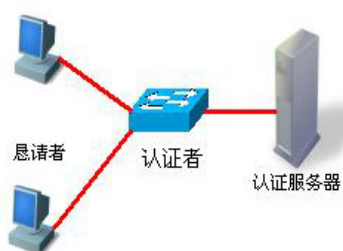
我们将从以下几个方面阐述 802.1x：

- 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

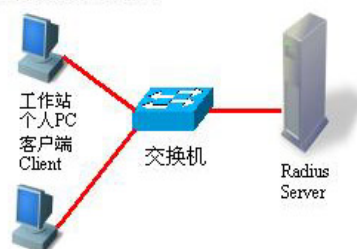
2.1.1 设备的角色

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。

在IEEE 802.1X协议中的角色



实际应用中的角色



■ 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。

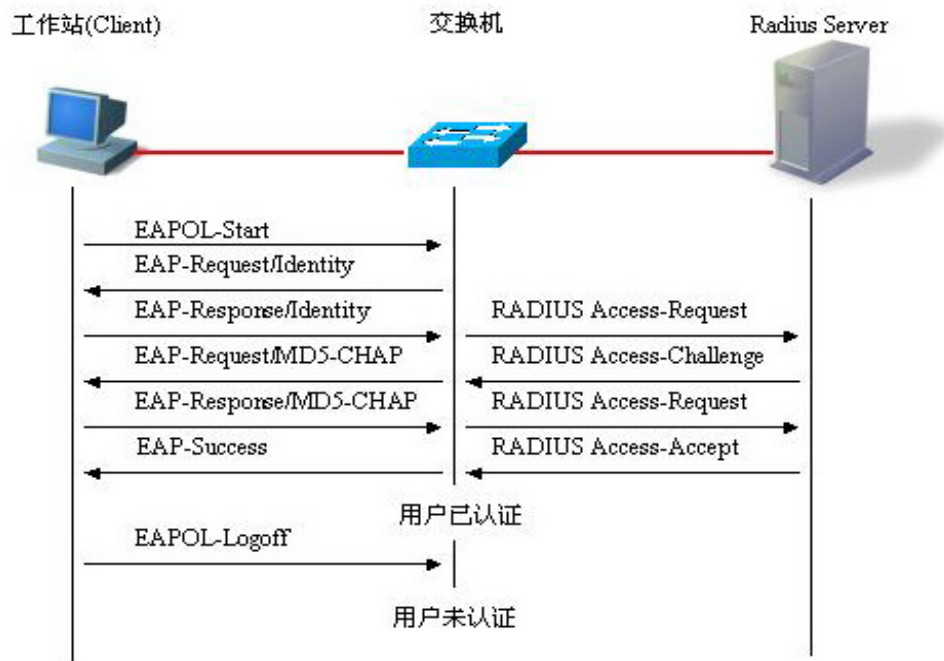
■ 认证服务器

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。

2.1.2 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：



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）。

2.1.3 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）。

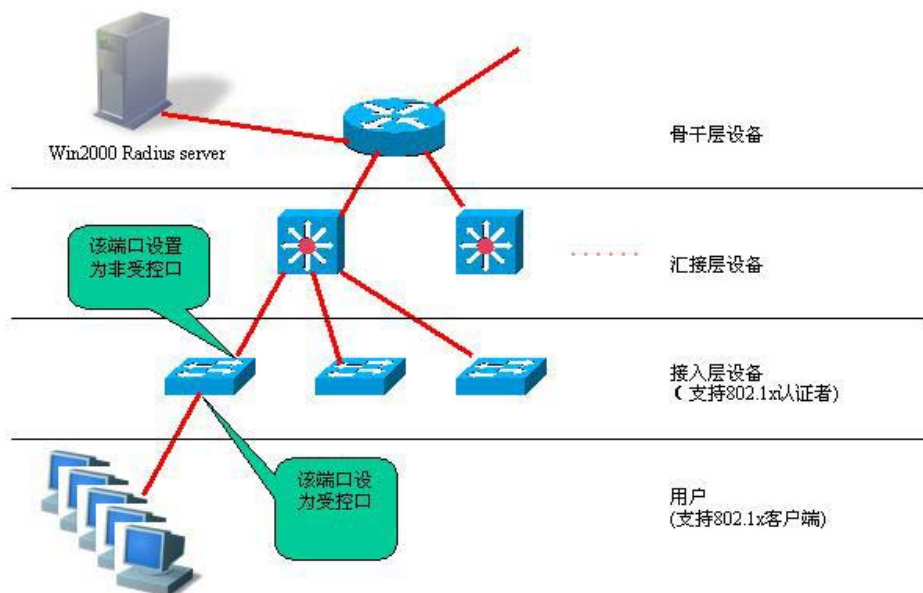
当设备的某个端口变为 LINK-DOWN 状态，该端口上的所有用户均变为未认证（unauthorized）状态。

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。

2.1.4 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



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。

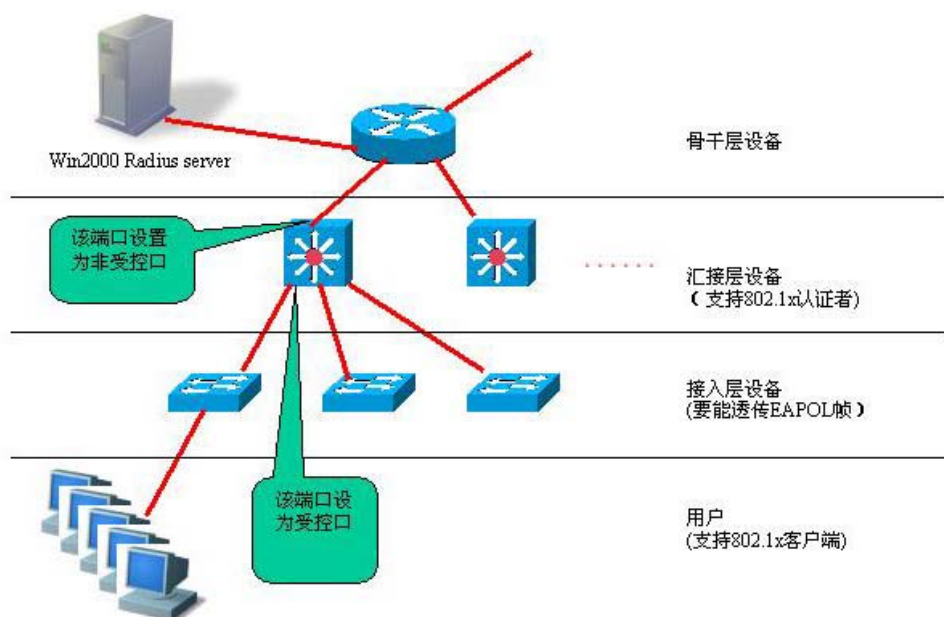
该方案的配置要点：

- 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



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-suppllicant 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。

2.2 配置 802.1X

2.2.1 802.1x 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

2.2.2 802.1X 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。

2.2.3 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

2.2.4 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。

2.2.5 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 为受控接口：

```
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。

2.2.6 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，使计费更准确。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。在根据时常进行计费的情况下，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
Authenticated 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。

2.2.7 打开/关闭 过滤非我司supplicant 功能的开关

当选用我司的 supplicant 产品作为 802.1x 认证的客户端时，如果用户同时也使用了其它的一些 802.1x 认证客户端(比如打开了 WindowsXP 自带的 802.1x 认证功能选项)，则有可能会使认证失败。

这时可以通过打开本功能，将非我司 supplicant 发出的 802.1x 报文过滤掉，来保证 supplicant 的认证不受其它 802.1x 客户端的影响。默认情况下，该功能是关闭的。

在特权模式下，按如下步骤打开、关闭过滤功能：

命令	作用
Ruijie(config)#dot1x private-supplicant-only	打开过滤功能
Ruijie#show dot1x	显示 dot1x 配置

以下例子是打开我司 supplicant 功能的开关的配置：

```

Ruijie# configure terminal
Ruijie(config)# dot1x private-supplicant-only
Ruijie(config)# end
Ruijie# show dot1x
802.1X Status:      enable
Authentication Mode: eap-md5
Total User Number:  0(exclude dynamic user)
Authenticated User Number: 0(exclude dynamic user)
Dynamic User Number: 0
Re-authen Enabled:  enable
Re-authen Period:   2 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
Private supplicant only: enable
Client Online Probe:  disable
Eapol Tag Enable:     disable
Authorization Mode:    disable

```

使用 **no dot1x private-supplicant-only** 命令关闭功能。

2.2.8 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

```

2.2.9 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

```

2.2.10 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
```

2.2.11 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
```

2.2.12 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

2.2.13 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

2.2.14 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：

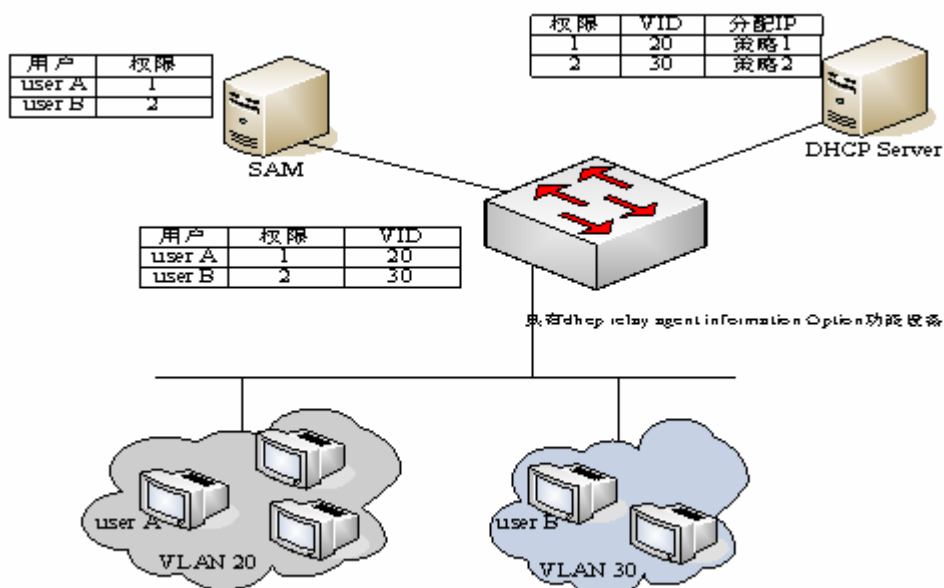
为了方便宽带运营商及其他特殊场合的用途，锐捷对 802.1x 的功能在标准的基础上进行了扩展（该扩展是完全基于标准之上，没有任何的与 IEEE 802.1x 不兼容）。

2.2.15 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：



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
```

2.2.16 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。

2.2.17 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。

2.2.18 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：

```

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+
|  Type      | Length    | Vendor-Id  |
+-----+-----+-----+-----+
| Vendor-Id (cont) | Vendor type | Vendor length |
+-----+-----+-----+-----+
| Attribute-Specific... |
+-----+-----+-----+-----+

```

对于最大数据率应填的值如下：

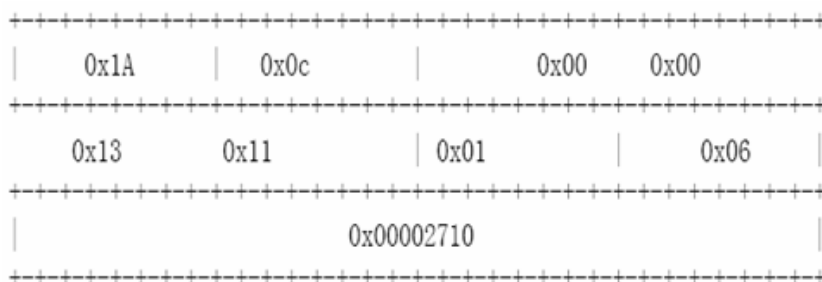
```

+-----+-----+-----+-----+
| 0x1A    | 0x0c    | 0x00    | 0x00    |
+-----+-----+-----+-----+
| 0x13    | 0x11    | 0x01    | 0x06    |
+-----+-----+-----+-----+
| 最大数据率的十六进制值 |
+-----+-----+-----+-----+

```

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：



自定义的头按照以上格式填，最大数据率为 10M，即 10000kbps，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。

2.2.19 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
```

2.2.20 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 <i>gs-name</i>	配置服务器组
Ruijie(config-gs-radius)#server <i>server</i>	配置服务器
Ruijie(config-gs-radius)#server <i>server server-backup</i>	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-11
Ruijie(config-gs-radius)# server 192.168.4.1
Ruijie(config-gs-radius)# server 192.168.4.12
Ruijie(config-gs-radius)# end
```

2.2.21 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。

2.2.22 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。

2.2.23 基于端口的流量计费

锐捷网络设备除了提供针对时长的计费外，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计费功能。

该功能无需配置设备，但需 Radius server 支持。

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 <i>host-ip</i>	配置 RADIUS 服务器
Ruijie(config)#radius-server key <i>text</i>	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 <i>list1</i> group radius	配置认证方法列表 <i>list1</i>
Ruijie(config)#aaa accounting network <i>list2</i> start-stop group radius	配置记账方法列表 <i>list2</i>

具体参见“配置 AAA”

■ 802.1X 选择方法列表

命令	作用
Ruijie(config)#dot1x authentication <i>list1</i>	选择认证方法列表为 <i>list1</i> ， <i>list1</i> 为步骤 3 中配置
Ruijie(config)#dot1x accounting <i>list2</i>	选择记账方法列表为 <i>list2</i> ， <i>list2</i> 为步骤 3 中配置

■ 接口使能 802.1X 认证

命令	作用
Ruijie(config)#interface <i>interface_id</i>	进入需要配置的接口模式下， <i>interface_id</i> 为所要进入接口
Ruijie(config-if-type <i>ID</i>)#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 <i>interface_id</i>	进入需要配置的接口模式下, <i>interface_id</i> 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 <i>session_id</i>	查看会话号为 <i>session_id</i> 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。

2.2.24 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。

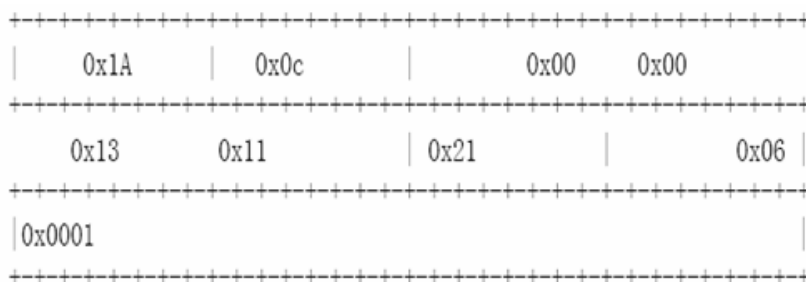
代理服务器屏蔽功能定义的 Vendor Type 为 0x20, 拨号屏蔽功能定义的 Vendor Type 为 0x21。

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:

0x1A	0x0c	0x00	0x00
0x13	0x11	0x20	0x06
0x0001			

若要屏蔽通过拨号上网, 用户应填如下信息:



2.2.25 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

2.2.26 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。

2.2.27 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

2.2.28 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

2.2.29 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
```

2.3 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

2.3.1 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
```

2.3.2 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
Authenticated 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
```

2.3.3 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
```

2.3.4 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
```

2.3.5 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
```

2.4 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。

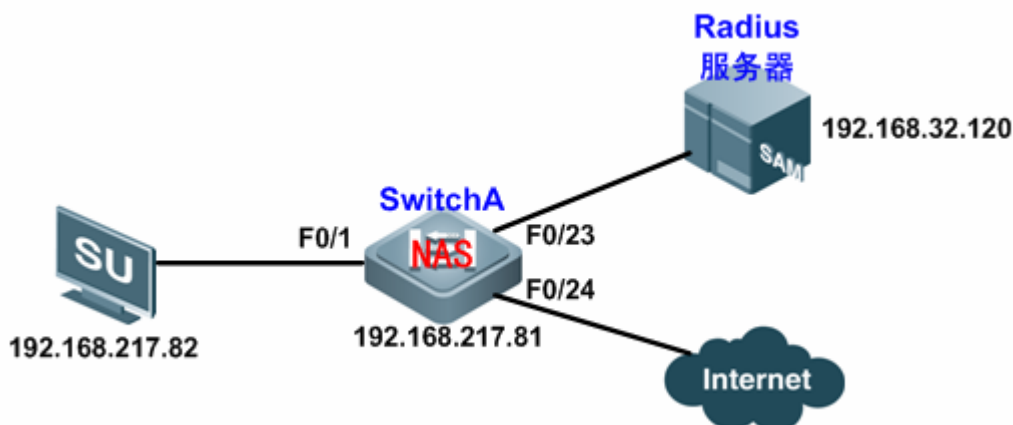
■ 在 Aggregate Port 口上开启受控功能之后，建议不要开启 dot1x redirect 命令，否则会导致该 Aggregate Port 口受控失败。

802.1X典型配置用例

2.4.1 基于 802.1X的AAA服务

拓扑图

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 记账，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：

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：

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
```

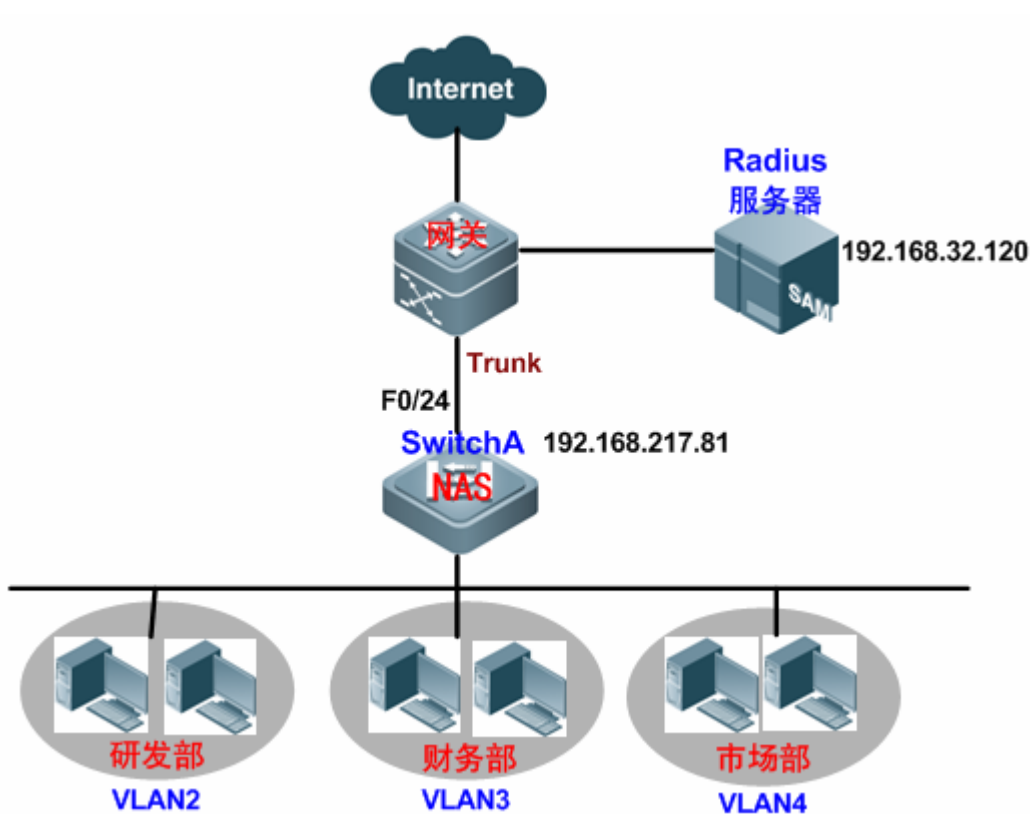
```
Authen Port:    1812
```

```
Server State:   ready
```

2.4.2 802.1X端口动态VLAN自动跳转应用

拓扑图

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：

- 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）
- 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：

添加用户组			
* 用户组名	development	* 父用户组名	root
* 默认用户模板	ceshi	描述	development

- 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：

基本信息			
* 用户名	de	用户姓名	
* 密码	●●●●●●●●	* 密码确认	●●●●●●●●
* 用户组	development	账户	☐ 创建并关联同名账户
用户模板	☐ 使用用户组默认模板 ☒ 自定义模板 模板: ceshi		
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	请选择
高级选项	☒ 显示高级用户设置选项		

功能信息			
下传 IP		用户所属 VLAN (0~4094)	2
用户访问权限 (0~2147483647)		VPN 服务器 ACL	
所属集团	请选择		
开户费	0		

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：

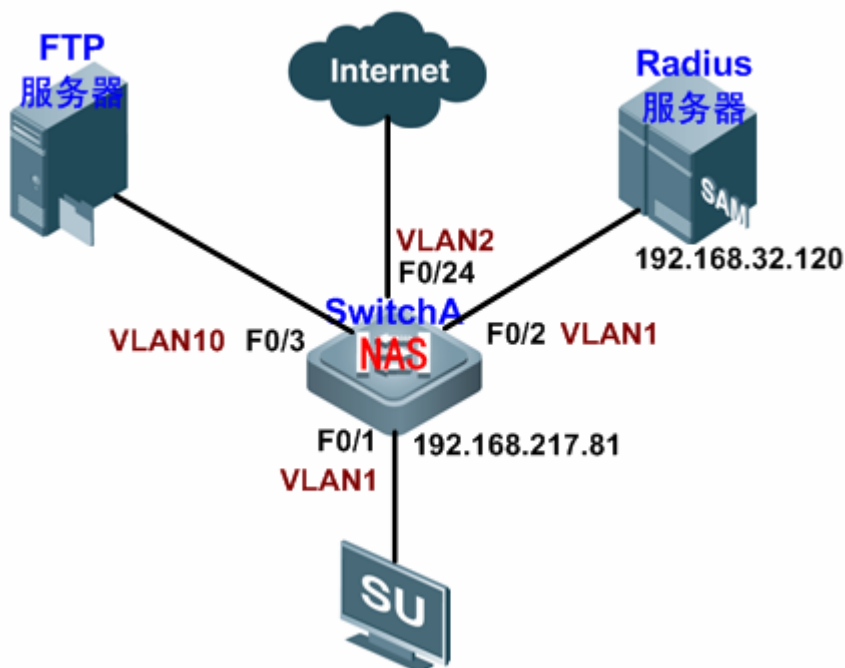
```
Ruijie#show dot1x user id 5

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 :
```

2.4.3 802.1X端口Guest VLAN及VLAN下发应用

拓扑图

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：

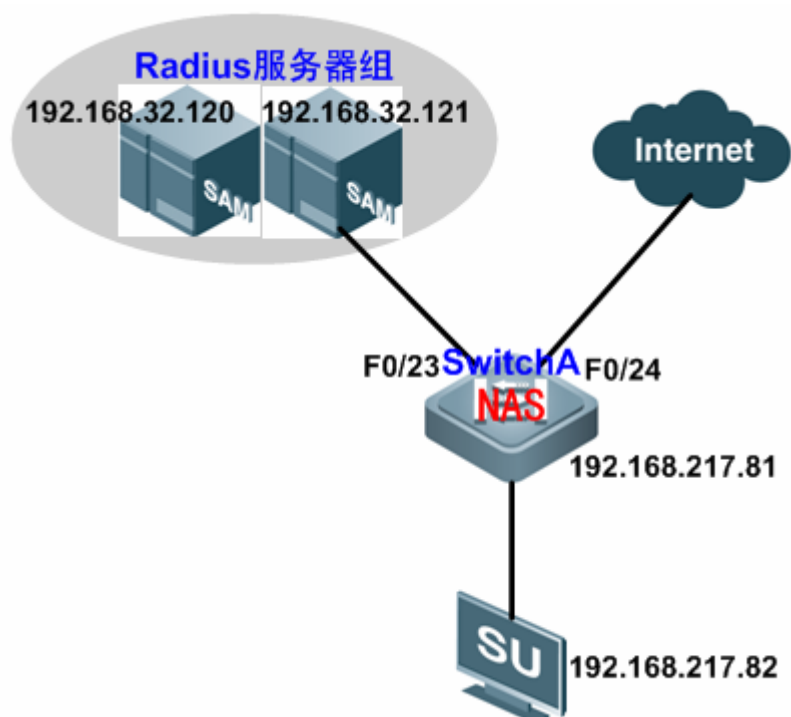
```
Ruijie#show dot1x user id 8
```

```
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 :
```

2.4.4 基于端口的用户 1X认证及IP授权应用

拓扑图

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。

3 SSH 终端服务

3.1 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。

3.2 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）

3.3 锐捷SSH支持

3.4 SSH配置

3.4.1 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

3.4.2 用户认证配置

1. 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)
2. 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。

3.4.3 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
Step 1	Ruijie# configure terminal	进入配置模式
Step 2	Ruijie(config)# enable service ssh-server	打开 SSH Server
Step 3	Ruijie(config)# crypto key generate {rsa dsa}	生成密钥

注意

1. 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。
2. SSH 模块不支持热备，因此在支持热备的产品中，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。

3.4.4 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
Step 1	Ruijie# configure terminal	进入配置模式
Step 2	Ruijie(config)# no enable service ssh-server	关闭 SSH Server

3.4.5 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
Step 1	Ruijie# configure terminal	进入配置模式
Step 2	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；

3.4.6 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
Step 1	Ruijie# configure terminal	进入配置模式
Step 2	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；

3.4.7 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
Step 1	Ruijie# configure terminal	进入配置模式
Step 2	Ruijie(config)# ip ssh authentication-retries <i>retry times</i>	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

注：上述命令具体配置请参见[SSH 命令参考手册]。

3.4.8 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
Step 1	Ruijie# configure terminal	进入配置模式
Step 2	Ruijie(config)# ip ssh peer test public-key rsa <i>flash:rsa.pub</i>	设置用户 <i>test</i> 关联的 RSA 公钥文件
Step 3	Ruijie(config)# ip ssh peer test public-key dsa <i>flash:dsa.pub</i>	设置用户 <i>test</i> 关联的 DSA 公钥文件

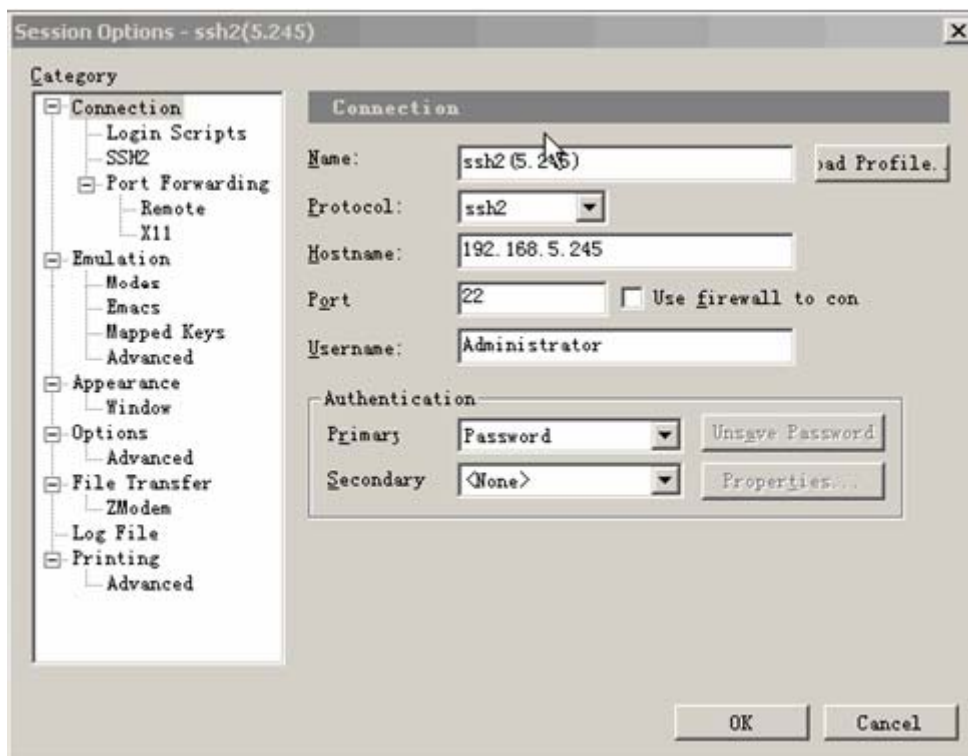
3.4.9 配置SCP服务功能

在网络设备上打开 SCP 服务功能，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
Step 1	Ruijie# configure terminal	进入配置模式
Step 2	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

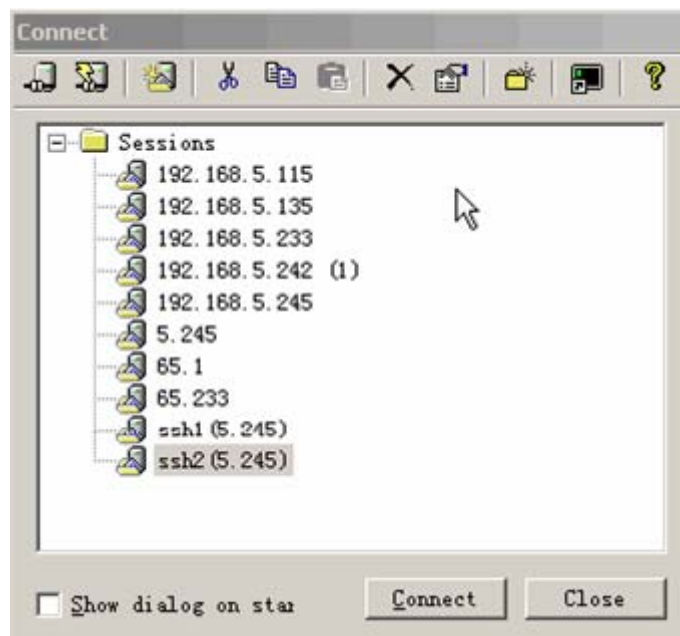
3.5 使用SSH进行设备管理

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：



如图 1 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：



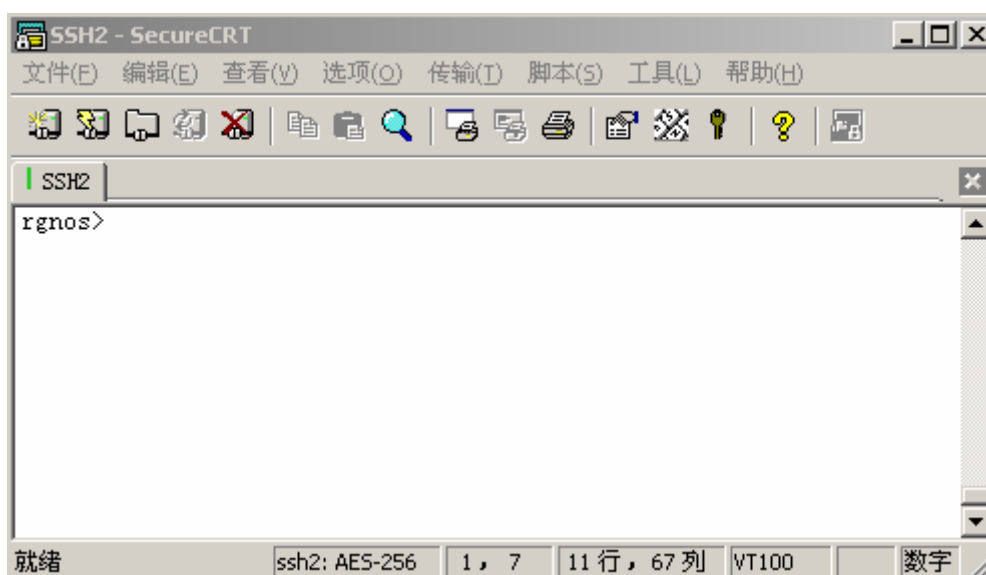
点击 Connect，登陆我们刚才配置的主机，如下图：



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:



此时输入 Telnet 登陆密码就可以进入和 Telnet 一样的界面了。如下图所示:

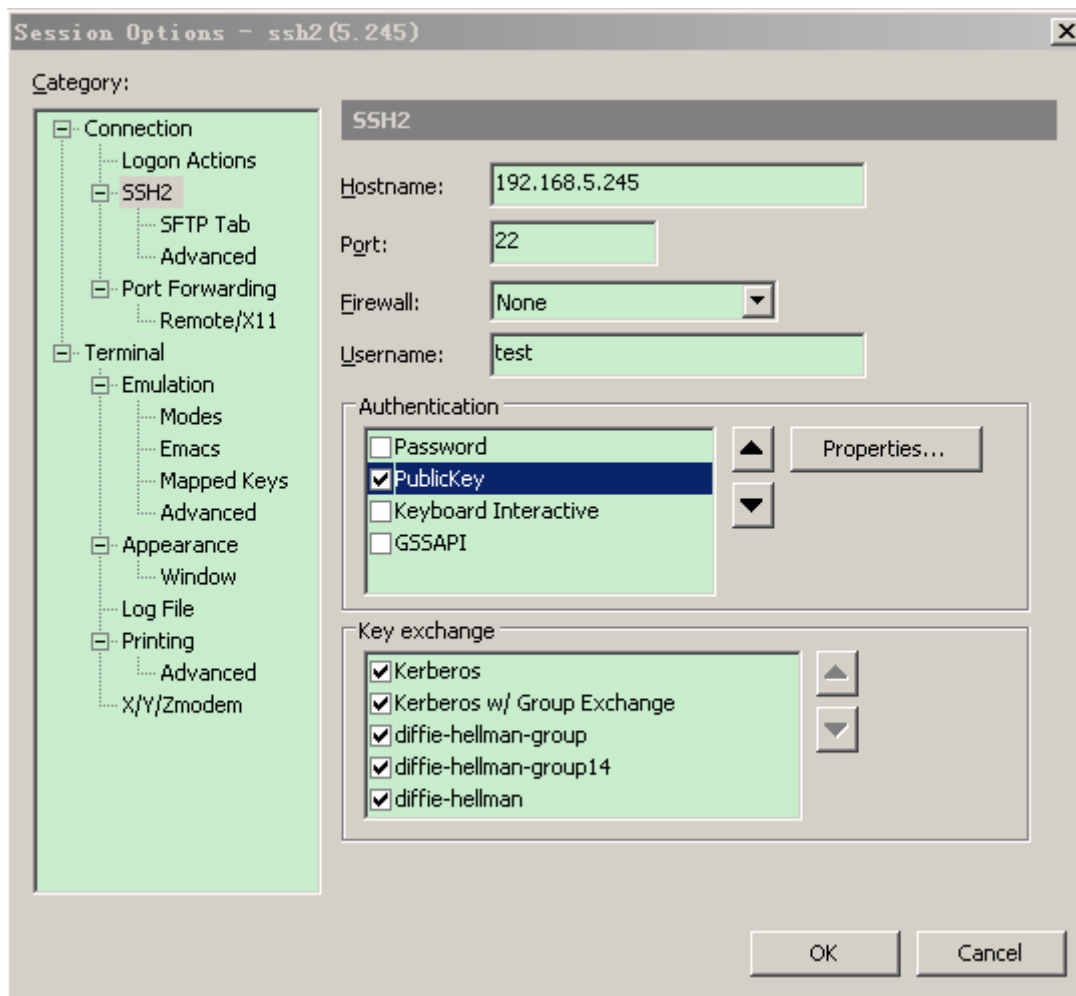


3.6 使用SSH基于公钥的认证

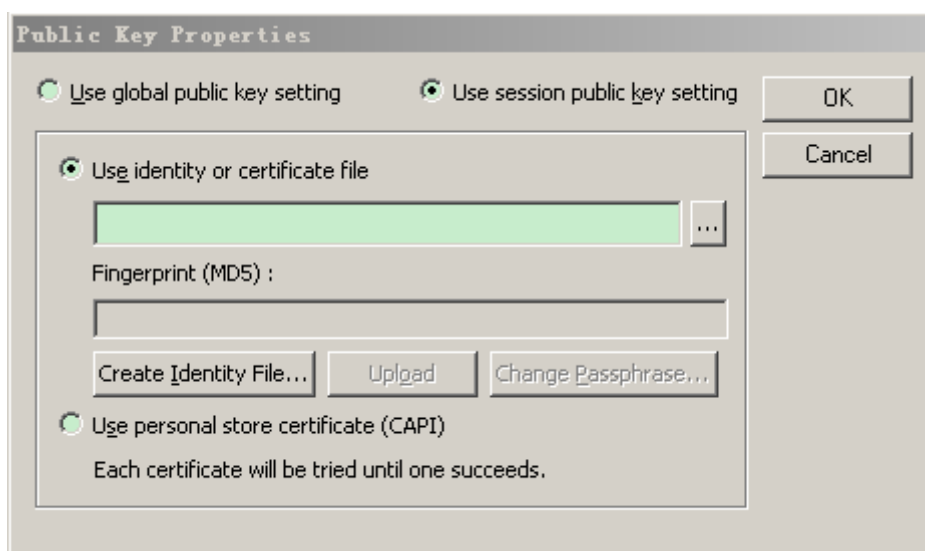
客户端操作

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。

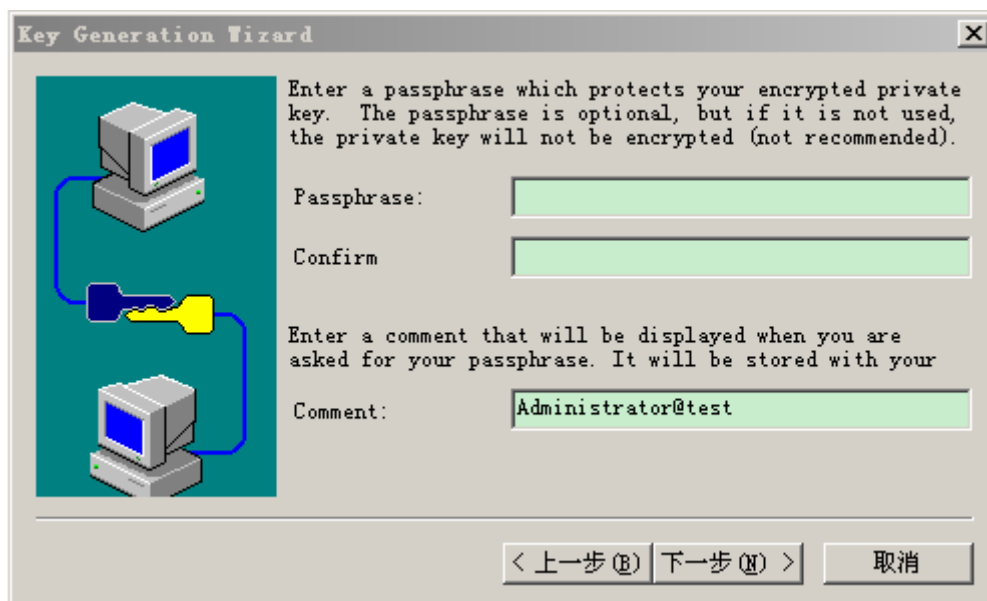
首先, 在 **Session Option** 中 **Authentication** 选项, 选择 **PublicKey**, 然后选择 **Properties**。如下:



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的公钥是一对的，否则不能认证通过。如下：

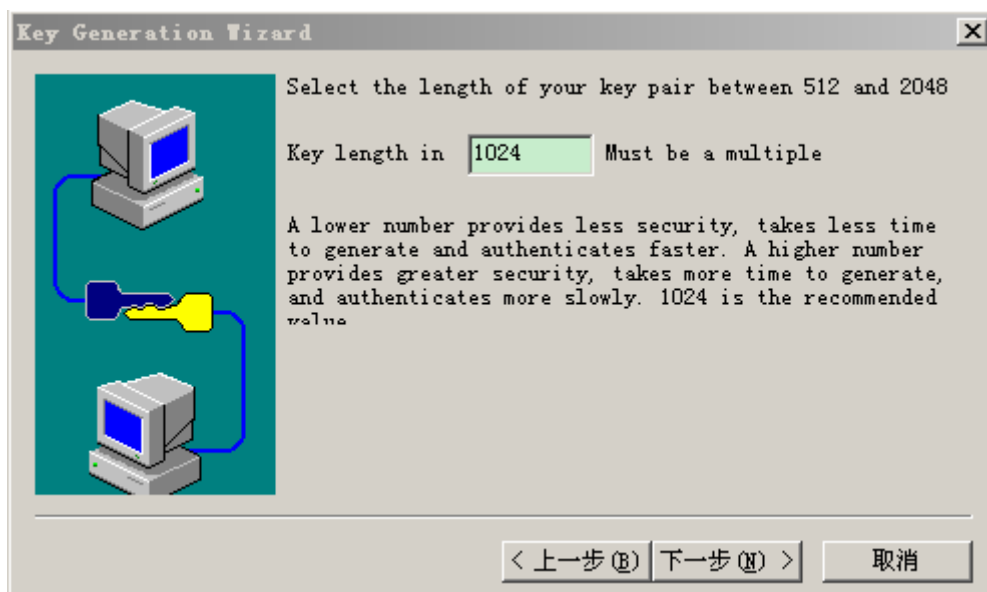


如果没有生成过，可以生成一个新的密钥对（**Create Identity File**）。在生成密钥中，可以为私钥再设置一个口令（可以为空），如果设置，则每次认证都需要输入这个口令。如下：



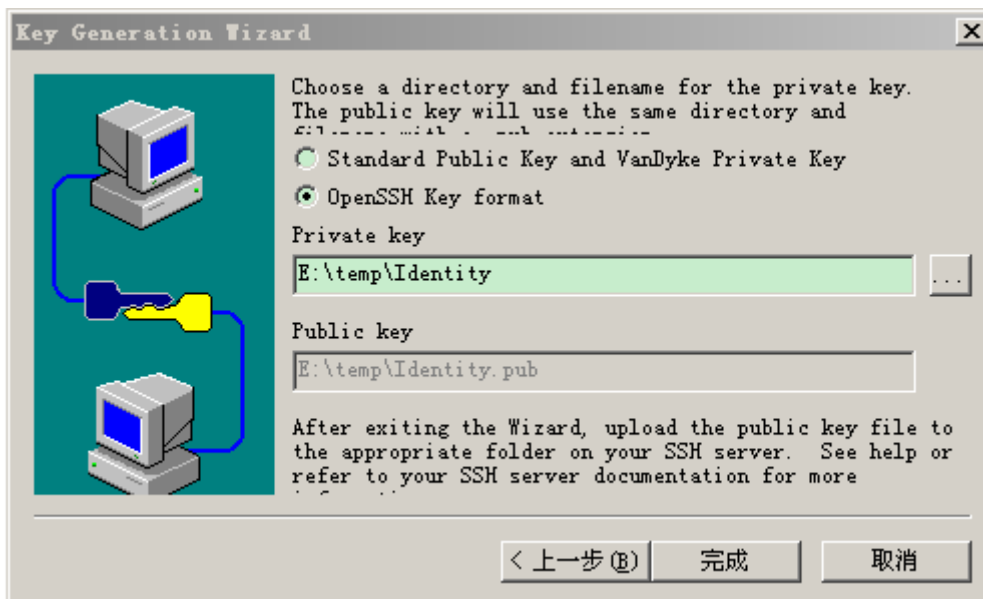
⚡ 注意

1. 生成密钥的时候要不断晃动鼠标，否则速度极慢。
2. 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。



⚡ 注意

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。



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。

3.7 使用SSH进行文件传输

服务器端操作

SSH 文件传输使用的是 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
```

 注意

1. 选项大部分与客户端有关, 少数是客户端和服务端都需要支持的选项, 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。
2. 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。

4 配置 CPU 保护

4.1 概述

4.1.1 CPU Protect的作用

在网络环境中经常发现一些恶意的攻击，这些攻击通常通过伪造各种大量的管理和协议报文使得交换机由于忙于处理这些攻击报文而无暇处理正常管理和协议报文，从而给交换机的安全以及网络的稳定带来破坏性的影响。

锐捷网络交换机通过提供 CPU Protect Policy(CPP)功能，能够有效的抵御网络中的恶意攻击，CPP 功能通过有报文识别以及攻击报文抑制达到。

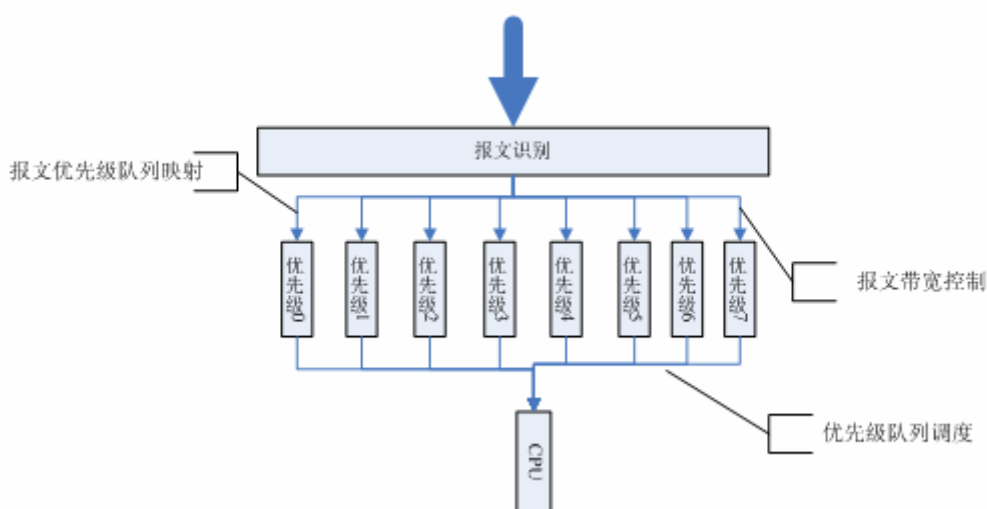
削弱攻击报文对交换机的影响(交换机处理器保护)。

保障不同优先级队列的报文得到均衡处理。

同时 CPP 提供灵活的报文策略配置，以方便网络管理员针对具体的网络环境进行特殊优化配置，从而保障交换机的安全以及网络的稳定。

4.1.2 CPU Protect的原理

CPP 功能通过报文识别、报文带宽控制、报文优先级队列映射以及队列调度这四项技术实现交换机处理器资源保护以及重要报文保障。



CPP 工作原理

报文识别

所有送到交换机进行协议处理的报文首先通过报文识别处理过程将报文进行分类，例如ARP、BPDU、GVRP等等(各产品的数据分类参看CPU Protect默认值章节)。

报文带宽控制

管理员可以配置每种类型报文带宽，通过这种方式可以有效地抑制网络中高速率的攻击报文。

报文优先级队列映射

交换机处理器共有 8 个优先级队列，通过配置每种类型报文的优先级队列可以将报文映射到相应的队列中。

队列调度

为了保证不同优先级队列的协议报文都能及时的送往 CPU 处理，当前采用轮询调度算法。在轮询调度算法中，每个队列的调度权重相等。

4.2 配置CPU Protect

4.2.1 配置每种类型报文的带宽

在全局配置模式下，按如下步骤设置每种类型报文的带宽：

	命令	作用
Step 1	Ruijie(config)# cpu-protect type {arp bpdu dhcp ipv6mc igmp rip ospf vrrp pim err-ttl unknown-ipmc dvmrp ...} pps pps_vaule	设置报文对应的带宽, <i>pps_value</i> 为整数。其中...表示为列举完的类型，具体每个产品支持的类型见 CPU Protect 的默认值章节描述。文档后续不再重复对...描述。
Step 2	Ruijie# end	退回到特权模式。

配置 BPDU 报文的带宽为 200 pps：

```
Ruijie(config)#cpu-protect type bpdu pps 200
Set packet type bpdu pps 100.
```

4.2.2 配置每种类型报文的优先级队列

在全局配置模式下，按如下步骤设置每种类型报文的优先级队列：

	命令	作用
Step 1	Ruijie(config)# cpu-protect type {arp bpdu dhcp ipv6mc igmp rip ospf vrrp pim err-ttl unknown-ipmc ...} pri pri_vaule	设置报文对应的优先级队列， <i>pri_vaule</i> 为整数。
Step 2	Ruijie# end	退回到特权模式。

配置 BPDU 报文的优先级队列为 7：

```
Ruijie(config)# cpu-protect type bpdu pri 7
Set packet type bpdu priority 7.
```

4.2.3 CPU Protect的默认值

以下是各系列交换机能够识别的报文类型以及出厂时的默认配置，通过执行 **no cpu-protect type** 命令，可以把报文的最大带宽和优先级队列设置恢复为默认值。

报文类型	描述	带宽(pps)	优先级队列
tp-guard	Topology Protection Protocol(TPP)协议报文	180	7
arp	ARP 协议报文	180	5
dot1x	802.1X EAPOL 报文	2000	4
rldp	Rapid Link Detection Protocol(RLDP)协议报文	180	7
bpdu	BPDU 协议报文	180	6

tunnel-bpdu	BPDU 隧道报文	180	6
dhcps-ipv4	DHCP V4 Snooping 报文	180	4
dhcps-ipv6	DHCP V6 Snooping 报文	600	4
gvrp	IEEE GVRP 协议报文	180	4
tunnel-gvrp	GVRP 隧道报文	180	3
igmp	IGMP 协议报文	180	3
mld	Mld 协议报文	600	3
stargv	组播* GVV4 报文	180	0
stargvv6	组播*GV V6 报文	180	0
unknown-ipmcv4	未知名的 IPV4 组播报文	180	2
err-ttl0	TTL=0 的 IPV4 报文	180	0
err-ttl1	TTL=1 的 IPV4 报文	180	0
ttl1-ipmcv6	未知名的 IPV6 组播报文	600	0
error-hop-limit	TTL=0/1 的 IPV6 单播报文	600	0
unknown-ipmcv6	未知 ipv6 组播报文	600	2
ipv6mc	IPV6 多播报文	600	0
dhcpx4-relay-s	DHCP V4 Relay 功能 DHCP Server 报文	180	4
dhcpx4-relay-c	DHCP V4 Relay 功能 DHCP Client 报文	180	4
option82	DHCP Option82 报文	180	4
udp-helper	UDP Helper 功能识别的 UDP 广播报文	180	4
dhcp-client	DHCP CLIENT 报文	180	4
nd-snp-ns-na	ND SNOOPING 邻居请求和邻居公告报文	600	3
nd-snp-rs	ND SNOOPING 路由器请求报文	600	4
nd-snp-ra-redirect	ND SNOOPING 路由器公告和重定向报文	600	4

4.3 查看CPU Protect信息

4.3.1 查看管理板/单机/堆叠系统的接收报文的统计信息

使用如下命令查看 CPP 管理板/单机/堆叠系统的接收报文的统计信息：

Step 1	命令	作用
	Ruijie# show cpu-protect mboard	查看管理板/单机/堆叠系统的接收报文的统计信息

以下例子是查看 CPP 管理板信息：

Ruijie# show cpu-protect mboard

Type	Pps	Total	Drop
tp-guard	0	0	0
arp	0	13	0
dot1x	0	0	0
rldp	0	0	0
rerp	0	0	0
reup	0	0	0
slow-packet	0	0	0
bpdu	0	0	0
isis	0	0	0
dhcps	0	0	0
gvrp	0	0	0
ripng	0	0	0
dvmrp	0	0	0
igmp	0	0	0
mpls	0	0	0
ospf	0	0	0
ospf3	0	0	0
pim	0	0	0
pimv6	0	0	0
rip	0	0	0
vrrp	0	0	0
vrrp6	0	0	0
dhcps6	0	0	0
dhcp6_client	0	0	0
dhcp6_server	0	0	0
mld	0	0	0
nd-snp-ns-na	0	0	0
nd-snp-rs	0	0	0
nd-snp-ra-redirect	0	0	0
unknown-ipmc	0	0	0
unknown-ipmcv6	0	0	0
stargv-ipmc	0	0	0
stargv6-ipmc	0	0	0
bgp_ttl1	0	34	0
tll1	0	0	0
hop_limit1	0	0	0
mpls-ttl1	0	0	0
tll0	0	22	0
mpls-ttl0	0	0	0
dhcp-relay-c	0	0	0
dhcp-relay-s	0	0	0
option82	0	0	0
udp-helper	0	0	0
tunnel-bpdu	0	0	0
tunnel-gvrp	0	0	0
ip4-packet-local	0	156	0
ip6-packet-local	0	0	0
ip4-packet-other	0	5	0
ip6-packet-other	0	0	0
ipv6mc	0	15	0
non-ip-packet-other	0	0	0

4.3.2 查看线卡接收报文统计信息

使用如下命令查看特定线卡接收报文的统计：

	命令	作用
Step 1	Ruijie# show cpu-protect slot slot_id	查看特定线卡的接收报文。slot_id：插槽号。

下面的示例是显示线卡插槽 2 的 CPU 保护信息。

Ruijie# show cpu-protect slot 2

Type	Pps	Total	Drop
tp-guard	0	0	0
arp	0	3	0
dot1x	0	0	0
rldp	0	0	0
rerp	0	0	0
reup	0	0	0
slow-packet	0	0	0
bpdu	0	0	0
isis	0	0	0
dhcps	0	0	0
gvrp	0	0	0
ripng	0	0	0
dvmrp	0	0	0
igmp	0	0	0
mpls	0	0	0
ospf	0	0	0
ospf3	0	0	0
pim	0	0	0
pimv6	0	0	0
rip	0	0	0
vrrp	0	0	0
vrrp6	0	0	0
dhcps6	0	0	0
dhcp6_client	0	0	0
dhcp6_server	0	0	0
mld	0	0	0
nd-snp-ns-na	0	0	0
nd-snp-rs	0	0	0
nd-snp-ra-redirect	0	0	0
unknown-ipmc	0	0	0
unknown-ipmcv6	0	0	0
stargv-ipmc	0	0	0
stargv6-ipmc	0	0	0
bgp_ttl1	0	0	0
ttl1	0	0	0
hop_limit1	0	0	0
mpls-ttl1	0	0	0
ttl0	0	0	0
mpls-ttl0	0	0	0
dhcp-relay-c	0	0	0
dhcp-relay-s	0	0	0
option82	0	0	0
udp-helper	0	0	0
tunnel-bpdu	0	0	0
tunnel-gvrp	0	0	0
ip4-packet-local	0	0	0
ip6-packet-local	0	0	0
ip4-packet-other	0	0	0
ip6-packet-other	0	0	0
ipv6mc	0	5	0
non-ip-packet-other	0	0	0

4.3.3 查看特定类型报文的接收统计信息

使用如下命令查看每种类型报文的接收统计信息：

	命令	作用
Step 1	Ruijie# show cpu-protect type arp bpdudhcp ipv6mc igmp rip ospf vrrp pim ttl1 unknown-ipmc dvmrp	查看每种类型报文的接收统计信息。

以下例子使用 **show cpu-protect type arp** 命令查看 arp 报文的统计信息：

```
Ruijie# show cpu-protect type arp
Slot      Type      Pps      Total      Drop
-----
MainBoard  arp        200      15         0
Slot-2     arp        200      15         0
```

4.3.4 查看所有报文类型的配置信息

使用如下命令查看每种类型报文的优先级队列和带宽：

	命令	作用
Step 1	Ruijie# show cpu-protect summary	查看所有报文类型的配置信息。

以下例子使用 **show cpu-protect summary** 命令查看所有报文类型的配置信息：

```
Ruijie# show cpu-protect summary
Type      Pps      Pri
-----
tp-guard  128      7
arp        10000    3
dot1x     128      4
rldp      128      6
rerp      128      6
reup      128      6
slow-packet 128      6
bpdudhcp  128      6
isis      128      5
dhcps     128      4
gvrp      128      5
ripng     128      5
dvmrp     128      5
igmp      1000     4
mpls      128      5
ospf      2000     5
ospf3     2000     5
pim       128      5
pimv6     128      5
rip       128      5
vrrp      128      6
vrrp6     128      6
dhcps6    128      4
dhcp6_client 128      4
dhcp6_server 128      4
mld       1000     4
nd-snp-ns-na 10000    3
nd-snp-rs  128      4
nd-snp-ra-redirect 128      4
unknown-ipmc 128      3
unknown-ipmcv6 128      3
```

stargv-ipmc	128	3
stargv6-ipmc	128	3
bgp_ttl1	128	1
ttl1	2000	1
hop_limit1	800	1
mpls-ttl1	128	1
ttl0	128	0
mpls-ttl0	128	1
dhcp-relay-c	128	4
dhcp-relay-s	128	4
option82	128	4
udp-helper	128	4
tunnel-bpdu	128	5
tunnel-gvrp	128	5
ip4-packet-local	4096	0
ip6-packet-local	4096	0
ip4-packet-other	200	0
ip6-packet-other	200	0
ipv6mc	128	0
non-ip-packet-other	4096	0

5 配置基于端口的流控制

5.1 风暴控制

5.1.1 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产生风暴。

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。

5.1.2 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
Step 1	<pre>Ruijie(config-if)# storm-control {broadcast multicast unicast} [{ level percent pps packets rate-bps}]</pre>	broadcast 打开对广播风暴的控制功能。 multicast 打开对未知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
```



说明

1. 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。
2. 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。

5.1.3 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
Step 1	Ruijie# 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
```

5.1.4 配置风暴控制全局模式

风暴控制全局模式配置命令如下：

	命令	作用
Step 1	Ruijie(config)# storm-control-mode {kbps level pps}	kbps 配置风暴控制全局模式为 kbps level 配置风暴控制全局模式为 level pps 配置风暴控制全局模式为 pps

通过命令 **no storm-control-mode** 配置命令将风暴控制全局模式恢复为缺省 kbps 模式

下面的例子说明了如何配置风暴控制全局模式

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# storm-control-mode level
Ruijie(config)# end
```



说明

端口限速功能需要在风暴控制全局模式为 kbps 模式下才可以配置，当配置风暴控制全局模式为非 kbps 模式时，在端口上配置端口限速将提示配置失败。

5.1.5 查看风暴控制全局模式

	命令	作用
Step 1	Ruijie# show storm-control-mode	查看风暴控制全局模式

通过命令 **show storm-control-mode** 来查看当前设置的风暴控制全局模式

```
Ruijie# show storm-control-mode
%the global storm-control-mode is: kbps
```

5.2 Protected Port

5.2.1 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。

5.2.2 配置Protected Port

设置接口为保护口：

	命令	作用
Step 1	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
```

5.2.3 显示Protected Port配置

	命令	作用
Step 1	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
```

5.3 端口安全

5.3.1 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。

5.3.2 配置端口安全

5.3.2.1 端口安全的缺省配置

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

5.3.2.2 端口安全配置指导

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。

5.3.2.3 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
Step 1	<code>Ruijie(config-if)# switchport port-security</code>	打开该接口的端口安全功能
Step 2	<code>Ruijie(config-if)# switchport port-security maximum value</code>	设置接口上安全地址的最大个数，缺省值为 128。
Step 3	<code>Ruijie(config-if)# switchport port-security violation {protect restrict shutdown}</code>	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 <code>errdisable recovery</code> 来将接口从错误状态中恢复过来。
Step 4	<code>Ruijie(config-if)# switchport port-security mac-address sticky</code>	启用 Sticky MAC 地址学习功能

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` 来关闭 Sticky Mac 学习功能。

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
```

 说明

1. 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；
2. 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；
3. 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；
4. 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。

5.3.2.4 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
Step 1	Ruijie(config)# switch port port-security interface <i>interface-id</i> mac-address <i>mac-address</i> vlan [<i>vlan_id</i>]	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
Step 1	Ruijie(config-if)# switchport port-security [mac-address <i>mac-address</i>] vlan [<i>vlan_id</i>]	接口模式下，手工配置接口上的安全地址。
Step 2	Ruijie(config-if)# switchport port-security [mac-address sticky <i>mac-address</i>] vlan [<i>vlan_id</i>]	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：

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitethernet 0/3
Ruijie(config-if)# no switchport port-security mac-address sticky
00d0.f800.073c vlan 1
Ruijie(config-if)# end
```

5.3.2.5 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
Step 1	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
Step 1	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
```

说明

1. 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。

5.3.2.6 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
Step 1	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。<i>Time</i> 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 gigabitethernet 0/3
Ruijie(config-if)# switchport port-security aging time 8
Ruijie(config-if)# switchport port-security aging static
Ruijie(config-if)# end
```

5.3.3 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
Step 1	Ruijie# show port-security interface [interface-id]	查看接口的端口安全配置信息
Step 2	Ruijie# show port-security address	查看安全地址信息
Step 3	Ruijie# show port-security binding	查看安全地址绑定信息
Step 4	Ruijie# show port-security address [interface-id]	显示某个接口上的安全地址信息
Step 5	Ruijie# 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 **gigabitethernet 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				

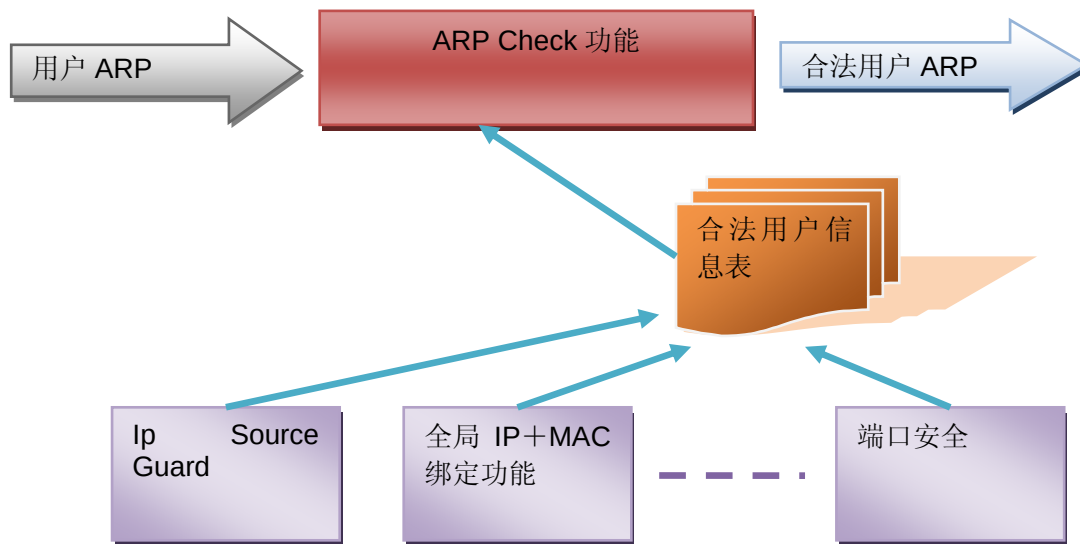
5.4 ARP-Check功能

5.4.1 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。

5.4.2 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。



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。

注意:

1. 打开 ARP Check 检测功能有可能会使相关安全应用的策略数/用户数减少

5.4.3 配置ARP-Check

从特权模式下开始配置 ARP-Check 功能

命令	作用
Ruijie# configure t	进入配置模式
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

5.4.3.1 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
Ruijie# 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

6 配置DoS保护

6.1 DoS保护配置

6.1.1 概述

DoS 保护功能支持防 Land 攻击、防非法 TCP 报文攻击。自身消耗攻击。

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。

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。

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：

1. **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。

2. **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。

3. **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。

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。

☺各产品支持情况

设备在开启防非法 TCP 报文攻击功能时，无法对以下两种报文生效：没有设置任何标志的 TCP 报文和设置了 FIN 标志却没有设置 ACK 标志的 TCP 报文。

6.1.2 配置DoS保护

6.1.2.1 缺省的Dos保护设置

下面列出 DoS 缺省配置：

功能特性	缺省值
land attack	Off
against invalid tcp attack	Off
against invalid l4-port attack	Off

6.1.2.2 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
Step 1	Ruijie# configure terminal	进入全局配置模式
Step 2	Ruijie(config)# ip deny land	开启防 Land 攻击功能
Step 3	Ruijie(config)# end	退回到特权模式

6.1.2.3 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
Step 1	Ruijie# configure terminal	进入全局配置模式
Step 2	Ruijie(config)# ip deny invalid-tcp	开启防非法 TCP 报文攻击功能
Step 3	Ruijie(config)# end	退回到特权模式

6.1.2.4 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
Step 1	Ruijie# configure terminal	进入全局配置模式
Step 2	Ruijie(config)# ip deny invalid-l4port	开启防自身消耗攻击功能
Step 3	Ruijie(config)# end	退回到特权模式

6.1.3 显示DoS保护的状态

6.1.3.1 显示防Land攻击的状态

在特权用户模式下，执行如下命令可以显示防 Land 攻击的状态：

命令	作用
Ruijie# 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
```

6.1.3.2 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
Ruijie# 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
```

6.1.3.3 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
```

6.2 防DOS攻击的入口过滤

6.2.1 概述

近年来，各种 DoS 攻击（Denial of Service，拒绝服务）报文在互联网上传播，给互联网用户带来很大烦恼。DoS 的攻击方式有很多种，最基本的 DoS 攻击就是利用合理的服务请求来占用过多的服务资源，从而使合法用户无法得到服务的响应。攻击报文主要采用伪装源 IP 以防暴露其踪迹。

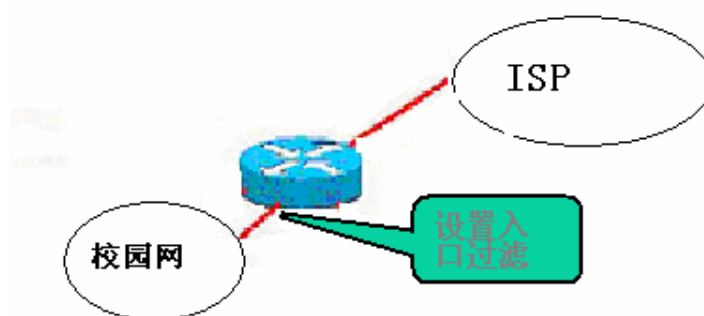
针对这种情况，RFC2827 提出在网络接入处设置入口过滤（Ingress Filtering），来限制伪装源 IP 的报文进入网络。这种方法更注重在攻击的早期和从整体上防止 DoS 的发生，因而具有较好效果。使用这种过滤也能够帮助 ISP 和网管来准确定位使用真实有效的源 IP 的攻击者。ISP 应该也必须采用此功能防止报文攻击进入 Internet；企业（校园网）的网管应该执行过滤来确保企业网不会成为此类攻击的发源地。

锐捷网络交换机采用基于 RFC2827 的入口过滤规则来防止 DoS 攻击，这种过滤是通过自动生成特定的 ACL 来实现，该过滤采用硬件实现而不会给网络转发增加负担。

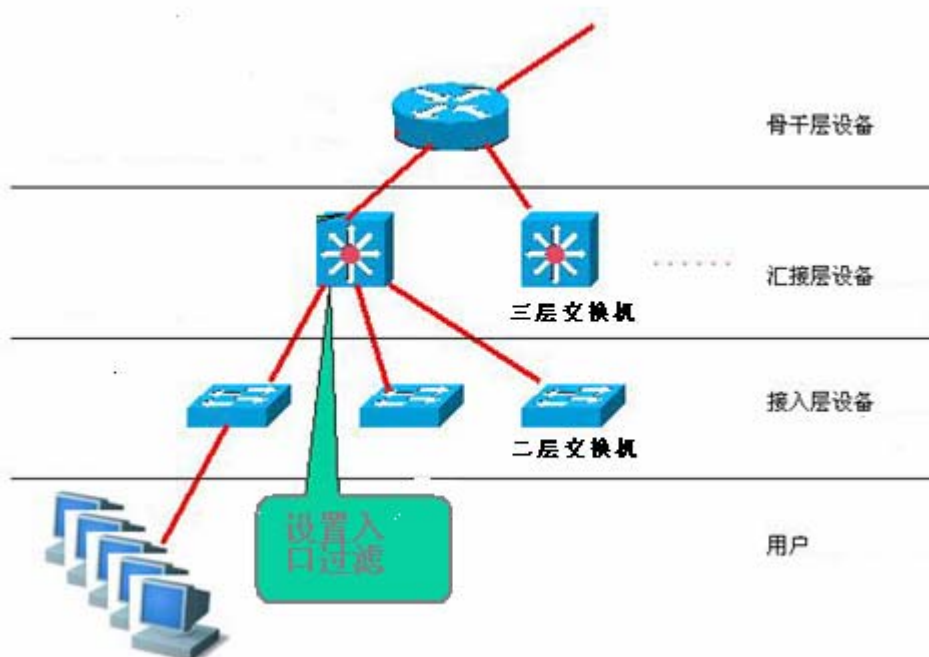
当然，您也可以使用锐捷网络交换机的地址绑定或 Dot1x 功能来达到过滤效果，您也可以通过设置 ACL 来实现过滤。

6.2.2 典型应用案例

A. ISP 在接入路由器上配置，防止伪装源 IP 报文进入 ISP 和 Internet:



B. 企业网（校园网）的三层交换机上配置，防止伪装源 IP 报文进入企业（校园）网:



6.2.3 配置预防DoS攻击的入口过滤

6.2.3.1 默认配置

预防 DoS 攻击的入口过滤在所有网络接口上均关闭。

6.2.3.2 配置注意事项

只有配置了网络地址的三层接口才支持预防 DoS 攻击的入口过滤功能。

用户打开指定三层接口的 **defeat DoS** 入口过滤，系统自动为网络接口动态创建防止伪装源 IP 通过的 ACL，并将其应用到三层接口入口。

例如：SVI 1 上配置的网络地址为 192.168.5.1/24，如果在接口模式下配置 **ip deny spoofing-source**，则会自动生成以下条目的 ACL，并自动关联到该 interface 中：

```
permit 192.168.5.0 0.0.0.255
permit host 0.0.0.0 (该 ACE 是为了通过源地址为 0.0.0.0 的 DHCP 请求报文)
deny any
```



- 只能在直连接口配置该过滤，在和骨干层相连的汇聚层接口(即 **uplink** 口)上设置入口过滤，会造成来自于 **internet** 各种源 **ip** 报文无法到达该汇聚层下链的主机。
- 在设置基于 **defeat DoS** 的入口过滤后，必须通过 **no** 命令关闭 **defeat Dos** 功能，才可以修改网络接口地址。

6.2.4 设置预防DoS攻击的入口过滤

在特权模式下，按如下步骤设置入口过滤：

	命令	作用
Step 1	Ruijie# configure terminal	进入全局配置模式。
Step 2	Ruijie(config)# interface interface-id	进入三层接口
Step 3	Ruijie(config-if)# ip deny spoofing-source	预防伪造源 IP 的 DOS 攻击的入口过滤功能。丢弃所有与此网络接口前缀不符合的输入报文。 (注意：只有三层接口才能配置该功能)
Step 4	Ruijie(config-if)# show running interface interface-id	验证入口过滤配置

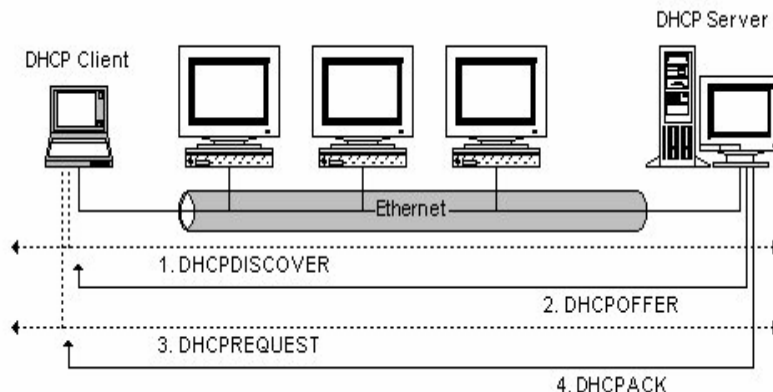
在接口下，使用 **no ip deny spoofing-source** 关掉指定接口的预防 DoS 攻击的入口过滤功能。

7 配置 DHCP Snooping

7.1 DHCP Snooping简介

7.1.1 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 的过程如下所示：



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 分配资源(如 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，请求获取服务器租约，并通告其他服务器已接受此服务器分配地址。

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资源。如果收到 DHCP NAK，则重新发送 DHCP DISCOVER 报文。

7.1.2 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服务器的过滤。下边对 DHCP Snooping 内使用到的一些术语及功能进行一些解释：

1) **DHCP Snooping TRUST 口:** 由于 DHCP 获取 IP 的交互报文是使用广播的形式，从而存在着非法服务器影响用户正常 IP 的获取，更有甚者通过非法服务器欺骗窃取用户信息的现象，为了防止非法服务器的问题，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 Reply 报文，而丢弃所有来自 UNTRUST 口 DHCP Reply 报文，这样我们把合法的 DHCP Server 连接的端口设置为 TRUST 口，其他口设置为 UNTRUST 口，就可以实现对非法 DHCP Server 的屏蔽。

2) **DHCP Snooping 报文过滤:** 在有些环境下，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。

3) **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。

4) **DHCP Snooping 绑定数据库:** 在 DHCP 环境的网络里经常会出现用户私自设置 IP 地址的问题, 用户私设 IP 地址不但使网络难以维护, 并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一个用户记录表项, 从而形成一个 DHCP Snooping 的用户数据库, 配合 ARP 检测功能或 ARP CHECK 功能的使用, 从而达到控制用户上网的目的。

5) **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 请求攻击、控制流向信任网络的 DHCP 请求速率。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, 直接丢弃接口上收到的 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, 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《CPU 保护配置》, NFPP 的配置请查看配置指南《NFPP 配置》。

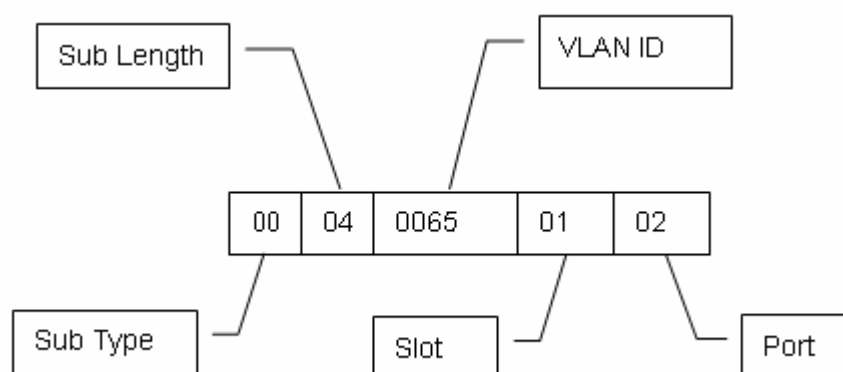
DHCP Snooping 通过对经过设备的 DHCP 报文进行合法性检查, 丢弃不合法的 DHCP 报文, 记录用户信息并生成 DHCP Snooping 绑定数据库供其他功能查询使用。以下几种类型的报文被认为是非法的 DHCP 报文:

- 1)、UNTRUST 口收到的 DHCP reply 报文, 包括 DHCPACK、DHCPNACK、DHCP OFFER 等。
- 2)、UNTRUST 口收到的带有网管信息[giaddr]的 DHCP request 报文。
- 3)、打开 mac 校验时, 源 MAC 与 DHCP 报文携带的 DHCP Client 字段值分别为不同的报文。
- 4)、用户的信息存在于 DHCP Snooping 绑定数据库中, 但是端口信息与设备保存在 DHCP 绑定数据库中的信息中的端口信息不一致的 DHCP RELEASE 报文。

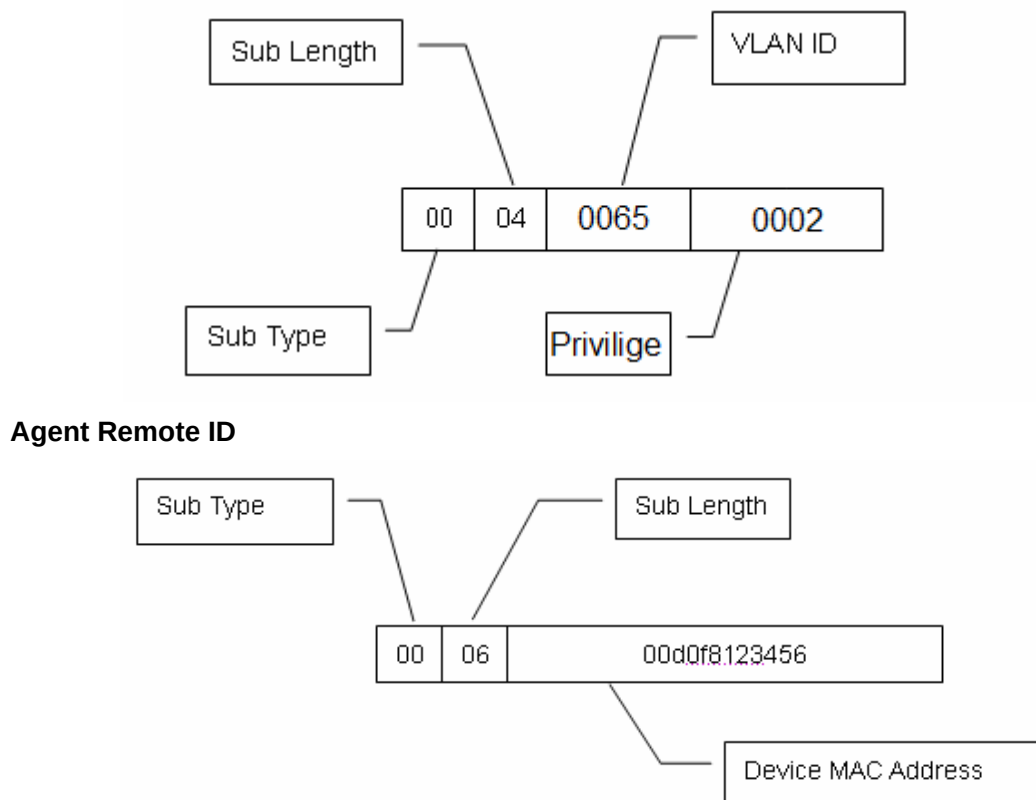
7.1.3 理解 DHCP Snooping information option

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 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, 通过 Option82 上传的内容, 服务器可以获取到更多用户的信息, 从而更准确地给用户分配 IP。DHCP snooping 上传得 Option82 的格式如下, 其中 Circuit ID 包含两种格式, 一种是用于标准和扩展格式, 另一种是用于 DOT1X 格式:

Agent Circuit ID (标准和扩展格式)



Agent Circuit ID (DOT1X 格式)



7.1.4 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私自修改使用静态的 IP 地址,而不是使用动态获取 IP 地址,而使用静态 IP 又会导致一些使用动态获取 IP 的用户的无法正常使用网络,从而使得网络应用环境变复杂,管理员管理网络的难度加大,而 DHCP 动态绑定是指设备在 DHCP snooping 的过程通过记录合法用户的 IP 获取信息,并进行相关记录,从而进行相关的安全处理,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。注意: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,所以会严重影响交换机的性能。

DHCP Snooping 模块和其他安全功能的优先级关系,可参考《产品技术白皮书—端口安全》和《安全功能应用部署产品技术白皮书》。

7.1.4.1 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[ip、mac]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《IP Source Guard 配置》。

DHCP Snooping 通过对 DHCP 过程的窥探,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,从而阻止用户私设 IP。

另外由于 DHCP 绑定只是对 IP 报文进行过滤,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 绑定的用户进行了 ARP 合法性检查,更多信息参考《DAI 配置》。

7.1.4.2 DHCP Snooping和ARP探测的关系

ARP 探测就是对经过设备的所有 ARP 报文进行检查，DHCP Snooping 需要提供数据库信息供 ARP 探测使用，在开启 DAI 功能的设备上，当收到 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。

7.1.4.3 DHCP Snooping和ARP CHECK的关系

ARP CHECK 和 ARP 探测类似，就是对经过设备的所有 ARP 报文进行检查，DHCP Snooping 需要提供数据库信息供 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。

7.1.5 DHCP Snooping配置的其他注意事项

DHCP Snooping 功能与 DHCP Relay 的 DHCP Option 82 功能是互斥的，即不能同时使用 DHCP Snooping 和 DHCP Relay 的 DHCP Option82

DHCP Snooping 仅对用户的 DHCP 过程进行窥探，若想控制用户必须使用 DHCP 分配的 IP 上网，则必须使用 ARP 探测功能，而 ARP 检测模块需要检测所有 ARP 报文，所以会对设备的整体性能产生影响，需要用户注意。

DHCP Snooping 采用 Hybrid 类型的接口通过 untagged VLAN 连接 DHCP 服务器的模型下必须打开 Share VLAN 功能，并将 untagged VLAN 配置为 share VLAN，系统可配置的 Share VLAN 个数请参看配置指南中 Share VLAN 章节。

7.2 DHCP Snooping配置

7.2.1 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
Step 1	Ruijie# configure terminal	进入配置模式
Step 2	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
```

7.2.2 配置端口过滤DHCP报文

缺省情况下,设备端口的 DHCP 请求报文过滤功能是关闭的,当配置功能之后,就打开端口 DHCP 请求报文过滤功能。

	命令	作用
Step 1	Ruijie# configure terminal	进入配置模式
Step 2	Ruijie(config)# interface interface	进入接口配置模式
Step 3	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
```

7.2.3 配置DHCP Snooping功能生效的VLAN

配置 DHCP Snooping 在对应的 VLAN 上生效,将该 VLAN 添加到 DHCP Snooping 生效的 VLAN 范围中;

	命令	作用
Step 1	Ruijie# configure terminal	进入配置模式
Step 2	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
Ruijie#
```



注意

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。

7.2.4 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报文。默认不检查。

	命令	作用
Step 1	Ruijie# configure terminal	进入配置模式
Step 2	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

```

7.2.5 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
Step 1	Ruijie# configure terminal	进入配置模式
Step 2	Ruijie(config)# [no] ip dhcp snooping information option [standard-format dot1x-format]	设置 DHCP snooping information option，包括扩展、标准以及 DOT1X 格式的 Option82
Step 3	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。
Step 4	Ruijie(config)# interface interface	进入接口配置模式
Step 5	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。
Step 6	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

```



注意

当配置此功能后，DHCP relay 的 information option82 功能就会失效。

7.2.6 配置定时写DHCP Snooping数据库信息到flash

为了防止设备断电重启导致设备上的 DHCP 用户信息丢失，所以 DHCP Snooping 提供可配置的定时把 DHCP Snooping 数据库信息写入 flash 的命令，默认情况下，定时为 0，即不定时写 flash。

命令	作用

Step 1	Ruijie# configure terminal	进入配置模式
Step 2	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#
```



注意

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。

7.2.7 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,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
Step 1	Ruijie# configure terminal	进入配置模式
Step 2	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
```

7.2.8 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
Step 1	Ruijie# configure terminal	进入配置模式
Step 2	Ruijie(config)# interface interface	进入接口配置模式
Step 3	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   :  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
```

**注意**

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。

7.2.9 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对应接口上收到 DHCP 报文的速率：

	命令	作用
Step 1	Ruijie# configure terminal	进入配置模式
Step 2	Ruijie(config)# interface interface	进入接口配置模式
Step 3	Ruijie(config-if)# [no] ip dhcp snooping limit rate rate-pps	设置端口接收 DHCP 报文的速率

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
 nfpd dhcp-guard policy per-port 100 200
```

**注意**

1.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。

2.从上面的 show run interface 结果可以看出， 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。

7.2.10 清空DHCP Snooping数据库动态用户信息

此命令用于清空当前的 DHCP Snooping 数据库的信息。

	命令	作用
Step 1	Ruijie# clear ip dhcp snooping binding	清空当前数据库的信息

下边的是手动清空当前数据库的信息：

```
Ruijie# clear ip dhcp snooping binding
```

7.3 DHCP snooping配置显示

7.3.1 显示DHCP snooping

您可以通过以下步骤显示 ip dhcp snooping 内容

	命令	作用
Step 1	Ruijie# 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  :  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
```

7.3.2 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

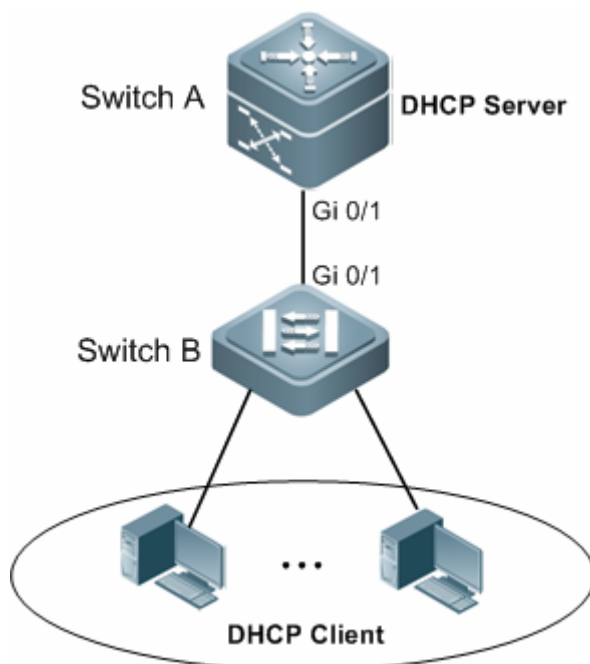
	命令	作用
Step 1	Ruijie# show ip dhcp snooping binding	查看 DHCP Snooping 绑定数据库的用户信息

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        863996      dhcp-snooping  1     GigabitEthernet 0/5
```

DHCP Snooping典型配置用例

7.3.2.1 拓扑图



DHCP Snooping 用例示意图

7.3.2.2 应用需求

DHCP 客户端用户通过合法 DHCP 服务器动态获取 IP 地址。

避免其他用户私设 DHCP 服务器。

7.3.2.3 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。

7.3.2.4 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
```

7.3.2.5 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
```

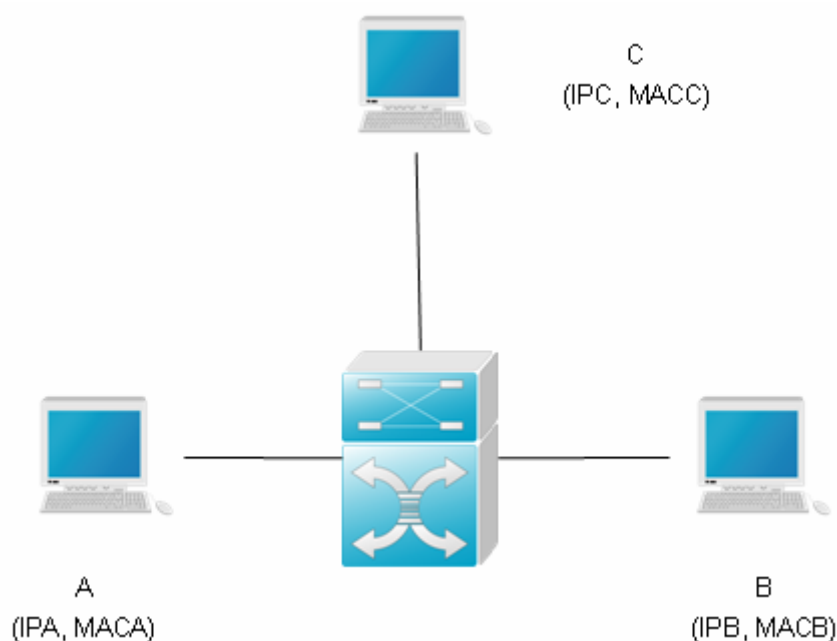
8 配置动态 ARP 检测

8.1 了解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。

8.1.1 了解ARP 欺骗攻击

由于 ARP 协议本身的缺陷, ARP 协议本身不对收到的 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, 最典型的的就是中间人攻击。中间人攻击描述如下:



如图所示: 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/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。

8.1.2 了解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。

释放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，具体请参考相应的配置指导《DHCP snooping 配置》。

8.1.3 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。



注意

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**。

8.2 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）

8.2.1 启用指定VLAN的DAI报文检查功能

缺省情况下，所有 VLAN 的 DAI 报文检查功能是关闭的。

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 <i>vlan-id</i>	启用 VLAN <i>vlan-id</i> 的 DAI 报文检查功能开关
Ruijie(config)# no ip arp inspection vlan [<i>vlan-id</i>]	关闭 VLAN <i>vlan-id</i> 的 DAI 报文检查功能开关 省略 <i>vlan-id</i> 时关掉所有 VLAN 的 DAI 报文检查功能

8.2.2 设置端口的信任状态

此命令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。

缺省情况下，所有二层端口都是不可信任的。

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

8.2.3 DHCP snooping database相关配置

参考《DHCP Snooping 配置》。

如果没有配置 DHCP Snooping database，则所有 ARP 报文通过检查

8.3 显示DAI配置

8.3.1 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
Ruijie(config)# show ip arp inspection vlan	显示各 VLAN 的启用状态

8.3.2 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
Ruijie(config)# show ip arp inspection interface	显示各二层接口的 DAI 配置（包括信任状态）

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。

9 配置 IP Source Guard

9.1 IP Source Guard简介

9.1.1 理解DHCP

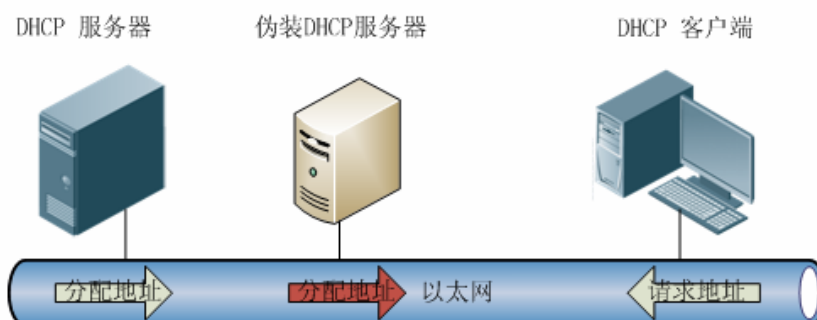
在典型的 DHCP 环境中，DHCP 服务器负责网络中地址的管理和分配，网络中的主机如果想要使用网络资源，必须向 DHCP 服务器申请合法的地址，只有获得了合法地址的客户端才能正常使用网络；



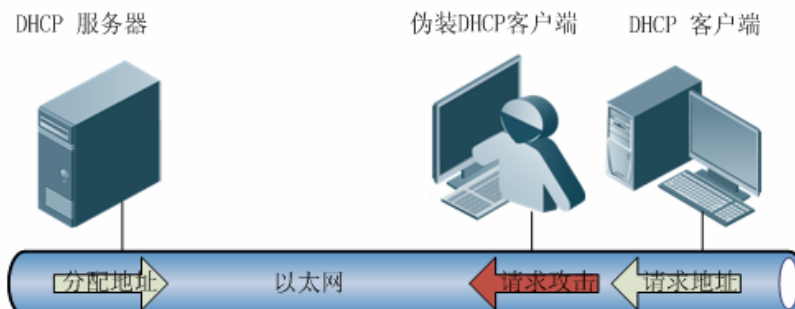
正常的 DHCP 地址分配

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；

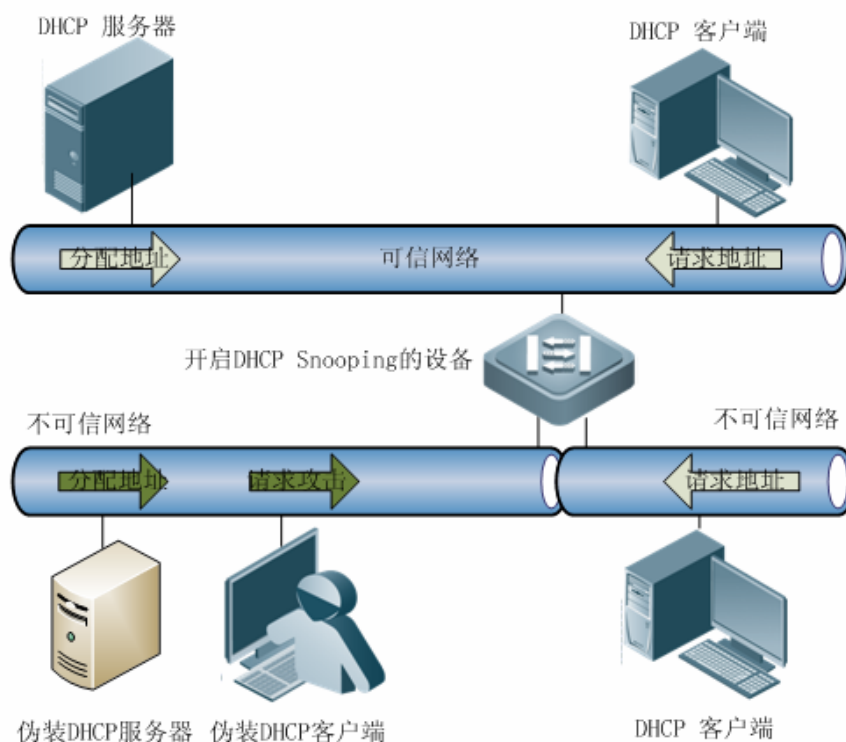
DHCP Snooping 的引入解决这一问题，在连接 DHCP 服务器与客户端的设备上开启 DHCP Snooping 功能，就可以解决传统 DHCP 模型中的大部分安全；DHCP Snooping 将网络分为两个部分：客户端网络-非信任网络，对来自该网络上的客户端请求进行安全检测；服务器网络-信任网络，将收到的合法的客户端请求转发到配置的信任服务器网络，由服务器完成地址的统一管理分配；通过这种方式，DHCP Snooping 解决了传统 DHCP 模型中的几个典型的安全问题：



存在伪装 DHCP 服务器的网络



存在伪装 DHCP 客户端进行攻击的网络



通过 DHCP Snooping 进行保护的网路

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；

9.1.2 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 设备上对客户端的进行严格过滤；

默认情况下，打开 IP Source Guard 的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，端口将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，IP Source Guard 功能开启后 ARP Check 默认配置下也将同时开启 ARP Check 功能，此时交换机使用 IP Source Guard 对 IP 报文进行 IP+MAC 或仅源 IP 过滤，ARP Check 功能对 ARP 报文中的 Sender IP+Sender MAC 或仅对 Sender IP 检查过滤。

IP Source Guard 的相关过滤功能都是基于硬件实现的，接口上的 IP Source Guard 过滤规则可以理解为基于接口的可以动态改变的 ACL，各系列产品的过滤表容量存在差异，因此在规划 IP Source Guard 应用之前请参看相关产品规格说明。

9.1.3 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；

9.2 IP Source Guard配置

9.2.1 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
Step 1	Ruijie(config)# interface interface	进入接口配置模式
Step 2	Ruijie(config)# [no] ip verify source [port-security]	打开接口上的 IP Source Guard 功能 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
```



注意

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。

9.2.2 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
Step 1	Ruijie# configure terminal	进入配置模式
Step 2	Ruijie(config)# [no] ip source binding mac-address vlan vlan_id ip-address interface interface-id	配置静态的 IP 源地址绑定用户到数据库

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
```

**注意**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。

9.3 IP Source Guard配置显示

9.3.1 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
Step 1	Ruijie# 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
```

9.3.2 显示IP源地址绑定数据库信息

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
Step 1	Ruijie# 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
```

10 配置防网关 ARP

10.1 防网关ARP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。

10.1.1 配置防网关ARP欺骗

10.1.1.1 设置防网关ARP欺骗

设置防网关 ARP 欺骗地址：

	命令	作用
Step 1	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。



注意

在上链口上不能配置防网关 ARP 欺骗。

10.1.2 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
Step 1	Ruijie # show anti-arp-spoofing	显示所有接口下的防网关 arp 欺骗信息

11 配置 NFPP

11.1 概述

网络基础保护策略 (Network Foundation Protection Policy),简称 NFPP。

11.1.1 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。

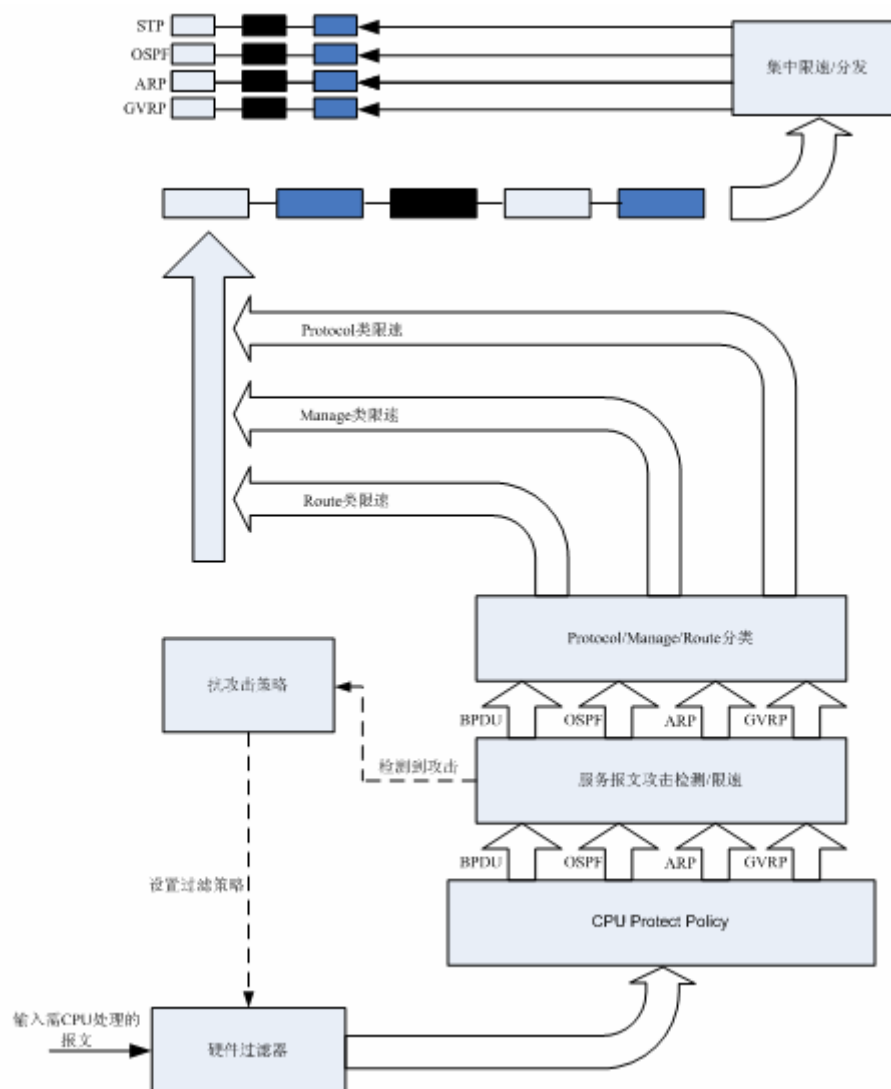
11.1.2 NFPP的原理

如图 1 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。

注意

■ 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。



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。

注意

- 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。

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(Policy)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。

三种分类原则

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。

11.2 配置NFPP

11.2.1 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。

11.2.2 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
Step 1	Ruijie#configure terminal	进入全局配置模式。
Step 2	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
Step 3	Ruijie(config)#end	退回到特权模式。
Step 4	Ruijie#show running-config	查看全局配置
Step 5	Ruijie#copy running-config startup-config	保存配置。

11.2.3 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
Step 1	Ruijie#configure terminal	进入全局配置模式。
Step 2	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
Step 3	Ruijie(config)#end	退回到特权模式。

Step 4	Ruijie#show running-config	查看全局配置
Step 5	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。

11.3 各种协议抗攻击

11.3.1 ARP抗攻击

11.3.1.1 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 拒绝服务攻击，而不是针对 ARP 欺骗或者是解决网络中的 ARP 攻击问题。

11.3.1.1.1 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
Step 1	Ruijie#configure terminal	进入全局配置模式。
Step 2	Ruijie(config)#nfpp	进入 NFPP 配置模式。
Step 3	Ruijie(config-nfpp)#arp-guard enable	全局打开 ARP 抗攻击功能，缺省情况下打开。
Step 4	Ruijie(config-nfpp)#end	退回到特权模式。
Step 5	Ruijie#configure terminal	进入全局配置模式。
Step 6	Ruijie(config)#interface interface-name	进入接口配置模式。
Step 7	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。
Step 8	Ruijie(config-if)#end	退回到特权模式。
Step 9	Ruijie#show nfpp arp-guard summary	核对配置参数

Step 10	Ruijie#copy running-config startup-config	保存配置。

注意

■ 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。

11.3.1.1.2 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
Step 1	Ruijie#configure terminal	进入全局配置模式。
Step 2	Ruijie(config)#nfpp	进入 NFPP 配置模式
Step 3	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。
Step 4	Ruijie(config-nfpp)#end	返回特权模式
Step 5	Ruijie#configure terminal	进入全局配置模式。
Step 6	Ruijie(config)#interface interface-name	进入接口配置模式。
Step 7	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。
Step 8	Ruijie(config-if)#end	退回到特权模式。
Step 9	Ruijie#show nfpp arp-guard summary	核对配置参数
Step10	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。

11.3.1.1.3 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

Step 1	Ruijie#configure terminal	进入全局配置模式。
Step 2	Ruijie(config)#nfpp	进入 NFPP 配置模式
Step 3	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。
Step 4	Ruijie(config-nfpp)#end	退回到特权模式。
Step 5	Ruijie#show nfpp arp-guard summary	核对配置参数
Step 6	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”。

注意

- 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。

11.3.1.1.4 设置受监控主机的最大数目

	命令	作用
Step 1	Ruijie#configure terminal	进入全局配置模式。
Step 2	Ruijie(config)#nfpp	进入 NFPP 配置模式。
Step 3	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。
Step 4	Ruijie(config-nfpp)#end	退回到特权模式。
Step 5	Ruijie#show nfpp arp-guard summary	核对配置参数
Step 6	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。

注意

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。

11.3.1.1.5 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。

注意

- 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-N O_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
Step 1	Ruijie#configure terminal	进入全局配置模式。
Step 2	Ruijie(config)#nfpp	进入 NFPP 配置模式
Step 3	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。
Step 4	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。
Step 5	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。 说明：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。
Step 6	Ruijie(config-nfpp)#end	退回到特权模式。
Step 7	Ruijie#configure terminal	进入全局配置模式。
Step 8	Ruijie(config)#interface interface-name	进入接口配置模式。

Step 9	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。 <i>rate-limit-pps</i> 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。 <i>attack-threshold-pps</i> 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，“per-src-mac”是基于链路层源 MAC/VID/端口识别主机。
Step 10	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。
Step 11	Ruijie(config-if)#end	退回到特权模式。
Step 12	Ruijie#show nfpp arp-guard summary	核对配置参数
Step 13	Ruijie#copy running-config startup-config	保存配置。

11.3.1.1.6 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
Step 1	Ruijie#configure terminal	进入全局配置模式。
Step 2	Ruijie(config)#nfpp	进入 NFPP 配置模式
Step 3	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。
Step 4	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。
Step 5	Ruijie(config-nfpp)#end	退回到特权模式。
Step 6	Ruijie#configure terminal	进入全局配置模式。
Step 7	Ruijie(config)#interface interface-name	进入接口配置模式。

Step 8	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。 <i>rate-limit-pps</i> 是限速水线，取值范围是 1 到 9999。 <i>attack-threshold-pps</i> 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。
Step 9	Ruijie(config-if)#end	退回到特权模式。
Step 10	Ruijie#show nfpp arp-guard summary	核对配置参数
Step 11	Ruijie#copy running-config startup-config	保存配置。

注意

- 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。

11.3.1.1.7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
Step 1	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。

11.3.1.1.8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
Step 1	Ruijie#clear nfpp arp-guard scan	清空 ARP 扫描表

11.3.1.1.9查看ARP抗攻击的相关信息

11.3.1.1.9.1 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
Step 1	Ruijie#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

说明

- 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。

11.3.1.1.9.2 查看受监控主机的信息

	命令	作用
Step 1	Ruijie#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。
Step 2	Ruijie#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
```

说明

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。

11.3.1.1.9.3 查看 ARP 扫描表

	命令	作用
Step 1	Ruijie#show nfpp arp-guard scan statistic	查看 ARP 扫描表的记录条数
Step 2	Ruijie#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)
```

11.3.2 IP 防扫描

11.3.2.1 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。

注意

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。二层交换机不支持 IP 防扫描，仅三层交换机支持 IP 防扫描。

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。

11.3.2.1.1 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
Step 1	Ruijie#configure terminal	进入全局配置模式。
Step 2	Ruijie(config)#nfpp	进入 NFPP 配置模式。
Step 3	Ruijie(config-nfpp)#ip-guard enable	全局打开 IP 防扫描功能，缺省情况下打开。
Step 4	Ruijie(config-nfpp)#end	退回到特权模式。
Step 5	Ruijie#configure terminal	进入全局配置模式。
Step 6	Ruijie(config)#interface interface-name	进入接口配置模式。
Step 7	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。
Step 8	Ruijie(config-if)#end	退回到特权模式。
Step 9	Ruijie#show nfpp ip-guard summary	核对配置参数
Step 10	Ruijie#copy running-config startup-config	保存配置。

注意

- 当关闭 IP 防扫描功能时，系统将自动清除受监控的主机。

11.3.2.1.2 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
Step 1	Ruijie#configure terminal	进入全局配置模式。
Step 2	Ruijie(config)#nfpp	进入 NFPP 配置模式
Step 3	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。
Step 4	Ruijie(config-nfpp)#end	返回特权模式
Step 5	Ruijie#configure terminal	进入全局配置模式。
Step 6	Ruijie(config)#interface interface-name	进入接口配置模式。
Step 7	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。
Step 8	Ruijie(config-if)#end	退回到特权模式。
Step 9	Ruijie#show nfpp ip-guard summary	核对配置参数
Step10	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。

11.3.2.1.3 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
Step 1	Ruijie#configure terminal	进入全局配置模式。
Step 2	Ruijie(config)#nfpp	进入 NFPP 配置模式
Step 3	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。
Step 4	Ruijie(config-nfpp)#end	退回到特权模式。

Step 5	Ruijie#show nfpp ip-guard summary	核对配置参数
Step 6	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”。

注意

- 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。

11.3.2.1.4 设置受监控主机的最大数目

	命令	作用
Step 1	Ruijie#configure terminal	进入全局配置模式。
Step 2	Ruijie(config)#nfpp	进入 NFPP 配置模式。
Step 3	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。
Step 4	Ruijie(config-nfpp)#end	退回到特权模式。
Step 5	Ruijie#show nfpp ip-guard summary	核对配置参数
Step 6	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。

注意

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。

11.3.2.1.5 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
Step 1	Ruijie#configure terminal	进入全局配置模式。
Step 2	Ruijie(config)#nfpp	进入 NFPP 配置模式
Step 3	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。
Step 4	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。
Step 5	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。
Step 6	Ruijie(config-nfpp)#end	退回到特权模式。
Step 7	Ruijie#configure terminal	进入全局配置模式。

Step 8	Ruijie(config)#interface interface-name	进入接口配置模式。
Step 9	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。 <i>rate-limit-pps</i> 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。 <i>attack-threshold-pps</i> 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。
Step 10	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。
Step 11	Ruijie(config-if)#end	退回到特权模式。
Step 12	Ruijie#show nfpp ip-guard summary	核对配置参数
Step 13	Ruijie#copy running-config startup-config	保存配置。

11.3.2.1.6 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
Step 1	Ruijie#configure terminal	进入全局配置模式。
Step 2	Ruijie(config)#nfpp	进入 NFPP 配置模式
Step 3	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。
Step 4	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。
Step 5	Ruijie(config-nfpp)#end	退回到特权模式。
Step 6	Ruijie#configure terminal	进入全局配置模式。
Step 7	Ruijie(config)#interface interface-name	进入接口配置模式。

Step 8	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。 <i>rate-limit-pps</i> 是限速水线，取值范围是 1 到 9999。 <i>attack-threshold-pps</i> 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。
Step 9	Ruijie(config-if)#end	退回到特权模式。
Step 10	Ruijie#show nfpp ip-guard summary	核对配置参数
Step 11	Ruijie#copy running-config startup-config	保存配置。

**注意**

- 基于源 IP 地址限速优先级高于基于端口限速。

11.3.2.1.7 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。

	命令	作用
Step 1	Ruijie#configure terminal	进入全局配置模式。
Step 2	Ruijie(config)#nfpp	进入 NFPP 配置模式
Step 3	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。
Step 4	Ruijie(config-nfpp)#end	退回到特权模式。
Step 5	Ruijie#show nfpp ip-guard trusted-host	查看配置的可信主机
Step 6	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
```

 注意

- 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。

11.3.2.1.8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
Step 1	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。

11.3.2.1.9查看IP防扫描的相关信息

11.3.2.1.9.1 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
Step 1	Ruijie#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

说明

- 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。

11.3.2.1.9.2 查看受监控主机的信息

	命令	作用
Step 1	Ruijie#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。
Step 2	Ruijie#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)
```

说明

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。

11.3.2.1.9.3 查看不监控的可信主机

命令	作用

Step 1

```
Ruijie# 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)
```

11.3.3 ICMP抗攻击

11.3.3.1 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/端口三者结合起来识别的。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。

11.3.3.1.1 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
Step 1	Ruijie#configure terminal	进入全局配置模式。
Step 2	Ruijie(config)#nfpp	进入 NFPP 配置模式。
Step 3	Ruijie(config-nfpp)#icmp-guard enable	打开 ICMP 抗攻击功能，缺省情况下启动。
Step 4	Ruijie(config-nfpp)#end	退回到特权模式。
Step 5	Ruijie#configure terminal	进入全局配置模式。
Step 6	Ruijie(config)#interface interface-name	进入接口配置模式。
Step 7	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。
Step 8	Ruijie(config-if)#end	退回到特权模式。
Step 9	Ruijie#show nfpp icmp-guard summary	核对配置参数
Step 10	Ruijie#copy running-config startup-config	保存配置。



注意

■ 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。

11.3.3.1.2 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
Step 1	Ruijie#configure terminal	进入全局配置模式。
Step 2	Ruijie(config)#nfpp	进入 NFPP 配置模式
Step 3	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。
Step 4	Ruijie(config-nfpp)#end	退回到特权模式。
Step 5	Ruijie#configure terminal	进入全局配置模式。
Step 6	Ruijie(config)#interface interface-name	进入接口配置模式。
Step 7	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。
Step 8	Ruijie(config-if)#end	退回到特权模式。
Step 9	Ruijie#show nfpp icmp-guard summary	核对配置参数
Step10	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。

11.3.3.1.3 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
Step 1	Ruijie#configure terminal	进入全局配置模式。
Step 2	Ruijie(config)#nfpp	进入 NFPP 配置模式

Step 3	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。
Step 4	Ruijie(config-nfpp)#end	退回到特权模式。
Step 5	Ruijie#show nfpp icmp-guard summary	核对配置参数
Step 6	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**”。

注意

- 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。

11.3.3.1.4 设置受监控主机的最大数目

	命令	作用
Step 1	Ruijie#configure terminal	进入全局配置模式。
Step 2	Ruijie(config)#nfpp	进入 NFPP 配置模式。
Step 3	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。
Step 4	Ruijie(config-nfpp)#end	退回到特权模式。
Step 5	Ruijie#show nfpp icmp-guard summary	核对配置参数
Step 6	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。

注意

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。

11.3.3.1.5 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>.
```



注意

■ 当无法为检测到的攻击者分配内存时，打印日志 “%NFPP_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
Step 1	Ruijie#configure terminal	进入全局配置模式。
Step 2	Ruijie(config)#nfpp	进入 NFPP 配置模式。
Step 3	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。
Step 4	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。
Step 5	Ruijie(config-nfpp)#end	退回到特权模式。
Step 6	Ruijie#configure terminal	进入全局配置模式。

Step 7	Ruijie(config)#interface interface-name	进入接口配置模式。
Step 8	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。 <i>rate-limit-pps</i> 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。 <i>attack-threshold-pps</i> 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。
Step 9	Ruijie(config-if)#end	退回到特权模式。
Step 10	Ruijie#show nfpp icmp-guard summary	核对配置参数
Step 11	Ruijie#copy running-config startup-config	保存配置。

11.3.3.1.6 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
Step 1	Ruijie#configure terminal	进入全局配置模式。
Step 2	Ruijie(config)#nfpp	进入 NFPP 配置模式。
Step 3	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。
Step 4	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。。
Step 5	Ruijie(config-nfpp)#end	退回到特权模式。
Step 6	Ruijie#configure terminal	进入全局配置模式。
Step 7	Ruijie(config)#interface interface-name	进入接口配置模式。

Step 8	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。 <i>rate-limit-pps</i> 是限速水线，取值范围是 1 到 9999。 <i>attack-threshold-pps</i> 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。
Step 9	Ruijie(config-if)#end	退回到特权模式。
Step 10	Ruijie#show nfpp icmp-guard configuration	核对配置参数
Step 11	Ruijie#copy running-config tartup-config	保存配置。

**注意**

基于源 IP 地址限速优先级高于基于端口限速。

11.3.3.1.7 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 ping 报文将被允许发往 CPU。

	命令	作用
Step 1	Ruijie#configure terminal	进入全局配置模式。
Step 2	Ruijie(config)#nfpp	进入 NFPP 配置模式。
Step 3	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。
Step 4	Ruijie(config-nfpp)#end	退回到特权模式。
Step 5	Ruijie#show nfpp icmp-guard trusted-host	查看不监控的可信主机。
Step 6	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
```

注意

- 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。

11.3.3.1.8 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
Step 1	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。

11.3.3.1.9 查看ICMP抗攻击的相关信息

11.3.3.1.9.1 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
Step 1	Ruijie#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

说明

- 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：
 - （1）“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。
 - （2）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。

11.3.3.1.9.2 查看受监控主机的信息

	命令	作用
Step 1	Ruijie#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。
Step 2	Ruijie#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)

说明

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。

11.3.3.1.9.3 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
Step 1	Ruijie#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)
```

11.3.4 DHCP抗攻击

11.3.4.1 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 耗尽”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尽 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。

11.3.4.1.1 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
Step 1	Ruijie#configure terminal	进入全局配置模式。
Step 2	Ruijie(config)#nfpp	进入 NFPP 配置模式。
Step 3	Ruijie(config-nfpp)#dhcp-guard enable	打开 DHCP 抗攻击功能，缺省情况下就是打开的。
Step 4	Ruijie(config-nfpp)#end	退回到特权模式。
Step 5	Ruijie#configure terminal	进入全局配置模式。
Step 6	Ruijie(config)#interface interface-name	进入接口配置模式。
Step 7	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。
Step 8	Ruijie(config-if)#end	退回到特权模式。
Step 9	Ruijie#show nfpp dhcp-guard summary	核对配置参数
Step 10	Ruijie#copy running-config startup-config	保存配置。



注意

- 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。

11.3.4.1.2 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
Step 1	Ruijie#configure terminal	进入全局配置模式。
Step 2	Ruijie(config)#nfpp	进入 NFPP 配置模块
Step 3	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。
Step 4	Ruijie(config-nfpp)#end	退回到特权模式。
Step 5	Ruijie#configure terminal	进入全局配置模式。
Step 6	Ruijie(config)#interface interface-name	进入接口配置模式。
Step 7	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。
Step 8	Ruijie(config-if)#end	退回到特权模式。
Step 9	Ruijie#show nfpp dhcp-guard summary	核对配置参数
Step10	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。

11.3.4.1.3 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
Step 1	Ruijie#configure terminal	进入全局配置模式。
Step 2	Ruijie(config)#nfpp	进入 NFPP 配置模式

Step 3	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。
Step 4	Ruijie(config-nfpp)#end	退回到特权模式。
Step 5	Ruijie#show nfpp dhcp-guard summary	核对配置参数
Step 6	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**”。

注意

- 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。

11.3.4.1.4 设置受监控主机的最大数目

	命令	作用
Step 1	Ruijie#configure terminal	进入全局配置模式。
Step 2	Ruijie(config)#nfpp	进入 NFPP 配置模式。
Step 3	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。
Step 4	Ruijie(config-nfpp)#end	退回到特权模式。
Step 5	Ruijie#show nfpp dhcp-guard summary	核对配置参数
Step 6	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。

注意

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。

11.3.4.1.5 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 报文的数据包包含如下描述信息：

```
Failed to isolate host<IP=N/A, MAC=0000.0000.0001,port=Gi4/1,VLAN=1>.
```



注意

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
Step 1	Ruijie#configure terminal	进入全局配置模式。
Step 2	Ruijie(config)#nfpp	进入 NFPP 配置模式。
Step 3	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。
Step 4	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。
Step 5	Ruijie(config-nfpp)#end	退回到特权模式。
Step 6	Ruijie#configure terminal	进入全局配置模式。

Step 7	Ruijie(config)#interface interface-name	进入接口配置模式。
Step 8	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。 <i>rate-limit-pps</i> 是限速水线，取值范围是 1 到 9999。 <i>attack-threshold-pps</i> 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。
Step 9	Ruijie(config-if)#end	退回到特权模式。
Step 10	Ruijie#show nfpp dhcp-guard summary	核对配置参数
Step 11	Ruijie#copy running-config startup-config	保存配置。

11.3.4.1.6 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
Step 1	Ruijie#configure terminal	进入全局配置模式。
Step 2	Ruijie(config)#nfpp	进入 NFPP 配置模式。
Step 3	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。
Step 4	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。
Step 5	Ruijie(config-nfpp)#end	退回到特权模式。
Step 6	Ruijie#configure terminal	进入全局配置模式。
Step 7	Ruijie(config)#interface interface-name	进入接口配置模式。

Step 8	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。 <i>rate-limit-pps</i> 是限速水线，取值范围是 1 到 9999。 <i>attack-threshold-pps</i> 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。
Step 9	Ruijie(config-if)#end	退回到特权模式。
Step 10	Ruijie#show nfpp dhcp-guard summary	核对配置参数
Step 11	Ruijie#copy running-config startup-config	保存配置。

**注意**

基于链路层源 MAC 地址限速优先于基于端口限速处理。

11.3.4.1.7 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
Step 1	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。

11.3.4.1.8 查看DHCP抗攻击的相关信息

11.3.4.1.8.1 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
Step 1	Ruijie#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

说明

- 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：
 - （1）“-/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。
 - （2）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。

11.3.4.1.8.2 查看受监控主机的信息

	命令	作用
Step 1	Ruijie#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。
Step 2	Ruijie#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)
```

说明

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。

11.3.5 ND抗攻击

11.3.5.1 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。

11.3.5.1.1 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
Step 1	Ruijie#configure terminal	进入全局配置模式。
Step 2	Ruijie(config)#nfpp	进入 NFPP 配置模式。
Step 3	Ruijie(config-nfpp)#nd-guard enable	打开 ND 抗攻击功能，缺省情况下就是打开的。
Step 4	Ruijie(config-nfpp)#end	退回到特权模式。
Step 5	Ruijie#configure terminal	进入全局配置模式。
Step 6	Ruijie(config)#interface interface-name	进入接口配置模式。
Step 7	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。
Step 8	Ruijie(config-if)#end	退回到特权模式。
Step 9	Ruijie#show nfpp nd-guard summary	核对配置参数
Step 10	Ruijie#copy running-config startup-config	保存配置。

11.3.5.1.2 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
Step 1	Ruijie#configure terminal	进入全局配置模式。
Step 2	Ruijie(config)#nfpp	进入 NFPP 配置模式。

Step 3	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。
Step 4	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。
Step 5	Ruijie(config-nfpp)#end	退回到特权模式。
Step 6	Ruijie#configure terminal	进入全局配置模式。
Step 7	Ruijie(config)#interface interface-name	进入接口配置模式。
Step 8	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。 <i>rate-limit-pps</i> 是限速水线，取值范围是 1 到 9999。 <i>attack-threshold-pps</i> 是攻击水线，取值范围是 1 到 9999。
Step 9	Ruijie(config-if)#end	退回到特权模式。
Step 10	Ruijie#show nfpp nd-guard summary	核对配置参数
Step 11	Ruijie#copy running-config startup-config	保存配置。

11.3.5.1.3 查看ND抗攻击的相关信息

11.3.5.1.3.1 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
Step 1	Ruijie#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

说明

- 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。

11.3.6 NFPP日志信息

11.3.6.1 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。

11.3.6.1.1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
Step 1	Ruijie#configure terminal	进入全局配置模式。
Step 2	Ruijie(config)#nfpp	进入 NFPP 配置模式。
Step 3	Ruijie(config-nfpp)# log-buffer entries <i>number</i>	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。
Step 4	Ruijie(config-nfpp)#end	退回到特权模式。
Step 5	Ruijie# show nfpp log summary	核对配置参数。

11.3.6.1.2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
Step 1	Ruijie#configure terminal	进入全局配置模式。
Step 2	Ruijie(config)#nfpp	进入 NFPP 配置模式。
Step 3	Ruijie(config-nfpp)# log-buffer logs <i>number_of_message interval length_in_seconds</i>	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 <i>number_of_message /length_in_seconds</i> ，生成系统消息的同时还会删除专用缓冲区中的对应信息 <i>number_of_message</i> ，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。 <i>length_in_seconds</i> ，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。 <i>number_of_message</i> 和 <i>length_in_seconds</i> 都为 0 表示日志立即生成系统消息。
Step 4	Ruijie(config-nfpp)#end	退回到特权模式。
Step 5	Ruijie# show nfpp log summary	核对配置参数。

11.3.6.1.3 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
Step 1	Ruijie#configure terminal	进入全局配置模式。
Step 2	Ruijie(config)#nfpp	进入 NFPP 配置模式。
Step 3	Ruijie(config-nfpp)# logging vlan <i>vlan-range</i>	指定需要记录哪些 VLAN 的日志。
	Ruijie(config-nfpp)# logging interface <i>interface-id</i>	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。
Step 4	Ruijie(config-nfpp)#end	退回到特权模式。
Step 5	Ruijie# show nfpp log summary	核对配置参数。

11.3.6.1.4 清除日志

	命令	作用
Step 1	Ruijie# clear nfpp log	清空日志缓冲区。

11.3.6.1.5 显示日志

	命令	作用
Step 1	Ruijie# show nfpp log summary	查看 NFPP 日志信息配置。
Step 2	Ruijie# 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）

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

注意

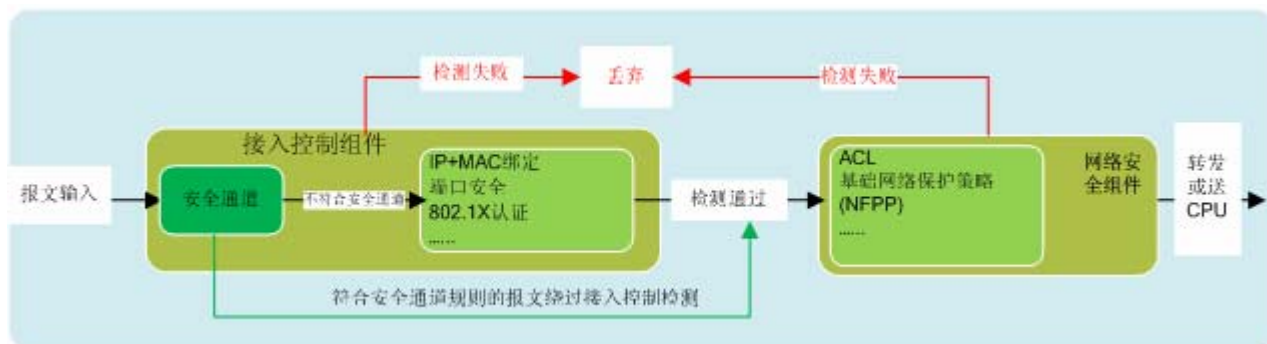
- 当日志缓冲区溢出时，后续的日志将被丢弃，同时在日志缓冲区中显示一条所有属性都为“-”的表项。管理员需要增加日志缓冲区容量或者提高生成系统消息的速率。
- 从日志缓冲区取日志生成的系统消息带有事件发生的时间戳，如下所示：
- %NFPP_ARP_GUARD-4-DOS_DETECTED: Host<IP=N/A,MAC=0000.0000.0004,port=Gi4/1,VLAN=1> was detected.(2009-07-01 13:00:00)

12 配置锐捷交换机安全功能兼容模式

12.1 理解锐捷交换机安全功能

12.1.1 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越高，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)。



锐捷交换机安全功能转发示意

12.1.2 锐捷交换机安全功能基本概念

12.1.2.1 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；
- GSN 绑定：要求符合 GSN 绑定的报文转发；
- 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 Source 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。

12.1.2.2 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；

- GSN 隔离和阻断：符合 GSN 阻断设置的报文被丢弃，符合 GSN 隔离的报文被隔离到特定的网段；
 - 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：符合 CPP 的报文被 COPY 一份到 CPU；
 - ACL：符合 ACL PERMIT 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。

12.1.2.3 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：

接入控制组件和网络安全组件的 ACL 共用时，转发面上，如果存在安全 ACL 的 PERMIT 表项，PERMIT 和默认 DENY 的 ACE 不会被安装到硬件，不生效，其他 DENY 表项的 ACE 正常生效。控制面上，通过接入控制组件检测的报文符合 CPP 的送 CPU，通不过接入控制组件的报文被丢弃；网络安全组件不对 CPP 报文的合法性做检测。

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 PERMIT 和 DENY 同时生效；但是此时硬件表项的损耗较大，假设接入控制用户为 M，安全 ACL 的 ACE 表项为 N，在 RGOS 兼容模式共存下，耗费的表项最大为 M+N 条；而在 RGOS 非兼容模式共存下，耗费的表项最大为 M X N 条。控制面上，通过接入控制组件检测的报文送 CPU，通不过接入控制组件的报文被丢弃；网络安全组件不对 CPP 报文的合法性做检测。

12.1.3 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 rgos-security compatible` 命令并保存配置重启，安全功能共存的兼容模式切换到 RGOS 非兼容模式。反之，设置 `rgos-security compatible` 命令并保存配置重启，安全共存的兼容模式切换到 RGOS 兼容模式。

12.1.4 协议规范

无。

12.2 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

12.3 配置安全功能兼容模式

12.3.1 安全功能兼容模式命令

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
Step 1	Ruijie# configure terminal	进入全局配置模式
Step 2	Ruijie(config)# rgos-security compatible	设置安全功能共存模式为 RGOS 兼容模式共存，使用 no rgos-security compatible 设置成 RGOS 非兼容模式共存
Step 3	Ruijie(config)# exit	退出全局配置模式。

注意

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。

12.3.2 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-config** 中将会看到 **no rgos-security compatible** 的配置：

命令	作用
Ruijie(config)# 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. 配置访问控制列表
2. 配置 QOS 命令

1 配置访问控制列表

1.1 理解访问控制列表

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。

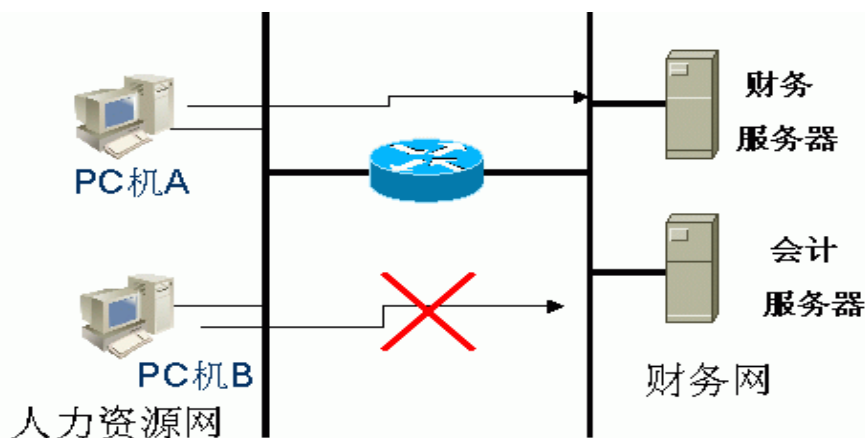
访问列表规则可以针对数据流的源地址、目标地址、上层协议, 时间区域等信息。

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。

如下图所示, 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。



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。

说明

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)：

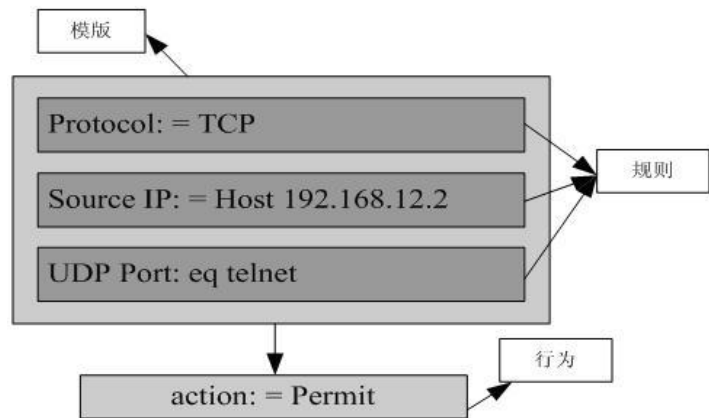
- 可以申明一个 TCP 的源端口、目的端口或者都申明
- 可以申明一个 UDP 的源端口、目的端口或者都申明

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。



对 ACE: permit tcp host 192.168.12.2 any eq telnet 的分析

说明

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)。

注意

1. 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;

2. 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。

1.2 IP访问列表配置

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。

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。

1.2.1.1 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。



注意

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。

1.2.1.2 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
Step 1	Ruijie(config)# access-list <i>id</i> { deny permit } { <i>src src-wildcard</i> <i>host src</i> any } [time-range <i>tm-rng-name</i>]	定义访问列表
Step 2	Ruijie(config)# interface <i>interface</i>	选择要应用访问列表的接口
Step 3	Ruijie(config-if)# ip access-group <i>id</i> { 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
Step 1	Ruijie(config)# ip access-list { standard extended } { <i>id</i> <i>name</i> }	进入配置访问列表模式
Step 2	Ruijie (config-xxx-nacl)# [<i>sn</i>] { permit deny } { <i>src src-wildcard</i> <i>host src</i> any } [time-range <i>tm-rng-name</i>]	为 ACL 添加表项,具体内容请参见命令参考
Step 3	Ruijie(config-xxx-nacl)# exit	退出访问控制列表模式
Step 4	Ruijie(config)# interface <i>interface</i>	选择要应用访问列表的接口
Step 4	Ruijie(config-if)# ip access-group <i>id</i> { in out }	将访问列表应用特定接口

说明

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

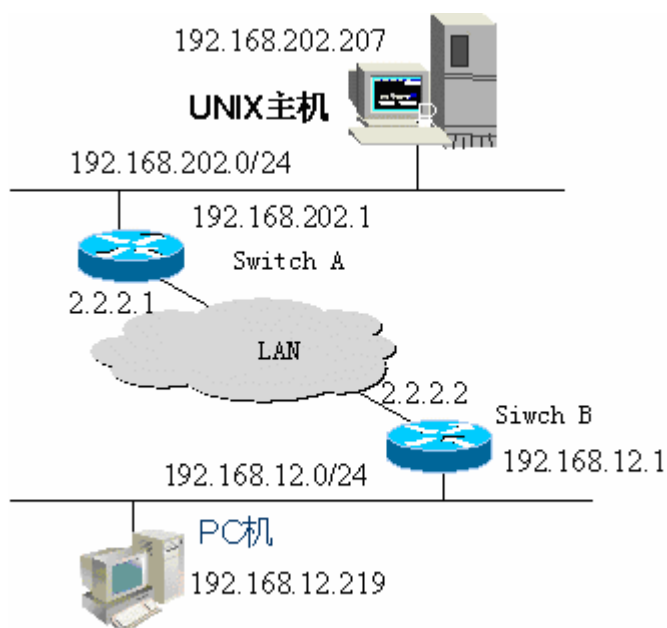
要监控访问列表，请在特权用户模式执行以下命令：

	命令	作用
Step 1	Ruijie# show access-lists [<i>id</i> <i>name</i>]	可以查看基本访问列表

1.2.4 IP访问列表示例

1.2.4.1 配置要求

有两台设备 Switch A 和 Switch B，如图所示：



基本访问列表示例

要求通过在 Switch 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 Switch B 控制台上不能访问 192.168.202.0/24 网段主机的所有服务。

说明

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。

1.2.4.2 设备配置

Switch 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
```

说明

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。

Switch A 的配置:

```
Switch 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
```

1.3 MAC扩展访问列表的配置

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
Step 1	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
Step 2	Ruijie(config)# interface interface	选择选择要应用访问列表的接口
Step 3	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
Step 1	Ruijie(config)# mac access-list extended {id name}	进入配置访问列表模式
Step 2	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
Step 3	Ruijie(config-mac-nacl)# exit	退出访问控制列表模式
Step 4	Ruijie(config)# interface interface	选择要应用访问列表的接口
Step 5	Ruijie(config-if)# mac access-group {id name} { in out }	将访问列表应用特定接口

说明

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）。

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
Step 1	Ruijie# show access-lists [id name]	可以查看基本访问列表

1.3.4 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

配置以太网口，在以太网口上应用访问列表 101，对以太网口上进出的所有报文进行检查

```
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
```

说明

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。

1.4 Expert扩展访问列表的配置

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
Step 1	Ruijie(config)# access-list <i>id</i> {deny permit} [prot {[ethernet-type] [cos cos]] [VID <i>vid</i>] {src <i>src-wildcard</i> host <i>src</i> } {host <i>src-mac-addr</i> any} {dst <i>dst-wildcard</i> host <i>dst</i> any}{host <i>dst-mac-addr</i> any} [precedence <i>precedence</i>] [tos <i>tos</i>] [dscp <i>dscp</i>] [fragment] [range <i>lower upper</i>] [time-range <i>tm-rng-name</i>]	定义访问列表,命令的具体内容请参见命令参考
Step 2	Ruijie(config)# interface <i>interface</i>	选择选择要应用访问列表的接口
Step 3	Ruijie(config-if)# expert access-group <i>id</i> {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
Step 1	Ruijie(config)# expert access-list extended { <i>id</i> <i>name</i> }	进入配置访问列表模式

Step 2	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
Step 3	Ruijie(config-exp-nacl)# exit	退出访问控制列表模式
Step 4	Ruijie(config)# interface interface	选择要应用访问列表的接口
Step 5	Ruijie(config-if)# expert access-group {id name} {in out}	将访问列表应用特定接口

说明

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)。

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
Step 1	Ruijie # show access-lists [id name]	可以查看 Expert 访问列表

1.4.4 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
petmit ip vid 20 any host 0013.2049.8272 any any
deny any any
```

1.5 配置访问列表ACL80

ACL80 也叫自定义访问列表，含义是匹配报文的前 80 个字节，对报文进行过滤。报文是由一系列的字节流组成，ACL80 可以让用户对报文的前 80 个字节中的指定 16 个字节按比特（bit）位进行匹配过滤。

 说明

报文的 SMAC/DMAC/SIP/DIP/ETYPE 不计算在任意指定的字段中，即报文匹配以上这点字段之后，还能再匹配另外指定的 16 个字节内容。

按照上述说明，对于任意一个 16 字节字段，可以按照 bit 形式与所设置的值进行比较或不比较。也就是说，它允许我们对这 16 个字节的任意一个比特设置该值为 0 或 1。在对任何一个字节进行过滤时，有两个要素：过滤规则和过滤域模板，二者的比特位是一一对应的。过滤规则指明需要过滤字段值，过滤域模板指明过滤规则中对应字段是否需要过滤（1 表示匹配对应过滤规则的比特位，0 表示不匹配），所以当需要匹配某个比特时，必须将过滤域模板中对应的比特为设置为 1。如果过滤域模板比特位设置为 0，无论过滤规则中对应的比特位是什么，都不会匹配。

例如：

```
Ruijie(config)# expert access-list advanced name
Ruijie(config-exp-dacl)# permit 00d0f8123456 ffffffff 0
Ruijie(config-exp-dacl)# deny 00d0f8654321 ffffffff 6
```

用户自定义访问控制列表根据用户的定义对二层数据帧的前 80 个字节中的任意字节进行匹配，对数据报文作出相应的处理。正确使用用户自定义访问控制列表需要用户对二层数据帧的构成有深入的了解。下图为二层数据帧的前 64 个字节的示意图（每个字母代表一个 16 进制数，每两个字母代表一个字节）。

AA AA AA AA AA AA BB BB BB BB BB BB CC CC DD DD
DD DD EE FF GG HH HH HH II II JJ KK LL LL MM MM
NN NN OO PP QQ QQ RR RR RR RR SS SS SS SS TT TT
UU UU VV VV VV VV WW WW WW WW XY ZZ aa aa bb bb

在上图中，各个字母的含义及偏移量取值如下表所示：

字母	含义	偏移量	字母	含义	偏移量
A	目的 MAC	0	O	TTL 字段	34
B	源 MAC	6	P	协议号	35
C	VLAN tag 字段	12	Q	IP 校验和	36
D	数据帧长度字段	16	R	源 ip 地址	38
E	DSAP(目的服务访问点)字段	18	S	目的 ip 地址	42
F	SSAP(源服务访问点)字段	19	T	TCP 源端口	46
G	Ctrl 字段	20	U	TCP 目的端口	48
H	Org Code 字段	21	V	序列号	50
I	封装的数据类型	24	W	确认字段	54
J	IP 版本号	26	XY	IP 头长度和保留比特位	58
K	TOS 字段	27	Z	保留比特位和 flags 比特位	59
L	IP 包的长度	28	a	Windows size 字段	60
M	ID 号	30	b	其他	62
N	Flags 字段	32			

上表中各个字段的偏移量是它们在 SNAP+tag 的 802.3 数据帧中的偏移量。在用户自定义访问控制列表中，用户可以使用规则掩码和偏移量两个参数共同从数据帧中提取前 80 个字节中的任意字节，然后和用户定义的规则比较，从而过滤出匹配的数据帧，作相应的处理。用户定义的规

则可以是数据的某些固定属性，比如用户要将所有的 TCP 报文过滤出来，可以将规则定义为“06”，规则掩码定义为“FF”，偏移量定义为 35，此时规则掩码和偏移量共同作用，把接收到的数据帧中的 TCP 协议号字段的内容提取出来，和规则比较，匹配出所有的 TCP 报文。

 **注意**

ACL80 可以支持匹配以太网报文，803.3snap 报文，802.3llc 报文，如果设置匹配 DSAP 到 cntl 字段的值为 AAAA03，则表示希望匹配 803.3snap 报文，如果设置匹配 DSAP 到 cntl 字段的值为 E0E003，则表示希望匹配 803.3llc 报文。以太网报文不能设置匹配该字段。

Acl80 可以任意匹配的资源只有 16 个字节，如果这 16 个字节的资源已经被使用，那么就无法再匹配这 16 个字节之外的字段。例如

```
Ruijie(config)# expert access-list advanced name
Ruijie(config-exp-dacl)#permit 11223344556677889900aabbccd
deeff ffffffffffffffffffffffffffffffffff 50
```

这里再添加一条 ace

```
Ruijie(config-exp-dacl)#permit 11223344556677889900aabbccd
deeff ffffffffffffffffffffffffffffffffff 54
```

将会配置失败，原因是 16 个字节的资源已经被第一条 ace 占用，而第二条 ace 想要匹配 16 个字节以外的区域就会失败。如果向想要匹配，则必须删除第一条 ace。

1.6 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。

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。

 **说明**

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
Step 1	Ruijie(config)# ip access-list extended { id name }	进入配置访问列表模式
Step 2	Ruijie(config-ext-nacl)# [sn] [permit deny] tcp source source-wildcard [operator port [port]] destination destination-wildcard [operator port [port]] [match-all flag-name][precedence precedence]	为 ACL 添加表项,命令的具体内容请参见命令参考
Step 3	Ruijie(config-exp-nacl)# exite	退出访问控制列表模式，选择选择要应用访问列表的接口
or		
	Ruijie(config)# interface interface	退出访问控制列表模式，选择选择要应用访问列表的接口

Step 4	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
■ 添加 deny 表项
■ 重复添加删除表项，
■ 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 deny tcp any any match-all fin

```

1.7 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 4 中的优先级添加 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。

1.8 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
Step 1	Ruijie# configure terminal	进入全局配置模式。
Step 2	Ruijie(config)# time-range <i>time-range-name</i>	通过一个有意义的显示字符串作为名字来标识一个
Step 3	Ruijie(config-time-range)# absolute [start 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
Step 4	Ruijie(config-time-range)# periodic <i>day-of-the-week time to [day-of-the-week] time</i>	设置周期时间(可选)，具体可参见 time range 的配置指南
Step 5	Ruijie# show time-range	验证您的配置
Step 6	Ruijie# copy running-config startup-config	保存配置
Step 7	Ruijie(config)# ip access-list extended <i>101</i>	进入 ACL 配置模式
Step 8	Ruijie(config-ext-nacl)# permit ip any any time-range <i>time-range-name</i>	配置时间区的 ACE

说明

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

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
```

1.9 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。

说明

- 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不能用来设置基于接口的安全通道。
- 全局安全通道的例外口最多可以设置 8 个。
- 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。

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
Step 1	Ruijie# configure terminal	进入全局配置模式。
Step 2	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
Step 1	Ruijie# configure terminal	进入全局配置模式。
Step 2	Ruijie(config)#interface idx	进入接口模式
Step 3	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

Step 1	Ruijie# configure terminal	进入全局配置模式。
Step 2	Ruijie(config)# interface idx	进入接口模式
Step 3	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 进入交换机。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。

1.10 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 的注释功能。

说明

- 一个 ACL 中最多配置 1 个 ACL 注释。
- 每个注释长度为 100 字节。

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
Step 1	Ruijie# configure terminal	进入全局配置模式。
Step 2	Ruijie(config)# ip access-list standard id	进入 ACL 配置模式(其他类型 ACL 类似)
Step 3	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
Step 1	Ruijie# configure terminal	进入全局配置模式。

Step 2	Ruijie(config)# access-list id list-remark comment

直接给 ACL 配置注释(其他类型 ACL 类似)

1.11 配置举例

1.11.1 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



如上图所示，通过三层交换机连接两个网络，网络 A 与交换机的 G3/1 口相连，网络 B 与交换机的 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 发起经过交换机 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

■ 定义访问控制列表

进入交换机的配置模式

```
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
```

■ 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
```

■ 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
```

2 配置 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 Service 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 QoS solution。

2.1.2 QoS处理流程

2.1.2.1 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。

说明

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。

说明

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。

2.1.2.2 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，报文也不会再在送往 **Marking** 动作之前被丢弃。

2.1.2.3 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。

2.1.2.4 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。

2.1.2.5 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。

2.2 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	1:15
DRR Weight Range	1:15
信任模式	No Trust
交换机 Buffer 管理模式	FC

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
Step 1	Ruijie# configure terminal	进入配置模式
Step 2	Ruijie(config)# interface interface	进入接口配置模式
Step 3	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 COS: trust dscp
```



```
Default COS: 0
Ruijie#
```

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
Step 1	Ruijie# configure terminal	进入配置模式
Step 2	Ruijie(config)# interface <i>interface</i>	进入接口配置模式
Step 3	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 COS: trust dscp
Default COS: 6
Ruijie#
```

2.2.4 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 { <i>id</i> <i>name</i> } ... Ruijie(config)# ip access-list standard { <i>id</i> <i>name</i> } ... Ruijie(config)# mac access-list extended { <i>id</i> <i>name</i> } ... Ruijie(config)# expert access-list extended { <i>id</i> <i>name</i> } ... Ruijie(config)# access-list <i>id</i> [...]	创建 ACL 请参见 ACL 章节
Ruijie(config)# [no] class-map <i>class-map-name</i>	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

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
```

2.2.5 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
Step 1	Ruijie# configure terminal	进入配置模式
Step 2	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
Step 3	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	为该数据流中的 IP 报文设置新的 ip dscp 值； 对于非 IP 报文，该设置不起作用； new-dscp 是要设置的新 DSCP 值，取值范围依产品不同而不同
	Ruijie(config-pmap-c)# police rate-bps burst-byte [exceed-action {drop dscp dscp-value}]	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 突发流量限制值(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。
	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



说明

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；

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
```

2.2.6 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
Step 1	Ruijie# configure terminal	进入配置模式
Step 2	Ruijie(config)# interface interface	进入接口配置模式
Step 3	Ruijie(config-if)# [no] service-policy input 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 为输入限速

2.2.7 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，RR 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
Step 1	Ruijie# configure terminal	进入配置模式
Step 2	Ruijie(config)# mls qos scheduler {sp rr wrr drr }	端口优先级队列调度方式， sp 为绝对优先级调度， rr 为 轮转调度， 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#
```

2.2.8 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
Step 1	Ruijie# configure terminal	进入配置模式
Step 2	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

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)#
```

2.2.9 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
Step 1	Ruijie# configure terminal	进入配置模式
Step 2	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
```

2.2.10 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
Step 1	Ruijie# configure terminal	进入配置模式
Step 2	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
```

2.2.11 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
Step 1	Ruijie# configure terminal	进入配置模式

Step 2

Ruijie(config)# mls qos map dscp-cos dscp-list to cos	设置 DSCP to COS Map, <i>dscp-list</i> : 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, <i>cos</i> : 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

2.2.12 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
Step 1	Ruijie# configure terminal	进入配置模式
Step 2	Ruijie(config)# interface interface	进入接口配置模式
Step 3	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 突发流量限制值(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 output 64 1024
Ruijie(config-if)# end
Ruijie#
```

2.2.13 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
Step 1	Ruijie# configure terminal	进入配置模式
Step 2	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-prec-dscp 56 48 46 40 34 32 26 24
Ruijie(config)# end
Ruijie# show mls qos maps ip-prec-dscp
ip-prec-dscp
-----
0      56
1      48
2      46
3      40
4      34
5      32
6      26
7      24
```

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, <i>policy-name</i> 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 [<i>interface</i> <i>policers</i>]	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 COS: 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 [<i>interface interface</i>]	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 <i>interface</i>	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
```



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. 配置 RLDP
2. 配置 VRRP
3. 配置 TPP
4. 配置 SEM

1 配置 RLDP

1.1 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。

工作原理

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：

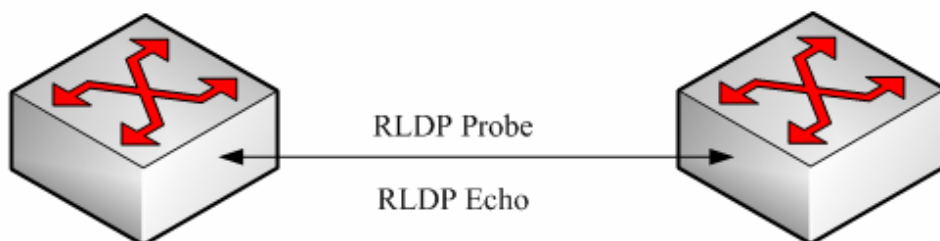


图 1

RLDP 定义了两类协议报文：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。

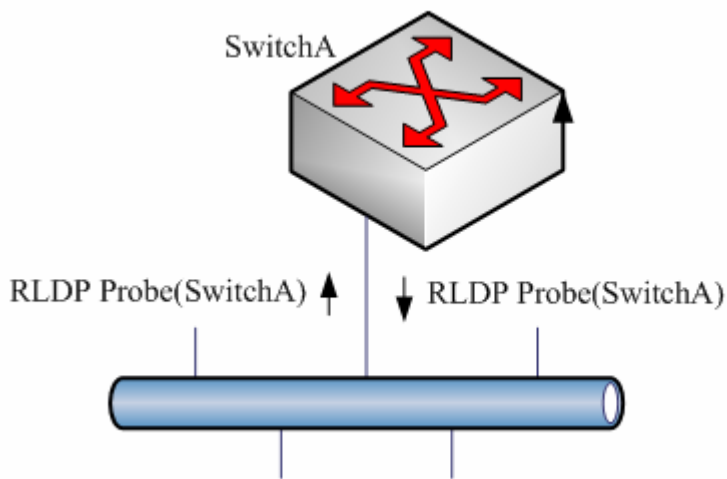
说明

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。

典型应用

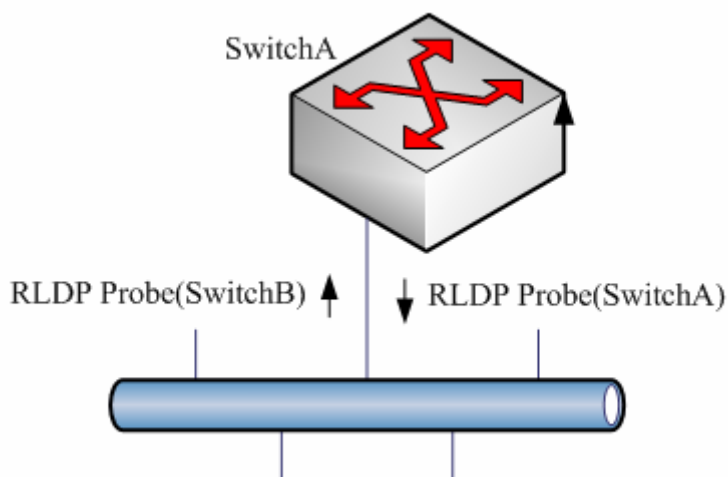
■ 环路检测

环路故障是指端口连接的链路上出现了环路。如下图所示，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。



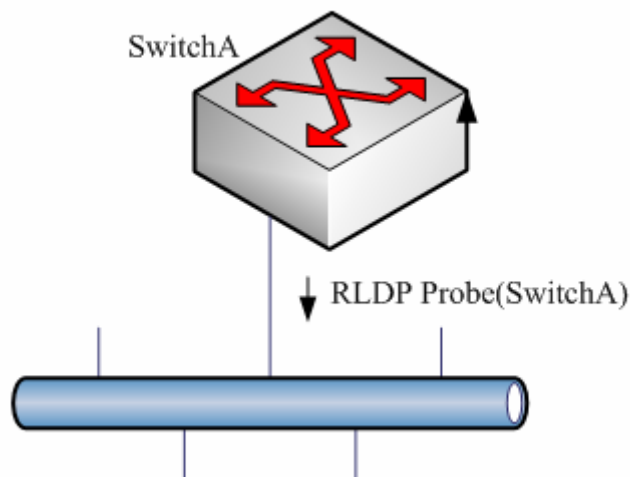
■ 单向链路检测

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。



■ 双向链路检测

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。



说明

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。

1.2 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	2S
最大探测次数	3 次

注意

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 AP 口及 SVI 上配置。

1.2.1 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
Step 1	Ruijie(config)# rldp enable	打开全局的 RLDP 功能开关。
Step 2	Ruijie(config)# end	退回到特权模式。

如果要关闭全局的 RLDP，请使用该命令的 **no** 选项。

1.2.2 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
Step 1	Ruijie(config)# interface <i>interface-id</i>	进入接口模式
Step 2	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。
Step 3	Ruijie(config-if)# end	退回特权模式

要关闭端口的 RLDP，请使用该命令的 **no** 选项逐一关闭已经配置的检测类型。

以下例子是在 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
```

配置端口检测有几个注意点：

- 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、故障处理方式为 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，所以建议您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 故障处理类型中的 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类型为 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，我们建议将错误处理类型配置为“shutdown-port”。

1.2.3 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
Step 1	Ruijie(config)# rldp detect-interval interval	配置探测间隔，interval 取值范围是 2-15s,默认是 3s。
Step 2	Ruijie(config)# end	退回到特权模式。

如果恢复默认值，请使用该命令的 no 选项。

1.2.4 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
Step 1	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。
Step 2	Ruijie(config)# end	退回到特权模式。

如果恢复默认值，请使用该命令的 no 选项。

说明

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。

1.2.5 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
Step 1	Ruijie# rldp reset	使所有 RLDP 检测失败的端口重新开始检测。

说明

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。

1.2.6 查看RLDP检测信息

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。
Ruijie# show rldp interface interface-id	查看指定端口的 RLDP 检测信息

```
Ruijie# show rldp
rldp state          : enable
rldp hello interval : 2
rldp max hello      : 3
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。

```
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。

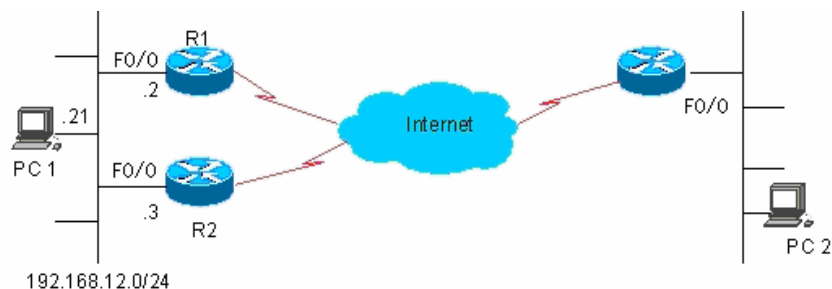
2 配置 VRRP

2.1 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 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 2338 规定了路由设备的切换规则:

- 1) 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, 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。
- 2) 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。



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。通讯过程如上图所示。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

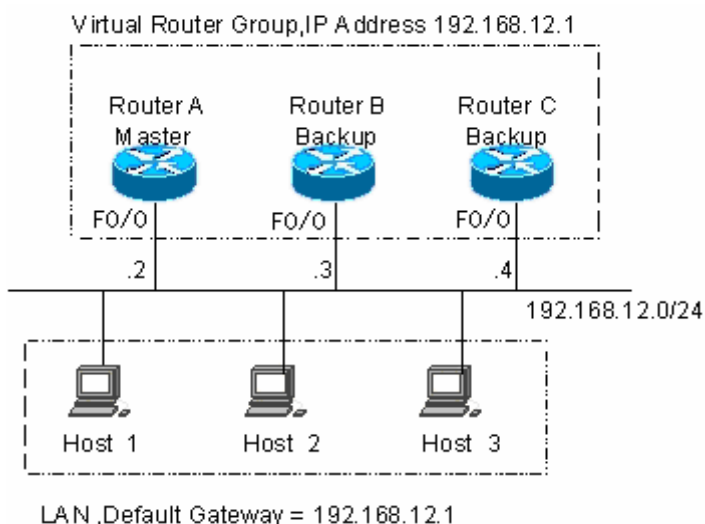
连接，路由设备 R1 与 R2 的 Fa0/0 接口上设置了 VRRP，局域网内的主机都以该 VRRP 组的虚拟路由设备 IP 地址作为默认网关。对于局域网内的主机而言，它们只能感受到由 VRRP 组的虚拟路由设备，而实际承担路由转发功能的 VRRP 组的主路由设备对它们而言则是透明的。譬如，局域网内的主机 PC 1 如果要与其它网络内的主机 PC 2 通讯，PC 1 会以虚拟路由设备为默认网关来发送通向 PC 2 的网络数据包，VRRP 组中的主路由设备在接收到该数据包后会将该数据包转发给 PC 2。在这个通讯过程中，PC 1 只能感受到虚拟路由设备而不知道扮演虚拟路由设备角色的主路由设备究竟是 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。

2.2 VRRP的应用

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。

2.2.1 路由冗余

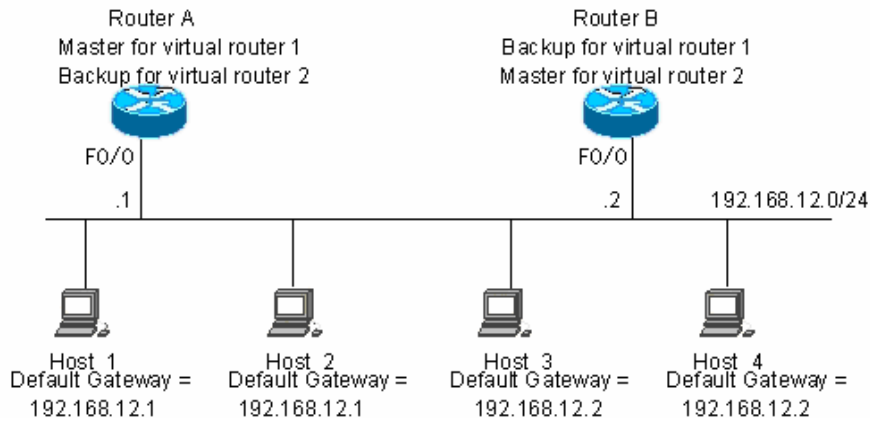
VRRP 的基本应用如下图所示。



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 2-2 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。

2.2.2 负载均衡

VRRP 的高级应用如下图所示。



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。

2.3 VRRP的配置

VRRP 协议是适用于多播或者广播的局域网如以太网等。VRRP 的配置就集中在以太网接口上。“启动 VRRP 备份功能”是必选配置，其它根据需要配置。

2.3.1 启动VRRP备份功能

通过设置备份组号和虚拟 IP 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 VRRP
Ruijie(config-if)# no vrrp group ip ipaddress [secondary]	关闭 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。

 注意

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。

在 NMX-2GEH 线卡上,每个接口最多支持 14 个 VRRP 备份组。如果配置的 VRRP 组数超过 14,则系统会提示错误。

2.3.2 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 VRRP 的验证字符串
Ruijie(config-if)# no vrrp group authentication	设置 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。

2.3.3 设置VRRP备份组的通告发送间隔

命令	作用
Ruijie(config-if)# vrrp group timers advertise interval	设置主路由设备 VRRP 通告间隔
Ruijie(config-if)# no vrrp group timers advertise	恢复主路由设备 VRRP 通告间隔的系统默认设置

如果当前路由设备 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。

 说明

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。

2.3.4 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 VRRP 备份组处于抢占模式
Ruijie(config-if)# no vrrp group preempt [delay]	设置 VRRP 备份组处于非抢占模式

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。

2.3.5 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 VRRP 备份组的优先级
Ruijie(config-if)# no vrrp group priority	恢复 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)。

2.3.6 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 VRRP 备份组监视的接口
Ruijie(config-if)# no vrrp group track interface-type number	取消 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)。

2.3.7 设置VRRP备份组监视的IP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。

命令	作用
Ruijie(config-if)# vrrp group track ip-address [[[interval interval-value] timeout timeout-value] priority]	设置 VRRP 备份组监视的 IP 地址
Ruijie(config-if)# no vrrp group track ip-address	取消 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 **priority** 取值范围为 1~255, 如果该参数缺省, 系统会取默认值即 10。

2.3.8 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, 它将从主路由设备的 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	设置定时设备学习功能
Ruijie(config-if)# no vrrp group timers learn	取消定时设备学习功能

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。

2.3.9 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 VRRP 组描述字符串
Ruijie(config-if)# no vrrp group description	取消 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。

说明

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。

2.3.10 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。

2.3.11 查看VRRP配置及状态信息

使用以下的 **show vrrp** 命令来考察本地路由设备的 VRRP 状态。

命令	作用
show vrrp [brief group]	查看当前的 VRRP 状态

show vrrp interface type number [brief]

显示指定网络接口上 VRRP 状态

下面给出使用这些命令的示例：

```
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 , pritority is 120
Master Advertisement interval is 3 sec
Master Down interval is 9 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 9 sec
```

上面的显示信息包括以太网口名称、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。

```
Ruijie# show vrrp brief
Interface      Grp Pri Time Own Pre State  Master addr  Group addr
FastEthernet0/0 1 100 - - P Backup 192.168.201.213 192.168.201.1
FastEthernet0/0 2 120 - - P Master 192.168.201.217 192.168.201.2
```

上面的显示信息包括以太网口名称、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。

```
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
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 9 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 9 sec
Ruijie#

```

上面的显示信息包括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。

2.3.12 查看VRRP调试信息

使用 Debug Vrrp 查看 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 vrrp errors	打开 VRRP 出错提示调试开关
Ruijie# no debug vrrp errors	关闭 VRRP 出错提示调试开关
Ruijie# debug vrrp events	打开 VRRP 事件调试开关
Ruijie# no debug vrrp events	关闭 VRRP 事件调试开关
Ruijie# debug vrrp packets	打开 VRRP 报文调试开关
Ruijie# no debug vrrp packets	关闭 VRRP 报文调试开关
Ruijie# debug vrrp state	打开 VRRP 状态调试开关
Ruijie# no debug vrrp state	关闭 VRRP 状态调试开关
Ruijie# debug vrrp	打开 VRRP 全部调试开关
Ruijie# no debug vrrp	关闭 VRRP 全部调试开关

下面给出使用这些命令的示例:

```
Ruijie# debug vrrp
Ruijie#
VRRP: Grp 1 Advertisement priority 120, ipaddr 192.168.201.213
VRRP: Grp 1 Event - Advert higher or equal priority
%VRRP-6-STATECHANGE: FastEthernet 0/0 Grp 1 state Master -> Backup
VRRP: Grp 1 Advertisement from 192.168.201.213 has invalid virtual address
192.168.1.1
%VRRP-6-STATECHANGE: FastEthernet 0/0 Grp 1 state Backup -> Master
Ruijie#
```

执行 **debug vrrp** 命令相当于同时执行 **debug vrrp errors**、**debug vrrp events**、**debug vrrp packets**、**debug vrrp state** 命令。

```
Ruijie# debug vrrp errors
Ruijie#
VRRP: Grp 1 Advertisement from 192.168.201.213 has invalid virtual address
192.168.1.1
VRRP: Grp 1 Advertisement from 192.168.201.213 has invalid virtual address
192.168.1.1
VRRP: Grp 1 Advertisement from 192.168.201.213 has invalid virtual address
192.168.1.1
```

上面的显示信息表明接收到来自 192.168.201.213 针对 VRRP 组 1 的 VRRP 通告, 在该通告中的虚拟 IP 地址 192.168.1.1 不存在于本地 VRRP 组 1。

```
Ruijie# debug vrrp events
Ruijie#
VRRP: Grp 1 Event - Advert higher or equal priority
VRRP: Grp 1 Event - Advert higher or equal priority
VRRP: Grp 1 Event - Advert higher or equal priority
Ruijie#
```

上面的显示信息表明本地 VRRP 组接收到的 VRRP 通告(Advertisement)中的优先级不低于本地优先级。

```
Ruijie# debug vrrp packets
Ruijie#
VRRP: Grp 2 sending Advertisement checksum DD4D
VRRP: Grp 2 sending Advertisement checksum DD4D
VRRP: Grp 2 sending Advertisement checksum DD4D
```

上面的显示信息表明本地 VRRP 组 2 正在发送 VRRP 通告, 其 VRRP 校验和为 0XDD4D。

```
Ruijie# debug vrrp packets
Ruijie#
```

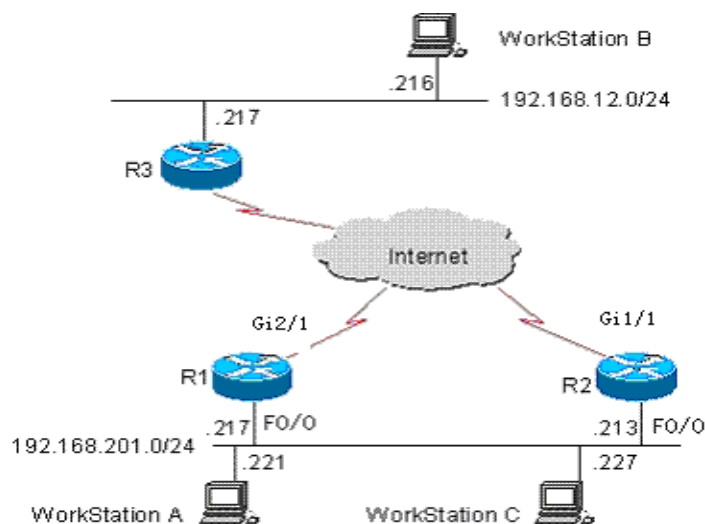
```
VRRP: Grp 1 Advertisement priority 120, ipaddr 192.168.201.213
VRRP: Grp 1 Advertisement priority 120, ipaddr 192.168.201.213
VRRP: Grp 1 Advertisement priority 120, ipaddr 192.168.201.213
```

上面的显示信息表明本地接收到来自 192.168.201.213 针对 VRRP 组 1 的 VRRP 通告，其优先级为 120。

```
Ruijie# debug vrrp state
VRRP State debugging is on
Ruijie#
%VRRP-6-STATECHANGE: FastEthernet 0/0 Grp 2 state Master -> Backup
%VRRP-6-STATECHANGE: FastEthernet 0/0 Grp 2 state Backup -> Master
Ruijie# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface fastethernet 0/0
Ruijie(config-if)# no shutdown
Ruijie(config-if)# end
Ruijie#
%VRRP-6-STATECHANGE: FastEthernet 0/0 Grp 2 state Master -> Init
Ruijie#
```

上面的显示信息表明 Fastethernet 0/0 上的 VRRP 组状态在 Master, Backup 以及 Init 之间转换。

2.4 配置举例



在路由设备 R1 与 R2 上配置了 VRRP 备份组来为内部网段 192.168.201.0 /24 提供 VRRP 服务，而在路由设备 R3 上没有配置 VRRP 而只是配置了普通路由功能。

路由设备 R3 上的配置：

```
!
!
hostname "R3"
```

```

!
!
!
interface FastEthernet 0/0
no switchport
ip address 192.168.12.217 255.255.255.0
!
interface GigabitEthernet 1/1
no switchport
ip address 60.154.101.5 255.255.255.0
!
interface GigabitEthernet 2/1
no switchport
ip address 202.101.90.61 255.255.255.0
!
router ospf
network 202.101.90.0 0.0.0.255 area 10
network 192.168.12.0 0.0.0.255 area 10
network 60.154.101.0 0.0.0.255 area 10
!
!
!
End

```

说明

以下配置示例中将只给出路由设备 R1 与 R2 上的配置。路由设备 R3 的配置不变。

2.4.1 VRRP单备份组

在这个配置示例中，用户工作站群(192.168.201.0/24)使用路由设备 R1 与 R2 组成的备份组，并将其网关指向该备份组设置的虚拟路由设备的 IP 地址 192.168.201.1，经由虚拟路由设备 192.168.201.1 访问远程用户工作站群(其工作网络为 192.168.12.0 /24)。在这里 R1 被设置成 VRRP 的 Master 路由设备。正常情况下，路由设备 R1 作为活动路由设备提供网关(192.168.201.)的功能，当路由设备 R1 由于关机或者出现故障而不可到达时，路由设备 R2 将替代它来提供网关(192.168.201.1)的功能。下面分别给出路由设备 R1 与 R2 的相关配置。

路由设备 R1 的配置：

```

!
!
hostname "R1"
!
!
interface FastEthernet 0/0

```

```
no switchport
ip address 192.168.201.217 255.255.255.0
vrrp 1 priority 120
vrrp 1 timers advertise 3
vrrp 1 ip 192.168.201.1
!
interface GigabitEthernet 2/1
no switchport
ip address 202.101.90.63 255.255.255.0
!
router ospf
network 202.101.90.0 0.0.0.255 area 10
network 192.168.201.0 0.0.0.255 area 10
!
```

路由设备 R2 的配置:

```
!
hostname "R2"
!
interface FastEthernet 0/0
no switchport
ip address 192.168.201.213 255.255.255.0
vrrp 1 ip 192.168.201.1
vrrp 1 timers advertise 3
!
interface GigabitEthernet 1/1
no switchport
ip address 60.154.101.3 255.255.255.0
!
!
router ospf
network 60.154.101.0 0.0.0.255 area 10
network 192.168.201.0 0.0.0.255 area 10
!
!
end
```

可见, 路由设备 R1 与 R2 同处于 VRRP 备份组 1 中, 指向相同的虚拟路由设备的 IP 地址 (192.168.201.1) 并且均处于 VRRP 的抢占模式下。由于路由设备 R1 的 VRRP 备份组优先级为 120, 而路由设备 R2 的 VRRP 备份组优先级取默认值 100, 所以路由设备 R1 在正常情况下充当 VRRP 的 Master 路由设备。

2.4.2 使用VRRP监视接口

在这个配置示例中，用户工作站群(192.168.201.0/24)使用路由设备 R1 与 R2 组成的备份组，并将其网关指向该备份组设置的虚拟路由设备的 IP 地址 192.168.201.1，经由虚拟路由设备 192.168.201.1 访问远程用户工作站群(其工作网络为 192.168.12.0/24)。在这里 R1 被设置成 VRRP 的 Master 路由设备。与单备份组配置示例不同的是，在这个配置示例中，路由设备 R1 中设置了 VRRP 监视接口 GigabitEthernet 2/1。正常情况下，路由设备 R1 作为活动路由设备提供虚拟网关(192.168.201.1)的功能，当路由设备 R1 由于关机或者出现故障而不可到达时，路由设备 R2 将替代它来提供虚拟网关(也就是虚拟路由设备的地址 192.168.201.1)的功能。特别的是在路由设备 R1 的与广域网的接口 GigabitEthernet 2/1 不可用的时候，路由设备 R1 将会按照设置降低自己的 VRRP 备份组的优先级，从而使得路由设备 R2 有机会成为主动路由设备并提供虚拟网关(192.168.201.1)的功能；如果此后路由设备 R1 与广域网的接口 GigabitEthernet 2/1 恢复正常，那么路由设备 R1 将恢复自己的 VRRP 备份组优先级再次成为主动路由设备并提供虚拟网关的功能。下面分别给出路由设备 R1 与 R2 的相关配置。

路由设备 R1 的配置：

```
!  
!  
hostname "R1"  
!  
!  
interface FastEthernet 0/0  
no switchport  
ip address 192.168.201.217 255.255.255.0  
vrrp 1 priority 120  
vrrp 1 timers advertise 3  
vrrp 1 ip 192.168.201.1  
vrrp 1 track GigabitEthernet 2/1 30  
!  
  
interface GigabitEthernet 2/1  
no switchport  
ip address 202.101.90.63 255.255.255.0  
!  
router ospf  
network 202.101.90.0 0.0.0.255 area 10  
network 192.168.201.0 0.0.0.255 area 10  
!  
!  
end
```

路由设备 R2 的配置：

```
!  
!  
hostname "R2"
```



```

!
interface FastEthernet 0/0
no switchport
ip address 192.168.201.213 255.255.255.0
vrrp 1 ip 192.168.201.1
vrrp 1 timers advertise 3
!
interface GigabitEthernet 1/1
no switchport
ip address 60.154.101.3 255.255.255.0
!
router ospf
network 60.154.101.0 0.0.0.255 area 10
network 192.168.201.0 0.0.0.255 area 10
!
!
end

```

可见，路由设备 R1 与 R2 同处于 VRRP 备份组 1 中，使用相同的 VRRP 备份组验证模式(无验证模式)、指向相同的虚拟 IP 地址(192.168.201.1)并且均处于 VRRP 的抢占模式下。路由设备 R2 与路由设备 R2 的 VRRP 的通告(Advertisement)间隔均为 3 秒。正常情况下，由于路由设备 R1 的 VRRP 备份组优先级为 120，而路由设备 R2 的 VRRP 备份组优先级取默认值 100，所以路由设备 R1 在正常情况下充当 Master 路由设备。如果路由设备 R1 在作为 Master 路由设备状态下发现与广域网的接口 GigabitEthernet 2/1 不可用，路由设备 R1 将降低自己的 VRRP 备份组优先级 30 而成为 90，这样路由设备 R2 就会成为 Master 路由设备。如果在此后，路由设备 R1 发现自己的与广域网的接口 GigabitEthernet 2/1 恢复可用，就增加自己的 VRRP 备份组优先级 30 而恢复到 120，这样路由设备 R1 将再次成为主路由设备。

2.4.3 VRRP多备份组

可以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。

在这个配置示例中，用户工作站群(192.168.201.0/24)使用路由设备 R1 与 R2 组成的备份组，其中部分用户工作站(如 A)将其网关指向备份组 1 的虚拟 IP 地址 192.168.201.1，部分用户工作站(如 C)则将其网关指向备份组 2 的虚拟 IP 地址 192.168.201.2。路由设备 R1 在备份组 2 中作为主路由设备，在备份组 1 中作为备份路由设备；而路由设备 R2 在备份组 2 中作为备份路由设备，在备份组 1 中作为主路由设备。下面给出路由设备 R1 与 R2 相关的配置。

路由设备 R1 的配置：

```

!
!
hostname "R1"
!
interface FastEthernet 0/0
no switchport

```

```
ip address 192.168.201.217 255.255.255.0
vrrp 1 timers advertise 3
vrrp 1 ip 192.168.201.1
vrrp 2 priority 120
vrrp 2 timers advertise 3
vrrp 2 ip 192.168.201.2
vrrp 2 track GigabitEthernet 2/1 30
!
interface GigabitEthernet 2/1
no switchport
ip address 202.101.90.63 255.255.255.0
!
router ospf
network 202.101.90.0 0.0.0.255 area 10
network 192.168.201.0 0.0.0.255 area 10
!
!
end
```

路由设备 R2 的配置:

```
!
!
hostname "R2"
!
!
interface Loopback 0
ip address 20.20.20.5 255.255.255.0
!
interface FastEthernet 0/0
no switchport
ip address 192.168.201.213 255.255.255.0
vrrp 1 ip 192.168.201.1
vrrp 1 timers advertise 3
vrrp 1 priority 120
vrrp 2 ip 192.168.201.2
vrrp 2 timers advertise 3
!
interface GigabitEthernet 1/1
no switchport
ip address 60.154.101.3 255.255.255.0
!
router ospf
network 60.154.101.0 0.0.0.255 area 10
network 192.168.201.0 0.0.0.255 area 10
!
!
```

```
!  
end
```

可见路由设备 R2 与 R2 相互备份，而且二者分别在 VRRP 备份组 1 与 2 中成为主路由设备提供不同的虚拟网关功能。

2.5 常见故障分析

故障现象：虚拟 IP 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 IP 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 表中是否有虚拟 IP 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 IP 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；
- 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 IP 地址不一致。

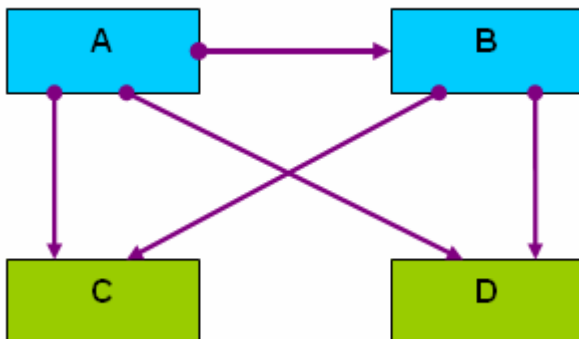
3 配置 TPP

3.1 概述

TPP(Topology Protection Protocol, 拓扑保护协议)用来保持拓扑稳定。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。

TPP 应用

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。



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 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。

3.2 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。

说明

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 `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。我们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。在 10.4（2b2）及之后的版本，`cpu topology-limit` 命令的缺省阈值为 60。

3.2.1 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。

配置命令如下：

	命令	作用
Step 1	Ruijie> enable	进入特权命令模式
Step 2	Ruijie# config terminal	进入全局配置模式
Step 3	Ruijie(config)# topology guard	使能全局拓扑防护
Step 4	Ruijie(config)# end	退回特权命令模式
Step 5	Ruijie# copy running-config startup-config	保存配置

使用 `no topology guard` 禁止设备的全局拓扑防护功能

3.2.2 配置端口拓扑防护

配置命令如下：

	命令	作用
Step 1	Ruijie> enable	进入特权命令模式
Step 2	Ruijie# config terminal	进入全局配置模式
Step 3	Ruijie(config)# interface gi 0/1	进入接口配置模式
Step 4	Ruijie(config-if)# tp-guard port enable	使能端口拓扑防护功能

Step 5	Ruijie(config-if)# end	退回特权命令模式

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。

 说明

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。

3.2.3 查看TTP配置、状态信息

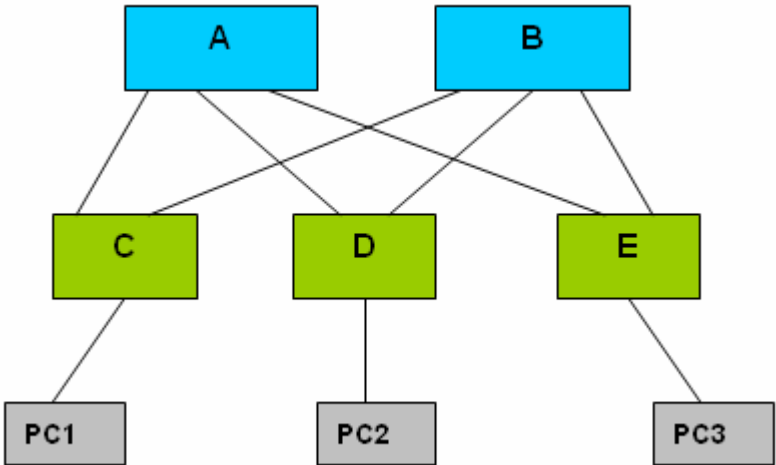
在特权模式下使用如下命令查看查看设备的 TTP 配置及状态：

命令	作用
show tpp	查看设备的 TPP 配置及状态。

```
Ruijie #show tpp
tpp state      : enable
tpp local bridge : 00d0.f822.35ad
```

3.3 典型应用

如下图为双核心组网拓扑图：



图中 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。

4 配置SEM

4.1 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。

4.1.1 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。

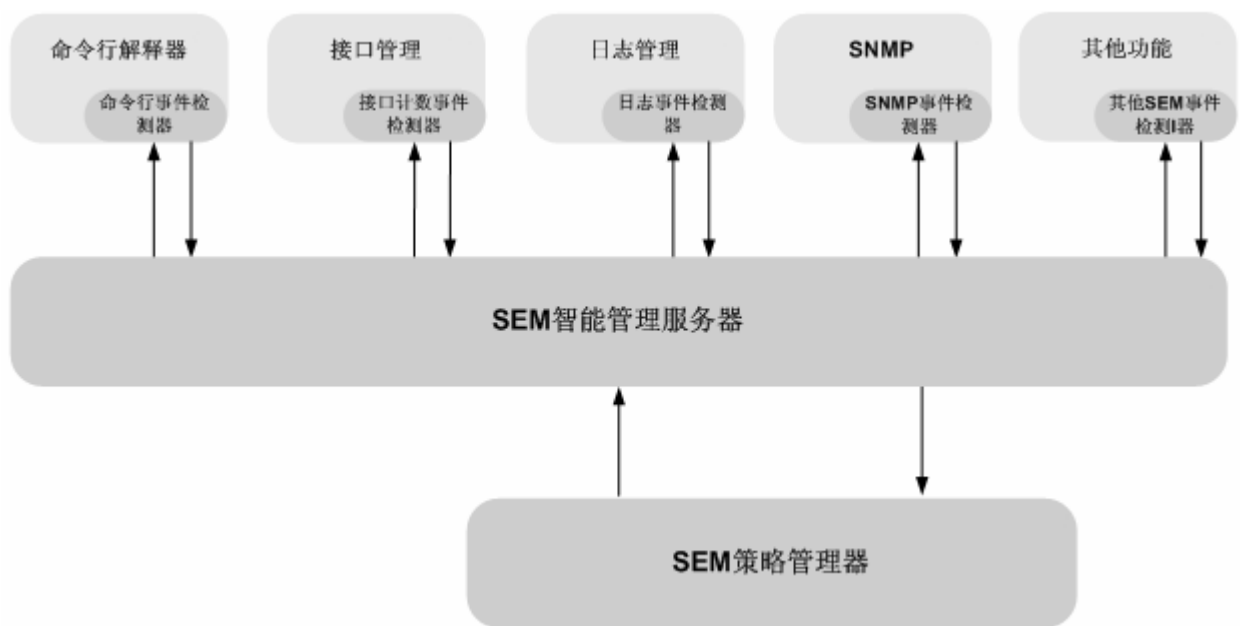
SEM 特定应用事件

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。

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。

4.1.2 工作原理



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。

4.1.3 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。

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。

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。
- 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。

4.1.4 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。
- 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。

4.1.5 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。

4.1.6 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。

4.2 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执行的执行需要，比如：配置 Syslog 行动项之前需要通过 **logging** 命令打开 Syslog 功能。

说明

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。

4.2.1 创建策略

命令	作用
Ruijie(config)# smart manager applet <i>applet-name</i> [class <i>class-options</i>]	创建策略并进入 SEM 配置模式， <i>applet-name</i> 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)#
```

说明

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。

4.2.2 配置事件

命令	作用
Ruijie(config)# smart manager applet <i>applet-name</i> [class <i>class-options</i>]	进入 SEM 配置模式, <i>applet-name</i> 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 <i>event-name</i> [correlate { andnot and or }] syslog pattern <i>regular-expression</i> [priority <i>priority-level</i>] [occurs <i>num-occurrences</i>] [period <i>period-value</i>] [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。

说明

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。

4.2.3 配置行动

命令	作用
Ruijie(config)# smart manager applet <i>applet-name</i> [class <i>class-options</i>]	进入 SEM 配置模式, <i>applet-name</i> 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 <i>label</i> syslog [priority <i>priority-level</i>] msg <i>msg-text</i> facility <i>string</i>	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。其他命令见 《SEM 命令参考》

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"
```

 说明

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。

4.2.4 配置描述

命令	作用
Ruijie(config)# smart manager applet <i>applet-name</i> [class <i>class-options</i>]	进入 SEM 配置模式， <i>applet-name</i> 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 <i>string</i>	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"
```

 说明

对描述信息的修改将立即生效，无须提交。

4.2.5 配置触发参数

命令	作用

Ruijie(config)# smart manager applet <i>applet-name</i> [class <i>class-options</i>]	进入 SEM 配置模式， <i>applet-name</i> 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 <i>occurs-value</i>] [occurs-period <i>occurs-period-value</i>] [correlate-start <i>period-start-value</i>] [correlate-period <i>correlate-period-value</i>] [delay <i>delay-value</i>] [maxrun <i>maxruntime-number</i>]	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
```

4.2.6 配置CLI行动项输出记录

命令	作用
Ruijie(config)# smart manager applet <i>applet-name</i> [class <i>class-options</i>]	进入 SEM 配置模式， <i>applet-name</i> 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
```

4.2.7 显示当前策略配置

命令	作用

Ruijie(config)# smart manager applet <i>applet-name</i> [class <i>class-options</i>]	进入 SEM 配置模式， <i>applet-name</i> 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)#
```

 说明

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。

4.2.8 提交配置

命令	作用
Ruijie(config)# smart manager applet <i>applet-name</i> [class <i>class-options</i>]	进入 SEM 配置模式， <i>applet-name</i> 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
```

 说明

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。

4.2.9 查看注册策略

命令	作用
Ruijie# show smart manager policy registered [policy <i>policy-name</i>] [event-type <i>event-name</i>] [class <i>class-options</i>] [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"
```

4.2.10 回退配置

命令	作用
Ruijie(config)# smart manager applet <i>applet-name</i> [class <i>class-options</i>]	进入 SEM 配置模式， <i>applet-name</i> 参数制定策略的名字， class 参数指定策略的类别（默认为 <code>default</code> 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
```

 说明

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。

4.2.11 配置多事件触发

命令	作用
Ruijie(config)# smart manager applet <i>applet-name</i> [class <i>class-options</i>]	进入 SEM 配置模式， <i>applet-name</i> 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 <i>event-name</i> [correlate { andnot and or }] syslog pattern <i>regular-expression</i> [priority <i>priority-level</i>] [occurs <i>num-occurrences</i>] [period <i>period-value</i>] [skip { yes no }]	配置首个事件
Ruijie(sem-applet)# event tag <i>event-name</i> [correlate { andnot and or }] syslog pattern <i>regular-expression</i> [priority <i>priority-level</i>] [occurs <i>num-occurrences</i>] [period <i>period-value</i>] [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”；其他事件为检测命令行输入，用户在接口模式下输入 **shutdown**。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 monitor_input cli pattern "shutdown" mode interface
Ruijie(sem-applet)# trigger correlate-period 180
```

 说明

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。

4.2.12 配置和使用变量

命令	作用
Ruijie# smart manager environment <i>variable-name string</i>	配置 SEM 全局变量
Ruijie(config)# smart manager applet <i>applet-name [class class-options]</i>	进入 SEM 配置模式， <i>applet-name</i> 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 <i>variable-name variable-value</i>	设置 SEM 局部变量
Ruijie(sem-applet)# action label syslog <i>[priority priority-level] msg msg-text</i> <i>[facility string]</i>	使用 SEM 变量（多种行动中都支持使用变量，此处以 Syslog 为例，具体请查阅《SEM 命令参考》）

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"
```

说明

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。

4.2.13 挂起/恢复调度器

命令	作用
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
```

说明

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。

4.2.14 暂停/恢复策略执行

命令	作用
<code>Ruijie# smart manager scheduler hold { all policy job-id class class-options }</code>	将执行中的策略暂停
<code>Ruijie# smart manager scheduler release { all policy policy-id class class-options }</code>	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
```

说明

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。

4.2.15 强制中止策略执行

命令	作用
<code>Ruijie# smart manager scheduler clear { all policy job-id class class-options }</code>	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
```

4.2.16 查看SEM历史信息

命令	作用
<code>Ruijie# show smart manager history events</code>	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
```

4.2.17 查看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
```

4.2.18 查看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
none           1.0
snmp           1.0
snmp-object    1.0
snmp-notification 1.0
timer          1.0
```

4.3 配置举例

4.3.1 SEM定时器事件

组网需求

Device A 与 Tftp Server 相连，Device 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



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

- 给 Device A 配置策略取名为 policy_a。
- 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。
- 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
- 将策略提交
- 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"
```

4.3.2 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



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

- 给 Device A 配置策略取名为 policy_a。
- 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”
- 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;
- 将策略提交
- 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
```

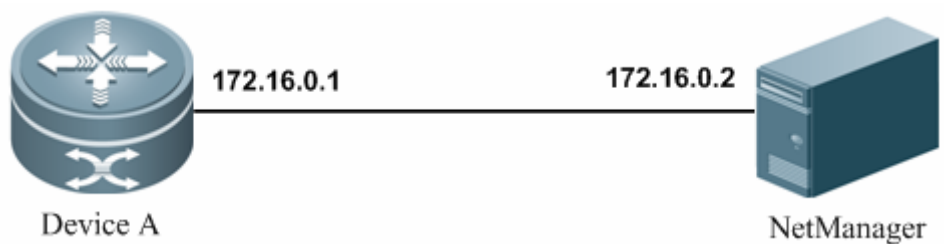
No.	Class	Event Type	Time Registered	Name
1	applet	cli	Mon Mar 8 19:30:00 2010	policy_a
event_1: cli: pattern "copy running-config startup-config" sync yes maxrun 20.000				
action action_1 cli command "enable"				
action action_2 cli command "copy startup-config tftp://172.16.0.2/device_a/conf_\${event_pub_time}"				
action action_3 exit 1				

4.3.3 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



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

- 给 Device A 配置策略取名为 policy_a。
- 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”；

- 给 policy_a 配置行动，记录到日志 snmp 操作被取消。
- 将策略提交
- 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"
```

4.3.4 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。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

- 给 Device A 配置策略取名为 policy_a。

- 给 policy_a 配置名为 event_1 的事件，类型为 none 类型，通过命令行手动触发。
- 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 ip 路由；
- 将策略提交
- 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)# 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 *"
```

4.3.5 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重启。

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

- 给 Device A 配置策略取名为 policy_a。
- 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。
- 给 policy_a 配置 reload 行动。
- 将策略提交
- 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 reload
```



配置指南-网管与监控

本分册介绍网管与监控配置指南相关内容，包括以下章节：

1. 配置 SNMP
2. 配置 RMON
3. 配置 NTP
4. 简单网络时间协议(SNTP)
5. 配置 SPAN
6. 配置 RSPAN
7. 配置 ERSPAN

1 配置 SNMP

1.1 SNMP相关知识

1.1.1 概述

SNMP 是 Simple Network Manager 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。

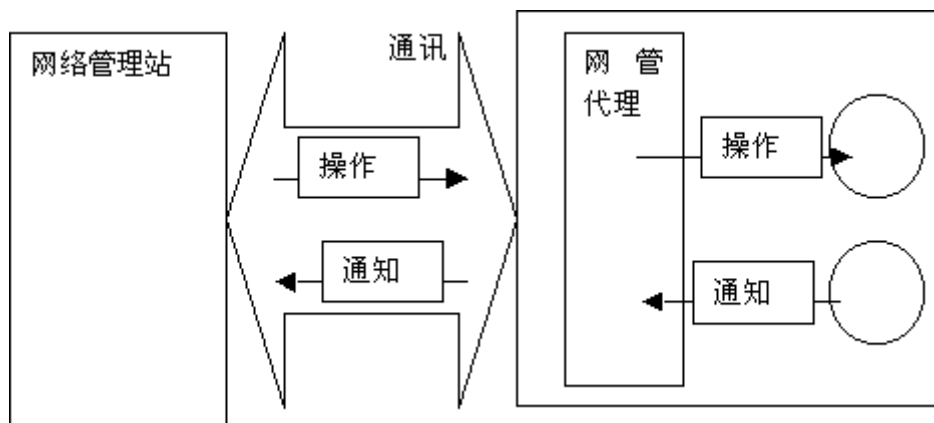
SNMP 是一个应用层协议，为客户机/服务器模式，包括三个部分：

- 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系统，也称为 NMS (Network Management System)。

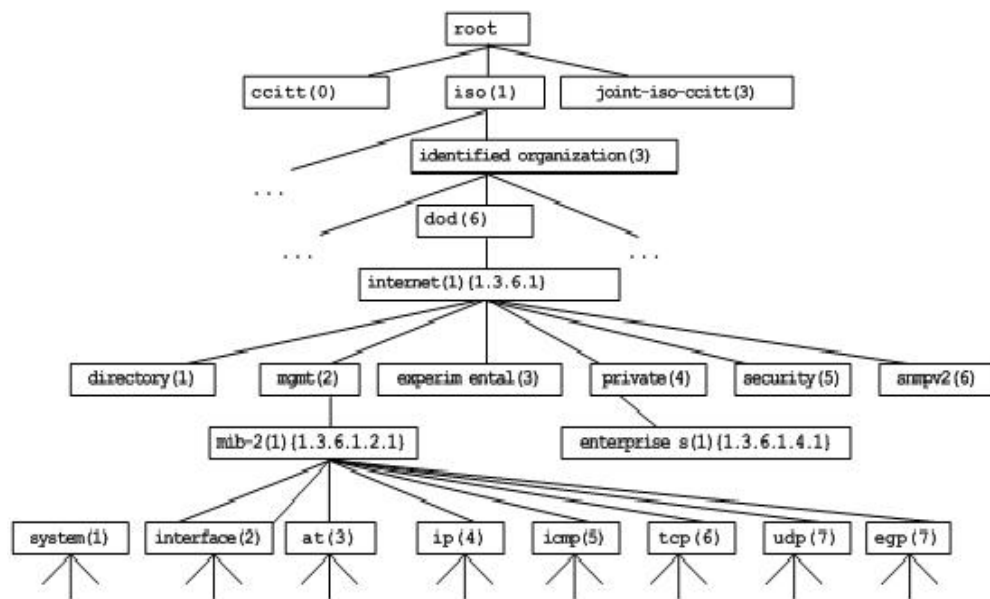
SNMP 代理 (SNMP Agent) 是运行在被管理设备上的软件，负责接受、处理并且响应来自 NMS 的监控和控制报文，也可以主动发送一些消息报文给 NMS。

NMS 和 Agent 的关系可以用如下的图来表示：



网络管理站 (NMS) 与网管代理 (Agent) 的关系图

MIB (Management Information Base) 是一个虚拟的网络管理信息库。被管理的网络设备中包含了大量的信息，为了能够在 SNMP 报文中唯一的标识某个特定的管理单元，MIB 采用树形层次结构来描述网络设备中的管理单元。树的节点表示某个特定的管理单元。如下图 MIB 对象命名树，为了唯一标识网络设备中的某个管理单元 System，可以采用一串的数字来表示，如 {1.3.6.1.2.1.1} 这一串数字即为管理单元的 Object Identifier (单元标识符)，MIB 则是网络设备的单元标识符的集合。



MIB 树形层次结构

1.1.2 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

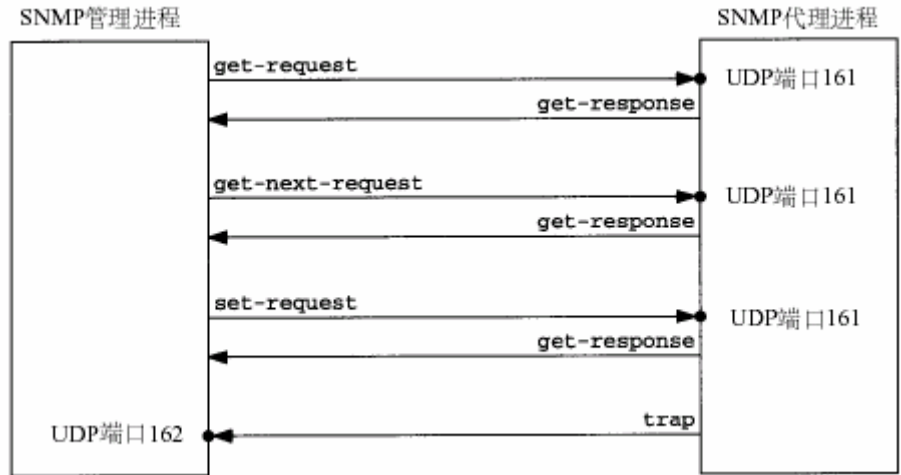
SNMP 协议中的 NMS 和 Agent 之间的交互信息，定义了 6 种操作类型：

- 1) Get-request 操作：NMS 从 Agent 提取一个或多个参数值。
- 2) Get-next-request 操作：NMS 从 Agent 提取一个或多个参数的下一个参数值。
- 3) Get-bulk 操作：NMS 从 Agent 提取批量的参数值；
- 4) Set-request 操作：NMS 设置 Agent 的一个或多个参数值。

5) Get-response 操作: Agent 返回的一个或多个参数值, 是 Agent 对 NMS 前面 3 个操作的响应操作。

6) Trap 操作: Agent 主动发出的报文, 通知 NMS 有某些事情发生。

前面的 4 个报文是由 NMS 向 Agent 发出的, 后面两个是 Agent 发给 NMS 的 (注意: SNMPv1 版本不支持 Get-bulk 操作)。下图描述了这几种操作。



SNMP 的报文类型

NMS 向 Agent 发出的前面 3 种操作和 Agent 的应答操作采用 UDP 的 161 端口。Agent 发出的 Trap 操作采用 UDP 的 162 端口。

1.1.4 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
Step 1	<code>Ruijie(config)# snmp-server community [0 7] string [view view-name] [ro rw] [host host-ip] [aclnum aclname]</code>	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 **no 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
Step 1	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，是否需要认证、是否需要加密；

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
Step 1	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。
Step 2	Ruijie(config)# snmp-server group groupname {v1 v2c v3 {auth noauth priv}} [read readview] [write writeview] [access { [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** 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

Step 1	Ruijie(config)# snmp-server user username groupname {v1 v2 v3 [encrypted] [auth { md5 sha } auth-password] [priv des56 priv-password] } [access { aclnum aclname] }	设置用户信息。

通过 **no snmp-server user username groupname** 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
Step 1	Ruijie(config)# snmp-server host host-addr traps [vrf vrfname] [version {1 2c 3 [auth noauth priv]]} community-string [udp-port port-num] [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、设备的网元编码信息、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
Step 1	Ruijie(config)# snmp-server contact text	设置系统的联系方式
Step 2	Ruijie(config)# snmp-server location text	设置系统的位置
Step 3	Ruijie(config)# snmp-server chassis-id number	设置系统的序列码
Step 4	Ruijie(config)# snmp-server net-id text	设置设备的网元编码信息

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
Step 1	Ruijie(config)# snmp-server packet-size 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
Step 1	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
Step 1	Ruijie(config)# no enable service snmp-agent	关闭 SNMP 代理服务

1.2.10 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
Step 1	Ruijie(config)# snmp-server enable traps [type] [option]	允许 Agent 主动发送 Trap 消息
Step 2	Ruijie(config)# no snmp-server enable traps [type] [option]	禁止 Agent 主动发送 Trap 消息

1.2.11 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
Step 1	Ruijie(config)# interface interface-id	进入端口配置模式
Step 2	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
```

1.2.12 配置TRAP消息携带私有字段

可以指定 Agent 发送 Trap 消息时，携带私有格式字段，目前支持的私有字段包含的信息有：

- 告警的序列号
- 网元标识名
- 告警原始级别：设备上报告警消息中的告警级别：1,严重；2,重要；3,次要；4,一般；5,不确定
- 告警原始类型：设备上报告警消息中的告警类型，包括通讯告警、环境告警、设备告警、处理错误告警、服务质量告警等
- 告警原因号：标识告警原因的内部告警号
- 告警原因：告警原因描述
- 告警发生时间
- 告警状态：表示告警是否被清除还是处于活跃状态
- 告警标题

- 告警内容

以上各个字段的具体数据类型和数据范围可参见《RUIJIE-TRAP-FORMAT-MIB.mib》文件说明。
具体配置命令如下：

	命令	作用
Step 1	Ruijie(config)# snmp-server trap-format private	配置 TRAP 消息携带私有字段
Step 2	Ruijie(config)# no snmp-server trap-format private	取消 TRAP 消息携带私有字段
 说明 当使用 SNMP v1 的版本发送 Trap 消息时，该配置不生效。		

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
Step 1	Ruijie(config)# snmp-server trap-source interface	指定发送 Trap 消息的源接口
Step 2	Ruijie(config)# snmp-server queue-length length	指定每个 Trap 消息报文的队列长度
Step 3	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: 800013110300000000000000
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。

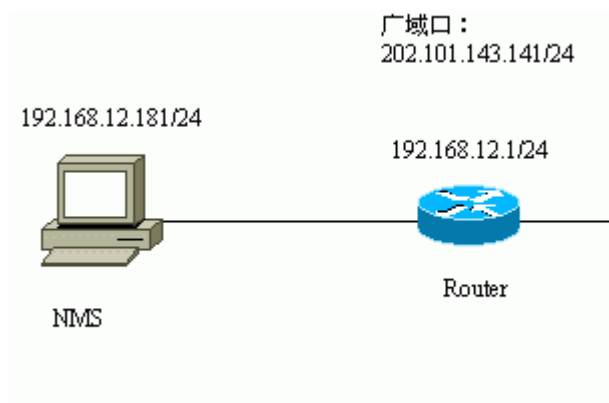
```
Ruijie# show snmp host
Notification host: 192.168.64.221
udp-port: 162   type: trap
user: public    security model: v1
Notification host: 2000:1234::64
udp-port: 162   type: trap
user: public    security model: v1
```

1.4 SNMP配置举例

1.4.1 典型配置实例

1.4.1.1 配置要求

如图，网络设备和网管工作站 NMS 通过以太网连接，NMS 的 IP 地址为 192.168.64.221，网络设备的 IP 地址为 192.168.64.111，在网管工作站上运行了网管软件。



SNMP 典型配置组网图

1.4.1.2 网络设备具体配置

启动 SNMP 代理服务：

```
Ruijie(config)# snmp-server community public R0
```

只需要在全局配置模式下，配置以上指令，网络设备便启动了 SNMP 代理服务功能，这时 NMS 便可以对网络设备进行 SNMP 的监控了，不过只配置了只读权限，不能修改网络设备的配置，只能是监控网络设备。其他的配置都是可选的。

如果有读写功能，可以采用如下的配置：

```
Ruijie(config)# snmp-server community private RW
```

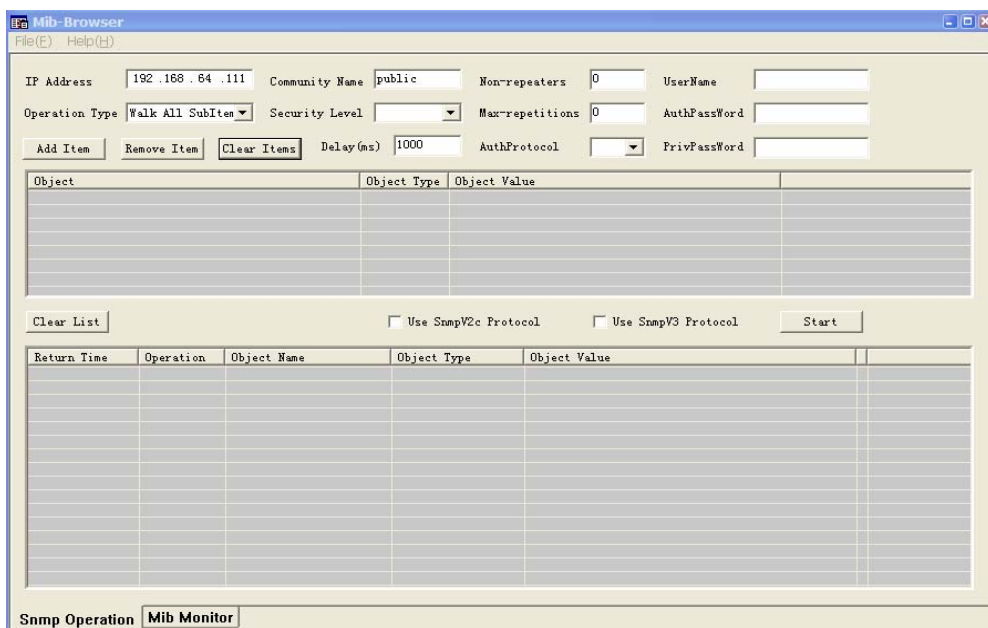
以下是配置网络设备 SNMP 的一些代理基本参数，NMS 可以通过这些参数得知网络设备的一些基本系统信息，该配置为可选配置：

```
Ruijie(config)# snmp-server location fuzhou
Ruijie(config)# snmp-server contact wugb@i-net.com.cn
Ruijie(config)# snmp-server chassis-id 1234567890
0987654321
```

以下的配置，是允许网络设备主动向 NMS 发送一些 Trap 消息，该配置为可选配置：

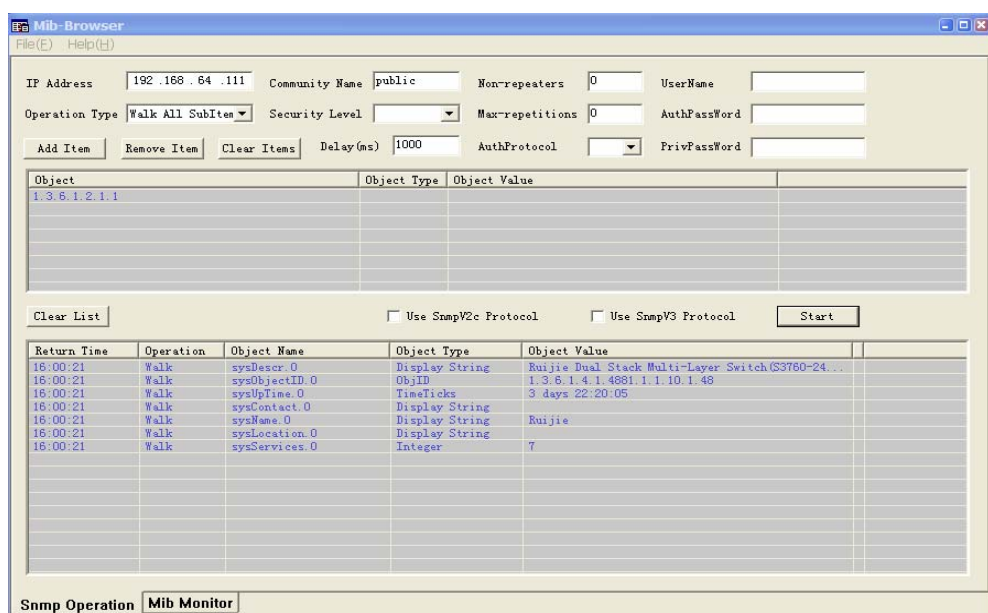
```
Ruijie(config)# snmp-server enable traps
Ruijie(config)# snmp-server host 192.168.64.221 public
```

通过如上配置，网络设备的 SNMP 代理已经配置完毕，NMS 便可以对网络设备进行监控和管理了，以锐捷的 MIB Browser 为例：



MIB Browser 界面

在 IP Address 中输入设备的 IP 地址：192.168.64.111，在 Community Name 中输入 Public，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：



MIB 查询界面

1.4.2 SNMP访问列表关联控制实例

锐捷产品可以设置访问列表关联的方式，只要访问列表中允许的NMS才可以利用SNMP对Agent进行监控和管理，限制NMS对网络设备的访问，提高SNMP的安全性。

在全局配置模式下：

```
Ruijie(config)# access-list 1 permit 192.168.12.181
Ruijie(config)# snmp-server community public RO 1
```

通过如上配置，只有IP地址为192.168.12.181的主机才能利用SNMP对网络设备进行监控和管理了。

1.4.3 SNMPv3 相关配置实例

以下的配置允许 SNMPv3 的管理者采用认证+加密模式通过用户名 v3user 对 MIB-2(1.3.6.1.2.1) 节点下的管理变量进行设置和查看。采用的认证模式为 MD5，使用的认证密码为 MD5-Auth，采用 DES 加密，加密密钥为 DES-Priv。同时允许向 192.168.65.199 以 SNMPv3 格式发送 Trap。发送 Trap 使用的用户名为 v3user,采用认证+加密模式发送，采用的认证模式为 MD5，使用的认证密码为 MD5-Auth，采用 DES 加密，加密密钥为 DES-Priv。

```
Ruijie(config)# snmp-server view v3userview 1.3.6.1.2.1 include
Ruijie (config)# snmp-server group v3usergroup v3 priv read v3userview write v3userview
Ruijie (config)# snmp-server user v3user v3usergroup v3 auth md5 md5-auth priv des56 des-priv
Ruijie (config)# snmp-server host 192.168.65.199 traps version 3 priv v3user
```

2 配置 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, 在网络上相当于一个网络节点, 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:

1. HistoryControl 组用来设置采样间隔时间、采样数据源等控制信息。
2. 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 RMON配置任务列表

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 <i>index</i> [<i>owner ownername</i>]	添加一个统计项
Ruijie(config-if)# no rmon collection stats <i>index</i>	删除一个统计项

注意

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 <i>index</i> [<i>owner ownername</i>] [buckets <i>bucket-number</i>] [interval <i>seconds</i>]	添加一个历史控制表项
Ruijie(config-if)# no rmon collection history <i>index</i>	删除一个历史控制表项

注意

我司产品当前版本只支持以太网的纪录。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 <i>number variable</i> <i>interval</i> { absolute delta } rising-threshold <i>value</i> [<i>event-number</i>] falling-threshold <i>value</i> [<i>event-number</i>] [<i>owner ownername</i>]	添加一个历史控制表项
Ruijie(config)# rmon event <i>number</i> [log] [trap community] [description <i>description-string</i>]	添加一个事件组表项
Ruijie(config)# no rmon alarm <i>number</i>	删除一个警告组
Ruijie(config)# no rmon event <i>number</i>	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

2.2.4 显示RMON状态

命令	作用
Ruijie(config)# show rmon alarm	显示警告组
Ruijie(config)# show rmon event	显示事件组
Ruijie(config)# show rmon history	显示历史组
Ruijie(config)# 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网端口 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

2.3.4.1 show rmon alarm

```
Ruijie# show rmon alarm  
Alarm : 1  
Interval : 1  
Variable : 1.3.6.1.2.1.4.2.0  
Sample type : absolute  
Last value : 64  
Startup alarm : 3  
Rising threshold : 10  
Falling threshold : 22  
Rising event : 0  
Falling event : 0  
Owner : zhangsan
```

2.3.4.2 show rmon event

```
Ruijie# show rmon event  
Event : 1  
Description : firstevent  
Event type : log-and-trap  
Community : public  
Last time sent : 0d:0h:0m:0s  
Owner : zhangsan  
Log : 1  
Log time : 0d:0h:37m:47s  
Log description : ipttl  
Log : 2  
Log time : 0d:0h:38m:56s  
Log description : ipttl
```

2.3.4.3 show rmon history

```
Ruijie# show rmon history  
Entry : 1  
Data source : Gi1/1  
Buckets requested : 65535  
Buckets granted : 10  
Interval : 1  
Owner : zhangsan  
Sample : 198  
Interval start : 0d:0h:15m:0s  
DropEvents : 0  
Octets : 67988  
Pkts : 726  
BroadcastPkts : 502  
MulticastPkts : 189  
CRCAlignErrors : 0  
UndersizePkts : 0  
OversizePkts : 0  
Fragments : 0  
Jabbers : 0  
Collisions : 0  
Utilization : 0
```

2.3.4.4 show rmon statistics

```
Ruijie# show rmon statistics
Statistics : 1
Data source : Gi1/1
DropEvents : 0
Octets : 1884085
Pkts : 3096
BroadcastPkts : 161
MulticastPkts : 97
CRCAlignErrors : 0
UndersizePkts : 0
OversizePkts : 1200
Fragments : 0
Jabbers : 0
Collisions : 0
Pkts64Octets : 128
Pkts65to127Octets : 336
Pkts128to255Octets : 229
Pkts256to511Octets : 3
Pkts512to1023Octets : 0
Pkts1024to1518Octets : 1200
Owner : zhangsan
```


3 配置 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，它可以提供高精度度的时间校正（LAN 上与标准间差小于 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

本章介绍怎样在我们的系统实现中配置 NTP 客户端和服务端。

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设置；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
Step 1	ntp authenticate	配置 NTP 全局安全识别机制。
Step 2	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 标示，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

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。
no ntp authentication-key key-id md5 key-string [enc-type]	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。



注意

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收到数据报的合法性。

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
Step 1	ntp trusted-key key-id	配置 NTP 全局信任密钥 ID。
Step 2	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。



注意

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
Step 1	ntp server ip-addr [version version][source if-name number][key keyid][prefer]	配置 NTP 服务器 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

Step 2	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，才能发起于服务器的加密通信，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
Step 1	interface interface-type number	进入接口配置模式
Step 2	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
ntp authenticate 或 ntp server ip-addr [version version][source if-name number][key keyid][prefer]	打开 NTP 功能
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
ntp update-calendar	配置更新硬件时钟
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的时钟源进行同步。

说明

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
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。
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

注意

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
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
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**。

注意

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 NTP信息显示

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
```

注: **starum** 代表当前时钟的等级, **reference** 为同步服务器的地址, **freq** 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 配置范例

在以下配置中, 网络中有一个指定为 **master** 的 NTP 服务器, 并打开了相应的认证机制, 配置了一个 **key-id** 为 6、**key-string** 为 **w00000p** 的密钥, 并设置该密钥为服务器信任密钥; 为了配置锐捷的客户机可以和网络上的 NTP 服务器进行时间同步, 我们将对客户进行如下配置, 启动安全认证, 并配置一个和 NTP 服务器端一样的密钥, 然后将我们的同步服务器设定为网络上的这个 NTP 服务器, 开始时间同步。

```
Ruijie(config)# no ntp  
Ruijie(config)# ntp authentication-key 6 md5 w00000p  
Ruijie(config)# ntp authenticate  
Ruijie(config)# ntp trusted-key 6  
Ruijie(config)# ntp server 192.168.210.222 key 6  
Ruijie(config)# interface gigabitEthernet 0/1  
Ruijie(config-if)# ntp disable
```

4 简单网络时间协议(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）。

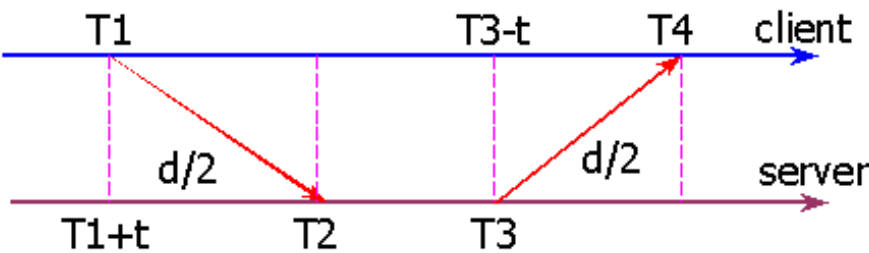
NTP 协议可以跨越各种平台和操作系统，用非常精密的算法，因而几乎不受网络的延迟和抖动的影响，可以提供 1-50 ms 精度。NTP 同时提供认证机制，安全级别很高。但是 NTP 算法复杂，对系统要求较高。

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。

4.1.1 SNTP原理

SNTP 协议采用客户/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。



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: 客户方发送查询请求时间(以客户方时间系统为参照)，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: 客户方收到时间信息包时间(以客户方时间系统为参照)，标记为 Destination Timestamp;

T: 服务器和客户端之间的时间偏差;

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 $T4 + t$

4.2 配置SNTP

本章节将介绍如何配置 SNTP

4.2.1 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

4.2.2 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**

2. 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”时间请勿小于 5 秒)。

Ruijie(config)# **sntp enable**

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**

您如果要关闭 SNTP，可以用 **no sntp enable** 全局配置命令来关闭 SNTP。

4.2.3 配置NTP 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做为交换机上的 NTP 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
```

2. 设置 SNTP Server 的 IP 地址。

```
Ruijie(config)# sntp server <ip-addr>
```

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
```

4.2.4 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。以下步骤将配置交换机和 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
```



注意

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。

4.2.5 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**

2. 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 time-zone** <time-zone>

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**

您可以通过 **no clock time-zone** 来恢复缺省值。

4.3 显示SNTP

步骤如下：

1. 查看 SNTP 的相关参数

Ruijie# **show sntp**

2. 使用 **show sntp** 查看系统保护的配置参数：

Ruijie# **show sntp**

SNTP state	: ENABLE	//SNTP 是否打开
SNTP server	: 192.168.4.12	//NTP Server
SNTP sync interval	: 60	//定时同步的时间间隔
Time zone	: +8	//本地时区

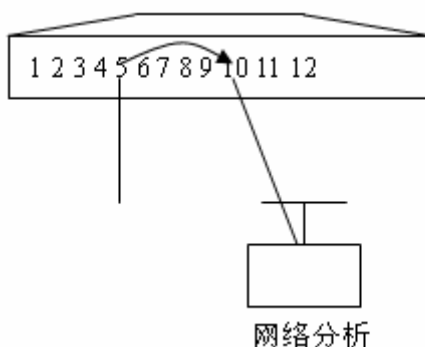
5 配置 SPAN

5.1 概述

5.1.1 理解SPAN

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。



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概念和术语

该部分描述和 SPAN 配置相关的一些概念和术语。

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

5.2.2.1 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。

5.2.2.2 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。

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

本部分描述如何在交换机上配置 SPAN，包含以下配置：

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
Step 1	Ruijie(config)# monitor session <i>session_num</i> source interface <i>interface-id</i> [, -] { both rx tx }	指定源端口。对于 <i>interface-id</i> , 请指定相应的接口号。
Step 2	Ruijie(config)# monitor session <i>session_num</i> destination interface <i>interface-id</i> { encapsulation switch }	指定目的端口。对于 <i>interface-id</i> , 请指定相应的接口号, 添加 encapsulation 参数将支持镜像口封装功能, 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
```

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
Step 1	Ruijie(config)# no monitor session <i>session_num</i> source interface <i>interface-id</i> [, -] { both rx tx }	指定需删除的源端口。对于 <i>interface-id</i> , 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 VSPAN配置

VSPAN 是 VLAN SPAN 的简称，是指将某些 VLAN 的数据流或将某些 VLAN 排除后的数据流作为数据源，镜像到目的端口。在全局配置模式下，按照以下步骤可以设置 VSPAN。

	命令	作用
Step 1	Ruijie(config)# [no] monitor session session_num source vlan vlan-id-list [rx tx both]	指定某些 VLAN 作为镜像的数据源
Step 2	Ruijie(config)# [no] monitor session session_num filter vlan vlan-id-list	指定某些 VLAN 不作为镜像的数据源

各产品支持情况

只支持 RX 方向 VSPAN 镜像，不支持 TX 方向的 VSPAN。

5.3.5 其他注意事项

- 请将网络分析仪连接到监控口。
- 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:
```

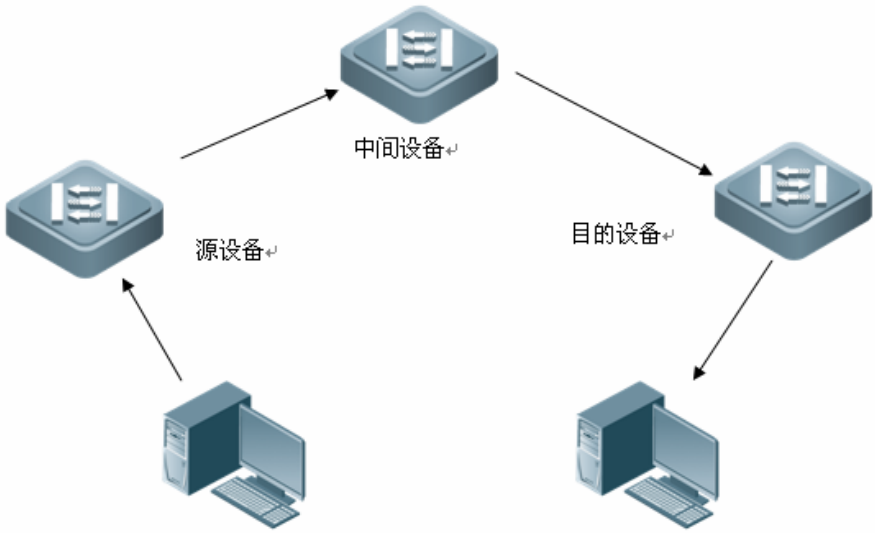
6 配置 RSPAN

本章描述锐捷设备的 RSPAN 配置。

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：



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。

 说明

- 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。
- Remote VLAN 不能是 VLAN 1，也不能是 Private VLAN。
- Remote VLAN 不参与 GVRP。

6.2 配置RSPAN

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

6.2.2.1 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。

6.2.2.2 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。

6.2.2.3 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。

6.2.2.4 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。

6.2.2.5 配置步骤

源设备的配置步骤如下所示：

	命令	作用
Step 1	Ruijie# configure	进入全局配置模式
Step 2	Ruijie(config)# vlan <i>vlan-id</i>	进入 Vlan 配置模式
Step 3	Ruijie(config-Vlan)# remote-span	设置 Vlan 为 remote-span Vlan
Step 4	Ruijie(config-Vlan)# exit	退到全局配置模式
Step 5	Ruijie(config)# monitor session <i>session_num</i> remote-source	配置远程源镜像
Step 6	Ruijie(config)# monitor session <i>session-num</i> source interface <i>interface-name</i> [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)
Step 7	Ruijie(config)# monitor session <i>session_num</i> destination remote <i>vlan remote_vlan-id</i> interface <i>interface-name</i> [switch]	配置远程源镜像组的 Remote VLAN Switch 关键字表示目的口参与交换
Step 8	Ruijie(config)# monitor session <i>session_number</i> source interface <i>interface-id</i> rx <i>acl name</i>	设定需要镜像的流所匹配的 acl name

说明

- 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
Step 1	Ruijie# configure	进入全局配置模式
Step 2	Ruijie(config)# vlan <i>vlan-id</i>	进入 Vlan 配置模式
Step 3	Ruijie(config-Vlan)# remote-span	设置 Vlan 为 remote-span Vlan
Step 4	Ruijie(config-Vlan)# exit	退到全局配置模式

6.2.4 目的交换机上的配置

6.2.4.1 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。

6.2.4.2 配置步骤

	命令	作用
Step 1	Ruijie# configure	进入全局配置模式
Step 2	Ruijie(config)# vlan <i>vlan-id</i>	进入 vlan 配置模式
Step 3	Ruijie(config-Vlan)# remote-span	设置 vlan 为 remote-span vlan
Step 4	Ruijie(config-Vlan)# exit	退到全局配置模式
Step 5	Ruijie(config)# monitor session <i>session_num</i> remote-destination	配置远程目的镜像
Step 6	Ruijie(config)# monitor session <i>session-num</i> destination remote vlan <i>vlan-id</i> interface <i>interface-name</i> [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
Step 7	Ruijie(config)# interface <i>interface-name</i>	进入远程镜像目的端口
Step 8	Ruijie(config-if)# switchport access vlan <i>vid</i> switchport trunk native vlan <i>vid</i>	<i>vid</i> 表示 remote-span vlan 的 <i>vid</i> 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)。

说明

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。

6.3 显示RSPAN会话

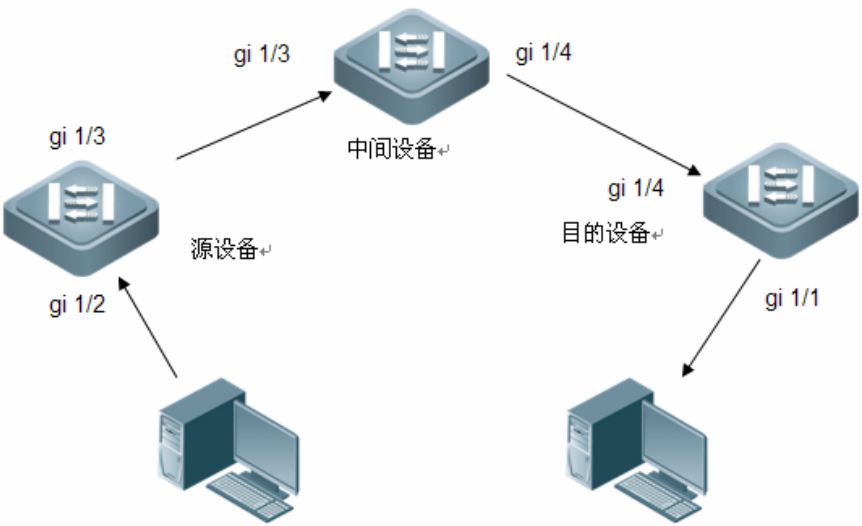
	命令	作用
Step 1	Ruijie# show monitor	显示镜像

示例：

```
Ruijie# show monitor
sess-num: 1
src-intf:
GigabitEthernet 0/4 frame-type Both
dest-intf:
GigabitEthernet 0/6
remote vlan 3
```

6.4 配置举例

设备拓扑如下所示：



SPAN 典型拓扑

6.4.1.1 源交换机配置

```
Ruijie# configure
Ruijie(config)# vlan 7
Ruijie(config-Vlan)# remote-span
Ruijie(config-Vlan)# exit
Ruijie(config)# interface gigabitEthernet1/3
Ruijie(config-if)# switchport mode trunk
```

```
Ruijie(config-if)# switchport trunk allowed vlan add 7
Ruijie(config-if)# exit
Ruijie(config)# monitor session 2 remote-source
Ruijie(config)# monitor session 2 source interface gigabitEthernet1/2
Ruijie(config)# monitor session 2 destination remote vlan 7 interface
gigabitEthernet 1/3 switch
```

6.4.1.2 中间交换机配置

```
Ruijie# configure
Ruijie(config)# vlan 7
Ruijie(config-Vlan)# remote-span
Ruijie(config-Vlan)# exit
Ruijie(config)# interface gigabitEthernet1/3
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# switchport trunk allowed vlan add 7
Ruijie(config-if)# exit
Ruijie(config)# interface gigabitEthernet1/4
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# switchport trunk allowed vlan add 7
```

6.4.1.3 目的交换机配置

```
Ruijie# configure
Ruijie(config)# vlan 7
Ruijie(config-Vlan)# remote-span
Ruijie(config-Vlan)# exit
Ruijie(config)# interface gigabitEthernet 1/4
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# switchport trunk allowed vlan add 7
Ruijie(config-if)# exit
Ruijie(config)# monitor session 2 remote- destination
Ruijie(config)# monitor session 2 destination remote vlan 7
Inter interface gigabitEthernet 1/1 switch
```

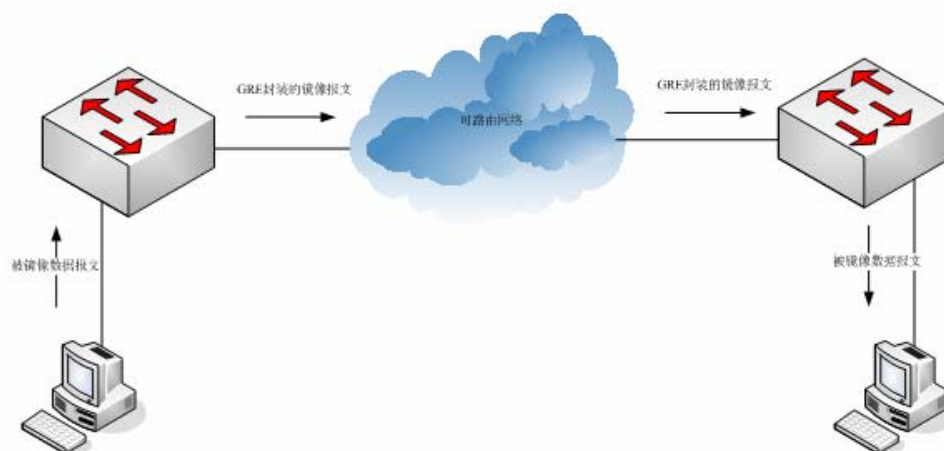
7 配置 ERSPAN

本章描述锐捷设备的 ERSPAN 配置。

7.1 概述

封装远程端口镜像(ERSPAN)是远程端口镜像(RSPAN)的扩展。普通的远程端口镜像，镜像数据报文只能在二层内传输，无法经过路由的网络，而封装远程端口镜像却可以将镜像报文在路由的网络间传输。

ERSPAN 实现的功能是将所有的被镜像报文通过一个 GRE 隧道封装成 IP 报文，路由到远端镜像设备的目的端口，典型应用拓扑如下所示：



ERSPAN 典型应用拓扑图

图中各设备的角色分为两种：

- 源交换机：封装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 GRE 封装成 IP 报文进行转发，传输给目的交换机。
- 目的交换机：封装远程镜像目的端口所在的交换机，将接收到的镜像报文通过镜像目的端口，进行解封装 GRE 报文后转发给监控设备。

要实现封装远程端口镜像功能，进行的 GRE 封装后的 IP 报文是必须可以在网络中正常路由到目的镜像设备的。

注意

目前我司设备还没有支持 ERSPAN 目的交换机功能的设备。对于目的交换机设备可以直接使用分析仪器设备，通过分析仪设备的软件报文解析工具来解析封装的 GRE 报文（如 PC 设备，可以使用 Ethereal, Wireshark, Sniffer 等主流报文解析软件都能支持 GRE 报文的解析）。

7.2 配置ERSPAN

- 配置准备
- 源交换机上的配置
- 配置举例

7.2.1 配置准备

- 确定源交换机、目的交换机
- 确定镜像源端口、镜像目的端口
- 确认从源交换机到目的交换机的三层路由互通性
- 确定被监控报文的方向

7.2.2 源交换机上的配置

- ERSPAN 会话
- 源端口
- ERSPAN 会话使能
- 封装源 IP 地址
- 封装目的 IP 地址
- 封装 IP TTL/DSCP 值等
- 配置步骤

7.2.2.1 ERSPAN会话

配置交换机设备的 ERSPAN 功能，区分设备的 ERSPAN 交换机的属性。

	命令	作用
Step 1	Ruijie(config)# monitor session session_num erspan-source	配置 ERSPAN 的会话，在源交换机上，通过配置 erspan-source 来完成。

7.2.2.2 源端口

源端口也被称为被监控口，在 ERSPAN 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 ERSPAN 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。

	命令	作用
Step 1	Ruijie(config-mon-erspan-src)# source {interface single_interface} [rx tx both]	配置镜像源端口

7.2.2.3 ERSAN会话使能

对 ERSPAN 会话使能，默认是开启 ERSPAN 镜像功能。

Step 1	Ruijie (config-mon-erspan-src)# shutdown	关闭 ERSPAN 镜像功能
	Ruijie (config-mon-erspan-src)# no shutdown	(默认)开启 ERSPAN 镜像功能

7.2.2.4 封装源IP地址

封装源 IP 地址是用来设置封装的 GRE 报文的源 IP 地址。

	命令	作用
Step 1	Ruijie(config-mon-erspan-src)# origin ip address ip-address	配置封装源 IP 地址

7.2.2.5 封装目的IP地址

封装目的 IP 地址是用来设置封装的 GRE 报文的目的 IP 地址，保证镜像报文可以正常的在网络中路由。

	命令	作用
Step 1	Ruijie(config-mon-erspan-src)# destination ip address ip-address	配置封装目的 IP 地址

7.2.2.6 封装IP TTL/DSCP等

封装 IP 报文的 TTL 和 DSCP 值。

	命令	作用
Step 1	Ruijie(config-mon-erspan-src)# ip ttl ttl_value	配置封装 IP 的 TTL 值，默认值为 64
	Ruijie(config-mon-erspan-src)# ip dscp dscp_value	配置封装 IP 的 DSCP 值，默认值为 0，该功能只有在镜像源端口配置了信任 DSCP 时才生效。

7.2.2.7 配置步骤

源设备的配置步骤如下所示：

	命令	作用
Step 1	Ruijie# configure terminal	开启全局配置模式
Step 2	Ruijie (config)# monitor session ERSPAN_source_session_number erspan-source	配置一个 ERSPAN 会话号，并进入 ERSPAN 源镜像设备的配置模式
	Ruijie (config)# no monitor session {session_number all}	清除镜像配置
Step 3	Ruijie (config-mon-erspan-src)# shutdown Ruijie (config-mon-erspan-src)# no shutdown	关闭 ERSPAN 镜像功能 (默认)开启 ERSPAN 镜像功能

Step 4	Ruijie (config-mon-erspan-src)# source {interface single_interface } [rx tx both]	关联 ERSPAN 镜像的源端口，并选择镜像的方向
Step 5	Ruijie (config-mon-erspan-src)# destination ip address ip_address	配置 ERSPAN 流目的 IP 地址。该地址必须是目的设备上的接口地址。
Step 6	Ruijie (config-mon-erspan-src)# original ip address ip_address	配置 ERSPAN 封装源 IP 地址
Step 7	Ruijie (config-mon-erspan-src)# ip ttl ttl_value	(可选)配置 ERSPAN 封装的 IP 头 TTL 值
Step 8	Ruijie (config-mon-erspan-src)# ip dscp dscp_value	(可选)配置 ERSPAN 封装的 IP 头 dscp 字段值

7.3 显示ERSPAN会话

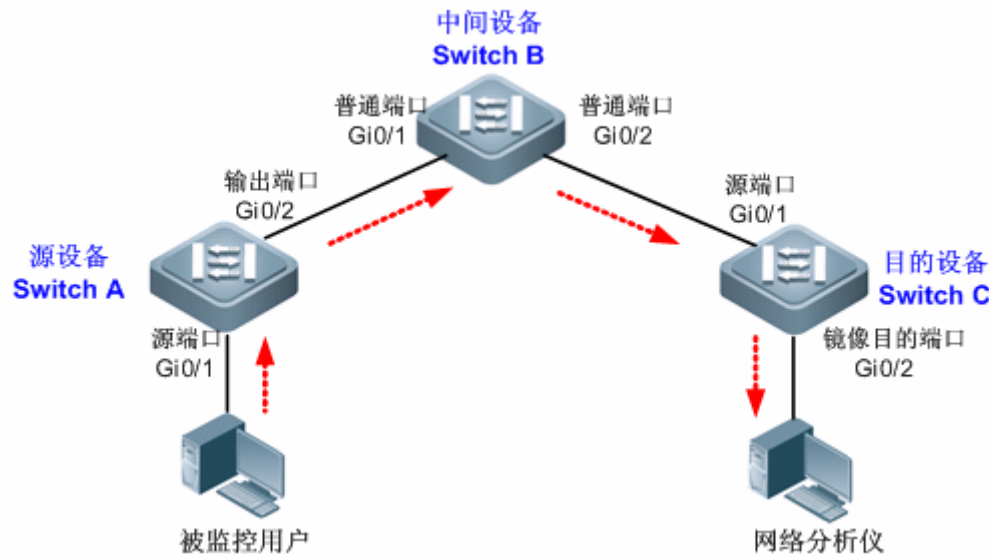
	命令	作用
Step 1	Ruijie# show monitor	显示镜像

示例：

```
Ruijie# show monitor
sess-num: 1
span-type: ERSPAN_SOURCE
src-intf:
GigabitEthernet 0/4 frame-type Both    status: Active
dest-intf:
GigabitEthernet 0/6
span-type erspan-source
origin ip address 10.1.1.2
destination ip address 12.1.1.2
ip ttl 64
ip dscp 0
```

7.4 ERSPAN典型配置用例

7.4.1.1 拓扑图



7.4.1.2 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。

7.4.1.3 配置要点

1. 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。
2. 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）分别为两个网段的 SVI 口的成员口，并保证这两个 IP 网段可以互通。

7.4.1.4 配置步骤

配置 ERSPAN 源设备。

！在 Switch A 上，创建 ERSPAN Session 1，设置为源设备，并设置端口 Gi 0/1 为源端口。

```
SwitchA(config)#monitor session 1 erspan-source
SwitchA(config-mon-erspan-src)#source interface gigabitEthernet 0/1 both
SwitchA(config-mon-erspan-src)#origin ip address 10.1.1.2
SwitchA(config-mon-erspan-src)#destination ip address 12.1.1.2
```

7.4.1.5 验证结果

第一步，查看设备配置信息。

！Switch A 的配置

```
SwitchA#show running-config
!
monitor session 1 erspan-src
source interface GigabitEthernet 0/1 both
origin ip address 10.1.1.2
destination ip address 12.1.1.2
```

第二步，查看设备的 RSPAN 信息

！查看 Switch A

```
SwitchA#show monitor
sess-num: 1                               //ERSPAN Session
span-type: ERSPAN_SOURCE                  //ERSPAN 源设备
src-intf:                                 //ERSPAN 源端口信息
GigabitEthernet 0/1                       frame-type Both status: Active
dest-intf:                                 //ERSPAN 输出端口信息
GigabitEthernet 0/2
origin ip address 10.1.1.2
destination ip address 12.1.1.2
ip ttl 64
ip dscp 0
```