配置手册

RG-NBS200F 系列交换机

RGOS 10.4(3b16)p7

文档版本号：V1.1

版权声明

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 (3b16)p7

读者对象

本书适合下列人员阅读

- 网络工程师
- 技术推广人员
- 网络管理员

技术支持

- 锐捷网络官方网站：http://www.ruijie.com.cn/
- 锐捷网络在线客服：http://webchat.ruijie.com.cn
- 锐捷网络官方网站服务与支持版块：http://www.ruijie.com.cn/service.aspx
- 7×24 小时技术服务热线：4001-000-078
- 锐捷网络技术论坛：http://ryzj.ruijie.com.cn/
- 常见问题搜索：http://www.ruijie.com.cn/service/know.aspx
- 锐捷网络技术支持与反馈信箱：4001000078@ruijie.com.cn

相关资料

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

本书约定

1) 命令行格式约定

命令行格式意义如下：

粗体：命令行关键字（命令中保持不变必须照输的部分）采用加粗字体表示。

斜体：命令行参数（命令中必须由实际值进行替代的部分）采用斜体表示

[ ] ：表示用[ ] 括起来的部分，在命令配置时是可选的。

{ x | y | ... }：表示从两个或多个选项中选取一个。

[x | y | ...]：表示从两个或多个选项中选取一个或者不选。

//：由双斜杠开始的行表示为注释行。

2) 各类标志

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

注意、警告、提醒操作中应注意的事项。

说明、提示、窍门、对操作内容的描述进行必要的补充。

对于产品支持情况进行必要的补充。

3) 说明

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

配置指南-系统配置

本分册介绍系统配置配置指南相关内容，包括以下章节：

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

1 命令行界面

本章节说明使用命令行界面的方法，您可以通过使用命令行界面来管理网络设备。

1.1 命令模式概述

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

在命令提示符下输入问号键（?）可以列出每个命令模式支持使用的命令。

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

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

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

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

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

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

1.2 界面配置

1.2.1 获得帮助

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

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

1.2.2 简写命令

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

例如 **show configuration** 命令可以写成：

```
Ruijie# show conf
```

1.2.3 使用命令的no和default选项

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

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

1.2.4 CLI的提示信息

下表列出了用户在使用 CLI 管理网络设备时可能遇到的错误提示信息。

常见的 CLI 错误信息：

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

1.2.5 使用历史命令

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

从历史命令记录重新调用输入过的命令，执行下表中的操作：

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

1.2.6 使用编辑特性

本节描述在进行命令行编辑时可能使用到的编辑功能。

编辑快捷键

下表列出编辑快捷键：

功能	快捷键	说明

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

命令行滑动窗口

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

编辑命令行时光标移动操作如下表：

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

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

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

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

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

默认的终端行宽是 80 个字符。

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

1.2.7 CLI输出信息的过滤和查找

使用 Show 命令的查找和过滤

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

命令	作用

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

支持在任意模式下执行 **Show** 命令。

查找的信息内容需要区分大小写，以下相同。

要在 **show** 命令的输出信息中过滤指定的内容，可以使用以下命令：

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

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

1.2.8 使用命令别名

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

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

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

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

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

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

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

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

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

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

```
start-terminal-service
```

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

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

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

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

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

命令别名在使用时必须完整输入，否则不能被识别。

使用 **show aliases** 命令可以查看系统中的别名设置。

1.2.9 访问CLI

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

2 基础管理

2.1 基础管理概述

2.1.1 通过命令的授权控制用户访问

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

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

2.1.2 登录认证控制

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

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

2.1.3 系统时间配置

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

2.1.4 系统名称和命令提示符

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

2.1.5 标题配置

当用户登录网络设备时，需要告诉用户一些必要的信息。可以通过设置标题来达到这个目的。可以创建两种类型的标题（banner）：每日通知和登录标题。每日通知针对所有连接到网络设备的用户，当用户登录网络设备时，通知消息将首

先显示在终端上。利用每日通知，可以发送一些较为紧迫的消息（比如系统即将关闭等）给网络用户。登录标题显示在每日通知之后，它的主要作用是提供一些常规的登录提示信息。缺省情况下，每日通知和登录标题均未设置。

2.1.6 查看系统信息

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

2.1.7 控制台速率配置

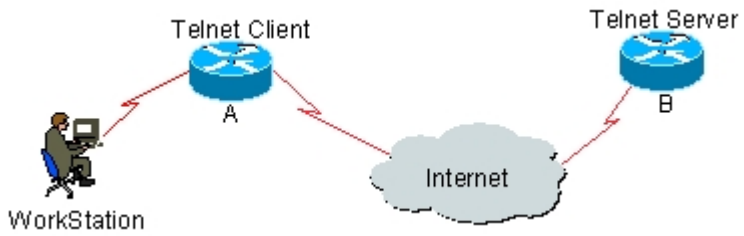
网络设备有一个控制台接口（Console），通过这个控制台接口，可以对网络设备进行管理。当网络设备第一次使用的时候，必须采用通过控制台口方式对其进行配置。可以根据需要改变网络设备串口的速率。需要注意的是，用来管理网络设备的终端的速率设置必须和网络设备的控制台的速率一致。

2.1.8 在网络设备上使用telnet

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

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

图 2-1



2.1.9 连接超时设置

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

2.2 基础管理配置

2.2.1 缺省的口令和特权级别配置

缺省没有设置任何级别的口令，缺省的级别是 15 级。

2.2.2 设置和改变各级别的口令

锐捷产品提供下面的命令用于设置和改变各级别的口令。

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

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

2.2.3 命令授权配置

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

你可以使用如下命令对命令进行授权：

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

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

2.2.4 命令授权配置实例

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

```
Ruijie# configure terminal
Ruijie(config)# privilege exec all level 1 reload
```

```
Ruijie(config)# enable secret level 1 0 test
Ruijie(config)# end
```

进入 1 级，可以看见命令和子命令：

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

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

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

进入 1 级，命令权限已经被收回：

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

2.2.5 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
Ruijie(config-line)# **password** [**0** | **7**] *line*	指定 line 线路口令 0：以明文方式配置口令； 7：以密文方式配置口令； Line：配置的口令字符串；
Ruijie(config-line)# **login**	启用 line 线路口令保护

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

2.2.6 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。

2.2.6.1 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
Ruijie(config)# **password policy min-size** *length*	设置口令最小长度 *length*：口令最小长度
Ruijie(config)# **no password policy min-size**	取消口令最小长度检查

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

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

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

2.2.6.2 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。弱口令是指：

- 与账号同名的口令；
- 只包含字符或数字的口令。

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

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

如果在配置强口令检查之后，配置弱强度的口令，将提示配置失败。

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

2.2.6.3 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** 配置。

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

重复口令检查是基于特权级别或者用户分别记录最近使用过的口令，具体区别如下：

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

如果用户配置最近几次已经使用过的命令，将提示配置失败。

2.2.6.4 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
Ruijie(config)# **password policy life-cycle** *days*	配置口令生存周期 *days:* 口令生存周期，单位：天
Ruijie(config)# **no password policy life-cycle**	取消口令生存周期

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

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

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

2.2.7 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，口令认证成功后，系统自动解锁。

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

2.2.8 配置本地用户

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

要建立用户名身份认证，请在全局配置模式下，根据具体需求执行以下命令：

命令	作用
Ruijie(config)# **username** *name* [**password** *password* | **password** *encryption-type encrypted password*]	使用加密口令建立用户名身份认证
Ruijie(config)# **username** *name* [**privilege** *level*]	为用户设置权限级别（可选）

2.2.9 配置用户文件操作权限

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

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

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

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

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

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

```
username test permission rx /
```

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

2.2.10 配置线路登录认证

要建立线路登录身份认证，请在线路配置模式下，根据具体需求执行以下命令：

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

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

2.2.11 设置系统时间

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

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

命令	作用

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

例如把系统时间改成 2003-6-20，10:10:12

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

2.2.12 查看系统时间

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

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

2.2.13 硬件时钟更新

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

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

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

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

使用如下命令可以将当前软件时钟的时间和日期复制到硬件时钟：

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

2.2.14 定时重启

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

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

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

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

指定系统在将来的某个时间点重启。输入的时间值必须是将来的某个时间点。参数 *year* 是可选的,如果用户没有输入，则默认的年份是系统时钟的年份，由于我们限制了时间跨度不能超过 31 天，所以一般地，如果当前系统日期是在 1 月 1 日到 11 月 30 日之间，则用户就没有必要输入年份。但是，如果当前系统月份为 12 月份，这时用户指定的重启时间就有可能并且允许是明年 1 月的某个时间 ，在这种情况下，用户就需要输入年份来通知系统重启时间是明年 1 月份而不是今年

1 月份，如果没有输入，则默认的会被认为是今年 1 月份，从而导致设置失败。*string* 的用法同上。比如当前系统时间是 2005-01-10 14:31，我们想要系统在明天上班时重启，我们可以键入 **reload at** *08:30 11 1 newday*。或者假如当前系统时间是 2005-12-10 14:31，我们想要系统在 2006-01-01 12:00 重启，我们可以键入 **reload at** *12:00 1 1 2006 newyear*。

```
reload  cancel
```

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

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

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

指定系统在某个时间重启

在特权模式下，通过如下命令，可以指定系统在将来的某个时间重启：

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

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

```
Ruijie# reload at 12:00 1 11 2005 midday//设置重启系统时间和日期
Ruijie# show reload                                  //确认修改重启时间生效
Reload scheduled in 16581 seconds.
At 2005-01-11 12:00
Reload reason: midday
```

指定系统一段时间后重启

在特权模式下，使用如下命令指定系统一段时间后重启：

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

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

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

或者是：

```
Ruijie# reload in 2:5 test                          //设置重启系统时间
```

```
Ruijie# show reload                              //确认修改重启时间生效
System will reload in 7485 seconds.
```

2.2.15 直接重启

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

2.2.16 删除已设置的重启策略

在特权模式下，使用如下命令删除已设置的重启计划：

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

如果之前没有设置重启计划，则会提示之前没有配置重启动计划。

2.2.17 配置系统名称

锐捷产品提供全局配置模式下的命令来配置系统的名称：

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

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

```
Ruijie# configure terminal                       //进入全局配置模式
Ruijie(config)# hostname RGOS       //设置网络设备名称为 RGOS
RGOS(config)#                                    //名称已经修改
```

2.2.18 配置命令提示符

如果你没有配置命令提示符，则系统名称（如果系统名称超过 32 个字符，则截取其前 32 个字符）将作为缺省提示符，提示符将随着系统名称的变化而变化。可以在全局配置模式下使用 **prompt** 命令配置命令提示符，命令的提示符只对 EXEC 模式有效。

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

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

2.2.19 配置每日通知

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

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

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

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

2.2.20 配置登录标题

可以通过以下全局配置模式的命令来设置登录标题信息：

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

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

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

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

2.2.21 显示标题

标题的信息将在你登录网络设备时显示，下面是一个标题显示的例子：

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

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

2.2.22 显示当前模式配置

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

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

2.2.23 查看系统、版本信息

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

命令	作用
show version	显示系统、版本信息

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

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

2.2.24 显示硬件实体信息

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

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

2.2.25 设置控制台速率

在线路配置模式下，可以使用以下命令来设置控制台的速率：

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

下面的例子表示如何将串口速率设置为 57600 bps：

```
Ruijie# configure terminal                          //进入全局配置模式
Ruijie(config)# line console 0                     //进入控制台线路配置模式
Ruijie(config-line)# speed 57600                   //设置控制台速率为 57600
Ruijie(config-line)# end                                 //回到特权模式
Ruijie# show line console 0                        //查看控制台配置
CON     Type    speed   Overruns
* 0     CON     57600   0
Line 0, Location: "", Type: "vt100"
Length: 25 lines, Width: 80 columns
Special Chars: Escape  Disconnect  Activation
               ^^x     none        ^M
Timeouts:      Idle EXEC    Idle Session
               never        never
History is enabled, history size is 10.
Total input: 22 bytes
Total output:  115 bytes
Data overflow:  0 bytes
stop rx interrupt:  0 times
Modem: READY
```

2.2.26 使用Telnet Client

可以通过网络设备上的 telnet 命令登录到远程设备上去：

命令	作用
Ruijie# **telnet** *host* [*port*] [**/source** {**ip** *A.B.C.D* **| interface** *interface-name*}]	通过 telnet 登录到远程设备，可以是 IPV4 主机名、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:
```

使用 Telnet Server

可以通过执行以下命令，来打开网络设备的 Telnet Server 服务：

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

2.2.27 连接超时

当前已接受的连接，在指定时间内，没有任何输入信息，服务器端将中断此连接。

锐捷产品提供 LINE 配置模式下的命令来配置连接超时时间：

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

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

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

2.2.28 会话超时

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

锐捷产品提供 LINE 配置模式下的命令来配置到远程终端的会话超时时间：

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

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

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

2.2.29 批处理执行文件中的命令

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

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

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

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

执行的结果：

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

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

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

2.2.30 服务开关设置

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

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

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

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

如果只需打开 http 服务，使用如下命令：

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

如果只需打开 https 服务，使用如下命令：

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

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

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

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

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

2.2.31 HTTP服务参数设置

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

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

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

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

使用如下命令配置 HTTPS 服务端口

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

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

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

使用如下命令验证 web 服务器状态：

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

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

2.2.32 多重引导功能配置

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

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

添加启动主程序配置

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

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

10.4（2）及以上的版本才支持使用 URL 前缀来定位文件（具体请参阅《文件系统配置指南》），在此之前的版本请使用路径进行文件定位。例如：

flash:/rgos.bin 表示设备内置 flash 根目录下的 rgos.bin 文件。

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

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

■ 指定本地 Flash 上的文件

可以如下指定本地 Flash 上文件为主程序文件：

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

当使用 prefix 指定本地文件时，“: ”后的路径必须是绝对路径。

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

1) 文件必须存在；

2) 文件为合法的 RGOS 主程序；

3) 文件完整，能通过 CRC 校验。

只要有任一条件不能满足，系统都将提示错误并拒绝设置，如：

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

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

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

■ 指定远程 TFTP 服务器上的文件

可以如下配置设备从 TFTP 服务器引导：

```
Ruijie(config)# boot system 2 tftp://192.168.7.24/rgos.bin
```

☑ 目前交换机设备尚不支持从 TFTP 服务器引导早于 10.4（3）版本的 RGOS 安装包文件。

要使设备能够在引导过程中通过 TFTP 协议下载主程序，还必须使用 **boot ip** 命令正确配置设备在启动过程中用于 TFTP 传输的本地 IP：

命令	作用
Ruijie(config)# **boot ip** *local-ip*	配置设备在启动过程中用于 TFTP 传输的本地 IP。
Ruijie(config)# **no boot ip**	清除 boot ip 配置

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

使用 TFTP 传输引导方式时需要设备内置 flash 上有足够的可用空间存放引导文件，引导时会在设备内置 flash 上以隐藏文件的方式存放该引导文件，下次引导前进行清除。

可以如下配置设备在启动阶段使用的 IP：

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

如果没有配置 **boot ip**，设备在引导过程中会因为没有本地 IP 无法通信的缘故导致所有 TFTP 服务器上的主程序文件加载失败。在这种情况下启机时会打印这样的提示：

```
Load program file: [tftp://192.168.7.24/rgos.bin]
[Failed] (Boot IP was not assigned)
Load program file: [/rgos.bin]
[OK]
Executing program, launch at: 0x00010000
......
```

修改主程序的引导优先级

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

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

```
=====================================================
```

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

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

调整后的结果如下：

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

删除启动主程序配置

使用如下命令删除启动主程序配置：

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

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

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

可以如下清空所有启动主程序文件名设置：

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

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

查看多重引导功能相关配置

可以使用以下命令查看多重引导功能相关的配置：

命令	作用
show boot system [**switch all** | *switchid*]	显示设备的启动主程序文件名配置信息。

可以如下显示设备在启动过程中使用的本地 IP 配置信息：

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

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

2.2.33 启动配置文件配置

锐捷的部分产品提供了指定启动配置文件的功能。这类设备的启动配置文件可以存放在本地 Flash 中。

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

以下将描述如何配置和使用指定启动配置文件功能。

设置启动配置文件

锐捷产品提供如下命令设置设备的启动配置文件名：

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

可以使用命令行的帮助信息来查看当前软件版本支持的 URL 前缀，例如：

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

在设备启动时，系统根据如下原则加载配置文件：

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

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

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

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

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

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

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

- 如果该文件所处的设备存在，系统将自动创建指定文件并写入系统配置；
- 如果该文件所处的设备不存在，则系统将询问是否要将当前配置保存于默认启动配置文件“/config”中，并根据用户的回答执行相应的操作。

查看启动配置文件相关配置

可以使用以下命令查看多重引导功能相关的配置：

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

可以如下显示设备当前配置的启动配置文件名：

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

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。

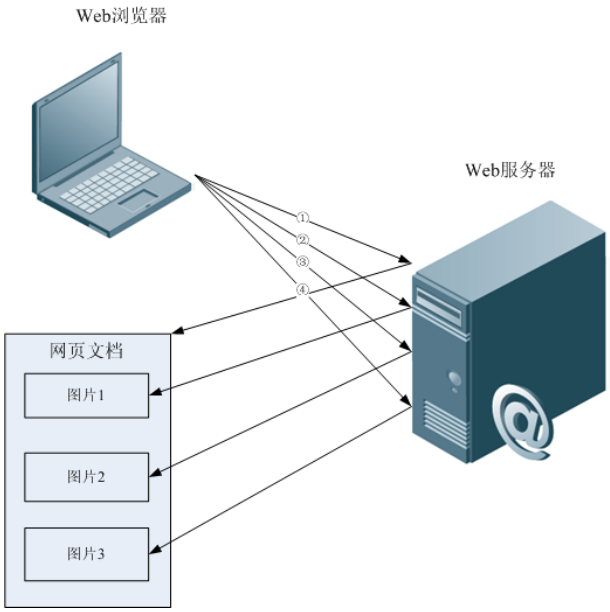
3.1.2 基本概念

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。

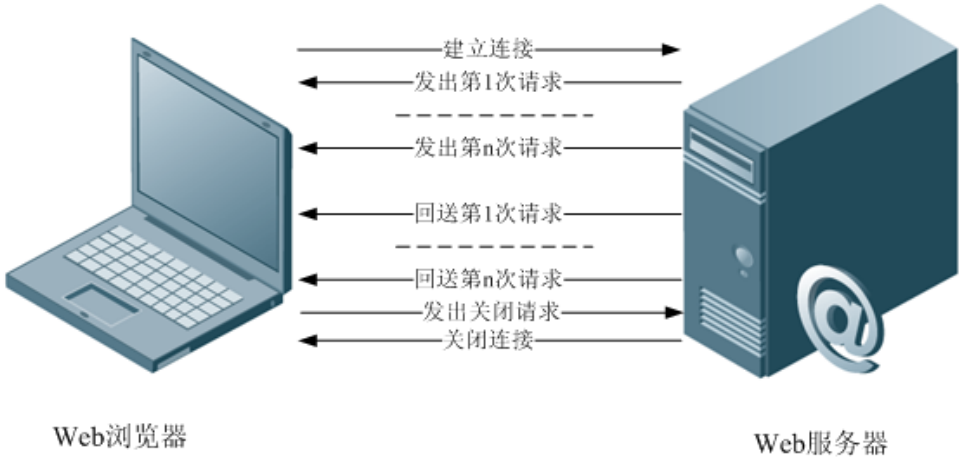
例如一个网页中可能需要很多图片，网页中包括的不是真正的图片内容，而是它们的 URL 连接地址，这样浏览器在访问过程中会发出多次请求，每次请求都要建立一个单独的连接，每次连接都是完全隔离的。建立和释放连接是一个相对费劲的过程，从而严重影响了客户机和服务器的性能，如图 3-1 所示。

图 3-1 HTTP/1.0 协议报文交互



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 3-2 所示。

图 3-2 HTTP/1.1 协议报文交互



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

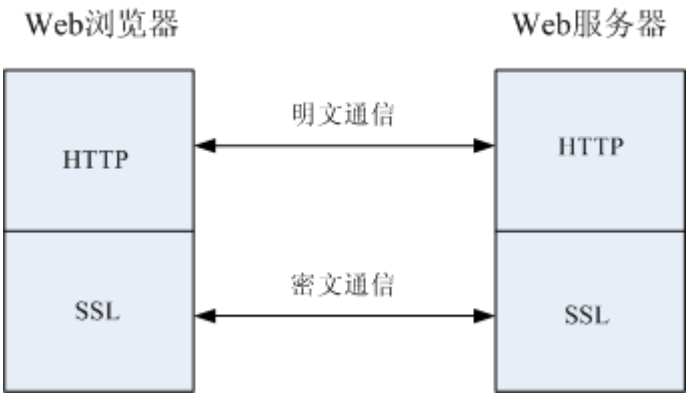
交换机使用哪种协议版本由 Web 浏览器决定。

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。

图 3-3 HTTPS 服务



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

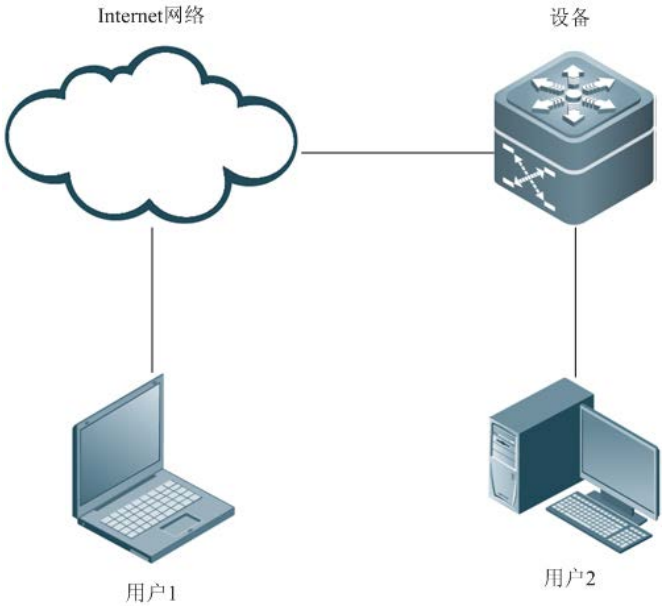
HTTP 应用服务

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陆到 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。

图 3-4 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。

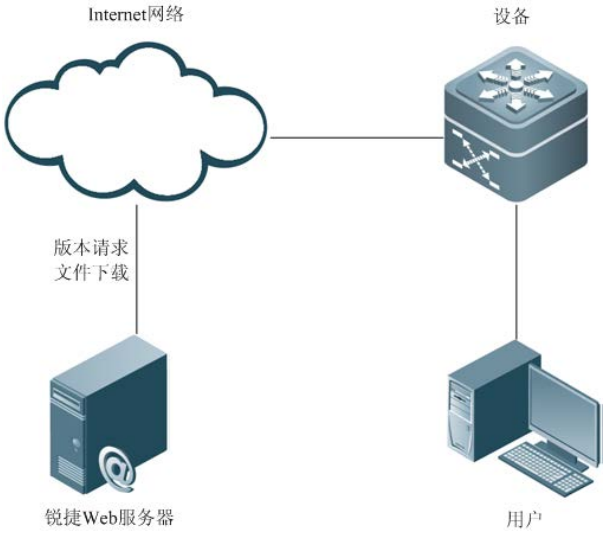
图 3-4 HTTP 应用场景



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 3-5 所示。

图 3-5 HTTP 远程升级



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。

使用 **ip http authentication** 命令配置

命令	作用
Ruijie# **configure terminal**	进入全局配置模式
Ruijie(config)#**ip http authentication { enable | local }**	“可选”；配置登陆认证方式。默认采用 **enable** 认证

如果选择 **enable** 方式，则登陆认证的用户名为空，密码为采用 **enable password** 或 **enable secret** 命令设置的口令。

如果选择 **local** 方式，则采用本地 **username** 命令设置的用户名和口令进行认证。

不管是 **enable** 方式还是 **local** 方式，都要求认证口令是 15 级权限。

配置举例：

例 1：配置在 Ruijie 设备中使用 **local** 方式进行 Web 页面认证。

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

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。

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

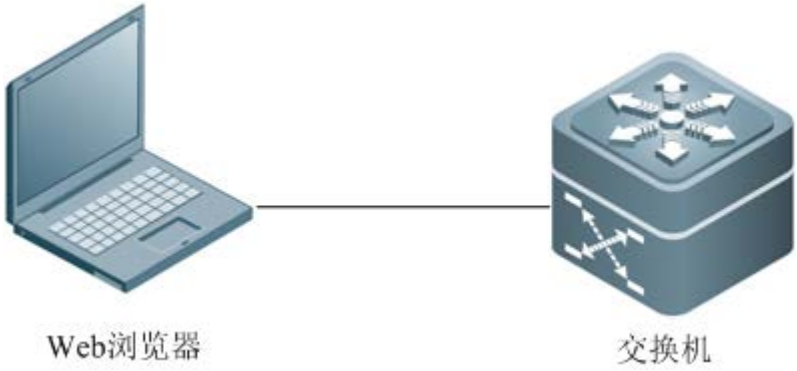
组网需求

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

图 3-6 HTTP 服务应用拓扑



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

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

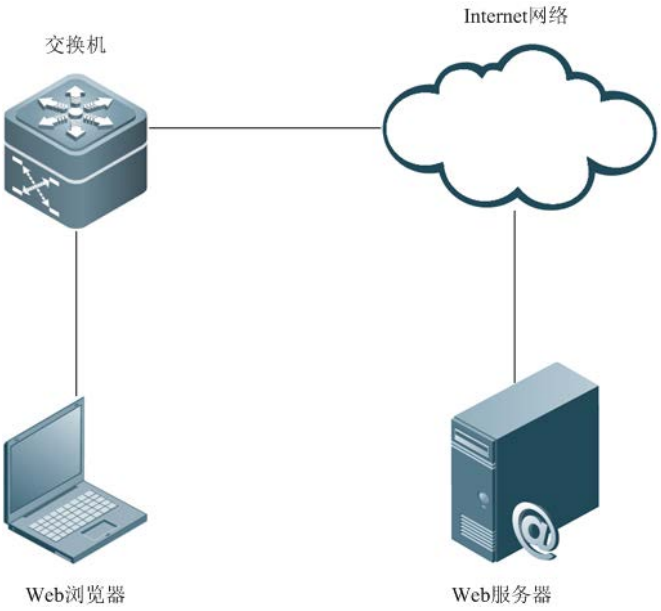
组网需求

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

图 3-7 HTTP 远程升级服务拓扑



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

图 3-8 本地升级服务拓扑

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

1) 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
```

2) 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
```

3) 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 LINE 模式

4.1 LINE模式配置

4.1.1 进入LINE模式

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

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

4.1.2 增加/减少LINE VTY数目

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

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

4.1.3 配置Line下的可通讯协议

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

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

4.1.4 配置Line下的访问控制列表

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

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

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

5 文件系统

5.1 文件系统概述

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

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

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

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

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

5.1.1 使用URL来定位文件

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

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

- 指定服务器上的文件
- 指定本地文件
- URL 的前缀说明

指定服务器上的文件

要指定服务器上的文件，可以使用如下的形式：

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

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

10.4(3)之前的软件版本，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。10.4(3)之后的软件版本，tftp 传输无大小限制。

指定本地文件

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

比如：

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

slave:/rgos.bin 可以表示从设备上根目录上的文件

在指定本地文件时，如果不使用 prefix，则表示当前路径上的文件系统类型。

当使用 prefix 指定本地文件时，“：”后的路径必须是绝对路径。

URL 的前缀说明

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

当前支持的 URL 前缀如下：

前缀	说明
flash:	flash 存储介质。这个前缀在所有设备上都可以使用。出厂时设备的启动主程序都保存在 flash 上。
tftp:	TFTP 网络服务器
xmodem:	使用 xmodem 协议向网络设备收发文件
slave:	机箱式设备中从管理板上的 flash

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

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

Ruijie#copy flash:/rgos.bin ?
  WORD     Copy to current file system
  flash:   Copy to flash file system
  ftp:     Copy to ftp: file system
```

```
  tftp:    Copy to tftp: file system
  xmodem:  Copy to xmodem: file system

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

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

5.1.2 显示文件系统信息

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

在特权用户模式下，使用如下命令：

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

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

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

5.1.3 管理本地设备上的文件

本地文件是指保存在设备上各种存储介质中的文件。例如 flash 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。

本地文件管理可执行如下的操作：□

- 文件复制
- 文件移动
- 文件删除
- 目录创建

- 目录删除
- 目录内容显示
- 当前工作路径显示
- 工作路径更改

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

在 flash、slave 上的文件系统中，文件大小写都是敏感的。例如 abc.txt 和 Abc.txt 是两个不同的文件。在指定文件时必须正确的书写大小写才能正确定位文件。

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。因此，建议在文件系统使用相当时间后，手动清理一些过时的无用文件。

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

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

RCMS 的配置文件（/rcms_config.ini）

Web 管理文件包（/web_management_pack.upd）

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

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

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

5.1.4 通过通信协议传递文件

- 通过 tftp 协议传递文件

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

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

在 CLI 特权模式下，使用如下命令完成文件的上传：

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

- 通过 xmodem 协议传递文件

在特权模式下使用以下命令下载文件到本地；

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

在特权模式下使用以下命令上载文件到服务器；

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

5.1.5 指定TFTP源地址与源接口号

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

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

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

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

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

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

5.2 典型配置举例

5.2.1 从tftp服务器下载文件

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

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

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

3) 登录到设备，进入特权模式，执行以下命令：

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

4) 使用 dir 命令查看设备上的文件

```
Ruijie#dir
Directory of flash:/
    Mode Link      Size               MTime Name
-------- ---- --------- ------------------- ------------------
            1    343040 2009-01-01 02:02:59 a.dat
            1  10838016 2009-01-01 00:08:38 rgos.bin
            1       399 2009-01-01 00:01:37 config.text
```

```
------------------------------------------------------------
3 Files (Total size 11181455 Bytes), 9 Directories.
Total 33030144 bytes (31MB) in this device, 20492288 bytes (19MB) available.
```

5.2.2 上传文件至tftp服务器

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

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

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

3) 登录到设备，进入特权模式，执行以下命令：

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

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

5.2.3 通过xmodem下载文件

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

1) 首先用串口线将 PC 的串口和设备的串口连接起来。

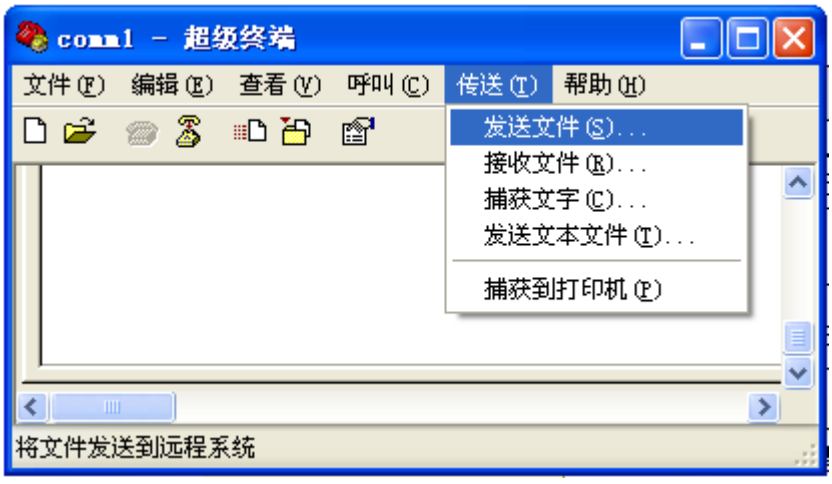
2) 打开 Windows 的超级终端，连接到设备控制台

3) 在特权模式下使用以下命令下载文件

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

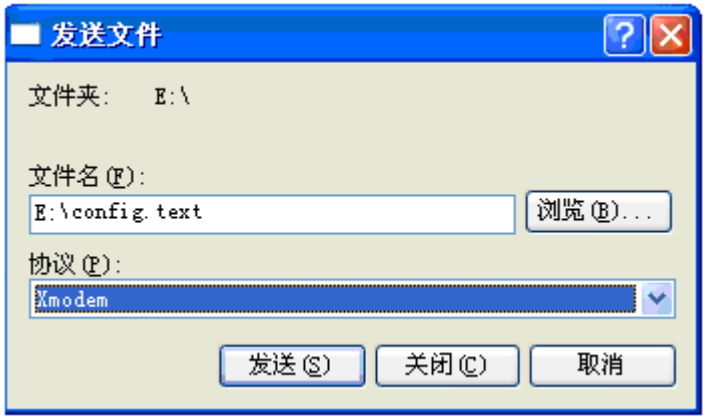
4) 在本地主机的 Windows 超级终端中，选择“传送”菜单中的“发送文件”功能，如下图所示：

图 6-1



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

图 6-2



6) 使用 dir 命令查看设备上的文件

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

5.2.4 通过xmodem上传文件

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

1) 首先用串口线将 PC 的串口和设备的串口连接起来。

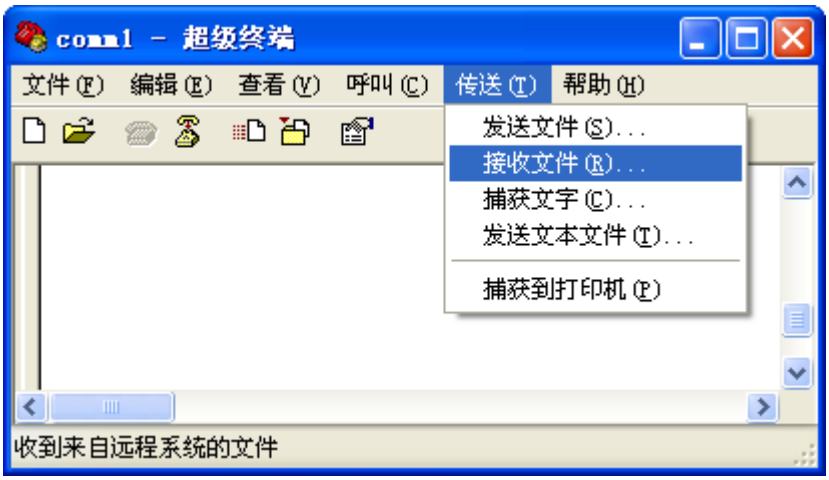
2) 打开 Windows 的超级终端，连接到设备控制台

3) 在特权模式下使用以下命令下载文件

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

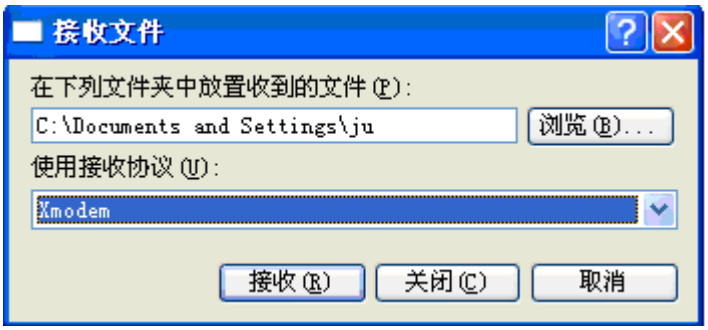
4) 最后在本地主机的 Windows 超级终端中，选择“传送”菜单中的“接收文件”功能。如下图所示：

图 6-3



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

图 6-4



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

5.2.5 删除目录

以下例子说明如何删除一个非空的 aaa 目录：

1) 查看当前目录状况

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

2) 确认 aaa 目录中是否存在文件

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

3) 删除非空目录

```
Ruijie# delete recursive aaa
```

4) 删除空目录

```
Ruijie# rmdir aaa
```

5) 确认目录确实被删除

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

6 配置文件管理

6.1 配置文件管理概述

随着网络的快速发展，网络环境越来越复杂，配置信息越来越多，对网管的要求也越来越高。配置信息的变化可能对整个网络产生不可预知的影响，因此，对配置变化的监控显得尤为重要。目前，只能通过拷贝当前运行配置文件（running-config）和启动配置文件（startup-config）、逐行比较两个文件中命令差异的方式来确定配置是否发生变化。这种方式虽然可以确认配置是否发生变化，但是仍然存在不少缺陷，比如：不能确定配置变化的先后顺序，不能及时通告网管人员，在配置发生变化导致网络出现问题时很难确认相关的责任人等。配置文件管理可以在配置发生变化时发出消息和日志提醒管理人员。

6.1.1 配置文件管理基本特性

配置文件管理包括配置变化时的消息和日志。

配置变化日志

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

6.1.2 工作原理

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

6.2 配置配置变化日志

6.2.1 缺省配置

下表用来描述配置文件管理功能的缺省配置。

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

6.2.2 打开变化日志功能

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

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

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

配置举例：

打开配置变化日志功能

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

6.2.3 指定配置日志中保留的条目最大个数

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

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

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

配置举例：

指定配置日志中保留的条目最大个数为 50。

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

6.2.4 打开密码隐藏功能

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

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

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

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

配置举例：

禁止在配置日志中显示密码信息。

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

6.2.5 打开配置变化通知功能

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

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

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

配置举例：

打开配置变化通知功能。

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

6.2.6 查看配置日志信息

配置变化日志提供了如下命令，用于显示配置日志信息及内存使用情况。

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

6.3 配置文件管理典型配置举例

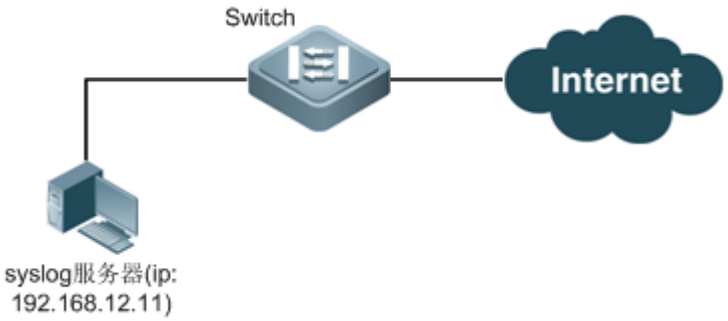
组网需求

为了及时跟踪配置变化情况，假设网管人员有如下要求：

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

组网拓扑

图 7-1 配置变化日志组网图



配置步骤

1) 打开配置变化日志功能

打开配置变化日志功能，以便跟踪配置变化情况

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

2) 设置配置日志中保留的最大条目个数为 1000

设置配置日志中保留的最大条目个数

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

3) 禁止在配置日志中显示密码信息

禁止在配置日志中显示密码信息

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

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

打开允许配置发生变化时通告远端日志服务器的功能

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

配置远端日志服务器

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

显示验证

查看配置日志信息

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

查看配置日志内存使用情况

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

7 系统管理

7.1 配置系统管理

7.1.1 显示系统CPU利用率

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

命令	作用
show cpu	查看系统 CPU 利用率信息

缺省情况下，设备的名称为 Ruijie。

下面举例显示 **show cpu** 运行的结果：

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

21	0%	0%	0%	dhcpa_task
22	0%	0%	0%	dhcpsnp_task
23	0%	0%	0%	igmp_snp
24	0%	0%	0%	mstp_event
25	0%	0%	0%	GVRP_EVENT
26	0%	0%	0%	rldp_task
27	0%	2%	1%	rerp_task
28	0%	0%	0%	reup_event_handler
29	0%	0%	0%	tpp_task
30	0%	0%	0%	ip6timer
31	0%	0%	0%	rtadvd
32	0%	0%	0%	tnet6
33	2%	0%	0%	tnet
34	0%	0%	0%	Tarptime
35	0%	0%	0%	gra_arp
36	0%	0%	0%	Ttcptimer
37	8%	1%	0%	ef_res
38	0%	0%	0%	ef_rcv_msg
39	0%	0%	0%	ef_inconsistent_daemon
40	0%	0%	0%	ip6_tunnel_rcv_pkt
41	0%	0%	0%	res6t
42	0%	0%	0%	tunrt6
43	0%	0%	0%	ef6_rcv_msg
44	0%	0%	0%	ef6_inconsistent_daemon
45	0%	0%	0%	imid
46	0%	0%	0%	nsmd
47	0%	0%	0%	ripd
48	0%	0%	0%	ripngd
49	0%	0%	0%	ospfd
50	0%	0%	0%	ospf6d
51	0%	0%	0%	bgpd
52	0%	0%	0%	pimd
53	0%	0%	0%	pim6d
54	0%	0%	0%	pdmd
55	0%	0%	0%	dvmrpd
56	0%	0%	0%	vty_connect
57	0%	0%	0%	aaa_task
58	0%	0%	0%	Tlogtrap
59	0%	0%	0%	dhcp6c
60	0%	0%	0%	sntp_recv_task
61	0%	0%	0%	ntp_task
62	0%	0%	0%	sla_deamon
63	0%	3%	1%	track_daemon
64	0%	0%	0%	pbr_guard
65	0%	0%	0%	vrrpd

66	0%	0%	0%	psnpd
67	0%	0%	0%	igsnpd
68	0%	0%	0%	coa_recv
69	0%	0%	0%	co_oper
70	0%	0%	0%	co_mac
71	0%	0%	0%	radius_task
72	0%	0%	0%	tac+_acct_task
73	0%	0%	0%	tac+_task
74	0%	0%	0%	dhcpd_task
75	0%	0%	0%	dhcps_task
76	0%	0%	0%	dhcpping_task
77	0%	0%	0%	dhcpc_task
78	0%	0%	0%	uart_debug_file_task
79	0%	0%	0%	ssp_init_task
80	0%	0%	0%	rl_listen
81	0%	0%	0%	ikl_msg_operate_thread
82	0%	0%	0%	bcmDPC
83	0%	0%	0%	bcmL2X.0
84	3%	3%	3%	bcmL2X.0
85	0%	0%	0%	bcmCNTR.0
86	0%	0%	0%	bcmTX
87	0%	0%	0%	bcmXGS3AsyncTX
88	0%	2%	1%	bcmLINK.0
89	0%	0%	0%	bcmRX
90	0%	0%	0%	mngpkt_rcv_thread
91	0%	0%	0%	mngpkt_recycle_thread
92	0%	0%	0%	stack_task
93	0%	0%	0%	stack_disc_task
94	0%	0%	0%	redun_sync_task
95	0%	0%	0%	conf_dispatch_task
96	0%	0%	0%	devprob_task
97	0%	0%	0%	rdp_snd_thread
98	0%	0%	0%	rdp_rcv_thread
99	0%	0%	0%	rdp_slot_change_thread
100	4%	2%	1%	datapkt_rcv_thread
101	0%	0%	0%	keepalive_link_notify
102	0%	0%	0%	rerp_msg_recv_thread
103	0%	0%	0%	ip_scan_guard_task
104	0%	0%	0%	ssp_ipmc_hit_task
105	0%	0%	0%	ssp_ipmc_trap_task
106	0%	0%	0%	hw_err_snd_task
107	0%	0%	0%	rerp_packet_send_task
108	0%	0%	0%	idle_vlan_proc_thread
109	0%	0%	0%	cmic_pause_detect
110	1%	1%	1%	stat_get_and_send

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

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

No：序号

5Sec：每一行表示的任务最近 5 秒钟内的 CPU 利用率

1Min：每一行表示的任务最近 1 分钟内的 CPU 利用率

5Min：每一行表示的任务最近 5 分钟内的 CPU 利用率

Process：任务名称

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

7.1.2 配置CPU利用率日志信息触发门限

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

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

默认情况下该高门限为 100%，低门限为 90%。

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

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

若 CPU 利用率高于 80%将显示如下信息：

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

若 CPU 利用率低于 70%将显示如下信息：

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

8 系统内存状态查看

8.1 基本系统管理

8.1.1 配置任务列表

显示系统内存使用情况。

8.1.2 查看系统内存使用情况

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

命令	作用
show memory	查看系统内存使用情况

缺省情况下，设备的名称为 Ruijie。

下面举例显示 **show memory** 运行的结果：

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

上面列表中的信息包含如下：

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

9 系统日志

9.1 日志概述

NBS200F 系列产品不支持 VSU 功能

设备在运行过程中，会发生各种状态变化如链路状态 UP、DOWN 等，也会遇到一些事件如收到异常报文、处理异常等。锐捷产品日志提供一种机制，在状态变化或发生事件时，就自动生成固定格式的消息（日志报文），这些消息可以被显示在相关窗口（控制台、VTY 等）上或被记录在相关媒介（内存缓冲区、FLASH）上或发送到网络上的一组日志服务器上，供管理员分析网络情况和定位问题。同时为了方便管理员对日志报文的读取和管理，这些日志报文可以被打上时间戳和序号，并按日志信息的优先级进行分级。

锐捷产品的日志报文格式如下：

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

其含义依次是：

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

例子：

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

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

9.2 日志配置

9.2.1 日志开关

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

要打开或关闭日志开关，请在全局配置模式下执行以下命令：

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

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

9.2.2 重定向日志开关

VSU 环境下面，重定向日志开关默认是开启的，从机或备机上面的日志信息不仅可以显示在从机或备机的 Console 窗口上，也可以重定向到主机上面进行输出，包括输出到主机的 Console 窗口、VTY 窗口上，也可以记录在主机的内存缓冲区、扩展 FLASH 和 Syslog Server 上。

要打开或关闭重定向日志开关，请在主机的全局配置模式下执行以下命令：

命令	作用
Ruijie(config)# **logging rd on**	打开重定向日志开关
Ruijie(config)# **no logging rd on**	关闭重定向日志开关

打开重定向日志开关后，从机或备机的日志信息将重定向到主机进行输出，输出时，会在日志信息内容的最前面添加上对应的角色标志串“(*设备号)”，用于标识该日志信息是重定向日志信息，在 VSU 环境下面，假设同时存在四个设备，主机设备号为 1，从机设备号为 2，备机设备号分别为 3 和 4，则主机自身产生的日志不会添加角色标志串，从机重定向到主机的日志将添加角色标志串：(*2)，备机重定向到主机的日志将分别添加角色标志串：(*3)和(*4)。

9.2.3 设置日志信息显示设备

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

要设置接收日志的不同显示设备，请在全局配置模式或特权用户层下执行以下命令：

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

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

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

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

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

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

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

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

9.2.4 启用日志信息时间戳开关

要在日志信息上添加或取消时间戳，请在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)# **service timestamps** [*message-type* [**uptime** | **datetime** [**msec**] [**year**]]]	启用日志信息中的时间戳
Ruijie(config)# **no service timestamps** [*message-type*]	关闭日志信息中的时间戳

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

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

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

9.2.5 启用日志信息系统名开关

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

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

9.2.6 启用标准日志格式显示开关

默认情况下，日志格式中时间戳前面带一个“*”、后面带一个“:”，标识串前面带一个“%”，若想按标准日志格式进行显示，即日志格式中时间戳前面不带“*”，后面不带“:”，请在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)# **service standard-syslog**	开启标准日志格式显示开关。
Ruijie(config)# **no service standard-syslog**	关闭标准日志格式显示开关。

默认情况下，设备上面的日志信息显示格式如下：

*timestamp: %facility-severity-mnemonic: description

依次是：*时间戳：%模块名-严重性级别-助记符信息：详细日志信息

例子如：*May 31 23:25:21: %SYS-5-CONFIG_I: Configured from console by console

若打开标准日志格式显示功能，设备上面的日志信息显示格式如下：

timestamp %facility-severity-mnemonic: description

依次是：时间戳 %模块名-严重性级别-助记符信息：详细日志信息

例子如：May 31 23:31:28 %SYS-5-CONFIG_I: Configured from console by console

其中，标准日志格式与默认日志格式的区别在于时间戳，标准日志格式的时间戳中前面少了一个“*”、后面少了一个“:”

9.2.7 启用私有日志格式显示开关

默认情况下，日志格式中时间戳前面带一个“*”、后面带一个“:”，标识串前面带一个“%”，若想按私有日志格式进行显示，即日志格式中时间戳前面不带“*”、后面不带“:”，标识串前面不带“%”，请在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)# **service private-syslog**	开启私有日志格式显示开关。
Ruijie(config)# **no service private-syslog**	关闭私有日志格式显示开关。

默认情况下，设备上面的日志信息显示格式如下：

*timestamp: %facility-severity-mnemonic: description

依次是：*时间戳：%模块名-严重性级别-助记符信息：详细日志信息

例子如：*May 31 23:25:21: %SYS-5-CONFIG_I: Configured from console by console

若打开私有日志格式显示功能，设备上面的日志信息显示格式如下：

timestamp facility-severity-mnemonic: description

依次是：时间戳 模块名-严重性级别-助记符信息：详细日志信息

例子如：May 31 23:31:28 SYS-5-CONFIG_I: Configured from console by console

其中，私有日志格式与默认日志格式的区别在于时间戳和标识串，私有日志格式的时间戳中前面少了一个“*”、后面少了一个“:”，标识串中前面少了一个“%”

9.2.8 启用日志信息统计功能开关

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

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

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

9.2.9 启用日志信息序列号开关

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

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

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

9.2.10 设置用户输入与日志信息输出同步

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

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

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

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

要设置用户输入与日志信息输出同步，请在线路配置模式下执行以下命令：

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

9.2.11 设置日志信息速率控制

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

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

9.2.12 设置重定向日志信息速率控制

正常情况， VSU 环境下面，从机和备机都不会产生大量的日志信息，为了防止从机或备机上面出现大量日志信息的情况，需要对重定向到主机的日志信息进行速率限制，否则会对系统造成负担，系统默认情况下，限制从机重定向到主机的日志信息每秒最多 200 条。

要修改重定向日志信息的控制速率，请在主机的全局配置模式下执行以下命令：

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

9.2.13 设置日志信息显示级别

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

要设置日志信息显示的级别，请在全局配置模式下执行以下命令：

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

锐捷产品的日志信息分为以下 8 个级别：

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

值越小，级别越高，即 0 级别的信息是最高级别的信息。

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

控制台默认允许显示的日志信息级别为 7。

VTY 窗口默认允许显示的日志信息级别为 7。

默认发送给 Syslog Server 日志信息级别为 6。

默认允许被记录在内存缓冲区的日志信息级别为 7。

默认允许被记录在扩展 FLASH 中日志信息级别为 6。

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

9.2.14 设置日志信息的设备值

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

要设置日志信息的设备值，请在全局配置模式下执行以下命令：

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

下面是各种设备值的含义：

Numerical Code	Facility
0	kernel messages
1	user-level messages
2	mail system
3	system daemons
4	security/authorization messages

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

锐捷产品默认设备值为 23。

9.2.15 设置日志报文的源地址

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

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

要设置日志报文的源地址，请在全局配置模式下执行以下命令：

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

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

9.2.16 设置发送用户LOG信息

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

9.2.17 日志监控

为了监控日志信息，请在特权用户模式下执行以下命令：

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

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

9.3 日志配置举例

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

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

10 设备冗余

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

10.1 设备冗余的NSF概述

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

10.1.1 NSF的优点及限制

NSF 技术的实现可为网络服务提供以下便利：

1) 提高了网络的可用性

NSF 技术在设备转换过程中维持了数据转发及用户会话的状态信息。

2) 避免邻居检测到 link flap

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

3) 避免 routing flaps

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

4) 用户会话(user sessions)不会丢失

在切换前已建立的用户会话由于状态进行了实时同步而不会丢失。

在交换机上使用 NSF 技术需要注意有以下限制：

在主从设备的软硬件构成完全一致的前提下方能保持 NSF 的正常工作；

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

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

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

这些特性（可高用性不兼容功能）不支持高可用，它们的状态数据没有进行同步，在高可用性启用时，这些特性不能使用，否则可能导致系统行为的不正常。

10.1.2 NSF的关键组成技术

实现 NSF 的关键技术包括：

状态同步

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

配置同步

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

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

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

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

自动同步的模式包含以下 3 种：

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

startup-config：同步运行时间的配置文件。

running-config：同步启动配置文件。

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

10.2 NSF配置

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

10.2.1 配置冗余管理

主设备的手动选择

允许您通过 CLI 所提供的命令来选择主从设备；

在特权用户模式下，执行如下命令可以强制切换主设备：

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

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

```
Ruijie# redundancy forceswitch
```

10.2.2 配置同步模式

执行以下命令可以配置需要同步的配置文件。

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

10.2.3 配置心跳检测时间

执行以下命令可以配置主从设备的心跳检测时间。

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

10.2.4 复位设备

执行以下命令可以指定复位指定设备

命令	作用
Ruijie> **enable**	进行特权配置模式

11 SRM

11.1 SRM概述

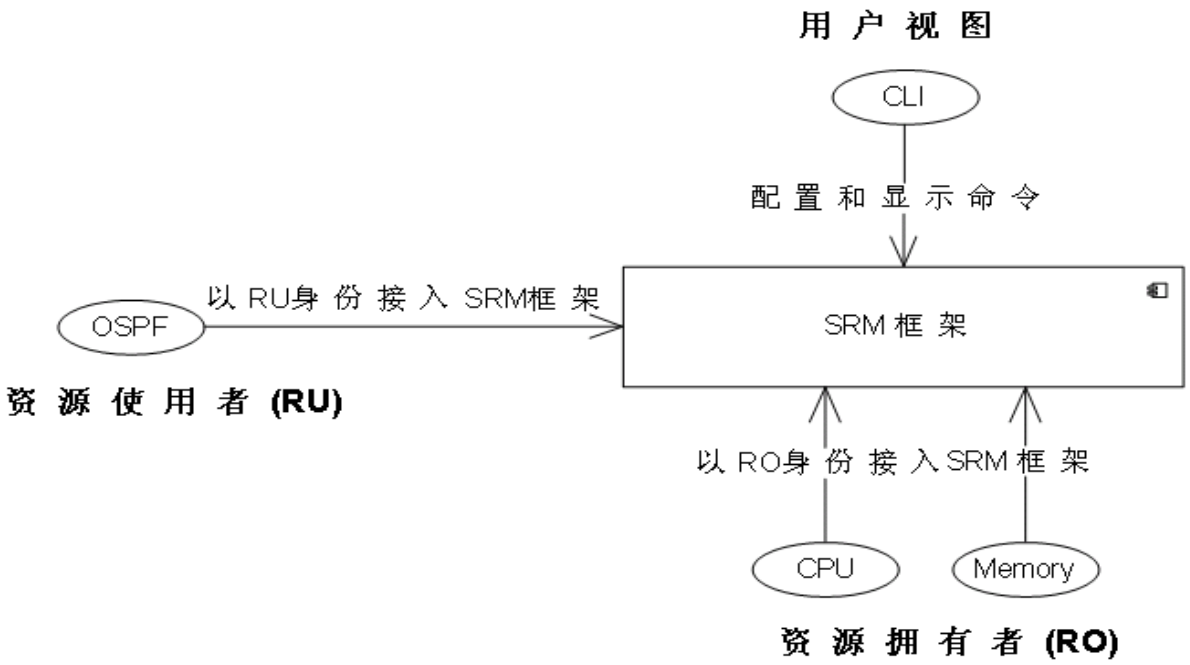
SRM（System Resources Manager，系统资源管理）用于监控嵌入式系统中有限内部资源的使用情况。通过对监控信息的分析，网管人员能够对设备的运行状态有更加全面的了解，对系统性能可以有更准确的衡量，并据此采取相应措施以提升可用性。

SRM 主要包括统计和监控功能：

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

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

图 13-1 SRM 构架



11.1.1 基本概念

资源使用者

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

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

资源拥有者

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

当前，RO 包括 cpu 和 memory 这两类资源。

SRM 框架

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

RU 组

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

SRM 中存在以下三类 RU 组：

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

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

策略

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

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

策略分为两种：

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

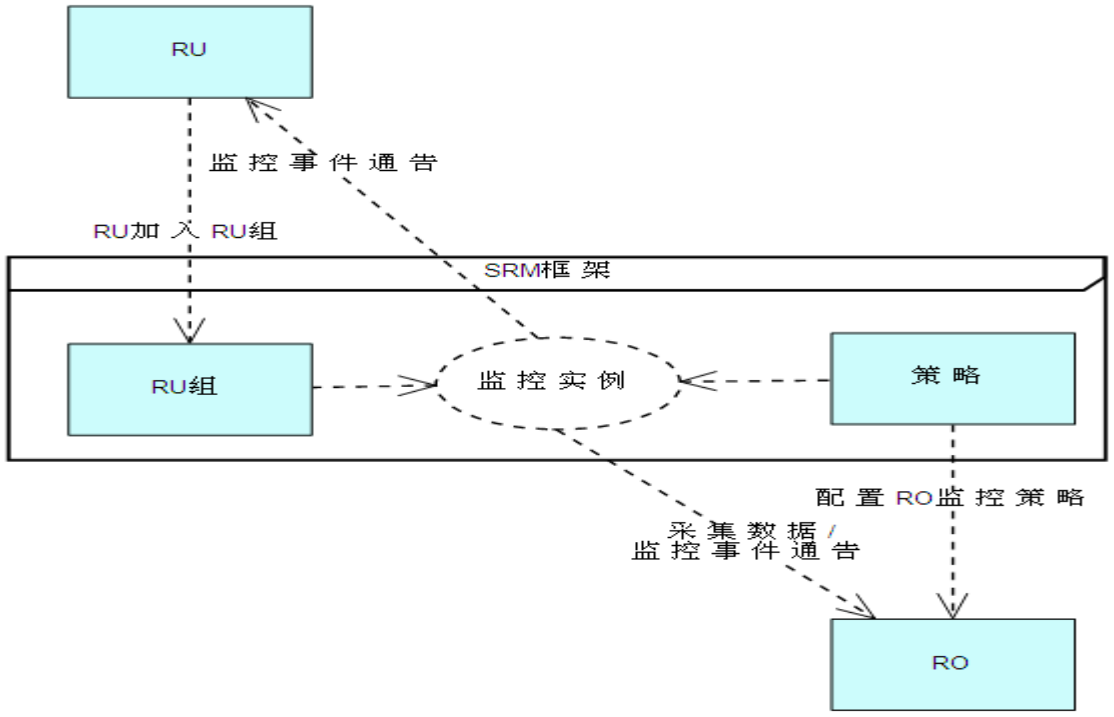
水线

水线包含如下属性：

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

11.1.2 工作原理

图 13-2 工作原理



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

11.2 配置SRM

以下章节描述如何配置 SRM 特性：

- （必选）配置策略

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

11.2.1 配置监控策略

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

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

配置举例：

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

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

11.2.2 应用监控策略

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

配置举例：

#配置一个名为 rgos_policy 的全局策略，并应用到全局组上。

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

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

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

#对 Group 应用 policy 的方式参见“配置 RU 组。

11.2.3 配置RU组

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

配置举例：

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

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

11.2.4 查看SRM配置与状态

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

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

11.3 SRM典型配置举例

组网需求

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

配置步骤

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

#配置一个全局策略对内存的使用进行监控

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

配置一个用户策略并应用到 snmpd。

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

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

配置策略和组，并关联

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

显示验证

1) 查看 SRM 数据库信息

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

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

2) 查看监控事件通告统计

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

3) 查看 RO 信息

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

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

4) 查看策略信息

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

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

5) 查看关联信息

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

6) 查看 RU 信息

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

12 硬件表项容量

12.1 概述

为了灵活应用硬件表项资源，以满足不同业务场景需求，提供了硬件容量配置功能。

12.2 配置硬件表项容量

用户可以自行指定如下几种硬件表项的最大条目数。系统自动换算得到 IPv4 单播路由的最大条目数。

- 共享池（shared-pool）最大数目
- 单播路由最大数目

以上配置，需保存，并重启设备后才会生效。

12.2.1 配置共享池最大数目

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

12.2.2 配置单播路由最大数目

命令	作用
Ruijie(config)# **initialization route unicast** *max-num*	设置单播路由最大数目，缺省值 130。
Ruijie(config)# **no initialization route unicast**	恢复为缺省配置
Ruijie(config)# **initialization route unicast** ？	查看当前允许配置的最大数目合法值

12.3 查看硬件表项容量

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

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

命令输出信息如下：

```
Ruijie #show initialization route

                            config  running  default
 unicast route entry:       130     130      130
 shared-pool entry:         1024    1024     1024
```

配置指南-以太网交换

本分册介绍以太网交换配置指南相关内容，包括以下章节：

1. 接口
2. MAC 地址
3. Aggregate Port
4. 链路聚合控制协议（LACP）
5. VLAN
6. Private VLAN
7. Voice VLAN
8. RSTP
9. 配置协议帧透传
10. GVRP
11. LLDP

1 接口

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

- 二层接口(L2 interface)
- 三层接口(L3 interface) (三层设备支持)

1.1 二层接口(L2 interface)

本节主要描述二层接口的类型及相关的定义，可分为以下几种类型

- Switch Port
- L2 Aggregate Port

1.1.1 Switch Port

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

Access Port

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

- 缺省 VLAN

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

- 帧的接收与发送

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

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

Trunk Port

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

■ 缺省 VLAN

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

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

■ 帧的接收与发送

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

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

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

Hybrid 端口

Hybrid 类型的端口可以属于多个 VLAN，可以接收和发送多个 VLAN 的报文，可以用于设备之间连接，也可以用于连接用户的计算机。Hybrid 端口和 Trunk 端口的不同之处在于 Hybrid 端口可以允许多个 VLAN 的报文发送时不打标签，而 Trunk 端口只允许缺省 VLAN 的报文发送时不打标签，需要注意的是：Hybrid 端口加入的 VLAN 必须已经存在。

1.1.2 L2 Aggregate Port

Aggregate port 是由多个物理成员端口聚合而成的。我们可以把多个物理链接捆绑在一起形成一个简单的逻辑链接，这个逻辑链接我们称之为一个 Aggregate Port（以下简称 AP ）。

对于二层交换来说 AP 就好像一个高带宽的 Switch port，它可以把多个端口的带宽叠加起来使用，扩展了链路带宽。此外，通过 L2 Aggregate port 发送的帧还将在 L2 Aggregate port 的成员端口上进行流量平衡，如果 AP 中的一条成员链路失效，L2 Aggregate port 会自动将这个链路上的流量转移到其他有效的成员链路上，提高了连接的可靠性。

L2 Aggregate Port 的成员端口类型可以为 Access port 或 Trunk Port，但同一个 AP 的成员端口必须为同一类型，要么全是 Access Port，要么全是 Trunk port。

1.2 三层接口(L3 interface)

本节主要描述三层接口的类型及相关的定义，可分为以下几种类型

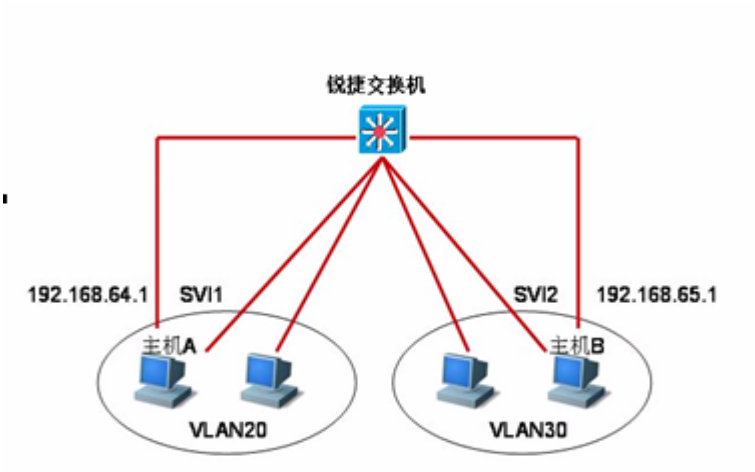
- SVI (Switch virtual interface)
- Routed Port
- L3 Aggregate Port

1.2.1 SVI

SVI(Switch virtual interface，交换虚拟接口)，用来实现三层交换的逻辑接口。SVI 可以做为本机的管理接口，通过该管理接口管理员可管理设备。您也可以创建 SVI 为一个网关接口，就相当于是对应各个 VLAN 的虚拟的子接口，可用于三层设备中跨 VLAN 之间的路由。创建一个 SVI 很简单，您可通过 **interface vlan** 接口配置命令来创建 SVI，然后给 SVI 分配 IP 地址来建立 VLAN 之间的路由。

如图所示，VLAN20 的主机可直接互相通讯，无需通过三层设备的路由，若 VLAN20 内的主机 A 想和 VLAN30 内的主机 B 通讯必须通过 VLAN20 对应的 SVI1 和 VLAN30 对应的 SVI2 才能实现。

图 1-1



1.2.2 Routed Port

一个 Routed Port 是一个物理端口，就如同三层设备上的一个端口，能用一个三层路由协议配置。在三层设备上，可以把单个物理端口设置为 Routed port，作为三层交换的网关接口。一个 Routed Port 与一个特定的 Vlan 没有关系，而是作为一个访问端口。Routed port 不具备二层交换的功能。您可通过 **no switchport** 命令将一个二层接口 Switch port 转变为 Routed port,然后给 Routed port 分配 IP 地址来建立路由。注意的是，当使用 **no switchport** 接口配置命令时，该端口关闭并重启，将删除该端口的所有二层特性。

当一个端口是 L2 Aggregate Port 的成员端口或者是未认证成功的 DOT1X 认证口时，是不能用 **switchport/ no switchport** 命令进行层次切换的。

1.3 配置接口

1.3.1 缺省配置

属性	缺省设置
工作模式	二层交换模式
Switch port 模式	access port
允许的 VLAN 范围	VLAN 1～4094
缺省 VLAN（对于 access port 而言）	VLAN 1
Native VLAN（对于 trunk port 而言）	VLAN 1
介质类型	copper
接口管理状态	Up
接口描述	空
速度	自协商
双工模式	自协商
流控	关闭
Aggregate port	无
风暴控制	关闭
保护端口	关闭

1.3.2 接口编号规则

对于 Switch Port，其编号由两个部分组成：插槽号，端口在插槽上的编号。例如端口所在的插槽编号为 2，端口在插槽上的编号为 3，则端口对应的接口编号为 2/3。插槽的编号是从 0－插槽的个数。插槽的编号规则是：面对设备的面板，插槽按照从前至后，从左至右，从上至下的顺序一次排列，对应的插槽号从 1 开始依次增加。插槽上的端口编号是从 1－插槽上的端口数，编号顺序是从左到右。对于可以选择介质类型的设备，端口包括两种介质（光口和电口），无论使用那种介质，都使用相同的端口编号。您也可以通过命令行中的 show 命令来查看插槽以及插槽上的端口信息。

- 对于 Aggregate Port，其编号的范围为 1－设备支持的 Aggregate Port 个数。
- 对于 SVI，其编号就是这个 SVI 对应的 VLAN 的 VID。

设备上的静态插槽的编号固定为 0，而动态插槽(可插拔模块或线卡)的编号从 1 开始。

1.3.3 接口配置命令的使用

您可在全局配置模式下使用 interface 命令进入接口配置模式。

命令	作用
Ruijie(config)# **interface** interface-id	在全局配置模式下输入 interface 命令，进入接口配置模式。用户也可以在全局配置模式下使用 interface range 或 interface range macro 命令配置一定范围的接口。但是定义在一个范围内的接口必须是相同类型和具有相同特性的

下例给出了进入 Gigabitethernet 2/1 接口的示例：

```
Ruijie(config)# interface gigabitethernet 2/1
Ruijie(config-if)#
```

在接口配置模式下您可配置接口的相关属性。

1.3.4 配置一定范围的接口

用户可以使用全局配置模式下的 **interface range** 命令同时配置多个接口。当进入 **interface range** 配置模式时，此时设置的属性适用于所选范围内的所有接口。

命令	作用
Ruijie(config)# **interface range** {*port-range* | **macro** *macro_name*}	输入一定范围的接口。 **interface range** 命令可以指定若干范围段。 macro 参数可以使用范围段的宏定义，参见配置和使用端口范围的宏定义。 每个范围段可以使用逗号（,）隔开。 同一条命令中的所有范围段中的接口必须属于相同类型。

当使用 **interface range** 命令时，请注意 range 参数的格式：

有效的接口范围格式：

- **vlan** *vlan-ID - vlan-ID*, VLAN ID 范围 1～4094；
- **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 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)#
```

配置和使用端口范围的宏定义

用户可以自行定义一些宏来取代端口范围的输入。但在用户使用 **interface range** 命令中的 **macro** 关键字之前，必须先在全局配置模式下使用 **define interface-range** 命令定义这些宏。

命令	作用
Ruijie(config)# **define interface-range** *macro_name interface-range*	定义接口范围的宏定义。 macro_name－宏定义的名字，不超过 32 个字符。 宏定义的内部可以包括多个范围段。 同一宏定义中的所有范围段中的接口必须属于相同类型。
Ruijie(config)# **interface range macro** *macro_name*	宏定义的字符串将被保存在内存中，使用 **interface range** 命令时，可以使用宏定义的名字来取代需要输入的表示接口范围的字符串。

在全局配置模式下使用 no define interface-range macro_name 命令来删除设置的宏定义。

当使用 define interface-range 命令来定义接口范围时，注意：

有效的接口范围格式：

- **vlan** *vlan-ID* - *vlan-ID*, VLAN ID 范围 1～4094；
- **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
```

1.3.5 选择接口介质类型

有些接口，可以有多种介质类型供用户选择。您可以选择其中一种介质使用。一旦您选定介质类型，接口的连接状态、速度、双工、流控等属性都是指该介质类型的属性，如果您改变介质类型，新选介质类型的这些属性将使用默认值，您可以根据需要重新设定这些属性。

有多种介质类型的接口支持接口介质自动选择。如果您配置接口介质自动选择，在接口只有一种介质连接上时，设备使用当前连接的介质；在接口的两种介质都连接上时，设备将使用您配置的优先介质。介质自动选择优先介质默认为电口，您可以通过配置 medium-type auto-select prefer fiber 来设置优先介质为光口。在自动选择模式下，接口的速度、双工、流控等属性将使用默认值。

配置为介质自动选择的端口，对方端口需要设置为自动协商，不能 disable，否则会出现介质切换错误。

此配置命令只对物理端口有效。Aggregate Port 和 SVI 接口不支持介质类型设置。

此配置命令只对支持介质选择的端口有效。

配置为 Aggregate Port 成员口的端口，其介质类型必须一致，否则无法加入到 AP 中。Aggregate Port 成员口的端口类型不能改变。配置为介质自动选择的接口不能加入 AP。

命令	作用
Ruijie(config-if)# **medium-type { auto-select [prefer [fiber | copper]] | fiber | copper }**	设置端口的介质类型

下面的例子显示了如何设置接口 Gigabitethernet 1/1 的介质类型：

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# medium-type fiber
Ruijie(config-if)# end
```

接口介质切换功能不支持百兆光模块。

1.3.6 配置接口的描述和管理状态

为了有助于您记住一个接口的功能，您可以为一个接口起一个专门的名字来标识这个接口，也就是接口的描述(Description)。您可以根据要表达的含义来设置接口的具体名称，比如，您想将 Gigabitethernet 1/1 分配给用户 A 专门使用，您就可以将这个接口的描述设置为“Port for User A”。

命令	作用
Ruijie(config-if)# **description** *string*	设置接口的描述，最多 32 个字符。

下面的例子显示了如何设置接口 Gigabitethernet 1/1 的描述：

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# description PortForUser A
Ruijie(config-if)# end
```

在某些情况下，您可能需要禁用某个接口。您可以通过设置接口的管理状态来直接关闭一个接口。如果关闭一个接口，则这个接口上将不会接收和发送任何帧，这个接口将丧失这个接口对应的所有功能。您也可以通过设置管理状态来重新打开一个已经关闭的接口。接口的管理状态有两种：Up 和 Down，当端口被关闭时，端口的管理状态为 down，否则为 up。

命令	作用
Ruijie(config-if)# **shutdown**	关闭一个接口

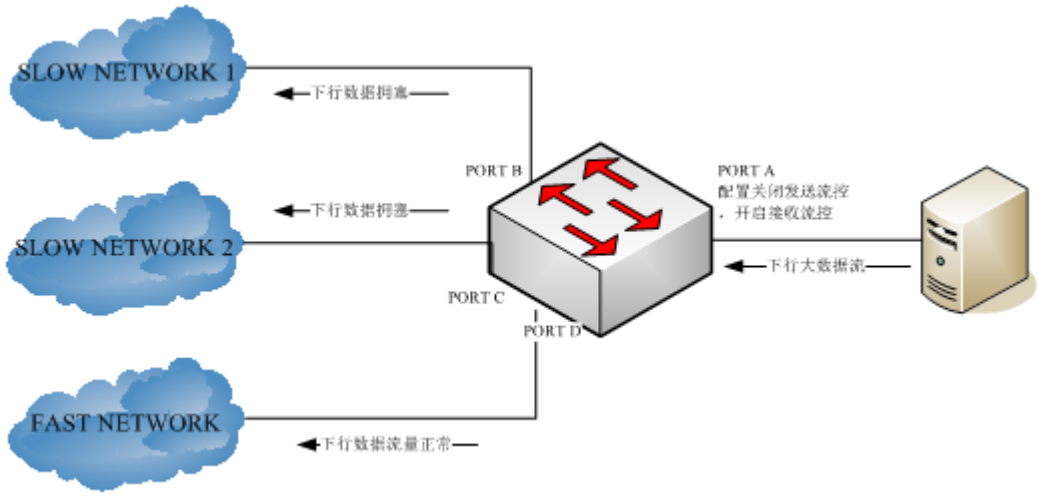
下面的例子描述如何关闭接口 Gigabitethernet 1/2：

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitethernet 1/2
Ruijie(config-if)# shutdown
Ruijie(config-if)# end
```

1.3.7 配置接口的速度，双工，流控

本节描述如何配置接口的速率、双工和流控模式。流控模式分为非对称流控模式和对称流控模式。在一般情况下，接口开启流控模式后，接口上将会处理接收到的流控帧，并在接口出现拥塞时发送流控帧，接收，发送流控帧的处理是一致的，这就是对称流控模式。但是，在一些情况下，设备希望某个接口能够处理接收到的流控帧保证报文不会因为拥塞而丢弃，又不想发出流控帧而导致整个网络速率下降，这个时候，就要通过配置非对称流控，将接收流控帧和发送流控帧的处理步调分开。如图所示：设备的端口 A 为上联口，端口 B-D 为下联端口，其中端口 B 和 C 对应的是一个慢速网络，假如端口 A 上开启了接收流控和发送流控功能，由于端口 B 和 C 对应的是一个慢速网络，在发送端口 B 的数据流过大，导致端口 B 和 C 拥塞，进而导致端口 A 上的入口拥塞，端口 A 上就会发送流控帧，当上联设备响应流控帧时，就会降低往端口 A 的数据流，间接导致端口 D 上的网速下降。这个时候，可以配置端口 A 的发送流控功能关闭，来保障整个网络带宽利用率。

图 1-2



以下配置命令只对 Switch Port,Routed Port 有效。

命令	作用
Ruijie(config-if)# **speed** {**10** | **100** | **1000** | **auto** }	设置接口的速率参数，或者设置为 auto。 1000 只对千兆口有效;
Ruijie(config-if)# **duplex** {**auto** | **full** | **half** }	设置接口的双工模式。 设备光口支持半双工设置。
Ruijie(config-if)# **flowcontrol** {**auto** | **on** | **off** }	设置接口的流控模式。 当 speed,duplex,flowcontrol 都设为非 auto 模式时，该接口关闭自协商过程
Ruijie(config-if)# **flowcontrol** {**receive** | **send**} {**auto** | **on** | **off**}	支持非对称流控设备设置非对称流控模式。 当 receive 和 send 模式设置一致时，将同该模式下的 flowcontrol 命令，并显示为同模式下的 flowcontrol 命令

在接口配置模式下使用 **no speed** ， **no duplex** 和 **no flowcontrol** 命令，将接口的速率、双工和流控配置恢复为缺省值（自协商）。下面的例子显示如何将 Gigabitethernet 1/1 的速率设为 1000M，双工模式设为全双工，流控关闭：

```
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)# end
```

1.3.8 配置接口的MTU

当端口进行大吞吐量数据交换时，可能会遇到大于以太网标准帧长度的帧，这种帧被称为 jumbo 帧。用户可以通过设置端口的 MTU 来控制该端口允许收发的最大帧长。

MTU 是指帧中有效数据段的长度，不包括以太网封装的开销。

端口收到或者转发的帧，如果长度超过设置的 MTU，将被丢弃。

MTU 允许设置的范围为 64~9216 字节，粒度为 4 字节，缺省为 1500 字节。

此配置命令只对物理端口有效。SVI 接口暂时不支持 MTU 设置。

命令	作用
Ruijie(config-if)# **mtu** *num*	设置端口的 MTU Num：<64-9216>

下面的例子显示了如何设置接口 Gigabitethernet 1/1 的 MTU：

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# mtu 64
Ruijie(config-if)# end
```

☑ NMX 系列产品的 MTU 是固定的，最大为 1532 字节(UNTAG，包含 FCS，如果是 TAG 报文，最大 1536 字节)，手工配置无效；

1.3.9 配置access/trunk port

本节主要讲述配置 Switchport 的操作模式(access/trunk port)及每种模式下的相关配置。

您可在接口配置模式下通过 **switchport** 或其他命令来配置 Switch Port 的相关属性：

命令	作用
Ruijie(config-if)# **switchport mode {access | trunk }**	配置接口的操作模式。

下例显示如何配置 gigabitethernet 1/2 的操作模式为 access port。

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitethernet 1/2
Ruijie(config-if)# switchport mode access
Ruijie(config-if)# end
```

命令	作用

Ruijie(config-if)# **switchport access vlan** *vlan-id*	配置 access port 所属的 VLAN。

下例显示如何配置 access port gigabitethernet 2/1 所属 vlan 为 100。

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitethernet 2/1
Ruijie(config-if)# switchport access vlan 100
Ruijie(config-if)# end
```

配置 trunk port 的 native VLAN

命令	作用
Ruijie(config-if)# **switchport trunk native vlan** *vlan-id*	配置 trunk port 的 NATIVE VLAN。

下例显示如何配置 Trunk Port Gigabitethernet 2/1 的 Native vlan 为 10。

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitethernet 2/1
Ruijie(config-if)# switchport trunk native vlan 10
Ruijie(config-if)# end
```

配置接口的速度，双工，流控请参照“配置接口的速度，双工，流控”。

1.3.10 配置Hybrid端口

您可以通过以下步骤配置 Hybrid 端口：

命令	作用
configure terminal	进入配置模式
interface *interface-id*	进入接口配置模式 百兆,千兆，万兆
switchport mode hybrid	配置为端口为 hybrid 口
no switchport mode	删除端口模式
switchport hybrid native vlan *id*	设置 hybrid 口的默认 VLAN
switchport hybrid allowed vlan [[add] [tagged | untaged]] |remove] vlist	设置端口的输出规则

配置举例：

```
Ruijie# configure terminal
Ruijie(config)# interface g 0/1
Ruijie(config-if)# switchport mode hybrid
Ruijie(config-if)# switchport hybrid native vlan 3
Ruijie(config-if)# switchport hybrid allowed vlan untagged 20-30
Ruijie(config-if)# end
```

```
Ruijie# show running interface g 0/1
```

1.3.11 配置L2 Aggregate Port

本节主要讲述如何创建 L2 Aggregate Port 及和 L2 Aggregate Port 相关的一些配置。

您可以在接口配置模式下使用 **aggregateport** 来创建 L2 Aggregate Port，具体的配置过程请参照“配置 Aggregate Port”。

1.3.12 配置三层接口

配置三层接口：

命令	作用
Ruijie(config-if)# **no switchport**	将该接口 Shut Down 并且重新转换成三层模式。该命令只适用于 Switch Port 和 L2 Aggregrate port。
Ruijie(config-if)# **ip address** *ip_address subnet_mask* {[**secondary** | **tertiary** | **quartus**][**broadcast**]}	配置 IP 地址和子网掩码。

删除一个三层接口的 IP 地址可以使用接口配置模式的 **no ip address** 命令。

一个 L2 Aggregate Port 的成员口，不能进行 **no switchport** 操作。

下面的例子是描述如何将一个二层接口配置成 Routed Port，并且给该接口分配 IP 地址：

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitethernet 2/1
Ruijie(config-if)# no switchport
Ruijie(config-if)# ip address 192.20.135.21 255.255.255.0
Ruijie(config-if)# no shutdown
Ruijie(config-if)# end
```

1.3.13 配置SVI

本节主要描述如何创建 SVI 及和 SVI 的一些相关配置。

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

命令	作用
Ruijie(config)# **interface vlan** *vlan-id*	进入 SVI 接口配置模式。

然后可对 SVI 的相关属性进行配置，详细的信息请参考“配置 IP 单址路由”。

下面的例子显示如何进入接口配置模式，并且给 SVI 100 分配 IP 地址：

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface vlan 100
Ruijie(config-if)# ip address 192.168.1.1 255.255.255.0
Ruijie(config-if)# end
```

1.3.14 配置Routed port

本节描述如何创建 Routed Port 及和 Routed Port 的一些相关配置。

您可在接口模式下，进入某个接口后，使用 **no switchport** 来创建 Routed port。

创建一个 Routed port 并给该 Routed port 分配 IP 地址：

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

当一个接口是 L2 Aggregate Port 的成员口时，是不能用 **switchport/ no switchport** 命令进行层次切换的。

下面的例子显示如何将一个二层接口配置成 Routed Port，并且给该接口分配 IP 地址：

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface fastethernet 1/6
Ruijie(config-if)# no switchport
Ruijie(config-if)# ip address 192.168.1.1 255.255.255.0
Ruijie(config-if)# no shutdown
Ruijie(config-if)# end
```

1.3.15 清除接口的统计值并复位该接口

在特权模式下您可通过 **clear** 命令清除接口的统计值并复位该接口。该命令只对 Switch Port,L2 Aggregrate port 的成员端口,Routed port,L3 Aggregate port 的成员端口有效，以下为 clear 命令：

命令	作用
Ruijie# **clear counters** [*interface-id*]	清除接口统计值。
Ruijie# **clear interrface** *interface-id*	接口硬件复位

接口的统计值可以通过特权模式命令 **show interfaces** 查看，在特权模式下使用 **clear counters** 命令，可以将接口的统计值清零。如果不指定接口，则将所有的 L2 接口计数器清零。

下面的例子显示如何清除 Gigabitethernet 1/1 的计数器：

```
Ruijie# clear counters gigabitethernet 1/1
```

☑ NMX 系列产品的 oversize 对超过 1518 字节的报文计数，对超出 1518 字节不大于 1532(UNTAG，包含 FCS,如果是 TAG 报文，不大于 1536)字节的报文，正常转发，对超出 1532(UNTAG，包含 FCS，如果是 TAG 报文，超出 1536)字节的报文丢弃。

1.3.16 显示接口配置和状态

本节描述接口的显示内容，显示实例。您可在特权模式下通过 **show** 命令可来查看接口状态。在特权模式下您可使用以下命令显示接口状态：

命令	作用
Ruijie# **show interfaces** [*interface-id*]	显示指定接口的全部状态和配置信息。
Ruijie# **show interfaces** [*interface-id*] **status**	显示接口的状态。
Ruijie# **show interfaces** [*interface-id*] **switchport**	显示可交换接口（非路由接口）的 administrative 和 operational 状态信息。
Ruijie# **show interfaces** [*interface-id*] **description**	显示指定接口的描述配置和接口状态。
Ruijie# **show interfaces** [*interface-id*] **counters**	显示指定端口的统计值信息，其中速率显示可能有 0.5%内的误差。
Ruijie# **show interfaces** [*interface-id*] **mtu**	显示接口的 MTU 值。
Ruijie# **show interfaces** [*interface-id*] **usage**	显示接口的带宽利用率。
Ruijie# **show interfaces counters vlan** *vlan-id*	显示指定 VLAN 下的成员口的报文统计信息。
Ruijie# **show interfaces counters module** *module-id*	显示指定模块上所有端口的报文统计信息。
Ruijie# **show interfaces counters nonzero**	显示所有报文统计值为非零的端口的报文统计信息。
Ruijie# **show interfaces status vlan** *vlan-id*	显示指定 VLAN 下的成员口的端口状态信息。
Ruijie# **show interfaces status module** *module-id*	显示指定模块上所有端口的端口状态信息。

以下例子为显示接口 Gigabitethernet 1/1 的接口状态：

```
SwitchA#show interfaces gigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is DOWN  , line protocol is DOWN
Hardware is Broadcom 5464 GigabitEthernet
Interface address is: no ip address
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Bridge, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  RXload is 1 ,Txload is 1
  Queueing strategy: FIFO
    Output queue 0/0, 0 drops;
    Input queue 0/75, 0 drops
  Switchport attributes:
    interface's description:""
    medium-type is copper
```

```
    lastchange time:0 Day: 0 Hour: 0 Minute:13 Second
    Priority is 0
    admin duplex mode is AUTO, oper duplex is Unknown
    admin speed is AUTO, oper speed is Unknown
    flow receive control admin status is OFF,flow send control admin status is OFF,flow receive control
oper status is Unknown,flow send control oper status is Unknown
broadcast Storm Control is OFF,multicast Storm Control is OFF,unicast Storm Control is OFF
 Port-type: trunk
   Native vlan:1
Allowed vlan lists:1-4094                  //Trunk 口的许可 VLAN 列表
Active vlan lists:1, 3-4  //实际生效的 vlan（即该设备上仅创建了 VLAN1、3 和 4）
  5 minutes input rate 0 bits/sec, 0 packets/sec
  5 minutes output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer, 0 dropped
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    0 packets output, 0 bytes, 0 underruns , 0 dropped
0 output errors, 0 collisions, 0 interface resets
```

以下例子为显示接口 Aggregate Port 3 的接口状态：

```
Ruijie# show interfaces aggregateport 3
Interface   : AggreatePort 3
Description :
AdminStatus : up
OperStatus  : down
Hardware    : -
Mtu         : 1500
LastChange  : 0d:0h:0m:0s
AdminDuplex : Auto
OperDuplex  : Unknown
AdminSpeed  : Auto
OperSpeed   : Unknown
FlowControlAdminStatus : Autonego
FlowControlOperStatus  : Disabled
Priority    : 0
```

以下例子显示接口 GigabitEthernet 1/1 的接口配置信息：

```
Ruijie# show interfaces gigabitEthernet 1/1 switchport
Interface  Switchport Mode      Access    Native    Protected VLAN lists
---------- ---------- --------- --------- --------- --------- ------------
gigabitethernet 1/1      Enabled  Access      1         1         Enabled   All
```

以下例子为显示接口 Gigabitethernet 2/1 的接口描述：

```
Ruijie# show interfaces gigabitethernet 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
```

以下例子为显示指定端口 GigabitEthernet 0/1 的 MTU 值：

```
Ruijie# show interfaces gigabitethernet 0/1 mtu
Interface                        MTU
-------------------------------- ------
GigabitEthernet 0/1              1500
```

以下例子为显示端口的 MTU 值(仅显示其中部分端口的信息，未显示出全部端口信息)：

```
Ruijie# show interfaces mtu
Interface                        MTU
-------------------------------- ------
GigabitEthernet 1/0/1            1500
GigabitEthernet 1/0/2            1500
```

```
GigabitEthernet 1/0/3            1500
GigabitEthernet 1/0/4            1500
GigabitEthernet 1/0/5            1500
```

以下例子为显示指定端口 GigabitEthernet 0/1 的带宽利用率值：

```
Ruijie# show interfaces gigabitethernet 0/1 usage
Interface                        Bandwidth     Bandwidth Usage
-------------------------------- ------------- -----------------
GigabitEthernet 0/1              100000   Kbit 0.0%
```

以下例子为显示端口的带宽利用率值(仅显示其中部分端口的信息，未显示出全部端口信息)：

```
Ruijie# show interfaces usage
Interface                        Bandwidth     Bandwidth Usage
-------------------------------- ------------- -----------------
GigabitEthernet 1/0/1            100000   Kbit 0.0%
GigabitEthernet 1/0/2            1000000  Kbit 0.0%
GigabitEthernet 1/0/3            1000000  Kbit 0.0%
GigabitEthernet 1/0/4            1000000  Kbit 0.0%
GigabitEthernet 1/0/5            1000000  Kbit 0.0%
```

以下例子为显示 VLAN 1 中所有成员端口的报文统计值(仅显示其中部分端口的信息，未显示出全部端口信息)：

```
Ruijie# show interfaces counters vlan 1
Interface : GigabitEthernet 1/0/1
5 minutes input rate  :0 bits/sec, 0 packets/sec
5 minutes output rate :0 bits/sec, 0 packets/sec
InOctets             : 408
InUcastPkts          : 4
InMulticastPkts      : 0
InBroadcastPkts      : 0
OutOctets            : 408
OutUcastPkts         : 4
OutMulticastPkts     : 0
OutBroadcastPkts     : 0
Undersize packets    : 0
Oversize packets     : 0
collisions           : 0
Fragments            : 0
Jabbers              : 0
CRC alignment errors : 0
AlignmentErrors      : 0
FCSErrors            : 0
dropped packet events (due to lack of resources): 0
packets received of length (in octets):
```

```
  64 : 0
  65-127 : 4
  128-255 : 0
  256-511 : 0
  512-1023 : 0
  1024-1518 : 0

Interface : GigabitEthernet 1/0/2
5 minutes input rate  :0 bits/sec, 0 packets/sec
5 minutes output rate :0 bits/sec, 0 packets/sec
InOctets              : 408
InUcastPkts           : 4
InMulticastPkts       : 0
InBroadcastPkts       : 0
OutOctets             : 408
OutUcastPkts          : 4
OutMulticastPkts      : 0
OutBroadcastPkts      : 0
Undersize packets     : 0
Oversize packets      : 0
collisions            : 0
Fragments             : 0
Jabbers               : 0
CRC alignment errors  : 0
AlignmentErrors       : 0
FCSErrors             : 0
dropped packet events (due to lack of resources): 0
packets received of length (in octets):
  64 : 0
  65-127 : 4
  128-255 : 0
  256-511 : 0
  512-1023 : 0
  1024-1518 : 0
```

以下例子为显示报文统计值为非零值的端口报文统计信息值(仅显示其中部分端口的信息，未显示出全部端口信息)：

```
Ruijie# show interfaces counters nonzero
Interface : GigabitEthernet 1/0/1
5 minutes input rate  :0 bits/sec, 0 packets/sec
5 minutes output rate :0 bits/sec, 0 packets/sec
InOctets              : 408
InUcastPkts           : 4
InMulticastPkts       : 0
```

```
InBroadcastPkts      : 0
OutOctets            : 408
OutUcastPkts         : 4
OutMulticastPkts     : 0
OutBroadcastPkts     : 0
Undersize packets    : 0
Oversize packets     : 0
collisions           : 0
Fragments            : 0
Jabbers              : 0
CRC alignment errors : 0
AlignmentErrors      : 0
FCSErrors            : 0
dropped packet events (due to lack of resources): 0
packets received of length (in octets):
  64 : 0
  65-127 : 4
  128-255 : 0
  256-511 : 0
  512-1023 : 0
  1024-1518 : 0

Interface : GigabitEthernet 1/0/2
5 minutes input rate  :0 bits/sec, 0 packets/sec
5 minutes output rate :0 bits/sec, 0 packets/sec
InOctets             : 408
InUcastPkts          : 4
InMulticastPkts      : 0
InBroadcastPkts      : 0
OutOctets            : 408
OutUcastPkts         : 4
OutMulticastPkts     : 0
OutBroadcastPkts     : 0
Undersize packets    : 0
Oversize packets     : 0
collisions           : 0
Fragments            : 0
Jabbers              : 0
CRC alignment errors : 0
AlignmentErrors      : 0
FCSErrors            : 0
dropped packet events (due to lack of resources): 0
packets received of length (in octets):
```

```
  64 : 0
  65-127 : 4
  128-255 : 0
  256-511 : 0
  512-1023 : 0
  1024-1518 : 0
```

以下例子为显示模块 1/0 上端口报文统计值(仅显示其中部分端口的信息，未显示出全部端口信息)：

```
Ruijie# show interfaces counters module 1/0
Interface : GigabitEthernet 1/0/1
5 minutes input rate  :0 bits/sec, 0 packets/sec
5 minutes output rate :0 bits/sec, 0 packets/sec
InOctets             : 408
InUcastPkts          : 4
InMulticastPkts      : 0
InBroadcastPkts      : 0
OutOctets            : 408
OutUcastPkts         : 4
OutMulticastPkts     : 0
OutBroadcastPkts     : 0
Undersize packets    : 0
Oversize packets     : 0
collisions           : 0
Fragments            : 0
Jabbers              : 0
CRC alignment errors : 0
AlignmentErrors      : 0
FCSErrors            : 0
dropped packet events (due to lack of resources): 0
packets received of length (in octets):
  64 : 0
  65-127 : 4
  128-255 : 0
  256-511 : 0
  512-1023 : 0
  1024-1518 : 0

Interface : GigabitEthernet 1/0/2
5 minutes input rate  :0 bits/sec, 0 packets/sec
5 minutes output rate :0 bits/sec, 0 packets/sec
InOctets             : 408
InUcastPkts          : 4
InMulticastPkts      : 0
```

```
InBroadcastPkts      : 0
OutOctets            : 408
OutUcastPkts         : 4
OutMulticastPkts     : 0
OutBroadcastPkts     : 0
Undersize packets    : 0
Oversize packets     : 0
collisions           : 0
Fragments            : 0
Jabbers              : 0
CRC alignment errors : 0
AlignmentErrors      : 0
FCSErrors            : 0
dropped packet events (due to lack of resources): 0
packets received of length (in octets):
  64 : 0
  65-127 : 4
  128-255 : 0
  256-511 : 0
  512-1023 : 0
  1024-1518 : 0
```

以下例子为显示 VLAN 1 中所有成员端口的状态值(仅显示其中部分端口的信息，未显示出全部端口信息)：

```
Ruijie# show interfaces status vlan 1
Interface                      Status    Vlan  Duplex   Speed     Type
------------------------------ --------  ----  -------  --------- ------
GigabitEthernet 1/0/18         down      1     Unknown  Unknown   copper
GigabitEthernet 1/0/21         down      1     Unknown  Unknown   copper
GigabitEthernet 1/0/22         down      1     Unknown  Unknown   copper
GigabitEthernet 1/0/23         down      1     Unknown  Unknown   copper
GigabitEthernet 1/0/24         down      1     Unknown  Unknown   copper
GigabitEthernet 1/0/25         down      1     Unknown  Unknown   copper
```

以下例子为显示模块 1/0 中所有端口的状态值(仅显示其中部分端口的信息，未显示出全部端口信息)：

```
Ruijie# show interfaces status module 1/0
Interface                      Status    Vlan  Duplex   Speed     Type
------------------------------ --------  ----  -------  --------- ------
GigabitEthernet 1/0/18         down      1     Unknown  Unknown   copper
GigabitEthernet 1/0/21         down      1     Unknown  Unknown   copper
GigabitEthernet 1/0/22         down      1     Unknown  Unknown   copper
GigabitEthernet 1/0/23         down      1     Unknown  Unknown   copper
GigabitEthernet 1/0/24         down      1     Unknown  Unknown   copper
GigabitEthernet 1/0/25         down      1     Unknown  Unknown   copper
```

1.3.17 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。

下表是 SFP 光模块和 XFP 光模块可能出现的告警信息描述表：

字段	说明
SFP	
RX loss of signal	接收信号丢失
RX power high	接收光功率高告警
RX power low	接收光功率低告警
TX fault	发送错误
TX bias high	偏置电流高告警
TX bias low	偏置电流低告警
TX power high	发送光功率高告警
TX power low	发送光功率低告警
Temp high	温度高告警
Temp low	温度低告警
Voltage high	电压高告警
Voltage low	电压低告警
Transceiver info checksum error	模块信息校验和错误
Transceiver info I/O error	模块信息读写错误
Transceiver type and port configuration mismatch	模块类型和端口速率配置不匹配
Transceiver type not supported by port hardware	端口不支持该类型模块
XFP	
RX loss of signal	接收信号丢失
RX not ready	接收状态未就绪
RX CDR loss of lock	RX CDR 时钟失锁
RX power high	接收光功率高告警
RX power low	接收光功率低告警
TX fault	发送错误
TX CDR loss of lock	TX CDR 时钟失锁
TX bias high	偏置电流高告警
TX bias low	偏置电流低告警
TX power high	发送光功率高告警

TX power low	发送光功率低告警
Module not ready	模块状态未就绪
Temp high	温度高告警
Temp low	温度低告警
Voltage high	电压高告警
Voltage low	电压低告警
Transceiver info checksum error	模块信息校验错误
Transceiver info I/O error	模块信息读写错误
Transceiver type and port configuration mismatch	模块类型和端口速率配置不匹配
Transceiver type not supported by port hardware	端口不支持该类型该模块

下表是光模块诊断参数显示信息描述表：

字段	说明
diagnostic information	接口携带的光模块的数字诊断信息
Current diagnostic parameters	当前的诊断参数
Temp.(°C)	数字诊断参数——温度，单位为°C，精确到 1°C。
Voltage(V)	数字诊断参数——电压，单位为 V，精确到 0.01V。
Bias(mA)	数字诊断参数——偏置电流，单位为 mA，精确到 0.01mA。
RX power(dBM)	数字诊断参数——接收光功率，单位为 dBM。
TX power(dBM)	数字诊断参数——发送光功率，单位为 dBM，精确到 0.01dBM。
OK	表示当前状态正常，无需用户干预
warning	表示当前状态超过设备允许状态，需要用户注意。
alarm	表示当前状态严重超过设备允许状态，需要用户立即采取行动

☑ 光模块信息显示，故障告警和诊断参数测量功能需要配合锐捷网络的光模块使用。

☑ 光模块故障告警(光模块类型和端口速率配置不匹配告警、端口不支持该类型光模块告警除外)和诊断参数测量需要光模块支持 Digital Diagnostic Monitoring 功能才能显示。

1.3.18 配置LinkTrap策略

在设备中可以基于接口配置是否发送该接口的 LinkTrap，当功能打开时，如果接口发生 Link 状态变化，SNMP 将发出 LinkTrap,反之则不发。缺省情况下，该功能打开。

配置命令

命令	作用
Ruijie(config-if)# [**no**] **snmp trap link-status**	打开或者关闭发送该接口 link trap 的功能.

配置举例

下面配置将配置接口为不发送 Link trap：

```
Ruijie(config)# interface gigabitEthernet 1/1
Ruijie(config-if)# no snmp trap link-status
```

2 MAC 地址

2.1 概述

通过识别报文的数据链路层信息对报文转发是以太网交换机的主要功能（称为二层转发功能），以太网交换机通过报文所携带的目的 MAC 地址信息将报文转发到相应的端口，以太网交换机采用 MAC 地址表存储报文转发时所需要的目的 MAC 地址与端口信息关系。

以太网交换机的 MAC 地址表中所有的 MAC 地址都和 VLAN 相关联，不同的 VLAN 允许相同的 MAC 地址。每个 VLAN 都维护它自己逻辑上的一份地址表。一个 VLAN 已学习的 MAC 地址，对于其他 VLAN 而言可能是未知的，仍然需要学习。

以太网交换机的 MAC 地址包含以下信息：

图 1-1 MAC 地址表项构成

- 状态：表示地址表项为动态地址、静态地址或过滤地址。
- VLAN：MAC 地址所属的 VLAN
- MAC 地址：表项的 MAC 地址信息
- 端口：MAC 地址对应的端口信息

以太网交换机的 MAC 地址表中的表项通过以下两种方式进行更新和维护：

- 动态地址学习
- 手工配置地址

以太网交换机在转发报文时通过报文的目的 MAC 地址以及报文所属的 VLAN ID 的信息在 MAC 地址表中查找相应的转发输出端口，根据查找的结果采取单播、组播或广播的方式转发报文：

- 单播转发：以太网交换机能够在 MAC 地址表中查到与报文的目的 MAC 地址和 VLAN ID 相对应的表项并且表项中的输出端口是唯一的，报文直接从表项对应的端口输出。
- 组播转发：以太网交换机能够在 MAC 地址表中查到与报文的目的 MAC 地址和 VLAN ID 相对应的表项并且表项中对应一组输出端口，报文直接从这组端口输出。
- 广播转发：以太网交换机收到目的地址为 ffff.ffff.ffff 的报文或者在 MAC 地址表中查找不到对应的表项时，报文被送到所属的 VLAN 中除报文输入端口外的其他所有端口输出。

本文只涉及动态地址、静态地址与过滤地址的管理，组播地址的管理不在本文内描述，请参看 IGMP Snooping 配置指南。

2.1.1 动态地址学习

动态地址

通过以太网交换机的自动地址学习过程产生的 MAC 地址表项被称为动态地址，只有动态地址才会被地址表的老化机制所删除。

地址学习过程

通常情况下 MAC 地址表的维护都是通过动态地址学习的方式进行，其工作原理如下：

1) 以太网交换机的 MAC 地址表为空的情况下，UserA 要与 UserB 进行通讯，UserA 首先发送报文到交换机的端口 GigabitEthernet 0/2，此时以太网交换机将 UserA 的 MAC 地址学习到 MAC 地址表中。
由于地址表中没有 UserB 的源 MAC 地址，因此以太网交换机以广播的方式将报文发送到除了 UserA 以外的所有端口，包括 User B 与 User C 的端口，此时 UserC 能够收到 UserA 所发出的不属于它的报文。

图 1-2 动态地址学习步骤一

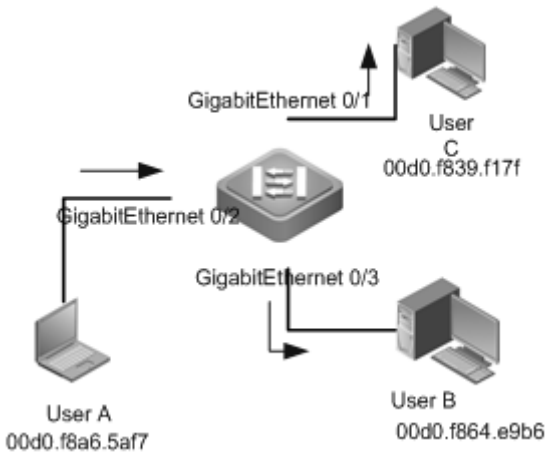


图 1-3 以太网交换 MAC 地址表一

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

2) UserB 收到报文后将回应报文通过以太网交换机的端口 GigabitEthernet 0/3 发送 UserA，此时以太网交换机的 MAC 地址表中已存在 UserA 的 MAC 地址，所以报文被以单播的方式转发到 GigabitEthernet 0/2 端口，同时以太网交换机将学习 UserB 的 MAC 地址，与步骤 1 中所不同的是 UserC 此时接收不到 UserB 发送给 UserA 的报文。

图 1-4 动态地址学习步骤二

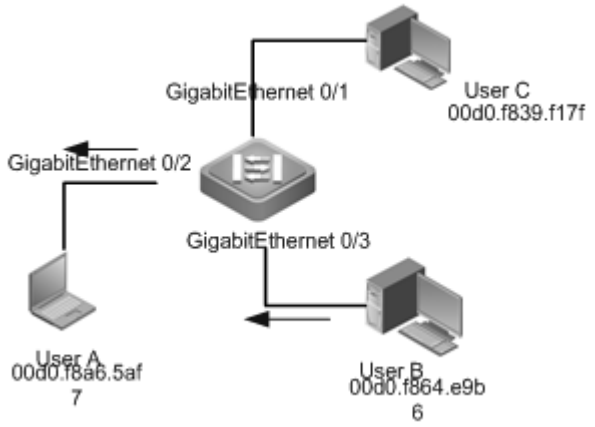


图 1-5 以太网交换机 MAC 地址表二

Status	VLAN	MAC地址	端口
动态	1	00d0.f8a6.5af7	GigabitEthernet 0/2
动态	1	00d0.f864.e9b6	GigabitEthernet 0/3

3) 通过 UserA 与 UserB 的一次交互过程后，以太网交换机学习到了 UserA 与 UserB 的源 MAC 地址，之后 UserA 与 UserB 之间的报文交互则采用单播的方式进行转发，此后 UserC 将不再接收到 UserA 与 UserB 之间的交互报文。

地址老化

以太网交换机的 MAC 地址表是有容量限制的，以太网交换机采用地址表老化机制进行不活跃的地址表项淘汰。

以太网交换机在学习到一个新的地址的同时启动该地址的老化记时，在达到老化记时前，如果以太网交换机没有再一次收到以该地址为源 MAC 地址的报文，那该地址在达到老化时间后会从 MAC 地址表中删除。

2.1.2 静态地址

手工配置的 MAC 地址表项，用于绑定 MAC 地址与端口关系，这类地址只能通过手工配置添加和删除，保存配置后设备重启，静态地址也不会丢失。

通过手工配置静态地址的方式可以在 MAC 地址表中绑定设备下接的网络设备的 MAC 地址与端口关系。

2.1.3 过滤地址

手工配置的 MAC 地址表项，用于在以太网交换机上丢弃以所配置的 MAC 地址为源地址或目的地址的报文，这类地址只能通过手工配置添加和删除，保存配置后设备重启，过滤地址也不会丢失。

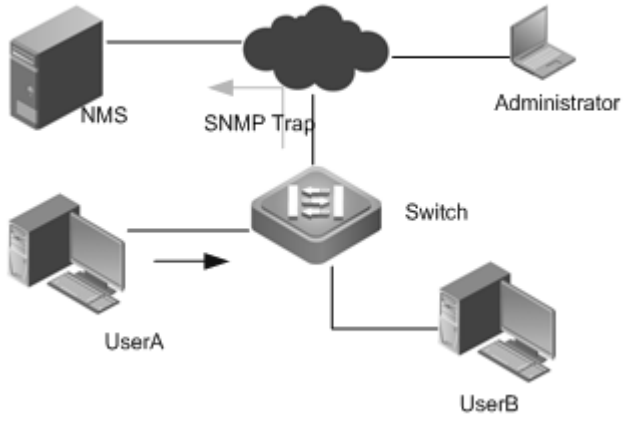
通过手工将网络中的非法接入用户的源 MAC 地址配置为过滤地址的方式可以实现过滤非法接入用户。

过滤地址对送 CPU 的报文无效。如：某个 ARP 报文的二层源 MAC 为一过滤地址，此时该 ARP 报文仍然会被送往 CPU，但其并不会被转发。

2.1.4 MAC 地址变化通知

以太网交换机的 MAC 地址通知功能通过与网络管理工作站（NMS）的协作为网络管理提供了监控网络以太网交换机下用户变化的机制。

图 1-6 地址变化通告



打开 MAC 地址通知的功能后，当以太网交换机学习到一个新的 MAC 地址或老化掉一个已学习到的 MAC 地址时，一个反映 MAC 地址变化的通知信息就会产生，并以 SNMP Trap 的方式将通知信息发送给指定的 NMS(网络管理工作站)。

当一个 MAC 地址增加的通知产生，就可以知道一个由此 MAC 地址标识的新用户开始使用网络，当一个 MAC 地址删除的通知产生，则表示一个用户在地址老化时间内没有新的报文发送，通常可以认为此用户已经停止使用网络了。

当使用以太网交换机下接的用户较多时，可能会出现在短时间内会有大量的 MAC 地址变化产生，导致网络流量增加。为了减轻网络负担，可以设置发送 MAC 地址通知的时间间隔。在达到配置的时间间隔之后，系统将这个时间内的通知信息封装成多个通知信息，此时在每条地址通知信息中，就包含了若干个 MAC 地址变化的信息，从而可以会有效地减少网络流量。

当 MAC 地址通知产生时，通知信息同时会记录到 MAC 地址通知历史记录表中。此时即便没有配置接收 Trap 的 NMS，管理员也可以通过查看 MAC 地址通知历史记录表来了解最近 MAC 地址变化的消息。

MAC 地址通知仅对动态地址有效，对于配置的静态地址与过滤地址的变化将不会产生通知信息。

2.1.5 IP 和 MAC 地址绑定

概述

通过手动配置 IP 和 MAC 地址绑定功能，可以对输入的报文进行 IP 地址和 MAC 地址绑定关系的验证。如果将一个指定的 IP 地址和一个 MAC 地址绑定，则设备只接收源 IP 地址和 MAC 地址均匹配这个绑定地址的 IP 报文；否则该 IP 报文将被丢弃。

利用地址绑定这个特性，可以严格控制设备的输入源的合法性。需要注意的是，通过地址绑定控制交换机的输入，将优先于 ACL 生效。

地址绑定模式

地址绑定的模式分为:兼容，宽松，严格三种模式，默认模式为严格模式。其相应的转发规则，见下表所示：

模式	IPv4 报文转发规则
严格	符合 IPV4+MAC 条件的报文转发
宽松	符合 IPV4+MAC 条件的报文转发
兼容	符合 IPV4+MAC 条件的报文转发

地址绑定例外端口

IP 地址和 MAC 地址绑定功能缺省对设备上的所有端口都生效，通过配置例外口的方式可以在使绑定功能在部份端口上不生效。

> 在应用中设备的上链端口的 IP 报文的绑定关系是不确定的，通常将设备的上链端口配置为例外口，此时上链端口则不进行 IP 地址与 MAC 地址的绑定检查。

2.2 协议规范

《IEEE Std 802.3™ Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications》

《IEEE Std 802.1Q™ Virtual Bridged Local Area Networks》

2.3 配置MAC地址

2.3.1 缺省配置

功能特性	缺省值
动态地址老化时间	300 秒
端口 MAC 地址学习能力	开启
动态地址学习模式	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

2.3.2 配置动态地址

配置端口 MAC 地址学习能力

命令	作用
Ruijie(config-if)# **no mac-address-learning**	关闭端口 MAC 地址学习能力，通过 show mac-address-learning 命令查看端口学习能力配置

MAC 地址学习能力缺省开启，如果端口上配置了 DOT1X，IP SOURCE GUARD 绑定功能，端口的学习能力不能开启；同样，关闭端口学习能力的端口不能开启接入控制功能。

清除动态地址

命令	作用
Ruijie#**clear mac-address-table dynamic**	删除设备上所有的动态地址
Ruijie#**clear mac-address-table dynamic address** *mac-address* **vlan** *vlan-id*	删除特定 MAC 地址 *mac-address*：指定要删除的 MAC 地址。 *vlan-id*：指定要删除的 MAC 地址所在的 VLAN。
Ruijie#**clear mac-address-table dynamic interface** *interface-id* [**vlan** *vlan-id*]	删除特定物理接口或 Aggregate Port 上的特定 VLAN 中的所有动态地址或接口上所有动态地址。 *interface-id*：指定的物理接口或是 Aggregate Port。 *vlan-id*：指定删除动态地址所属的 VLAN。
Ruijie#**clear mac-address-table dynamic vlan** *vlan-id*	删除特定 VLAN 上的所有动态地址 *vlan-id*：指定所要删除的动态地址所属的 VLAN。

下面的例子说明了如何配置删除设备接口 GigabitEthernet 0/1 下 VLAN 1 中的所有动态地下。

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

查看配置

命令	作用
Ruijie#**show mac-address-table dynamic**	查看设备上所有的动态地址信息。
Ruijie#**show mac-address-table dynamic address** *mac-address* [**vlan** *vlan-id*]	查看设备上特定动态 MAC 地址信息。 *mac-address*：查看的 MAC 地址。 vlan-id：查看特定的 VLAN 中的特定 MAC 地址。
Ruijie#**show mac-address-table dynamic interface** *interface-id* [**vlan** *vlan-id*]	查看设备上指定物理接口或 Aggregate Port 下的动态地址信息。 *interface-id*：指定的物理接口或是 Aggregate Port。 *vlan-id*：查看特定的 VLAN 中的动态地址。

Ruijie#**show mac-address-table dynamic vlan** *vlan-id*	查看设备上指定 VLAN 下的动态地址信息。 *vlan-id*：查看特定的 VLAN 中的动态地址。
Ruijie# **show mac-address-table count [interface** *interface-id* **| vlan** *vlan-id***]**	查看地址表的统计信息。 *interface-id*：查看指定接口的地址表项统计信息。 *vlan-id*：查看指定 VLAN 下的地址表项统计信息。

下面的例子说明了如何查看设备上物理接口 GigabitEthernet 0/1 下 VLAN 中的所有动态 MAC 地址信息。

```
Ruijie#show mac-address-table dynamic interface gigabitEthernet 0/1 vlan 1
Vlan          MAC Address           Type      Interface
----------  -------------------- -------- ------------------
   1          0000.5e00.010c        DYNAMIC  GigabitEthernet 0/1
   1          00d0.f822.33aa        DYNAMIC  GigabitEthernet 0/1
   1          00d0.f822.a219        DYNAMIC  GigabitEthernet 0/1
   1          00d0.f8a6.5af7        DYNAMIC  GigabitEthernet 0/1
```

下面的例子说明了如何查看设备上的地址表统计信息：

例 1：显示 MAC 地址各类型的表项数量：

```
Ruijie# show mac-address-table count
Dynamic Address Count  : 30
Static  Address Count  : 0
Filtering Address Count: 0
Total Mac Addresses    : 30
Total Mac Address Space Available: 8159
```

例 2：显示 VLAN 1 下的 MAC 地址数量：

```
Ruijie# show mac-address-table count vlan 1
Dynamic Address Count  : 7
Static  Address Count  : 0
Filter  Address Count  : 0
Total Mac Addresses     : 7
```

例 3：显示 interface g0/1 下的 MAC 地址数量：

```
Ruijie# show mac-address-table interface g0/1
Dynamic Address Count  : 10
Static  Address Count  : 0
Filter  Address Count  : 0
Total Mac Addresses     : 10
```

2.3.3 配置动态地址老化时间

配置老化时间

命令	作用
Ruijie(config)# **mac-address-table agint-time** [*0*|*10-1000000*]	设置一个地址被学习后将保留在动态地址表中的时间长度，单位是秒，范围是 10－1000000 秒，缺省为 300 秒。当你设置这个值为 0 时，地址老化功能将被关闭，学习到的地址将不会被老化。
Ruijie(config)# **no mac-address-table agint-time**	恢复地址老化时间为缺少值。

下面的例子说明了如何配置设备的地址老化时间为 180 秒。

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#mac-address-table aging-time 180
```

查看配置

命令	作用
Ruijie#**show mac-address-table aging-time**	查看所有的地址老化配置信息

下面的例子说明了如何查看设备上的地址老化时间配置。

```
Ruijie#show mac-address-table aging-time
Aging time    : 180 seconds
```

地址表的实际老化时间会与设定值存在一定偏差，但不会超过设定值的 2 倍。

2.3.4 配置静态地址

管理静态地址

命令	作用
Ruijie(config)# **mac-address-table static** *mac-address* **vlan** *vlan-id* **interface** *interface-id*	*mac-address*：指定表项对应的目的 MAC 地址。 *vlan-id*：指定该地址所属的 VLAN。 *interface-id*：包将转发到的接口(可以是物理端口或 Aggregate Port)。 当设备在 vlan-id 指定的 VLAN 上接收到以 mac-address 为目的地址的报文时，这个报文将被转发到 interface-id 所指定的接口上。
Ruijie(config)# **no mac-address-table static** *mac-address* **vlan** *vlan-id* **interface** *interface-id*	删除静态地址表项，参数与添加命令一致。

下面的例子说明了如何配置添加一个静态地址 00d0.f800.073c，当在 VLAN 4 中接收到目的地址为该地址的报文时，这个报文将被转发到指定的接口 Gigabitethernet 0/3 上。

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

```
Ruijie(config)# mac-address-table static 00d0.f800.073c vlan 4 interface gigabitethernet 0/3
```

下面的例子说明了如何配置删除上一例子中添加的静态地址 00d0.f800.073c。

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#no mac-address-table static 00d0.f800.073c vlan 4 interface gigabitethernet 0/3
```

查看配置

命令	作用
Ruijie# **show mac-address-table static**	查看所有的静态地址信息

下面的例子说明了如何查看设备上的所有静态地址信息。

```
Vlan          MAC Address           Type       Interface
----------  -------------------- -------- --------------------
   4        00d0.f800.073c        STATIC    GigabitEthernet 0/3
```

2.3.5 配置过滤地址

管理过滤地址

命令	作用
Ruijie(config)# **mac-address-table filtering** *mac-address* **vlan** *vlan-id*	*mac-address*：指定表项对应的 MAC 地址 *vlan-id*：指定该地址所属的 VLAN 当设备在 vlan-id 指定的 VLAN 上接收到以 mac-address 指定的地址为源地址或目的地址的报文将被丢弃。
Ruijie(config)# **no mac-address-table filtering** *mac-address* **vlan** *vlan-id*	删除过滤地址表项，参数与添加命令一致。

下面的例子说明了如何配置添加过滤地址。当在 VLAN 4 中接受到源地址或目的地址为 00d0.f800.073c 的报文时，将丢弃此报文。

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#mac-address-table filtering 00d0.f800.073c vlan 4
```

下面的例子说明了如何配置删除上一例子中的过滤地址 00d0.f800.073c。

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#no mac-address-table filtering 00d0.f800.073c vlan 4
```

查看配置

命令	作用
Ruijie#**show mac-address-table filtering**	查看过滤地址信息

下面的例子说明了如何查看设备上的所有静态地址信息。

```
Vlan          MAC Address           Type        Interface
-------  --------------- --------------------     -------------------
 4       00d0.f800.073c    FILTER                      GigabitEthernet 0/3
```

2.3.6 配置 MAC 地址变化通知

配置 MAC 地址变化通知

缺省情况下，MAC 地址的全局开关被关闭，所有接口的 MAC 地址通知功能也均被关闭。

配置设备 MAC 地址通知功能：

命令	作用
Ruijie(config)# **snmp-server host** *host-addr* **traps** [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**] }] *community-string*	配置接收 MAC 地址通知的 NMS。 *host-addr*：指明接收者的 IP。 **version**：指明发送哪种版本的 snmp trap 报文，对 v3 版本还可以指定是否认证以及安全等级参数。
Ruijie (config)#**snmp-server enable traps**	使能设备发送 trap 功能 。
Ruijie(config)#**mac-address-table notification**	打开 MAC 地址通知功能开关。
Ruijie(config)# **mac-address-table notification** { **interval** *value* | **history-size** *value*}	配置 MAC 地址通知的时间间隔与历史记录容量。 **interval** *value* ：设置产生 MAC 地址通知的时间间隔(可选)。时间间隔的单位为秒，范围为 1－3600，缺省为 1 秒。 **history-size** *value* ：MAC 通知历史记录表中记录的最大个数，范围 1－200，缺省为 50。
Ruijie(config-if)# **snmp trap mac-notification** {**added** |**removed**}	打开接口的 MAC 地址通知功能。 **added**：当地址增加时通知。 **removed**：当地址被删除时通知。

下面的例子说明了如何打开 MAC 地址通知功能，并以 public 为认证名向 IP 地址为 192.168.12.54 的 NMS 发送 MAC 地址变化通知的 Trap，产生 MAC 地址变化通知的间隔时间为 40 秒，MAC 地址通知历史记录表的大小为 100，打开接口 Gigabitethernet 0/1 上当 MAC 地址增加和减少时进行通知的功能：

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#snmp-server host 192.168.12.54 traps public
Ruijie(config)#snmp-server enable traps
Ruijie(config)#mac-address-table notification
Ruijie(config)#mac-address-table notification interval 40
```

```
Ruijie(config)#mac-address-table notification  history-size 100
Ruijie(config)#interface GigabitEthernet 0/1
Ruijie(config-if)#snmp trap mac-notification added
Ruijie(config-if)#snmp trap mac-notification removed
```

查看配置

在特权模式下，使用下表所列的命令来查看设备的 MAC 地址表信息：

命令	作用
Ruijie# **show mac-address-table notification**	查看 MAC 地址变化通知功能的全局配置信息。
Ruijie# **show mac-address-table notification interface**	查看接口的 MAC 地址变化通知的使能状况。
Ruijie# **show mac-address-table notification history**	查看 MAC 地址变化通知信息的历史记录表。

下面是查看 MAC 地址变化通知信息的例子。

查看 MAC 地址通知功能的全局配置信息：

```
Ruijie#show mac-address-table notification
MAC Notification Feature : Enabled
Interval(Sec): 2
Maximum History Size : 154
Current History Size : 2
Ruijie# show mac-address-table notification interface
Interface           MAC Added Trap  MAC Removed Trap
----------------- -------------- ----------------
Gi0/1                Disabled        Enabled
Gi0/2                Disabled        Disabled
Gi0/3                Enabled         Enabled
Gi0/4                Disabled        Disabled
Gi0/5                Disabled        Disabled
Gi0/6                Disabled        Disabled
Ruijie#show mac-address-table notification history
History Index:1
Entry Timestamp: 15091
MAC Changed Message :
Operation   VLAN  MAC Address    Interface
----------- ---- -------------- --------------------
Added         1    00d0.f808.3cc9  Gi0/1
Removed      1     00d0.f808.0c0c  Gi0/1
History Index:2
Entry Timestamp: 21891
MAC Changed Message :
Operation   VLAN  MAC Address    Interface
```

```
---------- ---- -------------- --------------------
Added      1    00d0.f80d.1083 Gi0/1
```

2.3.7 配置 IP 地址和 MAC 地址绑定

配置 IP 地址和 MAC 地址绑定

在全局模式下，可以通过以下步骤来设置地址绑定：

命令	作用
Ruijie(config)# **address-bind** *ip-address mac-address*	配置 IP 地址和 MAC 地址的绑定关系 *ip-address*：绑定的 IP 地址 *mac-address*：绑定的 MAC 地址
Ruijie(config)# **address-bind install**	使 IP 和 MAC 地址绑定生效

在全局配置模式下使用 **no address-bind** *ip-address mac-address* 删除一个 IP 地址和 MAC 地址的绑定项。

通过 **no address-bind install** 命令可关闭绑定功能，使地址绑定配置不生效。

下面是配置 IP 地址和 MAC 地址绑定模式的例子：

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#address-bind 192.168.5.1 00d0.f800.0001
Ruijie(config)#address-bind install
```

如果执行 address-bind install 之后，没有配置 IP+MAC 绑定，则所有 IP+MAC 绑定功能不生效，所有报文可以通过。

配置地址绑定例外端口

命令	作用
Ruijie(config)# **address-bind uplink** *interface-id*	配置地址绑定的例外端口 *interface-id*：端口或 Aggregate Port

通过 **no address-bind uplink** *interface-id* 命令取消指定例外口配置。

下面是配置端口 GigabitEthernet 0/1 为例外端口的例子：

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#address-bind uplink GigabitEthernet 0/1
```

查看配置

在特权模式下使用下列命令查看设备上的 IP 地址和 MAC 地址绑定的相关配置

命令	作用
Ruijie# **show address-bind**	查看设备上的 IP 地址与 MAC 地址绑定配置
Ruijie# **show address-bind uplink**	查看设备上的例外口信息

下面是查看设备的 IP 地址和 MAC 地址绑定配置的例子：

```
Ruijie#show address-bind
Total Bind Addresses in System : 1
IP Address          Binding MAC Addr
---------------     ----------------
    192.168.5.1     00d0.f800.0001
```

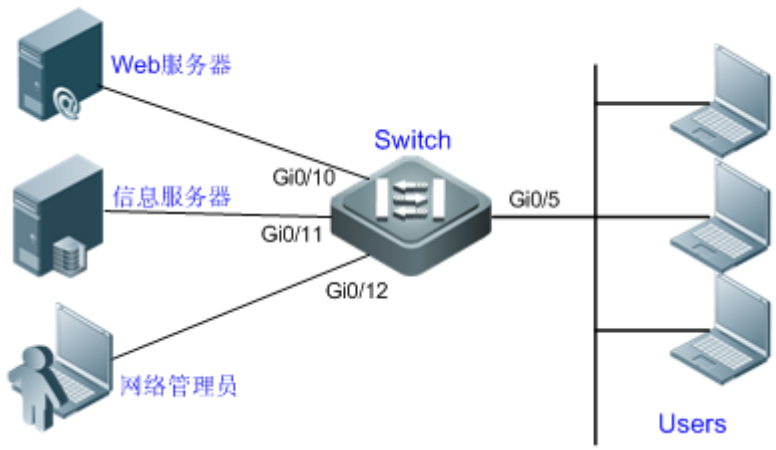
2.4 MAC地址表管理典型配置举例

2.4.1 静态 MAC 地址配置举例

拓扑图

下图为某信息系统组网图。Web 服务器、数据库服务器分别通过 Gi0/10、Gi0/11 连接到以太网交换机，服务器管理员通过 Gi0/12 口连接到以太网交换机，其他的一般用户通过以太网交换机的 Gi0/5 口接入访问 Web 服务器。所有的数据均在 VLAN 10 中转发。

图 1-7 静态 MAC 地址应用组网拓扑



应用需求

为保障 WEB 服务器与数据库之间交互的信息安全以及管理员与服务器之间交互的信息的安全，通过配置静态地址的方式保证 WEB 服务器与数据库服务器之间、管理员与各服务器之间的数据转发采用单播方式。这样可以有效的避免这些数据被以广播的方式转发到一般用户所使用的网络中。

配置要点

配置静态 MAC 地址表项，明确以下三个要素：

- 指定表项对应的目的 MAC 地址（Mac-address）
- 指定该地址所属的 VLAN（vlan-id）
- 接口 ID（Interface-id）

当交换机在 Vlan-id 指定的 VLAN 上接收到以 Mac-address 为目的地址的报文时，这个报文将被转发到 Interface-id 所指定的接口上。

本例的 MAC 地址同 VLAN、接口对应关系如下表所示：

角色	MAC 地址	VLAN ID	接口 ID
Web 服务器	00d0.3232.0001	VLAN2	Gi0/10
信息服务器	00d0.3232.0002	VLAN2	Gi0/11
网络管理员	00d0.3232.1000	VLAN2	Gi0/12

配置步骤

！进入交换机的全局配置模式

```
Ruijie>en
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

！添加静态 MAC 地址（指出所属 VLAN、接口）

```
Ruijie(config)#mac-address-table static 00d0.f8003232.0001 vlan 110 interface gigabitEthernet 0/10
Ruijie(config)#mac-address-table static 00d0.f8003232.0002 vlan 110 interface gigabitEthernet 0/211
Ruijie(config)#mac-address-table static 00d0.f800.00033232.1000 vlan 110 interface gigabitEthernet 0/312
```

查看设备配置

配置验证

在交换机上查看配置的静态 MAC 地址

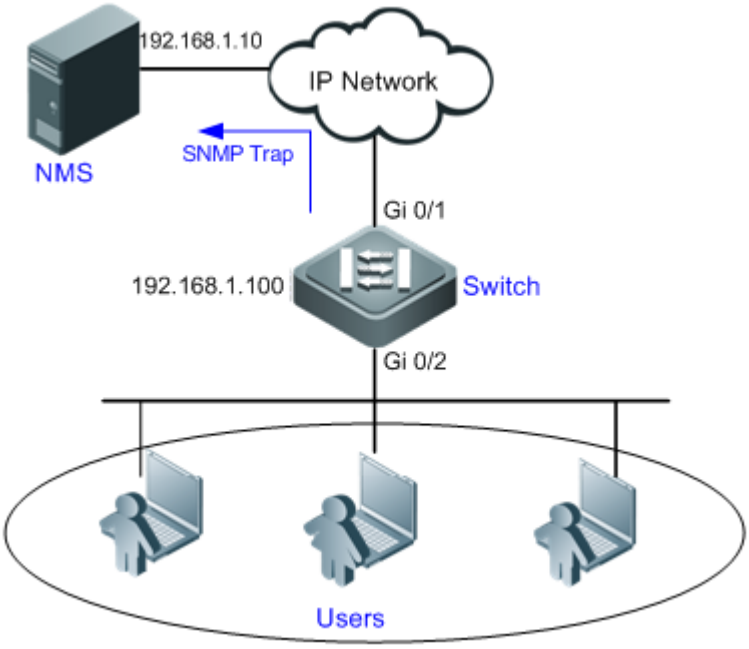
```
Ruijie#show mac-address-table static
Vlan        MAC Address          Type     Interface
----------  -------------------- -------- ------------------
   110        00d0.f8003232.0001       STATIC   GigabitEthernet 0/10
   110        00d0.f8003232.0002       STATIC   GigabitEthernet 0/211
   110        00d0.f800.3232.1000     STATIC   GigabitEthernet 0/312
```

2.4.2 动态 MAC 地址变化通知配置举例

拓扑图

下图为某企业内部网络示意图。下联用户通过 Gi0/2 口连接到交换机。

图 1-8 MAC 地址变化通知组网拓扑图



应用需求

为了便于管理员对下联用户使用网络情况信息的掌控，希望通过配置达到以下目的：

- 当交换机下联用户的接口学习到一个新的 MAC 地址或老化掉一个已学习到的地址时，将地址变化信息记录到 MAC 地址通知历史记录表中，供管理员了解最近的 MAC 地址变化信息。
- 同时，交换机能将 MAC 地址变化通知以 SNMP Trap 的方式将通知信息发送给指定的 NMS(网络管理工作站)
- 当交换机下联用户较多时，能尽量避免短时间内产生大量的 MAC 地址变化信息，减轻网络的负担。

配置要点

- 打开交换机全局 MAC 地址通知开关，在 Gi0/2 接口上配置 MAC 地址通知功能。
- 配置 NMS 主机地址，使能交换机主动发送 SNMP Trap 通知。交换机到 NMS（网络管理工作站）的路由可达。
- 设置交换机发送 MAC 地址通知的时间间隔为 300 秒（默认时间间隔为 1 秒）。交换机将该时间间隔内的通知信息封装成多个通知信息，这样，在每条地址通知信息中，就包含了若干个 MAC 地址变化的信息，从而达到减少网络流量的目的。

配置步骤

设备 IP 地址如图所示，具体配置过程此处省略。

第一步，打开交换机全局 MAC 地址变化通知开关

```
Ruijie>enable
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#mac-address-table notification
```

第二步，设置备发送 MAC 地址通知的时间间隔为 30 秒

```
Ruijie(config)#mac-address-table notification
```

第三步，打开 Gi0/2 接口的 MAC 地址通知功能

```
Ruijie(config)#mac-address-table notification interval 300
```

！进入 Gi0/2 接口配置模式

```
Ruijie(config)#interface gigabitEthernet 0/2
```

！设置当接口上有地址增加时发送通知

```
Ruijie(config-if-GigabitEthernet 0/2)# snmp trap mac-notification added
```

！设置当接口上有地址老化时也发送通知

```
Ruijie(config-if-GigabitEthernet 0/2)# snmp trap mac-notification removed
Ruijie(config-if-GigabitEthernet 0/2)#exit
```

第四步，配置接收 MAC 地址通知 Trap 信息的 NMS；NMS 地址为“192.168.1.10”，消息格式为 Version 2c，认证名为“comefrom2”

```
Ruijie(config)#snmp-server host 192.168.1.10 traps version 2c comefrom2
```

第五步，使能交换机主动发送 Trap 消息。

```
Ruijie(config)# snmp-server enable traps
```

配置验证

第一步，查看 MAC 地址通知功能的全局配置信息

```
Ruijie#show mac-address-table notification
MAC Notification Feature : Enabled
Interval(Sec): 300                    //发送 MAC 地址通知的时间间隔为 300 秒
Maximum History Size : 50   //默认 MAC 通知历史记录表的最大表项为 50 条
Current History Size : 0   //当前记录条目数
```

第二步，查看接口的 MAC 地址变化通知的使能状况

```
Ruijie#show mac-address-table notification interface gigabitEthernet 0/2
Interface               MAC Added Trap     MAC Removed Trap
-----------             --------------     --------------
GigabitEthernet 0/2    Enabled            Enabled
```

第三步，查看接口 MAC 地址表

```
Ruijie#show mac-address-table interface gigabitEthernet 0/2
Vlan        MAC Address          Type     Interface
----------  -------------------- -------- --------------------
   1        00d0.3232.0001       DYNAMIC  GigabitEthernet 0/2
   1        00d0.3232.0002       DYNAMIC  GigabitEthernet 0/2
   1        00d0.3232.0003       DYNAMIC  GigabitEthernet 0/2
```

第四步，功能验证。

使用 **clear mac-address-table dynamic address** *00d0.3232.0003* 模拟 00d0.3232.0003 地址的老化。

! 查看 MAC 地址通知功能的全局配置信息

```
Ruijie#show mac-address-table notification
MAC Notification Feature : Enabled
Interval(Sec): 300
Maximum History Size : 50
Current History Size : 1  // MAC 地址变化通知记录数，当前 1 条。
```

! 查看 MAC 地址变化通知信息的历史记录表

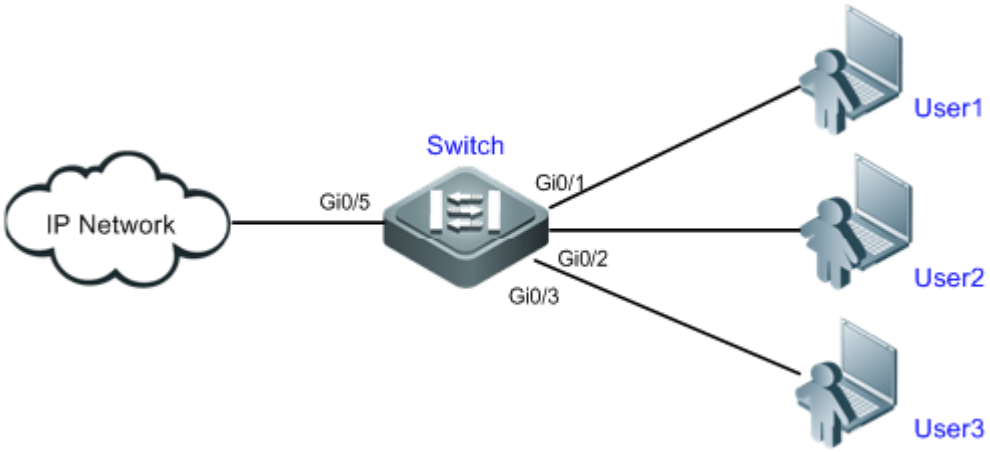
```
Ruijie#show mac-address-table notification history
History Index : 0
Entry Timestamp: 221683
MAC Changed Message :
Operation:DEL Vlan:1 MAC Addr: 00d0.3232.0003 GigabitEthernet 0/2
```

2.4.3 全局 IP/MAC 绑定配置举例

拓扑图

下图为某企业内部网络示意图。为了方便管理，企业为每台主机固定分配了一个 IP 地址。

图 1-9 全局 IP/MAC 绑定组网示意图



应用需求

- 防止员工非法盗用 IP，例如盗用权限更高人员的 IP 地址，以获得权限外的信息。
- 员工可在部门内实现移动办公。

配置要点

通过在交换机上手动配置全局 IP 和 MAC 地址绑定功能即可满足上述要求。配置要点如下：

- 手动配置全局 IP 和 MAC 地址绑定（本例列举 3 个用户）

用户	所属主机 MAC 地址	分配的 IP 地址
User1	00d0.3232.0001	192.168.1.10
User2	00d0.3232.0002	192.168.1.20
User3	00d0.3232.0003	192.168.1.30

- 全局使能 IP 和 MAC 地址绑定功能
- 将交换机的上链口（本例为 Gi0/5 口）配置为例外口

在应用中，由于交换机的上链口的 IP 报文的绑定关系是不确定的，通常将交换机的上链端口配置为例外口，此时上链端口则不进行 IP 地址与 MAC 地址的绑定检查。

配置步骤

第一步，配置全局 IP 和 MAC 地址绑定

```
Ruijie#configure terminal
```

！配置 User1 的 IP 和 MAC 地址绑定

```
Ruijie(config)#address-bind 192.168.1.10 00d0.3232.0001
```

！配置 User2 的 IP 和 MAC 地址绑定

```
Ruijie(config)#address-bind 192.168.1.20 00d0.3232.0002
```

！配置 User3 的 IP 和 MAC 地址绑定

```
Ruijie(config)#address-bind 192.168.1.30 00d0.3232.0003
```

第二步，全局使能 IP 和 MAC 地址绑定功能

```
Ruijie(config)#address-bind install
```

第三步，将交换机的上链口（本例为 Gi0/5 口）配置为例外口

```
Ruijie(config)#address-bind uplink gigabitEthernet 0/5
```

配置验证

第一步，查看交换机上的 IP 地址和 MAC 地址绑定配置。关注点：绑定关系是否正确。

```
Ruijie#show address-bind
IP Address          Binding MAC Addr
---------------     -----------------
   192.168.1.10     00d0.3232.0001
   192.168.1.20     00d0.3232.0002
   192.168.1.30     00d0.3232.0003
```

第二步，查看交换机上地址绑定例外口的配置

```
Ruijie#show address-bind uplink
Ports        State
------------ ------
Gi0/5        Enabled
```

第三步，测试验证。

交换机（除 Gi0/5 接口外）只接收源 IP 地址和 MAC 地址均匹配这些绑定地址的 IP 报文；对于不符合绑定条件的 IP 报文被丢弃。

3 Aggregate Port

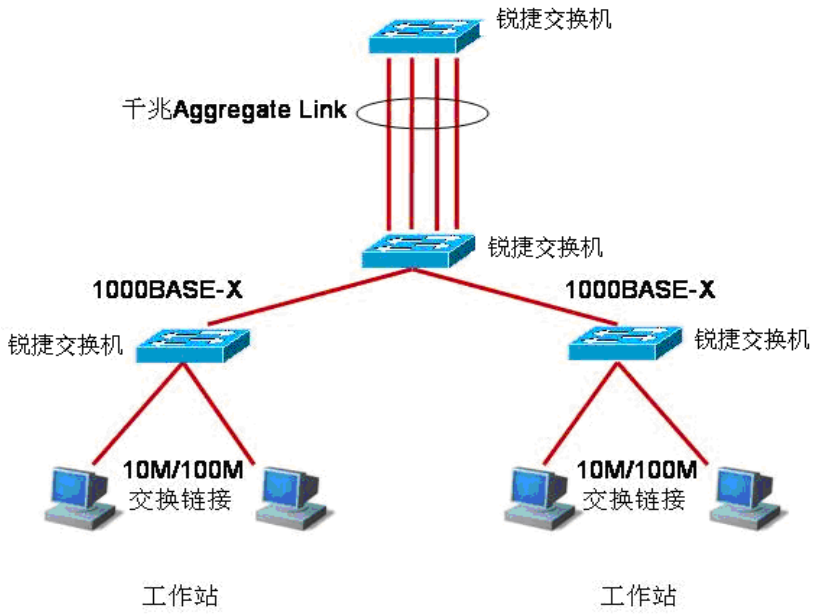
3.1 概述

将多个物理链接捆绑在一起形成一个逻辑链接，这个逻辑链接称为 Aggregate Port（简称 AP）。锐捷设备所提供的 AP 功能符合 IEEE802.3ad 标准，它可以用于扩展链路带宽，提供更高的连接可靠性。

AP 功能支持流量平衡，可以把流量均匀地分配给各成员链路。AP 功能还实现了链路备份，当 AP 中的一条成员链路断开时，系统会将该成员链路的流量自动地分配到 AP 中的其它有效成员链路上。AP 中一条成员链路收到的广播或者多播报文，将不会被转发到其它成员链路上。

☑ NBS200F 系列的每个 AP 口最多包含的成员口数量都为 8 个，支持最大 AP 数量为 120。

图 1-1 典型的 AP 配置



3.1.1 流量平衡

AP 可以根据报文的源 MAC 地址、目的 MAC 地址，源 MAC 地址+目的图 1-1MAC 地址、源 IP 地址，目的 IP 地址以及源 IP 地址+目的 IP 地址等特征值把流量平均地分配到 AP 的成员链路中。您可以用 **aggregateport load-balance** 设定流量分配方式。

源 MAC 地址流量平衡是根据报文的源 MAC 地址把报文分配到 AP 的各个成员链路中。不同源 MAC 的报文，根据源 MAC 地址在各成员链路间平衡分配；相同源 MAC 的报文，固定从同一个成员链路转发。

目的 MAC 地址流量平衡是根据报文的目的 MAC 地址把报文分配到 AP 的各个成员链路中。相同目的 MAC 的报文，固定从同一个成员链路转发；不同目的 MAC 的报文，根据目的 MAC 地址在各成员链路间平衡分配。

源 MAC+目的 MAC 地址流量平衡是根据报文的源 MAC 和目的 MAC 地址把报文分配到 AP 的各个成员链路中。具有不同的源 MAC+目的 MAC 地址的报文根据源 MAC+目的 MAC 地址在各成员链路间平衡分配，而具有相同的源 MAC+目的 MAC 地址的报文则固定分配给同一个成员链路。

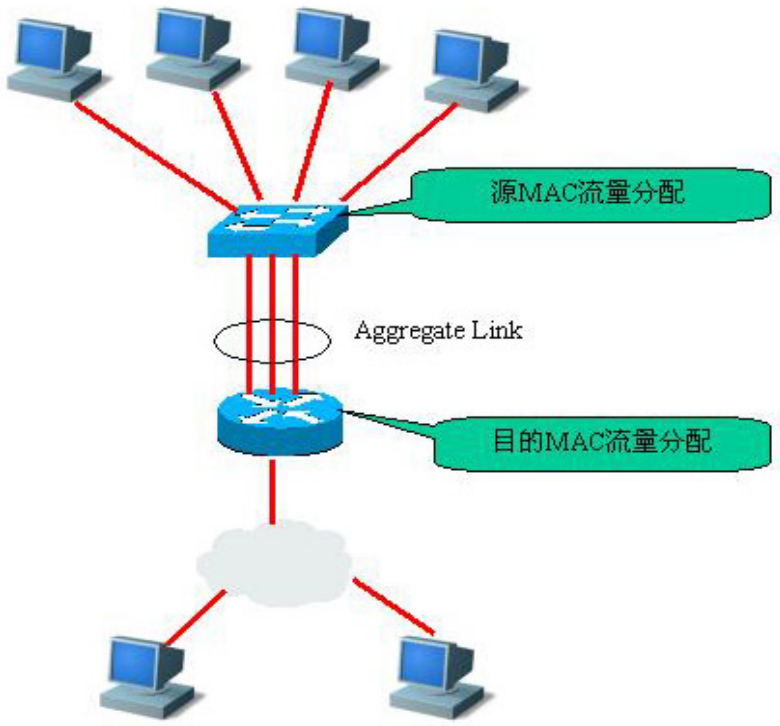
源 IP 地址或目的 IP 地址流量平衡是根据报文源 IP 或目的 IP 进行流量分配。不同源 IP 或目的 IP 的报文根据源 IP 或目的 IP 在各成员链路间平衡分配，相同源 IP 或目的 IP 的报文则固定通过相同的成员链路转发。该流量平衡方式用于三层报文，如果在此流量平衡模式下收到二层报文，则自动根据设备的默认方式进行流量平衡。

源 IP 地址+目的 IP 地址流量平衡是根据报文源 IP 和目的 IP 进行流量分配。该流量平衡方式用于三层报文，如果在此流量平衡模式下收到二层报文，则自动根据设备的默认方式进行流量平衡。具有不同的源 IP+目的 IP 地址的报文根据源 IP+目的 IP 地址在各成员链路间平衡分配，具有相同的源 IP+目的 IP 地址的报文则固定分配给相同的成员链路。

以上所有平衡模式都适用于二层 AP 和三层 AP，即源 IP 地址流量平衡、目的 IP 地址流量平衡、源 IP 地址+目的 IP 地址流量平衡模式也适用于二层 AP。用户应根据不同的网络环境设置合适的流量分配方式，以便能把流量较均匀地分配到各个链路上，充分利用网络的带宽。

在下图中，一个交换机通过 AP 与路由器进行通讯，所有内网中的设备（如图中的上面 4 台 PC 机）以路由器为网关，所有外网（如图中的下面 2 台 PC 机）经路由器发出的报文的源 MAC 都是网关的 MAC 地址，为了让路由器与其他主机之间的通讯流量能由其他链路来分担，应设置为根据目的 MAC 地址进行流量平衡；而在交换机处，则需要设置为根据源 MAC 地址进行流量平衡。

图 1-2 AP 流量平衡示意图



3.2 配置Aggregate Port

3.2.1 缺省配置

功能特性	缺省值
二层 AP 接口	无
三层 AP 接口	无
流量平衡	根据输入报文的源 MAC 和目的 MAC 进行流量分配

3.2.2 配置指导

- AP 成员端口的端口速率必须一致。
- 二层端口只能加入二层 AP，三层端口只能加入三层 AP；包含成员口的 AP 口不允许改变二层/三层属性。
- 一个端口加入 AP，端口的属性将被 AP 的属性所取代。
- 一个端口从 AP 中删除，则端口的属性将恢复为加入 AP 前的属性。

当一个端口加入 AP 后，不能在该端口上进行任何配置，直到该端口退出 AP。

3.2.3 配置 L2 Aggregate Port

4) （可选）创建一个 L2 AP。

命令	作用
Ruijie(config)# **interface aggregateport** *ap-number*	创建一个 L2 AP。

5) 向该 AP 中添加成员口。

命令	作用
Ruijie(config)# **interface** *interface-type interface-number*	进入某二层接口。
Ruijie(config-if)# **port-group** *ap-number*	将二层接口加入 L2 AP。

通过 **port-group** 命令将二层接口加入一个 AP 时，如果该 AP 不存在，则同时创建这个 AP。

在接口配置模式下使用 **no port-group** 命令将此成员口退出 AP。

例：将二层的以太网接口 0/1 配置成二层 AP 5 的成员口（同时创建 AP5）。

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

将普通端口加入某个 AP 口后，当该端口再次从 ap 口退出时，普通端口上的原先相关的配置可能会恢复为缺省的配置。不同功能对 ap 口的成员的原有配置的处理方式有所不同，因此建议在端口从 ap 口退出后，应查看并确认端口的配置。

3.2.4 配置 Aggregate Port 的流量平衡

命令	作用
Ruijie(config)# **aggregateport load-balance** {**dst-mac** | **src-mac** | **src-dst-mac** | **dst-ip** | **src-ip** | **src-dst-ip** | **src-port** | **src-dst-ip-l4port** }	设置 AP 的流量平衡算法。缺省为 src -dst-mac。 dst-mac：根据输入报文的目的 MAC 地址进行流量分配。 src-mac：根据输入报文的源 MAC 地址进行流量分配。 src-dst-ip：根据源 IP 与目的 IP 进行流量分配。 dst-ip：根据输入报文的目的 IP 地址进行流量分配。 src-ip：根据输入报文的源 IP 地址进行流量分配。 src-dst-mac：根据源 MAC 与目的 MAC 进行流量分配。 src-port：根据输入报文的源端口号进行流量分配。 src-dst-ip-l4port：根据源 IP 与目的 IP 和源 L4 端口号与目的 L4 端口号进行流量分配。

要将 AP 的流量平衡设置恢复到缺省值，可以在全局配置模式下使用 **no aggregateport load-balance** 命令。

3.2.5 显示 Aggregate Port

命令	作用
Ruijie# **show aggregateport** [*ap-number*] { **load-balance** | **summary** }	显示 AP 设置。

例：显示 AP 设置

```
Ruijie# show aggregateport load-balance
Load-balance : Source MAC address
Ruijie#show aggregateport 1 summary
AggregatePort MaxPorts SwitchPort Mode   Ports
------------- -------- ---------- ------
Ag1           8        Enabled    ACCESS
```

4 链路聚合控制协议(LACP)

4.1 概述

IEEE 802.3ad 标准的 LACP(Link Aggregation Control Protocol, 链路聚合控制协议)是一个关于动态链路聚合的协议，它通过协议报文 LACPDU(Link Aggregation Control Protocol Data Unit, 链路聚合控制协议数据单元)和相连的设备交互信息。

当端口启用 LACP 协议后，端口通过发送 LACPDU 来通告自己的系统优先级，系统 MAC，端口的优先级，端口号和操作 key 等。相连设备收到该报文后，根据所存储的其他端口的信息，选择端口进行相应的聚合操作，从而可以使双方在端口退出或者加入聚合组上达到一致。

4.1.1 动态链路聚合的模式

端口有 3 种聚合模式：主动(Active)模式、被动模式(Passive)和静态模式。

其中主动模式的端口会主动发起 LACP 报文协商；被动模式的端口则只会对收到的 LACP 报文做应答；静态模式不会发出 LACP 报文进行协商，具体配置请参见静态 AP 配置指南的说明。各个聚合模式的相邻端口聚合模式要求如下：

端口模式	相邻端口聚合模式要求
主动模式	主动模式或者被动模式
被动模式	主动模式
静态模式	静态模式

4.1.2 LACP端口的状态

聚合组内的成员有可能处于 3 种状态：

- 当端口的链路状态处于 Down 时，端口不可能转发任何数据报文，显示为”down”状态。
- 端口链路处于 Up 状态，并经过 LACP 协商后，端口被置于聚合状态(端口被作为一个聚合组的一个成员参与聚合组的数据报文转发)，显示为“bndl”状态。
- 当端口链路处于 UP 状态，但是由于对端没有启用 LACP，或者因为端口属性和主端口不一致等一些因素导致经过报文协商端口被置于挂起状态（处于挂起状态的端口不参与数据报文转发），显示为“susp”状态。

只有全双工的端口才能进行聚合。

成员端口的速率、流控、介质类型以及成员端口的二、三层属性必须一致才能聚合。

端口聚合后修改端口的上述属性将导致同聚合组内的其他端口也无法聚合。

☑ 已经启用禁止成员口加入或者退出 AP 功能的端口不能启用 LACP；同时 LACP 成员口上不能启用禁止成员口加入或者退出 AP 功能。启用禁止成员口加入或者退出功能的 AP，不能被配置为 LACP AP；LACP AP 不能启用禁止成员口加入或者退出 AP 的功能。

☑ 由于外部功能限制而导致 LACP 退出 AP 失败时，会打印成员口退出 AP 失败的 SYSLOG（比如，端口 FastEthernet 0/1 退出 AP1 失败的 SYSLOG： “%LACP-5-UNBUNDLE_FAIL: Interface FastEthernet 0/1 failed to leave the AggregatePort 1”）。请修改配置，去掉禁止成员口退出 AP 的相关配置，否则会影响 AP 的正常报文传输。

4.2 动态链路聚合的优先级关系

4.2.1 LACP的系统ID

每台设备仅能配置一个 LACP 聚合系统。每个 LACP 聚合系统都有唯一的系统优先级。系统 ID 由 LACP 的系统优先级和设备 MAC 地址组成。系统优先级越小，系统 ID 的优先级越高；在系统优先级相同的情况下，比较设备的 MAC 地址，设备 MAC 地址越小，系统 ID 的优先级越高。系统 ID 优先级较高的系统决定端口状态，低优先级系统的端口状态随高优先级系统的端口状态变化而变化。

4.2.2 LACP的端口ID

每个端口有独立的 LACP 端口优先级，这是一个可配置的数值。端口 ID 由 LACP 的端口优先级和端口号组成。端口优先级数值越小，端口 ID 的优先级越高；在端口优先级相同的情况下，端口号越小，端口 ID 的优先级越高。

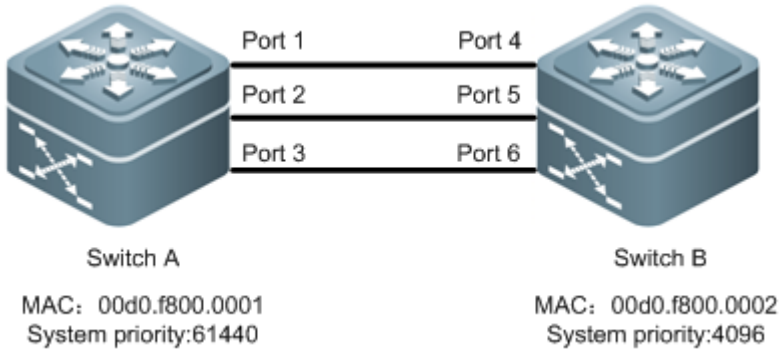
4.2.3 LACP的主端口

当有动态成员处于 up 状态时，LACP 会根据端口的速率，双工速率等关系，选择一个聚合组内端口 ID 优先级最高的端口作为主端口。只有和主端口属性相同的端口才能处于聚合状态，参与聚合组的数据转发。当端口的属性变化时，LACP 会重新选择主端口；当新的主端口不处于聚合状态时，LACP 会把同一个聚合组内的成员解聚合，重新聚合。

4.2.4 LACP的协商过程

在收到对端的 LACP 报文后，选取系统 ID 优先级比较高的系统。在系统 ID 优先级较高的一端，按照端口 ID 优先级从高到低的顺序，设置聚合组内端口的处于聚合状态。对端收到更新后的 LACP 报文后，也会把相应的端口设置成聚合状态。

图 1-1 LACP 协商



如上图所示，交换机 A 和交换机 B 通过 3 个端口连接在一起。设置交换机 A 的系统优先级为 61440，设置交换机 B 的系统优先级为 4096。在交换机 A，B 的 3 个直连端口上打开 LACP 链路聚合，设置 3 个端口的聚合模式为主动模式，设置 3 个端口的端口优先级为默认优先级 32768。

在收到对端的 LACP 报文后，交换机 B 发现自己的系统 ID 优先级比较高(交换机 B 的系统优先级比交换机 A 高)，于是按照端口 ID 优先级的顺序(端口优先级相同的情况下，按照端口号从小到大的顺序)设置端口 4，5，6 处于聚合状态。交换机 A 收到交换机 B 更新后的 LACP 报文后，发现对端的系统 ID 优先级比较高，并且把端口设置成聚合状态了，也把端口 1，2，3 设置成聚合状态了。

4.3 动态链路聚合的要求

动态链路聚合是 LACP 协议自动地添加和删除聚合组内的端口，两个端口被自动地聚合在一起有一定的要求。

- 只有相同的操作 key 才能被聚合在一起。
- 只有和主端口具有相同的速率和双工等基本属性的端口才能被动态聚合在一起。
- 端口链路处于 UP 状态，相连的端口启用 LACP，并且端口或者相连端口必须处于主动模式(Active)。

4.4 配置动态链路聚合(LACP)

你可以配置 LACP 的系统优先级，端口的优先级以及聚合组的管理 key。一台交换机所有的动态链路组只能有一个 LACP 系统优先级，修改这个值会影响到交换机上的所有聚合组。

在配置模式下,按如下步骤配置动态链路聚合：

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **lacp system-priority** *system-priority*	(可选)配置 LACP 系统的优先级，可选范围为 0-65535，默认优先级为 32768。
Ruijie(config)# **interface** *interface-id*	进入接口模式。
Ruijie(config-if)# **lacp port-priority** *port-priority*	(可选)配置端口的优先级,可选范围为 0-65535, 默认优先级为 32768。

Ruijie(config-if)# **port-group *key* mode active | passive**	把端口加入聚合组并指定端口的动态聚合模式，如果聚合组不存在，则会创建一个聚合组。 key 为聚合组的管理 key，key 取值范围根据不同产品支持的聚合组数量不同而变。 active 表示端口以主动模式加入动态聚合组，passive 表示端口以被动模式加入聚合组。
Ruijie(config-if)# **end**	退回特权模式。

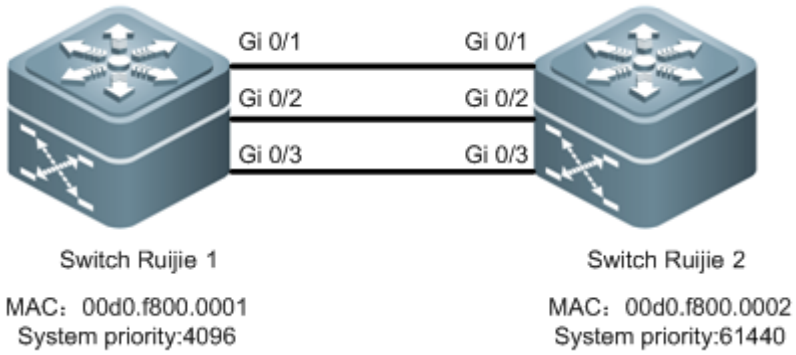
4.5 查看端口的动态链路聚合状态

在特权模式下使用如下命令来查看动态链路聚合的状态：

命令	作用
Ruijie# **show lacp summary [*key*]**	查看 LACP 系统的动态链路聚合状态.可指定显示特定聚合组的信息，参数 *key* 表示聚合组的 ID

4.6 LACP的配置用例

图 1-2 LACP 链路聚合



例如，如上图 2 所示拓扑，在交换机 Ruijie1 上设置 LACP 系统优先级为 4096,在端口 Gi 0/1、Gi 0/2、 Gi 0/3 上启用动态链路聚合协议，并设置端口的 LACP 端口优先级为 4096。

```
Ruijie1# configure terminal
Ruijie1(config)# lacp system-priority 4096
Ruijie1(config)# interface range GigabitEthernet 0/1-3
Ruijie1(config-if-range)# lacp port-priority 4096
Ruijie1(config-if-range)# port-group 3 mode active
Ruijie1(config-if-range)# end
```

在 Ruijie2 上设置 LACP 系统优先级为 61440，在端口 Gi 0/1、Gi 0/2、Gi 0/3 启用动态链路聚合协议，并设置端口的 LACP 端口优先级为 61440。

```
Ruijie2# configure terminal
Ruijie1(config)# lacp system-priority 61440
```

```
Ruijie2(config)# interface range GigabitEthernet 0/1-3
Ruijie2(config-if-range)# lacp port-priority 61440
Ruijie2(config-if-range)# port-group 3 mode active
Ruijie2(config-if-range)#end
```

配置完相关配置后，如果 LACP 协商成功，则会打印相应的 log：

```
*Feb 25 17:11:31: %LACP-5-BUNDLE: Interface Gi0/1 joined AggregatePort 3.
*Feb 25 17:11:32: %LACP-5-BUNDLE: Interface Gi0/2 joined AggregatePort 3.
*Feb 25 17:11:32: %LACP-5-BUNDLE: Interface Gi0/3 joined AggregatePort 3.
*Feb 25 17:11:32: %LINEPROTO-5-UPDOWN: Line protocol on Interface AggregatePort 3, changed state to up
```

表示端口 Gi 0/1、Gi 0/2、Gi 0/3 已经被成功地加入聚合组 3 了，这时在交换机 Ruijie1 上查看聚合组内成员口的状态。

```
Ruijie(config)#show LACP summary
Flags:  S - Device is requesting Slow LACPDUs
 F - Device is requesting Fast LACPDUs.
A - Device is in active mode.        P - Device is in passive mode.
Aggregate port 3:
Local information:
LACP port       Oper    Port     Port
Port     Flags     State     Priority        Key     Number  State
---------------------------------------------------------------
Gi0/1     SA        bndl        4096            0x3     0x1      0x3d
Gi0/2     SA        bndl        4096            0x3     0x2      0x3d
Gi0/3     SA        bndl        4096            0x3     0x3      0x3d
Partner information:
                    LACP port                   Oper    Port     Port
Port     Flags     Priority      Dev ID       Key     Number  State
---------------------------------------------------------------
Gi0/1     SA        61440     00d0.f800.0002   0x3     0x1     0x3d
Gi0/2     SA        61440     00d0.f800.0002   0x3     0x2     0x3d
Gi0/3     SA        61440     00d0.f800.0002   0x3     0x3     0x3d
```

其中，

“Local information”部分，显示的是本系统维护的端口的 LACP 信息。

“Port” 显示的是本系统内端口的 ID。

“Flags” 显示的是端口的一些状态标志：

‘S’标志着端口处于长超时状态，需要邻居慢速(每 30 秒发送一个)发送 LACPDU 报文。

‘F’标志着端口处于短超时状态，需要邻居快速(每秒发送一个) 发送 LACPDU 报文。

‘A’标志着端口是主动模式，‘P’标志着端口是被动模式。

“State” 显示的是端口状态：“bndl”标志着端口已经处于聚合状态了；其它状态说明参见前述“LACP 端口的状态”一节。

“LACP Port Priority” 显示的是端口的 LACP 优先级信息。

“Oper Key” 显示的是端口的操作 Key。

“Port Number” 显示的是端口的端口号。

“Port State” 显示的是端口的 LACP 协议状态。

“Partner infomation”部分，显示的是相连端口的 LACP 信息。

“Dev ID”部分显示的是端口相邻端口的系统 MAC 信息。

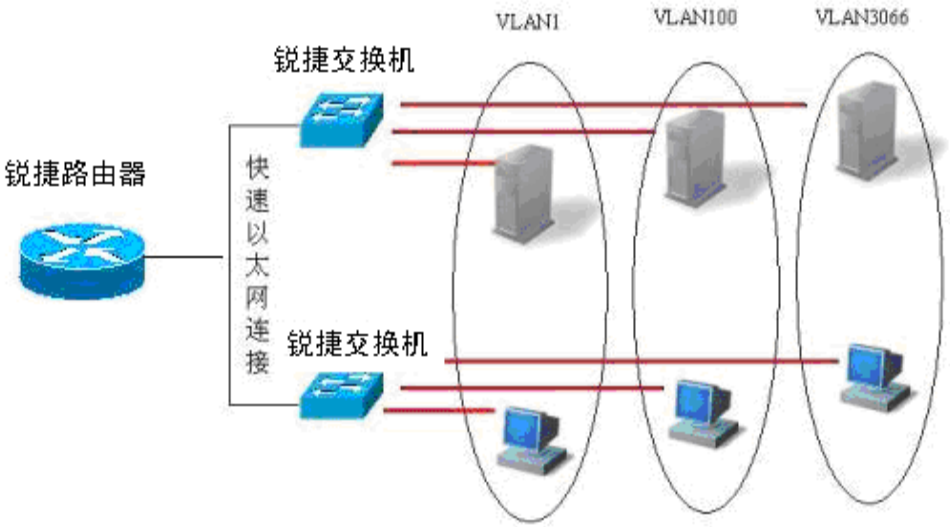
5 VLAN

5.1 概述

VLAN 是虚拟局域网（Virtual Local Area Network）的简称，它是在一个物理网络上划分出来的逻辑网络。这个网络对应于 ISO 模型的第二层网络。VLAN 的划分不受网络端口的实际物理位置的限制。VLAN 有着和普通物理网络同样的属性，除了没有物理位置的限制，它和普通局域网一样。第二层的单播、广播和多播帧在一个 VLAN 内转发、扩散，而不会直接进入其他的 VLAN 之中。所以，如果一个端口所连接的主机想要和其它不在同一个 VLAN 的主机通讯，则必须通过一个三层设备，见下图。

可以把一个端口定义为一个 VLAN 的成员，所有连接到这个特定端口的终端都是虚拟网络的一部分，并且整个网络可以支持多个 VLAN。当在 VLAN 中增加、删除和修改用户的时候，不必从物理上调整网络配置。

图 1-1



和一个物理网络一样，VLAN 通常和一个 IP 子网联系在一起。一个典型的例子是，所有在同一个 IP 子网中的主机属于同一个 VLAN，VLAN 之间的通讯必须通过三层设备。锐捷的三层设备可以通过 SVI 接口（Switch Virtual Interfaces）来进行 VLAN 之间的 IP 路由。关于 SVI 的配置，请见接口管理配置及 IP 单播路由配置。

5.1.1 支持的VLAN

产品支持的 VLAN 遵循 IEEE802.1Q 标准，最多支持 4094 个 VLAN(VLAN ID 1-4094)，其中 VLAN 1 是不可删除的默认 VLAN。

- 许可配置的 VLAN ID 范围为 1-4094
- 当硬件资源不足的情况下，系统将返回创建 VLAN 失败信息。

5.1.2 VLAN成员类型

可以通过配置一个端口的 VLAN 成员类型，来确定这个端口能通过怎样的帧，以及这个端口可以属于多少个 VLAN。关于 VLAN 成员类型的详细说明，请看下表：

命令	作用
Access	一个 Access 端口，只能属于一个 VLAN，并且是通过手工设置指定 VLAN 的。
Trunk（802.1Q）	一个 Trunk 口，在缺省情况下是属于本设备所有 VLAN 的，它能够转发所有 VLAN 的帧。也可以通过设置许可 VLAN 列表(Allowed-VLANs)来加以限制。

5.2 配置VLAN

一个 VLAN 是以 VLAN ID 来标识的。在设备中，用户可以添加、删除、修改 VLAN 2-4094，而 VLAN 1 是由设备自动创建，并且不可被删除。

可以在接口配置模式下配置一个端口的 VLAN 成员类型或加入、移出一个 VLAN。

5.2.1 VLAN配置信息的保存

当用户在特权命令模式下输入 **copy running-config startup-config** 命令后，VLAN 的配置信息便被保存进配置文件。要查看 VLAN 配置信息，可以使用 **show vlan** 命令。

5.2.2 缺省的VLAN配置

参数	缺省值	范围
VLAN ID	1	1－4094
VLAN Name	VLAN xxxx，xxxx 是 VLAN ID 数	无范围
VLAN State	Active	Active，Inactive

5.2.3 创建、修改一个VLAN

在全局配置模式下，用户可以创建或者修改一个 VLAN：

命令	作用
Ruijie(config)# **vlan** *vlan-id*	输入一个 VLAN ID。如果输入的是一个新的 VLAN ID，则设备会创建一个 VLAN，如果输入的是已经存在的 VLAN ID，则修改相应的 VLAN。
Ruijie(config-vlan)# **name** *vlan-name*	（可选）为 VLAN 取一个名字。如果没有进行这一步，则设备会自动为它起一个名字 VLAN xxxx，其中 xxxx 是用 0 开头的四位 VLAN ID 号。比如，VLAN 0004 就是 VLAN 4 的缺省名字。

如果用户想把 VLAN 的名字改回缺省名字，只需输入 **no name** 命令即可。

下面是一个创建 VLAN 888，将它命名为 Test888 的例子：

```
Ruijie# configure terminal
```

```
Ruijie(config)# vlan 888
Ruijie(config-vlan)# name test888
Ruijie(config-vlan)# end
```

5.2.4 删除一个VLAN

缺省 VLAN（VLAN 1）不允许删除。

在全局配置模式下删除一个已存在的 VLAN：

命令	作用
Ruijie(config)# **no vlan** *vlan-id*	输入一个 VLAN ID，删除它。

5.2.5 将当前Access口加入到指定VLAN

如果把一个接口分配给一个不存在的 VLAN，那么这个 VLAN 将自动被创建。

在接口配置模式下，将一个端口分配给一个 VLAN：

命令	作用
Ruijie(config-if)# **switchport mode access**	定义该接口的 VLAN 成员类型（二层 ACCESS 口）
Ruijie(config-if)# **switchport access vlan** *vlan-id*	将这个口分配给一个 VLAN

下面这个例子把 **GigabitEthernet** 0/10 作为 Access 口加入了 VLAN20：

```
Ruijie# configure terminal
Ruijie(config)# interface GigabitEthernet 0/10
Ruijie(config-if)# switchport mode access
Ruijie(config-if)# switchport access vlan 20
Ruijie(config-if)# end
```

下面这个例子显示了如何检查配置是否正确：

```
Ruijie# show interface GigabitEthernet 0/10 switchport
Interface         Switchport   Mode  Access Native Protected  VLAN lists
----------        --------     -----  ----- ------ ---------- -------
GigabitEthernet 0/10 enabled  ACCESS  20      1    Disabled  ALL
```

5.2.6 向当前VLAN添加Access口

在 VLAN 配置模式下，将指定的 Access 口加入该 VLAN。该命令的配置效果同在接口模式下指定该接口所属 VLAN 的命令（即 **switchport access vlan** *vlan-id*）效果一致。

命令	作用
Ruijie(config)# **vlan** *vlan-id*	输入一个 VLAN ID。如果输入的是一个新的 VLAN ID，则设备会创建一个 VLAN，如果输入的是已经存在的 VLAN ID，则修改相应的 VLAN。

Ruijie(config-vlan)# **add interface** { *interface-id* | **range** *interface-range* }	向当前 VLAN 中添加一个或一组 Access 接口。 缺省情况下，所有二层以太网口都属于 VLAN1
Ruijie(config-vlan)# ［**no**］**add interface** { *interface-id* | **range** *interface-range* }	从当前 VLAN 中删除一个或一组 Access 接口
Ruijie(config-vlan)#**show interface** *interface-id* **switchport**	查看二层接口信息

该命令只对 Access 口有效

对于两种形式的接口加入 VLAN 命令，配置生效的原则是后配置的命令覆盖前面配置的命令

下面这个例子把 Access 口 (GigabitEthernet 0/10)添加到 VLAN20：

```
Ruijie# configure terminal
SwitchA(config)#vlan 20
SwitchA(config-vlan)#add interface GigabitEthernet 0/10
```

下面这个例子显示了如何检查配置是否正确：

```
Ruijie# show interface GigabitEthernet 0/10 switchport
Interface         Switchport   Mode  Access Native Protected  VLAN lists
----------        --------     -----  ----- ------ ---------- -------
GigabitEthernet 0/10 enabled  ACCESS  20      1    Disabled   ALL
```

5.2.7 配置Dot1qVlanCurrentEntry表中的MIB节点dot1qVlanIndex的访问权限

在全局配置模式下，用户可以修改 Dot1qVlanCurrentEntry 表中的 MIB 节点 dot1qVlanIndex 的最大访问权限：

命令	作用
Ruijie(config)# **dot1q-vlan-current-entry mib dot1q-vlan-index max-access mode read-only**	修改 Dot1qVlanCurrentEntry 表中的 MIB 节点 dot1qVlanIndex 的最大访问权限为“只读”模式。配置该命令后，MIB 节点 dot1qVlanIndex 支持通过 SNMP 软件进行读取操作。

如果用户需要将 MIB 节点 dot1qVlanIndex 的最大访问权限恢复到缺省的“禁止访问”模式，只需输入 **no dot1q-vlan-current-entry mib dot1q-vlan-index max-access mode** 命令即可。

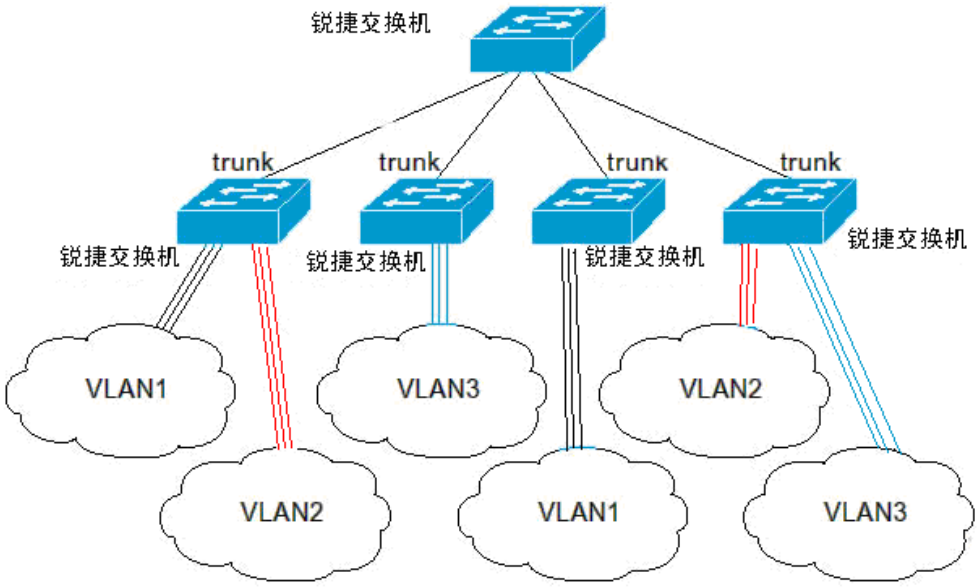
5.3 配置VLAN Trunks

5.3.1 Trunking概述

一个 Trunk 是将一个或多个以太网交换接口和其他的网络设备（如路由器或交换机）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 1-2



用户可以把一个普通的以太网端口，或者一个 Aggregate Port 设为一个 Trunk 口（关于 Aggregate Port 的详细说明，请见配置 Aggregate Port）。

如果要把一个接口在 ACCESS 模式和 TRUNK 模式之间切换，请用 **switchport mode** 命令：

命令	作用
Ruijie(config-if)# **switchport mode access**	将一个接口设置成为 Access 模式
Ruijie(config-if)# **switchport mode trunk**	将一个接口设置成为 Trunk 模式

必须为 Trunk 口指定一个 Native VLAN。所谓 Native VLAN，就是指在这个接口上收发的 UNTAG 报文，都被认为是属于这个 VLAN 的。显然，这个接口的缺省 VLAN ID（即 IEEE 802.1Q 中的 PVID）就是 Native VLAN 的 VLAN ID。同时，在 Trunk 上发送属于 Native VLAN 的帧，则必然采用 UNTAG 的方式。每个 Trunk 口的缺省 Native VLAN 是 VLAN 1。

在配置 Trunk 链路时，请确认连接链路两端的 Trunk 口使用相同的 Native VLAN。

5.3.2 配置一个Trunk口

Trunk 口基本配置

在接口配置模式下，可以将一个接口配置成一个 Trunk 口。

命令	作用
Ruijie(config-if)# **switchport mode trunk**	定义该接口的类型为二层 Trunk 口
Ruijie(config-if)# **switchport trunk native vlan** *vlan-id*	为这个口指定一个 Native VLAN

如果想把一个 Trunk 口的所有 Trunk 相关属性都复位成缺省值，请使用 **no switchport mode** 配置命令。

5.3.3 定义Trunk口的许可VLAN列表

一个 Trunk 口缺省可以传输本设备支持的所有 VLAN（1－4094）的流量。但是，用户也可以通过设置 Trunk 口的许可 VLAN 列表来限制某些 VLAN 的流量不能通过这个 Trunk 口。

在接口配置模式下，可以修改一个 Trunk 口的许可 VLAN 列表。

命令	作用
Ruijie(config-if)# **switchport trunk allowed vlan** {**all** | [**add** | **remove** | **except**] } *vlan-list*	（可选）配置这个 Trunk 口的许可 VLAN 列表。参数 *vlan-list* 可以是一个 VLAN，也可以是一系列 VLAN，以小的 VLAN ID 开头，以大的 VLAN ID 结尾，中间用-号连接。如：10–20。 all 的含义是许可 VLAN 列表包含所有支持的 VLAN； add 表示将指定 VLAN 列表加入许可 VLAN 列表； remove 表示将指定 VLAN 列表从许可 VLAN 列表中删除； except 表示将除列出的 VLAN 列表外的所有 VLAN 加入许可 VLAN 列表；

如果想把 Trunk 的许可 VLAN 列表改为缺省的许可所有 VLAN 的状态，请使用 **no switchport trunk allowed vlan** 接口配置命令。

下面是一个把 VLAN 2 从端口 FastEthernet 1/15 的许可列表中移出的例子：

```
Ruijie(config)# interface fastethernet 1/15
Ruijie(config-if)# switchport trunk allowed vlan remove 2
Ruijie(config-if)# end
Ruijie# show interfaces fastethernet 1/15 switchport
Interface Switchport Mode  Access Native Protected VLAN lists
--------- ---------- ----  ------ ------ -------- ----------
Fa1/15     enabled    TRUNK  1      1     Disabled   1,3－4094
```

5.3.4 配置Native VLAN

一个 Trunk 口能够收发 TAG 或者 UNTAG 的 802.1Q 帧。其中 UNTAG 帧用来传输 Native VLAN 的流量。缺省的 Native VLAN 是 VLAN 1。

在接口配置模式下，可以为一个 Trunk 口配置 Native VLAN。

命令	作用
Ruijie(config-if)# **switchport trunk native vlan** *vlan-id*	配置 Native VLAN

如果想把 Trunk 的 Native VLAN 列表改回缺省的 VLAN 1，请使用 **no switchport trunk native vlan** 接口配置命令。

如果一个帧带有 Native VLAN 的 VLAN ID，在通过这个 Trunk 口转发时，会自动被剥去 TAG。

把一个接口的 Native VLAN 设置为一个不存在的 VLAN 时，设备不会自动创建此 VLAN。此外，一个接口的 Native VLAN 可以不在接口的许可 VLAN 列表中。此时，Native VLAN 的流量不能通过该接口。

5.3.5 显示VLAN

在特权模式下，才可以查看 VLAN 的信息。显示的信息包括 VLAN VID、VLAN 状态、VLAN 成员端口以及 VLAN 配置信息。以下罗列了相关的显示命令：

命令	作用
show vlan [*vlan-id*]	显示所有或指定 VLAN 的参数

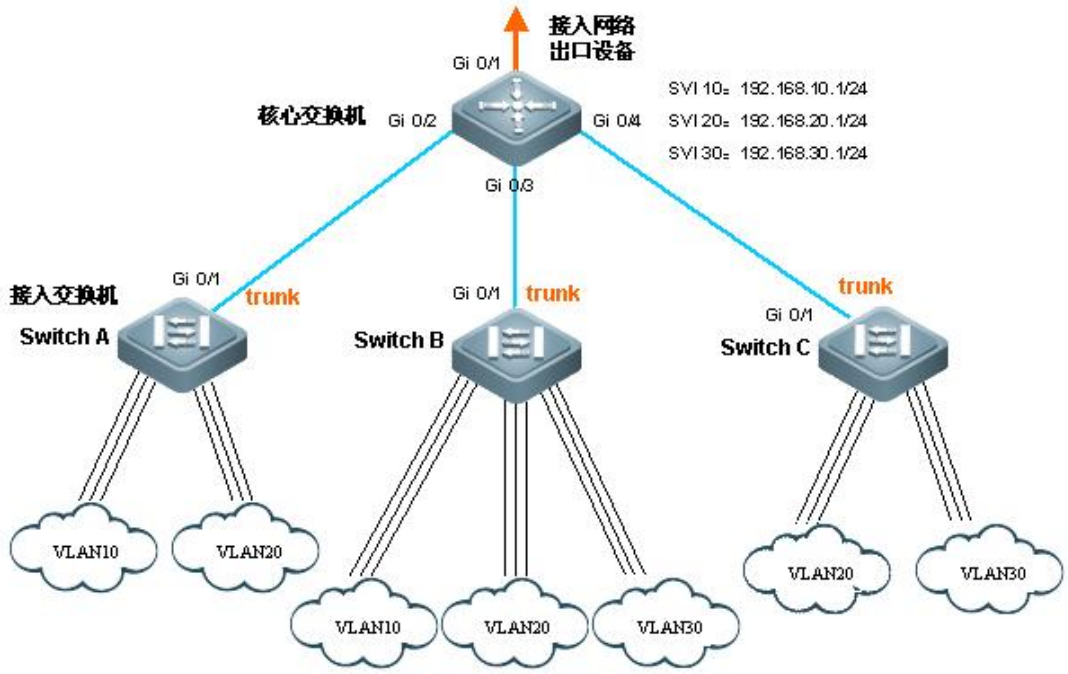
下面是一个显示 VLAN 的例子：

```
Ruijie# show vlan
VLAN Name                              Status    Ports
---------- ----------- ---------- ---------- ----------
   1 VLAN0001        STATIC    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                  Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                  Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                  Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                  Fa0/17, Fa0/19, Fa0/20, Fa0/21
                                  Fa0/22, Fa0/23, Fa0/24, Gi0/25
                                  Gi0/26, Gi0/27, Gi0/28
   2 VLAN0002        STATIC    Fa0/1, Fa0/2, Fa0/3
   3 VLAN0003        STATIC    Fa0/1, Fa0/2, Fa0/3
   4 VLAN0004        STATIC    Fa0/1, Fa0/2, Fa0/3
   5 VLAN0005        STATIC    Fa0/1, Fa0/2, Fa0/3
   6 VLAN0006        STATIC    Fa0/1, Fa0/2, Fa0/3
```

5.4 配置举例

组网拓扑

图 1-3



组网需求

如上图所示，某用户内网被划分为 VLAN 10、VLAN 20、VLAN 30，以实现相互间的 2 层隔离；3 个 VLAN 对应的 IP 子网分别为 192.168.10.0/24、192.168.20.0/24、192.168.30.0/24，3 个 VLAN 通过 3 层核心交换机的 IP 转发能力实现子网互连。

配置要点

本用例以核心交换机和 1 台接入交换机为例说明配置过程。要点如下：

- 在核心交换机配置 3 个 VLAN，配置下连接入交换机的端口为 trunk 口，并指定许可 vlan 列表，实现 2 层隔离；
- 在核心交换机配置 3 个 SVI 口，分别作为 3 个 VLAN 对应 IP 子网的网关接口，配置对应的 IP 地址；
- 分别在 3 台接入交换机创建 VLAN，为各 VLAN 分配 Access 口，指定上连核心交换机的 trunk 口。本用例以接入交换机 Switch A 为例说明配置步骤。

配置步骤

- 核心交换机上的配置

创建 VLAN

进入全局配置模式

```
Ruijie#configure terminal
```

创建 VLAN 10

```
Ruijie(config)#vlan 10
```

创建 VLAN 20

```
Ruijie(config-vlan)#vlan 20
```

创建 VLAN 30

```
Ruijie(config-vlan)#vlan 30
```

退回到全局配置模式

```
Ruijie(config-vlan)#exit
```

配置各下连 trunk 口，指定许可 vlan 列表

进入端口范围 Gi 0/2-4

```
Ruijie(config)#interface range GigabitEthernet 0/2-4
```

配置该端口 Gi 0/2-4 都为 trunk 口

```
Ruijie(config-if-range)#switchport mode trunk
```

退回到全局配置模式

```
Ruijie(config-if-range)#exit
```

进入端口 Gi 0/2

```
Ruijie(config)#interface GigabitEthernet 0/2
```

将所有 vlan 从该端口的许可 vlan 中删除

```
Ruijie(config-if)#switchport trunk allowed vlan remove 1-4094
```

重新添加该端口的许可 vlan 为 10、20

```
Ruijie(config-if)#switchport trunk allowed vlan add 10,20
```

进入端口 Gi 0/3

```
Ruijie(config-if)#interface GigabitEthernet 0/3
```

将所有 vlan 从该端口的许可 vlan 中删除

```
Ruijie(config-if)#switchport trunk allowed vlan remove 1-4094
```

重新添加该端口的许可 vlan 为 10、20、30

```
Ruijie(config-if)#switchport trunk allowed vlan add 10,20,30
```

进入端口 Gi 0/4

```
Ruijie(config-if)#interface GigabitEthernet 0/4
```

将所有 vlan 从该端口的许可 vlan 中删除

```
Ruijie(config-if)#switchport trunk allowed vlan remove 1-4094
```

重新添加该端口的许可 vlan 为 20、30

```
Ruijie(config-if)#switchport trunk allowed vlan add 20,30
```

退回到全局配置模式

```
Ruijie(config-if)#exit
```

在核心交换机上查看 vlan 配置

查看 vlan 信息，包括 vlan id、名称、状态、包括的端口

```
Ruijie#show vlan
VLAN  Name       Status                Ports
---- --------  --------   --------------------------------
   1 VLAN0001   STATIC     Gi0/1, Gi0/5, Gi0/6, Gi0/7
                           Gi0/8, Gi0/9, Gi0/10, Gi0/11
                           Gi0/12, Gi0/13, Gi0/14, Gi0/15
                           Gi0/16, Gi0/17, Gi0/18, Gi0/19
                           Gi0/20, Gi0/21, Gi0/22, Gi0/23
                           Gi0/24
  10 VLAN0010  STATIC      Gi0/2, Gi0/3
  20 VLAN0020  STATIC      Gi0/2, Gi0/3, Gi0/4
  30 VLAN0030  STATIC      Gi0/3, Gi0/4
```

查看端口 Gi 0/2 的 vlan 状态

```
Ruijie#show interface GigabitEthernet 0/2 switchport
Interface Switchport Mode  Access Native Protected VLAN lists
--------- ----------- -----  ------ ------ --------- ---------
Gi0/2      enabled   TRUNK    1       1      Disabled  10,20
```

查看端口 Gi 0/3 的 vlan 状态

```
Ruijie#show interface GigabitEthernet 0/3 switchport
Interface Switchport Mode  Access Native Protected VLAN lists
--------- ----------- -----  ------ ------ --------- -----------
Gi0/3      enabled   TRUNK    1       1      Disabled  10,20,30
```

查看端口 Gi 0/4 的 vlan 状态

```
Ruijie#show interface GigabitEthernet 0/4 switchport
Interface Switchport Mode  Access Native Protected VLAN lists
--------- ----------- -----  ------ ------ --------- -----------
Gi0/4      enabled   TRUNK    1       1      Disabled  20,30
```

创建 SVI 口，指定 IP 地址

进入全局配置模式

```
Ruijie#configure terminal
```

创建 SVI 10

```
Ruijie(config)#interface vlan 10
```

配置 SVI 10 的 IP 地址

```
Ruijie(config-if)#ip address 192.168.10.1 255.255.255.0
```

创建 SVI 20

```
Ruijie(config-if)#interface vlan 20
```

配置 SVI 20 的 IP 地址

```
Ruijie(config-if)#ip address 192.168.20.1 255.255.255.0
```

创建 SVI 30

```
Ruijie(config-if)#interface vlan 30
```

配置 SVI 30 的 IP 地址

```
Ruijie(config-if)#ip address 192.168.30.1 255.255.255.0
```

退回到全局配置模式

```
Ruijie(config-if)#exit
```

- 接入交换机 Switch A 上的配置

创建 VLAN

进入全局配置模式

```
Ruijie#configure terminal
```

创建 VLAN 10

```
Ruijie(config)#vlan 10
```

创建 VLAN 20

```
Ruijie(config-vlan)#vlan 20
```

退回到全局配置模式

```
Ruijie(config-vlan)#exit
```

- 为各 VLAN 分配 Access 口

进入端口范围 Gi 0/2-12

```
Ruijie(config)#interface range GigabitEthernet 0/2-12
```

将端口 Gi 0/2-12 配置为 Access 口

```
Ruijie(config-if)#switchport mode access
```

将端口 Gi 0/2-12 分配给 VLAN 10

```
Ruijie(config-if)#switchport access vlan 10
```

进入端口范围 Gi 0/13-24

```
Ruijie(config-if)#interface range GigabitEthernet 0/13-24
```

将端口 Gi 0/13-24 配置为 Access 口

```
Ruijie(config-if)#switchport mode access
```

将端口 Gi 0/13-24 分配给 VLAN 20

```
Ruijie(config-if)#switchport access vlan 20
```

退回到全局配置模式

```
Ruijie(config-if)#exit
```

指定上连核心交换机的 trunk 口

进入端口 Gi 0/1

```
Ruijie(config)#interface GigabitEthernet 0/1
```

配置该端口 Gi 0/1 都为 trunk 口

```
Ruijie(config-if)#switchport mode trunk
```

退回到全局配置模式

```
Ruijie(config-if)#exit
```

6 Private VLAN

6.1 Private VLAN技术

服务提供商如果给每个用户一个 VLAN，则由于一台设备支持的 VLAN 数最大只有 4096 而限制了服务提供商能支持的用户数；在三层设备上，每个 VLAN 被分配一个子网地址或一系列地址，这种情况导致 IP 地址的浪费，一种解决方法就是应用 Private VLAN 技术。

私有 VLAN(Private VLAN)将一个 VLAN 的二层广播域划分成多个子域，每个子域都由一个私有 VLAN 对组成：主 VLAN(Primary VLAN)和辅助 VLAN(Secondary VLAN)。

一个私有 VLAN 域可以有多个私有 VLAN 对，每一个私有 VLAN 对代表一个子域。在一个私有 VLAN 域中所有的私有 VLAN 对共享同一个主 VLAN。每个子域的辅助 VLAN ID 不同。

一个私有 VLAN 域中只有一个主 VLAN，辅助 VLAN 实现同一个私有 VLAN 域中的二层隔离，有两种类型的辅助 VLAN：

- 隔离 VLAN(Isolated VLAN)：同一个隔离 VLAN 中的端口不能互相进行二层通信。一个私有 VLAN 域中只有一个隔离 VLAN。
- 群体 VLAN(Community VLAN)：同一个群体 VLAN 中的端口可以互相进行二层通信，但不能与其它群体 VLAN 中的端口进行二层通信。一个私有 VLAN 域中可以有多个群体 VLAN。

混杂端口（Promiscuous Port），属于主 VLAN 中的端口，可以与任意端口通讯，包括同一个私有 VLAN 域中辅助 VLAN 的隔离端口和群体端口。

混杂 TRUNK 端口（Promiscuous Trunk Port），可以同时是多个普通 VLAN 和多个私有 VLAN 的成员端口，可以和同一 VLAN 内的任意端口通讯。在普通 VLAN 中，报文转发遵循 802.1Q 规则，在私有 VLAN 中，从混杂 TRUNK 端口转发出的带 TAG 报文，其 VID 如果是辅助 VLAN ID，会转成相应主 VLAN 的 VID 后，再输出。

隔离端口(Isolated Port)，隔离 VLAN 中的端口，只能与混杂口通讯。隔离端口接收到的报文可允许转发到 Trunk Port，但 Trunk Port 接收到 vid 是隔离 VLAN 的报文不能向隔离端口转发。

隔离 TRUNK 端口（Isolated Trunk Port），可以同时是多个普通 VLAN 和多个 PVLAN 的成员端口。在隔离 VLAN 中，只能与混杂口通讯；在群体 VLAN 中，可以与同一个群体 VLAN 的群体端口通讯，也可以同混杂口通讯；在普通 VLAN 中，遵循 802.1Q 规则。隔离 TRUNK 端口接收到的隔离 VLAN ID 的报文可允许转发到 Trunk Port，但 Trunk Port 接收到 vid 是隔离 VLAN 的报文不能向隔离端口转发。

从隔离 TRUNK 端口转发出的带 TAG 报文，其 VID 如果是主 VLAN ID，会转成相应辅助 VLAN 的 VID 后，再输出。

群体端口(Community port)，属于群体 VLAN 中的端口，同一个群体 VLAN 的群体端口可以互相通讯，也可以与混杂口通讯。不能与其它群体 VLAN 中的群体端口及隔离 VLAN 中的隔离端口通讯。

各种端口类型间的报文转发关系：

输出端口 / 输入端口	混杂端口	隔离端口	群体端口	隔离 TRUNK 端口(同 VLAN 内)	混杂 TRUNK 端口(同 VLAN 内)	TRUNK 端口（同 VLAN 内）
混杂端口	通	通	通	通	通	通
隔离端口	通	不通	不通	不通	通	通
群体端口	通	不通	通	通	通	通

隔离TRUNK端口(同VLAN 内)	通	不通	通	不通（隔离 VLAN 内不通，非隔离 VLAN 内通）	通	通
混杂TRUNK端口(同VLAN 内)	通	通	通	通	通	通
TRUNK 端口（同VLAN 内）	通	不通	通	不通（隔离 VLAN 内不通，非隔离 VLAN 内通）	通	通

各种端口类型间的报文转发后 VLAN TAG 变化关系：

输出端口 / 输入端口	混杂端口	隔离端口	群体端口	隔离 TRUNK 端口（同 VLAN 内）	混杂 TRUNK 端口（同 VLAN 内）	TRUNK 端口（同 VLAN 内）
混杂端口	不变	不变	不变	加上辅助 VLAN ID	加上主 VLAN ID TAG，其它非私有 VLAN 内不变。	加上主 VLAN ID TAG
隔离端口	不变	NA	NA	NA	加上主 VLAN ID TAG，其它非私有 VLAN 内不变。	加上隔离 VLAN ID TAG
群体端口	不变	NA	不变	加上群体 VLAN ID TAG	加上主 VLAN ID TAG，其它非私有 VLAN 内不变。	加上群体 VLAN ID TAG
隔离 TRUNK 端口（同 VLAN 内）	去掉 VLAN TAG	NA	去掉 VLAN TAG	非隔离 VLAN 内不变。	加上主 VLAN ID TAG，其它非私有 VLAN 内不变。	不变
混杂 TRUNK 端口（同 VLAN 内）	去掉 VLAN TAG	不变	不变	加上辅助 VLAN ID	加上主 VLAN ID TAG，其它非私有 VLAN 内不变。	不变
TRUNK 端口(同VLAN 内)	去掉 VLAN TAG	NA	去掉 VLAN TAG	主 VLAN 内转成辅助 VLAN ID，其它非隔离 VLAN 内不变。	加上主 VLAN ID TAG，其它非私有 VLAN 内不变。	不变
交换机 CPU	Untag	Untag	Untag	加上辅助 VLAN ID TAG	加上主 VLAN ID TAG，其它非私有 VLAN 内不变。	加上主 VLAN ID TAG

私有 VLAN 中，只有主 VLAN 可以创建 SVI 接口，辅助 VLAN 不可以创建 SVI。

私有 VLAN 中的端口可以为 SPAN 源端口，不可以为镜像目的端口。

6.2 Private VLAN配置

6.2.1 缺省Private VLAN设置

缺省情况下，没有 Private VLAN 的配置

6.2.2 配置VLAN作为私有VLAN

配置方法如下命令

命令	说明
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **vlan** *vid*	进入 VLAN 配置模式
Ruijie(config-vlan)# **private-vlan**{**community** | **isolated**| **primary**}	配置私有 VLAN 类型
Ruijie(config-vlan)# **no private-vlan**{**community** | **isolated** | **primary**}	取消私有 VLAN 配置
Ruijie(config-vlan)# **end**	退出 VLAN 模式
Ruijie# **show vlan private-vlan** [*type*]	显示私有 VLAN

在 802.1Q Vlan 中具有成员口情况不能声明为私有 VLAN,VLAN 1 不能声明为私有 VLAN,对于具有 Trunk 口或 Uplink 口的 802.1Q VLAN 中，先将该 VLAN 从许可 VLAN 列表中删除，对 Private VLAN 处于 ACTIVE 状态必须满足以下条件：1）具有 Priamry VLAN；2）具有 Secondary VLAN；3）Secondary VLAN 与 Primary VLAN 关联

以下命令将 802.1Q VLAN 配置为 Private VLAN：

```
Ruijie# configure terminal
Ruijie(config)# vlan 303
Ruijie(config-vlan)# private-vlan community
Ruijie(config-vlan)# end
Ruijie# show vlan private-vlan community
VLAN Type  Status    Routed   Interface   Associated VLANs
---- ----  --------  ------   ---------   ------------------
303 comm   inactive  Disabled              no association
Ruijie# configure terminal
Ruijie(config)# vlan 404
Ruijie(config-vlan)# private-vlan isolated
Ruijie(config-vlan)# end
Ruijie# show vlan private-vlan
VLAN Type  Status    Routed   Interface   Associated VLANs
---- ----  --------  ------   ---------   ------------------
303 comm  inactive  Disabled              no association
404 isol  inactive  Disabled              no association
```

6.2.3 关联Secondary VLAN和Primary VLAN

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

命令	说明
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **vlan** *p_vid*	进入 Primary VLAN 配置模式
Ruijie(config-vlan)# **private-vlan association** {*svlist* | **add** *svlist* | **remove** *svlist*}	关联 Secondary VLAN

Ruijie(config-vlan)# **no private-vlan association**	清除与所有 Secondary VLAN 的关联
Ruijie(config-vlan)# **end**	退出 VLAN 模式
Ruijie# **show vlan private-vlan** [*type*]	显示私有 VLAN

举例如下：

```
Ruijie# configure terminal
Ruijie(config)# vlan 202
Ruijie(config-vlan)# private-vlan association 303-307,309,440
Ruijie(config-vlan)# end
Ruijie# show vlan private-vlan
VLAN Type  Status    Routed   Interface   Associated VLANs
---- ----  --------  ------   ---------   ------------------
202 prim  inactive  Disabled              303-307,309,440
303 comm  inactive  Disabled              202
304 comm  inactive  Disabled              202
305 comm  inactive  Disabled              202
306 comm  inactive  Disabled              202
307 comm  inactive  Disabled              202
309 comm  inactive  Disabled              202
440 comm  inactive  Disabled              202
```

该操作在声明为 Primary VLAN 的 VLAN 配置模式进行。

6.2.4 映射Secondary VLAN和Primary VLAN的三层接口

您可以通过下面的设置步骤来完成：

命令	说明
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **interface vlan** *p_vid*	进入 Primary VLAN 的接口模式
Ruijie(config-if)# **private-vlan mapping** {*svlist* | **add** *svlist* | **remove** *svlist*}	映射 Secondary VLAN 到 Primary VLAN 的 SVI 三层交换。
Ruijie(config-if)# **end**	退出接口模式

下面例子配置 Secondary VLAN 路由：

```
Ruijie# configure terminal
Ruijie(config)# interface vlan 202
Ruijie(config-if)# private-vlan mapping add 303-307,309,440
Ruijie(config-if)# end
```

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

6.2.5 配置二层接口作为私有VLAN的主机端口

按照以下步骤配置二层接口作为私有 VLAN 的主机端口(Host Port)：

命令	说明
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **interface** *interface-id*	进入接口配置模式 *fastethernet*, *gigabitethernet*, *tengigabitethernet*
Ruijie(config-if)# **switchport mode private-vlan host**	配置为二层交换模式
Ruijie(config-if)# **no switchport mode**	清除私有 VLAN 配置
Ruijie(config-if)# **switchport private-vlan host-association** *p_vid s_vid*	关联二层口与私有 VLAN
Ruijie(config-if)# **no switchport private-vlan host-association**	清除关联

举例如下：

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/2
Ruijie(config-if)# switchport mode private-vlan host
Ruijie(config-if)# switchport private-vlan host-association 202 203
Ruijie(config-if)# end
```

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

6.2.6 配置二层接口作为PVLAN 隔离TRUNK端口

配置二层接口作为隔离 PVLAN TRUNK 端口，通过以下操作命令：

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config-if)# **interface** *interface-id*	进入接口配置模式 *fastethernet*, *gigabitethernet*, *tengigabitethernet*
Ruijie(config-if)# **switchport mode trunk**	配置为 trunk 模式
Ruijie(config-if)# **switchport private-vlan association trunk** *p_vid s_vid*	关联二层口与私有 VLAN，允许配置多对。p_vid 和 s_vid 参数分别是主 VLAN ID 和辅助 VLAN ID。
Ruijie(config-if)# **no switchport private-vlan association trunk** *p_vid s_vid*	清除关联
Ruijie(config-if)# **switchport trunk allowed vlan** {**all** | [**add** | **remove** | **except**] } *vlan-list*	（可选）配置这个 Trunk 口的许可 VLAN 列表。参数 *vlan-list* 可以是一个 VLAN，也可以是一系列 VLAN，以小的 VLAN ID 开头，以大的 VLAN ID 结尾，中间用-号连接。如：10–20。 all 的含义是许可 VLAN 列表包含所有支持的 VLAN； add 表示将指定 VLAN 列表加入许可 VLAN 列表；

	remove 表示将指定 VLAN 列表从许可 VLAN 列表中删除； except 表示将除列出的 VLAN 列表外的所有 VLAN 加入许可 VLAN 列表；
Ruijie(config-if)# **switchport trunk native vlan** *vlan-id*	配置 Native VLAN 如果想把 Trunk 的 Native VLAN 列表改回缺省的 VLAN 1，请使用 no switchport trunk native vlan 接口配置命令。

举例如下：

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/2
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# switchport private-vlan association trunk 202 203
Ruijie(config-if)# switchport trunk allowed vlan 100
Ruijie(config-if)# switchport trunk native vlan 100
Ruijie(config-if)# end
```

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

6.2.7 配置二层接口作为混杂TRUNK端口

配置二层接口作为混杂 PVLAN TRUNK 端口，通过以下操作命令：

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config-if)# **interface** *interface-id*	进入接口配置模式 *fastethernet*, *gigabitethernet*, *tengigabitethernet*
Ruijie(config-if)# **switchport mode trunk**	配置为 trunk 模式
Ruijie(config-if)# **switchport private-vlan promiscuous trunk** *p_vid s_list*	关联二层口与私有 VLAN，允许配置多对。p_vid 和 s_list 参数分别是主 VLAN ID 和辅助 VLAN ID 列表。
Ruijie(config-if)# **no switchport private-vlan promiscuous trunk** *p_vid s_list*	清除关联
Ruijie(config-if)# **switchport trunk allowed vlan** {**all** | [**add** | **remove** | **except**] } *vlan-list*	（可选）配置这个 Trunk 口的许可 VLAN 列表。参数 *vlan-list* 可以是一个 VLAN，也可以是一系列 VLAN，以小的 VLAN ID 开头，以大的 VLAN ID 结尾，中间用-号连接。如：10–20。 all 的含义是许可 VLAN 列表包含所有支持的 VLAN； add 表示将指定 VLAN 列表加入许可 VLAN 列表； remove 表示将指定 VLAN 列表从许可 VLAN 列表中删除； except 表示将除列出的 VLAN 列表外的所有 VLAN 加入许可 VLAN 列表；
Ruijie(config-if)# **switchport trunk native vlan** *vlan-id*	配置 Native VLAN 如果想把 Trunk 的 Native VLAN 列表改回缺省的 VLAN 1，请使用 no switchport trunk native vlan 接口配置命令。

举例如下：

```
Ruijie# configure terminal
```

```
Ruijie(config)# interface gigabitEthernet 0/2
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# switchport private-vlan promiscuous trunk 202 203
Ruijie(config-if)# switchport trunk allowed vlan 100
Ruijie(config-if)# switchport trunk native vlan 100
Ruijie(config-if)# end
```

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

6.2.8 配置二层接口作为私有VLAN的混杂端口

配置二层接口作为私有 VLAN 的端口，通过以下操作命令：

命令	说明
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **interface** *interface-id*	进入接口配置模式 百兆,千兆，万兆
Ruijie(config-if)# **switchport mode private-vlan promiscuous**	配置为私有 VLAN 二层交换模式
Ruijie(config-if)# **no switchport mode**	删除端口私有 VLAN 配置
Ruijie(config-if)# **switchport private-vlan mapping** *p_vid*{*svlist* | **add** *svlist* | **remove** *svlist*}	配置私有 VLAN 混杂端口所在的 Primary VLAN 以 Secondary VLAN 列表
Ruijie(config-if)# **no switchport private-vlan mapping**	取消混杂所有的的 seconary VLAN.

下面例子描述配置过程：

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/2
Ruijie(config-if)# switchport mode private-vlan promiscuous
Ruijie(config-if)# switchport private-vlan mapping 202 add 203
Ruijie(config-if)# end
```

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

6.2.9 显示private VLAN

您可以通过以下步骤显示 Private VLAN 内容：

命令	说明
show vlan private-vlan [*type*]	显示 private VLAN 的内容

```
Ruijie# show vlan private-vlan
VLAN Type  Status    Routed   Interface   Associated VLANs
---- ----  --------  ------   ---------   ------------------
202  prim  active    Enabled    Gi0/1       303-307,309,440
```

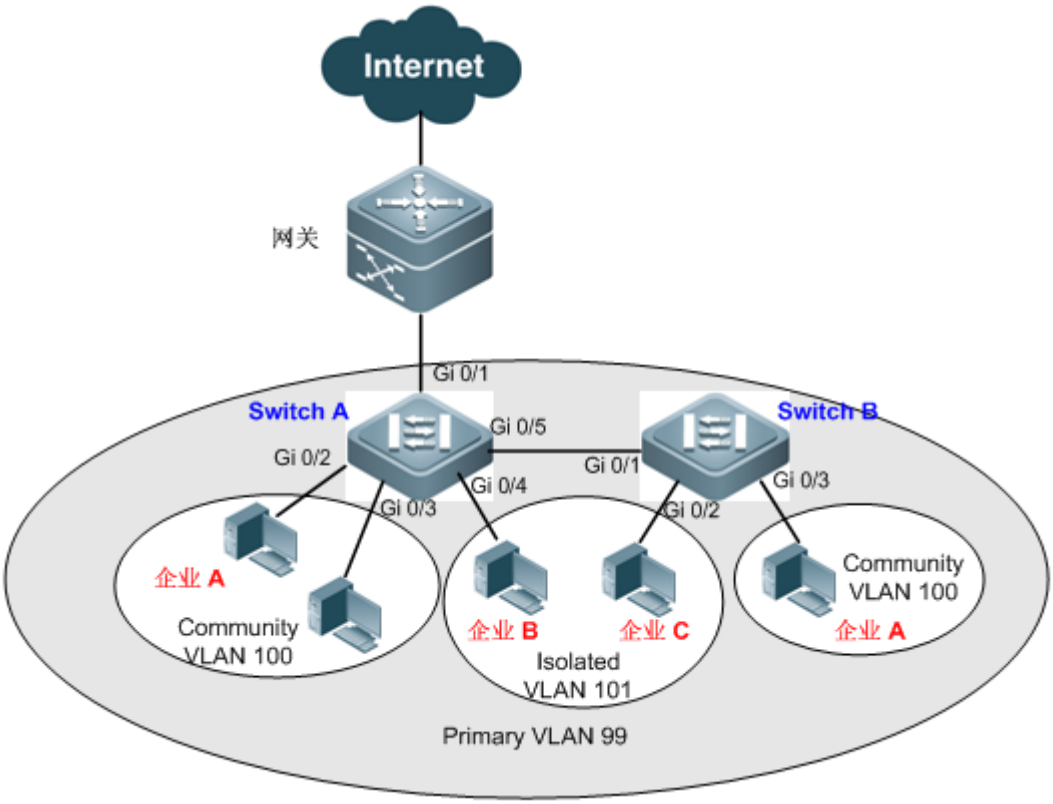
```
303 comm    active    Disabled    Gi0/2        202
304 comm    active    Disabled    Gi0/3        202
305 comm    active    Disabled    Gi0/4        202
306 comm    active    Disabled                 202
307 comm    active    Disabled                 202
309 comm    active    Disabled                 202
440 comm    active    Enabled     Gi0/5        202
```

6.3 PVLAN典型配置用例

6.3.1 PVLAN跨设备二层应用

拓扑图

图 1-1 PVLAN 跨设备二层应用拓扑



应用需求

如上图所示，在主机托管业务运营网络中，各企业用户通过设备 Switch A、Switch B 接入网络。主要需求如下：

- 企业内用户之间可以进行通信，企业间用户通信隔离

- 所有企业用户共享一个网关地址，可以与外网通信。

配置要点

- 将所有企业配置属于同一个 PVLAN（本例为 Primary VLAN 99），所有企业用户均通过该 VLAN 共享一个三层接口，实现外网通信。
- 如果企业内有多个用户，可以将各企业划分属于不同的 Community VLAN（本例将企业 A 划分属于 Community VLAN 100），实现企业内用户互相通信，企业间用户通信隔离。
- 如果企业内仅有一个用户，可以将这些企业划分属于同一个 Isolated VLAN（本例将企业 B 和 C 划分属于 Isolated VLAN 101），实现企业间用户通信隔离。

☑ 跨设备运行 PVLAN，需要将相连的端口配置为 Trunk Port。

☑ 与网关相连的端口需要配置为 Promiscuous Port；对端口网关设备接口可以配置为 Trunk Port 或 Hybrid Port，且 Native VLAN 是 PVLAN 的 Primary VLAN。

配置步骤

第一步，在设备上创建 Primary VLAN 和 Secondary VLAN。

！在 Switch A 上配置 Primary VLAN 99、Community VLAN 100、Isolated VLAN 101。

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

！Switch B 的配置同上。

第二步，在设备上关联 Secondary VLAN 和 Primary VLAN。

！在 Switch A 上配置 Community VLAN 100、Isoated VLAN 101 和 Primary VLAN 99 关联。

```
SwitchA(config)#vlan 99
SwitchA(config-vlan)#private-vlan association 100-101
SwitchA(config-vlan)#exit
```

！Switch B 的配置同上。

第三步，配置上链口，用于连接网关设备。

！将 Switch A 的端口 Gi 0/1 设置为 Promiscuous Port

```
SwitchA(config)#interface gigabitEthernet 0/1
SwitchA(config-if-GigabitEthernet 0/1)#switchport mode private-vlan promiscuous
SwitchA(config-if-GigabitEthernet 0/1)#switchport private-vlan mapping 99 100-101
SwitchA(config-if-GigabitEthernet 0/1)#exit
```

第四步，将各企业用户接入端口划分属于相应的 Secondary VLAN（如上图所示）。

！在 Switch A 上配置端口 Gi 0/2、Gi 0/3 属于 Community VLAN 100，端口 Gi 0/4 属于 Isolated VLAN 101。

```
SwitchA(config)#interface range gigabitEthernet 0/2-3
SwitchA(config-if-range)#switchport mode private-vlan host
SwitchA(config-if-range)#switchport private-vlan host-association 99 100
SwitchA(config-if-range)#exit
SwitchA(config)#interface gigabitEthernet 0/4
SwitchA(config-if-GigabitEthernet 0/4)#switchport mode private-vlan host
SwitchA(config-if-GigabitEthernet 0/4)#switchport private-vlan host-association 99 101
```

！在 Switch B 上配置端口 Gi 0/2 属于 Isoated VLAN 101，端口 Gi 0/3 属于 Community VLAN 100。

```
SwitchB(config)#interface gigabitEthernet 0/2
SwitchB(config-if-GigabitEthernet 0/2)#switchport mode private-vlan host
SwitchB(config-if-GigabitEthernet 0/2)# switchport private-vlan host-association 99 101
SwitchB(config-if-GigabitEthernet 0/2)#exit
SwitchB(config)#interface gigabitEthernet 0/3
SwitchB(config-if-GigabitEthernet 0/3)#switchport mode private-vlan host
SwitchB(config-if-GigabitEthernet 0/3)# switchport private-vlan host-association 99 100
SwitchB(config-if-GigabitEthernet 0/3)#exit
```

第五步，配置 PVLAN 跨设备运行的连接口。

！配置 Switch A 的端口 Gi 0/5 为 Trunk Port

```
SwitchA(config)#interface gigabitEthernet 0/5
SwitchA(config-if-GigabitEthernet 0/5)#switchport mode trunk
SwitchA(config-if-GigabitEthernet 0/5)#exit
```

！配置 Switch B 的端口 Gi 0/1 为 Trunk Port。

```
SwitchB(config)#interface gigabitEthernet 0/1
SwitchB(config-if-GigabitEthernet 0/1)#switchport mode trunk
SwitchB(config-if-GigabitEthernet 0/1)#exit
```

配置验证

第一步，查看设备的配置信息。

！Switch A 的配置信息

```
SwitchA#show running-config
!
```

```
vlan 99
 private-vlan primary
 private-vlan association add 100-101
!
vlan 100
 private-vlan community
!
vlan 101
 private-vlan isolated
!
interface GigabitEthernet 0/1
 switchport mode private-vlan promiscuous
 switchport private-vlan mapping 99 add 100-101
!
interface GigabitEthernet 0/2
 switchport mode private-vlan host
 switchport private-vlan host-association 99 100
!
interface GigabitEthernet 0/3
 switchport mode private-vlan host
 switchport private-vlan host-association 99 100
!
interface GigabitEthernet 0/4
 switchport mode private-vlan host
 switchport private-vlan host-association 99 101
!
interface GigabitEthernet 0/5
 switchport mode trunk
!
```

！Switch B 的配置信息

```
SwitchB#show running-config
!
vlan 99
 private-vlan primary
 private-vlan association add 100-101
!
vlan 100
 private-vlan community
!
vlan 101
 private-vlan isolated
!
interface GigabitEthernet 0/1
 switchport mode trunk
!
```

```
interface GigabitEthernet 0/2
 switchport mode private-vlan host
 switchport private-vlan host-association 99 101
!
interface GigabitEthernet 0/3
 switchport mode private-vlan host
 switchport private-vlan host-association 99 100
!
```

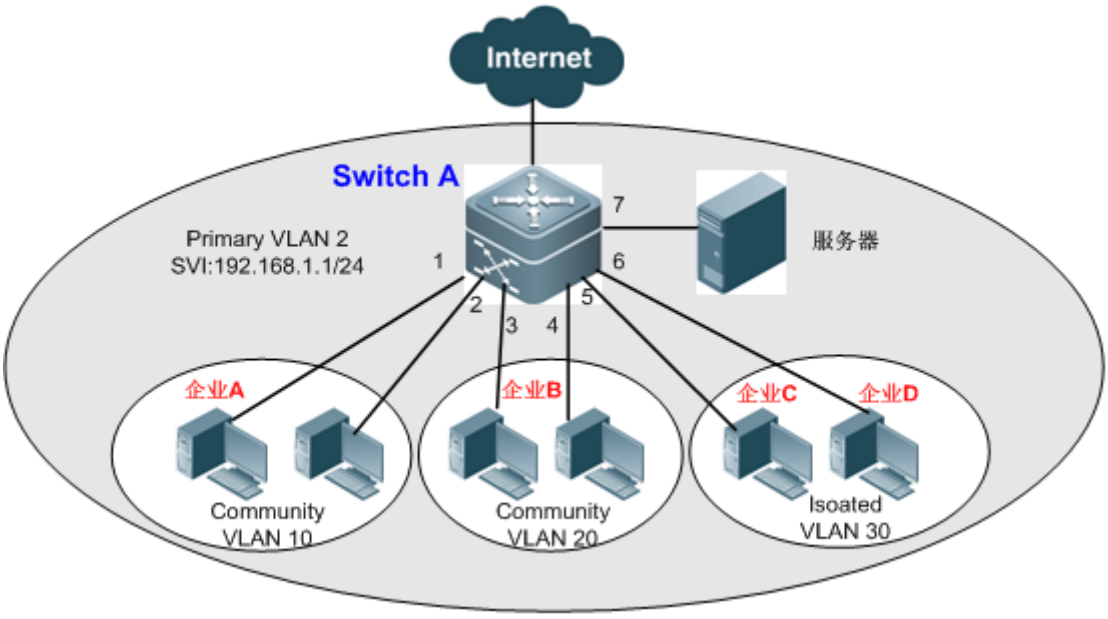
第二步，在设备上查看 PVLAN 的相关配置信息。

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

6.3.2 PVLAN单台设备三层应用

拓扑图

图 1-2 PVLAN 单台设备三层应用拓扑



应用需求

如上图所示，在主机托管业务运营网络中，各企业用户通过三层设备 Switch A 接入网络。主要需求如下：

- 企业内用户之间可以通信，企业间用户通信隔离。

- 所有企业用户都可以访问服务器
- 所有企业用户共享一个网关地址，可以与外网通信。

配置要点

- 在设备上（本例为 Switch A）配置 PVLAN 功能，具体配置要点可参考“PVLAN 跨设备二层应用”章节的配置要点。
- 将直连服务器的端口（本例为端口 Gi 0/7）设置为 Promiscuous Port，所有企业用户都可以通过 Promiscuous Port 和服务器通信。
- 在三层设备(本例为 Switch A)配置 PVLAN 的网关地址(本例配置 VLAN 2 的 SVI 为 192.168.1.1/24)，并配置 Primary VLAN（本例为 VLAN 2）和 Secondary VLAN（本例为 VLAN 10、20、30）的三层接口映射关系，所有企业用户可以通过这个网关地址与外网通信。

配置步骤

第一步，在设备上创建 Primary VLAN 和 Secondary VLAN。

！在 Switch A 上配置 Primary VLAN 2、Community VLAN 10、Community VLAN 20、Isolated VLAN 30。

```
SwitchA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)#vlan 2
SwitchA(config-vlan)#private-vlan primary
SwitchA(config-vlan)#exit
SwitchA(config)#vlan 10
SwitchA(config-vlan)#private-vlan community
SwitchA(config-vlan)#exit
SwitchA(config)#vlan 20
SwitchA(config-vlan)#private-vlan community
SwitchA(config-vlan)#exit
SwitchA(config)#vlan 30
SwitchA(config-vlan)#private-vlan isolated
SwitchA(config-vlan)#exit
```

第二步，在设备上关联 Secondary VLAN 和 Primary VLAN。

！在 Switch A 上配置 Community VLAN 10、Community VLAN 20、Isoated VLAN 30 和 Primary VLAN 2 关联。

```
SwitchA(config)#vlan 2
SwitchA(config-vlan)#private-vlan association 10,20,30
SwitchA(config-vlan)#exit
```

第三步，将各企业用户接入端口划分属于相应的 Secondary VLAN（如上图所示）。

！在 Switch A 上配置端口 Gi 0/1、Gi 0/2 属于 Community VLAN 10，端口 Gi 0/3、Gi 0/4 属于 Community VLAN 20，端口 Gi 0/5、Gi 0/6 属于 Isloated VLAN 30。

```
SwitchA(config)#interface range gigabitEthernet 0/1-2
SwitchA(config-if-range)#switchport mode private-vlan host
```

```
SwitchA(config-if-range)#switchport private-vlan host-association 2 10
SwitchA(config-if-range)#exit
SwitchA(config)#interface range gigabitEthernet 0/3-4
SwitchA(config-if-range)#switchport mode private-vlan host
SwitchA(config-if-range)#switchport private-vlan host-association 2 20
SwitchA(config-if-range)#exit
SwitchA(config)#interface range gigabitEthernet 0/5-6
SwitchA(config-if-range)#switchport mode private-vlan host
SwitchA(config-if-range)#switchport private-vlan host-association 2 30
SwitchA(config-if-range)#exit
```

第四步，配置服务器连接端口。

！将 Switch A 的端口 Gi 0/7 配置为 Promiscuous Port

```
SwitchA(config)#interface gigabitEthernet 0/7
SwitchA(config-if-GigabitEthernet 0/7)#switchport mode private-vlan promiscuous
SwitchA(config-if-GigabitEthernet 0/7)#switchport private-vlan maping 2 10,20,30
SwitchA(config-if-GigabitEthernet 0/7)#exit
```

第五步，在三层设备配置 PVLAN 的网关地址

！在 Switch A 上配置 Primary VLAN 2 的 SVI 为 192.168.1.1/24，并配置映射 Community VLAN 10、Community VLAN 20 和 Isolated VLAN 30。

```
SwitchA(config)#interface vlan 2
SwitchA(config-if-VLAN 2)#ip address 192.168.1.1 255.255.255.0
SwitchA(config-if-VLAN 2)#private-vlan mapping 10,20,30
SwitchA(config-if-VLAN 2)#exit
```

配置验证

第一步，查看 Switch A 的配置信息。

```
SwitchA#show running-config
!
vlan 2
 private-vlan primary
 private-vlan association add 10,20,30
!
vlan 10
 private-vlan community
!
vlan 20
 private-vlan community
!
vlan 30
 private-vlan isolated
!
```

```
interface GigabitEthernet 0/1
 switchport mode private-vlan host
 switchport private-vlan host-association 2 10
!
interface GigabitEthernet 0/2
 switchport mode private-vlan host
 switchport private-vlan host-association 2 10
!
interface GigabitEthernet 0/3
 switchport mode private-vlan host
 switchport private-vlan host-association 2 20
!
interface GigabitEthernet 0/4
 switchport mode private-vlan host
 switchport private-vlan host-association 2 20
!
interface GigabitEthernet 0/5
 switchport mode private-vlan host
 switchport private-vlan host-association 2 30
!
interface GigabitEthernet 0/6
 switchport mode private-vlan host
 switchport private-vlan host-association 2 30
!
interface GigabitEthernet 0/7
 switchport mode private-vlan promiscuous
 switchport private-vlan mapping 2 add 10,20,30
!
interface VLAN 2
 no ip proxy-arp
 ip address 192.168.1.1 255.255.255.0
 private-vlan mapping add 10,20,30
!
```

第二步，查看 PVLAN 的相关配置信息

```
SwitchA#show vlan private-vlan
VLAN  Type   Status   Routed   Ports  Associated VLANs
------------------------------ ------------------
2     primary    active   Enabled  Gi0/7         10,20,30
10    community  active   Enabled  Gi0/1, Gi0/2    2
20    community  active   Enabled  Gi0/3, Gi0/4    2
30    isolated   active   Enabled  Gi0/5, Gi0/6    2
```

7 Voice VLAN

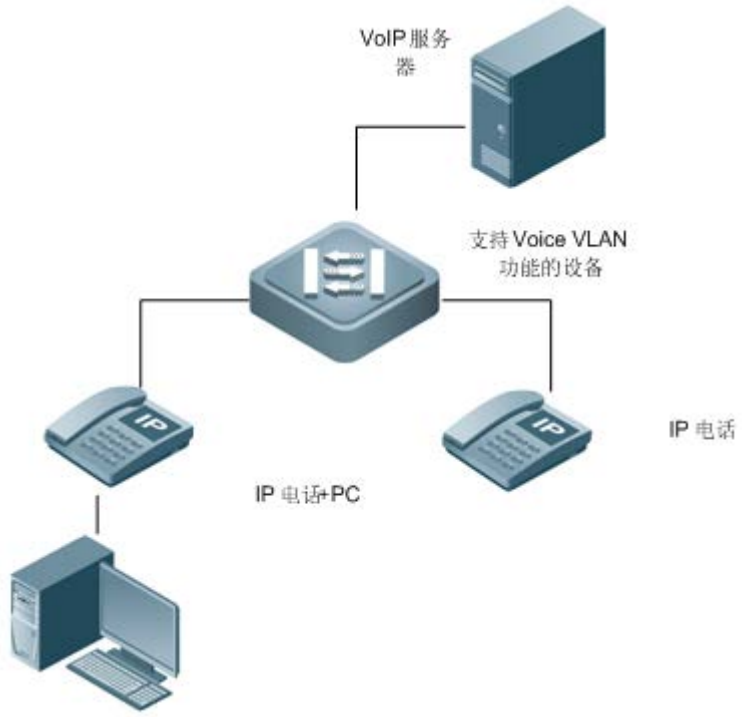
7.1 Voice VLAN概述

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 1-1 Voice VLAN 基本组网图



IP 电话和 Voice VLAN 的连接常用的有 2 种（参见上图）：

1. IP 电话单独接入 Voice VLAN 中，该链路中只有一条语音流。这类链接一般用于会议室部署 IP 电话，或无需用到 PC 进行数据业的场合。

2. PC 和 IP 电话组成菊花链接入网络。该链路中同时有语音流和数据流。此时，语音流和数据流分别在 Voice VLAN 和数据 VLAN 中，保证其互不干扰。一般办公人员需使用 PC 进行数据业务通信，同时也需通过 IP 电话进行语音通信时采用该种链接。

基本组网图中的各角色定义如下：

角色	作用
VoIP 服务器	通常 VoIP 应用中所需的服务器组（可以是 1 台承载多种应用服务的服务器，也可是多台提供不同服务的服务器），可能是 Call Agent、DHCP server（给 IP 电话自动分配 IP 地址、Voice VLAN ID 等信息）、录音服务器，等等。
互连设备	提供 Voice VLAN 功能的设备
用户终端设备	IP 电话与用户办公 PC

支持 Voice VLAN 功能的设备可以根据进入端口的数据报文中的源 MAC 地址字段，判断该数据流是否为指定语音设备的语音数据流，源 MAC 地址符合系统设置的语音设备 OUI（Organizationally Unique Identifier，全球统一标识符）地址的报文被认为是语音数据流，被划分到 Voice VLAN 中传输。

OUI 地址为 MAC 地址的前 24 位，是 IEEE（Institute of Electrical and Electronics Engineers，电气和电子工程师学会）为不同设备供应商分配的一个全球唯一的标识符，从 OUI 地址可以判断出该设备是哪一个厂商的产品。

7.1.1 Voice VLAN基本概念

7.1.1.1 Voice VLAN的自动模式与手动模式

Voice VLAN 中的端口可工作在 Voice VLAN 的自动模式或手动模式，在不同的工作模式下端口加入 Voice VLAN 的方式不同。

自动模式

当用户 IP 电话启动时，所发出的协议报文经支持 Voice VLAN 的设备时，设备通过识别该报文的源 MAC，匹配交换机上所配置的 Voice VLAN 的 OUI 地址。OUI 地址匹配成功后，设备自动将该语音报文的输入端口添加到 Voice VLAN，并下发策略，将语音报文的优先级修改为设备上所配置的 Voice VLAN 中语音流的优先级。

同时，用户可在设备上设置 Voice VLAN 的老化时间，当在老化时间内，系统没有从输入端口收到任何语音报文时，系统将把该端口从 Voice VLAN 中删除。端口加入 Voice VLAN 或从 Voice VLAN 中删除的过程由系统自动实现。端口的老化机制可以避免长时间不使用语音设备的端口一直驻留在 Voice VLAN 中。

手动模式

用户手工地在支持 Voice VLAN 的设备上将 IP 电话所连接的端口加入到 Voice VLAN 中。用户 IP 电话通讯过程中，设备通过识别该报文的源 MAC，匹配设备上所配置的 Voice VLAN 的 OUI 地址。OUI 地址匹配成功后，设备自动将该语音报文的输入端口添加到 Voice VLAN，并下发策略，将语音报文的优先级修改为设备上所配置的 Voice VLAN 中语音流的优先级。

手动模式下，端口加入 Voice VLAN 或从 Voice VLAN 中删除的过程由管理员手动进行配置。

对于 IP 电话发出的携带 tag 标签的报文，两种模式处理方式一致，与 VLAN 功能的转发规则相同，根据标签进行转发。

按照是否自动获取 IP 地址与 VLAN 信息来划分，一般来说，IP 电话有 2 种：

自动获取 IP 地址及 Voice VLAN 编号的电话，这类电话可以发送 untagged 或 tagged 的语音流。

手工设置 IP 地址及 Voice VLAN 编号的电话，这类电话只能发送 tagged 语音流。

Voice VLAN 功能支持使用 Access Port、Trunk Port 与 Hybrid Port 传输语音数据，依照连接的 IP 电话类型的不同，需要用户保证端口的类型、Voice VLAN 工作模式与 IP 电话类型能够匹配，具体匹配关系如下表所示：

Voice VLAN 工作模式	语音流类型	端口类型	支持条件
自动模式	Tagged 语音流	Access Port	不支持
		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
		Uplink 口	支持，接入端口的 native VLAN 必须存在且不能是 Voice VLAN，同时接入端口应允许 native VLAN 的报文通过
	Untagged 语音流	Access Port	不支持
		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
手动模式	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 Voice VLAN，且在接入端口允许通过的 untagged VLAN 列表中
		Uplink 口	不支持

- 如果用户的 IP Phone 发出的是 tagged 语音流，且接入的端口上使能了 802.1x 认证和 Guest VLAN 功能，为保证各种功能的正常使用，请为 Voice VLAN、端口的缺省 VLAN 和 802.1x 的 Guest VLAN 分配不同的 VLAN ID。
- 由于 Protocol VLAN 只对 Trunk Port/Hybrid Port 输入的 untagged 报文生效，而 Voice VLAN 自动模式下的 Trunk/Hybrid Port 只能对 tagged 语音流进行处理，因此请不要将某个 VLAN 同时设置为 Protocol VLAN 与 Voice VLAN。
- 在使用自动模式时，请不要将 OUI 地址配置为静态地址，否则会影响自动模式的使用。
- NBS200F 系列产品，加入 Voice VLAN 的端口若绑定 IP+MAC 或仅 IP 的安全地址，该安全地址绑定对符合 Voice VLAN OUI 地址的语音流不生效，即不符合绑定但符合 Voice VLAN OUI 地址的语音流不被过滤。
- NBS200F 系列产品，配置全局 IP 地址和 MAC 地址绑定，对于加入 Voice VLAN 的端口，该绑定对符合 Voice VLAN OUI 地址的语音流不生效。
- NBS200F 系列不支持 Voice VLAN 语音流的 CoS 值设置，输出报文的 COS 值为 DSCP 通过 QoS 映射表映射后的值。

7.1.1.2 Voice VLAN的安全模式

为了能够更好地进行用户语音流与数据流分离传输，Voice VLAN 提供安全模式功能。安全模式打开时，Voice VLAN 只允许传输语音流，设备会对报文的源 MAC 地址进行检查，当报文源 MAC 地址是可识别的 Voice VLAN OUI 地址时，允许该报文在 Voice VLAN 内传输，否则将该报文丢弃。安全模式关闭时，不对报文的源 MAC 地址进行检查，所有报文均可在 Voice VLAN 内进行传输。

安全模式下，仅对 untagged 报文及带有 Voice VLAN tag 的报文进行源 MAC 地址检查，对于带有其它非 Voice VLAN tag 的报文，设备按照 VLAN 规则对报文进行转发和丢弃的处理，不受 Voice VLAN 安全/普通模式的影响。

建议用户尽量不要在 Voice VLAN 中同时传输语音和业务数据。若的确有此需要，请确认 Voice VLAN 的安全模式已关闭。

7.2 Voice VLAN工作原理

支持 Voice VLAN 功能的设备，通过将数据流和语音流分别限制在数据 VLAN 和 Voice VLAN 中，从而保证语音通话与业务报文互不影响。同时下发优先级策略提高语音流的优先级，保证通话质量。其基本工作方式如下所述：

第一步，由用户在设备上创建 1 个专用传输语音报文的 VLAN，即 Voice VLAN，并使能连接 IP 电话的端口的 Voice VLAN 功能。

第二步，连接 IP 电话的端口加入 Voice VLAN，这是关键的一步。加入的方式视 Voice VLAN 的工作模式为自动模式或手动模式而有所不同，具体如下：

自动模式下，当设备从该端口收到一个 untagged 报文以后，会将其源 MAC 地址和合法 OUI 地址相匹配。如果该源 MAC 为 OUI 地址，即认为该报文为语音报文。设备将该端口自动加入到 Voice VLAN 中，同时在该端口上学习这个 MAC 地址。

手动模式下，由用户手动配置连接 IP 电话的端口加入到 Voice VLAN。

第三步，无论是自动模式还是手动模式，当端口加入 Voice VLAN 时，设备会下发策略，提高所有通过 Voice VLAN 的源 MAC 匹配该 OUI 的报文的优先级。将能够匹配该 OUI 地址的语音报文的优先级设置为 cos=6，dscp=46。

经过上述步骤后，连接 IP 电话的端口加入到专用的 Voice VLAN 中，语音报文在 Voice VLAN 中集中传输，同时语音报文以高优先级从设备中转发出去。

如果 IP 电话支持 LLDP 协议，则用户无需配置 OUI，设备可以通过捕捉 IP 电话发出的 LLDP 协议，对协议报文中的设备能力字段进行识别，对于标识其能力为“telephone”的设备识别为语音设备，将协议报文中的源 MAC 提取出来作为语音设备 MAC 进行处理，从而实现语音设备的自动识别。

LLDP 的配置方法请参见《LLDP》章节。

7.3 配置Voice VLAN基本特性

以下章节描述如何配置 Voice VLAN 的基本特性：

- （必选）使能 Voice VLAN 功能
- （必选）使能端口 Voice VLAN 功能
- （可选）配置端口的 Voice VLAN 工作模式
- （可选）配置 Voice VLAN 老化时间
- （可选）配置 Voice VLAN OUI 地址

- （可选）配置 Voice VLAN 的安全模式
- （可选）配置 Voice VLAN 的语音流优先级
- 查看 Voice VLAN 配置和状态

7.3.1 缺省配置

下表用来描述 Voice VLAN 的缺省配置。

功能特性	缺省值
Voice VLAN 使能状态	Disable，Voice VLAN 功能关闭
Voice VLAN 安全模式	打开
Voice VLAN 老化时间	1 天（1440 分钟），仅在自动模式下有效
Voice VLAN CoS	6
Voice VLAN DSCP	46
端口的 Voice VLAN 使能状态	关闭
端口的 Voice VLAN 工作模式	自动模式

7.3.2 使能Voice VLAN功能

缺省情况下，Voice VLAN 功能关闭，进入特权模式，按以下步骤开启 Voice VLAN 功能：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **vlan** *vlan-id*	创建 Voice VLAN。
Ruijie(config-vlan)# **exit**	退出 VLAN 配置模式。
Ruijie(config)# **voice vlan** *vlan-id*	使能 Voice VLAN，设置一个 VLAN 为 Voice VLAN。

如果要关闭 Voice VLAN 功能，可用 **no voice vlan** 全局配置命令进行设置。

配置举例：

全局使能 Voice VLAN 功能，并设置 VLAN 2 为 Voice VLAN。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# vlan 2
Ruijie(config-vlan)# exit
Ruijie(config)# voice vlan 2
```

当端口同时打开 802.1x 与 Voice VLAN 功能时，符合 Voice VLAN OUI 设置的 IP 电话无需认证即可使用 Voice VLAN 通信。譬如在同一个端口上接入 PC 和 IP 电话，打开 802.1x 认证功能后，PC 使用网络需进行 1x 认证，而 IP 电话不受影响。

配置 Voice VLAN 之前，须先创建对应的 VLAN。

- VLAN 1 是默认 VLAN，无需创建，但 VLAN 1 不能被设置为 Voice VLAN。
- 不允许将某个 VLAN 同时设置为 Voice VLAN 与 Super VLAN。
- 如果接入的端口上开启了 802.1x VLAN 自动跳转功能，为保证功能的正常使用，请不要将下发的 VID 设置为 Voice VLAN ID。
- 不要将 RSPAN 的 Remote VLAN 与 Voice VLAN 配置成同 1 个 VLAN，否则可能会影响远程端口镜像功能与 Voice VLAN 功能。

7.3.3 使能端口Voice VLAN功能

缺省情况下端口的 Voice VLAN 功能关闭，进入特权模式，按以下步骤开启端口的 Voice VLAN 功能：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **interface** *interface-name*	进入端口的配置模式，可使能 Voice VLAN 的端口为物理端口。
Ruijie(config-if)# **voice vlan enable**	使能端口的 Voice VLAN 功能。 缺省情况下端口的 Voice VLAN 功能关闭。

如果要关闭端口的 Voice VLAN 功能，可用 **no voice vlan enable** 命令进行设置。

配置举例：

打开端口 FastEthernet 0/1 的 Voice VLAN 功能，并显示当前 Voice VLAN 正在工作中的端口

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# voice vlan enable
```

- 在全局 Voice VLAN 关闭的情况下，也允许使能端口的 Voice VLAN 功能，但不生效。
- Voice VLAN 仅支持二层物理口（Access Port/Trunk Port/Hybrid Port/Uplink Port/ Private VLAN 端口等），不支持在 AP 口与 Routed Port 上打开 Voice VLAN 功能。
- 端口使能了 Voice VLAN 功能后，为保证功能运行正常，请不要切换端口的二层模式（Access Port/Trunk Port/Hybrid Port 等）。若需切换，请先关闭端口的 Voice VLAN 功能。

7.3.4 配置端口的Voice VLAN工作模式

Voice VLAN 的工作模式分为自动模式与手动模式，基于端口配置，关于自动模式与手动模式的概念请参见 Voice VLAN 的自动模式与手动模式部分说明。

缺省情况下，端口的 Voice VLAN 工作模式为自动模式，进入特权模式按以下步骤开启端口的 Voice VLAN 功能：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **interface** *interface-name*	进入端口的配置模式。
Ruijie(config-if)# **voice vlan mode auto**	设置端口的 Voice VLAN 模式为自动模式。 缺省情况下，Voice VLAN 工作在自动模式。 各个端口 Voice VLAN 的工作模式相互独立，不同的端口可以设置为不同的模式。

如果要设置端口的工作模式为手动模式，则使用 **no voice vlan mode auto** 命令进行设置。

配置举例：

设置端口 FastEthernet 0/1 的 Voice VLAN 模式为自动模式

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-vlan)# voice vlan mode auto
```

端口使能了 Voice VLAN 功能后，不允许进行手动模式和自动模式的切换，若需进行模式切换，请先关闭端口的 Voice VLAN 功能。

自动模式下，不允许通过手工配置命令将端口加入 Voice VLAN 或从 Voice VLAN 中删除。

当端口使能了 Voice VLAN 并工作在手工模式时，必须手工将端口加入 Voice VLAN，才能保证 Voice VLAN 功能生效。

当端口工作于自动模式时，为保证功能运行正常，请注意不要将端口的 native VLAN 设置为 Voice VLAN。

锐捷产品 Trunk Port/Hybrid Port 缺省可以传输所有 VLAN 的报文，请先将 Voice VLAN 从端口的 VLAN 许可列表中移出，再打开 Voice VLAN 功能，以保证未连接语音设备的端口不会加入 Voice VLAN，或长时间不使用的端口一直驻留在 Voice VLAN 中。

7.3.5 配置Voice VLAN老化时间

用户可在设备上设置 Voice VLAN 的老化时间，当在老化时间内，设备没有从输入端口收到任何语音报文时，将把该端口从 Voice VLAN 中删除。老化时间仅对自动模式生效。

进入特权模式，按以下步骤配置老化时间：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **voice vlan aging** *minutes*	配置 Voice VLAN 的老化时间，取值范围为 5-10000 分钟，缺省为 1440 分钟。

如果要将老化时间恢复到缺省值，可用 **no voice vlan aging** 全局配置命令进行设置。

配置举例：

设置 Voice VLAN 老化时间为 10 分钟

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# voice vlan aging 10
```

7.3.6 配置Voice VLAN OUI地址

锐捷产品提供 Voice VLAN 可识别的 OUI 地址设置，OUI 地址的说明请参见 Voice VLAN 概述部分。支持 Voice VLAN 功能的设备通过识别输入报文的源 MAC，是否匹配设备上所配置的 Voice VLAN 的 OUI 地址，来判断该数据流是否为指定语音设备的语音数据流。

进入特权模式，按以下步骤配置 Voice VLAN OUI 地址：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **voice vlan mac-address** *mac-addr* **mask** *oui-mask* [**description** *text*]	配置设备可识别的 Voice VLAN OUI 地址
Ruijie(config)# **show voice vlan oui**	查看 Voice VLAN OUI 地址

如果要删除设备上设置的某个 OUI 地址，可用 **no voice vlan mac-address** *oui* 全局配置命令进行设置。

配置举例：

设置 OUI 地址 0012.3400.0000 为 Voice VLAN 的合法地址，厂商为 Company A

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# voice vlan mac-address 0012.3400.0000 mask ffff.ff00.0000 description Company A
Ruijie(config)# show voice vlan oui
Oui Address     Mask              Description
0012.3400.0000  ffff.ff00.0000  Company A
```

7.3.7 配置Voice VLAN的安全模式

为了更好地进行用户语音流与数据流分离传输，锐捷产品的 Voice VLAN 提供安全模式功能，安全模式打开时 Voice VLAN 内只允许传输语音流，更好地保证语音流传输质量

进入特权模式，按以下步骤配置 Voice VLAN 的安全模式：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **voice vlan security enable**	打开 Voice VLAN 的安全模式。 缺省情况下，Voice VLAN 的安全模式打开。

如果要关闭 Voice VLAN 的安全模式，可用 **no voice vlan security enable** 全局配置命令进行设置。

配置举例：

打开 Voice VLAN 的安全模式

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# voice vlan security enable
```

7.3.8 配置Voice VLAN的语音流优先级

设备通过修改 Voice VLAN 的语音流的 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
Ruijie# **configure terminal**	进入全局配置模式。
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。
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
```

☑ NBS200F 系列产品不支持 **voice vlan cos** *cos-value* 命令。

☑ NBS200F 系列产品，Voice VLAN 所配置的 DSCP 值与 802.1x 功能下发的 DSCP 属性冲突时，以 Voice VLAN 配置的 DSCP 值生效。

7.3.9 查看Voice VLAN配置和状态

Voice VLAN 提供了如下的显示命令用于查看各种配置信息及运行时信息，各命令的功能说明如下：

命令	作用
show voice vlan	显示 Voice VLAN 的配置信息与当前状态，包括使能 Voice VLAN 功能的端口的工作模式。
show voice vlan oui	显示当前设备支持的 OUI 地址、OUI 地址掩码和描述信息。

show vlan	显示当前 Voice VLAN 正在工作中的端口，同普通 VLAN 的显示命令。

7.4 Voice VLAN典型配置举例

7.4.1 Voice VLAN自动模式配置举例

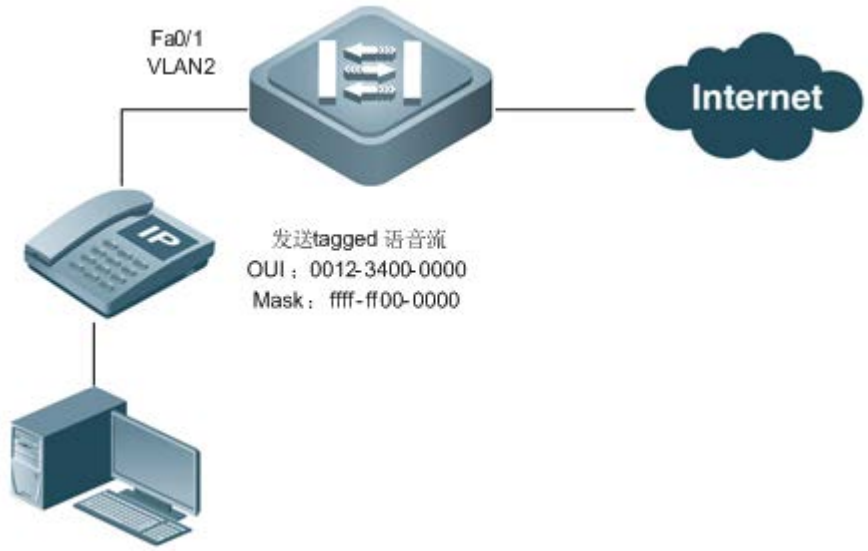
组网需求

假设 Voice VLAN 自动模式配置有以下需求：

- 创建 VLAN2 为 Voice VLAN。
- Voice VLAN 老化时间为 1000 分钟。
- IP 电话 MAC 地址为 0012.3456.7890，发送 tagged 语音流，接入端口是 Trunk 类型端口 Fa0/1（此处为示例说明，在使用 Voice VLAN 功能时请参见 Voice VLAN 的自动模式与手动模式章节中的端口模式与 IP 电话语音流类型匹配关系表），端口的 native VLAN 为 VLAN 5。
- 设备允许 OUI 地址为 0012.3400.0000，掩码是 ffff.ff00.0000 的语音报文通过 Voice VLAN 转发。
- 接入端口 Fa0/1 下连的 PC 需要使用 802.1x 认证。

组网拓扑

图 1-2 Voice VLAN 自动模式配置组网图



配置要点

依据组网需求，设备的 Voice VLAN 配置需要注意：由于 Fa0/1 下连的是发送 tagged 语音流，且为 Trunk Port，Voice VLAN 模式为自动模式，依据匹配关系要求，Fa0/1 的 native VLAN 必须存在且不能是 Voice VLAN，同时该端口允许 native VLAN 通过。

组网需求中 Fa0/1 的 native VLAN 为 5，非 Voice VLAN（VLAN2），可满足上述要求。同时由于 Trunk Port 缺省包含所有 VLAN，为更好地使用自动模式，使不连接语音设备的端口不加入 Voice VLAN，需要先将 Voice VLAN（VLAN5）从 Fa0/1 的 VLAN 许可列表中移出。

配置步骤

1）创建 VLAN2 为 Voice VLAN

#创建 VLAN2，使能 VLAN2 的 Voice VLAN 功能

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# vlan 2
Ruijie(config-vlan)# exit
Ruijie(config)# voice vlan 2
```

2）Voice VLAN 老化时间为 1000 分钟

设置 Voice VLAN 的老化时间

```
Ruijie(config)# voice vlan aging 1000
```

3）设备允许 OUI 地址为 0012.3400.0000，掩码是 ffff.ff00.0000 的语音报文通过 Voice VLAN 转发。

设置 Voice VLAN OUI 地址

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

4）接入端口是 Trunk 类型端口 Fa0/1，端口的 native VLAN 为 VLAN 5。

设置 Fa0/1 为 Trunk Port

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# switchport mode trunk
```

设置 Fa0/1 的 native VLAN 为 VLAN5

```
Ruijie(config-if)# switchport trunk native vlan 5
```

将 Voice VLAN 从加入 Fa0/1 的 VLAN 列表中移出

```
Ruijie(config-if)# switchport trunk allowed vlan remove 2
```

使能 Fa0/1 的 Voice VLAN 功能

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# voice vlan enable
```

5）若接入端口需同时打开 802.1x 功能，则需做如下配置。

802.1x 功能的设置 Fa0/1 为 802.1x 受控口

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# dot1x port-control auto
```

其余 802.1x 功能的配置方法，请参见 802.1x 配置章节

显示验证

查看设备当前的 Voice VLAN 状态

```
Ruijie(config)# show voice vlan
Voice Vlan status: ENABLE             // 全局 Voice VLAN 使能
Voice Vlan ID        : 2                // Voice VLAN ID 为 2
Voice Vlan security mode: Security  // 全局安全模式打开
Voice Vlan aging time: 1440minutes
Voice Vlan cos       : 6
Voice Vlan dscp      : 46
Current voice vlan enabled port mode:
PORT                 MODE
-------------------- ----------
Fa0/1                AUTO             // Fa0/1 使能 Voice VLAN，为自动模式
# 查看设备的 Voice VLAN OUI 地址
Ruijie(config)# show voice vlan oui
Oui Address     Mask              Description        Status
0012.3400.0000  ffff.ff00.0000                       static
```

7.4.2 Voice VLAN手动模式配置举例

组网需求

1）创建 VLAN2 为 Voice VLAN。

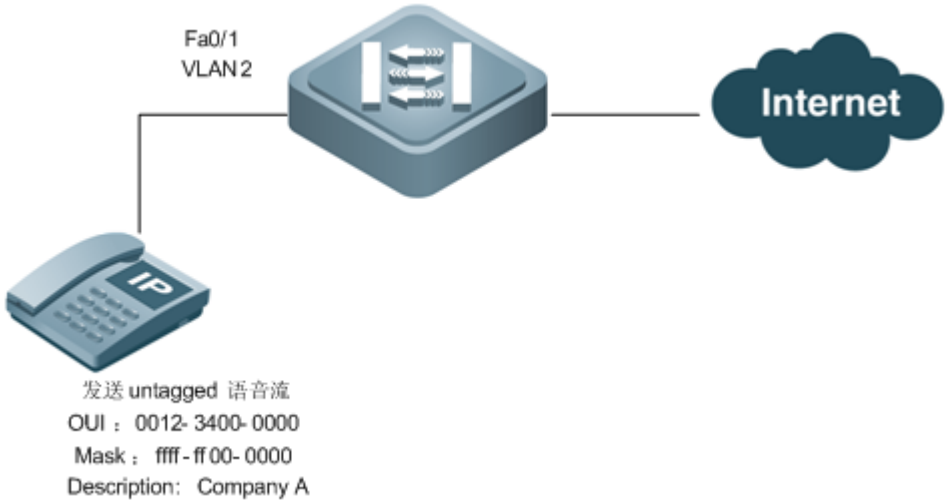
2）IP 电话 MAC 地址为 0012.3456.7890，发送 untagged 语音流，接入端口是 Hybrid 类型端口 Fa0/1。

3）Fa0/1 工作在手动模式。

4)设备允许 OUI 地址为 0012.3400.0000,掩码是 ffff.ff00.0000 的语音报文通过 Voice VLAN 转发,描述符为 Company A。

组网拓扑

图 1-3 Voice VLAN 手动模式配置组网图



配置要点

依据组网需求，设备的 Voice VLAN 配置需要注意：由于 Fa0/1 下连的是发送 untagged 语音流，且 Fa0/1 为 Hybrid Port，Voice VLAN 模式为手动模式，依据匹配关系要求，Fa0/1 的 native VLAN 必须是 Voice VLAN，且 Voice VLAN 须在端口的允许通过的 untagged VLAN 列表中。因此，组网需求中 Fa0/1 的 native VLAN 应设置为 2（Voice VLAN ID），同时配置时需要将 VLAN2 加入 Fa0/1 允许通过的 untagged VLAN 列表中。

配置步骤

1）创建 VLAN2 为 Voice VLAN

#创建 VLAN2，使能 VLAN2 的 Voice VLAN 功能

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# vlan 2
Ruijie(config-vlan)# exit
Ruijie(config)# voice vlan 2
```

2）设备允许 OUI 地址为 0012.3400.0000，掩码是 ffff.ff00.0000 的语音报文通过 Voice VLAN 转发，描述符为 Company A。

设置 Voice VLAN OUI 地址

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

3）接入端口是 Hybrid 类型端口 Fa0/1，端口的 native VLAN 为 VLAN 2

设置 Fa0/1 为 Hybrid Port

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# switchport mode hybrid
```

设置 Voice VLAN 为 Fa0/1 的 native VLAN

```
Ruijie(config-if)# switchport hybrid native vlan 2
```

将 Voice VLAN（即 VLAN2）加入 Fa0/1 的 untagged 列表

```
Ruijie(config-if)# switchport hybrid allowed vlan add untagged 2
```

使能 Fa0/1 的 Voice VLAN 功能

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# voice vlan enable
```

显示验证

查看设备当前的 Voice VLAN 状态

```
Ruijie(config)# show voice vlan
Voice Vlan status: ENABLE             // 全局 Voice VLAN 使能
Voice Vlan ID        : 2                // Voice VLAN ID 为 2
Voice Vlan security mode: Security  // 全局安全模式打开
Voice Vlan aging time: 1440minutes
Voice Vlan cos       : 6
Voice Vlan dscp      : 46
Current voice vlan enabled port mode:
PORT                 MODE
-------------------- ----------
Fa0/1                MANUAL             // Fa0/1 使能 Voice VLAN，为手动模式
```

查看设备的 Voice VLAN OUI 地址

```
Ruijie(config)# show voice vlan oui
Oui Address     Mask              Description       Status
0012.3400.0000  ffff.ff00.0000  Company A         static
```

8 RSTP

8.1 STP、RSTP概述

本设备既支持 STP 协议，也支持 RSTP 协议，遵循 IEEE 802.1D 和 IEEE 802.1w 标准。

STP 协议是用来避免链路环路产生的广播风暴、并提供链路冗余备份的协议。

对二层以太网来说，两个 LAN 间只能有一条活动着的通路，否则就会产生广播风暴。但是为了加强一个局域网的可靠性，建立冗余链路又是必要的，其中的一些通路必须处于备份状态，如果当网络发生故障，另一条链路失效时，冗余链路就必须被提升为活动状态。手工控制这样的过程显然是一项非常艰苦的工作，STP 协议就自动地完成这项工作。它能使一个局域网中的设备起以下作用：

- 发现并启动局域网的一个最佳树型拓朴结构。
- 发现故障并随之进行恢复，自动更新网络拓朴结构，使在任何时候都选择了可能的最佳树型结构。

局域网的拓朴结构是根据管理员设置的一组网桥配置参数自动进行计算的。使用这些参数能够生成最好的一棵拓朴树。只有配置得当，才能得到最佳的方案。

RSTP 协议完全向下兼容 802.1D STP 协议，除了和传统的 STP 协议一样具有避免回路、提供冗余链路的功能外，最主要的特点就是“快”。如果一个局域网内的网桥都支持 RSTP 协议且管理员配置得当，一旦网络拓朴改变而要重新生成拓朴树只需要不超过 1 秒的时间（传统的 STP 需要大约 50 秒）。

8.1.1 Bridge Protocol Data Units(简写为BPDU)：

要生成一个稳定的树型拓朴网络需要依靠以下元素：

- 每个网桥拥有的唯一的桥 ID（Bridge ID），由桥优先级和 Mac 地址组合而成。
- 网桥到根桥的路径花费（Root Path Cost），以下简称根路径花费。
- 每个端口 ID（Port ID），由端口优先级和端口号组合而成。

网桥之间通过交换 BPDU（Bridge Protocol Data Units，网桥协议数据单元）帧来获得建立最佳树形拓朴结构所需要的信息。这些帧以组播地址 01-80-C2-00-00-00（十六进制）为目的地址。

每个 BPDU 由以下这些要素组成：

- Root Bridge ID（本网桥所认为的根桥 ID）。
- Root Path Cost（本网桥的根路径花费）。
- Bridge ID（本网桥的桥 ID）。
- Message Age（报文已存活的时间）
- Port ID（发送该报文端口的 ID）。

Forward-Delay Time、Hello Time、Max-Age Time 三个协议规定的时间参数。

其他一些诸如表示发现网络拓朴变化、本端口状态的标志位。

当网桥的一个端口收到高优先级的 BPDU（更小的 Bridge ID，更小的 Root Path Cost 等），就在该端口保存这些信息，同时向所有端口更新并传播这些信息。如果收到比自己低优先级的 BPDU，网桥就丢弃该信息。

这样的机制就使高优先级的信息在整个网络中传播开，BPDU 的交流就有了下面的结果：

- 网络中选择了一个网桥为根桥（Root Bridge）。
- 除根桥外的每个网桥都有一个根口（Root Port），即提供最短路径到 Root Bridge 的端口。
- 每个网桥都计算出了到根桥（Root Bridge）的最短路径。
- 每个 LAN 都有了指派网桥（Designated Bridge），位于该 LAN 与根桥之间的最短路径中。指派网桥和 LAN 相连的端口称为指派端口（Designated Port）。
- 根口（Root port）和指派端口（Designated Port）进入 Forwarding 状态。
- 其他不在生成树中的端口就处于 Discarding 状态

8.1.2 Bridge ID

按 IEEE 802.1W 标准规定，每个网桥都要有单一的网桥标识（Bridge ID），生成树算法中就是以它为标准来选出根桥（Root Bridge）的。Bridge ID 由 8 个字节组成，后 6 个字节为该网桥的 mac 地址，前 2 个字节如下表所示，前 4 bit 表示优先级（Priority），后 8 bit 表示 System ID，为以后扩展协议而用，在 RSTP 中该值为 0，因此给网桥配置优先级就要是 4096 的倍数。

	Bit 位	值
Priority value	16	32768
	15	16384
	14	8192
	13	4096
System ID	12	2048
	11	1024
	10	512
	9	256
	8	128
	7	64
	6	32
	5	16
	4	8
	3	4
	2	2
	1	1

8.1.3 Spanning-Tree Timers（生成树的定时器）

以下描述影响到整个生成树性能的三个定时器。

- Hello timer：定时发送 BPDU 报文的时间间隔。
- Forward-Delay timer：端口状态改变的时间间隔。当 RSTP 协议以兼容 STP 协议模式运行时，端口从 Listening 转变向 Learning，或者从 Learning 转向 Forwarding 状态的时间间隔。
- Max-Age timer：BPDU 报文消息生存的最长时间。当超出这个时间，报文消息将被丢弃。

8.1.4 Port Roles and Port States

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

- Root port：提供最短路径到根桥（Root Bridge）的端口。
- Designated port：每个 LAN 的通过该口连接到根桥。
- Alternate port：根口的替换口，一旦根口失效，该口就立该变为根口。
- Backup port：Designated Port 的备份口，当一个网桥有两个端口都连在一个 LAN 上，那么高优先级的端口为 Designated Port，低优先级的端口为 Backup Port。
- Disable port：当前不处于活动状态的口，即 Operation State 为 Down 的端口都被分配了这个角色。

以下为各个端口角色的示意图 1、2、3：

R = Root Port　　D = Designated Port　　A = Alternate Port　　B = Backup Port

在没有特别说明情况下，端口优先级从左到右递减。

图 1-1

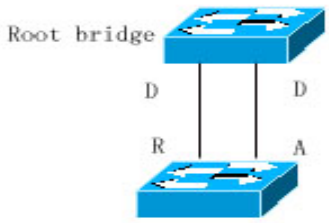


图 1-2

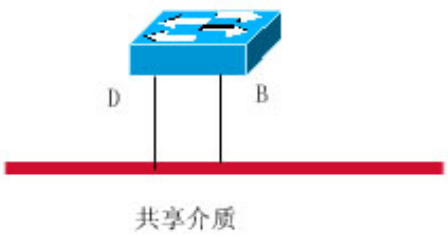
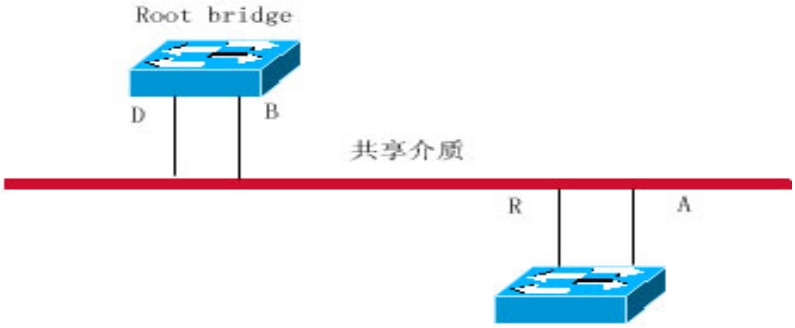


图 1-3



每个端口有三个状态（Port State）来表示是否转发数据包，从而控制着整个生成树拓朴结构。

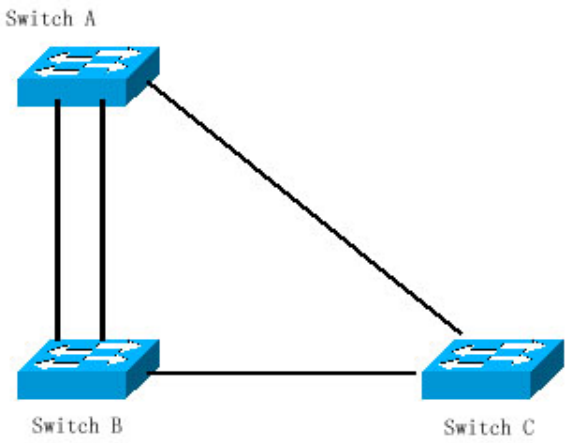
- Discarding：既不对收到的帧进行转发，也不进行源 Mac 地址学习。
- Learning：不对收到的帧进行转发，但进行源 Mac 地址学习，这是个过渡状态。
- Forwarding：既对收到的帧进行转发，也进行源 Mac 地址的学习。

对一个已经稳定的网络拓朴，只有 Root Port 和 Designated Port 才会进入 Forwarding 状态，其它端口都只能处于 Discarding 状态。

8.1.5 网络拓朴树的生成（典型应用方案）

现在就可以说明 STP、RSTP 协议是如何把杂乱的网络拓朴生成一个树型结构了。如下图 4 所示，假设 Switch A、B、C 的 bridge ID 是递增的，即 Switch A 的优先级最高。A 与 B 间是千兆链路，A 和 C 间为十兆链路，B 和 C 间为百兆链路。Switch A 做为该网络的骨干设备，对 Switch B 和 Switch C 都做了链路冗余，显然，如果让这些链路都生效是会产生广播风暴的。

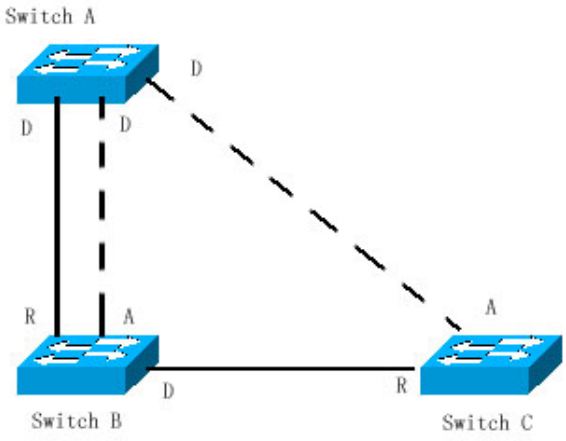
图 1-4



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

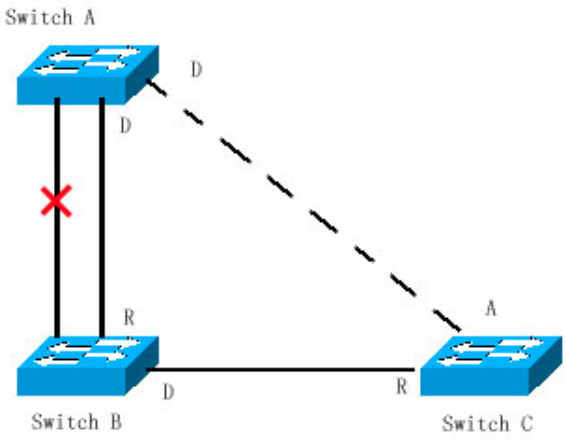
直接到 A 的低（各种链路对应的链路花费请查表），于是 Switch C 就选择了与 B 相连的端口为 Root port，与 A 相连的端口为 Alternate port。都选择好端口角色（Port Role）了，就进入各个端口相应的状态了，于是就生成了相应的图 5。

图 1-5



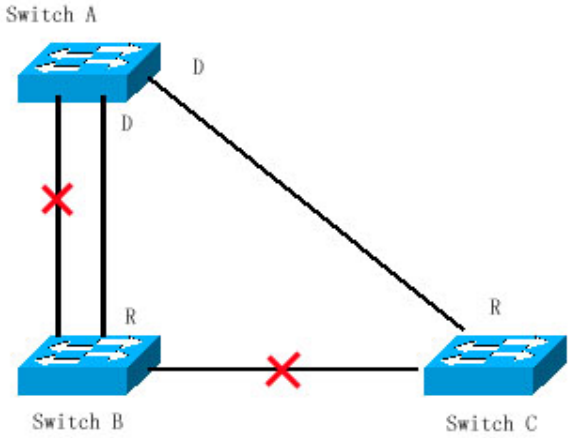
如果 Switch A 和 Switch B 之间的活动链路出了故障，那备份链路就会立即产生作用，于是就生成了相应的图 6。

图 1-6



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 1-7



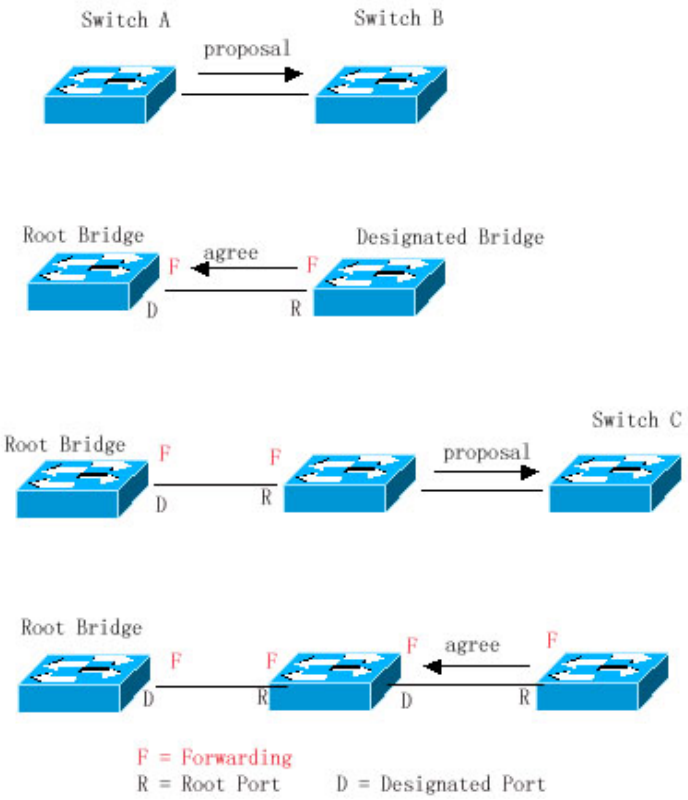
8.1.6 RSTP的快速收敛

现在开始介绍 RSTP 所特有的功能，即能让端口“快速”的 Forwarding。

STP 协议是选好端口角色（Port Role）后等待 30 秒(为 2 倍的 Forward-Delay Time，Forward-Delay Time 可配置，默认为 15 秒)再 Forwarding 的，而且每当拓朴发生变化后，每个网桥重新选出的 Root Port 和 Designated Port 都要经过 30 秒再 Forwarding，因此要等整个网络拓朴稳定为一个树型结构就大约需要 50 秒。

而 RSTP 端口的 Forwarding 过程就大不一样了，如图所示，Switch A 发送 RSTP 特有“Proposal”报文，Switch B 发现 Switch A 的优先级比自身高，就选 Switch A 为根桥，收到报文的端口为 Root Port，立即 Forwarding，然后从 Root Port 向 Switch A 发送“Agree”报文。Switch A 的 Designated Port 得到“同意”，也就 Forwarding 了。然后 Switch B 的 Designated Port 又发送“Proposal”报文依次将生成树展开。因此在理论上，RSTP 是能够在网络拓朴发生变化的一瞬间恢复网络树型结构，达到快速收敛。

图 1-8



以上的“握手”过程是有条件的，就是端口间必须是“Point-to-point Connect（点对点连接）”。为了让设备发挥最大的功效，最好不要使设备间为非点对点连接。

本章中除图 9 外，其它示意图均为“点对点连接”，以下列出了“非点对点连接”的范例图。

非点对点连接范例：

图 1-9

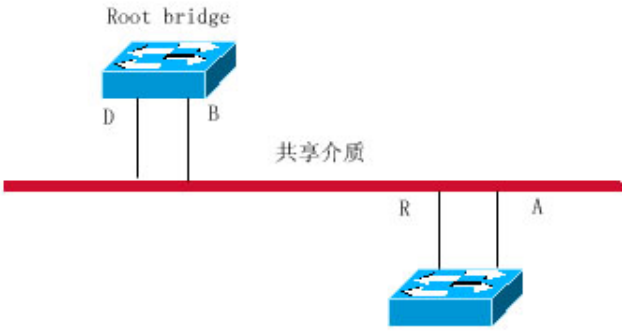
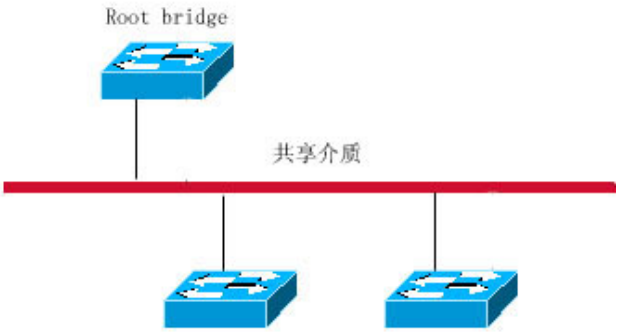
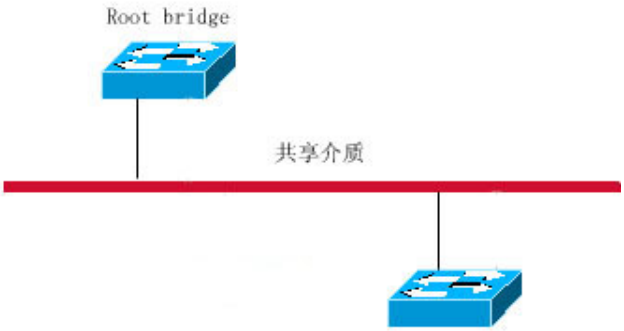


图 1-10



另外、下图为“点对点”连接，请用户注意区分

图 1-11



8.1.7 RSTP与STP的兼容

RSTP 协议可以与 STP 协议完全兼容，RSTP 协议会根据收到的 BPDU 版本号来自动判断与之相连的网桥是支持 STP 协议还是支持 RSTP 协议，如果是与 STP 网桥互连就只能按 STP 的 Forwarding 方法，过 30 秒再 Forwarding，无法发挥 RSTP 的最大功效。

另外，RSTP 和 STP 混用还会遇到这样一个问题。如图所示，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，如图所示。

图 1-12

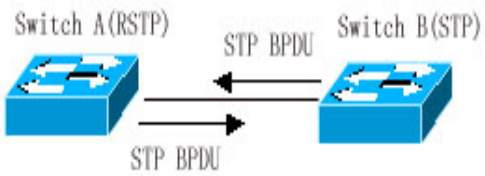
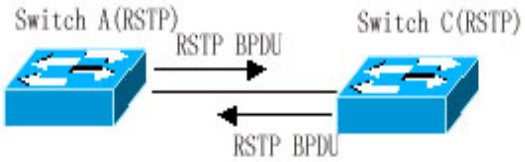


图 1-13

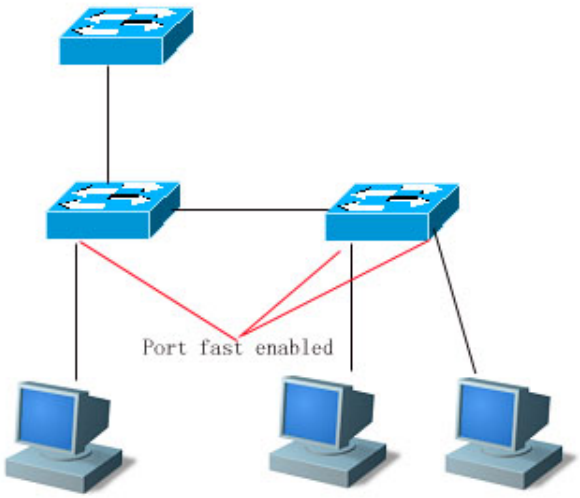


8.2 RSTP可选特性

8.2.1 Port Fast

如果设备的端口直连着网络终端，那么就可以设置该端口为 Port Fast，端口直接 Forwarding，这样可免去端口等待 Forwarding 的过程（如果不配置 Port Fast 的端口，就要等待 30 秒 Forwarding）。下图表示了一个设备的哪些端口可以配置为 Port Fast enable。

图 1-14



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。

8.2.2 BPDU Guard

BPDU Guard 既能全局的 enable，也能针对单个 Interface 进行 enable。这两者有些细小的差别。

可以在全局模式中用 **spanning-tree portfast bpduguard default** 命令打开全局的 BPDU Guard enabled 状态，在这种状态下，如果某个 Interface 打开了 Port Fast，或该接口自动识别为边缘口，而该 Interface 收到了 BPDU，该端口就会进入 Error-disabled 状态，以示配置错误；同时整个端口被关闭，表示网络中可能被非法用户增加了一台网络设备，使网络拓朴发生改变。

也可以在 Interface 配置模式下用 **spanning-tree bpduguard enable** 命令来打开单个 Interface 的 BPDU Guard（与该端口是否打开 Port Fast 无关）。在这个情况下如果该 Interface 收到了 BPDU，就进入 Error-disabled 状态。

8.2.3 BPDU Filter

BPDU Filter 既能全局的 enable，也能针对单个 Interface 进行 enable。这两者有些细小的差别。

可以在全局模式中用 **spanning-tree portfast bpdufilter default** 命令打开全局的 BPDU Filter enabled 状态，在这种状态下，Port Fast enabled 的 Interface 将既不收 BPDU，也不发 BPDU，这样，直连 Port Fast enabled 端口的主机就收不到 BPDU。而如果 Port Fast enabled 的 Interface 因收到 BPDU 而使 Port Fast Operational 状态 disabled，BPDU Filter 也就自动失效。

也可以在 Interface 配置模式下用 **spanning-tree bpdufilter enable** 命令设置了单个 Interface 的 BPDU Filter enable（与该端口是否打开 Port Fast 无关）。在这个情况下该 Interface 既不收 BPDU，也不发 BPDU，并且是直接 Forwarding 的。

8.2.4 Tc-protection

TC-BPDU 报文是指携带 TC 标志的 BPDU 报文，交换机收到这类报文表示网络拓扑发生了变化，会进行 MAC 地址表的删除操作，对三层交换机，还会引发快转模块的重新打通操作，并改变 ARP 表项的端口状态。为避免交换机受到伪造 TC-BPDU 报文的恶意攻击时频繁进行以上操作，负荷过重，影响网络稳定，可以使用 TC-protection 功能进行保护。

Tc-protection 只能全局的打开和关闭，缺省情况下为打开此功能。

在打开相应功能时，收到 TC-BPDU 报文后的一定时间内（一般为 4 秒），只进行一次删除操作，同时监控该时间段内是否收到 TC-BPDU 报文。如果在该时间段内收到了 TC-BPDU 报文，则设备在该时间超时后再进行一次删除操作。这样可以避免频繁的删除 MAC 地址表项和 ARP 表项。

8.2.5 TC Guard

Tc-Protection 功能可以保证网络产生大量 tc 报文时减少动态 MAC 地址和 ARP 的删除，但在遇到 TC 报文攻击的时候还是会产生很多的删除操作，并且 TC 报文是可扩散的，将影响整个网络。使用 TC Guard 功能，我们允许用户在全局或者端口上禁止 TC 报文的扩散。当一个端口收到 TC 报文的时候，如果全局配置了 TC Guard 或者是端口上配置了 TC Guard，则该端口将屏蔽掉该端口接收或者是自己产生的 TC 报文，使得 TC 报文不会扩散到其它端口，这样能有效控制网络中可能存在的 TC 攻击，保持网络的稳定，尤其是在三层设备上，该功能能有效避免接入层设备的振荡引起核心路由中断的问题。

- 错误的使用 tc-guard 功能会使网络之间的通讯中断。
- 建议在确认网络当中有非法的 tc 报文攻击的情况下再打开此功能。
- 打开全局的 tc-guard,则所有端口都不会对外扩散 tc 报文。适用于桌面接入设备上开启。
- 打开接口的 tc-guard,则对于该接口产生的拓扑变化以及收到的 tc 报文，将不向其它端口扩散。适合在上链口，尤其是汇聚接核心的端口开启该功能。

8.2.6 TC过滤

配置 TC Guard 功能，端口将不扩散 TC 报文到本设备上其它参与生成树计算的端口，这里的不扩散包括了两种情况：一种是端口收到的 TC 报文不扩散，一种是端口自己产生的 TC 报文不扩散。端口自己产生的 TC 报文是指当端口转发状态发生变化时(例如从 block 到 forwarding 的转变)，端口会产生 TC 报文，此时表示拓扑可能发生了变化。

这样，可能引发的问题时，由于 TC Guard 阻止了 TC 报文的扩散，导致当发生拓扑变化的时候，设备没有清除相应端口的 MAC 地址，转发数据出错。

因此，引入了 TC 过滤的概念。TC 过滤是指对于端口收到的 TC 报文不处理，而正常的拓扑变化的情况，能够处理。这样，解决了未配置 Portfast 的端口频繁地 UP/DOWN 引起的清地址和核心路由中断的问题，又能保证发生拓扑变化时，核心路由表项能够得到及时地更新。

TC 过滤功能缺省情况下关闭。

8.2.7 BPDU源MAC检查

BPDU 源 MAC 检查是为了防止通过人为发送 BPDU 报文来恶意攻击交换机而使 RSTP 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。

8.2.8 BPDU非法长度过滤

BPDU 的以太网长度字段超过 1500 时，该 BPDU 帧将被丢弃，以防止收到非法 BPDU 报文。

8.2.9 边缘口的自动识别

指派口在一定的时间范围内(为 3 秒)，如果收不到下游端口发送的 BPDU，则认为该端口相连的是一台网络设备，从而设置该端口为边缘端口，直接进入 Forwarding 状态。自动标识为边缘口的端口因收到 BPDU 而自动识别为非边缘口。

可以通过 **spanning-tree autoedge disabled** 命令取消边缘口的自动识别功能。

该功能是缺省打开的。

边缘口的自动标识功能与手工的 Port Fast 冲突时，以手工配置的为准。

该功能作用于指派口与下游端口进行快速协商转发的过程中，所以 STP 协议不支持该功能。同时如果指派口已经处于转发状态，对该端口进行 Autoedge 的配置不会生效，只有在重新快速协商的过程中才生效，如拔插网线。

端口如果先打开了 BPDU Filter,则该端口直接 Forwarding，不会自动识别为边缘口。

该功能只适用与指派口。

8.2.10 ROOT Guard功能

在网络设计中常常将根桥和备份根桥划分在同一个域内，由于维护人员的错误配置或网络中的恶意攻击，根桥有可能收到优先级更高的配置信息，从而失去当前根桥的位置，引起网络拓扑的错误的变动。Root Guard 功能就是为了防止这种情况的出现。

接口打开 Root Guard 功能时，强制其在所有实例上的端口角色为指定端口，一旦该端口收到优先级更高的配置信息时，Root Guard 功能会将该接口置为 root-inconsistent (blocked)状态,在足够长的时间内没有收到更优的配置信息时，端口会恢复成原来的正常状态。

当端口因 Root Guard 而处于 blocked 状态时，可以通过手动恢复为正常状态，即关闭端口的 ROOT Guard 功能或关闭接口的保护功能（在接口模式下配置 spanning-tree guard none）。

- 错误的使用 ROOT Guard 特性会导致网络链路的断开。
- 在非指派口上打开 ROOT Guard 功能会强制其为指派口，同时端口会进入 BKN 状态，该状态表示端口因 Root 不一致而进入 blocked 状态。
- 如果端口在 RST0 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。

8.2.11 LOOP Guard功能

由于单向链路的故障，根口或备份口由于收不到 BPDU 会变成指派口进入转发状态，从而导致了网络中环路的产生，LOOP Guard 功能防止了这种情况的发生。

对于配置了环路保护的端口，如果收不到 BPDU，会进行端口角色的迁移，但端口状态将一直被设成 discarding 状态。直到重新收到 BPDU 而进行生成树的重计算。

- 可以基于全局或接口打开 LOOP Guard 特性。
- 端口的 ROOT Guard 和 LOOP Guard 同一时刻只能有一个生效。

8.3 配置RSTP

8.3.1 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	RSTP
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)。

8.3.2 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 RSTP 协议。
设备的缺省状态是关闭 Spanning-tree 协议。
进入特权模式，按以下步骤打开 Spanning Tree 协议：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **spanning-tree**	打开 Spanning Tree 协议。
Ruijie(config)# **end**	退回到特权模式。
Ruijie# **show spanning-tree**	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

如果要关闭 Spanning Tree 协议，可用 **no spanning-tree** 全局配置命令进行设置。

8.3.3 配置Spanning Tree的模式

按 802.1 相关协议标准，STP、RSTP 这两个版本的 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。设备的缺省模式是 RSTP 模式。
进入特权模式，按以下步骤打开 Spanning Tree 协议：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **spanning-tree mode rstp / stp**	切换 Spanning Tree 模式。
Ruijie(config)# **end**	退回到特权模式。
Ruijie# **show spanning-tree**	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

如果要恢复 Spanning Tree 协议的缺省模式，可用 **no spanning-tree mode** 全局配置命令进行设置。

8.3.4 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朴结构。建议管理员把核心设备的优先级设得高些（数值小），这样有利于整个网络的稳定。

如 Bridge ID 所讲，优先级的设置值有 16 个，都为 4096 的倍数，分别是 0，4096，8192，12288，16384，20480，24576，28672，32768，36864，40960，45056，49152，53248，57344，61440。缺省值为 32768。
进入特权模式，按以下步骤配置设备优先级：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **spanning-tree priority** *priority*	*priority*，取值范围为 0 到 61440，按 4096 的倍数递增，缺省值为 32768。
Ruijie(config)# **end**	退回到特权模式。
Ruijie# **show running-config**	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

您如果要恢复到缺省值，可用 **no spanning-tree mst** *instance-id* **priority** 全局配置命令进行设置。

8.3.5 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。

和设备的优先级一样，可配置的优先级值也有 16 个，都为 16 的倍数，分别是 0，16，32，48，64，80，96，112，128，144，160，176，192，208，224，240。缺省值为 128。
进入特权模式，按以下步骤配置端口优先级：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **interface** *interface-id*	进入该 interface 的配置模式，合法的 interface 包括物理端口和 Aggregate Link。
Ruijie(config-if)# **spanning-tree port-priority** *priority*	*priority*，配置该 interface 的优先级，取值范围为 0 到 240，按 16 的倍数递增，缺省值为 128
Ruijie(config-if)# **end**	退回到特权模式。
Ruijie# **show spanning-tree interface** *interface-id*	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

您如果要恢复到缺省值，可用 **no spanning-tree port-priority** 接口配置命令进行设置。

8.3.6 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。
进入特权模式，按以下步骤配置端口路径花费：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **interface** *interface-id*	进入该 interface 的配置模式，合法的 interface 包括物理端口和 Aggregate Link。
Ruijie(config-if)# **spanning-tree cost** *cost*	*cost*，配置该端口上的花费，取值范围为 1 到 200,000,000。缺省值为根据 interface 的链路速率自动计算。
Ruijie(config-if)# **end**	退回到特权模式。
Ruijie# **show spanning-tree interface** *interface-id*	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

您如果要恢复到缺省值，可用 no spanning-tree mst cost 接口配置命令进行设置。

8.3.7 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-1998 和 IEEE 802.1t 对相同的链路速率规定了不同 Path Cost 值，802.1d-1998 的取值范围是短整型（short）（1—65535），802.1t 的取值范围是长整型（long）(1—200,000,000)。其中对于 AP 的 Cost 值有两个方案：我司的私有方案固定为物理口的 Cost 值*95%；标准推荐的方案为 20,000,000,000/(AP 的实际链路带宽)，其中 AP 的实际链路带宽为成员口的带宽*UP 成员口个数。请管理员一定要统一好整个网络内 Path Cost 的标准。缺省模式为私有长整型模式。

下表列出两种方法对不同链路速率自动设置的 Path Cost。

端口速率	Interface	IEEE 802.1d（short）	IEEE 802.1t（long）	IEEE 802.1t（long standard）
10M	普通端口	100	2000000	2000000
	Aggregate Link	95	1900000	2000000÷linkupcnt
100M	普通端口	19	200000	200000
	Aggregate Link	18	190000	200000÷linkupcnt
1000M	普通端口	4	20000	20000
	Aggregate Link	3	19000	20000÷linkupcnt
10000M	普通端口	2	2000	2000
	Aggregate Link	1	1900	2000÷linkupcnt

默认采用我司的私有长整型模式。修改成标准推荐方案的 path cost 方案后，AP 的 cost 会随着 UP 成员口数量的变化而变化，而端口 cost 值变化会导致网络拓扑发生变化。

AP 为静态 AP 时，表格中的 linkupcnt 为 UP 成员口个数；AP 为 LACP AP 时，表格中的 linkupcnt 为参与 AP 数据转发的成员口个数；当 AP 内没有任何成员口 linkup 时，linkupcnt 为 1。具体 AP 和 LACP 的配置，请参见《AP-SCG.doc》和《LACP-SCG.doc》的说明。

进入特权模式，按以下步骤配置端口路径花费的缺省计算方法：

命令	作用

Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **spanning-tree pathcost method** {{**long** [**standard**]} | **short**}	配置端口路径花费的缺省计算方法，设置值为私有长整型（long）、标准长整形(standard long)或短整型（short），缺省值为私有长整型（long）。
Ruijie(config)# **end**	退回到特权模式。
Ruijie# **show running-config**	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

您如果要恢复到缺省值，可用 **no spanning-tree pathcost method** 全局配置命令进行设置。

8.3.8 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
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **spanning-tree hello-time** *seconds*	配置 hello_time，取值范围为 1 到 10 秒，缺省值为 2 秒。
Ruijie(config)# **end**	退回到特权模式。
Ruijie# **show running-config**	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

您如果要恢复到缺省值，可用 no spanning-tree hello-time 全局配置命令进行设置。

8.3.9 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
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **spanning-tree forward-time** *seconds*	配置 forward delay time，取值范围为 4 到 30 秒，缺省值为 15 秒。
Ruijie(config)# **end**	退回到特权模式。
Ruijie# **show running-config**	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

您如果要恢复到缺省值，可用 **no spanning-tree forward-time** 全局配置命令进行设置。

8.3.10 配置Max-Age Time

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **spanning-tree max-age** *seconds*	配置 max age time，取值范围为 6 到 40 秒，缺省值为 20

	秒。
Ruijie(config)# **end**	退回到特权模式。
Ruijie# **show running-config**	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

您如果要恢复到缺省值，可用 **no spanning-tree max-age** 全局配置命令进行设置。

Hello Time、Forward-Delay Time、Max-Age Time 除了有一个自身的取值范围外，这三个之间还有一个制约关系，就是：2*(Hello Time + 1.0 seconds) <= Max-Age Time <= 2*(Forward-Delay – 1.0seconds)。您配置的这三个参数必须满足这个条件，否则有可能导致拓扑不稳定。

8.3.11 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
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **spanning-tree tx-hold-count** *numbers*	配置每秒最多发送 BPDU 个数，取值范围为 1 到 10 个，缺省值为 3 个。
Ruijie(config)# **end**	退回到特权模式。
Ruijie# **show running-config**	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

您如果要恢复到缺省值，可用 **no spanning-tree tx-hold-count** 全局配置命令进行设置。

8.3.12 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
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **interface** *interface-id*	进入接口配置模式
Ruijie(config-if)# **spanning-tree link-type point-to-point / shared**	配置该 interface 的连接类型，缺省值为根据端口“双工”状态来自动判断是不是“点对点连接”。全双工为“点对点连接”，即可以快速 FORWARDING。
Ruijie(config-if)# **end**	退回到特权模式。
Ruijie# **show running-config**	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

您如果要恢复到缺省值，可用 **no spanning-tree link-type** 接口配置命令进行设置。

8.3.13 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
Ruijie# **clear spanning-tree detected-protocols**	对所有端口强制版本检查
Ruijie# **clear spanning-tree detected-protocols interface** *interface-id*	针对一个端口进行版本检查

8.3.14 配置Maximum-Hop Count

配置 Maximum-Hop Count，指定了 BPDU 在一个 Region 内经过多少台设备后被丢弃。它对所有 Instance 有效。

进入特权模式，按以下步骤配置 Maximum-Hop Count：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **spanning-tree max-hops** *hop-count*	配置 Maximum-Hop Count，范围为 1－40，缺省值为 20
Ruijie(config)# **end**	退回到特权模式。
Ruijie# **show running-config**	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

您如果要恢复到缺省值，可用 **no spanning-tree max-hops** 全局配置命令进行设置。

8.3.15 清除STP统计信息

该设置是清除 STP 的收发包统计信息。收发包统计信息可以通过 **show spanning-tree counters** 命令查看。

命令	作用
Ruijie# **clear spanning-tree counters**	清除所有端口的收发包统计信息
Ruijie# **clear spanning-tree counters interface** *interface-id*	清除指定端口的收发包统计信息

8.4 配置RSTP可选特性

8.4.1 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功能缺省打开外，其它功能缺省都是关闭的。

8.4.2 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
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **interface** *interface-id*	进入该 interface 的配置模式，合法的 interface 包括物理端口和 Aggregate Link。
Ruijie(config-if)# **spanning-tree portfast**	打开该 interface 的 portfast。
Ruijie(config-if)# **end**	退回到特权模式。
Ruijie# **show spanning-tree interface** *interface-id* **portfast**	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

您如果要关闭 Port Fast，在 Interface 配置模式下用 **spanning-tree portfast disable** 命令进行设置。

您可以用全局配置命令 **spanning-tree portfast default** 来打开所有端口的 Portfast。

8.4.3 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
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **spanning**-tree **portfast Bpduguard default**	全局的打开 BPDU guard
Ruijie(config)# **interface** *interface-id*	进入该 interface 的配置模式，合法的 interface 包括物理端口和 Aggregate Link。
Ruijie(config-if)# **spanning-tree portfast**	打开该 interface 的 portfast。全局的 BPDU guard 配置才生效。
Ruijie(config-if)# **end**	退回到特权模式。
Ruijie# **show running-config**	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

您如果要关闭 BPDU Guard，可在全局配置命令 **no spanning-tree portfast bpduguard default** 进行设置。

您如果要针对单个 Interface 打开 BPDU Guard，您可用 Interface 配置命令 **spanning-tree bpduguard enable** 进行设置，用 **spanning-tree bpduguard disable** 关闭 BPDU guard。

8.4.4 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
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **spanning-tree portfast bpdufilter default**	全局的打开 BPDU filter
Ruijie(config)# **interface** *Interface-id*	进入该 interface 的配置模式，合法的 interface 包括物理端口和 Aggregate Link。
Ruijie(config-if)# **spanning-tree portfast**	打开该 interface 的 portfast。全局的 BPDU filter 配置才生

	效。
Ruijie(config-if)# **end**	退回到特权模式。
Ruijie# **show running-config**	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

您如果要关闭 BPDU Filter，可以用全局配置命令 **no spanning-tree portfast bpdufilter default** 进行设置。

您如果要针对单个 Interface 打开 BPDU Filter，您可以用 Interface 配置命令 **spanning-tree bpdufilter enable** 进行设置，用 **spanning-tree bpdufilter disable** 关闭 BPDU Guard。

8.4.5 打开Tc_Protection

进入特权模式，按以下步骤配置 Tc_Protection：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **spanning-tree tc-protection**	打开 tc-protection
Ruijie(config)# **end**	退回到特权模式。
Ruijie# **show running-config**	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

您如果要关闭 Tc_Protection，可以用全局配置命令 **no spanning-tree tc-protection** 进行设置。

8.4.6 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
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **spanning-tree tc-protection tc-guard**	打开全局的 TC Guard
Ruijie(config)# **end**	退回到特权模式。
Ruijie# **show running-config**	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

进入特权模式，按以下步骤配置接口下的 TC Guard

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **interface** *Interface-id*	进入该 interface 的配置模式，合法的 interface 包括物理端口和 Aggregate Link。
Ruijie(config-if)# **spanning-tree tc-guard**	打开该 interface 的 TC Guard。
Ruijie(config-if)# **end**	退回到特权模式。
Ruijie# **show running-config**	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

8.4.7 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
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **interface** *Interface-id*	进入该 interface 的配置模式，合法的 interface 包括物理端口和 Aggregate Link。
Ruijie(config-if)# **spanning-tree ignore tc**	打开该 interface 的 TC 过滤
Ruijie(config-if)# **end**	退回到特权模式。
Ruijie# **show running-config**	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

您如果需要关闭 TC 过滤功能，可以在接口模式下使用 **no spanning-tree ignore tc** 命令进行设置。

8.4.8 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
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **interface** *Interface-id*	进入该 interface 的配置模式，合法的 interface 包括物理端口和 Aggregate Link。
Ruijie(config-if)#**bpdu src-mac-check** *H.H.H*	打开 bpdu 源 mac 检查。
Ruijie(config-if)# **end**	退回到特权模式。
Ruijie# **show running-config**	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

您如果要关闭 bpdu 源 mac 检查，可以用接口下配置命令 **no bpdu src-mac-check** 进行设置。

8.4.9 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
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **interface** *interface-id*	进入该 interface 的配置模式，合法的 interface 包括物理端口和 Aggregate Link。
Ruijie(config-if)# **spanning-tree autoedge**	打开该 interface 的 autoedge。
Ruijie(config-if)# **end**	退回到特权模式。
Ruijie# **show spanning-tree interface** *interface-id*	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

您如果要关闭 Autoedge，在 Interface 配置模式下用 **spanning-tree autoedge disabled** 命令进行设置。

8.4.10 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
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **interface** Interface-id	进入该 interface 的配置模式，合法的 interface 包括物理端口和 Aggregate Link。
Ruijie(config-if)# **spanning-tree guard root**	打开接口的 ROOT Guard 特性
Ruijie(config-if)# **end**	退回到特权模式。
Ruijie# **show running-config**	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

8.4.11 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
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **spanning-tree Loopguard default**	打开全局的 LOOP Guard。
Ruijie(config)# **end**	退回到特权模式。
Ruijie# **show running-config**	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

进入特权模式，按以下步骤配置接口下的 LOOP Guard

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **interface** *Interface-id*	进入该 interface 的配置模式，合法的 interface 包括物理端口和 Aggregate Link。
Ruijie(config-if)# **spanning-tree guard loop**	打开该 interface 的 Loop Guard。
Ruijie(config-if)# **end**	退回到特权模式。
Ruijie# **show running-config**	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

8.4.12 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
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **interface** *Interface-id*	进入该 interface 的配置模式，合法的 interface 包括物理端口和 Aggregate Link。
Ruijie(config-if)# **spanning-tree guard none**	关闭接口的 guard 功能
Ruijie(config-if)# **end**	退回到特权模式。
Ruijie# **show running-config**	核对配置条目。

Ruijie# **copy running-config startup-config**	保存配置。

8.5 显示RSTP配置和状态

MSTP 提供了如下的显示命令命令用于查看各种配置信息及运行时信息，各命令的功能说明如下：

命令	作用
show spanning-tree	显示 RSTP 的各项参数信息及生成树的拓扑信息
show spanning-tree counters	显示 RSTP 的收发包统计信息
show spanning-tree summary	显示 RSTP 的各 instance 的信息及其端口转发状态信息
show spanning-tree inconsistentports	显示因根保护或环路保护而 block 的端口
show spanning-tree interface *interface-id*	显示指定 interface 的所有 instance 的 RSTP 信息
show spanning-tree forward-time	显示 forward-time
show spanning-tree hello time	显示 Hello time
show spanning-tree max-hops	显示 max-hops
show spanning-tree tx-hold-count	显示 tx-hold-count
show spanning-tree pathcost method	显示 pathcost method

9 配置协议帧透传

9.1 概述

协议帧透传功能是指在开启特定的协议后，保证协议帧可以继续转发到其他网络设备上。

支持的协议帧透传有：BPDU，GVRP，802.1X，保留组播协议，CISCO 私有 PVST 协议。各协议帧的说明如下：

BPDU 协议帧：生成树协议使用的协议帧，包括 IEEE 标准规定的协议帧和锐捷私有的协议帧。该配置文档中可配置透传的是锐捷私有的 BPDU 协议帧，协议帧通过二层目的 MAC 地址来标识，目的 MAC 地址为 01D0:F800:0000。

GVRP 协议帧：通用 VLAN 注册协议帧，包括 IEEE 标准规定的协议帧和锐捷私有的协议帧。该配置文档中可配置透传的是锐捷私有的 GVRP 协议帧，协议帧通过二层目的 MAC 地址来标识，目的 MAC 地址为 01D0:F800:0021。

802.1X 协议帧：IEEE 制定关于用户接入网络的认证标准协议帧，包括 IEEE 标准规定的协议帧和锐捷私有的协议帧。协议帧通过二层目的 MAC 地址来标识，标准协议帧的目的 MAC 地址为 0180:C200:0003，锐捷私有的 802.1X 协议帧的目的 MAC 地址为 01D0:F800:0003。

保留组播协议帧：IEEE 标准规定保留组地址。这些保留组地址通过二层目的 MAC 地址来标识，该配置文档中可配置透传的组地址范围为：0180:C200:0000 – 0180:C200:FFFF。对于该配置中同 802.1X 协议帧冲突部分地址，以 802.1X 协议帧配置为准。

PVST 协议帧：CISCO 私有的生成树协议帧。该协议帧通过目的 MAC 标识，目的 MAC 地址为：0100:0CCC:CCCD。

☑ 目前 NBS200F 系列设备只支持 BPDU、GVRP、802.1X 这三种协议帧的透传。

9.2 配置协议帧透传

下面列出协议帧透传的缺省配置，在未开启对应协议情况下，这些协议帧将被认为是二层组播地址。

功能特性	缺省值
BPDU 协议帧透传	关闭
GVRP 协议帧透传	关闭
802.1X 协议帧透传	开启
保留组播协议帧透传	开启
PVST 协议帧透传	开启

9.2.1 BPDU协议帧透传配置

在全局配置模式下，执行如下命令可以在设备上开启 BPDU 协议帧透传功能：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式
Ruijie(config)# **bridge-frame forwarding protocol bpdu**	开启 BPDU 协议帧透传功能

Ruijie(config)# **end**	退回到特权模式

9.2.2 GVRP协议帧透传配置

在全局配置模式下，执行如下命令可以在设备上开启 GVRP 协议帧透传功能：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式
Ruijie(config)# **bridge-frame forwarding protocol gvrp**	开启 GVRP 协议帧透传功能
Ruijie(config)# **end**	退回到特权模式

9.2.3 802.1X协议帧透传配置

在全局配置模式下，执行如下命令可以在设备上开启 802.1X 协议帧透传功能：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式
Ruijie(config)# **bridge-frame forwarding protocol 802.1x**	开启 802.1X 协议帧透传功能
Ruijie(config)# **end**	退回到特权模式

10 GVRP

10.1 概述

GVRP（GARP VLAN Registration Protocol）是一种动态配置和扩散 VLAN 成员关系的 GARP（Generic Attribute Registration Protocol，通用属性注册协议）应用。

通过 GVRP 协议，设备可以：

设备监听各端口上的 GVRP PDU，从 GVRP PDU 中学习到与之相连的 GVRP-aware 设备的 VLAN 信息，并据此配置接收 GVRP PDU 的端口上的 VLAN 成员。

通过发送 GVRP PDU 的方式，设备可以在各端口上通告端口的 VLAN 信息。通告的 VLAN 信息包括本机的静态配置及通过 GVRP 从其它设备上学习到的信息。

通过 GVRP，交换网内的设备可动态创建 VLAN，并且实时保持 VLAN 配置的一致性。通过在网络内部自动通告 VLAN ID，GVRP 降低了由于配置不一致而产生错误的可能性。而且，当一个设备上的 VLAN 配置发生变化时，GVRP 可以自动改变相连设备上的 VLAN 配置，从而减少用户的手工配置工作。

GARP 与 GVRP 是由下列标准定义的：

- IEEE standard 802.1D
- IEEE standard 802.1Q

10.2 配置GVRP

10.2.1GVRP 缺省配置

下表显示 GVRP 缺省配置：

功能特性	缺省值
GVRP global enable state	Disabled
GVRP dynamic creation of VLANs	Disabled
GVRP base vlan id	VLAN 1(仅在 MSTP 环境中起作用)
GVRP registration mode	Enable
GVRP applicant state	Normal, (Ports do not declare VLANs when in STP blocking state)
GVRP timers	Join Time: 200 ms Leave Time: 600 ms Leaveall Time: 10,000 ms

10.2.2 GVRP 配置指南

相互连接进行通信的两台设备都应启动 GVRP，GVRP 信息只在 Trunk Links 中传播，但传播的信息包括当前设备的所有 VLAN 信息，不管 VLAN 是动态学习的，或是手工设置的。

在运行 STP（Spanning-tree Protocol）的情况下，只有状态为 Forwarding 的端口才会参与 GVRP 的运行，如接收、发送 GVRP PDU，只有状态为 Forwarding 的端口的 VLAN 信息会被 GVRP 扩散。

所有由 GVRP 添加的 VLAN Port 都是 Tagged Port。

所有由 GVRP 动态学习的 VLAN 信息都未保存在系统中，当设备复位时，这些信息将全部丢失。用户也不可以保存这些动态学习到的 VLAN 信息。

由 GVRP 创建的动态 VLAN 的参数不能修改。

网络中所有需要交换 GVRP 信息的设备的 GVRP Timers（Join，Leave，Leaveall）必须保持一致。

10.2.3 启动 GVRP

只有在全局使能允许的情况下 GVRP 才会启动。

在 GVRP 未全局使能的状态下，其它 GVRP 参数可以进行配置，但只有在 GVRP 开始运行时，这些 GVRP 选项设置才能发生作用。

全局控制 GVRP：

命令	作用
Ruijie(config)# [**no**] **gvrp enable**	启用 GVRP(如果为关闭的话)

举例如下：

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

10.2.4 控制动态 VLAN 的创建

当一个端口接收到的信息（仅限于 Joinin Joinempty）中所指示的 VLAN 在本地设备不存在时，GVRP 可能会创建这个 VLAN。是否允许动态创建 VLAN 由用户控制。

控制创建动态 VLAN：

命令	作用
Ruijie(config)# [**no**] **gvrp dymanic-vlan-creation enable**	允许 GVRP 动态创建 VLAN (如果为关闭的话)

用户不能修改由 GVRP 创建的动态 VLAN 的参数。

举例如下：

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

10.2.5 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。

10.2.6 配置端口的登记方式

端口有两种登记模式：

- GVRP Registration Normal
- GVRP Registration Disabled

将一个端口设置为 **normal registration** 模式，将允许动态创建（如果 Dynamic VLAN Creation Enabled）、登记或注销端口上的 VLAN。

当端口设置为 **disabled registration** 模式时，禁止任何动态登记或注销 VLAN 的行动。

设置端口的 GVRP Registration Mode：

命令	作用
Ruijie(config-if)# [**no**] **gvrp registration mode {normal | disabled}**	设置端口的 GVRP 登记模式

这两种登记模式不会影响端口上的静态 VLAN，用户创建的静态 VLAN 永远都是 Fixed Registrar。

打开端口 1 的 Registration Mode 的示例：

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# gvrp registration mode enable normal
Ruijie(config-if)# end
```

10.2.7 配置端口的通告模式

端口有两种通告模式，控制端口是否发送 GVRP 通告。

- GVRP Normal Applicant

允许在端口上通告本端口的 VLAN，包括所有动态及静态 VLAN。

- GVRP Non-Applicant

禁止在端口上通告本端口的 VLAN。

设置端口的通告模式：

命令	作用
Ruijie(config-if)# [**no**] **gvrp applicant state** {**normal** | **non-applicant**}	设置端口的 GVRP 通告模式

设置端口 1 的 Applicant State 的示例：

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# gvrp applicant state normal
Ruijie(config-if)# end
```

10.2.8 设置 GVRP 定时器

GVRP 中使用了三个定时器：

- Join Timer

Join Timer 控制端口发出通告前的最大时延，实际发送间隔在 0 到这个最大时延之间。缺省值是 200ms。

- Leave Timer

Leave Timer 控制端口在接收到 Leave Message 后，将端口从 VLAN 中删除前所要等待的时间，如果在这个时间段内端口重新收到 Join Message，则端口的 VLAN 成员关系仍然保留，同时定时器失效；如果在定时器超时前仍未收到 Join Message，则端口的状态变为 Empty，端口从 VLAN 成员表中删除。缺省值是 600ms。

- LeaveAll Timer

LeaveAll Timer 控制在端口上发送 LeaveAll Message 的最小间隔，如果在定时器超时前端口收到 LeaveAll Message，则定时器开始重新计时；如果定时器超时，则在端口上发送 LeaveAll Message，LeaveAll Message 同时也发送给端口本身，从而触发 Leave Timer 也开始计数。缺省值是 10,000ms。实际发送间隔在 Leaveall 与 Leaveall + Join 之间。

设置定时器时，必须保证 Leave Value 大于或等于三倍的 Join Value(Leave >= Join * 3)，同时 Leaveall 必须大于 Leave(Leaveall > Leave)。 如果不能满足以上条件，设置定时器操作将返回失败。例如，如果在设置 Leave

Timer 为 600ms 后，设置 Join Timer 为 320ms 将会显示出错提示。要使操作成功，当 Join Timer 为 350ms 时，Leave Timer 要不小于 1050ms。

在实际组网中，建议用户将 GVRP 定时器配置为以下的推荐值：

Join Timer：6000ms（6 秒钟）；

Leave Timer：30000ms（30 秒钟）；

LeaveAll Timer：120000ms（2 分钟）。

定时器设置的有效粒度是 10ms。

要保证所有互联的 GVRP 设备中的 GVRP Timer 设置保持一致，否则 GVRP 可能工作异常。

调整 GVRP Timer 的数值：

命令	作用
Ruijie(config)# **[no] gvrp timer {join | leave | leaveall}** *timer-value*	设置端口的定时器值

设置 GVRP Join Timer 的示例：

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

10.2.9 显示 GVRP 的配置和状态

显示 GVRP 的统计值

GVRP 的统计值是以端口为单位计算的，显示统计值命令的详细使用方法及各项统计值的含义请参照命令行接口 **show gvrp statistics**。

显示端口的 GVRP 统计值：

命令	作用
Ruijie# **show gvrp statistics** {*interface-id* | **all**}	显示端口的统计值

显示 GVRP 统计值的示例：

```
Ruijie# show gvrp statistics gigabitethernet 1/1
Interface  GigabitEthernet 3/1
RecValidGvrpPdu    0
RecInvalidGvrpPdu   0
RecJoinEmpty    0
RecJoinIn       0
```

```
RecEmpty        0
RecLeaveEmpty   0
RecLeaveIn      0
RecLeaveAll     0
SentGvrpPdu     0
SentJoinEmpty   0
SentJoinIn      0
SentEmpty       0
SentLeaveEmpty  0
SentLeaveIn     0
SentLeaveAll    0
JoinIndicated   0
LeaveIndicated  0
JoinPropagated  0
LeavePropagated  0
```

清除 GVRP 的统计值，使其重新开始计数：

命令	作用
Ruijie# **clear gvrp statistics** {*interface-id* | **all**}	清除端口的统计值

清除端口一上 GVRP 统计值的示例：

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

显示 GVRP 的运行状态

GVRP 的当前运行状态可通过 **show gvrp status** 命令来察看。这条命令可以显示当前的动态创建的 VLAN，及静态 VLAN 的动态逻辑端口。

命令	作用
Ruijie# **show gvrp status**	显示当前 GVRP 的运行状态

举例如下：

```
Ruijie# show gvrp status
VLAN 1
Dynamic Ports:
DVLAN 5
Dynamic Ports:
Port:GigabitEthernet 3/1
```

显示 GVRP 的当前配置

GVRP 的当前运行状态可通过 **show gvrp configuration** 命令来察看。这条命令可以显示当前的动态创建的 VLAN，及静态 VLAN 的动态逻辑端口。

命令	作用
Ruijie# **show gvrp configuration**	显示当前 GVRP 的配置状态

举例如下：

```
Ruijie# show gvrp configuration
Global GVRP Configuration:
GVRP Feature:enabled
GVRP dynamic VLAN creation:enabled
Join Timers(ms):200
Join Timers(ms):600
Join Timers(ms):10000
Port based GVRP Configuration:
Port:GigabitEthernet 3/1 app mode:normal reg mode:normal
Port:GigabitEthernet 3/2 app mode:normal reg mode:normal
Port:GigabitEthernet 3/3 app mode:normal reg mode:normal
Port:GigabitEthernet 3/4 app mode:normal reg mode:normal
Port:GigabitEthernet 3/5 app mode:normal reg mode:normal
Port:GigabitEthernet 3/6 app mode:normal reg mode:normal
Port:GigabitEthernet 3/7 app mode:normal reg mode:normal
Port:GigabitEthernet 3/8 app mode:normal reg mode:normal
Port:GigabitEthernet 3/9 app mode:normal reg mode:normal
Port:GigabitEthernet 3/10 app mode:normal reg mode:normal
Port:GigabitEthernet 3/11 app mode:normal reg mode:normal
Port:GigabitEthernet 3/12 app mode:normal reg mode:normal
```

11 LLDP

11.1 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。

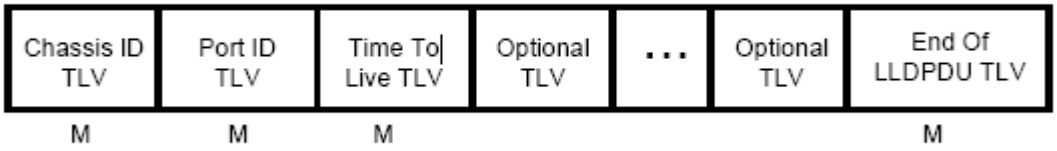
通过 LLDP，网络管理系统可以掌握拓扑的连接情况，比如设备的哪些端口与其它设备相连接，链路连接两端的端口的速率、双工是否匹配等，管理员可以根据这些信息快速地定位及排查故障。

11.1.1 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 1-1 LLDPDU 格式



其中：

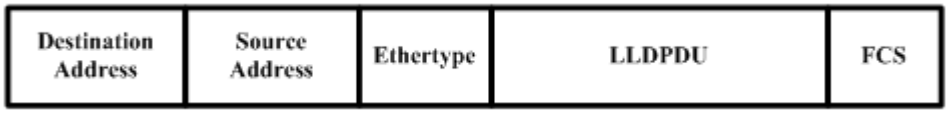
- M 表示是固定的 TLV。
- 在 LLDPDU 中，Chassis ID TLV、Port ID TLV、Time To Live TLV 和 End Of LLDPDU TLV 是必须携带的，而其它类型的 TLV 是可选携带。

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 1-2 Ethernet II 格式封装的 LLDP 报文

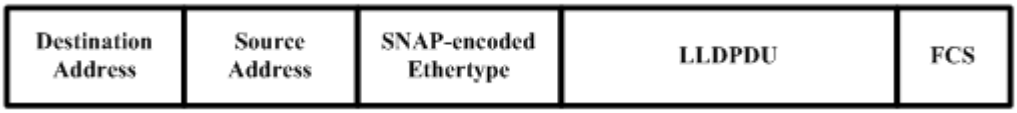


其中：

- 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 1-3 SNAP 格式封装的 LLDP 报文



其中：

- Destination Address：目的 MAC 地址，为 LLDP 的组播地址 01-80-C2-00-00-0E。
- Source Address：源 MAC 地址，为设备的二层 MAC 地址。
- SNAP-encoded Ethertype：SNAP 封装的以太网类型，为 AA-AA-03-00-00-00-88-CC.。
- LLDPDU：LLDP 协议数据单元。
- FCS：帧校验序列。

TLV

LLDPDU 中封装的 TLV 可以分成二个大类：

- 基本管理 TLV
- 组织定义 TLV

基本管理 TLV 是一组用于网络管理的基础 TLV 集合。组织定义 TLV 是由标准组织和其它机构定义的 TLV，比如 IEEE 802.1 组织、IEEE 802.3 组织分别定义了各自的 TLV 集合。

6) 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。

7) 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：

8) 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。

9) 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。

10) 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。

11.1.2 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。

11.1.3 协议规范

LLDP 相关的协义规范和标准有：

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

11.2 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

11.2.1 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

11.2.2 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
```

11.2.3 配置 LLDP 工作模式

缺省情况下，接口的 LLDP 功能处于打开状态，且缺省工作在 TxRx 模式，用户可根据实际需要将工作模式修改为 Tx 或 Rx 模式。按以下步骤配置 LLDP 工作模式。

命令	作用
Ruijie(config)# **interface** *interface-name*	进入接口配置模式。LLDP 运行在实际的物理接口上（对于 AP 口，则实际是运行在 AP 成员口上）。堆叠口，VSL 口不支持 LLDP。
Ruijie(config-if)#**lldp mode** { **tx** | **rx** | **txrx** }	配置 LLDP 工作模式。可配置的工作模式为 tx、rx、txrx。
Ruijie(config-if)#**show lldp status interface** *interface-name*	显示接口的 LLDP 状态信息

配置举例：

配置接口上的 LLDP 工作模式为 Tx，并查看接口的 LLDP 状态信息

```
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#lldp mode tx
Ruijie(config-if-GigabitEthernet 0/1)#show lldp status interface gigabitethernet 0/1
Port [GigabitEthernet 0/1]
Port status of LLDP             : Enable
Port state                      : UP
Port encapsulation              : Ethernet II
Operational mode                : TxOnly
Notification enable             : NO
Error detect enable             : YES
Number of neighbors             : 0
Number of MED neighbors         : 0
```

11.2.4 配置允许发布的 TLV 类型

缺省情况下，接口上允许发布除 Location Identification TLV 之外的所有类型的 TLV。按以下步骤配置接口允许发布的 TLV 类型。

命令	作用
Ruijie(config)# **interface** *interface-name*	进入接口配置模式。LLDP 运行在实际的物理接口上（对于 AP 口，则实际是运行在 AP 成员口上）。堆叠口，VSL 口不支持 LLDP。
Ruijie(config-if)# **lldp tlv-enable** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** | **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] } | **dot3-tlv** { **all** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **location** { **civic-location** | **elin** } **identifier** *id* | **network-policy profile** [*profile-num*] | **power-over-ethernet** } }	缺省情况下，接口上允许发布除 Location Identification TLV 之外的所有类型的 TLV
Ruijie(config-if)# **show lldp tlv-config interface** *interface-name*	显示指定接口允许发布的 TLV 属性

配置基本管理 TLV、IEEE 802.1 组织定义 TLV、IEEE 802.3 组织定义 TLV 时，如果指定 **all** 参数，将发布该类型的所有可选 TLV。

配置 LLDP-MED TLV 时，如果指定 **all** 参数，将发布除 Location Identification TLV 之外的所有类型的 LLDP-MED TLV。

配置允许发布 LLDP-MED Capability TLV 时，需要先配置允许发布 LLDP 802.3 MAC/PHY TLV；取消发布 LLDP 802.3 MAC/PHY TLV 时，需要先取消发布 LLDP-MED Capability TLV。

配置 LLDP-MED TLV 时，必须先配置允许发布 LLDP-MED Capability TLV，才可以配置允许发布 LLDP-MED 其它类型的 TLV。

取消发布 LLDP-MED TLV，必须先取消发布 LLDP-MED 其它类型的 TLV，才允许取消发布 LLDP-MED Capability TLV。

关于 lldp tlv-enable 命令的各关键字的含义，请参见 LLDP 配置指导中的描述。

当设备下联 IP 电话，若 IP 电话支持 LLDP-MED，则可以通过配置 network policy TLV 下发策略给 IP 电话。

配置举例：

#配置取消发布 IEEE 802.1 组织定义的 Port And Protocol VLAN ID TLV。

```
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#no lldp tlv-enable dot1-tlv protocol-vlan-id
```

```
Ruijie(config-if-GigabitEthernet 0/1)#show lldp tlv-config interface gigabitethernet 0/1
LLDP tlv-config of port [GigabitEthernet 0/1]
               NAME                  STATUS DEFAULT
------------------------------ ------ -------
Basic optional TLV:
Port Description TLV              YES    YES
System Name TLV                    YES    YES
System Description TLV            YES    YES
System Capabilities TLV           YES    YES
Management Address TLV            YES    YES

IEEE 802.1 extend TLV:
Port VLAN ID TLV                   YES    YES
Port And Protocol VLAN ID TLV    NO     YES
VLAN Name TLV                       YES    YES

IEEE 802.3 extend TLV:
MAC-Physic TLV                      YES    YES
Power via MDI TLV                  YES    YES
Link Aggregation TLV               YES    YES
Maximum Frame Size TLV             YES    YES

LLDP-MED extend TLV:
Capabilities TLV                    YES    YES
Network Policy TLV                  YES    YES
Location Identification TLV       NO     NO
Extended Power via MDI TLV        YES    YES
Inventory TLV                          YES    YES
```

11.2.5 配置 LLDP 报文中发布管理地址

管理地址是提供给网络管理系统用于标识某台网络设备并能进行管理的地址。缺省情况下，在 LLDP 报文中发布管理地址，发布的管理地址为接口允许通过的最小 VLAN 的 IPv4 地址。

按以下步骤配置 LLDP 报文中发布管理地址：

命令	作用
Ruijie(config)# **interface** *interface-name*	进入接口配置模式。LLDP 运行在实际的物理接口上（对于 AP 口，则实际是运行在 AP 成员口上）。堆叠口，VSL 口不支持 LLDP。
Ruijie(config-if)#**lldp management-address-tlv** [*ip-address*]	配置 LLDP 报文中发布的管理地址

Ruijie(config-if)#**show lldp local-information interface** *interface-name*	显示指定接口的 LLDP 本地信息

缺省情况下,LLDP 报文发布管理地址。发布的管理地址为端口允许通过的最小 VLAN 的 IPv4 地址,如果该 VLAN 未配置 IPv4 地址，则继续查找下一个允许通过的最小 VLAN，直到找到 IPv4 地址为止。

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
```

11.2.6 配置快速发送 LLDP 报文的个数

当发现新的邻居，或者 LLDP 工作模式从关闭或 Rx 转变为 TxRx 或 Tx 时，为了让邻居设备尽快地学习到本设备的信息，将启动快速发送机制，快速发送机制缩短 LLDP 报文的发送周期为 1 秒，并连续发送一定数量的 LLDP 报文后再恢复正常的发送周期。

命令	作用
Ruijie(config)#**lldp fast-count** *count*	配置快速发送 LLDP 报文的个数，缺省为 3 个，可配置的范围为 1-10
Ruijie(config-if)#**show lldp status**	显示 LLDP 状态信息

配置举例：

配置快速发送 LLDP 报文的个数为 5 个。

```
Ruijie(config)#lldp fast-count 5
Ruijie(config)#show lldp status
Global status of LLDP                 : Enable
Neighbor information last changed time :
Transmit interval                     : 30s
Hold multiplier                       : 4
Reinit delay                          : 2s
Transmit delay                        : 2s
Notification interval                 : 5s
Fast start counts                     : 5
```

11.2.7 配置 TTL 乘数和 LLDP 报文发送时间间隔

LLDP 报文中 Time To Live TLV 的值=TTL 乘数×报文发送时间间隔+1。因此，通过调整 TTL 乘数可以控制本设备信息在邻居设备的存活时间。

而通过调整 LLDP 报文发送时间间隔，可以调整 LLDP 报文的发送周期。按以下步骤配置 TTL 乘数和 LLDP 报文的发送时间间隔：

命令	作用
Ruijie(config)#**lldp hold-multiplier** *value*	配置 TTL 乘数，缺省值为 4，可配置的范围为 2-10

Ruijie(config)#**lldp timer tx-interval** *seconds*	配置发送 LLDP 报文的时间间隔。缺省发送时间间隔为 30 秒，可配置的范围为 5-32768 秒
Ruijie(config-if)#**show lldp status**	显示 LLDP 状态信息

配置举例：

配置 TTL 乘数为 3，LLDP 报文的发送间隔为 20 秒，此时，本地设备信息在邻居设备的存活时间为 61 秒。

```
Ruijie(config)#lldp hold-multiplier 3
Ruijie(config)#lldp timer tx-interval 20
Ruijie(config)#show lldp status
Global status of LLDP                 : Enable
Neighbor information last changed time :
Transmit interval                     : 20s
Hold multiplier                       : 3
Reinit delay                          : 2s
Transmit delay                        : 2s
Notification interval                 : 5s
Fast start counts                     : 3
```

11.2.8 配置 LLDP 报文的发送延迟时间

当本地信息发生变化时，会立即向邻居设备发送 LLDP 报文。为了避免本地信息频繁变化引起的频繁地发送 LLDP 报文，可以配置 LLDP 报文的发送延迟时间来限制 LLDP 报文的频繁发送。缺省的发送延迟时间为 2 秒，按以下步骤配置 LLDP 报文的发送延迟时间：

命令	作用
Ruijie(config)#**lldp timer tx-delay** *seconds*	配置发送 LLDP 报文的延迟时间
Ruijie(config)#**show lldp status**	显示 LLDP 状态信息

配置举例：

配置发送 LLDP 报文的延迟时间为 3 秒，同时查看 LLDP 状态信息。

```
Ruijie(config)#lldp timer tx-delay 3
Ruijie(config)#show lldp status
Global status of LLDP                 : Enable
Neighbor information last changed time :
Transmit interval                     : 30s
Hold multiplier                       : 4
Reinit delay                          : 2s
Transmit delay                        : 3s
Notification interval                 : 5s
Fast start counts                     : 3
```

11.2.9 配置端口初始化的延迟时间

当端口的工作模式发生变化时，端口将对协议状态机进行初始化操作。为了避免端口的工作模式的频繁变化引起地频繁地初始化状态机，可以配置端口初始化的延迟时间。按以下步骤配置端口初始化的延迟时间：

命令	作用
Ruijie(config)#**lldp timer reinit-delay** *seconds*	配置端口初始化的延迟时间
Ruijie(config)#**show lldp status**	显示 LLDP 状态信息

配置举例：

#配置端口初始化的延迟时间为 3 秒，并显示 LLDP 的状态信息。

```
Ruijie(config)#lldp timer reinit-delay 3
Ruijie(config)#show lldp status
Global status of LLDP                  : Enable
Neighbor information last changed time :
Transmit interval                      : 30s
Hold multiplier                        : 4
Reinit delay                           : 3s
Transmit delay                         : 2s
Notification interval                  : 5s
Fast start counts                      : 3
```

11.2.10 配置 LLDP Trap 功能

通过配置 Trap 功能，可以将本地设备的 LLDP 信息（例如发现新邻居、检测到与邻居的通信链路故障等信息）发送给网管服务器，管理员可以根据此信息监控网络的运行状况。

同时为了防止 LLDP Trap 信息地频繁发送，可以配置发送 LLDP Trap 的时间间隔。在这段时间间隔内，检测到 LLDP 信息变化，将发送 Trap 给网管服务器。

缺省情况下，LLDP Trap 功能处于关闭状态。

按以下步骤可配置 LLDP Trap 功能：

命令	作用
Ruijie(config)#**lldp timer notification-interval** *seconds*	配置发送 LLDP Trap 信息的时间间隔，缺省的时间间隔是 5 秒，可配置的范围是 5-3600
Ruijie(config)# **interface** *interface-name*	进入接口配置模式。LLDP 运行在实际的物理接口上（对于 AP 口，则实际是运行在 AP 成员口上）。堆叠口，VSL 口不支持 LLDP。
Ruijie(config-if)#**lldp notification remote-change enable**	使用 LLDP Trap 功能，缺省情况下，LLDP Trap 功能处于关闭状态。
Ruijie(config-if)#**show lldp status**	显示 LLDP 状态信息

配置举例：

#使能 LLDP Trap 功能，并配置 LLDP Trap 信息的发送时间间隔为 10 秒。

```
Ruijie(config)#lldp timer notification-interval 10
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#lldp notification remote-change enable
Ruijie(config-if-GigabitEthernet 0/1)#show lldp status
Global status of LLDP                 : Enable
Neighbor information last changed time :
Transmit interval                     : 30s
Hold multiplier                       : 4
Reinit delay                          : 2s
Transmit delay                        : 2s
Notification interval                 : 10s
Fast start counts                     : 3
------------------------------------------------------------
Port [GigabitEthernet 0/1]
------------------------------------------------------------
Port status of LLDP             : Enable
Port state                      : UP
Port encapsulation              : Ethernet II
Operational mode                : RxAndTx
Notification enable             : YES
Error detect enable             : YES
Number of neighbors             : 0
Number of MED neighbors         : 0
```

11.2.11配置 LLDP 错误检测功能

配置 LLDP 错误检测功能，错误检测包括链路两端的 VLAN 配置检测、端口状态检测、端口聚合配置检测、MTU 配置检测及环路检测。当 LLDP 检测到错误时，将打印 LOG 信息提示管理员。

按以下步骤配置 LLDP 错误检测功能：

命令	作用
Ruijie(config)# **interface** *interface-name*	进入接口配置模式。LLDP 运行在实际的物理接口上（对于 AP 口，则实际是运行在 AP 成员口上）。堆叠口，VSL 口不支持 LLDP。
Ruijie(config-if)#**lldp error-detect**	配置 LLDP 错误检测功能，缺省情况下，LLDP 错误检测功能打开。
Ruijie(config-if)#**show lldp status interface** *interface-name*	显示接口的 LLDP 状态信息

配置举例：

#配置 LLDP 错误检测功能。

```
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#lldp error-detect
Ruijie(config-if-GigabitEthernet 0/1)#show lldp status interface gigabitethernet 0/1
Port [GigabitEthernet 0/1]
Port status of LLDP             : Enable
Port state                      : UP
Port encapsulation              : Ethernet II
Operational mode                : RxAndTx
Notification enable             : NO
Error detect enable             : YES
Number of neighbors             : 0
Number of MED neighbors         : 0
```

11.2.12配置 LLDP 报文封装格式

缺省情况下，LLDP 报文采用 Ethernet II 格式封装。可配置的封装格式为 Ethernet II 和 SNAP。

配置成 Ethernet II 格式封装时，设备只能发送和接收 Ethernet II 格式的 LLDP 报文。

配置成 SNAP 格式封装时，设备只能发送和接收 SNAP 格式的 LLDP 报文。

按以下步骤配置 LLDP 报文封装格式：

命令	作用
Ruijie(config)# **interface** *interface-name*	进入接口配置模式。LLDP 运行在实际的物理接口上（对于 AP 口，则实际是运行在 AP 成员口上）。堆叠口，VSL 口不支持 LLDP。
Ruijie(config-if)#**lldp encapsulation snap**	配置 LLDP 报文封装格式为 SNAP。
Ruijie(config-if)#**show lldp status interface** *interface-name*	显示接口的 LLDP 状态信息

为了保证本地设备和邻居设备的正常通信，必须将 LLDP 报文配置成相同的封装格式。

配置举例：

#配置 LLDP 报文的封装格式为 SNAP 并查看相应的配置。

```
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#lldp encapsulation snap
Ruijie(config-if-GigabitEthernet 0/1)#show lldp status interface gigabitethernet 0/1
Port [GigabitEthernet 0/1]
Port status of LLDP             : Enable
Port state                      : UP
Port encapsulation              : Snap
```

```
Operational mode                : RxAndTx
Notification enable             : NO
Error detect enable             : YES
Number of neighbors             : 0
Number of MED neighbors         : 0
```

11.2.13配置 LLDP Network Policy 策略

缺省情况下，LLDP 报文采用无应用类型的 network policy tlv。

用户可以按以下步骤配置 network policy：

命令	作用
Ruijie(config)# **lldp network-policy profile** *profile-num*	进入 LLDP network-policy 配置模式。
Ruijie(config-lldp-network-policy)# **{ voice | voice-signaling } vlan { { *vlan-id* [cos *cvalue* | dscp *dvalue*] } | { dot1p [cos *cvalue* | dscp *dvalue*] } | none | untagged }** **no { voice | voice-signaling } vlan**	配置 LLDP network-policy 策略。

当设备下联 IP 电话，若 IP 电话支持 LLDP-MED，则可以通过配置 Network Policy TLV 下发策略给 IP 电话，由 IP 电话修改语音流 Tag 和 QOS。在设备上，除配置上述策外，还需要配置步骤为：1.使能 Voice VLAN 功能，把连接 IP 电话的端口静态加入 Voice VLAN；2.把连接 IP 电话的端口配置为 QOS 信任口（推荐使用信任 DSCP 模式）；3.如果在此端口上同时开启了 1X 认证，则还需要配置一条安全通道，允许 Voice VLAN 内的报文通过。若 IP 电话不支持 LLDP-MED，则必须使能 Voice VLAN 功能，并将话机 MAC 地址手动配置到 Voice VLAN OUI 列表中。

QOS 信任模式的配置方法请参见《IP QOS》章节；Voice VLAN 的配置方法请参见《Voice VLAN》章节；安全通道的配置方法请参见《ACL》章节。

配置举例：

#配置接口 1 发布的 LLDP 报文中 Network Policy TLV 策略为 1：voice 应用类型 vlan id 是 3，cos 是 4，dscp 是 6。

```
Ruijie#config
Ruijie(config)#lldp network-policy profile 1
Ruijie(config-lldp-network-policy)# voice vlan 3 cos 4
Ruijie(config-lldp-network-policy)# voice vlan 3 dscp 6
Ruijie(config-lldp-network-policy)#exit
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# lldp tlv-enable med-tlv network-policy profile 1
```

11.2.14配置设备的普通地址信息

用户可以按以下步骤配置设备的地址信息:

命令	作用
Ruijie(config)# **lldp location civic-location identifier** *id*	进入 LLDP Civic Address 配置模式。
Ruijie(config-lldp-civic)# **device-type** *device-type*	配置设备类型，缺省配置为交换机。
Ruijie(config-lldp-civic)# **{ country | state | county | city | division | neighborhood | street-group | leading-street-dir | trailing-street-suffix | street-suffix | number | street-number-suffix | landmark | additional-location-information | name | postal-code | building | unit | floor | room | type-of-place | postal-community-name | post-office-box | additional-code}** *ca-word*	配置 LLDP 普通地址信息。

配置举例：

#配置设备接口 1 的地址为：交换机设备，地址是国家：CH，城市：Fuzhou，邮编：350000。

```
Ruijie#config
Ruijie(config)#lldp location civic-location identifier 1
Ruijie(config-lldp-civic)# country CH
Ruijie(config-lldp-civic)# city Fuzhou
Ruijie(config-lldp-civic)# postal-code 350000
Ruijie(config-lldp-civic)# exit
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# lldp tlv-enable location civic-location identifier 1
```

11.2.15配置设备的紧急电话号码信息

用户可以按以下步骤配置设备的紧急电话号码信息：

命令	作用
Ruijie(config)# **lldp location elin identifier** *id* **elin-location** *tel-number*	配置紧急电话号码信息。

配置举例：

#配置设备接口 1 的紧急电话号码为：085285555556。

```
Ruijie#config
Ruijie(config)#lldp location elin identifier 1 elin-location 085283671111
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# lldp tlv-enable location elin identifier 1
```

11.2.16查看和清除配置

命令	作用
show lldp local-information [**global** | **interface** *interface-name*]	显示准备发给邻居的设备信息
show lldp location { **civic-location** | **elin** } { **identifier** *id* | **interface** *interface-name* | **static** }	显示本地设备的普通地址信息或者紧急电话号码信息
show lldp neighbors [**interface** *interface-name*] [**detail**]	显示该端口所连接的邻居的设备信息
show lldp network-policy profile [*profile-num*]	显示 LLDP network-policy 配置信息
show lldp statistics [**global** | **interface** *interface-name*]	显示 LLDP 统计信息
show lldp status [**interface** *interface-name*]	显示 LLDP 状态信息
show lldp tlv-config [**interface** *interface-name*]	显示可发布的可选 TLV 信息
clear lldp statistics [**interface** *interface-name*]	清除 LLDP 统计信息
clear lldp table [**interface** *interface-name*]	清除 LLDP 邻居信息

配置举例：

#显示指定端口连接的邻居设备的信息：

```
Ruijie# show lldp neighbors detail
Lldp neighbor-information of port [GigabitEthernet 0/1]
  Neighbor index                    : 1
  Device type                       : LLDP Device
  Update time                       : 12minutes 40seconds
Aging time                          : 5seconds
  Chassis ID type                   : MAC address
  Chassis id                        : 00d0.f822.33cd
  System name                       : System name
  System description               : System description
  System capabilities supported     : Repeater, Bridge, Router
  System capabilities enabled       : Repeater, Bridge, Router

  Management address subtype        : 802 mac address
  Management address                : 00d0.f822.33cd
  Interface numbering subtype       :
  Interface number                  : 0
  Object identifier                 :

  LLDP-MED capabilities             :
  Device class                      :
  HardwareRev                       :
  FirmwareRev                       :
  SoftwareRev                       :
```

```
  SerialNum                          :
  Manufacturer name                  :
  Asset tracking identifier          :

  Port ID type                       : Interface name
  Port id                            : GigabitEthernet 0/2
  Port description                   :

  802.1 organizationally information
  Port VLAN ID                       : 1
  Port and protocol VLAN ID(PPVID)   : 1
      PPVID Supported                : YES
      PPVID Enabled                  : NO
  VLAN name of VLAN 1                : VLAN0001
  Protocol Identity                  :
  802.3 organizationally information
  Auto-negotiation supported         : YES
  Auto-negotiation enabled           : YES
  PMD auto-negotiation advertised    : 1000BASE-T full duplex mode, 100BASE-TX full duplex mode, 100BASE-TX
half duplex mode, 10BASE-T full duplex mode, 10BASE-T half duplex mode
  Operational MAU type               : speed(100)/duplex(Full)
  PoE support                        : NO
  Link aggregation supported         : YES
  Link aggregation enabled           : NO
  Aggregation port ID                : 0
  Maximum frame Size                 : 1500

  LLDP-MED organizationally information
  Power-via-MDI device type          :
  Power-via-MDI power source         :
  Power-via-MDI power priority       :
  Power-via-MDI power value          :
```

关于 LLDP 显示信息的具体含义，请参见《LLDP 命令参考》中的描述。

11.3 LLDP典型配置举例

11.3.1 利用 LLDP 查看拓扑连接情况

组网需求

■ 设备需求

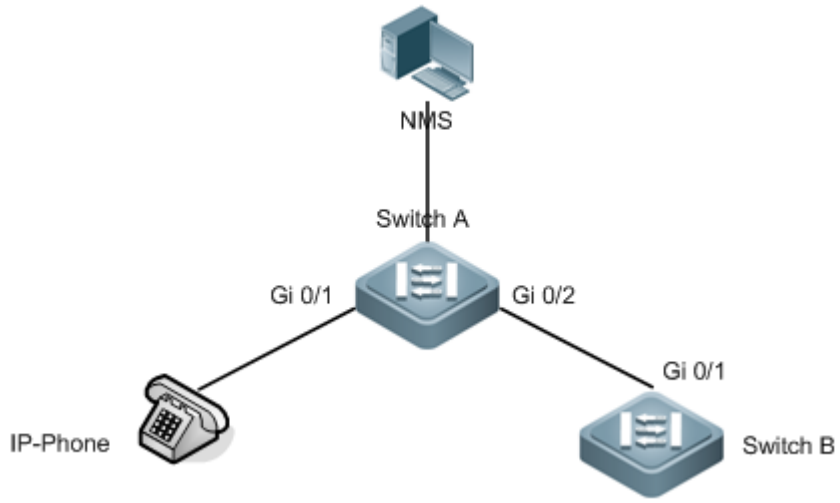
以太网交换机二台（分别以 Switch A 和 Switch B 表示）、MED 设备一台（以 IP Phone 为例）、NMS（Network Management System，网络管理系统）一台。

■ 配置需求

LLDP 功能默认打开，不需要再行配置。

组网拓扑

图 1-4 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         :
```

11.3.2 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 1-5 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。

配置指南-IP 地址及应用

本分册介绍 IP 地址及应用配置指南相关内容，包括以下章节：

1. IP 地址/服务
2. DHCP
3. DNS
4. 网络通信监测工具
5. TCP

1 IP 地址与服务

1.1 配置IP地址

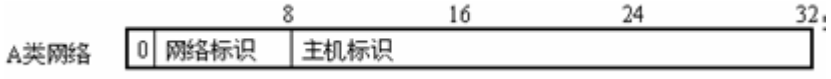
1.1.1 IP地址简介

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

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

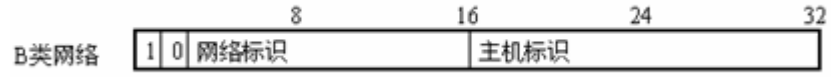
A 类地址，最高比特位为“0”，有 7 个比特位表示网络号，24 个比特位表示本地地址。这样总共有 128 个 A 类网络。

图 1-1



B 类地址，前两个最高比特位为“10”，有 14 个比特位表示网络号，16 个比特位表示本地地址。这样总共有 16,348 个 B 类网络。

图 1-2

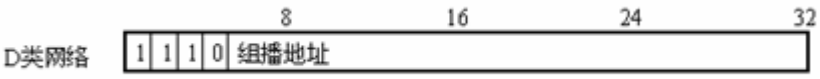


C 类地址，前三个最高比特位为“110”，有 21 个比特位表示网络号，8 个比特位表示本地地址。这样总共有 2,097,152 个 C 类网络。

图 1-3

D 类地址，前四个最高比特位为“1110”，其余比特位为组播地址。

图 1-4



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

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

下表为保留与可用的地址列表：

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

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

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

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

1.1.2 配置IP地址

IP 地址配置任务包括以下各项，但只有第一项配置是必须要做，其它任务可以根据网络的具体需要决定是否要执行。

- 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 配置接口IP地址

一个设备只有配置了 IP 地址，才可以接收和发送 IP 数据包，接口配置了 IP 地址，说明该接口允许运行 IP 协议。

要分配一个接口的 IP 地址，在接口配置模式中执行以下命令：

命令	作用
Ruijie(config-if)# **ip address** *ip-address mask*	设置一个接口的 IP 地址
Ruijie(config-if)# **no ip address**	取消一个接口的 IP 地址配置

网络掩码也是一个 32 比特的数值，标识着该 IP 地址的哪几个比特为网络部分。网络掩码中，值为“1”的比特对应的 IP 地址比特位就是网络部分，值为“0”的比特对应的 IP 地址比特位就是主机地址部分。如 A 类网络对应的网络掩码为“255.0.0.0”。您可以利用网络掩码对一个网络进行子网划分，子网划分就是将主机地址部分的一些比特位也作为网络部分，缩小主机容量，增加网络的数量，这时的网络掩码就称为子网掩码。

理论上，子网掩码的比特位可以是主机地址部分中的任何一段比特位。

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。

接口配置多个 IP 地址

锐捷产品可以支持一个接口配置多个 IP 地址，其中一个为主 IP 地址，其余全部为次 IP 地址。次 IP 地址的配置理论上没有数目限制，但是次 IP 地址与主 IP 以及次 IP 之间地址必须属于不同网络。在网络建设中，会经常使用到次 IP 地址，通常在以下情况下应该考虑使用次 IP 地址：

- 一个网络没有足够多的主机地址。例如，现在一般局域网需要一个 C 类网络，可分配 254 台主机。但是当局域网主机超过 254 台时，一个 C 类网络将不够分配，有必要分配另一个 C 类网络地址。这样设备就需要连接两个网络，所以就需要配置多个 IP 地址。
- 许多旧的网络是基于第二层的桥接网络，没有进行子网的划分。次 IP 地址的使用可以使该网络很容易升级到基于 IP 层的路由网络。对于每个子网，设备都配置一个 IP 地址。
- 一个网络的两个子网被另外一个网络隔离开，您可以创建一个被隔离网络的子网，通过配置次 IP 地址的方式，将隔离的子网连接起来。一个子网不能在设备的两个或两个以上接口出现。

配置次 IP 地址之前，需要确定已经配置了主 IP 地址。如果网络上的一台设备配置了次 IP 地址，则其它设备也必须配置同一网络的次 IP 地址。当然如果其它设备原先没有分配 IP 地址，可以配置为主地址。

要配置次 IP 地址，在接口配置模式中执行以下命令：

命令	作用
Ruijie(config-if)# **ip address** *ip-address mask*	设置接口次 IP 地址
Ruijie(config-if)# **no ip address** *ip-address mask*	取消接口次 IP 地址配置

1.1.2.2 配置地址解析协议（ARP）

在局域网中，每个 IP 网络设备都有两个地址：1）本地地址，由于它包含在数据链路层的帧头中，更准确地说应该是数据链路层地址，但实际上对本地地址进行处理的是数据链路层中的 MAC 子层，因此习惯上称为 MAC 地址，MAC 地址在局域网上代表着 IP 网络设备；2）网络地址，在互联网上代表着 IP 网络设备，同时它也说明了该设备所属的网络。

局域网上两台 IP 设备之间需要通信，必须要知道对方的 48 比特的 MAC 地址。根据 IP 地址来获知 MAC 地址的过程称为地址解析（ARP）。而根据 MAC 地址获知 IP 地址的过程称为反向地址解析（RARP）。地址解析的方式有两类：1）地

址解析协议（ARP）；2）代理地址解析协议（Proxy ARP）。关于 ARP 、Proxy ARP、RARP，分别在 RFC 826，RFC 1027，RFC 903 文档中描述。

ARP 是用来绑定 MAC 地址和 IP 地址的，以 IP 地址作为输入，ARP 能够知道其关联的 MAC 地址。一旦知道了 MAC 地址，IP 地址与 MAC 地址对应关系就会保存在设备的 ARP 缓冲中。有了 MAC 地址，IP 设备就可以封装链路层的帧，然后将数据帧发送到局域网上去。缺省配置下，以太网上 IP 和 ARP 的封装为 Ethernet II 类型，也可以封装成其它类型的以太网帧类型如 SNAP。

RARP 的工作原理与 ARP 类似，不过 RARP 是以 MAC 地址作为输入，然后得到关联的 IP 地址。RARP 通常应用在无盘工作站上。

通常情况下，不需要特别配置设备的地址解析已经可以工作了。

静态配置 ARP

ARP 协议提供了 IP 地址和 MAC 地址动态映射的功能，通常情况下不需要进行静态配置。锐捷产品通过配置静态 ARP，还可以响应不是属于自己 IP 地址的 ARP 请求。

要配置静态 ARP，在全局配置模式中执行以下命令：

命令	作用
Ruijie(config)# **arp** *ip-address mac-address arp-type*	定义静态 ARP，其中 arp-type 目前只支持 arpa 类型。
Ruijie(config)# **no arp** *ip-address*	取消静态 ARP

ARP 封装设置

目前 ARP 封装只支持 Ethernet II 类型，在锐捷产品中也表示为 ARPA 关键字。

ARP 超时设置

ARP 超时设置只对动态学习到的 IP 地址和 MAC 地址映射起作用。超时时间设置得越短，ARP 缓冲中保存的映射表就越真实，但是 ARP 消耗网络带宽也越多，所以需要权衡利弊。除非有特别的需要，否则一般不需要配置 ARP 超时时间。

要配置 ARP 超时时间，在接口配置模式中执行以下命令：

命令	作用
Ruijie(config-if)# **arp timeout** *seconds*	配置 ARP 超时时间，范围 0-2147483，其中 0 表示不老化
Ruijie(config-if)# **no arp timeout**	恢复缺省配置

缺省情况下，超时时间为 3600 秒，即 1 个小时。

关闭 IP 路由

IP 路由功能缺省情况下是启动的，除非确定不需要 IP 路由功能，否则不要执行该操作。关闭 IP 路由将使设备丢失所有的路由，而且没有路由转发的功能。

要关闭 IP 路由功能，在全局配置模式中执行以下命令：

命令	作用

Ruijie(config)# **no ip routing**	关闭 IP 路由功能
Ruijie(config)# **ip routing**	启动 IP 路由功能

1.1.2.3 配置广播包处理

广播包是指目标地址为某个物理网络上所有主机的数据包。锐捷产品支持两种类型广播包：1）定向广播，是指数据包接收者为一个指定网络的所有主机，目标地址的主机部分全为“1”；2）淹没广播，是指数据包接收者为所有网络的主机，目标地址 32 比特位全为“1”时。广播包目前被一些 IP 协议的泛滥使用，其中包括十分重要的 IP 协议。所以如何控制和使用广播包是一个网络管理人员的基本职责。

如果 IP 网络设备转发淹没广播，可能会引起网络的超负载，严重影响网络的运行，这种情况称为广播风暴。设备提供了一些办法能够将广播风暴限制在本地网络，阻止其继续扩张。解决广播风暴最好的办法就是给每个网络指定一个广播地址，这就是定向广播，这要求使用广播包的 IP 协议尽可能应用定向广播而不是淹没广播进行数据传播。

关于广播问题的详细描述，请参见 RFC 919 和 RFC 922。

创建 IP 广播地址

当前使用最多的广播包，其目标地址为全“1”，表示为 255.255.255.255。锐捷产品可以通过软件定义产生其它地址的广播包，而且可以接收所有类型的广播包。

要配置有别于 255.255.255.255 的广播地址，在接口配置模式中执行以下命令：

命令	作用
Ruijie(config-if)# **ip broadcast-address** *ip-address*	创建新的广播地址
Ruijie(config-if)# **no ip broadcast-address**	取消新的广播地址

定向广播到物理广播转换

IP 定向广播报文是指目标地址为某个 IP 子网广播地址的 IP 报文，如目标地址为 172.16.16.255 的报文就称为定向广播报文。但是产生该报文的节点又不是目标子网的成员。

没有与目标子网直连的设备接收到 IP 定向广播报文，跟转发单播报文一样处理定向广播报文。当定向广播报文到达直连该子网的设备后，设备将把定向广播报文转换为淹没广播报文（一般指目标 IP 地址为全“1”的广播报文），然后以链路层广播方式发送给目标子网上的所有主机。

您可以在指定的接口上，启动定向广播到物理广播转换的功能，这样该接口就可以转发到直连网络的定向广播了。该命令只影响到达最终目标子网的定向广播报文的最后传输，而不影响其它定向广播报文的正常转发。

在接口上，您还可以通过定义访问控制列表来控制转发某些定向广播。当定义了访问列表，只有符合访问列表中定义的数据包才进行定向广播到物理广播的转换。

要配置定向广播到物理广播的转换，在接口配置模式中执行以下命令：

命令	作用
Ruijie(config-if)# **ip directed-broadcast** [*access-list-number*]	在接口上，启动定向广播到物理广播的转换
Ruijie(config-if)# **no ip directed-broadcast**	取消转换

1.1.3 监视和维护IP地址

1.1.3.1 清除缓冲和表内容

您可以删除一些特定缓冲、表、数据库的全部内容，主要包括三个方面：

- 清除 ARP 缓冲；
- 清除主机名到 IP 地址的映射表；
- 清除路由表。

命令	作用
Ruijie# **clear arp-cache**	清除 ARP 缓冲
Ruijie# **clear ip route** {*network* [*mask*] | *}	清除 IP 路由表

1.1.3.2 显示系统和网络状态

您可以查看 IP 路由表、缓冲、数据库的所有内容，通过这些信息对网络故障的排除十分有帮助。通过测试本地设备网络的可达到性，您可以知道数据包在离开本设备后将往哪条路径发送。

要显示系统和网络统计量，在特权用户模式中执行以下命令：

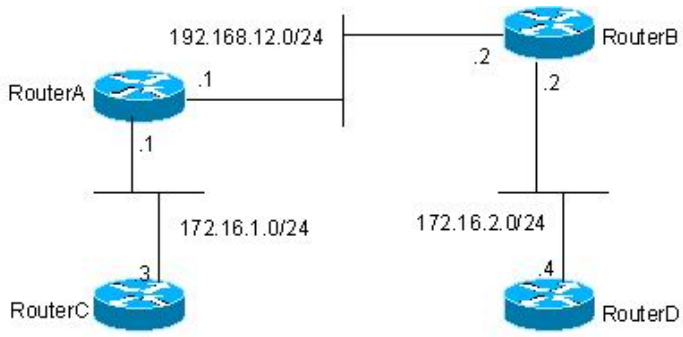
命令	作用
show arp [[*ip* [*mask*] | *mac-address*] | **static** | **complete** | **incomplete**]	显示 ARP 缓冲表，其中 complete / incomplete 关键字是用来分别显示动态 ARP 中已解析 / 未解析的表项。
show ip arp	显示 IP ARP 缓冲表
show ip interface [*interface-type interface-number*]	显示接口 IP 信息
show ip route [*network* [*mask*]]	显示路由表
show ip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

1.1.4 IP地址配置范例

配置要求

IP 地址分配和网络设备连接图如下：

图 1-5 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 配置IP服务

1.2.1 IP连接管理

IP 协议栈提供了许多服务用来控制和管理 IP 连接，ICMP 就提供了许多这些服务。当网络发生任何问题，设备或接入服务器将发送 ICMP 消息给主机或其它设备。详细的 ICMP 消息定义，请参见 RFC 792。

启用 ICMP 协议不可达消息

当设备接收到目标为自己的非广播包，该数据包中采用了设备不能处理的 IP 协议，设备就向源地址发送 ICMP 协议不可达消息。另外，如果设备由于不知道路由而不能转发数据包时，也会发送 ICMP 主机不可达消息。这种特性缺省是启用的。

如果要重新启用 ICMP 协议不可达消息，在接口配置模式中执行以下命令：

命令	作用
Ruijie(config-if)# **ip unreachables**	启用 ICMP 协议不可达和主机不可达消息
Ruijie(config-if)# **no ip unreachables**	关闭 ICMP 协议不可达和主机不可达消息

启用 ICMP 重定向消息

路由有时会不够优化，使得设备从一个接口接收到的数据包，还要从该接口发送出去。如果设备将数据包从接收接口重新发送出去，设备就会给数据源发送一个 ICMP 重定向消息，告诉数据源到该目标地址的网关为同一子网上的另外一台设备。这样数据源就会将后续的数据包按照最佳的路径进行发送。该特性缺省是启用。

要配置 ICMP 重定向消息，在接口配置模式中执行以下命令：

命令	作用
Ruijie(config-if)# **ip redirects**	启用 ICMP 重定向消息，缺省启用
Ruijie(config-if)# **no ip redirects**	关闭 ICMP 重定向消息

启用 ICMP 掩码应答消息

网络设备有时需要知道互联网上某个子网的子网掩码，为了获取该信息，网络设备 可以发送 ICMP 掩码请求消息，接收到 ICMP 掩码请求消息的网络设备就会发送掩码应答消息。锐捷产品可以响应 ICMP 掩码请求消息，缺省情况下是启用该特性的。

要配置 ICMP 掩码应答消息，在接口配置模式中执行以下命令：

命令	作用
Ruijie(config-if)# **ip mask-reply**	启用掩码应答消息
Ruijie(config-if)# **no ip mask-reply**	关闭掩码应答消息

设置 IP MTU

设备所有的接口都有缺省的 MTU（最大传输单元）值，所有大于 MTU 的数据包要从该接口转发出去必须分段，否则发送失败。

锐捷产品允许调整接口的 MTU 值，而且 MTU 的变化会引起 IP MTU 的变化，IP MTU 总是会自动与接口 MTU 保持一致。但是反之不行，如果调整了 IP MTU 值，接口 MTU 不会跟着改变。

一个物理网络上的设备接口，相同协议 MTU 值必须保持一致。

要设置 IP MTU 值，在接口配置模式中执行以下命令：

命令	作用
Ruijie(config-if)# **ip mtu** *bytes*	设置 MTU 值，范围 68~1500
Ruijie(config-if)# **no ip mtu**	恢复缺省值

配置 IP 源路由

锐捷产品支持 IP 源路由。当设备接收到 IP 数据包时，会对 IP 报头的严格源路由、宽松源路由、记录路由等选项进行检查，这些选项在 RFC 791 中有详细描述。如果检测到该数据包启用了其中一个选项，就会执行响应的动作；如果检测到无效的选项，就会给数据源发送一个 ICMP 参数问题消息，然后丢弃该数据包。锐捷产品缺省情况下支持 IP 源路由特性。

要配置 IP 源路由，在全局模式中执行以下命令：

命令	作用
Ruijie(config)# **ip source-route**	启用 IP 源路由
Ruijie(config)# **no ip source-route**	关闭 IP 源路由

2 DHCP

2.1 DHCP 概述

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

DHCP 有三种机制分配 IP 地址：

1) 自动分配，DHCP 给客户端分配永久性的 IP 地址；

2) 动态分配，DHCP 给客户端分配过一段时间会过期的 IP 地址（或者客户端可以主动释放该地址）；

3) 手工配置，由网络管理员给客户端指定 IP 地址。管理员可以通过 DHCP 将指定的 IP 地址发给客户端。

三种地址分配方式中，只有动态分配可以重复使用客户端不再需要的地址。

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

2.1.1 DHCP 工作原理

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

■

2.1.2 DHCP 客户端

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

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

☑ 锐捷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。

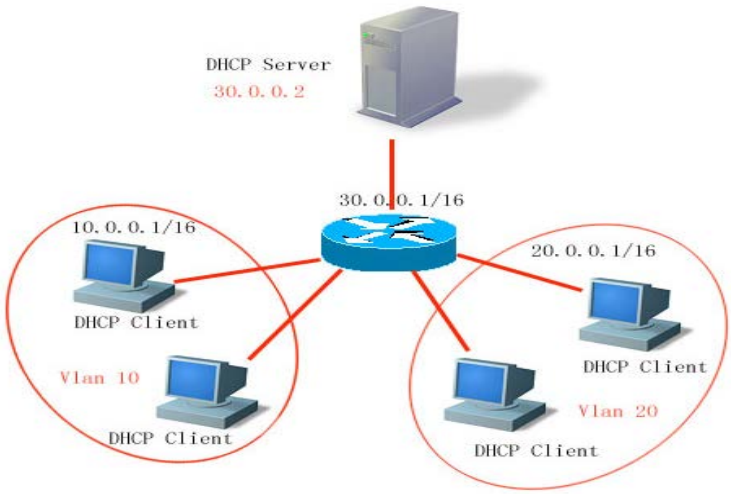
2.1.3 DHCP 中继代理

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

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

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

图 3-1



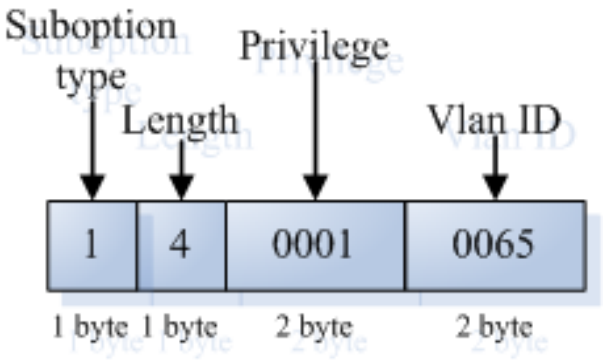
VLAN 10 和 VLAN 20 分别对应 10.0.0.1/16 和 20.0.0.1/16 的网络，而 DHCP 服务器在 30.0.0.1/16 的网络上，30.0.0.2 的 DHCP 服务器要对 10.0.0.1/16 和 20.0.0.1/16 的网络进行动态 IP 管理，只要在作为网关的设备上打开 DHCP 中继功能，并配置 30.0.0.2 为 DHCP 服务器的 IP 地址。

2.1.3.1 理解DHCP Relay Agent Information(option 82)

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

- relay agent information option dot1x：此种应用方案需要结合 802.1x 认证以及锐捷网络产品 RG-SAM。DHCP 中继根据 RG-SAM 在 802.1x 认证过程中下发的 IP 权限，以及 DHCP 客户端所属 vid，组合构成 Circuit ID 子选项。选项格式如下图所示：

图 3-2



- 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。选项格式如图 3-3、图 3-4 所示：

图 3-3 Agent Circuit ID

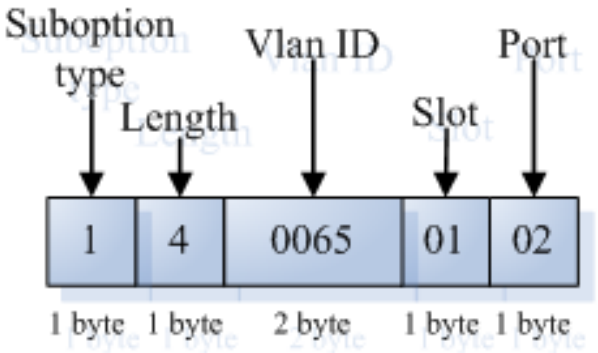
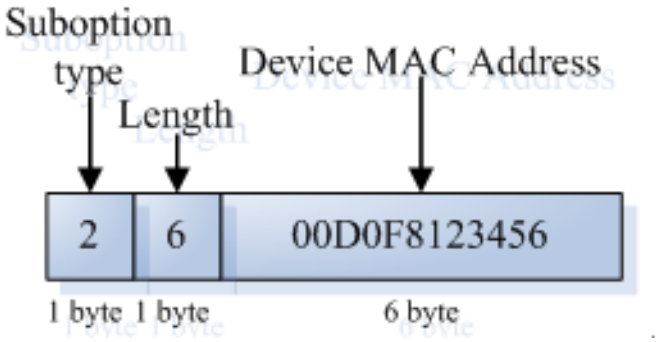


图 3-4 Agent Remote ID



2.1.3.2 理解DHCP relay Check Server-id功能

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

2.2 配置DHCP客户端

配置 DHCP 客户端任务列表如下：

- 配置以太网接口 DHCP 客户端（可选）
- 配置 PPP 封装链路上的 DHCP 客户端（可选）
- 配置 FR 封装链路上的 DHCP 客户端（可选）
- 配置 HDLC 封装链路上的 DHCP 客户端（可选）

2.2.1 配置以太网接口 DHCP 客户端

☑ 锐捷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

2.2.2 配置 PPP 封装链路上的 DHCP 客户端

☑ 锐捷产品支持 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

2.2.3 配置 FR 封装链路上的 DHCP 客户端

☑ 锐捷产品支持 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

2.2.4 配置 HDLC 封装链路上的 DHCP 客户端

☑ 锐捷产品支持 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

☑ 在 RGOS 10.1 及以后版本的部分产品上，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。

2.3 配置DHCP中继

2.3.1 启用 DHCP 中继代理

在全局配置模式下，请按如下步骤配置 DHCP 中继代理：

命令	作用
Ruijie (config)# **service dhcp**	启用 DHCP 代理
Ruijie(config)# **no service dhcp**	关闭 DHCP 代理。

2.3.2 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。

全局配置模式下可对 dhcp relay 的 cycle-mode 参数进行配置，当不启用 cycle-mode 的时候表示 dhcp relay 允许把接收到的 dhcp client 请求报文转发到以上规则的所有 dhcp server 上；当启用 cycle-mode 的时候表示 dhcp relay 只把接收到的 dhcp client 请求报文转发到以上规则的第一个 dhcp server 上。cycle-mode 只在全局配置模式下配置，作用于全局和接口，默认为不启用。

配置 DHCP 服务器地址请按如下方式进行：

命令	作用
Ruijie(config)# **ip helper-address** [**global**] *A.B.C.D*	添加一个全局的 DHCP 服务器地址。可以显示的指定服务器所属的 VPN 或者全局空间
Ruijie(config)# **ip helper-address cycle-mode**	启用 dhcp relay 的 cycle-mode 功能
Ruijie(config-if)# **ip helper-address** [**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。
Ruijie(config)# **no ip helper-address** [**global**] *A.B.C.D*	删除一个全局的 DHCP 服务器地址
Ruijie(config)# **no ip helper-address cycle-mode**	关闭 dhcp relay 的 cycle-mode 功能
Ruijie(config-if)# **no ip helper-address** [**global**] *A.B.C.D*	删除一个接口的 DHCP 服务器地址

2.3.3 配置 DHCP option dot1x

通过理解 DHCP Relay Agent Information 的描述可知，在网络如果需要根据用户权限的不同而给用户分配不同权限 IP 时，我们就可以通过配置 **ip dhcp relay information option dot1x** 来配置打开 DHCP 中继设备的 option dot1x 功能。当设备做为 DHCP 中继转发 DHCP 请求报文时，结合 802.1x，在 DHCP 请求报文中添 option 选项信息。该功能和 dot1x 功能结合使用。

在全局配置模式下，请按如下步骤配置 DHCP option dot1x：

命令	作用
Ruijie(config)# **ip dhcp relay information option dot1x**	启用 DHCP option dot1x 功能
Ruijie(config)# **no ip dhcp relay information option dot1x**	关闭 DHCP option dot1x 功能。

2.3.4 配置 DHCP option dot1x access-group

在 option dot1x 的应用方案中，需要设备控制未认证或低权限的 IP 只有访问特定的一些 IP 地址的权限，以及限制低权限用户之间的互相访问，此时可以通过配置命令 **ip dhcp relay information option dot1x access-group** *acl-name* 来实现。这里的 *acl-name* 所定义的 ACL 必须预先配置，用以对某些内容进行过滤，主要是用于禁止未认证用户之间的互相访问。另外，这里所关联的 ACL 被应用到设备所有端口上，并且该 ACL 没有缺省的 ACE，与其它接口所关联的 ACL 没有冲突关系，例如：

为未认证的所用用户规划一类 IP 地址，为 192.168.3.2-192.168.3.254，192.168.4.2-192.168.4.254，192.168.5.2-192.168.5.254；另外 192.168.3.1、192.168.4.1、192.168.5.1 作为网关地址，不分配给用户。则用户在未认证之前使用 192.168.3.x-5.x 的地址到达 web portal 以下载客户端软件。因此需要在设备上配置如下：

```
Ruijie# configure terminal
Ruijie(config)# ip access-list extended DenyAccessEachOtherOfUnauthrize
Ruijie(config-ext-nacl)# permit ip any host 192.168.3.1
```

//允许发往网关的报文

```
Ruijie(config-ext-nacl)# permit ip any host 192.168.4.1
Ruijie(config-ext-nacl)# permit ip any host 192.168.5.1
Ruijie(config-ext-nacl)# permit ip host 192.168.3.1 any
```

//允许源 IP 地址为网关的报文通讯

```
Ruijie(config-ext-nacl)# permit ip host 192.168.4.1 any
Ruijie(config-ext-nacl)# permit ip host 192.168.5.1 any
Ruijie(config-ext-nacl)# deny ip 192.168.3.0 0.0.0.255 192.168.3.0 0.0.0.255
```

//禁止未认证用户相互访问

```
Ruijie(config-ext-nacl)# deny ip 192.168.3.0 0.0.0.255 192.168.4.0  0.0.0.255
Ruijie(config-ext-nacl)# deny ip 192.168.3.0 0.0.0.255 192.168.5.0  0.0.0.255
Ruijie(config-ext-nacl)# deny ip 192.168.4.0 0.0.0.255 192.168.4.0  0.0.0.255
Ruijie(config-ext-nacl)# deny ip 192.168.4.0 0.0.0.255 192.168.5.0  0.0.0.255
```

```
Ruijie(config-ext-nacl)# deny ip 192.168.5.0 0.0.0.255 192.168.5.0  0.0.0.255
Ruijie(config-ext-nacl)# deny ip 192.168.5.0 0.0.0.255 192.168.3.0  0.0.0.255
Ruijie(config-ext-nacl)# deny ip 192.168.5.0 0.0.0.255 192.168.4.0  0.0.0.255
Ruijie(config-ext-nacl)# exit
```

然后再使用命令 **ip dhcp relay information option dot1x access-group DenyAccessEachOtherOfUnauthrize** 把命令应用全局接口上。在全局配置模式下，请按如下步骤配置 **DHCP option dot1x access-group**：

命令	作用
Ruijie(config)# **ip dhcp relay information option dot1x access-group** *acl-name*	应用 DHCP option dot1x acl
Ruijie(config)# **no ip dhcp relay information option dot1x access-group** *acl-name*	取消 DHCP option dot1x acl 的应用。

2.3.5 配置 DHCP option 82

当配置命令 **ip dhcp relay information option82** 命令时，设备做为 DHCP 中继，在转发 DHCP 请求报文过程中，在 DHCP 请求报文中添加 option 信息。

在全局配置模式下，请按如下步骤配置 DHCP option82：

命令	作用
Ruijie(config)# **ip dhcp relay information option82**	启用 DHCP option82 功能
Ruijie(config)# **no ip dhcp relay information option82**	关闭 DHCP option82 功能。

2.3.6 配置 DHCP relay check server-id

当配置命令 **ip dhcp relay check server-id** 后，DHCP Relay 仅将 DHCP 请求报文转发到 option server-id 中指定的服务器。如果没有配置该命令，则向所有配置的 DHCP 服务器转发 DHCP 请求报文。

在全局配置模式下，请按如下步骤配置 **DHCP relay check server-id** 功能：

命令	作用
Ruijie(config)# **ip dhcp relay check server-id**	启用 DHCP relay check server-di 功能
Ruijie(config)# **no ip dhcp relay check server-id**	关闭 DHCP relay check server-id 功能。

2.3.7 配置 DHCP relay suppression

在指定接口上配置命令 **ip dhcp relay suppression** 后，将屏蔽该接口上收到的 DHCP 请求报文；而对于其他接口上收到的 DHCP 请求报文，则正常转发。

在接口配置模式下，请按如下步骤配置 **ip dhcp relay suppression** 功能：

命令	作用
Ruijie(config-if)# **ip dhcp relay suppresson**	启用 DHCP relay suppresson 功能
Ruijie(config-if)# **no ip dhcp relay suppresson**	关闭 DHCP relay suppresson 功能。

2.3.8 配置 DHCP relay 的其他注意事项

配置 DHCP option dot1x 的注意事项

- 此命令的实际生效需要在 AAA/802.1x 相关的配置正确的情况下。
- 在应用此方案时需要启用 802.1x 的 DHCP 模式的 IP 授权。
- 此命令与 dhcp option82 命令互斥，不能同时使用。
- 在启用了 802.1x 的 DHCP 模式的 IP 授权的模式下，也会设置 MAC + IP 的绑定，所以不能与 DHCP 动态绑定功能同时启用。

配置 DHCP option82 的注意事项

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

2.3.9 DHCP Relay 配置实例

如下命令打开了 dhcp relay 功能、添加了两组服务器地址的例子：

```
Ruijie# configure  terminal
Ruijie(config)# service dhcp                //打开 DHCP 中继功能
Ruijie(config)# ip dhcp relay information option82    //打开 DHCP option82 功能
Ruijie(config)# ip helper-address 192.18.100.1 //添加全局服务器地址
Ruijie(config)# ip helper-address 192.18.100.2
Ruijie(config)# interface gigabitEthernet 0/3
Ruijie(config-if-gigabitEthernet 0/3)# ip helper-address 192.18.200.1    //添加接口服务器地址
Ruijie(config-if-gigabitEthernet 0/3)# ip helper-address 192.18.200.2
Ruijie(config-if-gigabitEthernet 0/3)# end
```

2.4 监视和维护信息

2.4.1 显示 DHCP 配置

请在特权模式下用 **show running-config** 命令显示 DHCP 配置。

```
Ruijie# show running-config
Building configuration...
Current configuration : 1464 bytes
version RGNOS 10.1.00(1), Release(11758)(Fri Mar 30 12:53:11 CST 2007 -nprd
hostname Ruijie
vlan 1
```

```
ip helper-address 192.18.100.1
ip helper-address 192.18.100.2
ip dhcp relay information option dot1x
interface GigabitEthernet 0/1
interface GigabitEthernet 0/2
interface GigabitEthernet 0/3
no switchport
ip helper-address 192.168.200.1
ip helper-address 192.168.200.2
interface VLAN 1
ip address 192.168.193.91 255.255.255.0
line con 0
exec-timeout 0 0
line vty 0
exec-timeout 0 0
login
password 7 0137
line vty 1 2
login
password 7 0137
line vty 3 4
login
end
```

2.4.2 监视和维护 DHCP 中继

监视和维护 DHCP 中继命令：

命令	作用
Ruijie# **clear ip dhcp relay statistics**	清除 DHCP 代理统计状态
show ip dhcp relay-statistics	显示 DHCP 代理统计信息

2.4.3 监视和维护 DHCP 客户端

监视和维护 DHCP 客户有两类命令，可以通过在客户端上进行以下操作：

1) 调试（debug）命令，输出必要的调试信息，主要用于故障诊断和排除.

2) 显示命令，显示 DHCP 相关信息。

要进行 DHCP 客户的调试，在命令执行模式中执行以下命令：

命令	作用
Ruijie# **debug ip dhcp client**	调试 DHCP 客户

要显示 DHCP 客户获得的租约信息，在命令执行模式中执行以下命令：

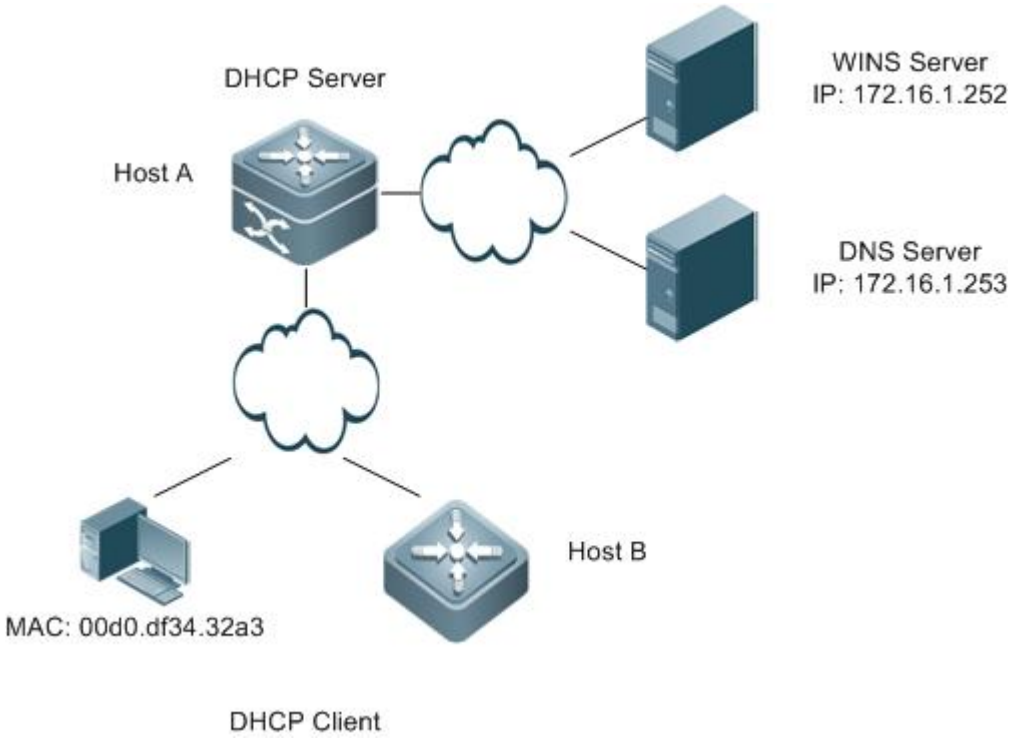
命令	作用
show dhcp lease	显示 DHCP 租约信息

2.5 DHCP配置用例

2.5.1 DHCP 典型配置用例

拓扑图

图 3-5 DHCP 案例示意图



应用需求

- Host A 可以作为 DHCP Server 为一部分客户端用户分配动态 IP 地址。可分配地址的网段为 172.16.1.0/24，缺省网关为 172.16.1.254，域名为 ruijie.com，域名服务器为 172.16.1.253，WINS 服务器为 172.16.1.252，NetBIOS 节点类型为复合型，地址租期为 1 天。在地址的网段中除了 172.16.1.2~172.16.1.100 地址外，其余地址均为可分配地址。
- Host A 为一部分客户端用户分配固定 IP 地址。对 MAC 地址为 00d0.df34.32a3 的 DHCP 客户端分配的 IP 地址为 172.16.1.101，掩码为 255.255.255.0，主机名为 admin，缺省网关为 172.16.1.254，域名服务器为 172.16.1.253，WINS 服务器为 172.16.1.252，NetBIOS 节点类型为复合型。
- HOST B 为设备接口 FastEthernet 0/0 配置 DHCP 自动分配地址。

配置要点

- 在 Host A 上开启 DHCP 服务器功能，创建一个地址池，用于配置动态分配 IP 地址，另外创建一个地址池，用于手工绑定 IP 地址。并在相应的地址池指定域名服务器地址（本例为 DNS Server 和 WINS Server 的地址）以及客户端的域名。
- 在 Host B 上指定接口开启 DHCP 客户端功能，自动获取 IP 地址。

配置步骤

第一步，在 Host A 上，创建新的 DHCP 地址池，配置动态分配 IP 地址。

！配置地址池名为“dynamic”，并进入 DHCP 配置模式。

```
HostA# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
HostA(config)# ip dhcp pool dynamic
```

！在 DHCP 配置模式下，配置一个可分配给客户的 IP 地址网段，并配置该地址网段的默认网关。并设置租期为 2 天。

```
HostA(dhcp-config)# network 172.16.1.0 255.255.255.0
HostA(dhcp-config)# default-router 172.16.1.254
HostA(dhcp-config)# lease 2
```

第二步，指定“dynamic”地址池的 DNS Server，并配置客户端的域名。

！假设 DNS Server 的 IP 地址是 172.16.1.253，在地址池中配置域名服务器，并配置客户端域名为 ruijie.com。

```
HostA(dhcp-config)# dns-server 172.16.1.253
HostA(dhcp-config)# domain-name ruijie.com
```

第三步，指定“dynamic”地址池的 WINS Server，并配置客户端 NetBIOS 节点类型。

!假设 WIN Server 的 IP 地址是 172.16.1.252,在地址池中配置 NetBIOS WINS 服务器,并配置 NetBIOS 节点类型为 Hybrid。

```
HostA(dhcp-config)# netbios-name-server 172.16.1.252
HostA(dhcp-config)# netbios-node-type h-node
```

第四步，在全局模式下配置排斥地址。

！如上，IP 地址为 172.16.1.254、172.16.1.253、172.16.1.252 已经分配作为对应网段的网关、DNS 服务器、WINS 服务器的地址，并且地址范围 172.16.1.2~172.16.1.100 也不允许分配。通过排斥地址配置明确这些地址不允许分配给客户端用户。

```
HostA(dhcp-config)# exit
HostA(config)# ip dhcp excluded-address 172.16.1.252 172.16.1.254
HostA(config)# ip dhcp excluded-address 172.16.1.2 172.16.1.100
```

第五步，创建另一个地址池，配置手工绑定 IP 地址。

！配置地址池名为“static”，并进入 DHCP 配置模式。

```
HostA(config)# ip dhcp pool static
```

！ 指明 IP 地址为 172.16.1.101/24 手工绑定 MAC 地址为 00d0.df34.32a3，客户端名称为 admin。注意：定义客户端的标识需增加网络媒介类型标识（以太网类型为“01”），即手工绑定的 MAC 地址对应的客户端标识为 00d0.df34.32a3.14。

```
HostA(dhcp-config)# host 172.16.1.101 255.255.255.0
HostA(dhcp-config)# client-identifier 00d0.df34.32a3.14
HostA(dhcp-config)# client-name admin
```

第六步，指定“static”地址池对应的网关地址。

！配置网关地址为 172.16.1.254。

```
HostA(dhcp-config)# default-router 172.16.1.254
```

第七步，指定“static”地址池的 DNS Server，并配置客户端的域名。

！同上，假设 DNS Server 的 IP 地址是 172.16.1.253，在地址池中配置域名服务器，并配置客户端域名为 ruijie.com。

```
HostA(dhcp-config)# dns-server 172.16.1.253
HostA(dhcp-config)# domain-name ruijie.com
```

第八步，指定“static”地址池的 WINS Server，并配置客户端 NetBIOS 节点类型。

！同上，假设 WIN Server 的 IP 地址是 172.16.1.252，在地址池中配置 NetBIOS WINS 服务器，并配置 NetBIOS 节点类型为 Hybrid。

```
HostA(dhcp-config)# netbios-name-server 172.16.1.252
HostA(dhcp-config)# netbios-node-type h-node
HostA(dhcp-config)# exit
```

第九步，在 Host A 上启用 DHCP Server。

```
HostA(dhcp-config)# exit
HostA(config)# service dhcp
```

第十步，在 Host B 上启用 DHCP Client。

！此例默认客户端的接口为三层口，启动 DHCP client。

```
HostB(config)# interface fastEthernet 0/1
HostB(config-if-fastEthernet 0/1)# ip address dhcp
```

验证结果

第一步，查看 Host A 的配置信息

```
HostA# show running-config
!
service dhcp
!
ip dhcp excluded-address 172.16.1.252 172.16.1.254
ip dhcp excluded-address 172.16.1.2 172.16.1.100
!
!
```

```
ip dhcp pool dynamic
 netbios-node-type h-node
 netbios-name-server 172.16.1.252
 domain-name ruijie.com
 lease 2 0 0
 network 172.16.1.0 255.255.255.0
 dns-server 172.16.1.253
 default-router 172.16.1.254
!
ip dhcp pool static
 client-name admin
 client-identifier 00d0.df34.32a3.14
 host 172.16.1.101 255.255.255.0
 netbios-node-type h-node
 netbios-name-server 172.16.1.252
 domain-name ruijie.com
 dns-server 172.16.1.253
 default-router 172.16.1.254
!
```

第二步，查看 Host B 的配置信息

```
HostB# show running-config
!
interface fastEthernet 0/1 //注：如果是交换机设备，这里应该还有 no switchport 命令，将接口设置为三层口
ip address dhcp
```

第三步，接入一台 MAC 地址为 0013.2049.9014 的 PC，在 Host A 上查看 DHCP Server 分配 IP 地址信息。

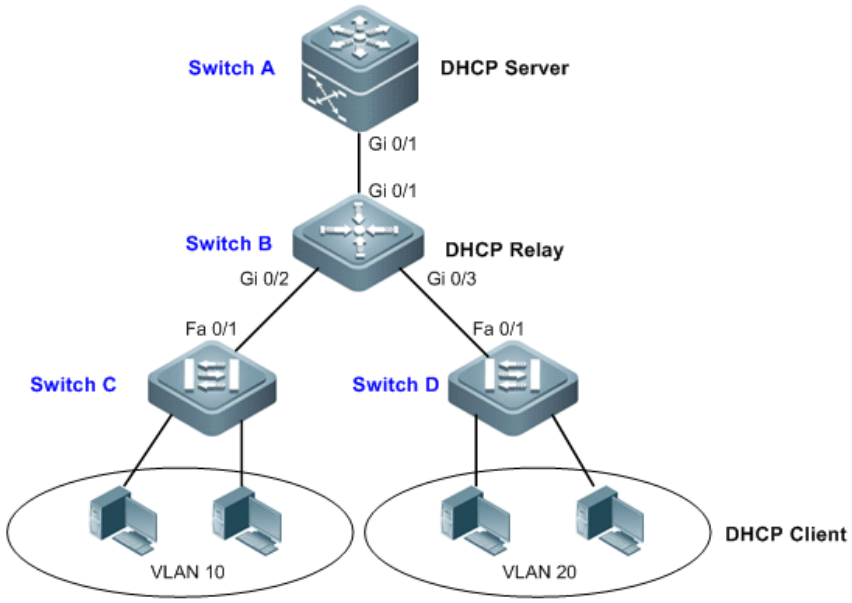
```
Ruijie#show ip dhcp binding
IP address    Client-Identifier/     Lease expiration         Type
                Hardware address
172.16.1.101  00d0.df34.32a3.14      IDLE                       Manual 172.16.1.102  0100.e04c.70b7.e2 000
days 23 hours 48 mins Automatic
```

2.6 DHCP Relay配置用例

2.6.1 DHCP Relay 典型配置用例（交换机）

拓扑图

图 3-6 DHCP Relay 用例示意图



应用需求

如上图所示，Switch C 和 Switch D 作为接入设备，分布着 VLAN 10 和 VLAN 20 的 PC 用户，Switch B 作为网关设备，Switch A 作为核心路由设备。主要需求如下：

- Switch A 可以充当 DHCP Server，为不同 VLAN 用户动态分配不同网段的 IP 地址。
- Switch C 和 Switch D 下的接入用户可以跨网段动态获取 IP 地址。

配置要点

- **配置 DHCP Server**：在 Switch A 上，分别为 VLAN 10 和 VLAN 20 的用户创建 DHCP 地址池，开启 DHCP Server 功能。（DHCP Server 的相关配置可参见《DHCP 配置指南》）
- **配置 DHCP Relay**：在 Switch B 上，指定 DHCP 服务器地址（本例配置 DHCP Server 地址为 10.1.1.2/24），并开启 DHCP Server 功能。

> Switch C 和 Switch D 上仅需根据具体情况配置对应端口所属 VLAN，一旦接入 PC 即可动态获取 IP 地址。此处不再详细列举。

配置步骤

第一步，配置 DHCP Server

！在全局模式下，在 Switch A 上创建一个 DHCP 地址池，命名为“vlan10”，对应的 IP 网段为 192.168.1.0/24，网关地址为 192.168.1.1。

```
SwitchA(config)#ip dhcp pool vlan10
SwitchA(dhcp-config)#network 192.168.1.0 255.255.255.0
SwitchA(dhcp-config)#default-router 192.168.1.1
```

```
SwitchA(dhcp-config)#exit
```

！同上，创建“vlan20”地址池，IP 网段为 192.168.2.0/24，网关地址为 192.168.2.1.

```
SwitchA(config)#ip dhcp pool vlan20
SwitchA(dhcp-config)#network 192.168.2.0 255.255.255.0
SwitchA(dhcp-config)#default-router 192.168.2.1
SwitchA(dhcp-config)#exit
```

！在全局模式下，配置排斥地址为 192.168.1.1 和 192.168.2.1，避免分配的 IP 地址与网关地址冲突。

```
SwitchA(config)#ip dhcp excluded-address 192.168.1.1
SwitchA(config)#ip dhcp excluded-address 192.168.2.1
```

！开启 DHCP Server。

```
SwitchA(config)#service dhcp
```

第二步，配置 Switch A 与 Switch B 之间三层通信。

！在 Switch A 上，配置端口 Gi 0/1 为 Route Port，对应的 IP 地址为 10.1.1.2/24。

```
SwitchA(config)#interface gigabitEthernet 0/1
SwitchA(config-if-GigabitEthernet 0/1)#no switchport
SwitchA(config-if-GigabitEthernet 0/1)#ip address 10.1.1.2 255.255.255.0
SwitchA(config-if-GigabitEthernet 0/1)#exit
```

！在 Switch B 上，配置端口 Gi 0/1 为 Route Port，对应的 IP 地址为 10.1.1.3/24

```
SwitchB(config)#interface gigabitEthernet 0/1
SwitchB(config-if)#no switchport
SwitchB(config-if)#ip address 10.1.1.3 255.255.255.0
SwitchB(config-if)#exit
```

！在 Switch A 上配置缺省路由

```
SwitchA(config)#ip route 0.0.0.0 0.0.0.0 10.1.1.3
```

第三步，配置接入用户的网关

！在 Switch B 上，配置 VLAN 10 的 SVI 为 192.168.1.1/24。

```
SwitchB(config)#vlan 10
SwitchB(config-vlan)#exit
SwitchB(config)#interface vlan 10
SwitchB(config-if)#ip address 192.168.1.1 255.255.255.0
SwitchB(config-if)#exit
```

！同上，配置 VLAN 20 的 SVI 为 192.168.2.1/24。

```
SwitchB(config)#vlan 20
SwitchB(config-vlan)#exit
SwitchB(config)#interface vlan 20
SwitchB(config-if)#ip address 192.168.2.1 255.255.255.0
```

```
SwitchB(config-if)#exit
```

第四步，配置 DHCP Relay

！在 Switch B 上，全局配置 DHCP 服务器的地址为 10.1.1.2，并开启 DHCP Server。

```
SwitchB(config)#ip helper-address 10.1.1.2
SwitchB(config)#service dhcp
```

第五步，配置 Switch B 和 Switch C、D 之间的二层通信

！在 Switch B 上，配置端口 Gi 0/2 和 Gi 0/3 为 Trunk Port。

```
SwitchB(config)#interface range gigabitEthernet 0/2-3
SwitchB(config-if-range)#switchport mode trunk
```

！同理，配置 Switch C、D 的端口 Fa 0/1 为 Trunk Port，此处不列举。

验证结果

第一步，查看各设备的配置信息。

！Switch A 的配置

```
SwitchA#show running-config
!
service dhcp
!
ip dhcp excluded-address 192.168.1.1
ip dhcp excluded-address 192.168.2.1
!
ip dhcp pool vlan10
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
!
ip dhcp pool vlan20
 network 192.168.2.0 255.255.255.0
 default-router 192.168.2.1
!
interface GigabitEthernet 0/1
 no switchport
 no ip proxy-arp
 ip address 10.1.1.2 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 10.1.1.3
!
```

！Switch B 的配置

```
SwitchB#show running-config
```

```
!
vlan 10
!
vlan 20
!
service dhcp
ip helper-address 10.1.1.2
!
interface GigabitEthernet 0/1
 no switchport
 no ip proxy-arp
 ip address 10.1.1.3 255.255.255.0
!
interface GigabitEthernet 0/2
 switchport mode trunk
!
interface GigabitEthernet 0/3
 switchport mode trunk
!
interface VLAN 10
 no ip proxy-arp
 ip address 192.168.1.1 255.255.255.0
!
interface VLAN 20
 no ip proxy-arp
 ip address 192.168.2.1 255.255.255.0
!
```

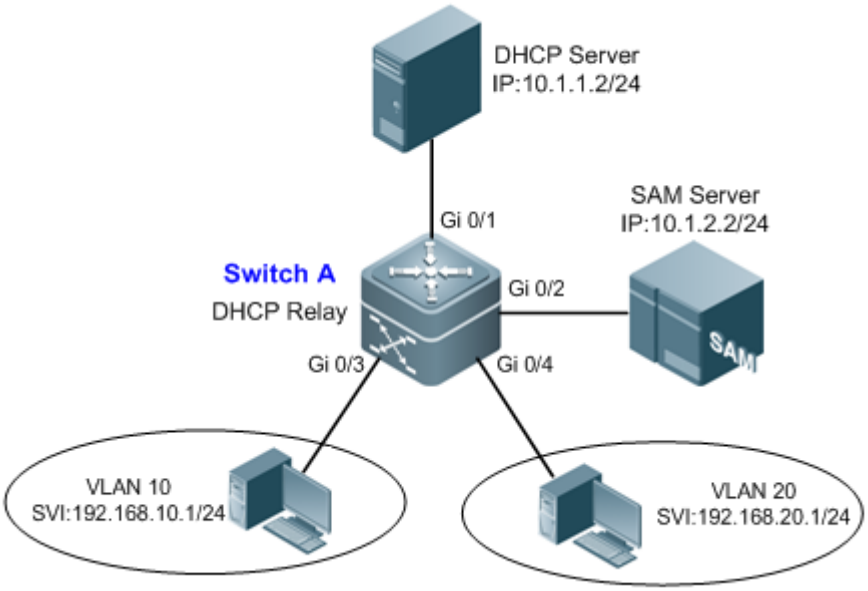
第二步，将两台 PC 分别接入 VLAN 10 和 VLAN 20 下的端口，查看 PC 动态获取 IP 地址的情况。

```
SwitchA#show ip dhcp binding
IP address    Client-Identifier/     Lease expiration         Type
                Hardware address192.168.1.2    0100.1320.4990.14     000 days 23 hours 59 mins  Automatic
192.168.2.2    0100.e04c.70b7.e2     000 days 23 hours 59 mins  Automatic
```

2.6.2 DHCP Option dot1x 典型配置用例

拓扑图

图 3-7DHCP Option Dot1X 用例示意图



应用需求

- Switch A 作为三层设备，实现不同网段之间的路由通信。
- 接入用户划分属于不同 VLAN，通过 Dot1x 认证上网，SAM Server 为不同用户下发不同的访问权限。
- DHCP Server 可以基于认证用户的权限为其分配 IP 地址。

配置要点

- **配置基本 DHCP Relay 功能**：在 Switch A 上，指定 DHCP 服务器地址（本例为 10.1.1.2/24），开启 DHCP Server 功能。通过以上配置，用户可以跨网段动态获取 IP 地址。
- **配置 802.1X 认证**：在 Switch A 上，设置 802.1X 认证的开关，指定用户端口为受控端口（本例为 Gi 0/3 和 Gi 0/4）。通过以上配置，用户需要通过 Dot1x 认证才能上网。
- **配置下发权限 IP**：在 Switch A 上，开启 DHCP Option dot1x 功能，配置 IP 授权模式为 DHCP Server。通过以上配置，DHCP Server 可以基于用户的权限分配 IP 地址。

对于 802.1X 的相关配置说明请参考《802.1X 配置指南》

本例的应用实现需要关联配置 SAM 和 DHCP 服务器，此处不再列举。

配置步骤

- 配置 Switch A

第一步，配置用户的网关地址以及服务器的接口地址。

！配置端口 Gi 0/3 和 Gi 0/4 对应的 VLAN，并配置各 VLAN 对应的 SVI。

```
Ruijie#configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#interface gigabitEthernet 0/3
Ruijie(config-if-GigabitEthernet 0/3)#switchport access vlan 10
Ruijie(config-if-GigabitEthernet 0/3)#exit
Ruijie(config)#interface gigabitEthernet 0/4
Ruijie(config-if-GigabitEthernet 0/4)#switchport access vlan 20
Ruijie(config-if-GigabitEthernet 0/4)#exit
Ruijie(config)#interface vlan 10
Ruijie(config-if-VLAN 10)#ip address 192.168.10.1 255.255.255.0
Ruijie(config-if-VLAN 10)#exit
Ruijie(config)#interface vlan 20
Ruijie(config-if-VLAN 20)#ip address 192.168.20.1 255.255.255.0
Ruijie(config-if-VLAN 20)#exit
```

！配置 DHCP Server 和 SAM Server 的接口地址。

```
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#no switchport
Ruijie(config-if-GigabitEthernet 0/1)#ip address 10.1.1.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/1)#exit
Ruijie(config)#interface gigabitEthernet 0/2
Ruijie(config-if-GigabitEthernet 0/2)#no switchport
Ruijie(config-if-GigabitEthernet 0/2)#ip address 10.1.2.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/2)#exit
```

第二步，配置 DHCP Relay 相关功能。

！配置 DHCP Server 的地址为 10.1.1.2/24，并开启 DHCP 服务。

```
Ruijie(config)#ip helper-address 10.1.1.2
Ruijie(config)#service dhcp
```

！开启 DHPC Option dot1x 功能。

```
Ruijie(config)#ip dhcp relay information option dot1x
```

第三步，配置 802.1X 相关功能。

！开启 AAA，指定 Radius Server 的地址为 10.1.2.2/24，配置 Radius Key 为“ruijie”。

```
Ruijie(config)#aaa new-model
Ruijie(config)#radius-server host 10.1.2.2
Ruijie(config)#radius-server key ruijie
```

！创建 Dot1x 认证方法列表“d1x”，并配置 Dot1x 应用该认证方法列表。

```
Ruijie(config)#aaa authentication dot1x d1x group radius
Ruijie(config)#dot1x authentication d1x
```

！配置用户端口 Gi 0/3 和 Gi 0/4 为受控口。

```
Ruijie(config)#interface range gigabitEthernet 0/3-4
```

```
Ruijie(config-if-range)#dot1x port-control auto
Ruijie(config-if-range)#exit
```

！配置 IP 授权模式为 DHCP Server。

```
Ruijie(config)#aaa authorization ip-auth-mode dhcp-server
```

验证结果

第一步，查看各设备的配置信息。

！Switch A 的配置

```
Ruijie#show running-config
!
aaa new-model
!
aaa authorization ip-auth-mode dhcp-server
aaa authentication dot1x d1x group radius
!
vlan 10
!
vlan 20
!
service dhcp
ip helper-address 10.1.1.2
!
ip dhcp relay information option dot1x
!
radius-server host 10.1.2.2
radius-server key ruijie
!
dot1x authentication d1x
interface GigabitEthernet 0/1
 no switchport
 no ip proxy-arp
 ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet 0/2
 no switchport
 no ip proxy-arp
 ip address 10.1.2.1 255.255.255.0
!
interface GigabitEthernet 0/3
 switchport access vlan 10
 dot1x port-control auto
!
```

```
interface GigabitEthernet 0/4
 switchport access vlan 20
 dot1x port-control auto
!
interface VLAN 10
 no ip proxy-arp
 ip address 192.168.10.1 255.255.255.0
!
interface VLAN 20
 no ip proxy-arp
 ip address 192.168.20.1 255.255.255.0
!
```

3 DNS

3.1 DNS概述

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

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

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

3.2 配置域名解析

3.2.1 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

3.2.2 打开DNS域名解析服务

本节描述如何打开 DNS 域名解析功能开关。

命令	作用
Ruijie(config)# **ip domain-lookup**	打开 DNS 域名解析功能开关

使用 **no ip domain-lookup** 命令关闭 DNS 域名解析的功能

```
Ruijie(config)# ip domain-lookup
```

3.2.3 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*] 命令。其中参数 **ip-address** 表示删除指定的域名服务器，否则删除所有的域名服务器。

命令	作用
Ruijie(config)# **ip name-server** *ip-address*	添加 DNS Server 的 IP 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。

3.2.4 静态配置主机名和IP地址的映射

本节描述如何配置主机名和 IP 地址的映射。本地维护了一张主机名和 IP 地址的对应表，也叫主机名到 IP 地址的映射表。主机名到 IP 地址的映射表内容有两个来源：手工配置和动态学习。在不能动态学习的情况下，手工配置就有必要了。

命令	作用
Ruijie(config)# **ip host *host-name*** *ip-address*	手工配置主机名和 IP 地址映射

使用该命令的 **no** 形式就可以删除主机名和 IP 地址的映射。

3.2.5 清除动态主机名缓存表

本节描述如何清除动态主机名缓存表。如果输入 **clear host** 或 **clear host *** 命令将清除动态缓存表。否则只删除指定域名的表项。

命令	作用
Ruijie# **clear host** [*host-name*]	清除动态主机名缓存表。 该命令不能删除静态配置的主机名。

3.2.6 域名解析信息显示

本节描述如何显示 DNS 的相关配置信息：

命令	作用
show hosts [*host-name*]	查看 DNS 的相关参数

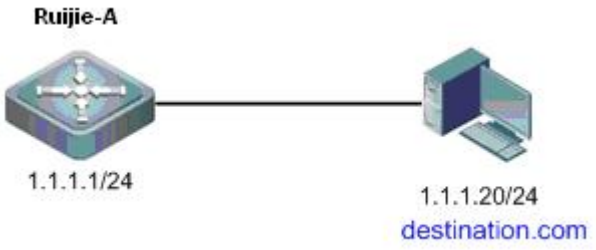
```
Ruijie# show hosts
Name servers are:
192.168.5.134  static

Host                    type        Address            TTL(sec)
www.163.com           static     192.168.5.243     ---
```

3.3 DNS典型配置举例

3.3.1 静态域名解析配置举例

拓扑图

图 5-1 静态域名解析配置组网图



应用需求

由于网络设备 Ruijie-A 经常访问域名为 destination.com 的主机，可利用静态域名解析功能，实现通过 destination.com 主机名访问 IP 地址为 1.1.1.20 的主机，提高域名解析的效率。

配置要点

1) 确保设备和主机间路由可达

2) 主机名和 IP 地址间的映射正确

配置步骤

手工配置主机名和 IP 地址间的映射；本例中，配置主机名为 destination.com 其对应 IP 地址为 1.1.1.20

```
Ruijie-A(config)#ip host destination.com 1.1.1.20
```

配置验证

第一步，查看域名解析信息；关注点主机、IP 地址间的映射关系是否正确。

```
Ruijie-A# show host
Name servers are:
Host                  type    Address                   TTL(sec)
destination.com    static  1.1.1.20                  ---
```

第二步，使用 **ping** *destination.com* 命令，查看执行结果。

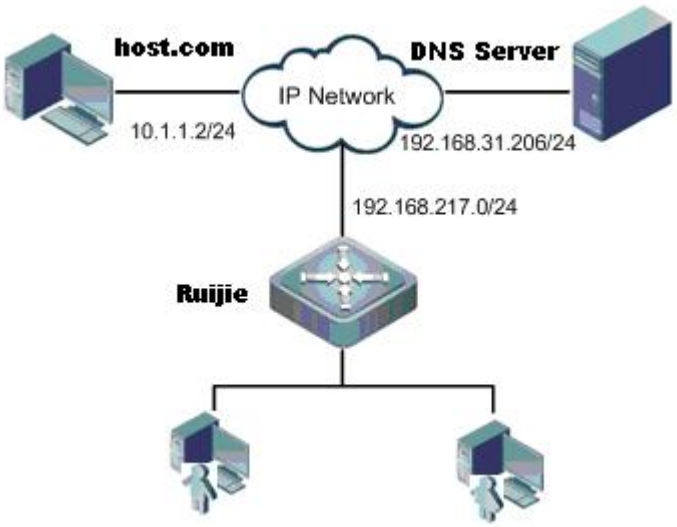
```
Ruijie-A# ping destination.com
Translating "destination.com"...[OK]
Sending 5, 100-byte ICMP Echoes to 1.1.1.20, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

从以上显示信息可以看出，Ruijie-A 通过静态域名解析，成功实现通过 destination.com 主机名访问 IP 地址为 1.1.1.20 的主机。

3.3.2 动态域名解析配置举例

拓扑图

图 5-2 动态域名解析配置组网图



应用需求

- DNS 域名服务器的 IP 地址为 192.168.31.206/24。
- 网络设备为 DNS 客户端，通过动态域名解析功能，实现通过 host.com 主机名访问 IP 地址为 10.1.1.2 的主机。

配置要点

1) DNS 客户端和 DNS 服务器端、访问主机间的路由要可达

2) DNS 域名解析开关打开。域名解析功能开关默认开启。

3) 正确配置 DNS 域名服务器的 IP 地址

配置步骤

第一步，配置 DNS 域名服务器

不同域名服务器的配置方法不同，请根据实际情况搭建 DNS 服务器。具体方法在此不做具体说明。

在 DNS 服务器上添加主机和 IP 地址的映射。本例中，设置主机名：host.com；IP 地址为 10.1.1.2/24

第二步，配置 DNS 客户端

DNS 客户端和 DNS 服务器端、访问主机间的路由要可达。接口 IP 配置如拓扑图所示。具体配置过程此处省略。

！打开 DNS 域名解析功能开关；该功能默认开启

```
Ruijie(config)#ip domain-lookup
```

！配置域名服务器的 IP 地址为 192.168.31.206

```
Ruijie(config)#ip name-server 192.168.31.206
```

配置验证

第一步，使用 **ping** *host.com* 命令，查看执行结果。

```
Ruijie# ping host.com
Translating " host.com "...[OK]
Sending 5, 100-byte ICMP Echoes to 10.1.1.2, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

从以上显示信息可以看出，客户端设备能 ping 通主机，且对应的目的 IP 地址为 10.1.1.2。设备通过动态域名解析，成功实现通过 host.com 主机名访问 IP 地址为 10.1.1.2 的主机。

第二步，查看域名解析信息；关注点主机名、主机 IP 地址。

```
Ruijie# show host
Name servers are:
192.168.31.206 static
Host                    type        Address           TTL(sec)
host.com             dynamic      10.1.1.2           3503
```

从以上显示信息可以看出，主机名同主机 IP 地址的映射表项正确。

4 网络通信检测工具

4.1 Ping连通性测试

为了测试网络的连通性，很多的网络设备都支持 Echo 协议，该协议包括发送一个特殊的数据包给指定的网络地址，然后等待该地址应答回来的数据包，通过 Echo 协议，可以评估网络的连通性、延时和网络的可靠性，利用 RGOS 提供的 Ping 工具，可以有效的帮助用户诊断、定位网络中的连通性问题。

Ping 命令运行在普通用户模式和特权用户模式下，在普通用户模式下，只能运行基本的 **Ping** 功能，而在特权用户模式下，还可以运行 Ping 的扩展功能。

命令	作用
Ruijie# **ping** [**ip**] [*address* [**length** *length*] [**ntimes** *times*] [**data** *data*][**source** *source*] [**timeout** *seconds*] [**df-bit**] [**validate**]]	**Ping**：网络连通性测试工具

普通的 Ping 功能，可以在普通用户模式和特权用户模式下执行，缺省将 5 个长度为 100Byte 的数据包发送到指定的 IP 地址，在指定的时间（缺省为 2 秒）内，如果有应答，则显示‘!’符号；如果没有应答，则显示‘.’符号。最后输出一个统计信息。以下为普通 ping 的实例：

```
Ruijie# ping 192.168.5.1
Sending 5, 100-byte ICMP Echoes to 192.168.5.1, timeout is 2 seconds:
< press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

扩展的 Ping 功能，只能在特权用户模式下执行。在扩展 Ping 中，可以指定发送数据包的个数、长度、超时的时间等等。和普通的 Ping 功能一样，最后也输出一个统计信息， 以下为一个扩展 Ping 的实例：

```
Ruijie# ping 192.168.5.197 length 1500 ntimes 100 data ffff source 192.168.4.190 timeout 3
Sending 100, 1500-byte ICMP Echoes to 192.168.5.197, timeout is 3 seconds:
  < press Ctrl+C to break >
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 2/2/3 ms
```

4.2 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 TTL 超时的错误数据包给源地址。根据这个规则，**Traceroute** 命令的执行过程是：首先给目的地址发送一个 TTL 为 1 的数据包，第一个网关便送回一个 ICMP 错误消息，以指明此数据包不能被发送，因为 TTL 超时，之后将数据包的 TTL 域加 1 后重新发送，同样第二个网关返回 TTL 超时错误，这个过程一直继续下去，直到到达目

的地址，记录每一个回送 ICMP TTL 超时信息的源地址，便记录下了数据从源地址到达目的地址，IP 数据包所经历的整个完整的路径。

Traceroute 命令可以在普通用户模式和特权用户模式下执行，具体的命令格式如下：

命令	作用
Ruijie# **traceroute** [**ip**] [*address* [**probe** *probe*] [**ttl** *minimum maximum*] [**source** *source*] [**timeout** *seconds*]]	跟踪数据包发送网络路径

以下为应用 Traceroute 的两个例子，一个为网络连接畅通，一个为网络连接存在某些网关不通的情况。

- 网络畅通的 Traceroute 例子：

```
Ruijie# traceroute 61.154.22.36
  < press Ctrl+C to break >
Tracing the route to 61.154.22.36
1       192.168.12.1         0 msec  0 msec  0 msec
2       192.168.9.2          4 msec  4 msec 4 msec
3       192.168.9.1          8 msec  8 msec  4 msec
4       192.168.0.10         4 msec  28 msec  12 msec
5       202.101.143.130     4 msec  16 msec  8 msec
6       202.101.143.154    12 msec  8 msec  24 msec
7       61.154.22.36         12 msec  8 msec  22 msec
```

从上面的结果可以清楚地看到，从源地址要访问 IP 地址为 61.154.22.36 的主机，网络数据包都经过了哪些网关（1－6），同时给出了到达该网关所花费的时间，这对于网络分析，是非常有用的。

- 网络中某些网关不通的 Traceroute 例子：

```
Ruijie# traceroute 202.108.37.42
< press Ctrl+C to break >
Tracing the route to 202.108.37.42
1       192.168.12.1         0 msec  0 msec  0 msec
2       192.168.9.2          0 msec  4 msec 4 msec
3       192.168.110.1       16 msec  12 msec  16 msec
4       *  *  *
5       61.154.8.129         12 msec  28 msec  12 msec
6       61.154.8.17           8 msec  12 msec  16 msec
7       61.154.8.250         12 msec  12 msec  12 msec
8       218.85.157.222       12 msec  12 msec  12 msec
9       218.85.157.130       16 msec  16 msec  16 msec
10      218.85.157.77        16 msec  48 msec  16 msec
11      202.97.40.65         76 msec  24 msec  24 msec
12      202.97.37.65         32 msec  24 msec  24 msec
13      202.97.38.162        52 msec  52 msec  224 msec
14      202.96.12.38         84 msec  52 msec  52 msec
15      202.106.192.226      88 msec  52 msec  52 msec
16      202.106.192.174      52 msec  52 msec  88 msec
```

```
17      210.74.176.158     100 msec  52 msec  84 msec
18      202.108.37.42        48 msec  48 msec  52 msec
```

从上面的结果可以清楚地看到，从源地址要访问 IP 地址为 202.108.37.42 的主机，网络数据包都经过了哪些网关（1－17），并且网关 4 不回应 ICMP 报文。

5 TCP

5.1 概述

TCP 模块为应用层提供了一个可靠的、有连接的基于 IP 的传输层协议。

应用层向 TCP 层发送用于网间传输的、用 8 位字节表示的数据流，然后 TCP 把数据流分割成适当长度的报文段，最大传输段大小（MSS）通常受该计算机连接的网络的数据链路层的最大传送单元（MTU）限制。之后 TCP 把结果包传给 IP 层，由它来通过网络将包传送给接收端实体的 TCP 层。

TCP 为了保证不发生丢包，就给每个字节一个序号，同时序号也保证了传送到接收端实体的包的按序接收。然后接收端实体对已成功收到的字节发回一个相应的确认(ACK)；如果发送端实体在合理的往返时延(RTT)内未收到确认，那么对应的数据（假设丢失了）将会被重传。

- 在数据正确性与合法性上，TCP 用一个校验和函数来检验数据是否有错误，在发送和接收时都要计算校验和；同时可以使用 md5 认证对数据进行加密。
- 在保证可靠性上，采用超时重传和捎带确认机制。
- 在流量控制上，采用滑动窗口协议，协议中规定，对于窗口内未经确认的分组需要重传。
- 在拥塞控制上，采用广受好评的 TCP 拥塞控制算法（也称 AIMD 算法）。该算法主要包括三个主要部分：1）加性增、乘性减；2）慢启动；3）对超时事件做出反应。

5.2 配置TCP

5.2.1 修改建立TCP连接的超时时间

建立 TCP 连接需要经过三次握手：主动端先发送 SYN 报文，被动放回应 SYN+ACK 报文，然后主动端再回应 ACK。

- 在主动端发送 SYN 后，如果被动端一直不回应 SYN+ACK 报文，主动端会不断的重传 SYN 报文直到超过一定的重传次数或超时时间。
- 在主动端发送 SYN 后，被动端回应 SYN+ACK 报文，但主动端不再回复 ACK，被动端也会一直重传直到超过一定的重传次数或超时时间。（SYN 报文攻击会出现这种情况）

可以通过以下命令配置 SYN 报文的超时时间（发送 SYN 报文到三次握手成功的最大时间），也就是建立 TCP 连接的超时时间。

命令	作用
Ruijie(config)# **ip tcp syntime-out** *seconds*	修改建立 TCP 连接的超时时间。 单位秒，取值范围 5-300，缺省值 20

使用 **no ip tcp syntime-out** 命令恢复参数缺省值。

本命令仅对 IPv4 TCP 生效。

5.2.2 修改缓冲区大小

TCP 的接收缓冲区是用来缓存从对端接收到的数据，这些数据后续会被应用程序读取。一般情况下，TCP 报文的窗口值反映接收缓冲区的空闲空间的大小。对于带宽比较大、有大批量数据的连接，增大接收缓冲区的大小可以显著提供 TCP 传输性能。TCP 的发送缓冲区是用来缓存应用程序的数据，发送缓冲区的每个字节都有序列号，被应答确认的序列号对应的数据会从发送缓冲区删除掉。增大发送缓冲区可以提高 TCP 跟应用程序的交互能力，也因此会提高性能。但是增大接收和发送缓冲区会导致 TCP 占用比较多的内存。

命令	作用
Ruijie(config)# **ip tcp window-size** *size*	修改 TCP 连接的接收和发送缓冲区大小。 单位字节，取值范围 0-65535，缺省值 4096。

使用 **no ip tcp window-size** 命令恢复接收和发送缓冲区大小为缺省值。

本命令只支持 IPv4 TCP。

本命令对于已经存在的 TCP 连接不生效，只对新建立的 TCP 连接生效。

本命令对接收缓冲区和发送缓冲区同时生效。

5.2.3 禁止端口不可达时的重置报文

TCP 模块在分发 TCP 报文时，如果找不到该报文所属的 TCP 连接会主动回复一个 reset 报文以终止对端的 TCP 连接。攻击者可能利用大量的端口不可达的 TCP 报文对设备进行攻击。

可以使用以下命令禁止/恢复在收到端口不可达的 TCP 报文时发送 reset 报文。

命令	作用
Ruijie(config)# **ip tcp not-send-rst**	禁止在接收到端口不可达的 TCP 报文时发送 reset 报文。

使用 **no ip tcp not-send-rst** 命令恢复发送 reset 报文。

本命令仅对 IPv4 TCP 生效。

5.2.4 限制TCP连接的MSS的最大值

MSS 是最大传输段大小的缩写，指一个 TCP 报文的数据载荷的最大长度，不包括 TCP 选项。

在 TCP 建立连接的三次握手中，有一种很重要的工作那就是进行 MSS 协商。连接的双方都在 SYN 报文中增加 MSS 选项，其选项值表示本端最大能接收的段大小，即对端最大能发送的段大小。连接的双方取本端发送的 MSS 值和接收对端的 MSS 值的较小者作为本连接最大传输段大小。

发送 SYN 报文时的 MSS 选项值的计算方法如下。

- 非直连网络中：mss = 默认值 536。

- 直连网络中：mss = 对端 ip 地址对应的出口的 MTU - 20 字节 ip 头 - 20 字节 tcp 头。
  一般来说如果出口配置的某些应用影响了接口的 mtu，那么该应用会相应的设置 mtu，如隧道口，vpn 口等。

10.4(3)的直连网络中被动连接方回复的 syn+ack 报文的 mss 选项值并不是通过 mtu 计算出来，而是采用默认值 536。

计算出来的 mss 不能超过接收缓冲区的大小并且不能超过用户配置的 **ip tcp mss** 大小，如果超过取最小者。

如果该连接支持某些选项，那么 mss 还要减去选项 4 字节对齐后的长度值。如 md5 选项要减去 20 字节，md5 选项长度 18 字节，对齐后 20 字节。

到这里得到的 rmss 值就是要发送的 syn 报文 mss 选项的值。举例：一般情况下在直连网络中建立 bgp 邻居，那么该连接的发送的 mss 为 1500 – 20 – 20 – 20 = 1440。

ip tcp mss 命令的作用是限制即将建立的 TCP 连接的 MSS 的最大值。任何新建立的连接协商的 MSS 值不能超过配置的值。

命令	作用
Ruijie(config)# **ip tcp mss** *max-segment-size*	限制 TCP 连接的 MSS 的最大值。 单位为字节，取值范围 68-10000。

使用 **no ip tcp mss** 命令取消此限制。

本命令仅对 IPv4 TCP 生效。

5.2.5 启用PMTU发现功能

TCP 的路径最大传输单元（PMTU）发现功能是按 RFC1191 实现的，这个功能可以提高网络带宽的利用率。当用户使用 TCP 来批量传输大块数据时，该功能可以使传输性能得到明显提升。

命令	作用
Ruijie(config)# **ip tcp path-mtu-discovery** [**age-timer** *minutes* **| age-timer infinite**]	启用 PMTU 发现功能。 **age-timer** *minutes*：TCP 在发现 PMTU 后，重新进行探测的时间间隔。单位分钟，取值范围 10-30。缺省值 10。 **age-timer infinite**：TCP 在发现 PMTU 后，不重新探测。

按 RFC1191 的描述，TCP 在发现 PMTU 后，隔一段时间可以使用更大的 MSS 来探测新的 PMTU。这个时间间隔就是使用参数 **age-timer** 来指定。当设备发现的 PMTU 比 TCP 连接两端协商出来的 MSS 小时，设备就会按上述配置时间间隔，去尝试发现更大的 PMTU。直到 PMTU 达到 MSS 的值，或者用户停止这个定时器，这个探测过程才会停止。停止这个定时器，使用 **age-timer infinite** 参数。

使用 **no ip tcp path-mtu-discovery** 命令关闭 PMTU 发现功能。

此功能的启用与关闭，对于已经存在的 TCP 连接不生效，只对新建立的 TCP 连接生效。

5.3 监视与维护

命令	作用
Ruijie# **show tcp connect**	显示系统当前 TCP 连接的基本信息
Ruijie# **show tcp pmtu**	显示 TCP PMTU 的信息

Ruijie# **show tcp port**	显示系统当前 TCP 端口使用情况

配置指南-组播

本分册介绍组播配置指南相关内容，包括以下章节：

1. IGMP Snooping
2. 组播转发控制

1 IGMP Snooping

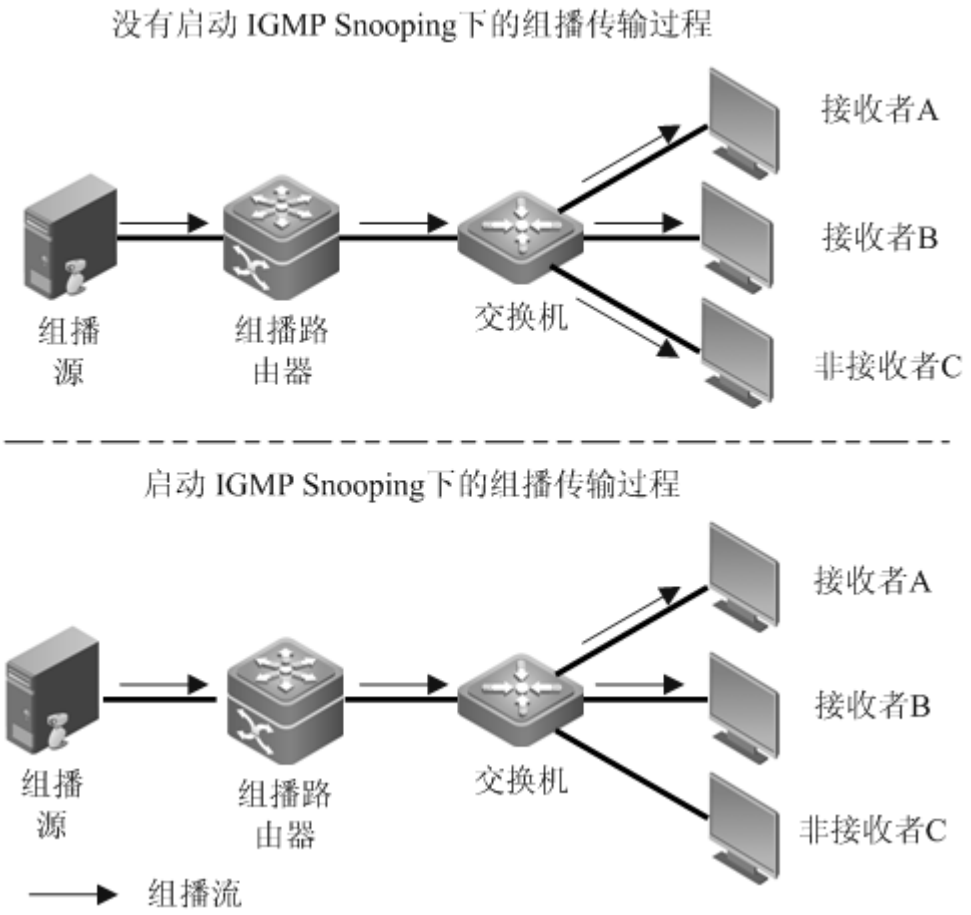
1.1 概述

1.1.1 IGMP Snooping 的工作原理

IGMP Snooping 是 Internet Group Management Protocol（组播侦听者发现协议窥探）的简称。它是运行在 VLAN 上的 IP 组播约束机制，用于管理和控制 IP 组播流在 VLAN 内的转发，属于二层组播功能。下面描述的 IGMP Snooping 功能，都是指在 VLAN 内进行的，相关的端口也是指 VLAN 内部的成员口。

运行 IGMP Snooping 的设备通过对收到的 IGMP 报文进行分析，为端口和组播地址建立起映射关系，并根据这样的映射关系转发 IP 组播数据报文。如图 1 所示，当交换机没有运行 IGMP Snooping 时，IP 组播数据报文在 VLAN 内被广播；当交换机运行了 IGMP Snooping 后，已知 IP 组播组的组播数据报文不会在 VLAN 内被广播，而是发给指定的接收者。

图 1-1 VLAN 上运行 IGMP Snooping 前后的对比

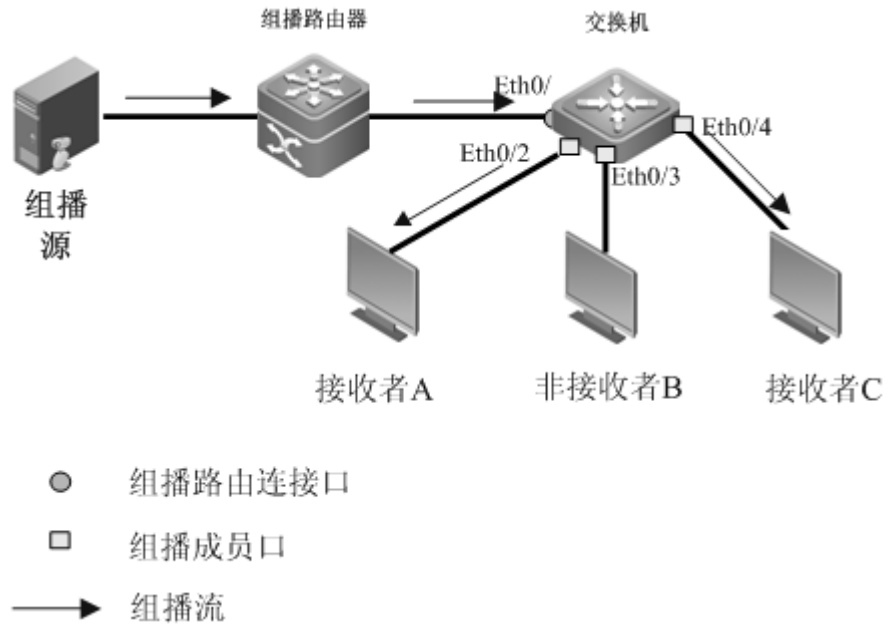


锐捷推出的组播设备支持二层组播(IGMP Snooping)与三层组播(Multicast-routing)共同使用。即在一台设备上，既支持三层组播的路由转发，又支持在 VLAN 内的窥探，以实现更为精确的报文转发功能。

1.1.2 IGMP Snooping 的两类端口

如图所示，Router 连接组播源，在 Switch A 运行 IGMP Snooping，Host A 和 Host C 为接收者主机（即 IP 组播组成员）。

图 1-2 IGMP Snooping 的两类端口



- 路由连接口（Multicast Router Port）：交换机上连接组播路由器（三层组播设备），如 Switch A 的 Eth0/1 端口。交换机将本设备上的所有路由连接口（包括动态和静态端口）都记录在路由连接口列表中。路由连接口缺省情况下是对应 VLAN 内组播数据的接收者，也会被添加到 IGMP Snooping 转发表中。
- 成员端口（Member Port）：IP 组播组成员端口的简称，又称侦听者端口（Listener Port），表示交换机上连接 IP 组播组成员侧的端口，如 Switch A 的 Eth0/2、Eth0/3 和 Eth0/4 端口。交换机将本设备上的所有成员端口（包括动态和静态端口）都记录在 IGMP Snooping 转发表中。

1.1.3 动态端口的老化定时器

类型	描述	触发定时器启动的事件	超时后交换机的动作
动态路由连接口的老化定时器	交换机为每个动态路由连接口都启动一个定时器，其超时时间就是动态路由连接口的老化时间	收到 IGMP 普遍组查询报文或 PIM Hello 报文	将该端口从路由连接口列表中删除
动态成员端口的老化定时器	交换机为该端口启动一个定时器，其超时时间就是动态成员端口老化时间	收到 IGMP 的查询报文	将该端口从 IGMP Snooping 组播组的转发表中删除

1.1.4 IGMP Snooping 的工作机制

普遍组查询和特定组查询

IGMP 查询者定期向本地网段内的所有主机与路由器（地址为 224.0.0.1）发送普通组查询报文，以查询该网段有哪些 IP 组播组的成员。在收到 IGMP 普遍组查询报文时，交换机将查询报文向本 VLAN 内的所有端口转发出去，并对该报文的接收端口做如下处理：

- 如果该端口已经在路由连接口列表中，则重置其老化定时器。
- 如果该端口不在路由连接口列表中，则将其添加到路由连接口列表中，并启动其老化定时器。

在收到 IGMP 的普遍组查询报文后，组播设备会对所有的成员端口启动各自的老化定时器，定时器时间为配置的对 IGMP 查询报文的最长响应时间，当定时器超时时，则认为该端口不再有成员接收组播流，组播设备就会把该端口从 IGMP Snooping 的转发表中删除。

在收到 IGMP 的特定组查询报文后，组播设备会对该特定组的所有成员端口启动老化定时器，定时器时间为最长响应时间，当定时器超时了还没有接收到主机的应答，则认为该端口不再有成员接收组播流，组播设备就会把该端口从 IGMP Snooping 的转发表中删除。对于 IGMP 的特定组源查询报文，不做定时器的更新处理。

报告成员关系

以下情况，主机会向 IGMP 查询者发送 IGMP 成员关系报告报文：

- 当 IP 组播组的成员主机收到 IGMP 查询(普遍组查询或特定组查询)报文后，会应答 IGMP 成员关系报告报文。
- 如果主机要加入某个 IP 组播组，它会主动向 IGMP 查询者发送 IGMP 成员关系报告报文以声明加入该 IP 组播组。

在收到 IGMP 成员关系报告报文时，交换机将其通过给 VLAN 内的所有路由连接口转发出去，从该报文中解析出主机要加入的 IP 组播组地址，并对该报文的接收端口做如下处理：

- 如果不存在该 IP 组播组所对应的转发表项，则创建转发表项，将该端口作为动态成员端口添加到出端口列表中，并启动其老化定时器；
- 如果已存在该 IP 组播组所对应的转发表项，但其出端口列表中不包含该端口，则将该端口作为动态成员端口添加到出端口列表中，并启动其老化定时器；
- 如果已存在该 IP 组播组所对应的转发表项，且其出端口列表中已包含该动态成员端口，则重置其老化定时器。

离开组播组

当主机离开 IP 组播组时，会通过发送 IGMP 离开组报文，以通知组播路由器自己离开了某个 IP 组播组。当前锐捷产品提供两种离开方式：

- 自动离开：当交换机从某动态成员端口上收到 IGMP 离开组报文时，将直接向路由连接口转发。同时启动一个组成员超时定时器，定时器超时前还没有收到相应的应答报文，将相关成员口老化；
- 快速离开：当交换机从某动态成员端口上收到 IGMP 离开组报文时，将直接向路由连接口转发。同时直接删除相关的组成员接口。

1.1.5 IGMP Snooping 的各种工作模式

- DISABLE 模式。在 DISABLE 模式下，IGMP Snooping 不起作用，即二层组播不起作用，VLAN 内不“窥探”主机与路由设备之间的 IGMP 报文，组播帧在 VLAN 内被广播。
- IVGL 模式(Independent VLAN Group Learning)。在 IVGL 模式下，各 VLAN 间的组播流是相互独立的。主机只能朝与自己处于同一个 VLAN 的路由连接口请求接收组播流；交换机在接收到任何一个 VLAN 的组播流时，只能往相同 VLAN 内的成员口转发。

1.1.6 IGMP Snooping 查询器

在运行了 IGMP 的组播网络中，会有一台三层组播设备充当 IGMP 查询者，负责发送 IGMP 查询报文，使三层组播设备能够在网络层建立并维护组播转发表项，从而在网络层正常转发组播数据。

但是，在一个没有三层组播设备的网络中，由于二层设备并不支持 IGMP，因此无法实现 IGMP 查询器的相关功能。为了解决这个问题，可以在二层设备上使能 IGMP Snooping 查询器，使二层设备能够在数据链路层建立并维护组播转发表项，从而在数据链路层正常转发组播数据。

1.1.7 组播安全控制

组播权限控制

IGMP 本身没有对用户是否能加入某个组播组进行控制的办法，而由于组播数据流是在接入节点进行复制的，因此在接入节点对用户是否允许获得某个组播视频流的控制，对视频数据的安全性、保障运营商利益、防止非法用户等方面显得尤为重要。目前，可以通过设备管理功能在用户端口预先设定个性化的 Profile，对于特定的一个或一组组播节目设置访问权限，允许或禁止用户的加入、控制组播业务，防止非法用户占用网络资源。通过类似的功能，还可以在接入节点上对用户访问组播节目进行更精细的控制，如组播预览等功能，对于特定用户，限制其可以观看的节目和数量等，从而有效保护网络带宽资源。

锐捷推出的组播设备中，支持对用户进行多样化的控制：

- 基于端口控制用户点播组播流的权限
  在某些情况下，可能需要在端口上，对用户点播组播流的权限进行控制，此时可以采用基于端口的组播过滤器进行配置。详细配置见“配置端口过滤器”章节描述。
- 基于 VLAN 控制用户点播组播流的权限
  在某些情况下，可能需要在对不同 VLAN，允许点播不同范围的组播流，此时可以采用基于 VLAN 的组播过滤器进行配置。详细配置见“配置 VLAN 过滤器”章节描述。
- 基于端口控制用户所能点播的组播流数量
  如果用户在同一个端口点播多条组播流，对网络带宽会产生较大的压力，此时通过配置端口允许的组播流数量，可以有效地控制用户点播的组播流。详细配置见“配置 IGMP Filtering”章节描述。
- 组播预览
  对于一些组播视频流，如果用户没有开通点播此视频流的权限，而服务提供商又想能够让用户进行预览，达到预览时间后，再停止组播流。要实现这种功能，需要设备能够提供基于用户的组播预览功能。

1.2 配置IGMP Snooping

- 当在 Private VLAN 或者 Super VLAN 上开启二层组播后，当子 VLAN 内存在组播源时，由于组播转发时需要进行入口合法性检查，此时需要多复制一条表项，入口为组播流进入的子 VLAN。造成的影响是多占用了一条组播硬件表项，表现出来的组播容量减少 1。部署网络时，建议组播流从 Private VLAN 或者 Super VLAN 的主 VLAN 进入，其它子 VLAN 作为出口 VLAN 连接主机接受组播流。
- 当在 Private VLAN 或者 Super VLAN 上开启二层组播，作为组播流转发出口的端口建议为 Access 口。如果组播流转发出口为 Trunk 口，可能会导致该 Trunk 口转发出多份重复组播流的情况发生。
- 当设备启动 IGMP Snooping 功能后，VLAN 内部的组播协议报文将不能在 VLAN 内进行硬件广播，此时这些组播协议报文将由软件进行广播，由于软件广播比硬件广播的转发性能低，因此 VLAN 内如果存在大量组播协议报文转发需求的情况下，建议关闭 IGMP Snooping 功能，以保证组播协议报文的转发性能。

1.2.1 启动 IGMP Snooping（IVGL 模式）

命令	作用
Ruijie(config)# **ip igmp snooping ivgl**	启动并设置 IGMP Snooping 为 IVGL 模式。

启动 IGMP Snooping 的时候，必须指定 IGMP Sooping 的工作模式。缺省情况下，IGMP Snooping 处于关闭状态。

例：打开并设置 IGMP Snooping 为 IVGL 模式

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping ivgl
Ruijie(config)# show ip igmp snooping
IGMP Snooping running mode: IVGL
SVGL vlan: 1
SVGL profile number: 0
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable
```

1.2.2 关闭 IGMP Snooping

命令	作用
Ruijie(config)# **no ip igmp snooping**	关闭所有 VLAN 的 IGMP Snooping。
Ruijie(config)# **no ip igmp snooping vlan** *num*	关闭指定 VLAN 的 IGMP Snooping。
Ruijie(config)# **ip igmp snooping vlan** *num*	打开指定 VLAN 的 IGMP Snooping。

当全局打开 IGMP Snooping，所有 VLAN 也将自动打开 IGMP Snooping 功能。使用 **no ip igmp snooping vlan** 命令可以仅在特定 VLAN 上关闭 IGMP Snooping 功能。

例：关闭 IGMP Snooping

```
Ruijie# configure terminal
Ruijie(config)# no ip igmp snooping
Ruijie(config)# show ip igmp snooping
IGMP Snooping running mode: DISABLE
SVGL vlan: 1
SVGL profile number: 0
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable
```

例：关闭 vlan 3 的 IGMP Snooping

```
Ruijie# configure terminal
Ruijie(config)# no ip igmp snooping vlan 3
Ruijie(config)# show ip igmp snooping
IGMP Snooping running mode: IVGL
SVGL vlan: 1
SVGL profile number: 0
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable

vlan 1
-------------
IGMP Snooping                   :Enabled
Multicast router learning mode  :pim-dvmrp
IGMPv2 immediate leave          :Disabled

vlan 2
-------------
IGMP Snooping                   :Enabled
Multicast router learning mode  :pim-dvmrp
IGMPv2 immediate leave          :Disabled

vlan 3
-------------
IGMP Snooping                   :Disabled
Multicast router learning mode  :pim-dvmrp
IGMPv2 immediate leave          :Disabled

vlan 4
-------------
IGMP Snooping                   :Enabled
Multicast router learning mode  :pim-dvmrp
```

```
IGMPv2 immediate leave          :Disabled
```

1.2.3 配置路由连接口

静态路由连接口

命令	作用
Ruijie(config)# **ip igmp snooping vlan** *vlan-id* **mrouter interface** *interface-id*	设置接口为静态路由连接口。
Ruijie(config)# **no ip igmp snooping vlan** *vlan-id* **mrouter interface** *interface-id*	取消接口为静态路由连接口。

在 IVGL 模式下，所有 VLAN 的静态路由连接口的配置均可生效。

动态路由连接口

命令	作用
Ruijie(config)# **ip igmp snooping vlan** *vlan-id* **mrouter learn pim-dvmrp**	在 VLAN 上启动动态学习路由连接口的功能。缺省启动。
Ruijie(config)# **no ip igmp snooping vlan** *vlan-id* **mrouter learn pim-dvmrp**	关闭动态学习路由连接口的功能，并清空所有动态学习到的路由连接口。
Ruijie(config)# **ip igmp snooping dyn-mr-aging-time** *time*	配置动态路由连接口老化时间，取值范围 1-3600，默认值为 300s。
Ruijie(config)# **no ip igmp snooping dyn-mr-aging-time**	恢复动态路由连接口的老化时间为默认值。

对于动态路由连接口，如果在其老化时间超时前没有收到 IGMP 普遍组查询报文或者 PIM Hello 报文，交换机将把该端口从路由器端口列表中删除。

动态路由连接口的老化时间值应该根据实际网络拓扑及配置决定，即配置取值应该大于相关组播设备 Hello 消息发送间隔。建议配置成组播设备 Hello 消息发送间隔的 3.5 倍。

动态路由连接口老化时间并非即配即用。在下一次定时器更新时，才会启用该配置值。

例：设置以太网接口 1/1 为 VLAN1 的静态路由连接口，并启动 VLAN1 动态学习路由连接口功能

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping vlan 1 mrouter interface gigabitEthernet 1/1
Ruijie(config)# ip igmp snooping vlan 1 mrouter learn pim-dvmrp
Ruijie(config)# end
Ruijie# show ip igmp snooping mrouter
Vlan    Interface             State
----    -------------------   ------
1       GigabitEthernet 1/1   static
1       GigabitEthernet 0/2   dynamic
Ruijie# show ip igmp snooping mrouter learn
Vlan    learn method
```

```
----    ------------------
1       pim-dvmrp
```

例：配置动态路由连接口老化时间为 100s

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping dyn-mr-aging-time 100
```

1.2.4 配置成员口

静态成员口

命令	作用
Ruijie(config)# **ip igmp snooping vlan** *vlan-id* **static** *ip-addr* **interface** *interface-id*	配置一个静态成员口。 • *vlan-id*：组播流的 vid • *ip-addr*：组播地址 • *interface-id*： 端口号
Ruijie(config)# **no ip igmp snooping vlan** *vlan-id* **static** *ip-addr* **interface** *interface-id*	删除一个静态成员口。 • *vlan-id*：组播流的 vid • *ip-addr*：组播地址 • *interface-id*： 端口号

如果某端口所连接的主机需要固定接收发往某 IP 组播组的 IP 组播数据，可以配置该端口静态加入该 IP 组播组，成为静态成员端口。

可以用 **no ip igmp snooping vlan** *vlan-id* **static** *ip-addr* **interface** *interface-id* 删除组播成员的静态配置。

例：配置 IGMP snooping 静态成员端口

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping vlan 1 static 233.3.3.4 interface GigabitEthernet 0/7
Ruijie(config)# end
Ruijie# show ip igmp snooping gda
Abbr: M - mrouter
      D - dynamic
      S - static
VLAN  Address      Member ports
----  -----------  ----------------------
1     233.3.3.4    GigabitEthernet 0/7(S)
```

在 IVGL 模式下，所有 VLAN 的静态成员口的配置均可生效。

动态成员端口老化时间

命令	作用

Ruijie(config)# **ip igmp snooping host-aging-time** *time*	配置 IGMP 动态成员口存活时间，范围为 1-65535，缺省值为 260s。
Ruijie(config)# **no ip igmp snooping host-aging-time**	恢复 IGMP 查询报文的最长响应时间为缺省值。

动态成员端口老化时间是指当交换机的某端口收到主机发送的加入某 IP 组播组的 IGMP 加入报文时，为这个动态成员端口设置的老化时间。

在收到 IGMP 加入报文后，会重置这个动态成员端口的老化定时器，定时器时间为 host-aging-time。如果定时器超时，则认为该端口下不存在接收组播报文的用户主机，组播设备就会把该端口从 IGMP Snooping 的成员口中删除。配置完该命令，后面收到的 IGMP 加入报文时设置的动态成员端口老化定时器的值为 host-aging-time。该配置在下一次收到加入报文时生效，当前已启动的成员口的定时器不会被更新。

例：配置 IGMP 动态端口老化时间为 30s

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping host-aging-time 30
```

配置 IGMP 组查询的最大响应时间

命令	作用
Ruijie(config)# **ip igmp snooping query-max-response-time** *time*	配置 IGMP 查询报文的最长响应时间，范围为 1-65535，缺省值为 10s。
Ruijie(config)# **no ip igmp snooping query-max-response-time**	恢复 IGMP 查询报文的最长响应时间为缺省值，缺省值为 10s。

在收到 IGMP 普通查询报文后，组播设备会重置所有动态成员口的老化定时器，定时器时间为 query-max-response-time。如果定时器超时，则认为该端口下不存在接收组播报文的用户主机，组播设备就会把该端口从 IGMP Snooping 的成员口中删除。

在收到 IGMP 特定组查询报文后，组播设备会重置该特定组的所有动态成员口的老化定时器，定时器时间为 query-max-response-time。如果定时器超时，则认为该端口下不存在接收组播报文的用户主机，组播设备就会把该端口从 IGMP Snooping 的成员口中删除。

对于 IGMPv3 的特定组源查询报文，不做定时器的更新处理。该配置在下一次收到查询报文时生效，当前已启动的定时器不会被更新。

例：配置 IGMP 查询报文的最长响应时间为 15s

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping query-max-response-time 15
```

成员口快速离开

命令	作用
Ruijie(config)# **ip igmp snooping fast-leave enable**	打开成员口快速离开功能。缺省关闭。
Ruijie(config)# **no ip igmp snooping fast-leave enable**	关闭端口快速离开功能。

端口快速离开是指当交换机从某端口收到主机发送的离开某 IP 组播组的 IGMP 离开组报文时，直接把该端口从对应转发表项的成员口中删除。在交换机上，如果端口下只连接有一个接收者，则可以通过使能端口快速离开功能以节约带宽和资源。该功能运用在相关端口下只存在一个点播者的情况。

例：打开成员口快速离开功能

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping fast-leave enalbe
```

1.2.5 配置 IGMP report 报文抑制

命令	作用
Ruijie(config)# **ip igmp snooping suppression enable**	打开 IGMP Report 报文抑制功能，缺省关闭。
Ruijie(config)# **no ip igmp snooping suppression enable**	关闭 IGMP Report 报文抑制功能。

每当成员口收到一个 IGMP Report 报文，都会将该报文转发给路由连接口。如果在一个查询间隔内，某 VLAN 的成员口上收到了多份相同的 Report 报文，路由连接口上就会收到多份相同的 Report 报文。如果打开 Report 报文抑制功能，则在一个查询间隔内，路由连接口只会将收到的某 IP 组播组的第一个 IGMP report 报文发送出去。否则路由连接口会将所有收到的 IGMP report 报文发送出去。打开 IGMP Report 报文抑制功能，有利于减少网络中的报文数量。

例：打开 IGMP Report 报文抑制功能

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping suppression enable
```

1.2.6 配置 IGMP Profiles

命令	作用
Ruijie(config)# **ip igmp profile** *profile-number*	进入 Profile 模式，分配一个数字以供标识，该数字范围为 1－1024，缺省情况下没有配置任何一条 profile。
Ruijie (config-profile)# **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。
Ruijie(config-profile)# **range** *low-address high_address*	设定组地址范围，该值即可以是一个单个的 IP 组地址也可以是一个组地址的区间（前面的为低 IP 组地址，后面为高 IP 组地址），同时可以配置多个 range 范围。

profile 是一种针对组的“过滤器”，供其它功能引用。配置步骤：

1，使用 ip igmp profile 命令创建一个 profile，并进入 profile 模式

2，使用 permit 命令允许指定范围内的组通过过滤器、使用 deny 命令将指定范围内的组过滤掉。

3，使用 range 命令定义组范围

> 如果要删除其中一个 profile，可以用 **no ip igmp profile** *profile number* 来执行。如果要删除 profile 里的一个 range，可以用 **no range** *ip multicast address* 来执行。

例：配置 profile 1，允许组 224.2.2.2～224.2.2.244

```
Ruijie(config)# ip igmp profile 1
Ruijie(config-profile)# permit
```

```
Ruijie(config-profile)# range 224.2.2.2 224.2.2.244
```

1.2.7 配置端口过滤器

命令	作用
Ruijie(config-if)# **ip igmp snooping filter** *profile-number*	应用 Profile 于该端口，*profile number* 范围为 1- 1024。缺省情况下，一个端口不关联任何的 profile。
Ruijie(config-if)# **no ip igmp snooping filter**	删除接口上关联的 profile，接口上将允许所有组通过。
Ruijie(config-if)# **ip igmp snooping max-groups** *number*	限制端口能够动态加入的组数，参数范围为 0 – 1024。缺省情况下，无限制。

在某些情况下，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。

例：配置端口过滤器

```
Ruijie# configure terminal
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# ip igmp snooping filter 1
Ruijie(config-if)# ip igmp snooping max-groups 1000
Ruijie(config-if)# end
Ruijie# show ip igmp snooping interface fastEthernet 0/1
Interface          Filter profile number  max-group
-----------------  ---------------------  ---------
FastEthernet 0/1   1                      1000
```

1.2.8 配置 VLAN 过滤器

命令	作用
Ruijie(config)# **ip igmp snooping vlan** *num* **filter** *profile-number*	应用 Profile 于该 VLAN，*profile number* 范围为 1- 1024。缺省情况下，一个 VLAN 不关联任何的 profile。
Ruijie(config-if)# **no ip igmp snooping vlan** *num* **filter**	删除 VLAN 上关联的 profile，VLAN 上将允许所有组通过。

在某些情况下，您可能需要控制特定 VLAN 出口的组播数据流接收权限。基于 VLAN 的过滤器满足了这种需求。

您可以把某一个 IGMP Profile 应用在一个 VLAN 下，如果该 VLAN 下的端口收到 IGMP Report 报文，则二层组播设备就会查找这个端口所要加入的组播地址是否在 IGMP Profile 允许范围之内。若是，则允许加入，之后才进行后续处理。

例：配置 VLAN 过滤器

```
Ruijie# configure terminal
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# ip igmp snooping vlan 2 filter 1
```

1.2.9 配置组播预览

命令	作用
Ruijie(config)# **ip igmp snooping preview** *profile-number*	应用 Profile 于该预览信息，*profile number* 范围为 1- 1024。缺省情况下，不允许任何组播流进行预览。
Ruijie(config)# **ip igmp snooping preview interval** *num*	配置预览时间，*num* 范围为<1- 300>,缺省情况为 60sec。
Ruijie(config)# **no ip igmp snooping preview**	不允许预览。

例：允许对不满足 profiles1 但满足 profiles2 的组播流进行组播预览

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping preview 2
Ruijie(config)# int fa 0/1
Ruijie(config-if)# ip igmp snooping filter 1
```

1.2.10 配置 IGMP Snooping 查询器

启动 IGMP Snooping 查询器

命令	作用
Ruijie(config)# **ip igmp snooping querier**	全局启动 IGMP Snooping 查询器功能。
Ruijie(config)# **no ip igmp snooping querier**	全局关闭 IGMP Snooping 查询器功能。
Ruijie(config)# **ip igmp snooping vlan** *num* **querier**	启动某 VLAN 的 IGMP Snooping 查询器功能。
Ruijie(config)# **no ip igmp snooping vlan** *num* **querier**	关闭某 VLAN 的 IGMP Snooping 查询器功能。

配置查询报文最大响应时间

命令	作用
Ruijie(config)# **ip igmp snooping querier max-response-time** *num*	全局设置发送查询报文的最大响应时间。缺省值为 10sec。
Ruijie(config)# **no ip igmp snooping querier max-response-time**	全局恢复发送查询报文的最大响应时间为缺省值。
Ruijie(config)# **ip igmp snooping vlan** *num* **querier max-response-time** *num*	设置某 VLAN 的发送查询报文的最大响应时间。缺省值为 10sec。
Ruijie(config)# **no ip igmp snooping vlan** *num* **querier max-response-time**	恢复某 VLAN 的发送查询报文的最大响应时间为缺省值。

例：全局配置查询报文最大响应时间

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping querier 20
```

例：配置某 VLAN 的查询报文最大响应时间

```
Ruijie# configure terminal
```

```
Ruijie(config)# ip igmp snooping vlan 2 querier 20
```

配置查询报文查询间隔

命令	作用
Ruijie(config)# **ip igmp snooping querier query-interval** *num*	全局设置 IGMP 定时发送查询报文的时间间隔。缺省值为 60sec。
Ruijie(config)# **no ip igmp snooping querier query-interval**	全局恢复 IGMP 定时发送查询报文的时间间隔为缺省值。
Ruijie(config)# **ip igmp snooping vlan** *num* **querier query-interval** *num*	设置某 VLAN 的 IGMP 定时发送查询报文的时间间隔。缺省值为 60sec。
Ruijie(config)# **no ip igmp snooping vlan** *num* **querier query-interval**	恢复某 VLAN 的 IGMP 定时发送查询报文的时间间隔为缺省值。

例：全局配置查询报文查询间隔

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping querier query-interval 300
```

例：配置某 VLAN 的查询报文查询间隔

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping vlan 2 querier query-interval 300
```

配置非查询者超时时间

命令	作用
Ruijie(config)# **ip igmp snooping querier timer expiry** *num*	全局配置非查询者超时时间。
Ruijie(config)# **no ip igmp snooping querier timer expiry**	全局配置非查询者超时时间为缺省值。
Ruijie(config)# **ip igmp snooping vlan** *num* **querier timer expiry** *num*	配置某 VLAN 的非查询者超时时间。
Ruijie(config)# **no ip igmp snooping vlan** *num* **querier timer expiry**	配置某 VLAN 的非查询者超时时间为缺省值。

例：全局配置非查询者超时时间

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping querier timer expiry 70
```

例：配置某 VLAN 的非查询者超时时间

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping vlan 2 querier timer expiry 70
```

配置 IGMP Snooping 查询器运行的 IGMP 版本

命令	作用
Ruijie(config)# **ip igmp snooping querier version** *num*	全局配置查询器运行的 IGMP 版本。取值范围为<1-2>,缺省值为 2。
Ruijie(config)# **no ip igmp snooping querier version**	全局恢复 IGMP 版本的缺省值。
Ruijie(config)# **ip igmp snooping vlan** *num* **querier version** *num*	VLAN 上配置查询器运行的 IGMP 版本。取值范围为<1-2>,缺省值为 2。
Ruijie(config)# **no ip igmp snooping vlan** *num* **querier version**	VLAN 上恢复 IGMP 版本的缺省值。

例：全局配置查询器运行的 IGMP 版本

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping querier version 1
```

例：VLAN 上配置查询器运行的 IGMP 版本

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping vlan 2 querier version 1
```

1.3 监视与维护

1.3.1 查看 IGMP Snooping 配置信息

命令	作用
Ruijie# **show ip igmp snooping**	查看 IGMP Snooping 当前的工作模式及全局配置。

例：查看 IGMP Snooping 配置信息

```
Ruijie# show ip igmp snooping
IGMP Snooping running mode: IVGL
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable
IGMP Globle Querier: Disable
IGMP Preview: Disable
IGMP Preveiw group aging time : 60(Seconds)
Dynamic Mroute Aging Time : 300(Seconds)
Tunnel IGMP Packet:  Disable

vlan 1
-------------
IGMP Snooping state: Enabled
Multicast router learning mode: pim-dvmrp
IGMPv2 fast leave: Disabled
IGMP VLAN querier: Disable
```

1.3.2 查看和清除 IGMP Snooping 的统计值

命令	作用
Ruijie# **show ip igmp snooping statistics** [**vlan** *vlan-id*]	查看 IGMP Snooping 的统计信息。
Ruijie# **clear ip igmp snooping statistics**	清除 IGMP Snooping 的统计信息

例：查看 IGMP Snooping 的统计信息

```
Ruijie# show ip igmp snooping statistics
Current number of Gda-table entries: 1
Configured Statistics database limit: 1024
Current number of IGMP Query packet received : 1957
Current number of IGMPv1/v2 Report packet received: 5
Current number of IGMPv3 Report packet received: 4
Current number of IGMP Leave packet received: 1

 GROUP     Interface  Last         Last       Report  Leave
                      report time  reporter   pkts    pkts
---------  ---------  -----------  ---------  ------  --------
233.3.3.3   gi1/1    00:02:40      1.1.1.1    3       1
```

1.3.3 查看路由连接口

命令	作用
Ruijie# **show ip igmp snooping mrouter**	查看 IGMP Snooping 的路由连接口信息。

例：查看 IGMP Snooping 的路由连接口

```
Ruijie# show ip igmp snooping mrouter
Multicast Switching Mroute Port
  D: DYNAMIC
  S: STATIC
(*, *, 1):
  VLAN(1)  1 MROUTES:
GigabitEthernet 0/2(S)
```

1.3.4 查看和清除 IGMP Snooping 的转发表

命令	作用
Ruijie# **show ip igmp snooping gda-table**	查看 IGMP Snooping 的转发表。 转发表即 GDA（Group Destination Address）表。
Ruijie# **clear ip igmp snooping gda-table**	清除动态成员口。 此命令不能删除静态成员口。

例：查看 GDA 表

```
Ruijie# show ip igmp snooping gda-table
Multicast Switching Cache Table
  D: DYNAMIC
  S: STATIC
  M: MROUTE
(*, 233.3.6.29, 1):
  VLAN(1) 3 OPORTS:
    GigabitEthernet 0/3(S)
    GigabitEthernet 0/2(M)
    GigabitEthernet 0/1(D)

(*, 233.3.6.30, 1):
  VLAN(1) 2 OPORTS:
    GigabitEthernet 0/2(M)
    GigabitEthernet 0/1(D)
```

如果在 Private-vlan 或者 Super-vlan 上启动了 IGMP Snooping，那么此时建立的 gda 转发表项都是基于 Private-vlan 或者 Super-vlan 的主 VLAN 创建的。该转发表项表明，所有转发出口都可以接收来自主 VLAN 过来的组播流信息；对于从子 VLAN 转发过来的组播流信息，其转发规则还需要遵循 Private-vlan 或者 Super-vlan 的转发规则进行。在这种情况下，每个 gda 的转发表项可能会对应多个硬件转发表项，所以会有可能表现出转发表项容量低于指标值的情况。

1.3.5 查看 Profile

命令	作用
Ruijie# **show ip igmp profile** *profile-number*	查看 Profile 的信息。

例：查看 Profile 的信息

```
Ruijie# show ip igmp profile 1
Profile     1
        Permit
        range 224.0.1.0,    239.255.255.255
```

1.3.6 查看端口过滤器

命令	作用
Ruijie# **show ip igmp snooping interface** *interface*	查看端口过滤器的信息

例：查看 IGMP Filtering 的信息

```
Ruijie# show ip igmp snooping interface GigabitEthernet 0/7
Interface            Filter Profile number  max-groups
-------------------  ---------------------  -----------
GigabitEthernet 0/7  1                      4294967294
```

1.3.7 查看 IGMP Snooping 查询器

命令	作用
Ruijie# **show ip igmp snooping querier**	查看 IGMP Snooping 查询器的信息。
Ruijie# **show ip igmp snooping querier detail**	查看 IGMP Snooping 查询器的详细信息。

例：查看 IGMP Snooping 查询器的信息

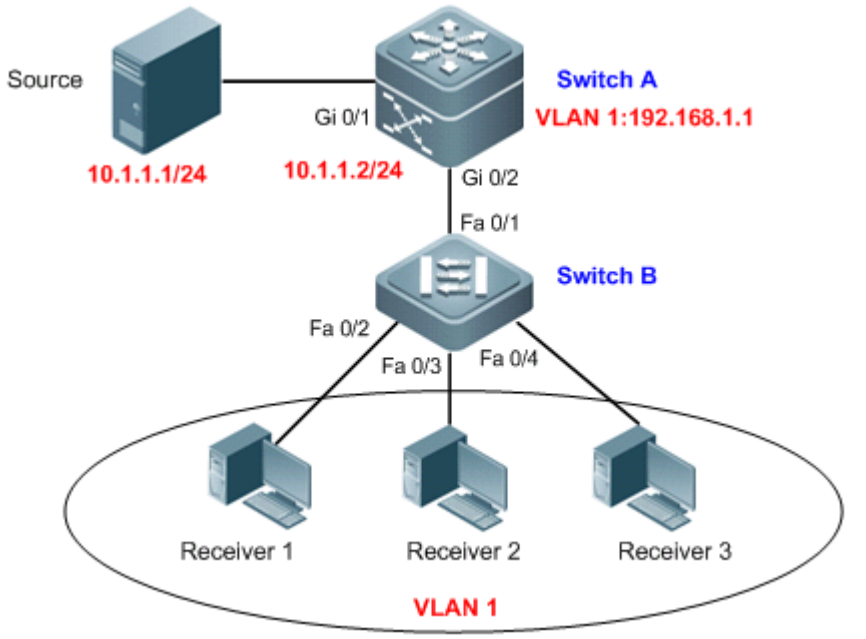
```
Ruijie# show ip igmp snooping querier detail
Vlan      IP Address           IGMP Version           Port
-----------------------------------------------------------


Global IGMP switch querier status
-----------------------------------------------------------
admin state                    : Enable
admin version                  : 2
source IP address              : 1.1.1.1
query-interval (sec)           : 125
max-response-time (sec)        : 10
querier-timeout (sec)          : 60

Vlan 1:   IGMP switch querier status
-----------------------------------------------------------
admin state                    : Enable
admin version                  : 2
source IP address              : 1.1.2.2
query-interval (sec)           : 125
max-response-time (sec)        : 10
querier-timeout (sec)          : 60
operational state              : Disable
operational version            : 2

Vlan 2:   IGMP switch querier status
-----------------------------------------------------------
admin state                    : Disable
admin version                  : 2
source IP address              : 1.1.1.1
query-interval (sec)           : 125
max-response-time (sec)        : 10
querier-timeout (sec)          : 60
operational state              : Disable
operational version            : 2
```

1.4 配置举例

1.4.1 IVGL 模式典型应用

拓扑图

图 1-3



应用需求

如上图所示，Switch A 作为组播路由设备直连组播源，Switch B 作为二层接入设备下联多个组播接收者，属于同一个 VLAN。主要需求如下：

- 在 Switch A 上，实现三层组播路由；在 Switch B 上，组播数据流不会在 VLAN 内广播，能够发给指定的接收者。
- Receiver 1 能够固定接收组地址为 224.1.1.1 的 IP 组播数据流；Receiver 2 仅允许接收组地址为 225.1.1.1~226.1.1.1 的 IP 组播数据流；Receiver 3 仅允许加入 100 个 IP 组播组。
- 在 Switch B 上，所有接入端口能够快速离开某 IP 组播组。
- 在 Switch B 上，抑制 IGMP 成员转发给 Switch A 的响应报文，减轻 Switch A 的负担。

配置要点

- 在组播路由设备上（本例为 Switch A）开启相应的组播路由转发功能并在相应三层接口上配置组播路由协议（本例为 Gi 0/1 和 VLAN 1）；在二层组播设备上（本例为 Switch B）配置 IGMP Snooping 为 IVGL 模式，路由连接口可通过动态生成，也可以静态配置（本例配置端口 Fa 0/1 为静态路由连接口）。

- 将 Receiver 1 直连的端口（本例为 Fa 0/2）配置为对应组的静态成员端口；将 Receiver 2 直连的端口（本例为 Fa 0/3）配置 IGMP Filtering 功能；将 Receiver 3 直连的端口（本例为 Fa 0/4）配置允许最多动态加入的组播组数。
- 在运行 IGMP Snooping 的设备上（本例为 Switch B）配置端口快速离开功能。
- 在运行 IGMP Snooping 的设备上（本例为 Switch B）配置 IGMP Snooping 成员关系报告报文的响应抑制功能。

配置步骤

第一步，在组播路由设备上配置组播路由功能。

！在 Switch A 上全局开启组播路由转发功能。

```
SwitchA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)#ip multicast-routing
```

！将 Switch A 的端口 Gi 0/1 配置为 Route Port，用于连接组播源，并配置组播路由协议

```
SwitchA(config)#interface gigabitEthernet 0/1
SwitchA(config-if-GigabitEthernet 0/1)#no switchport
SwitchA(config-if-GigabitEthernet 0/1)#ip address 10.1.1.2 255.255.255.0
SwitchA(config-if-GigabitEthernet 0/1)#ip pim dense-mode
SwitchA(config-if-GigabitEthernet 0/1)#exit
```

！配置 VLAN 1 的 SVI，并在 SVI 上配置组播路由协议。

```
SwitchA(config)#interface vlan 1
SwitchA(config-if-VLAN 1)#ip address 192.168.1.1 255.255.255.0
SwitchA(config-if-VLAN 1)#ip pim dense-mode
SwitchA(config-if-VLAN 1)#exit
```

！将端口 Gi 0/2 配置为 Trunk Port，用于连接二层组播设备。

```
SwitchA(config)#interface gigabitEthernet 0/2
SwitchA(config-if-GigabitEthernet 0/2)#switchport mode trunk
SwitchA(config-if-GigabitEthernet 0/2)#exit
```

第二步，在二层组播设备上使能 IGMP Snooping，并设置路由连接口。

！在 Switch B 上，全局配置 IGMP Snooping 为 IVGL 模式，并配置 Fa 0/1 为 VLAN 1 的路由连接口。

```
SwitchB(config)#ip igmp snooping ivgl
SwitchB(config)#ip igmp snooping vlan 1 mrouter interface fastEthernet 0/1
```

第三步，配置 Receiver 1、2、3 相应要求。

！将端口 Fa 0/2 配置为 VLAN 1、组地址为 224.1.1.1 的静态成员端口。

```
SwitchB(config)#ip igmp snooping vlan 1 static 224.1.1.1 interface fastEthernet 0/2
```

！定义 IGMP Profile1 仅允许接收组地址为 225.1.1.1~226.1.1.1 的 IP 组播数据流，并应用在端口 Fa 0/3 上。

```
SwitchB(config)#ip igmp profile 1
```

```
SwitchB(config-profile)#permit
SwitchB(config-profile)#range 225.1.1.1 226.1.1.1
SwitchB(config-profile)#exit
SwitchB(config)#interface fastEthernet 0/3
SwitchB(config-if-FastEthernet 0/3)#ip igmp snooping filter 1
SwitchB(config-if-FastEthernet 0/3)#exit
```

！配置端口 Fa 0/4 仅允许最多动态加入 100 个组播组。

```
SwitchB(config)#interface fastEthernet 0/4
SwitchB(config-if-FastEthernet 0/4)#ip igmp snooping max-groups 100
SwitchB(config-if-FastEthernet 0/4)#exit
```

第四步，在二层组播设备上配置所有接入端口能够快速离开某 IP 组播组，并配置 IGMP 成员响应报文的抑制功能。

！在 Switch B 上，使能端口快速离开功能。

```
SwitchB(config)#ip igmp snooping fast-leave enable
```

！在 Switch B 上，使能 IGMP Snooping 成员关系报告报文的响应抑制功能。

```
SwitchB(config)#ip igmp snooping suppression enable
```

验证结果

第一步，查看设备的配置信息

！Switch A 的配置

```
SwitchA#show running-config
!
ip multicast-routing
!
interface GigabitEthernet 0/1
 no switchport
 ip pim dense-mode
 no ip proxy-arp
 ip address 10.1.1.2 255.255.255.0
!
interface GigabitEthernet 0/2
 switchport mode trunk
!
interface VLAN 1
 ip pim dense-mode
 no ip proxy-arp
 ip address 192.168.1.1 255.255.255.0
```

！Switch B 的配置

```
SwitchB#show running-config
```

```
!
interface FastEthernet 0/3
 ip igmp snooping filter 1
!
interface FastEthernet 0/4
 ip igmp snooping max-group 100
!
ip igmp profile 1
permit
range 225.1.1.1 226.1.1.1
ip igmp snooping ivgl
ip igmp snooping vlan 1 static 224.1.1.1 interface FastEthernet 0/2
ip igmp snooping vlan 1 mrouter interface FastEthernet 0/1
ip igmp snooping fast-leave enable
ip igmp snooping suppression enable
```

第二步，查看 Switch B 的 IGMP Snooping 基本信息

```
SwitchB#show ip igmp snooping
IGMP Snooping running mode: IVGL
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Enable
IGMP Report suppress: Enable
IGMP Globle Querier: Disable
IGMP Preview: Disable
IGMP Preveiw group aging time : 60(Seconds)
Dynamic Mroute Aging Time : 300(Seconds)
Tunnel IGMP Packet:  Disable


vlan 1
-------------
IGMP Snooping state: Enabled
Multicast router learning mode: pim-dvmrp
IGMPv2 fast leave: Disabled
IGMP VLAN querier: Disable
```

第三步，查看 Switch B 的路由连接口信息

```
SwitchB#show ip igmp snooping mrouter
Multicast Switching Mroute Port
  D: DYNAMIC
  S: STATIC
(*, *, 1):
  VLAN(1)  1 MROUTES:
    FastEthernet 0/1 (S)
```

第四步，查看 IGMP Snooping 的接口配置情况

```
SwitchB#show ip igmp snooping interfaces
Interface         Filter profile number  max-group
----------------  ---------------------  ---------
FastEthernet 0/3  1                      4294967294
FastEthernet 0/4  0                      100
```

第五步，通过 Source 发送组地址为 224.2.2.2 的 IP 组播数据流，在 Switch B 的端口 Fa 0/2 上点播组播，查看 Switch A 的组成员状况以及 Switch B 的 GDA 表如下：

！查看 Switch A

```
SwitchA#show ip igmp groups
IGMP Connected Group Membership
Group Address  Interface  Uptime    Expires   Last Reporter
224.2.2.2      VLAN 1     00:00:51  00:03:55  0.0.0.0
```

！查看 Switch B

```
SwitchB#show ip igmp snooping gda-table
Multicast Switching Cache Table
  D: DYNAMIC
  S: STATIC
  M: MROUTE
(*,224.1.1.1, 1):
  VLAN(1) 2 OPORTS:
    FastEthernet 0/1(M)
    FastEthernet 0/2(S)
(*,224.2.2.2, 1):
  VLAN(1) 2 OPORTS:
    FastEthernet 0/1(M)
    FastEthernet 0/2(D)
```

2 组播转发控制

2.1 配置组播不间断转发参数

命令	作用
Ruijie(config)# **msf nsf convergence-time** *time*	配置等待组播协议收敛所需的最大时间，取值范围 0~3600 秒，缺省值 70 秒。
Ruijie(config)# **msf nsf leak** *time*	配置组播报文泄漏的时间，取值范围 0~3600 秒，缺省值 80 秒。

正常运行状态下，SSP 将硬件组播转发表实时同步到从管理板。 当管理板切换后，原从管理板组播控制面配置命令加载，组播协议（如 PIM-SM，IGMP Snooping 等）重新收敛。组播不间断转发（Non-Stop Forwarding）功能保证在组播协议重新收敛的这段时间内，组播数据流的转发不间断。

当设置的协议收敛时间超时后，在协议收敛时间内未被更新过的所有组播转发表项将被删除。

从管理板成为主管理板后，组播协议重新收敛，需要组播数据流触发。所以切换后，虽然硬件转发表已经存在。但是 SSP 仍然需要将组播流限速的送往 CPU，这个时间持续的长短可以通过配置 leak time 来控制。

2.2 监视与维护

命令	作用
Ruijie# **debug msf api**	查看 IPv4 多层组播转发提供的 API 接口被调用的处理过程。
Ruijie# **debug msf event**	查看 IPv4 下关于多层组播转发事件的处理过程。
Ruijie# **debug msf forwarding**	查看 IPv4 多层组播报文转发的处理过程。
Ruijie# **debug msf mfc**	查看 IPv4 下对多层组播转发表项的操作过程。
Ruijie# **debug msf ssp**	查看 IPv4 多层组播转发操作底层硬件的处理过程。
Ruijie# **show msf msc**	查看 IPv4 多层组播转发表。
Ruijie# **show msf nsf**	查看 IPv4 组播不间断转配置。

配置指南-安全

本分册介绍安全配置指南相关内容，包括以下章节：

1. AAA
2. SSH 终端服务
3. 基于端口的流控制
4. CPU 保护
5. DoS 保护
6. DHCP Snooping
7. 动态 ARP 检测
8. IP Source Guard
9. 防网关 ARP 欺骗
10. NFPP

1 AAA

访问控制是用来控制哪些人可以访问网络服务器以及用户在网络上可以访问哪些服务的。身份认证、授权和记账（AAA）是进行访问控制的一种主要的安全机制。

☑ NBS200F 系列产品不支持 RADIUS、802.1x 和 TACACS+功能

1.1 AAA基本原理

AAA 是 Authentication Authorization and Accounting（认证、授权和记账）的简称，它提供了对认证、授权和记账功能进行配置的一致性框架，锐捷网络设备产品支持使用 AAA。

AAA 以模块方式提供以下服务：

认证：验证用户是否可获得访问权，可选择使用 RADIUS 协议、TACACS+协议或 Local（本地）等。身份认证是在允许用户访问网络和网络服务之前对其身份进行识别的一种方法。

授权：授权用户可使用哪些服务。AAA 授权通过定义一系列的属性对来实现，这些属性对描述了用户被授权执行的操作。这些属性对可以存放在网络设备上，也可以远程存放在安全服务器上。

记账：记录用户使用网络资源的情况。当 AAA 记账被启用时，网络设备便开始以统计记录的方式向安全服务器发送用户使用网络资源的情况。每个记账记录都是以属性对的方式组成，并存放在安全服务器上，这些记录可以通过专门软件进行读取分析，从而实现对用户使用网络资源的情况进行记账、统计、跟踪。

尽管 AAA 是最主要的访问控制方法，锐捷产品同时也提供了在 AAA 范围之外的简单控制访问，如本地用户名身份认证、线路密码身份认证等。不同之处在于它们提供对网络保护程度不一样，AAA 提供更高级别的安全保护。

使用 AAA 有以下优点：

- 灵活性和可控制性强
- 可扩充性
- 标准化认证
- 多个备用系统

1.1.1 AAA基本原理

AAA 可以对单个用户（线路）或单个服务器动态配置身份认证、授权以及记账类型。通过创建方法列表来定义身份认证、记账、授权类型，然后将这些方法列表应用于特定的服务或接口。

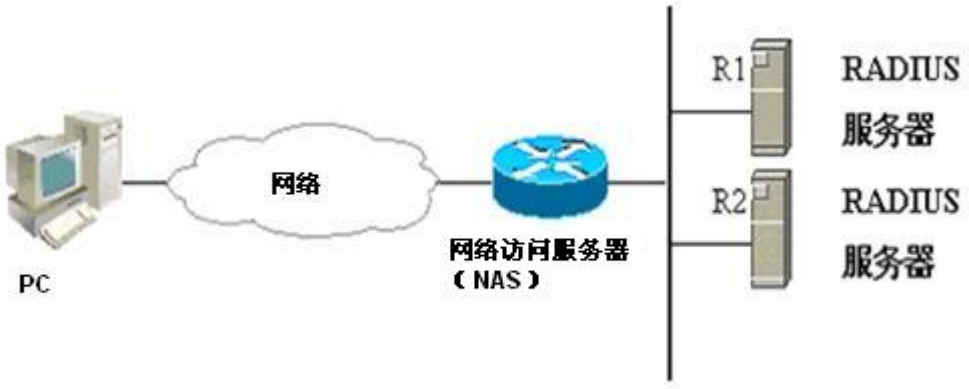
1.1.2 方法列表

由于对用户进行认证、授权和记账可以使用不同的安全方法，您需要使用方法列表定义一个使用不同方法对用户进行认证、授权和记账的前后顺序。方法列表可以定义一个或多个安全协议，这样可以确保在第一个方法失败时，有备用系统可用。锐

捷产品使用方法列表中列出的第一个方法时，如果该方法无应答，则选择方法列表中的下一个方法。这个过程一直持续下去，直到与列出的某种安全方法成功地实现通信或用完方法列表。如果用完方法列表而还没有成功实现通信，则该安全功能宣告失败。

只有在前一种方法没有应答的情况下，锐捷产品才会尝试下一种方法。例如在身份认证过程中，某种方法拒绝了用户访问，则身份认证过程结束，不再尝试其他的身份认证方法。

图 1-1



上图说明了一个典型的 AAA 网络配置，包含两台安全服务器：R1 和 R2 是 RADIUS 服务器。以及一台网络访问服务器（NAS），可以作为 RADIUS 客户端。

假设系统管理员已定义了一个方法列表，在这个列表中，R1 首先被用来获取身份信息，然后是 R2，最后是访问服务器上的本地用户名数据库。如果一个远程 PC 用户试图拨号进入网络，网络访问服务器首先向 R1 查询身份认证信息，假如用户通过了 R1 的身份认证，R1 将向网络访问服务器发出一个 ACCEPT 应答，这样用户即获准访问网络。如果 R1 返回的是 REJECT 应答，则拒绝用户访问网络，断开连接。如果 R1 无应答，网络访问服务器就将它看作 TIMEOUT，并向 R2 查询身份认证信息。这个过程会一直在余下的指定方法中持续下去，直到用户通过身份认证、被拒绝或对话被中止。如果所有的方法返回 TIMEOUT，则认证失败，连接将被断开。

REJECT 应答不同于 TIMEOUT 应答。REJECT 意味着用户不符合可用身份认证数据库中包含的标准，从而未能通过身份认证，访问请求被拒绝。TIMEOUT 则意味着安全服务器对身份认证查询未作应答，当检测到一个 TIMEOUT 时，AAA 选择身份认证方法列表中定义的下一个身份认证方法将继续进行身份认证过程。

在本文中，与 AAA 安全服务器相关的认证、授权和记账配置，均以 RADIUS 为例，而与 TACACS+有关的内容请另外参考“配置 TACACS+”。

1.2 配置AAA基本步骤

首先您必须决定要采用哪种安全解决方案，而且需要评估特定网络中的潜在安全风险，并选择适当的手段来阻止未经授权的访问。我们建议，在可能的情况下，尽量使用 AAA 确保网络安全。

1.2.1 AAA配置过程概述

如果理解了 AAA 运作的基本过程，配置 AAA 就相对简单了。在锐捷网络设备上配置 AAA 地步骤如下：

- 启用 AAA，使用全局配置模式命令 **aaa new-model**。
- 如果决定使用安全服务器，请配置安全协议的参数，如 RADIUS。
- 定义身份认证方法列表，使用 **aaa authentication** 命令。
- 如有需要，可将该方法列表应用于特定的接口或线路。

在应用特定方法列表时，如果没有明确指定使用命名的方法列表，则使用默认的身份认证方法列表进行身份认证。因此，如果不准备使用默认的身份认证方法列表，则需要指定特定的方法列表。

对于本章中使用的命令的完整描述，请参见命令手册“AAA 命令”。

1.2.2 启用AAA

要使用 AAA 安全特性，必须首先启用 AAA。

要启用 AAA，在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)#**aaa new-model**	启用 AAA。

1.2.3 停用AAA

要停用 AAA，在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)#**no aaa new-model**	停用 AAA。

1.2.4 后续的配置过程

启用 AAA 以后，便可以配置与安全方案相关的其他部分，下表说明了可能要完成的配置任务以及相关内容所在的章节。

AAA 访问控制安全解决方案方法。

配置任务	步骤	所在章节
配置 RADIUS 安全协议参数	2	配置 RADIUS
配置本地登录(Login)身份认证	3	配置认证
定义认证方法列表	4	配置认证
将方法列表应用于特定的接口或线路	5	配置认证

如果使用 AAA 实现身份认证，请参考“配置认证”中的相关部分。

1.3 配置认证

身份认证是在允许用户使用网络资源以前对其进行识别，在大多数情况下，身份认证是通过 AAA 安全特性来实现的。我们建议，在可能的情况下，最好使用 AAA 来实现身份认证。

1.3.1 定义AAA认证方法列表

要配置 AAA 身份认证，首先得定义一个身份认证方法的命名列表，然后各个应用使用已定义列表进行认证。方法列表定义了身份认证的类型和执行顺序。对于已定义的身份认证方法，必须有特定的应用才会被执行。默认方法列表是唯一的例外。所有应用在未进行配置时使用默认方法列表。

方法列表仅是定义将要被依次查询的、并用于认证用户身份的一系列安全方法。方法列表使您能够指定一个或多个用于身份认证的安全协议，这样确保在第一种方法失败的情况下，可以使用身份认证备份系统。我司产品使用第一种方法认证用户的身份，如果该方法无应答，将选择方法列表中的下一种方法。 这个过程一直持续下去，直到与列出的某种身份认证方法成功地实现通信或用完方法列表。如果用完方法列表而还没有成功实现通信，则身份认证宣告失败。

只有在前一种方法没有应答的情况下，锐捷产品才会尝试下一种方法。如果在身份认证过程中，某种方法拒绝了用户访问，则身份认证过程结束，不再尝试其他的身份认证方法。

1.3.2 方法列表举例

在典型 AAA 网络配置图中，它包含 2 个服务器：R1 和 R2 是 RADIUS 服务器。假设系统管理员已选定一个安全解决方案，NAS 认证采用一个身份认证方法对 Telnet 连接进行身份认证：首先使用 R1 对用户进行认证，如果无应答，则使用 R2 进行认证；如果 R1、R2 都没有应答，则身份认证由访问服务器的本地数据库完成，要配置以上身份认证列表，执行以下命令：

命令	作用
Ruijie(config)#**aaa authentication login default group radius local**	配置一个默认身份认证方法列表，其中“default”是方法列表的名称。这个方法列表中包含的协议，按照它们将被查询的顺序排列在名称之后。为所有应用的默认方法列表。

如果系统管理员希望该方法列表仅应用于一个特定的 Login 连接，必须创建一个命名方法列表，然后将它应用于特定的连接。下面的例子说明了如何将身份认证方法列表仅应用于线路 2：

命令	作用
Ruijie(config)#**aaa new-model**	打开 AAA 开关。
Ruijie(config)#**aaa authentication login** *test* **group radius local**	在全局配置模式下，定义了一个名为“test”的方法列表。
Ruijie(config-line)#**line vty** *2*	进入 VTY 线路 2 配置模式。
Ruijie(config-line)#**login authentication** *test*	在 line 配置模式下，将名为“test”方法列表应用于线路。

当远程 PC 用户试图 Telnet 访问网络设备(NAS)，NAS 首先向 R1 查询身份认证信息，假如用户通过了 R1 的身份认证，R1 将向 NAS 发出一个 ACCEPT 应答，这样用户即获准访问网络。如果 R1 返回的是 REJECT 应答，则拒绝用户访问网络，断开连接。如果 R1 无应答，NAS 就将它看作 TIMEOUT，并向 R2 查询身份认证信息。这个过程会一直在余下的指定方法中持续下去，直到用户通过身份认证、被拒绝或对话被中止。如果所有的服务器(R1、R2)返回 TIMEOUT，则认证由 NAS 本地数据库完成。

REJECT 应答不同于 TIMEOUT 应答。REJECT 意味着用户不符合可用的身份认证数据库中包含的标准，从而未能通过身份认证，访问请求被拒绝。TIMEOUT 则意味着安全服务器对身份认证查询未作应答，当验证 TIMEOUT 时，AAA 选择认证方法列表中定义的下一个认证方法继续进行认证过程。

1.3.3 认证类型

我司产品目前支持以下认证类型：

- Login（登录）认证
- Enable 认证
- PPP 认证
- DOT1X（IEEE802.1x）认证

其中 Login 认证针对的是用户终端登录到 NAS 上的命令行界面（CLI），在登录时进行身份认证；Enable 认证针对的是用户终端登录到 NAS 上的 CLI 界面以后，提升 CLI 执行权限时进行认证；PPP 认证针对 PPP 拨号用户进行身份认证；DOT1X 认证针对 IEEE802.1x 接入用户进行身份认证。

1.3.4 配置AAA身份认证的通用步骤

要配置 AAA 身份认证，都必须执行以下任务：

- 使用 **aaa new-model** 全局配置命令启用 AAA。
- 如果要使用安全服务器，必须配置安全协议参数，如 RADIUS 和 TACACS+。具体的配置请参见“配置 RADIUS”和“配置 TACACS+”。
- 使用 **aaa authentication** 命令定义身份认证方法列表。
- 如果可能，将方法列表应用于某个特定的接口或线路。

我司产品 DOT1X 认证目前不支持 TACACS+。

1.3.5 配置AAA Login认证

本节将具体介绍如何配置锐捷产品所支持的 AAA Login（登录）身份认证方法：

只有在全局配置模式下执行 **aaa new-model** 命令启用 AAA，AAA 安全特性才能进行配置使用（下同）。关于更详细的内容，请参见“AAA 概述”。

在很多情况下，用户需要通过 Telnet 访问网络访问服务器(NAS)，一旦建立了这种连接，就可以远程配置 NAS，为了防止网络未经授权的访问，要对用户进行身份认证。

AAA 安全服务使网络设备对各种基于线路的 Login（登录）身份认证变得容易。不论您要决定使用哪种 Login 认证方法，只要使用 **aaa authentication login** 命令定义一个或多个身份认证方法列表，并应用于您需要进行 Login 认证的特定线路就可以了。

要配置 AAA Login 认证，在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)#**aaa new-model**	启用 AAA。

Ruijie(config)#**aaa authentication login** {**default** | *list-name*} *method1* [*method2*...]	定义一个认证方法列表，如果需要定义多个方法列表，重复执行该命令。
Ruijie(config)# **line vty** *line-num*	进入您需要应用 AAA 身份认证的线路。
Ruijie(config-line)#**login authentication** {**default** | *list-name*}	将方法列表应用线路。

关键字 *list-name* 用来命名创建身份认证方法列表，可以是任何字符串；关键字 *method* 指的是认证实际算法。仅当前面的方法返回 ERROR（无应答），才使用后面的其他认证方法；如果前面的方法返回 FAIL(失败)，则不使用其他认证方法。为了使认证最后能成功返回，即使所有指定方法都没有应答，可以在命令行中将 **none** 指定为最后一个认证方法。

例如，在下例中，即使 RADIUS 服务器超时(TIMEOUT)，仍然能够通过身份认证：**aaa authentication login default group radius none**。

> 由于关键字 **none** 使得拨号的任何用户在安全服务器没有应答情况下都能通过身份认证，所以仅将它作为备用的身份认证方法。我们建议：一般情况下，不要使用 **none** 身份认证，在特殊情况下，如所有可能的拨号用户都是可信任的，而且用户的工作不允许有由于系统故障造成的耽搁，可以在安全服务器无应答的情况下，将 **none** 作为最后一种可选的身份认证方法，建议在 **none** 认证方法前加上本地身份认证方法。

关键字	描述
local	使用本地用户名数据库进行身份认证。
none	不进行身份认证。
group radius	使用 RADIUS 服务器组进行身份认证。
group tacacs+	使用 TACACS+服务器组进行身份认证。

上表列出了锐捷产品支持的 AAA Login 认证方法。

使用本地数据库进行 Login 认证

要配置使用本地数据库进行 Login 认证时，首先需要配置本地数据库，锐捷产品支持基于本地数据库的身份认证，建立用户名身份认证，请在全局配置模式下，根据具体需求执行以下命令：

命令	作用
Ruijie(config)#**username name** [**password** *password*]	建立本地用户，设置口令。

定义本地 Login 认证方法列表并应用认证方法列表，可使用以下命令：

命令	作用
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**aaa new-model**	打开 AAA 开关。
Ruijie(config)#**aaa authentication login** {**default** | *list-name*} **local**	定义使用本地认证方法。
Ruijie(config)#**end**	退出到特权模式。
Ruijie#**show aaa method-list**	确认配置的方法列表。
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**line** vty *line-num*	进入线路配置模式。
Ruijie(config-line)#**login authentication** {**default** | *list-name*}	应用方法列表。
Ruijie(config-line)#**end**	退出到特权模式。
Ruijie#**show running-config**	确认配置。

使用 RADIUS 进行 Login 认证

要配置用 RADIUS 服务器进行 Login 认证，首先要配置 RADIUS 服务器。配置 RADIUS 服务器，请在全局配置模式下，根据具体需求执行以下命令：

命令	作用
Ruijie(config)#**aaa new-model**	打开 AAA 开关。
Ruijie(config)#**radius-server host** *ip-address* [**auth-port** *port*] [**acct-port** *port*]	配置 RADIUS 服务器。
Ruijie#**show radius server**	显示 RADIUS 服务器。

配置好 RADIUS 服务器后，在配置 RADIUS 进行身份认证以前，请确保与 RADIUS 安全服务器之间已经成功进行了通信，有关 RADIUS 服务器配置的信息，请参见“配置 RADIUS”。

现在就可以配置基于 RADIUS 服务器的方法列表了，在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)#**aaa new-model**	打开 AAA 开关。
Ruijie(config)#**aaa authentication login** {**default** | *list-name*} **group radius**	定义使用 RADIUS 认证方法。
Ruijie(config)#**end**	退出到特权模式。
Ruijie#**show aaa method-list**	确认配置的方法列表。
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**line vty** *line-num*	进入线路配置模式。
Ruijie(config-line)#**login authentication** {**default** | *list-name*}	应用方法列表。
Ruijie(config-line)#**end**	退出到特权模式。
Ruijie#**show running-config**	确认配置。

1.3.6 配置AAA Enable认证

本节将具体介绍如何配置锐捷产品所支持的 AAA Enable 认证方法：

在很多情况下，用户需要通过 Telnet 等方法访问网络访问服务器(NAS)，在进行了身份认证以后，就可以进入命令行界面（CLI），此时会被赋予一个初始的执行 CLI 命令的权限（0~15 级）。不同的级别，可以执行的命令是不同的，可以使用 **show privilege** 命令查看当前的级别。关于更详细的内容，请参见“使用命令行界面”。

如果登录到命令行界面后，由于初始权限过低，不能执行某些命令，则可以使用 enable 命令来提升权限。为了防止网络未经授权的访问，在提升权限的时候，需要进行身份认证，即 Enable 认证。

要配置 AAA Enable 认证，在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)#**aaa new-model**	启用 AAA。
Ruijie(config)#**aaa authentication enable default** *method1* [*method2*...]	定义一个 Enable 认证方法列表，可以指定采用的认证方法，例如 RADIUS。

Enable 认证方法列表全局只能定义一个，因此不需要定义方法列表的名称；关键字 *method* 指的是认证实际方法。仅当前面的方法返回 ERROR（无应答），才使用后面的其他身份方法；如果前面的方法返回 FAIL(失败)，则不使用其他认证方法。为了使认证最后能成功返回，即使所有指定方法都没有应答，可以在命令行中将 **none** 指定为最后一个认证方法。

Enable 认证方法配置以后立即自动生效。此后，在特权模式下执行 **enable** 命令的时候，如果要切换的级别比当前级别要高，则会提示进行认证。如果要切换的级别小于或等于当前级别，则直接切换，不需要进行认证。

> 如果进入 CLI 界面的时候经过了 Login 身份认证（**none** 方法除外），将记录当前使用的用户名。此时，进行 Enable 认证的时候，将不再提示输入用户名，直接使用与 Login 认证相同的用户名进行认证，注意输入的口令要与之匹配。
>
> 如果进入 CLI 界面的时候没有进行 Login 认证，或在 Login 认证的时候使用了 **none** 方法，将不会记录用户名信息。此时，如果进行 Enable 认证，将会要求重新输入用户名。这个用户名信息不会被记录，每次进行 Enable 认证都要重新输入。

一些认证方法，在认证时可以绑定安全级别。这样，在认证过程中，除了根据安全协议返回的成功或失败的应答外，还需要检查绑定的安全级别。如果服务协议能绑定安全级别，则需要在认证时校验绑定的级别。如果绑定的级别大于或等于要切换的目的级别，则 Enable 认证成功，并切换到目的级别；而如果绑定的级别小于要切换的目的级别，则 Enable 认证失败，提示失败信息，维持当前的级别不变。如果服务协议不能绑定安全级别，则不校验绑定的级别，就可以切换到目的级别。

目前能够绑定安全级别的认证方法只有 RADIUS 和本地认证，因此只对这两种方法进行检查，如果采用其他认证方法则不进行检查。

使用本地数据库进行 Enable 认证

使用本地数据库进行 Enable 认证时，可以在设置本地用户时，为用户设置权限级别。如果没有设置，则默认的用户级别为 1 级。要配置使用本地数据库进行 Enable 身份认证时，首先需要配置本地数据库，并为用户设置权限级别，请在全局配置模式下，根据具体需求执行以下命令：

命令	作用
Ruijie(config)#**username** *name* [**password** *password*]	建立本地用户，设置口令。
Ruijie(config)#**username** *name* [**privilege** *level*]	为用户设置权限级别（可选）。

定义本地 Enable 认证方法列表，可使用以下命令：

命令	作用
Ruijie(config)#**aaa new-model**	打开 AAA 开关。
Ruijie(config)#**aaa authentication enable default local**	定义使用本地认证方法。
Ruijie#**show aaa method-list**	确认配置的方法列表。

使用 RADIUS 进行 Enable 认证

标准的 RADIUS 服务器可以通过 Service-Type 属性（标准属性号为 6）绑定权限，可以指定 1 级或 15 级权限；锐捷扩展的 RADIUS 服务器（例如 SAM）可以设置设备管理员的级别（私有属性号为 42），可以指定 0~15 级权限。有关 RADIUS 服务器配置的信息，请参见“配置 RADIUS”中的“指定 RADIUS 私有属性类型”章节。

要配置用 RADIUS 认证服务器进行 Enable 认证，首先要配置 RADIUS 服务器，然后再配置基于 RADIUS 服务器的 Enable 方法列表。在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)#**aaa new-model**	打开 AAA 开关。
Ruijie(config)#**aaa authentication enable default group radius**	定义使用 RADIUS 认证方法。
Ruijie#**show aaa method-list**	确认配置的方法列表。

1.3.7 配置PPP用户使用AAA认证

PPP 协议是提供在点到点链路上承载网络层数据包的一种链路层协议。在很多情况下，用户需要通过异步或 ISDN 拨号访问 NAS（网络访问服务器），一旦建立了这种连接，将启动 PPP 协商，为了防止网络未经授权的访问，PPP 在协商过程中要对拨号用户进行身份认证。

本节将具体介绍如何配置我司产品所支持的 AAA PPP 认证方法，要配置 AAA PPP 认证，在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)#a**aa new-model**	启用 AAA。
Ruijie(config)#**aaa authentication ppp** {**default** | *list-name*} *method1* [*method2*...]	定义一个 PPP 认证方法列表，可以指定采用的认证方法，目前支持 RADIUS 和 TACACS+远程认证，以及使用本地数据库进行认证。
Ruijie(config)#**interface** *interface-type interface-number*	进入需要应用 AAA 身份认证的异步或 ISDN 接口。
Ruijie(config-if-*type ID*)#**ppp authentication** {**chap** | **pap**} {**default** | *list-name*}	将身份认证方法列表应用于异步或 ISDN 接口。

PPP 协议更具体的配置方式参见“PPP、MP 协议配置”中相关章节。

1.3.8 配置 802.1x用户使用AAA认证

IEEE802.1x（Port-Based Network Access Control）是一个基于端口的网络存取控制标准，为 LAN 提供点对点式的安全接入，提供一种对连接到局域网设备的用户进行认证的手段。

本节将具体介绍如何配置我司产品所支持的 802.1x 认证方法，要配置 802.1x 认证，在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)#**aaa new-model**	启用 AAA。
Ruijie(config)#**aaa authentication dot1x** {**default** | *list-name*} *method1* [*method2*...]	定义一个 IEEE802.1x 认证方法列表，可以指定采用的认证方法，目前支持 RADIUS 远程认证，以及使用本地数据库进行认证。
Ruijie(config)#**dot1x authentication** *list-name*	802.1x 应用认证方法列表。

IEEE802.1x 协议更具体的配置方式参见“配置 802.1x”。

1.3.9 配置认证示例

下面示例演示如何配置网络设备，使用“RADIUS+本地身份”进行认证。

```
Ruijie(config)# aaa new-model
Ruijie(config)# username Ruijie password starnet
Ruijie(config)# radius-server host 192.168.217.64
Ruijie(config)# radius-server key test
Ruijie(config)# aaa authentication login test group radius local
Ruijie(config)# line vty 0
Ruijie(config-line)# login authentication test
```

```
Ruijie(config-line)# end
Ruijie# show running-config
!
aaa new-model
!
!
aaa authentication login test group radius local
username Ruijie password 0 starnet
!
radius-server host 192.168.217.64
radius-server key 7 093b100133
!
line con 0
line vty 0
login authentication test
line vty 1 4
!
!
```

上面例子中，访问服务器使用 RADIUS 服务器（IP 为 192.168.217.64）对登录的用户进行认证，如果 RADIUS 服务器没有应答，则使用本地数据库进行身份认证。

1.3.10 终端服务应用下认证示例

在终端服务的应用环境下，终端接到设备的异步串口上，再通过 IP 网络连接到网络中心服务器进行业务作业。但是，如果打开了 AAA 功能，则所有的线路都需要进行登录（Login）认证，那么终端需要先通过了设备的登录认证，才能连接到服务器，这样对终端服务的业务产生了影响。我们可以通过配置将两种线路分开，既让使用终端服务的线路不进行登录认证，直接连接服务器；同时连接到本设备的线路又可以使用登录认证来保证设备的安全。即：设置一个终端服务专用的登录认证列表，但认证方法为 none；然后将这个登录认证列表应用在打开终端服务的线路上（其他可以连接到本地的线路不变）；这样该终端就不需要进行本地的登录认证了。配置步骤如下：

```
Ruijie(config)# aaa new-model
Ruijie(config)# username Ruijie password starnet
Ruijie(config)# radius-server host 192.168.217.64
Ruijie(config)# radius-server key test
Ruijie(config)# aaa authentication login test group radius local
Ruijie(config)# aaa authentication login terms none
Ruijie(config)# line tty 1 4
Ruijie(config-line)# login authentication terms
Ruijie(config-line)# exit
Ruijie(config)# line tty 5 16
Ruijie(config-line)# login authentication test
Ruijie(config-line)# exit
Ruijie(config)# line vty 0 4
Ruijie(config-line)# login authentication test
```

```
Ruijie(config-line)# end
Ruijie# show running-config
!
aaa new-model
!
!
aaa authentication login test group radius local
aaa authentication login terms none
username Ruijie password 0 starnet
!
radius-server host 192.168.217.64
radius-server key 7 093b100133
!
line con 0
line aux 0
line tty 1 4
login authentication terms
line tty 5 16
login authentication test
line vty 0 4
login authentication test
!
!
```

上面例子中，访问服务器使用 RADIUS 服务器（IP 为 192.168.217.64）对登录的用户进行认证，如果 RADIUS 服务器没有应答，则使用本地数据库进行身份认证。我们使用 tty 1-4 作为终端服务使用的线路，不需要登录认证，而其他 tty 和 vty 线路需要进行登录认证。

1.4 配置授权

AAA 授权使管理员能够对用户可使用的服务或权限进行控制。启用 AAA 授权服务以后，网络设备通过本地或服务器中的用户配置文件信息对用户的会话进行配置。完成授权以后，该用户只能使用配置文件中允许的服务或只具备许可的权限。

1.4.1 授权类型

锐捷产品目前支持以下 AAA 授权类型：

- Exec 授权
- Command（命令）授权
- Network（网络）授权

其中 Exec 授权针对的是用户终端登录到 NAS 上的 CLI 界面时，授予用户终端的权限级别（分为 0~15 级）；命令授权针对的是用户终端登录到 NAS 上的 CLI 界面以后，针对具体命令的执行授权；而网络授权针对的是授予网络连接上的用户会话可使用的服务。

命令授权功能目前仅 TACACS+协议支持，具体内容请参考“配置 TACACS+”。

1.4.2 授权的准备工作

在配置 AAA 授权以前，必须完成下述任务：

- 启用 AAA 服务。关于如何启用 AAA 服务，请参见“AAA 概述”。
- （可选）配置 AAA 认证。授权一般是在用户通过认证之后进行，但在某些情况下，没有经过认证也可以单独授权。关于 AAA 认证的信息，请参见“配置认证”。
- （可选）配置安全协议参数。如果需要使用安全协议进行授权，需要配置安全协议参数。锐捷产品 Network 授权支持 RADIUS 和 TACACS+协议，Exec 授权支持 RADIUS 和 TACACS+协议，关于 RADIUS 协议的信息，请参见“配置 RADIUS”，关于 TACACS+协议的信息，请参见“配置 TACACS+”。
- （可选）如果需要使用本地授权，则需要使用 **username** 命令定义用户权限。

1.4.3 配置授权列表

要启用 AAA 授权，请在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)#**aaa new-model**	打开 AAA 开关。
Ruijie(config)#**aaa authorization exec** {**default** | *list-name*} *method1* [*method2*|…]	定义 AAA Exec 授权方法。
Ruijie(config)#**aaa authorization network**{default | *list-name*} *method1* [*method2*|…]	定义 AAA Network 授权方法。

1.4.4 配置AAA Exec授权

锐捷产品支持针对登录到网络访问服务器（NAS）的用户终端，授予其执行命令的权限，即 Exec 授权。体现为用户登录到 NAS 的 CLI 界面时（例如通过 Telnet），具备的级别（成功登录后，可以使用 **show privilege** 命令查看）。

不论您要决定使用哪种 Exec 授权方法，只要使用 **aaa authorization exec** 命令定义一个或多个 Exec 授权方法列表，并应用于您需要进行 Exec 授权的特定线路就可以了。

要配置 AAA Exec 授权，在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)#**aaa new-model**	启用 AAA。
Ruijie(config)#**aaa authorization exec** {**default** | *list-name*} *method1* [*method2*...]	定义一个授权方法列表，如果需要定义多个方法列表，重复执行该命令。
Ruijie(config)#**line vty** *line-num*	进入您需要应用 AAA Exec 授权的线路。
Ruijie(config-line)#**authorization exec** {**default** | *list-name*}	将方法列表应用线路。

关键字 *list-name* 用来命名创建授权方法列表，可以是任何字符串；关键字 *method* 指的是授权实际算法。仅当前面的方法返回 ERROR（无应答），才使用后面的其他方法；如果前面的方法返回 FAIL(失败)，则不使用其他授权方法。为了使授权最后能成功返回，即使所有指定方法都没有应答，可以在命令行中将 **none** 指定为最后一个授权方法。

例如，在下例中，即使 RADIUS 服务器超时(TIMEOUT)，仍然能够通过 Exec 授权：aaa authorization exec default group radius none

命令	作用
local	使用本地用户名数据库进行 Exec 授权。
none	不进行 Exec 授权。
group radius	使用 RADIUS 服务器组进行 Exec 授权。
group tacacs+	使用 TACACS+服务器组进行 Exec 授权。

上表列出了锐捷产品支持的 AAA Exec 授权方法。

Exec 授权通常结合 Login 认证一起使用，并可以在同一个线路上同时使用 Login 认证和 Exec 授权。但是要注意，由于授权和认证可以采用不同的方法和不同的服务器，因此对于相同的用户，认证和授权可能有不同的结果。用户登录时，如果 Exec 授权失败，即使已经通过了 Login 认证，也不能进入到 CLI 界面。

使用本地数据库进行 Exec 授权

要配置使用本地数据库进行 Exec 授权时，首先需要配置本地数据库。可以在设置本地用户时，为用户设置权限级别。如果没有设置，则默认的用户级别为 1 级。请在全局配置模式下，根据具体需求执行以下命令：

命令	作用
Ruijie(config)#**username** *name* [**password** *password*]	建立本地用户，设置口令。
Ruijie(config)#**username** *name* [**privilege** *level*]	为用户设置权限级别（可选）。

定义本地 Exec 授权方法列表并应用授权方法列表，可使用以下命令：

命令	作用
Ruijie(config)#**aaa new-model**	打开 AAA 开关。
Ruijie(config)#**aaa authorization exec** {**default** | *list-name*} **local**	定义使用本地认证方法。
Ruijie#**Show aaa method-list**	确认配置的方法列表。
Ruijie(config)#**line vty** *line-num*	进入线路配置模式。
Ruijie(config-line)#**authorization exec** {**default** | *list-name*}	应用方法列表。

使用 RADIUS 进行 Exec 授权

要配置用 RADIUS 服务器进行 Exec 授权，首先要配置 RADIUS 服务器，有关 RADIUS 服务器配置的信息，请参见“RADIUS 配置指导”。

配置好 RADIUS 服务器后，就可以配置基于 RADIUS 服务器的方法列表了，在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)#**aaa new-model**	打开 AAA 开关。
Ruijie(config)#**aaa authorization exec** {**default** | *list-name*} **group radius**	定义使用 RADIUS 认证方法。
Ruijie#**show aaa method-list**	确认配置的方法列表。

Ruijie(config)#**line vty** *line-num*	进入线路配置模式。
Ruijie(config-line)#**authorization exec** {**default** | *list-name*}	应用方法列表。

配置 Exec 授权示例

下例演示如何进行 Exec 授权。我们设置 VTY 线路 0~4 上的用户登录时采用 Login 认证，并且进行 Exec 授权。其中 Login 认证采用本地认证，Exec 授权先采用 RADIUS、如果没有响应可以采用本地授权。远程 RADIUS 服务器地址为 192.168.217.64，共享密钥为 test；本地用户名为 ruijie，口令为 ruijie，绑定级别是 6 级。如下：

```
Ruijie# configure terminal
Ruijie(config)# aaa new-model
Ruijie(config)# radius-server host 192.168.217.64
Ruijie(config)# radius-server key test
Ruijie(config)# username ruijie password ruijie
Ruijie(config)# username ruijie privilege 6
Ruijie(config)# aaa authentication login mlist1 local
Ruijie(config)# aaa authorization exec mlist2 group radius local
Ruijie(config)# line vty 0 4
Ruijie(config-line)# login authentication mlist1
Ruijie(config-line)# authorization exec mlist2
Ruijie(config)# end
Ruijie# show running-config
aaa new-model
!
aaa authorization exec mlist2 group radius local
aaa authentication login mlist1 local
!
username ruijie password ruijie
username ruijie privilege 6
!
radius-server host 192.168.217.64
radius-server key 7 093b100133
!
line con 0
line vty 0 4
 authorization exec mlist2
 login authentication mlist1
!
End
```

1.4.5 配置AAA Network授权

我司产品支持对包括 PPP、SLIP 等网络连接进行 Network（网络）授权，这些网络连接通过 Network 授权，可以获得诸如流量、带宽、超时等服务配置。Network 授权支持通过 RADIUS 和 TACACS+协议进行，服务器下发的授权信息封装在 RADIUS 或 TACACS+属性里，针对不同的网络连接应用，服务器下发的授权信息可能不相同。

目前该配置不支持 802.1X 的 AAA 授权，802.1X 通过另外的命令完成，具体参见“802.1X 配置”。

要配置 AAA Network 授权，在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)#**aaa new-model**	启用 AAA。
Ruijie(config)#**aaa authorization network** {**default** | *list-name*} *method1* [*method2*...]	定义一个授权方法列表，如果需要定义多个方法列表，重复执行该命令。

关键字 *list-name* 用来命名创建授权方法列表，可以是任何字符串；关键字 *method* 指的是授权实际算法。仅当前面的方法返回 ERROR（无应答），才使用后面的其他授权方法；如果前面的方法返回 FAIL(失败)，则不使用其他授权方法。为了使授权最后能成功返回，即使所有指定方法都没有应答，可以在命令行中将 **none** 指定为最后一个授权方法。

使用 RADIUS 进行 Network 授权

要配置用 RADIUS 服务器进行 Network 授权，首先要配置 RADIUS 服务器，有关 RADIUS 服务器配置的信息，请参见“配置 RADIUS”。

配置好 RADIUS 服务器后，就可以配置基于 RADIUS 服务器的方法列表了，在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)#**aaa new-model**	打开 AAA 开关。
Ruijie(config)#**aaa authorization network** {**default** | *list-name*} **group radius**	定义使用 RADIUS 授权方法。

配置 Network 授权示例

下例演示如何进行网络授权。

```
Ruijie# configure terminal
Ruijie(config)# aaa new-model
Ruijie(config)# radius-server host 192.168.217.64
Ruijie(config)# radius-server key test
Ruijie(config)# aaa authorization network test group radius none
Ruijie(config)# end
Ruijie# show running-config
aaa new-model
!
aaa authorization network test group radius none
!
radius-server host 192.168.217.64
```

```
radius-server key 7 093b100133
!
```

1.5 配置记账

AAA 记账功能够跟踪用户使用的服务和网络资源。启用记账功能以后，网络访问服务器或设备实时地以属性对的方式将用户访问网络的情况发送给安全服务器。您可以使用一些分析软件对这些数据进行分析，实现对用户的活动进行计费、审计以及跟踪等功能。

1.5.1 记账类型

锐捷产品目前支持以下记账类型：

- Exec 记账
- Command（命令）记账
- Network（网络）记账

其中 Exec 记账针对的是用户终端登录到 NAS 上的命令行界面（CLI），在登入和登出时分别进行记账；命令记账针对的是用户终端登录到 NAS 上的 CLI 界面以后，记录其具体执行的命令；而网络记账针对的与网络连接上的用户会话有关的信息。

命令记账功能目前仅 TACACS+协议支持，具体内容请参考“配置 TACACS+”。

1.5.2 记账的准备工作

在配置 AAA 记账以前，必须完成以下任务：

- 启用 AAA 安全服务。关于如何启用 AAA 的信息，请参见“AAA 概述”。
- 定义安全协议参数。进行记账，需要配置安全协议参数。锐捷产品 Network 记账支持 RADIUS 和 TACACS+安全协议；Exec 记账支持 RADIUS 和 TACACS+协议；Command 记账仅支持 TACACS+协议。关于 RADIUS 协议的信息，请参见“配置 RADIUS”， 关于 TACACS+协议的信息，请参见“配置 TACACS+”。
- （可选）配置 AAA 认证。某些记账需要在用户通过认证之后才进行（例如 Exec 记账），其他情况下，没有经过认证也可以进行记账。关于 AAA 认证的信息，请参见“配置认证”。

1.5.3 配置AAA Exec记账

Exec 记账对于已登录到 NAS 的用户终端，可以记录其进入和退出 CLI 界面的信息。在用户终端登录并进入到 NAS 的 CLI 界面时，会向安全服务器发送一个记账开始（Start）信息，在退出 CLI 界面时，会向服务器发送一个记账结束（Stop）信息。

只有登录到 NAS 的用户终端通过了 Login 认证，才会进行 Exec 记账。如果没有设置 Login 认证，或者认证时候采用了 none 方法，则不会进行 Exec 记账。针对同一个用户终端的登录，登入时如果没有进行过 Start 记账，登出时也就不会进行 Stop 记账。

要配置 AAA Exec 记账，在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)#**aaa new-model**	启用 AAA。
Ruijie(config)#**aaa accounting exec** {**default** | *list-name*} **start-stop** *method1* [*method2*...]	定义一个记账方法列表，如果需要定义多个方法列表，重复执行该命令。
Ruijie(config)#**line vty** *line-num*	进入您需要应用 AAA Exec 记账的线路。
Ruijie(config-line)#**accounting exec** {**default** | *list-name*}	将方法列表应用线路。

关键字 *list-name* 用来命名创建记账方法列表，可以是任何字符串；关键字 *method* 指的是记账实际算法。仅当前面的方法返回 ERROR（无应答），才使用后面的其他记账方法；如果前面的方法返回 FAIL(失败)，则不使用其他记账方法。为了使记账最后能成功返回，即使所有指定方法都没有应答，可以在命令行中将 **none** 指定为最后一个记账方法。

使用关键字 **start-stop**，网络访问服务器在用户开始和结束访问网络服务时都给安全服务器发送记账信息。

使用 RADIUS 进行 Exec 记账

要配置用 RADIUS 服务器进行 Exec 记账，首先要配置 RADIUS 服务器，有关 RADIUS 服务器配置的信息，请参见“配置 RADIUS”。

命令	作用
Ruijie(config)#**aaa new-model**	打开 AAA 开关。
Ruijie(config)#**aaa accounting exec** {**default** | *list-name*} **start-stop group radius**	定义使用 RADIUS 记账方法。
Ruijie(config)#**show aaa method-list**	确认配置的方法列表。
Ruijie(config)#**line vty** *line-num*	进入线路配置模式。
Ruijie(config-line)#**accounting exec** {**default** | *list-name*}	应用方法列表。

配置 Exec 记账示例

下例演示如何进行 Exec 记账。我们设置 VTY 线路 0~4 上的用户登录时采用 Login 认证，并且进行 Exec 记账。其中 Login 认证采用本地认证，Exec 记账采用 RADIUS。远程 RADIUS 服务器地址为 192.168.217.64，共享密钥为 test。本地用户名为 ruijie，口令为 ruijie。如下：

```
Ruijie# config
Ruijie(config)# aaa new-model
Ruijie(config)# radius-server host 192.168.217.64
Ruijie(config)# radius-server key test
Ruijie(config)# username ruijie password ruijie
Ruijie(config)# aaa authentication login auth local
Ruijie(config)# aaa accounting exec acct start-stop group radius
Ruijie(config)# line vty 0 4
Ruijie(config-line)# login authentication auth
Ruijie(config-line)# accounting exec acct
Ruijie(config)# end
Ruijie# show running-config
```

```
!
aaa new-model
!
aaa accounting exec acct start-stop group radius
aaa authentication login auth local
!
username ruijie password ruijie
!
radius-server host 192.168.217.64
radius-server key 7 093b100133
!
line con 0
line vty 0 4
 accounting exec acct
 login authentication auth
!
end
```

1.5.4 配置AAA Network记账

Network（网络）记账提供了关于用户会话的记账信息，包括报文的个数及字节数、IP 地址、用户名等。Network 记账目前只支持 RADIUS 协议。

> RADIUS 记账信息的格式随不同的 RADIUS 安全服务器而变化。记账记录中的内容可能会由于锐捷产品版本的不同而有些变化。

要配置 AAA Network 记账，在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)#**aaa new-model**	启用 AAA。
Ruijie(config)#**aaa accounting network** {**default** | *list-name*} **start-stop** *method1* [*method2*...]	定义一个记账方法列表，如果需要定义多个方法列表，重复执行该命令。

关键字 *list-name* 用来命名创建记账方法列表，可以是任何字符串；关键字 *method* 指的是记账实际算法。仅当前面的方法返回 ERROR（无应答），才使用后面的其他记账方法；如果前面的方法返回 FAIL(失败)，则不使用其他记账方法。为了使记账最后能成功返回，即使所有指定方法都没有应答，可以在命令行中将 **none** 指定为最后一个记账方法。

使用 RADIUS 进行 Network 记账

要配置用 RADIUS 服务器进行 Network 记账，首先要配置 RADIUS 服务器，有关 RADIUS 服务器配置的信息，请参见“配置 RADIUS”。

配置好 RADIUS 服务器后，就可以配置基于 RADIUS 服务器的方法列表了，在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)#**aaa new-model**	打开 AAA 开关。

Ruijie(config)#**aaa accounting network** {**default** | *list-name*} **start-stop group radius**	定义使用 RADIUS 记账方法。

配置 Network 记账示例

以下是使用 RADIUS 进行 Network 记账的一个例子：

```
Ruijie# config
Ruijie(config)# aaa new-model
Ruijie(config)# radius-server host 192.168.217.64
Ruijie(config)# radius-server key test
Ruijie(config)# aaa accounting network acct start-stop group radius
Ruijie(config)# end
Ruijie# show running-config
!
aaa new-model
!
aaa accounting network acct start-stop group radius
!
username Ruijie password 0 starnet
username Ruijie privilege 6
!
radius-server host 192.168.217.64
radius-server key 7 093b100133
```

1.6 监视AAA用户

命令	作用
show aaa user { *id* | **all** }	查看当前 AAA 用户信息。

1.7 配置支持VRF的AAA组

Virtual Private Networks (VPNs)为用户提供了一种安全的方式在 ISP 骨干网上共享带宽。一个 VPN 即是共享路由的站点集。用户站点通过一到多个接口链接到服务提供商网络，VPN 路由表也叫 VPN routing/forwarding (VRF) table，AAA 可以为每个自定义服务器组指定 VRF。

要配置 AAA 组的 VRF，请在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)#**aaa new-model**	打开 AAA 开关。
Ruijie(config)#**aaa group server radius** *gs_name*	配置 RADIUS 服务器组，进入服务器组配置模式。
Ruijie(config-gs-radius)#**ip vrf forwarding** *vrf_name*	为组选择 vrf。

需要产品支持 vrf 功能。

1.8 配置Login的用户认证失败锁定

Login 登录锐捷设备，为了防止 Login 用户破解密码，提供配置命令用于限制用户尝试密码的失败次数；超过尝试失败次数，用户被锁定多长时间不能登录。

要配置 Login 登录参量，请在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)#**aaa new-model**	打开 AAA 开关。
Ruijie(config)#**aaa local authentication attempts** *<1-2147483647>*	配置 login 登录，用户尝试失败次数。
Ruijie(config)#**aaa local authentication lockout-time** *<1-2147483647>*	配置 login 登录，用户尝试超过配置的失败次数，被锁定的时间长度（小时）。
Ruijie#**show aaa user lockout**	显示当前被锁定的用户列表。
Ruijie#**clear aaa local user lockout** {**all** | **user-name** *<word>*}	清除被锁定的用户列表。

默认情况下，Login 尝试失败次数为 3 次，被锁定的时间限制为 15 小时。

1.9 配置基于域名的AAA服务

目前基于域名的 AAA 服务，仅被应用于 IEEE802.1x 认证服务，IEEE802.1x 协议更具体的配置方式参见“配置 802.1x”中相关章节。

1.9.1 概述

在多域环境下，同一台网络访问服务器（NAS）设备可为不同域中的用户提供 AAA 服务，各域中用户的属性（例如用户名及密码、服务类型、权限等）有可能各不相同，因此有必要通过设置域的方法把它们区分开，并为每个域单独配置包括 AAA 服务方法列表（例如使用的 RADIUS）在内的属性集。

本产品支持以下几种的形式的用户名

1) userid@domain-name

2) domain-name\userid

3) userid.domain-name

4) userid

对于第 4 种不带 domain-name 的形式的用户名（即以上第 4 种：userid），认为其域名称为 default，即为默认的域名。

设备基于域名的 AAA 服务基本原理如下：

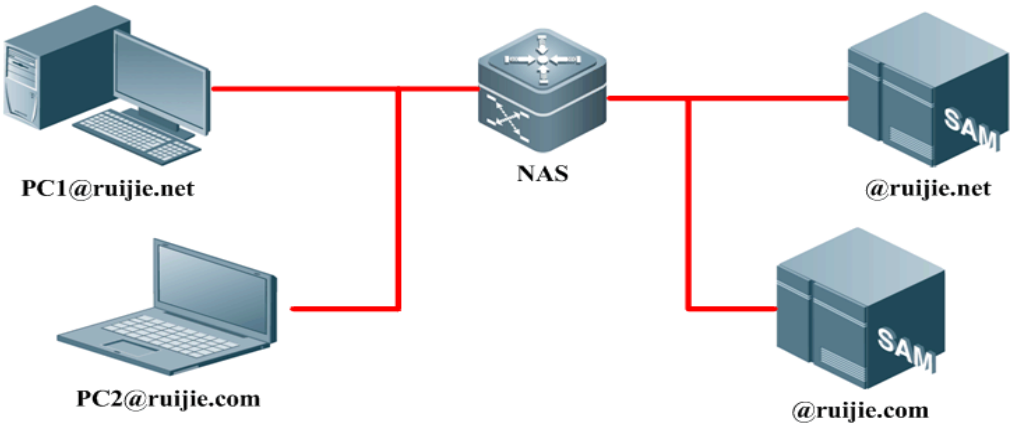
- 解析用户携带的域名称
- 根据域名称查找用户所配置的域
- 根据设备上域配置信息查找相应的 AAA 服务的方法列表名
- 根据方法列表名在系统中查找对应的方法列表

- 使用该方法列表提供 AAA 服务

上述任何一个步骤失败，用户将无法使用申请的 AAA 服务。

以下是典型的多个域环境拓扑图：

图 1-2 典型多个域网络图



1.9.2 基于域名的AAA服务配置

按如下顺序配置基于域名的 AAA 服务：

1) 启用 AAA 服务

2) 定义 AAA 服务的方法列表

3) 启用基于域名的 AAA 服务

4) 创建域

5) 配置域属性集

6) 查看域配置

系统最多支持配置 32 个域。

启用 AAA

命令	作用
Ruijie(config)#**aaa new-model**	打开 AAA 开关。

具体命令说明请参见“启用 AAA” 章节。

定义 AAA 服务的方法列表

命令	作用
Ruijie(config)#**aaa authentication dot1x** {**default** | *list-name*} *method1* [*method2*...]	定义一个 IEEE802.1x 认证方法列表。
Ruijie(config)#**aaa accounting network** {**default** | *list-name*} start-stop *method1* [*method2*...]	定义一个 Network 记账方法列表。
Ruijie(config)#**aaa authorization network** {**default** | *list-name*} *method1* [*method2*...]	定义一个 Network 授权方法列表。

具体说明请参见“配置认证”，“配置记账”和“配置授权”相关章节。

打开基于域名的 AAA 服务开关

命令	作用
Ruijie(config)#**aaa domain enable**	打开基于域名的 AAA 服务开关。

创建域

基于用户名查找匹配的域名时，遵循如下规则：

1) 支持使用单个‘. ‘ 、‘\’ 、‘@ ‘字符区分用户名与域名。

2) 单个 ‘@’字符后跟随的字符串为“域名”。用户名中存在多个‘@’字符时，取最后 1 个‘@’字符后跟随的字符串为域名。如用户名为 a@b@c@d 时，取 a@b@c 为用户名，d 为域。

3) 单个 ‘ \’字符之前的字符串为“域名”。用户名中存在多个‘\’字符时，取第一个‘\’字符之前的字符串为域名。如用户名为 a\b\c\d 时，取 b\c\d 为用户名，a 为域名。

4) 单个 ‘.’ 字符后跟随的字符串为“域名”，用户名中存在多个‘.’字符时，根据预先的配置，取最后 1 个‘.’字符后跟随的字符串为域名。如用户名为 a.b.c.d 时，取 a.b.c 为用户名，d 为域名。

5) 若用户名中同时存在‘. ‘ ‘\’ ‘@ ‘三种字符，匹配域名时，将先进行‘@’字符规则判断，再进行‘\’字符规则判断，最后采用‘.’的判断规则。

命令	作用
Ruijie(config)#**aaa domain** *domain-name*	创建域名为 *domain-name* 的域，并进入域配置模式。

基于域名的 AAA 服务支持最长 64 个字符的域名，不区分大小写。

配置域属性集

在域配置模式下，为已存在的域，选择关联 AAA 服务的方法列表：

命令	作用
Ruijie(config-aaa-domain)#**authentication dot1x** {**default** | *list-name*}	在域配置模式下，选择认证方法列表。
Ruijie(config-aaa-domain)#**accounting network** {**default** | *list-name*}	在域配置模式下，选择记账方法列表。
Ruijie(config-aaa-domain)#**authorization network** {**default** | *list-name*}	在域配置模式下，选择授权方法列表。

配置域状态：

命令	作用
Ruijie(config-aaa-domain)#**state** {**block** | **active**}	在域配置模式下，配置域的状态。

配置是否在用户名中携带域名信息：

命令	作用
Ruijie(config-aaa-domain)#**username-format** {**without-domain** | **with-domain**}	在域配置模式下，配置 NAS 与服务器交互时域中用户名是否携带域名信息。

配置域支持的最大用户数目：

命令	作用
Ruijie(config-aaa-domain)#**access-limit** *num*	在域配置模式下，配置该域能够容纳的最大用户数目，默认情况不限制用户的数目（只对 802.1x 用户生效）。

在域配置模式下，选择 AAA 服务方法列表时，这些方法列表是在进入域配置模式前已经定义；否则在域配置模式下，允许选择 AAA 方法列表名，但提示配置不存在；

缺省域（default）：在基于域名的 AAA 服务开关打开情况下，如果用户没有携带域信息，则使用缺省域。如果用户携带的域在系统中没有配置，则判定为非法用户，不提供 AAA 服务；

域配置模式下，没有选择方法列表的情况下，系统默认分配缺省方法列表；

查看域配置

配置完成基于域名的 AAA 服务后，通过以下命令可以查看相应的配置：

命令	作用
show aaa domain [*domain-name*]	显示当前基于域名的 AAA 服务域信息。

1.9.3 配置基于域名的AAA服务配置注意事项

配置基于域名的 AAA 服务需要注意以下几个方面：

1) 基于域名的 AAA 服务开关打开的情况下，使用域中选择的方法列表。开关关闭的情况下，按照接入协议（例如 802.1X 等）选定的方法列表进行 AAA 服务。例如开关关闭情况下，802.1X 中以命令 **dot1x authentication** *authen-list-name*，**dot1x accounting** *acct-list-name* 中的 *authen-list-name* 及 *acct-list-name* 为认证和记账方法列表名提供 AAA 服务。

2) 基于域名的 AAA 服务开关打开时，默认情况下没有配置缺省域，需要手动配置完成。缺省域的名称为“default”，若配置缺省域后，用户不携带域信息时，使用缺省域进行提供 AAA 服务。若缺省域没有配置，则不携带域信息的用户不能使用 AAA 服务。

3) 如果认证用户携带有域信息，而域没有在设备上配置，不能为该用户提供 AAA 服务。

4) 域选择的 AAA 服务方法列表名称必须和 AAA 服务所定义的方法列表名称必须一致。若不一致，不能够为该域中的用户提供合适的 AAA 服务。

5) 用户所携带的域名称与设备上所配置的域名的匹配采用最准确匹配。例如：设备上配置了 domain.com 和 domain.com.cn 两个域，一个用户的请求信息携带为 aaa@domain.com。则设备认为会判定该用户所属于的域为 domain.com 而不是域 domain.com.cn。

1.9.4 配置基于域名的AAA服务示例

基于域名的 AAA 服务配置示例：

```
Ruijie(config)# aaa new-model
Ruijie(config)# radius-server host 192.168.197.154
Ruijie(config)# radius-server key test
Ruijie(config)# aaa authentication dot1x default group radius
Ruijie(config)# aaa domain domain.com
Ruijie(config-aaa-domain)# authentication dot1x default
Ruijie(config-aaa-domain)# username-format without-domain
```

上面配置后，如果 radius 服务器上有用户 a1，这时使用 802.1x 客户端进行登录认证，使用用户名为 a1@domain.com，再输入正确的密码进行认证就可认证成功。相关域名信息显示如下：

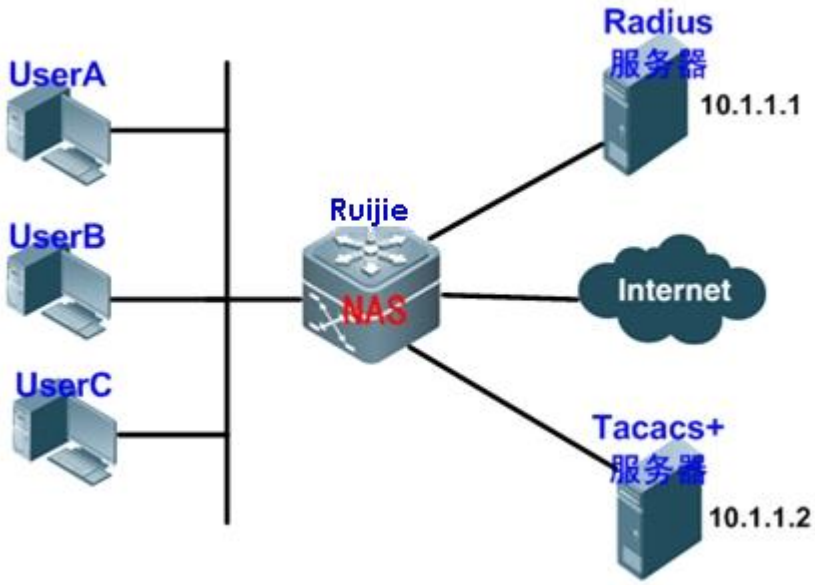
```
Ruijie#show aaa domain domain.com

=============Domain domain.com=============
State: Active
Username format: Without-domain
Access limit: No limit
802.1X Access statistic: 0

Selected method list:
 authentication dot1x default
```

1.10 AAA配置举例

1.10.1 AAA典型应用举例

组网图

图 1-3 AAA 典型应用图



应用需求

在上图的网络应用中，为了更好地对网络访问控制器设备（NAS，以下简称网络设备）进行安全管理，需要满足如下应用要求：

1) 不同的管理人员有各自的用户账号，其用户名和口令不能共享，便于帐号管理和防止泄漏；

2) 对网络设备的访问需经过认证，用户认证的实现方式可以分为本地认证和集中认证，应采用集中认证和本地认证相结合的方式，集中认证为主用、本地认证为备用。在集中认证过程中，要求先通过 Radius 服务器认证，若无响应再转本地认证。

3) 在认证时，不同的用户可以被限制只能访问特定的网络设备；

4) 对用户进行分权限管理：把网络管理用户分为超级用户和普通用户。其中，超级用户对网络设备拥有查看和配置的权限，普通用户对网络设备只拥有特定的查看权限；

5) 服务器端可将用户的认证信息、授权信息和网络行为记录在服务器中，以供日后查看和审计（本例采用 TACACS+进行记账）；

配置要点

通过“应用需求”部分的分析，部署 AAA 可以很好地满足上述需求，其对用户（线路）或服务器动态配置身份认证、授权以及记账类型。通过创建方法列表来定义身份认证、记账、授权类型，然后将这些方法列表应用于特定的服务或接口。具体详见下述“配置步骤”中各个配置点前的说明。

配置步骤

第一步：启用 AAA

！设备启用 AAA 功能

```
Ruijie# configure terminal
```

```
Ruijie(config)# aaa new-model
```

第二步：配置安全服务器

网络中的安全服务器负责认证、授权和记账。服务器上存储管理员的用户信息，服务器上的软件具备事后审计功能（服务器上的软件通过日志可以记录、统计和分析各种信息）。

！ 配置 Radius 服务器信息(设备和 RADIUS 服务器进行通讯的共享密码为 ruijie)

```
Ruijie(config)# radius-server host 10.1.1.1
Ruijie(config)# radius-server key ruijie
```

！ 配置 Tacacs+服务器信息（设备和 TACACS+服务器进行通讯的共享密钥为 redgiant）

```
Ruijie(config)# tacacs-server host 10.1.1.2
Ruijie(config)# tacacs-server key redgiant
```

第三步：配置本地用户

！ 配置口令加密以防止泄漏（配置后本地的口令以及安全服务器的密钥信息等均以简单加密形式保存和显示）

```
Ruijie(config)# service password-encryption
```

！ 配置本地用户数据库（配置用户名和口令信息并绑定用户级别）

```
Ruijie(config)# username bank privilege 10 password yinhang
Ruijie(config)# username super privilege 15 password star
Ruijie(config)# username normal privilege 2 password normal
Ruijie(config)# username test privilege 1 password test
```

！ 配置本地 enable 口令，用于本地 enable 认证

```
Ruijie(config)# enable secret w
```

！ 配置线路登陆口令（在 AAA 模式打开的情况下，终端线路上的登陆口令不起作用。配置这个口令的一般目的，是为了防止关闭 AAA 模式的情况下，终端因没有配置口令而无法登陆成功）

```
Ruijie(config)# line vty 0 15
Ruijie(config-line)# password w
```

！ 配置线路用户级别（如果未打开 Exec 授权，或者该线路未应用任何 Exec 授权方法列表并且不存在默认的 Exec 授权方法列表，该级别将被使用）

```
Ruijie(config)# line vty 0 15
Ruijie(config-line)# privilege level 10
```

第四步：配置认证

■ Login 认证

网络设备上配置 Login 认证，Login 认证可以控制用户是否能访问。定义认证方法列表，首先是 Radius 认证方法，然后是 Local 方法，在远程认证没有响应的情况下转本地认证。

！ 配置 login 认证方法列表（按 Radius、Local 的次序），然后应用到相应线路。

```
Ruijie(config)# aaa authentication login hello group radius local
```

```
Ruijie(config)# line vty 0 15
Ruijie(config-line)# login authentication hello
```

为了防止用户在 Login 认证的时候，使用穷举法破解密码，AAA 可以限制用户 Login 尝试次数，在 Login 失败达到一定次数时，用户将被锁定一段时间不能登录（默认情况下，login 尝试失败次数为 3 次，被锁定的时间限制为 15 小时）。

！ 配置失败次数为 2 次，锁定时间 10 小时

```
Ruijie(config)# aaa local authentication attempts 2
Ruijie(config)# aaa local authentication lockout-time 10
```

■ Enable 认证

网络设备上配置 Enable 认证，用户切换权限级别需要进行认证。这样，如果普通用户想通过 enable 命令切换到超级用户的权限，还需要进行一次认证过程。配置时，首先是 Radius 认证方法，远程认证没有响应的情况下转本地 Enable 认证方法。Enable 认证只能配置默认的方法列表，配置以后，会自动被应用。

！配置 enable 认证方法列表（按 Radius、Tacacs+、Local 的次序）

```
Ruijie(config)# aaa authentication enable default group radius local
```

配置授权

■ Exec 授权

网络设备上配置 Exec 授权，通过授予不同的用户级别控制其执行命令的权限。例如 15 级是超级用户，14 级是配置用户，2 级是普通用户。配置时，首先配置远程 Exec 授权，远程授权没有响应转本地授权。

！ 配置 exec 授权方法列表（按 Tacacs+、Local 的次序），然后应用到线路

```
Ruijie(config)# aaa authorization exec shouquan group tacacs+ local
Ruijie(config)# line vty 0 15
Ruijie(config-line)# authorization exec shouquan
```

！ 控制台线路若要配置进行 Exec 授权（控制台线路默认不进行 Exec 授权），配置如下：

```
Ruijie(config)# aaa authorization console
```

■ Command 授权

网络设备上配置 Command 授权，对于关键命令的执行权限只授予部分管理人员。命令授权是根据命令本身的级别，而不是用户当前的级别。例如 configure terminal 命令是 2 级的，即用户级别如果小于 2 级的，在设备 CLI 界面上将无法看见这条命令，自然也无法执行。如果将 2 级命令配置了 Command 授权，则即使当前是执行命令的是超级用户，也要通过了 Command 授权过程才能执行该命令。该授权不支持 Radius 协议。

！配置 command 授权方法列表（按 Tacacs+、Local 的次序），然后应用到线路

```
Ruijie(config)# aaa authorization commands 2 abc group tacacs+ local
Ruijie(config)# line vty 0 15
Ruijie(config-line)# authorization commands 2 abc
```

配置记账

■ Exec 记账

网络设备上配置 Exec 记账，这样设备将用户的登陆和退出信息发送到服务器，以备查看和统计，以及事后审计。

！ 配置 exec 记账方法列表（使用 TACACS+服务器记账），默认应用到所有线路

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

■ Command 记账

网络设备可以配置 Command 记账，设备将用户执行过的某一级别的命令发送到服务器，以备查看和统计，以及事后审计。

！配置 command 记账方法列表（只支持 tacacs+），默认应用到所有线路。

```
Ruijie(config)# aaa accounting commands 2 default start-stop group tacacs+
```

配置验证

第一步，可通过 show running-config 命令来查看当前配置信息的正确性：

```
Ruijie# show running-config
......
!
aaa new-model
aaa local authentication attempts 2
aaa local authentication lockout-time 10
aaa authorization exec shouquan group tacacs+ local
aaa authorization commands 2 abc group tacacs+
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 2 default start-stop group tacacs+
aaa authentication login hello group radius local
aaa authentication enable default group radius local
!
username bank password 7 09361c1c2f041c4d
username bank privilege 10
username super password 7 093c011335
username super privilege 15
username normal password 7 09211a002a041e
username normal privilege 2
username test password 7 093b100133
service password-encryption
!
tacacs-server key 7 072c062b121b260b06
tacacs-server host 10.1.1.2
radius-server host 10.1.1.1
radius-server key 7 072c16261f1b22
enable secret 5 $1$2MjW$xr1t0s1Euvt76xs2
!
line con 0
```

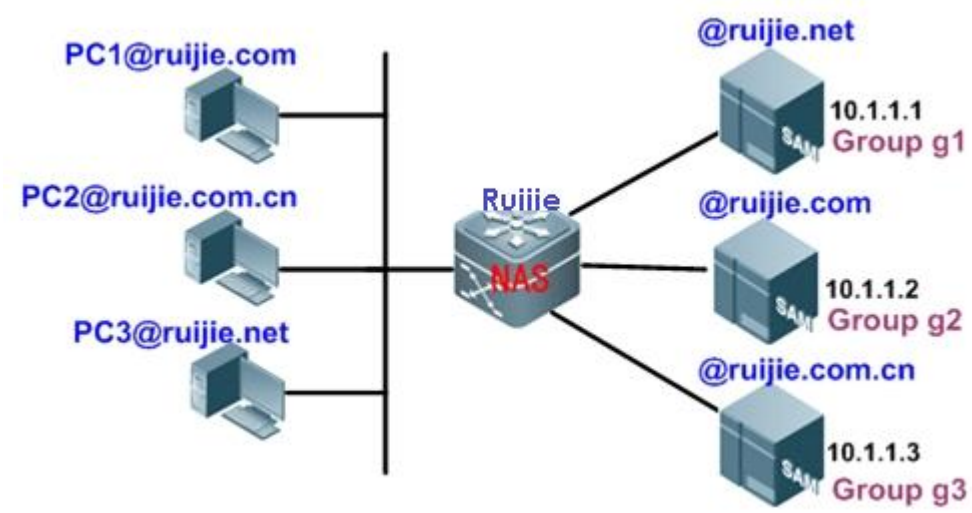
```
line vty 0 4
 authorization exec shouquan
 authorization commands 2 abc
 privilege level 10
 login authentication hello
 password 7 0938
line vty 5 15
 authorization exec shouquan
 authorization commands 2 abc
 privilege level 10
 login authentication hello
 password 7 005d
!
end
```

第二步，在实际应用中，可通过 **show aaa user** { *id* | **all** }命令来查看当前登录的 AAA 用户信息（此处显示省略说明）。

1.10.2 AAA多域认证应用举例

组网图

图 1-4 AAA 多域认证应用图



应用需求

通过配置网络访问控制器设备（NAS，以下简称网络设备）实现基于域名的 AAA 服务，包括认证、授权、记账功能：

- 使用 802.1x 客户端进行登录认证，使用用户名为 PC1@ruijie.com 或 PC2@ruijie.com.cn 或 PC3@ruijie,.net，再输入正确的密码进行认证就可认证成功。
- 对用户进行分权限管理：把网络管理用户分为超级用户和普通用户。其中，超级用户对网络设备拥有查看和配置的权限，普通用户对网络设备只拥有特定的查看权限；

■ 认证服务器端可将用户的认证信息、授权信息和网络行为记录在服务器中，以供日后查看和审计；

配置要点

通过配置基于域名的 AAA 服务，可以满足上述需求，具体说明见下述每项配置步骤前的说明。

本用例以 802.1x 客户端为例，因此网络设备必须支持 802.1x 客户端接入，若不支持则本用例不适用。

配置步骤

启用 AAA

```
Ruijie# configure terminal
Ruijie(config)# aaa new-model
```

配置安全服务器

网络中的安全服务器负责认证、授权和记账。服务器上存储管理员的用户信息，服务器上的软件具备事后审计功能（服务器上的软件通过日志可以记录、统计和分析各种信息）。

！ 配置 Radius 服务器组信息,并配置设备和 Radius 服务器进行通讯的共享密码为 ruijie

```
Ruijie(config)# aaa group server radius g1
Ruijie(config-gs-radius)# server 10.1.1.1
Ruijie(config-gs-radius)# exit
Ruijie(config)# aaa group server radius g2
Ruijie(config-gs-radius)# server 10.1.1.2
Ruijie(config-gs-radius)# exit
Ruijie(config)# aaa group server radius g3
Ruijie(config-gs-radius)# server 10.1.1.3
Ruijie(config-gs-radius)# exit
Ruijie(config)# radius-server key ruijie
```

配置本地用户

！ 配置口令加密以防止泄漏（配置后本地的口令以及安全服务器的密钥信息等均以简单加密形式保存和显示）

```
Ruijie(config)# service password-encryption
```

！ 配置本地用户数据库（配置用户名和口令信息并绑定用户级别）

```
Ruijie(config)# username bank privilege 10 password yinhang
Ruijie(config)# username super privilege 15 password star
Ruijie(config)# username normal privilege 2 password normal
Ruijie(config)# username test privilege 1 password test
```

！ 配置本地 enable 口令，用于本地 enable 认证

```
Ruijie(config)# enable secret w
```

定义 AAA 服务的方法列表

！ 配置 dot1x 认证

```
Ruijie(config)# aaa authentication dot1x renzheng group radius local
```

！ 配置 network 授权

```
Ruijie(config)# aaa authorization network shouquan group radius
```

！ 配置 network 记账

```
Ruijie(config)# aaa accounting network jizhang start-stop group radius
```

打开基于域名的 AAA 服务开关

```
Ruijie(config)# aaa domain enable
```

创建域并配置域属性集

！ 创建域

```
Ruijie(config)# aaa domain ruijie.com
```

！ 关联 AAA 服务的方法列表

```
Ruijie(config-aaa-domain)# authentication dot1x renzheng
Ruijie(config-aaa-domain)# authorization network shouquan
Ruijie(config-aaa-domain)# accounting network jizhang
```

！配置域状态

```
Ruijie(config-aaa-domain)# state active
```

！配置在用户名中不携带域名信息

```
Ruijie(config-aaa-domain)# username-format without-domain
!
Ruijie(config)# aaa authentication dot1x renzheng group g2
Ruijie(config)# aaa authorization network shouquan group g2
!
Ruijie(config)# aaa accounting network jizhang start-stop group g2
!
```

同理，域名为 ruijie.com.cn 和 ruijie.net 的配置方法与上述相同（此处不再赘述）。

配置验证

第一步，可通过 show running-config 命令来查看当前配置信息的正确性（以域名为 `ruijie.com` 为例）：

```
Ruijie# show running-config
......
!
aaa new-model
aaa domain enable
!
aaa domain ruijie.com
 authentication dot1x renzheng
 accounting network jizhang
 authorization network shouquan
 username-format without-domain
!
!
aaa group server radius g1
 server 10.1.1.1
!
aaa group server radius g2
 server 10.1.1.2
!
aaa group server radius g3
 server 10.1.1.3
!
!
aaa accounting network jizhang start-stop group g2
aaa authorization network shouquan group g2
aaa authentication dot1x renzheng group g2
!
no service password-encryption
!
radius-server key ruijie
!
```

第二步，显示当前基于域名的 AAA 服务域信息：

```
Ruijie#show aaa domain

=============Domain ruijie.com=============
State: Active
Username format: Without-domain
Access limit: No limit
802.1X Access statistic: 0

Selected method list:
 authentication dot1x renzheng
 authorization network shouquan
 accounting network jizhang
```

2 SSH 终端服务

2.1 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 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）

2.2 SSH配置

2.2.1 缺省的SSH配置

项目	缺省值
SSH 服务端状态	关闭
SSH 版本	兼容模式（支持版本 1 和 2）
SSH 用户认证超时时间	120s
SSH 用户重认证次数	3 次

2.2.2 用户认证配置

- 基于 SSH 连接安全性的考虑，禁止使用无认证方式登录。因此在用户登录认证时，所使用的登录认证方式必须设置密码；（Telnet 可以设置无认证登录）
- 每次输入的用户名(Username)与密码(Password)长度必须大于零。如果当前认证方式不需要用户名时，用户名可以任意输入，但是输入长度必须大于零。

2.2.3 打开SSH Server

缺省情况下，SSH Server 处于关闭状态。打开 SSH Server，需要在全局配置模式下，执行 **enable service ssh-server** 命令，同时需要生成 SSH 密钥，使 SSH Server 的状态成为 ENABLE。

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **enable service ssh-server**	打开 SSH Server
Ruijie(config)# **crypto key generate** {**rsa**|**dsa**}	生成密钥

- 删除密钥时，不存在命令**[no] crypto key generate**；而是通过命令 **crypto key zeroize** 命令删除密钥。
- SSH 模块不支持热备，因此在支持管理板热备份的产品中，管理板切换动作发生后，若新的主板上没有 SSH 密钥文件，则必须通过命令 **crypto key generate** 重新生成密钥后方可使用 SSH。

2.2.4 关闭SSH Server

关闭 SSH Server，需要在全局配置模式下，执行 **no enable service ssh-server** 命令，使 SSH Server 的状态成为 DISABLE。

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **no enable service ssh-server**	关闭 SSH Server

2.2.5 配置SSH server支持版本

缺省情况下，SSH Server 兼容版本 1 和 2。使用以下命令配置 SSH 使用版本。

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **ip ssh version** {**1**|**2**}	配置 SSH 支持的版本
Ruijie(config)# **no ip ssh version**	恢复 SSH 为缺省配置，支持 SSHv1 与 SSHv2；

2.2.6 配置SSH用户认证超时时间

缺省情况下，SSH Server 的用户认证超时时间为 120 秒。使用以下命令配置 SSH 的用户认证超时时间。

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **ip ssh time-out** *time*	配置 SSH 的超时时间（范围 1-120sec）
Ruijie(config)# **no ip ssh time-out**	恢复 SSH 的缺省用户认证超时时间为 120 秒；

2.2.7 配置SSH重认证次数

该配置命令用来设置 SSH 用户请求连接的认证重试次数，防止恶意猜测等非法行为。缺省情况下，SSH Server 的重认证次数为 3 次，即可以允许用户尝试三次输入用户名与密码进行认证尝试。使用以下命令配置 SSH 的重认证次数。

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **ip ssh authentication-retries** *retry times*	配置 SSH 的重认证次数（范围 0-5）
Ruijie(config)# **no ip ssh authentication-retries**	恢复 SSH 的重认证次数为 3 次

上述命令具体配置请参见[SSH 命令参考手册]。

2.2.8 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
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **ip ssh peer** *test* **public-key rsa flash**:*rsa.pub*	设置用户 *test* 关联的 RSA 公钥文件
Ruijie(config)# **ip ssh peer** *test* **public-key dsa flash**:*dsa.pub*	设置用户 *test* 关联的 DSA 公钥文件

上述命令具体配置请参见《SSH 命令》手册。

2.2.9 配置SCP服务功能

在网络设备上打开 SCP 服务器功能，用户可以直接对网络设备上的文件进行下载，以及将本地文件上传至网络设备，同时所有交互数据以密文形式进行传输，具有认证和安全性等特性。

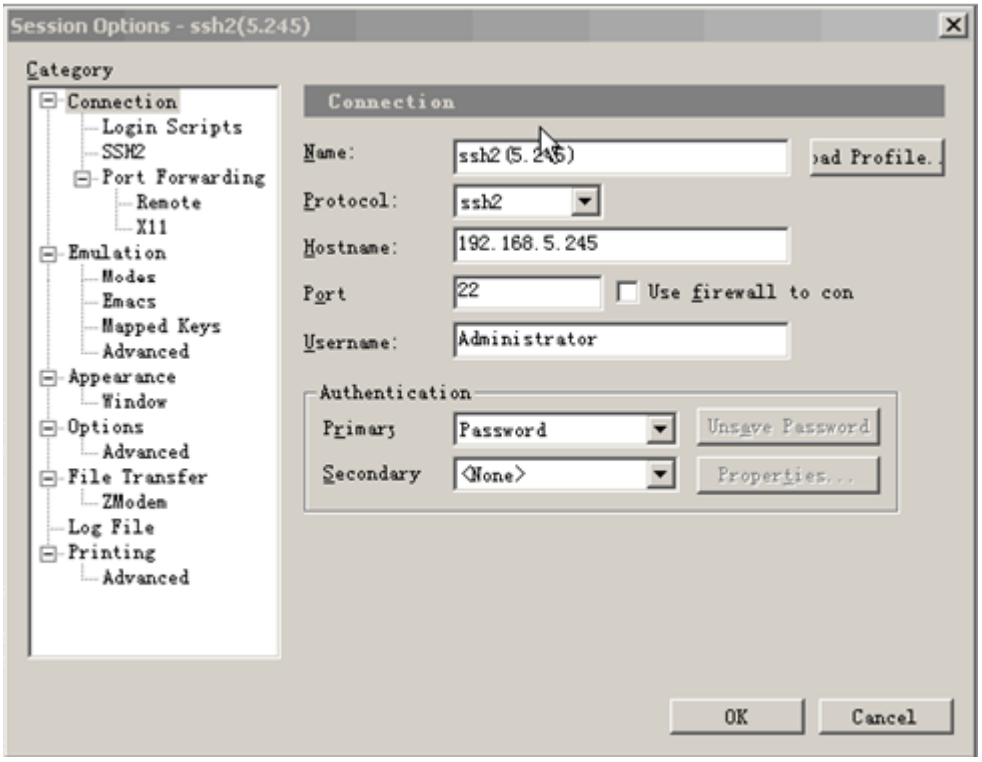
命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)#**ip scp server enable**	开启 SCP 服务器功能
Ruijie(config)# **no ip scp server enable**	关闭 SCP 服务器功能

上述命令具体配置请参见《SSH 命令》手册。

2.3 使用SSH进行设备管理

您可以使用 SSH 对设备进行管理，前提是必须打开 SSH Server 功能，默认情况下是关闭该功能的。由于 Windows 自带的 Telnet 组件不支持 SSH，因此必须使用第三方客户端软件，当前兼容性较好的客户端包括：Putty，Linux，SecureCRT。下面以客户端软件 SecureCRT 为例介绍 SSH 客户端的配置，配置界面如下图：

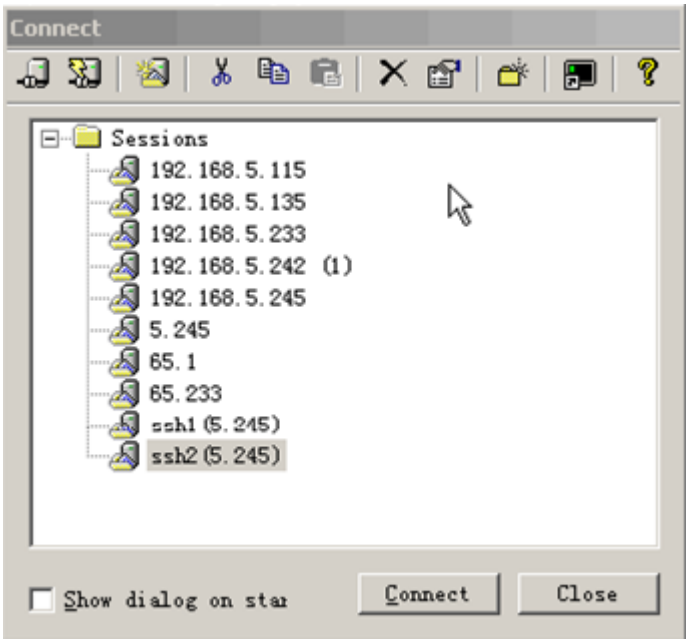
图 6-1



如图使用协议 2 进行登陆，因此在 Protocol 选择 SSH2，Hostname 就是要登陆的主机的 IP 地址，这里为 192.168.5.245，端口为 22 即 SSH 监听的默认端口号，Username 为用户名，当设备只要求密码时，该用户名不会起作用，Authentication 为认证方式，我们只支持用户名密码的认证方式。使用的密码和 Telnet 密码是一致的。

然后点击 OK，进入出现以下的对话框：

图 6-2



点击 Connect，登陆我们刚才配置的主机，如下图：

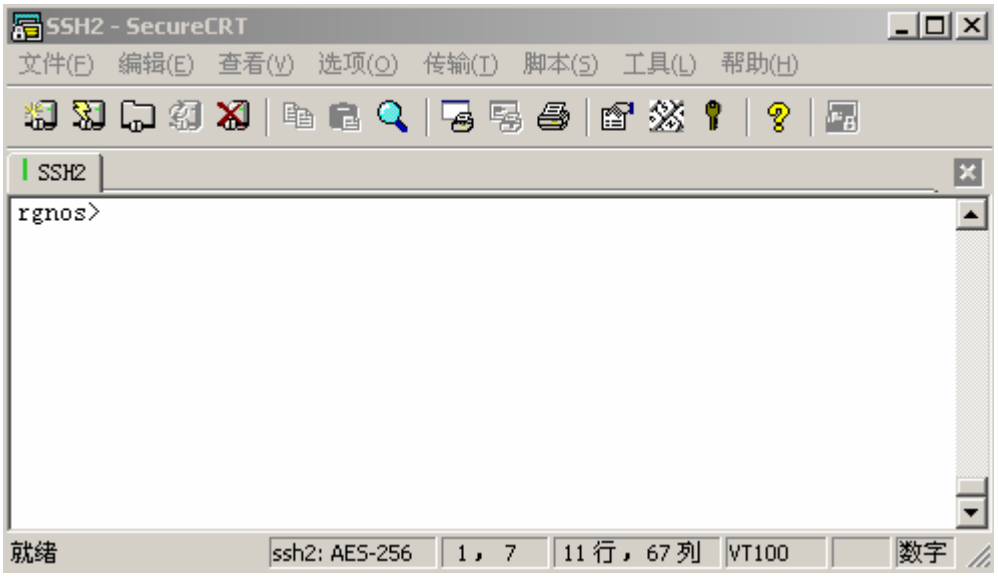
图 6-3

询问正在登陆主机 192.168.5.245 的机器，是否接收服务端发送过来的密钥，选择 Accept & Save（接受而且保存）或者 Accept Once（只接受一次），接着会出现下面的密码认证对话框，如下图：

图 6-4

此时输入 Telnet 登陆密码就可以进入和 Telnet 一样的界面了。如下图显示：

图 6-5



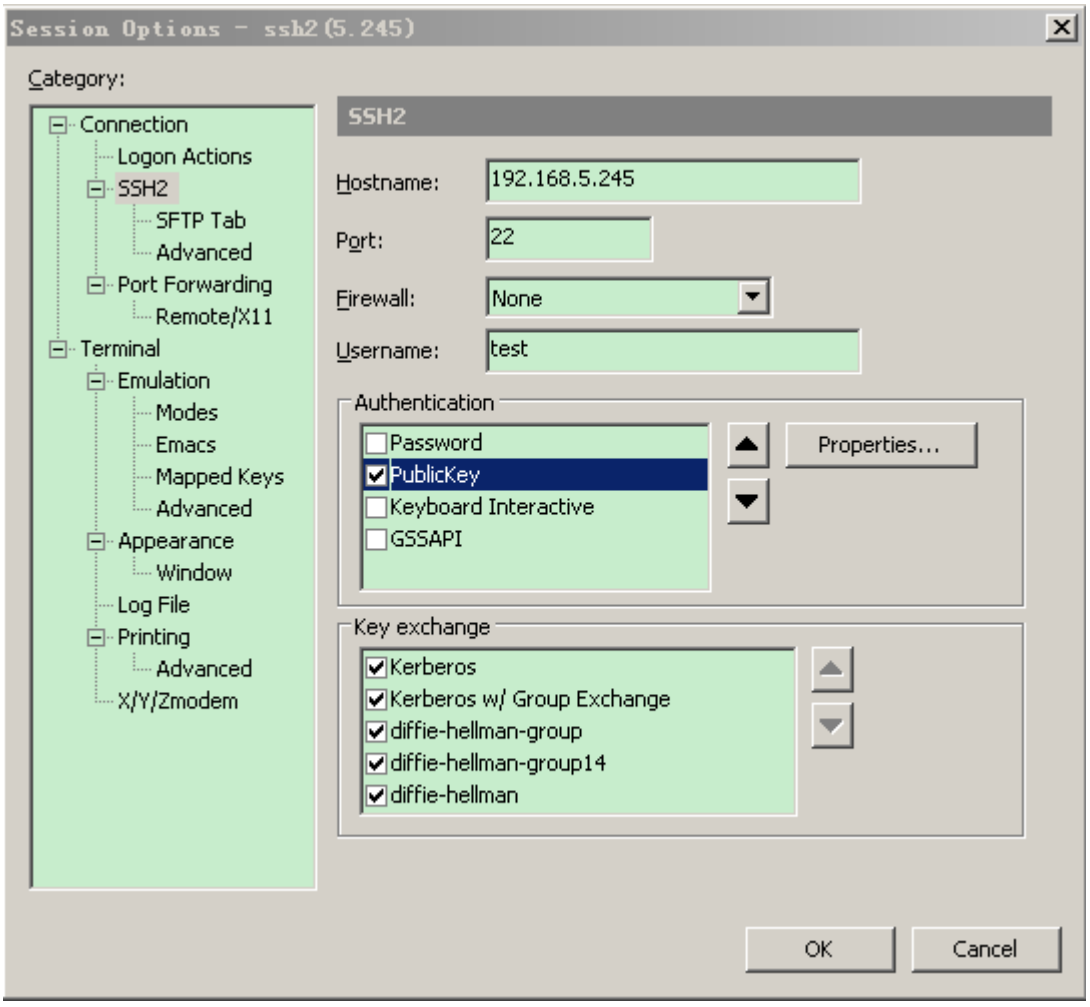
2.4 使用SSH基于公钥的认证

客户端操作

客户端公钥认证方式，首先要在客户端生成一个密钥对（RSA 或 DSA），然后将其中的公钥放置在 SSH 服务器上，然后选择使用 PublicKey 认证方式。下面以以客户端软件 SecureCRT 为例，介绍在客户端生成密钥对的方法。

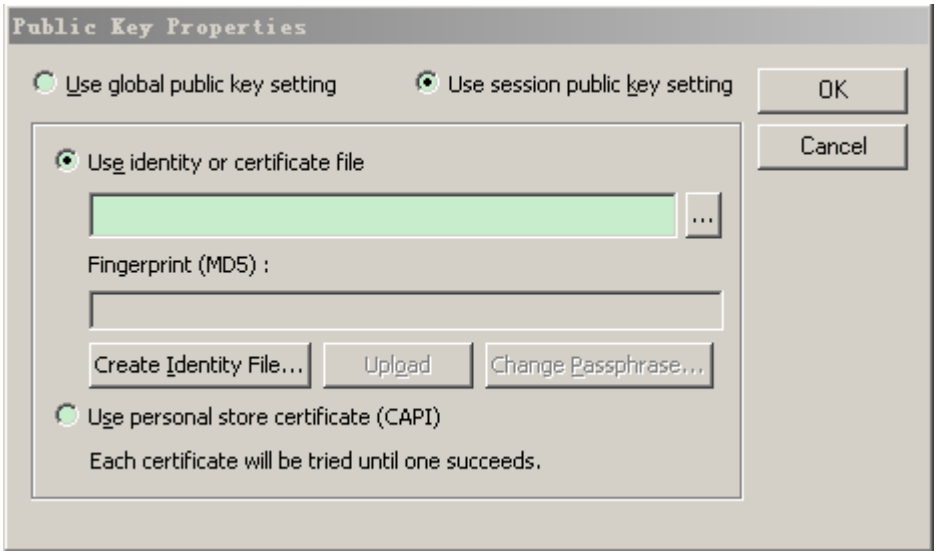
首先，在 Session Option 中 Authentication 选项，选择 PublicKey，然后选择 Properties。如下：

图 6-6



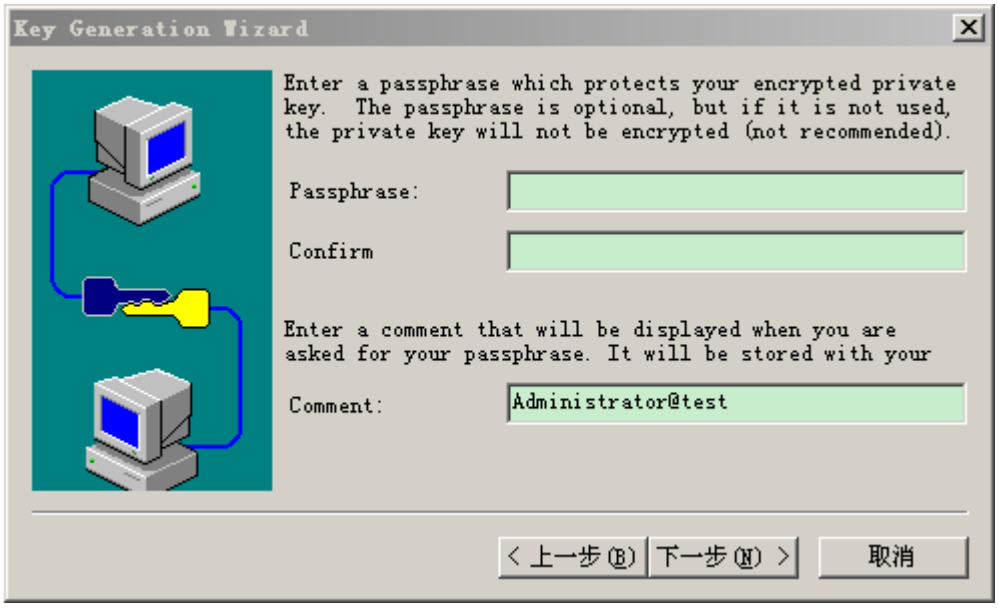
然后点击 Properties...。如果已经生成过密钥对，则可以选择使用的私钥（Use identity or certificate file），注意这个私钥一定要和服务器上的公钥是一对的，否则不能认证通过。如下：

图 6-7



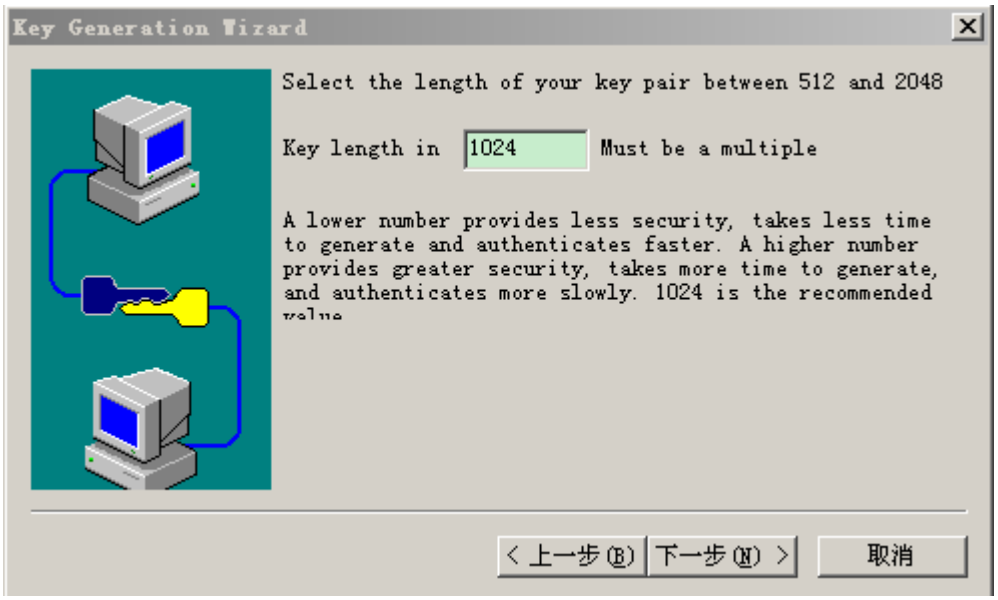
如果没有生成过，可以生成一个新的密钥对（Create Identity File）。在生成密钥中，可以为私钥再设置一个口令（可以为空），如果设置，则每次认证都需要输入这个口令。如下：

图 6-8



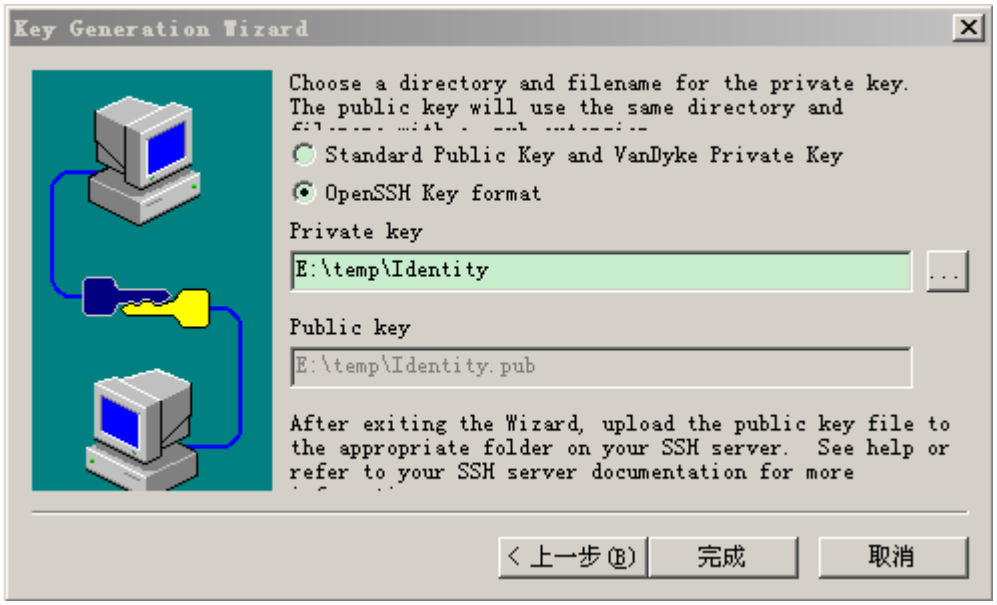
- 生成密钥的时候要不断晃动鼠标，否则速度极慢；
- 一定要选择使用 OpenSSH 格式的密钥文件，否则不能使用。如果使用 Putty 作为客户端，还需要使用 puttygen.exe 工具把私钥转换成 Putty 格式（puttygen.exe 能生成 OpenSSH 格式的密钥对，但是 Putty 却不能直接使用）。放在服务器上的公钥文件不需要转换，还是 OpenSSH 格式。如下：

图 1-9



为了保证 RSA 公钥认证的安全性，生成 RSA 密钥对时，RSA 密钥对的长度必须大于或等于 768 位。

图 6-10



服务器端操作

在客户端生成了密钥以后，SSH 服务器端（即网络设备）需要将客户端的公钥文件复制到 flash 中，并且与 SSH 用户名关联。每个用户可以关联一个 RSA 公钥和一个 DSA 公钥。如下：

```
Ruijie# configure terminal
Ruijie(config)# ip ssh peer test public-key rsa flash:rsa.pub
Ruijie(config)# ip ssh peer test public-key dsa flash:dsa.pub
```

这样，客户端就可以使用公钥认证方式登录网络设备了。

2.5 使用SSH进行文件传输

服务器端操作

SSH 文件传输使用是 SCP 协议（Secure CoPy），客户端要使用 SCP，将文件传输到网络设备上，或者从网络设备上下载文件，首先需要在网络设备上开启 SCP 服务器功能。如下：

```
Ruijie# configure terminal
Ruijie(config)# ip scp server enable
```

这样，客户端就可以使用 SCP 连接服务器并传输文件了。SCP 服务器使用的是 SSH 线程，客户端连接网络设备进行 SCP 传输时候会占用一个 VTY 连接（通过 show user 命令查看的时候，会发现用户类型为 SSH）。

客户端操作

在 Unix 和 Linux 平台上都带有 SCP 命令，以 Ubuntu Linux 为例，介绍 SCP 命令的使用。如下：

```
SCP 命令的语法：
     scp [-1246BCpqrv] [-c cipher] [-F ssh_config] [-i identity_file]
         [-l limit] [-o ssh_option] [-P port] [-S program]
         [[user@]host1:]file1 [...] [[user@]host2:]file2
部分选项说明：
-1 ： 使用 SSH1 版本（若不指定则默认使用 SSH2）；
-2 ： 使用 SSH2 版本（默认）；
-C ： 指定使用压缩传输；
-c ： 指定使用的加密算法；
-r ： 指定传输整个目录；
-i ： 指定使用的密钥文件；
-l ： 限制传输速度（单位 Kbits）；
其他具体的参数可以查看 scp.0 文件。
```

文件传输举例，以在 Ubuntu 7.10 系统上操作为例：

指定用户名是 test，从 IP 为 192.168.195.188 的网络设备上，将 config.text 文件复制到本地的/root 目录下。如下：

```
root@dhcpd:~# scp test@192.168.195.188:/config.text /root/config.text
test@192.168.195.188's password:
config.text                   100% 1506     1.5KB/s   00:00
Read from remote host 192.168.195.188: Connection reset by peer
```

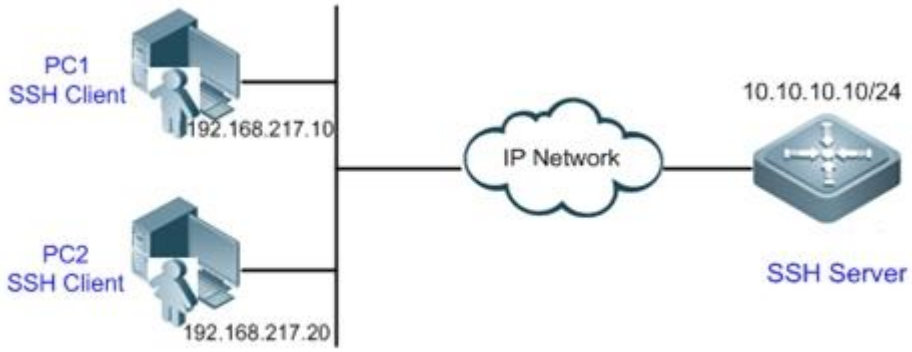
选项大部分与客户端有关，少数是客户端和服务器都需要支持的选项，但我司网络设备上的 SCP 服务器端不支持-d -p –q -r 选项，使用这些选项时候会提示不支持。

下载文件时候，如果没有进行限速（即使用-l 选项），则下载过程中会导致网络设备的 CPU 利用率升高，下载结束以后恢复正常。控制台仍然可以使用，但其他应用态的任务会受到影响。

2.6 SSH典型配置举例

2.6.1 SSH本地线路认证配置举例

图 6-9 SSH 本地线路口令保护组网图



应用需求

如上图所示，为了保证数据信息交换的安全，PC1、PC2 作为 SSH 客户端，采用 SSH 协议登录到打开 SSH Server 的网络设备上。具体要求如下：

- SSH 用户采用的认证方式为线路口令认证。
- 同时启用 0-4 这五条线路，其中线路 0 的登录口令为“passzero”，其余四条线路的登录口令均为“pass”，用户名任意。

配置要点

- SSH Server 的配置要点如下：

1) 全局打开 SSH Server。SSH Server 默认支持 SSH1 和 SSH2 两个版本。

2) 配置密钥。通过该密钥，SSH 服务器将从 SSH 客户端那收到的口令密文进行解密，将解密后的明文同服务器上保存的口令进行比较，并返回认证成功或失败的消息。SSH 1 使用 RSA 密钥；SSH 2 使用 RSA 或者 DSA 密钥。

3) 配置 SSH 服务器 Gi 1/1 接口的 IP 地址。SSH 客户端通过该地址连接 SSH 服务器。SSH 客户端至 SSH 服务器路由可达。

- SSH Client 的设置：

SSH 客户端软件有多种，例如 Putty、Linux、OpenSSH 等，本文中仅以客户端软件 SecureCRT 为例，说明 SSH 客户端的配置方法。具体配置方法请参见“配置步骤”

配置步骤

- SSH Server 的配置

配置 SSH 相关功能之前，请先确保 SSH 用户到 SSH 服务器所在网段的路由可达。接口 IP 配置如拓扑图所示。具体 IP 及路由配置过程此处省略。

第一步，打开 SSH Server 功能

```
Ruijie(config)# enable service ssh-server
```

第二步，生成 RSA 密钥

```
Ruijie(config)#crypto key generate rsa
% You already have RSA keys.
% Do you really want to replace them? [yes/no]:
Choose the size of the key modulus in the range of 360 to 2048 for your
Signature Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]:
% Generating 512 bit RSA1 keys ...[ok]
% Generating 512 bit RSA keys ...[ok]
```

第三步，配置 Gi 1/1 的接口地址，客户端将通过该地址连接 SSH 服务器。

```
Ruijie(config)#interface gigabitEthernet 1/1
Ruijie(config-if-gigabitEthernet 1/1)#ip address 10.10.10.10 255.255.255.0
Ruijie(config-if-gigabitEthernet 1/1)#exit
```

第四步，配置线路登录口令

！配置线路 0 的登录口令为“passzero”

```
Ruijie(config)#line vty 0
Ruijie(config-line)#password passzero
Ruijie(config-line)#privilege level 15
Ruijie(config-line)#exit
```

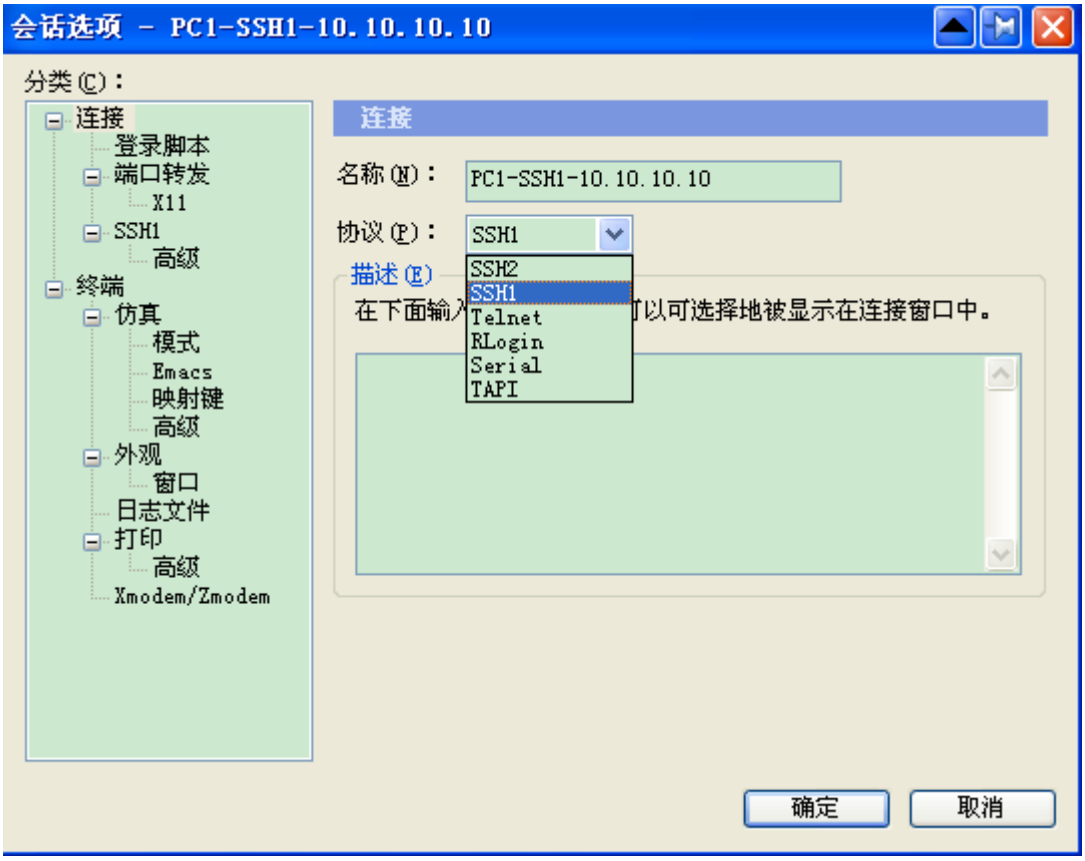
！配置线路 1 - 4 的登录口令为“pass”

```
Ruijie(config)#line vty 1 4
Ruijie(config-line)#password pass
Ruijie(config-line)#privilege level 15
Ruijie(config-line)#exit
```

- SSH Client（PC1/PC2）的配置

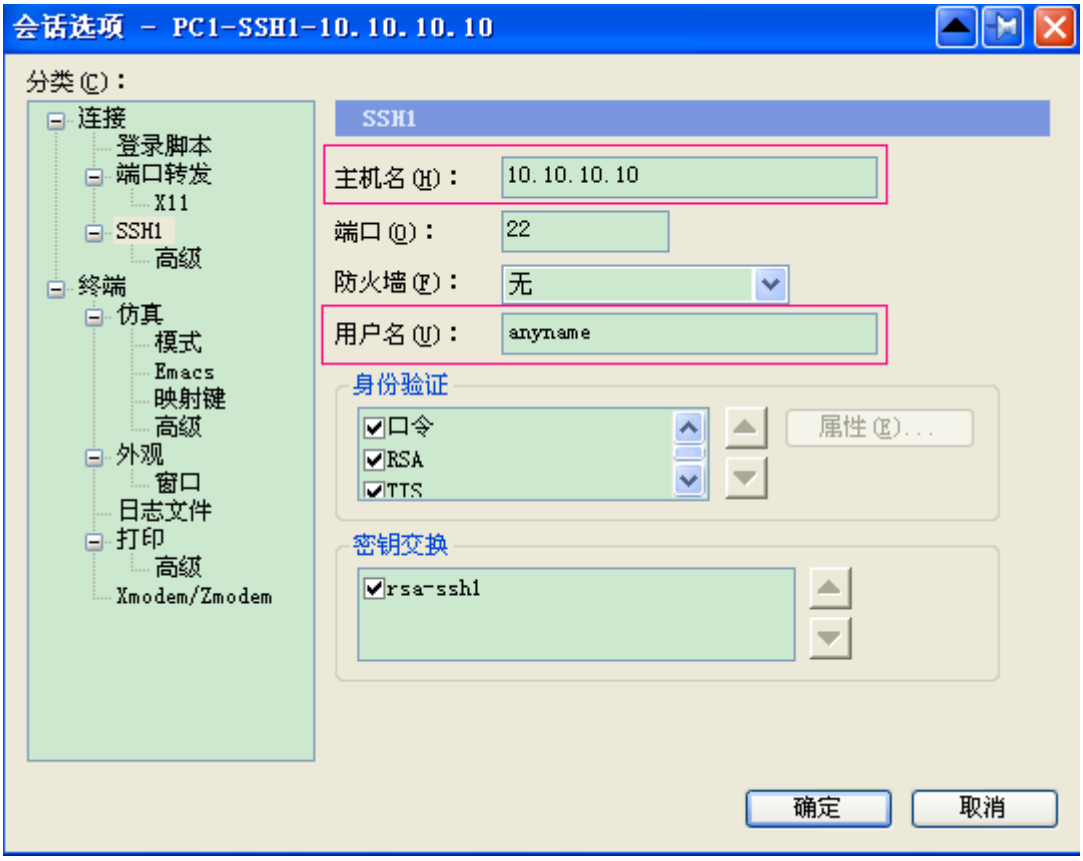
打开 SecureCRT 的连接框，如下图所示，选择使用 SSH1 进行认证登录。会话名称任意（本例名称设置为 PC1-SSH1-10.10.10.10）。

图 6-10



进行 SSH 属性设置。主机名为 SSH 服务器的 IP 地址，本例为 10.10.10.10。由于当前认证方式不需要用户名，此处“用户名”文本框中的用户名信息可以任意输入，但是不能为空（本例用户名设置为 anyname）。

图 6-11



配置验证

- 验证 SSH Server 的配置

第一步，可通过 **show running-config** 命令来查看当前配置信息的正确性：

```
Ruijie#show running-config
Building configuration...
!
enable secret 5 $1$eyy2$xs28FDw4s2q0tx97
enable service ssh-server
!
interface gigabitEthernet 1/1
 ip address 10.10.10.10 255.255.255.0
!
line vty 0
privilege level 15
 login
 password passzero
line vty 1 4
privilege level 15
 login
 password pass
!
```

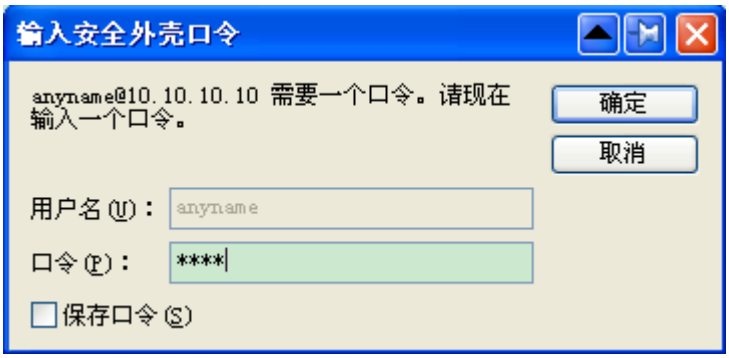
```
end
```

■ 验证 SSH Client 的配置

第一步，建立远程连接。

建立连接，输入正确的口令。线路 0 的登录口令线路 0 的登录口令为“passzero”，其余四条线路的登录口令均为“pass”，即可进入 SSH Server 的操作界面。

图 6-12

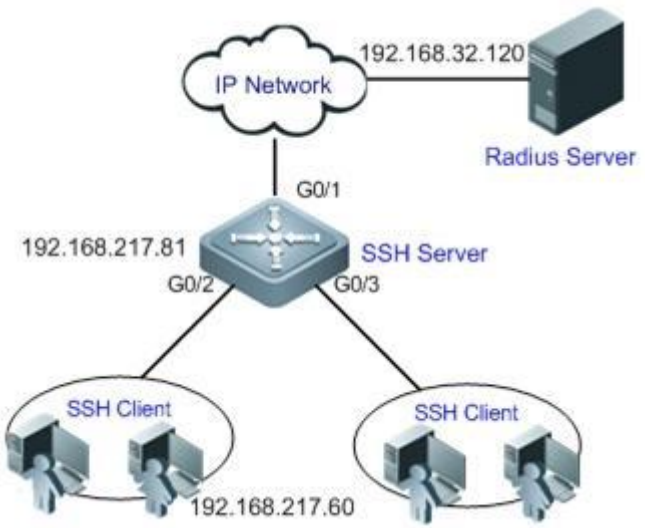


第二步，查看登录用户。

```
Ruijie#show users
    Line         User         Host(s)              Idle       Location
   0 con 0                   idle                 00:03:16
   1 vty 0                   idle                 00:02:16   192.168.217.10
*  2 vty 1                   idle                 00:00:00   192.168.217.20
```

2.6.2 SSH的AAA认证配置举例

图 6-13 SSH AAA 认证组网图



应用需求

如上图所示，为了保证数据信息交换的安全，PC 作为 SSH 客户端，采用 SSH 协议登录到打开 SSH Server 的网络设备上。

为了更好地进行安全管理，SSH 客户端登录用户界面采用 AAA 认证方式；同时出于稳定性方面考虑，在 AAA 认证方法列表中配置两种认证方法：Radius 服务器认证和本地认证。优先选择 Radius 服务器，当 Radius 服务器没有响应时选择本地认证方法。

配置要点

- SSH 客户端到 SSH 服务器端的路由可达，SSH 服务器到 Radius 服务器端的路由可达。
- 在网络设备上进行 SSH Server 相关配置。配置要点在上一个例子中已有描述，不再重复说明。
- 在网络设备上进行 AAA 认证相关配置。AAA 通过创建方法列表来定义身份认证、类型，然后将这些方法列表应用于特定的服务或接口上。具体说明请参见“配置步骤”章节。

配置步骤

SSH 客户端到 SSH 服务器、Radius 服务器间的路由可达。有关路由相关配置本例不具体说明，请参见本手册路由配置部分。

- 在网络设备上配置 SSH 相关功能

第一步，打开 SSH Server 功能

```
Ruijie(config)# enable service ssh-server
```

第二步，生成密钥

！生成 RSA 密钥

```
Ruijie(config)#crypto key generate rsa
% You already have RSA keys.
% Do you really want to replace them? [yes/no]:
Choose the size of the key modulus in the range of 360 to 2048 for your
Signature Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]:
% Generating 512 bit RSA1 keys ...[ok]
% Generating 512 bit RSA keys ...[ok]
```

！生成 DSA 密钥

```
Ruijie(config)#crypto key generate dsa
Choose the size of the key modulus in the range of 360 to 2048 for your
Signature Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]:
% Generating 512 bit DSA keys ...[ok]
```

第三步，配置设备的 IP 地址，客户端将通过该地址连接 SSH 服务器。

```
Ruijie(config)#interface gigabitEthernet 1/1
Ruijie(config-if-gigabitEthernet 1/1)#ip address 192.168.217.81 255.255.255.0
Ruijie(config-if-gigabitEthernet 1/1)#exit
```

■ 在网络设备上配置 AAA 认证相关功能

第一步，设备启用 AAA 功能

```
Ruijie#configure terminal
Ruijie(config)#aaa new-model
```

第二步，配置 Radius 服务器信息(设备和 RADIUS 服务器进行通讯的共享密码为“aaaradius”

```
Ruijie(config)#radius-server host 192.168.32.120
Ruijie(config)#radius-server key aaaradius
```

第三步，配置 AAA 认证方法列表

！配置 login 认证方法列表（按 Radius、Local 的次序），方法列表名为“*method*”

```
Ruijie(config)#aaa authentication login method group radius local
```

第四步，在线路上应用该方法列表

```
Ruijie(config)#line vty 0 4
Ruijie(config-line)#login authentication method
Ruijie(config-line)#exit
```

第五步，配置本地用户数据库

！ 配置本地用户数据库（配置用户名和口令信息并绑定用户级别）

```
Ruijie(config)#username user1 privilege 1 password 111
Ruijie(config)#username user2 privilege 10 password 222
Ruijie(config)#username user3 privilege 15 password 333
```

！ 配置本地 enable 口令，用于本地 enable 认证

```
Ruijie(config)#enable secret w
```

配置验证

第一步，可通过 **show running-config** 命令来查看当前配置信息的正确性：

```
Ruijie#show run
aaa new-model
!
aaa authentication login method group radius local
!
username user1 password 111
username user2 password 222
```

```
username user2 privilege 10
username user3 password 333
username user3 privilege 15
no service password-encryption
!
radius-server host 192.168.32.120
radius-server key aaaradius
enable secret 5 $1$hbgz$ArCsyqty6yyzzp03
enable service ssh-server
!
interface gigabitEthernet 1/1
 no ip proxy-arp
 ip address 192.168.217.81 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 192.168.217.1
!
line con 0
line vty 0 4
 login authentication method
!
end
```

第二步，在 Radius Server 上的设置。本例以 SAM 服务器为例进行说明。

【系统管理】-【设备管理】中，添加设备 IP 地址：192.168.217.81，添加设备 Key：aaaradius

【安全管理】-【设备管理权限】中，设置登录用户的权限。

【安全管理】-【设备管理员】中，添加用户名：user；口令：pass。

第三步，在 PC 机上建立远程 SSH 连接。

SSH 客户端软件设置、建立连接；SSH 客户端的创建方法请参见上例。

输入正确的口令，SSH 用户名为：user；口令为：pass。登录成功。

第四步，查看登录用户。

```
Ruijie#show users
    Line         User         Host(s)              Idle       Location
   0 con 0                    idle                 00:00:31
 * 1 vty 0     user          idle                 00:00:33   192.168.217.60
```

3 基于端口的流控制

3.1 风暴控制

3.1.1 概述

当 LAN 中存在过量的广播、多播或未知名单播数据流时，就会导致网络变慢和报文传输超时机率大大增加。这种情况我们称之为 LAN 风暴。拓朴协议的执行错误或对网络的错误配置都有可能导致风暴的产生。

我们可以分别针对广播、多播和未知名单播数据流进行风暴控制。当交换机端口接收到的广播、多播或未知名单播数据流的速率超过所设定的带宽时，设备将只允许通过所设定带宽的数据流，超出带宽部分的数据流将被丢弃，直到数据流恢复正常，从而避免过量的泛洪数据流进入 LAN 中形成风暴。

3.1.2 配置风暴控制

在接口配置模式下，请使用如下命令配置风暴控制：

命令	作用
Ruijie(config-if)# **storm-control** {**broadcast** | **multicast** | **unicast**} [{ **level** *percent* | **pps** *packets* | *rate-bps*]	**broadcast** 打开对广播风暴的控制功能。 **multicast** 打开对未知名多播风暴的控制功能 **unicast** 打开对未知名单播风暴的控制功能。 **level** *percent*： 以带宽的百分比进行设置 如 20 表示端口速率限制为 20%带宽。 **pps** *packet*：以报文为单位进行设置 即 packets per second，每秒允许通过的报文数。 *rate-bps*：以 bit 为单位进行设置，即 Kbits per second, 每秒允许通过的千比特数。

接口配置模式下通过命令 **no storm-control broadcast** ， **no storm-control multicast** ， **no storm-control unicast** 来关闭接口相应的风暴控制功能。

下面的例子打开 GigabitEthernet 0/1 上的多播风暴控制功能，并且设置允许的速 率为 4M。

```
Ruijie# configure terminal
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# storm-control multicast 4096
Ruijie(config-if)# end
```

NBS200F 系列设备基于 pps 的风暴控制，对长度的大于 64 bytes 的报文有一定的误差。报文长度越长，相较设置值误差越大，误差公式为（报文长度-64）/84;

设备基于 level 的风暴控制，带宽基准值直接采用设置风暴控制的物理口支持的最大带宽值，不采用物理口实际工作时的带宽值进行换算。

如果仅使能风暴控制功能，如配置 **storm-control broadcast**，这时风暴控制采用缺省设置，缺省设置值为端口带宽的百分之一。

3.1.3 查看风暴控制使能状态

查看接口的风暴控制使能状态：

命令	作用
show storm-control [*interface-id*]	显示风暴控制信息。

下面的例子为显示接口 Gi0/3 的风暴控制功能的使能状态：

```
Ruijie# show storm-control gigabitEthernet 0/3
Interface  Broadcast Control  Multicast Control  Unicast Control action
GigabitEthernet 0/3 Disabled  Disabled   Disabled    none
```

一次查看所有接口的风暴控制功能的使能状态：

```
Ruijie# show storm-control
Interface  Broadcast Control  Multicast Control  Unicast Control Action
---------  -----------------  -----------------  -------  -------
GigabitEthernet 0/1   Disabled   Disabled   Disabled   none
GigabitEthernet 0/2   Disabled   Disabled   Disabled   none
GigabitEthernet 0/3   Disabled   Disabled   Disabled   none
GigabitEthernet 0/4   Disabled   Disabled   Disabled   none
GigabitEthernet 0/5   Disabled   Disabled   Disabled   none
GigabitEthernet 0/6   Disabled   Disabled   Disabled   none
GigabitEthernet 0/7   Disabled   Disabled   Disabled   none
GigabitEthernet 0/8   Disabled   Disabled   Disabled   none
GigabitEthernet 0/9   Disabled   Disabled   Disabled   none
GigabitEthernet 0/10  Disabled   Disabled   Disabled   none
GigabitEthernet 0/11  Disabled   Disabled   Disabled   none
GigabitEthernet 0/12  Disabled   Disabled   Disabled   none
GigabitEthernet 0/13  Disabled   Disabled   Disabled   none
GigabitEthernet 0/14  Disabled   Disabled   Disabled   none
GigabitEthernet 0/15  Disabled   Disabled   Disabled   none
GigabitEthernet 0/16  Disabled   Disabled   Disabled   none
GigabitEthernet 0/17  Disabled   Disabled   Disabled   none
GigabitEthernet 0/18  Disabled   Disabled   Disabled   none
GigabitEthernet 0/19  Disabled   Disabled   Disabled   none
GigabitEthernet 0/20  Disabled   Disabled   Disabled   none
GigabitEthernet 0/21  Disabled   Disabled   Disabled   none
GigabitEthernet 0/22  Disabled   Disabled   Disabled   none
GigabitEthernet 0/23  Disabled   Disabled   Disabled   none
GigabitEthernet 0/24  Disabled   Disabled   Disabled   none
```

3.2 Protected Port

3.2.1 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。

3.2.2 配置Protected Port

设置接口为保护口：

命令	作用
Ruijie(config-if)# **switchport protected**	将该接口设置为保护口

通过命令 **no switchport protected** 接口配置命令将一个端口重新设置为非保护口。

下面的例子说明了如何把 Gigabitethernet 0/3 设置为保护口

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitethernet 0/3
Ruijie(config-if)# switchport protected
Ruijie(config-if)# end
```

3.2.3 显示Protected Port配置

命令	作用
Ruijie(config-if)# **show interfaces Switchport**	显示交换口配置

通过命令 **show interfaces switchport** 来查看保护口设置

```
Ruijie# show interfaces gigabitethernet 0/3 switchport
Interface            Switchport  Mode   Access  Native  Protected  VLAN lists
-------------------  ----------  ----   ------  ------  ---------  ----------
GigabitEthernet 0/3  enabled     Trunk  1       1       Enabled    ALL
```

3.3 ARP-Check功能

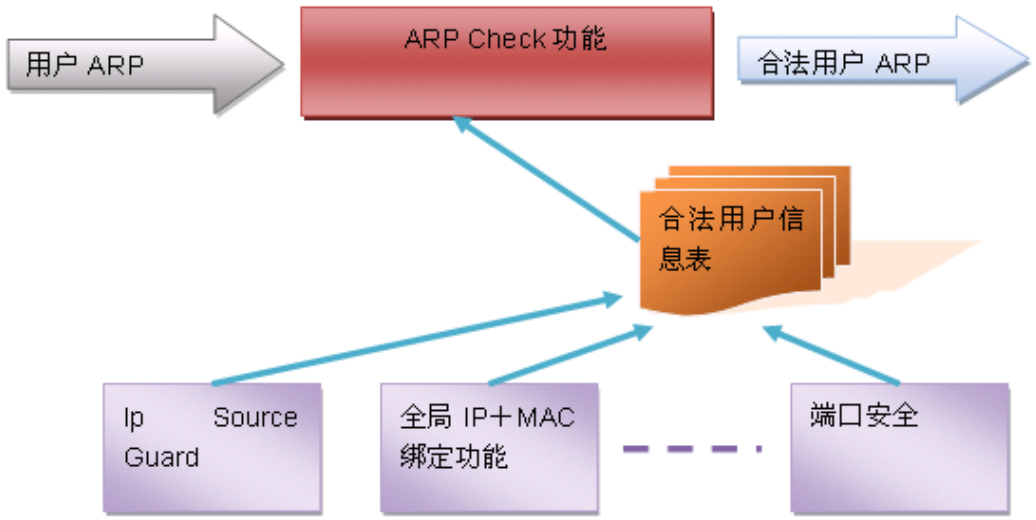
3.3.1 概述

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。

3.3.2 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 绑定等等）这些安全应用通过对用户 IP 报文进行有效的数据过滤，从而避免网络中的非法用户使用网络资源。在支持 ARP Check 功能的交换机中，ARP Check 功能能够根据这些应用模块所合法用户信息(IP 或 IP+MAC)产生相应的 ARP 过滤信息，从而实现对网络中的非法 ARP 报文的过滤。

图 8-1 Arp Check 功能与其它安全功能



如上图所示，交换机各安全功能模块产生的合法用户信息(仅有 IP 或 IP＋MAC)，ARP Check 功能使用这些信息用于检测逻辑端口下的所有的 ARP 报文中的 Sender IP 字段或<Sender IP, Sender MAC>是否满足合法用户信息表中的匹配关系，所有不在合法用户信息表中的 ARP 报文将被丢弃，目前 ARP Check 支持的安全功能模块包括：

1) 仅检测 IP 字段： Ip Source Guard 手工配置的仅 IP 模式。

2) 检测 IP+MAC 字段：全局 IP＋MAC 绑定功能， Ip Source Guard 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) Ip Source Guard

无论端口上有没有安全配置都检查 ARP 报文。如果端口上没有合法用户，则来自这个端口的所有 arp 报文都将被丢弃。

■ 关闭模式

不检查端口上的 ARP 报文。

打开 ARP Check 检测功能有可能会使相关安全应用的策略数/用户数减少

NBS200F 系列产品的转发面检查 ARP 报文以太网首部的源 MAC 地址和 Sender Ip 字段，控制面检查 ARP 协议内部的 Sender Mac 和 Sender Ip 字段。

3.3.3 配置ARP-Check

从特权模式下开始配置 ARP-Check 功能

命令	作用
Ruijie(config)#**interface** *interface-id*	进入接口模式
Ruijie(config-if)# **arp-check**	设置 ARP-Check 为打开模式
Ruijie(config-if)# **no arp-check**	设置 ARP-Check 为关闭模式

3.3.4 查看接口下实际生效的ARP Check表项

ARP-Check 功能支持查询实际端口的 ARP-Check 所产生的 ARP-Check 的表项信息：

命令	作用
show interface { *interface-type interface-number* } **arp-check list**	查看 ARP-Check 所产生成的表项

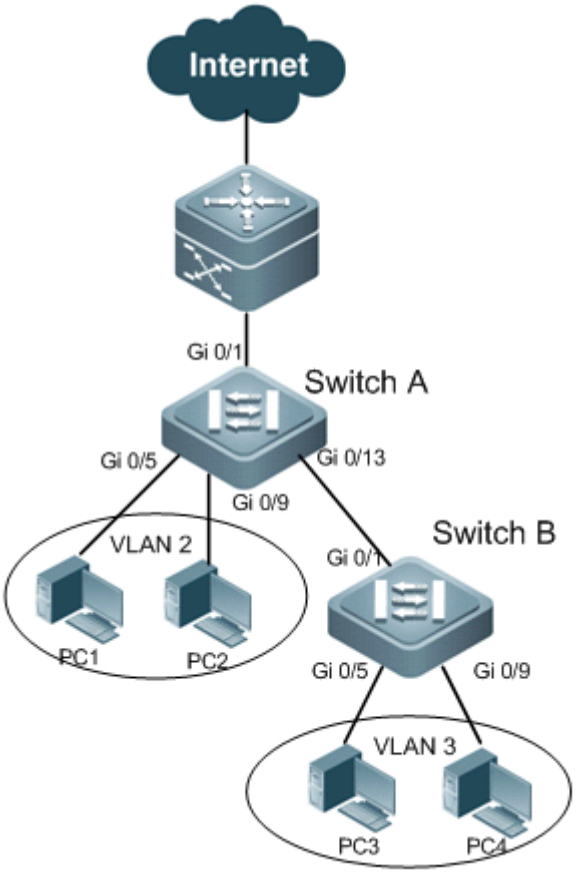
例如，查看 ARP-Check 产生表项信息如下：

```
Ruijie#show interfaces arp-check list
   Interface              Sender MAC        Sender IP       Policy Source
------------------------ ----------------- ---------------- --------------------
   Gi 0/1                 00D0.F800.0003    192.168.1.3       address-bind
   Gi 0/1                 00D0.F800.0001    192.168.1.1       port-security
   Gi 0/4                                   192.168.1.3       port-security
   Gi 0/5                 00D0.F800.0003    192.168.1.3       address-bind
   Gi 0/7                 00D0.F800.0006    192.168.1.6       AAA ip-auth-mode
   Gi 0/8                 00D0.F800.0007    192.168.1.7       GSN
```

3.4 基于端口的流控制组合配置用例

拓扑图

图 8-2



应用需求

上图是典型企业网络的简化拓扑，组网需求如下：

防止设备受到广播、多播、未知名单播报文攻击。

1) 只允许直连用户（本例指 Switch A 的直连用户）以指定的 IP/MAC 地址上网，源地址与指定 IP/MAC 不匹配的报文将被丢弃，防止源 IP,/源 MAC 欺骗。

2) 不允许接入用户（本例为 Switch B 的接入用户）之间进行二层报文通信，避免接入用户之间互相干扰（如 ARP 欺骗或 DOS 攻击等）

配置要点

- 配置要点

在所有接入设备（本例为 Switch A、Switch B）的端口上开启风暴控制。

1) 在接入设备（本例为 Switch B）上配置端口保护功能，可满足第三个需求。

配置步骤

- 配置 Switch A

第一步，创建交换机的 VLAN，并设置端口属性。

！创建 VLAN 2

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#vlan 2
Ruijie(config-vlan)#exit
```

！设置端口属性

```
Ruijie(config)#interface gigabitEthernet 0/5
Ruijie(config-if-GigabitEthernet 0/5)#switchport access vlan 2
Ruijie(config-if-GigabitEthernet 0/5)#exit
Ruijie(config)#interface gigabitEthernet 0/9
Ruijie(config-if-GigabitEthernet 0/9)#switchport access vlan 2
Ruijie(config-if-GigabitEthernet 0/9)#exit
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#switchport mode trunk
Ruijie(config-if-GigabitEthernet 0/1)#exit
Ruijie(config)#interface gigabitEthernet 0/13
Ruijie(config-if-GigabitEthernet 0/13)#switchport mode trunk
Ruijie(config-if-GigabitEthernet 0/13)#exit
```

第二步，在所有接入端口上开启风暴控制。

```
Ruijie(config)#interface range gigabitEthernet 0/1,0/5,0/9,0/13
Ruijie(config-if-range)#storm-control broadcast
Ruijie(config-if-range)#storm-control multicast
Ruijie(config-if-range)#storm-control unicast
Ruijie(config-if-range)#exit
```

■ 配置 Switch B

第一步，创建交换机的 VLAN，并设置端口属性

！创建 VLAN 3

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#vlan 3
Ruijie(config-vlan)#exit
Ruijie(config)#interface gigabitEthernet 0/5
Ruijie(config-if-GigabitEthernet 0/5)#switchport access vlan 3
Ruijie(config-if-GigabitEthernet 0/5)#exit
Ruijie(config)#interface gigabitEthernet 0/9
Ruijie(config-if-GigabitEthernet 0/9)#switchport access vlan 3
Ruijie(config-if-GigabitEthernet 0/9)#exit
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#switchport mode trunk
Ruijie(config-if-GigabitEthernet 0/1)#exit
```

第二步，在所有接入端口上开启风暴控制

```
Ruijie(config)#interface range gigabitEthernet 0/1,0/5,0/9
Ruijie(config-if-range)#storm-control broadcast
Ruijie(config-if-range)#storm-control multicast
Ruijie(config-if-range)#storm-control unicast
Ruijie(config-if-range)#exit
```

第三步，在接入端口上开启端口保护功能。

```
Ruijie(config)#interface gigabitEthernet 0/5
Ruijie(config-if-GigabitEthernet 0/5)#switchport protected
Ruijie(config-if-GigabitEthernet 0/5)#exit
Ruijie(config)#interface gigabitEthernet 0/9
Ruijie(config-if-GigabitEthernet 0/9)#switchport protected
Ruijie(config-if-GigabitEthernet 0/9)#exit
```

3.5 端口IP地址接入数量限定

3.5.1 概述

锐捷交换机支持多种接入控制应用（例如：Ip Source Guard、全局 IP+MAC 绑定等等），这些安全接入应用通过用户源 IP 地址信息进行接入控制，对用户 IP 报文进行有效的数据过滤，从而避免网络中的非法用户使用网络资源。

端口 IP 地址接入数量限定功能用于限定这些安全接入应用在端口上绑定的接入 IP 地址个数，用于限定共享交换机端口带宽的用户数量。

可以为每个端口配置可允许接入网络的 IP 地址数量，当端口下各个接入应用绑定的 IP 地址没有达到限定数量时，各个接入应用能够继续进行合法用户绑定和添加；当端口下 IP 地址数达到限定数量时，各个接入应用将不能再进行合法用户绑定。

当端口下的接入 IP 地址个数超出限定数量时，超出的 IP 地址不允许进行通行

- 端口 IP 接入数限定需要在接入控制应用的 IP+MAC 绑定或仅 IP 绑定生效情况下才有效，当端口下没有配置任何接入应用（或为全局 IP+MAC 绑定的例外口）时，限定的 IP 地址数不生效；
- IP+MAC 绑定和仅 IP 绑定同时绑定了同一个 IP 地址时，将被统计为 2 个用户 IP；
- 端口 IP 地址接入数量限定仅对 IPV4 报文生效；
- 除全局 IP+MAC 绑定的例外口外，全局 IP+MAC 绑定添加的用户将被统计到各个端口限定的 IP 地址数中；

3.5.2 端口IP地址接入数量限定的缺省配置

下表显示端口 IP 地址接入数量限定的缺省配置：

功能特性	缺省值
端口 IP 地址接入数量限定开关	所有端口均关闭 IP 地址接入数量限定功能，缺省值为 0

3.5.3 配置端口IP地址接入数量限定

从特权模式下开始配置端口 IP 地址接入数量限定：

命令	作用
Ruijie(config)#**interface** *interface-id*	进入接口模式
Ruijie(config-if)#**nac-author-user maximum** *value*	限定端口 IP 地址接入数量
Ruijie(config-if)#**no nac-author-user maximum**	关闭端口 IP 地址接入数量限定

3.5.4 查看端口IP地址接入数量

端口 IP 地址接入数量限定功能支持查询实际端口配置限定的接入 IP 地址数，以及已绑定的 IP 地址个数：

命令	作用
show nac-author-user	查看端口限定的 IP 地址接入数量配置及已绑定的 IP 地址个数

如下：

```
Ruijie#show nac-author-user
 Port      Cur_num  Max_num
 --------  -------  -------
 Fa0/1     2         50
 Fa0/2     0         0
 Fa0/3     2         100
 Fa0/4     0         0
 Fa0/5     0         200
 Fa0/6     0         0
 Fa0/7     0         0
 Fa0/8     0         0
```

4 CPU 保护

4.1 概述

在网络环境中，有各种攻击报文在网络上传播，其会导致交换机的 CPU 利用率过高，影响协议运行，甚至无法正常管理交换机。针对这种情况，必须对交换机的 CPU 进行保护，即对送往交换机的 CPU 处理的各种报文进行流量控制和优先级处理，保护其正常处理能力。

CPU Protect 的实现模型分为 Classifying、Queuing、Scheduling 和 Shaping 四个阶段，下面对这四个阶段进行详细的说明。

- Classifying：

Classifying 对每个需要送到 CPU 的报文进行分类，分类是根据报文的 L2、L3 以及 L4 信息，具体如下表所示：

报文类型	分类标准
bpdu	目的 MAC 地址为 01-80-C2-00-00-00 的报文
arp-request	arp request 报文
arp-reply	arp replayt 报文
tpp	目的 MAC 地址为 01-d0-f8-00-00-04，以太网类型为 0xBEEF 的报文
gvrp	目的 MAC 地址为 01-80-C2-00-00-21 的报文
rldp	目的 MAC 地址为 01-d0-f8-00-00-02，以太网类型为 0x788 的报文
lacp	目的 MAC 地址为 01-80-C2-00-00-02 的报文
lldp	目的 MAC 地址为 01-80-C2-00-00-0E 的报文
dhcp	dhcp 协议报文,包括 IPv4 dhcp
unknown_v4mc	地址表或路由表中不能查找到的 IPv4 播报文
known_v4mc	地址表或路由表中查找到的 IPv4 播报文
udp-helper	指定端口号的 UDP 广播报文
dvmrp	目的 IP 地址为 224.0.0.4，协议号为 2 的报文
icmp	IPv4 icmp 协议报文
rip	rip 协议报文,包括 rip 和 ripng 报文
error_ttl	IPv4 TTL = 0 或 1 的报文
local-telnet	telnet 本地管理报文
local-snmp	SNMP 本地管理报文
local-http	HTTP 本地管理报文
local-tftp	Tftp 本地管理报文
local-other	其他本地管理报文
v4uc-route	IPv4 单播报文
rt-host	rt-host 报文，组播地址为 224.0.0.1、224.0.0.2 和 FF02::1、FF02::2 的报文
nd	nd 协议报文
other	非上述分类的需要送到 CPU 的报文

☑ 二层交换机不支持三层报文，三层报文包括三层协议报文（如 pim，ospf，rip，isis 等）和 udp-helper、error-ttl、error-hop-limit、v4uc-route。

- Queuing：

Queuing 动作负责将各种不同类型的报文送到指定的队列，在不同队列的报文具有不同的传输优先级。

CPU 端口共有 8 个优先级队列，您可以配置每种类型的报文对应的队列，Queuing 根据您的配置自动地将这种类型的报文的送到指定队列。

- Scheduling：

当多个队列有报文需要传输时，Scheduling 负责从中选择一个队列并传输这个队列的报文。

CPU 端口 Scheduling 采用严格优先级(SP)算法，队列 7 具有最高优先级，队列 6 次之，以此类推，队列 0 具有最低优先级，高优先级队列报文总是先于低优先级队列的报文被传输。这样您可以根据每种报文的重要性将它们对应到不同的优先级的队列，确保重要的报文总是优先被传输。

☑ NBS200F 系列交换机中 CPU 端口软件队列调度：

高优先级队列和低优先级队列同时存在限速报文流时，会有少数低优先级队列的报文被传输。

- Shaping：

Shaping 控制每个传输队列的最大速率，超过最大速率的报文将被丢弃。您可以根据网络实际情况配置每个队列的最大速率，同时，您还可以配置整个 CPU 端口的最大速率。

地址学习风暴控制

除了这些报文攻击外，还可能出现 MAC 地址振荡攻击，即相同的源 MAC 地址在多个不同源端口出现，导致交换机不断的更新这些学习到的 MAC 地址。针对这种情况，我们实现了地址学习风暴控制，限制地址学习/更新源 MAC 地址的速率。

4.2 配置CPU Protect

4.2.1 CPU Protect默认配置

由于不同类型的交换机应用在不同的网络环境中，具有不同的网络攻击，CPU 保护也应该采用不同策略对应这些工具。所以对不同的交换机产品，我们精心地给您准备了不同的 CPU 的保护缺省配置。

☑ NBS200F 系列交换机

- 报文类型以及和队列的对应关系：

报文类型	队列
bpdu	6
arp-request	3
arp-replay	3
tpp	6

gvrp	5
rldp	5
lacp	5
lldp	5
dhcp	2
icmp	4
local-telnet	4
local-snmp	4
local-http	4
local-tftp	4
local-other	4
v4uc-route	0
nd	3
cfm	6
other	0

■ 每个队列默认最大速率：

队列	默认速率(pps)
6	3500
5	1500
4	1500
3	1500
2	1500
1	1000
0	1000
CPU 端口	6000

4.2.2 CPU Protect配置指导

☑ 在配置 NBS200F 系列交换机的 CPU 端口和每个队列速率时，速率的单位是 pps。

☑ NBS200F 系列交换机送往 CPU 端口的 bfd、dldp 报文队列不能通过 cpp 功能接口修改。

4.2.3 配置报文和队列的对应关系

在配置模式下，按如下步骤设置报文和队列的对应关系：

命令	作用

Ruijie(config)# **cpu-protect type** { **arp-reply | arp-request | bpdu | dhcp | dvmrp | error-hop-limit | error-ttl | gvrp | icmp | known-v4mc | lacp | lldp | local-http | local-other | local-snmp | local-telnet | local-tftp | nd | other | pim | rip | rldp | rt-host | tpp | udp-helper | unknown-v4mc | v4uc-route** } **traffic-class** *traffic-class-num*	设置报文对应的队列，*traffic-class-num* 的取值范围为 0－6。

如果要恢复其中一种类型报文对应的队列，可以用 **no cpu-protect type** { **arp-reply | arp-request | bpdu | dhcp | dvmrp | error-hop-limit | error-ttl | gvrp | icmp | known-v4mc | lacp | lldp | local-http | local-other | local-snmp | local-telnet | local-tftp | nd | other | pim | rip | rldp | rt-host | tpp | udp-helper | unknown-v4mc | v4uc-route** } **traffic-class** 来执行。

以下例子是表示报文对应的队列的配置过程：

```
Ruijie(config)# cpu-protect type bpdu traffic-class 5
Ruijie(config)# end
Ruijie # show cpu-protect type bpdu
Packet Type       Traffic-class  Bandwidth(pps)  Rate(pps)  Drop(pps)
---------------   -------------  --------------  ---------  ---------
bpdu              5              1000            0          0
```

按以上配置，bpdu 报文就对应到队列 5。

对于不同的产品，通过 cpu-protect type 命令可以配置的报文类型可能也不同，具体能够支持的类型参考 Classifying 章节。

4.2.4 配置每个队列的最大速率

在配置模式下，按如下步骤设置一个队列的最大速率：

命令	作用
Ruijie(config)# **cpu-protect traffic-class id id_num bandwidth** *bandwidth_value*	配置每个队列的最大速率（kbps），*id_num* 取值范围为 0－6，*bandwidth-value* 取值范围为 32－131072(pps)
Ruijie(config)# **cpu-protect traffic-class all bandwidth** *bandwidth_value*	配置所有队列的最大速率（kbps），*bandwidth-value* 取值范围为 32－131072(pps)

如果要恢复每个队列的缺省最大速率值，可以用 **no cpu-protect traffic-class** 来执行

以下例子是设置队列 6 的最大速率为 3500(pps)：

```
Ruijie# configure terminal
Ruijie(config)# cpu-protect traffic-class id 6  bandwidth 3500
Ruijie(config)#end
Ruijie# show cpu-protect traffic-class id 6
Traffic-class   Bandwidth(pps)  Rate(pps)
-------------   --------------  ---------
6               3500            0
```

NBS200F 系列交换机速率配置单位为 pps。

4.2.5 配置CPU端口的最大速率

在配置模式下，按如下步骤配置 CPU 端口最大速率：

命令	作用
Ruijie(config)# **cpu-protect cpu bandwidth** *bandwidth_value*	配置 CPU 端口的最大速率（pps），*bandwidth-value* 取值范围为 64－1000000(pps)。

您可以通过 **no cpu-protect cpu** 命令来恢复 CPU 端口的最大速率值。

以下是配置 CPU 端口最大速率为 6000（pps）的实例：

```
Ruijie# configure terminal
Ruijie(config)# cpu-protect cpu bandwidth 6000
Ruijie(config)# end
Ruijie# show cpu-protect cpu
%cpu port bandwidth: 6000(pps)
```

☑ NBS200F 系列交换机速率配置单位为 pps，取值范围略有不同。

4.2.6 配置地址学习风暴控制

在配置模式下，按如下步骤地址学习风暴控制功能：

命令	作用
Ruijie(config)# **cpu-protect mac-address storm-control enable** *value*	配置地址学习风暴控制，*value* 取值范围为 200－51200((address/second kbps))。

您可以通过 **no cpu-protect mac-address storm-control** 命令来恢复 CPU 端口的最大速率值。

以下是配置 MAC 地址学习风暴控制为 3000 个每秒的例子

```
Ruijie# configure terminal
Ruijie(config)# cpu-protect mac-address storm-control enable 3000
Ruijie(config)#end
Ruijie# show cpu-protect mac-address storm-control
%MAC address storm control state: enable
%MAC address storm control rate:  3000(address/second)
```

4.3 显示CPU Protect配置

4.3.1 查看每种类型报文对应的队列

在特权模式下使用如下命令查看每种类型报文对应的队列：

命令	作用

show cpu-protect type { bpdu | arp-request | arp-reply | tpp | gvrp | rldp | lacp | lldp | dhcp | unknown-v4mc | known-v4mc | udp-helper | dvmrp | icmp | pim | rip | error-ttl | error-hop-limit_| local-telnet | local-snmp | local-http | local-tftp | local-other | v4uc-route | rt-host | nd | other }	查看每种类型报文对应的队列。

☑ 使用 **show cpu-protect type all** 命令查看所有报文对应的队列:

```
Packet Type       Traffic-class  Bandwidth(pps)  Rate(pps)  Drop(pps)
----------------  -------------  --------------  ---------  ---------
bpdu              6              1000            0          0
arp-request       2              1000            0          0
arp-reply         2              1000            0          0
tpp               6              1000            0          0
gvrp              5              1000            0          0
rldp              5              1000            0          0
lacp              5              1000            0          0
lldp              5              180             0          0
dhcp              1              1000            0          0
unknown-v4mc      0              180             0          0
known-v4mc        0              180             0          0
udp-helper        0              1000            0          0
dvmrp             4              180             0          0
icmp              3              1000            0          0
pim               4              180             0          0
rip               4              1000            0          0
error-ttl         0              1000            0          0
error-hop-limit   0              1000            0          0
local-telnet      3              1000            0          0
local-snmp        3              1000            0          0
local-http        3              1000            0          0
local-tftp        3              1000            0          0
local-other       3              1000            0          0
v4uc-route        0              1000            0          0
rt-host           4              1000            0          0
nd                2              1000            0          0
other             0              1000            0          0
```

对于不同的产品，由于支持的类型不同，所以通过 **show cpu-protect type all** 命令显示的的类型也不完全相同，具体能够支持的类型参考 **Classifying** 章节.

4.3.2 查看每个队列的最大速率

在特权模式下使用如下命令查看每个队列的最大速率：

命令	作用
Ruijie# **show cpu-protect traffic-class id** *id_num*	查看每个队列的最大速率。*id_num* 的取值范围为 0－7
Ruijie# **show cpu-protect traffic-class all**	查看所有队列的最大速率

以下例子使用 **show cpu-protect traffic-class all** 命令查看所有队列的最大速率：

```
Ruijie# show cpu-protect traffic-class all
Traffic-class   Bandwidth(pps)  Rate(pps)
-------------   --------------  ---------
0               1000            0
1               1000            0
2               1500            0
3               1500            0
4               1500            0
5               1500            0
6               3500            0
```

4.3.3 查看CPU端口最大速率

在特权模式下使用如下命令查看 CPU 端口最大速率：

命令	作用
show cpu-protect cpu	查看 CPU 端口最大速率。

以下例子是查看 CPU 端口最大速率：

```
Ruijie# show cpu-protect cpu
%cpu port bandwidth: 6000(pps)
```

4.3.4 查看地址学习风暴控制

在特权模式下使用如下命令查看地址学习风暴控制：

命令	作用
show cpu-protect mac-address storm-control	查看地址学习风暴控制。

以下例子是查看 CPU 端口最大速率：

```
Ruijie# show cpu-protect mac-address storm-control
%MAC address storm control state: enable
%MAC address storm control rate:  8000(address/second)
```

5 DoS 保护

5.1 概述

DoS 保护功能支持防 Land 攻击、防非法 TCP 报文攻击、防非法 L4 报文攻击。

5.1.1 Land 攻击

Land 攻击主要是攻击者将一个 SYN 包的源地址和目的地址都设置为目标主机的地址，源和目的端口号设置为相同值，造成被攻击主机因试图与自己建立 TCP 连接而陷入死循环，甚至系统崩溃。

5.1.2 非法TCP报文攻击

在 TCP 报文的报头中，有几个标志字段：

1) SYN：连接建立标志，TCP SYN 报文就是把这个标志设置为 1，来请求建立连接。

2) ACK：回应标志，在一个 TCP 连接中，除了第一个报文（TCP SYN）外，所有报文都设置该字段作为对上一个报文的响应。

3) FIN： 结束标志，当一台主机接收到一个设置了 FIN 标志的 TCP 报文后，会拆除这个 TCP 连接。

4) RST：复位标志，当 IP 协议栈接收到一个目标端口不存在的 TCP 报文的时候，会回应一个 RST 标志设置的报文。

5) PSH：通知协议栈尽快把 TCP 数据提交给上层程序处理。

6) 非法 TCP 报文攻击是通过非法设置标志字段致使主机处理的资源消耗甚至系统崩溃，例如以下几种经常设置的非法 TCP 报文：

- SYN 比特和 FIN 比特同时设置的 TCP 报文

  正常情况下，SYN 标志（连接请求标志）和 FIN 标志（连接拆除标志）不能同时出现在一个 TCP 报文中，而且 RFC 也没有规定 IP 协议栈如何处理这样的畸形报文。因此各个操作系统的协议栈在收到这样的报文后的处理方式也不相同，攻击者就可以利用这个特征，通过发送 SYN 和 FIN 同时设置的报文，来判断操作系统的类型，然后针对该操作系统，进行进一步的攻击。

- 没有设置任何标志的 TCP 报文

  正常情况下，任何 TCP 报文都会设置 SYN，FIN，ACK，RST，PSH 五个标志中的至少一个标志，第一个 TCP 报文（TCP 连接请求报文）设置 SYN 标志，后续报文都设置 ACK 标志。有的协议栈基于这样的假设，没有针对不设置任何标志的 TCP 报文的处理过程，因此这样的协议栈如果收到了这样的报文可能会崩溃。攻击者利用了这个特点，对目标主机进行攻击。

- 设置了 FIN 标志却没有设置 ACK 标志的 TCP 报文

正常情况下，除了第一报文（SYN 报文）外，所有的报文都设置 ACK 标志，包括 TCP 连接拆除报文（FIN 标志设置的报文）。但有的攻击者却可能向目标主机发送设置了 FIN 标志却没有设置 ACK 标志的 TCP 报文，这样可能导致目标主机崩溃。

5.1.3 自身消耗攻击

自身消耗攻击主要事攻击者向目标主机发送与目标主机服务的 4 层端口号相同的报文，导致目标主机给自己发送 TCP 请求和连接。该攻击会使得目标主机的资源很快耗尽，甚至系统崩溃。

5.2 配置DoS保护

5.2.1 缺省的Dos保护设置

下面列出 DoS 缺省配置：

功能特性	缺省值
防 Land 攻击	缺省关闭
防非法 TCP 报文攻击	缺省关闭
防自身消耗报文攻击	缺省关闭

5.2.2 防Land攻击

在全局配置模式下，执行如下命令可以在设备上开启防 Land 攻击功能：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式
Ruijie(config)# **ip deny land**	开启防 Land 攻击功能
Ruijie(config)# **end**	退回到特权模式

5.2.3 预防非法TCP报文攻击

在全局配置模式下，执行如下命令可以在设备上开启防非法 TCP 报文攻击功能：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式
Ruijie(config)# **ip deny invalid-tcp**	开启防非法 TCP 报文攻击功能
Ruijie(config)# **end**	退回到特权模式

5.2.4 预防自身消耗攻击

在全局配置模式下，执行如下命令可以在设备上开启防自身消耗攻击功能：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式
Ruijie(config)# **ip deny invalid-l4port**	开启防自身消耗攻击功能
Ruijie(config)# **end**	退回到特权模式

5.3 显示DoS保护的状态

5.3.1 显示防Land攻击的状态

在任意模式下，执行如下命令可以显示防 Land 攻击的状态：

命令	作用
show ip deny land	显示防 Land 攻击的状态

下面的例子显示了如何查看防 Land 攻击的状态：

```
Ruijie# show ip deny land
          DoS Protection Mode               State
-----------------------------------     -----
  protect against land attack             On
```

5.3.2 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
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
```

5.3.3 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
```

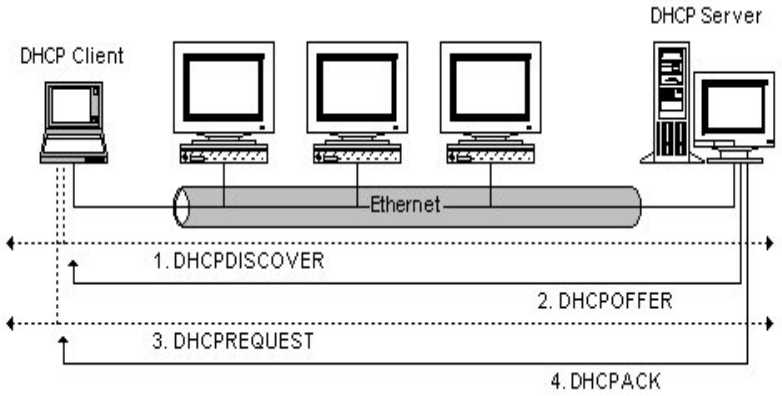
6 DHCP Snooping

6.1 DHCP Snooping简介

6.1.1 理解DHCP

DHCP 协议被广泛用来动态分配可重用的网络资源，如 IP 地址。一次典型的 DHCP 获取 IP 地址的过程如下所示：

图 11-1



- DHCP Client 发出 DHCP DISCOVER 广播报文给 DHCP Server，若 Client 在一定时间内没有收到服务器的响应，则重发 DHCP DISCOVER 报文。
- DHCP Server 收到 DHCP DISCOVER 报文后，根据一定的策略来给 Client 分配 IP 地址，然后发出 DHCP OFFER 报文。
- DHCP Client 收到 DHCP OFFER 报文后，发出 DHCP REQUEST 请求，请求租用服务器地址池中的 IP 地址，并通告其他服务器已接受此服务器分配的 IP 地址。
- 服务器收到 DHCP REQUEST 报文，验证资源是否可以分配，如果可以分配，则发送 DHCP ACK 报文；如果不可分配，则发送 DHCP NAK 报文。DHCP Client 收到 DHCP ACK 报文，就开始使用服务器分配的 IP 地址。如果收到 DHCP NAK，则重新发送 DHCP DISCOVER 报文。

6.1.2 理解DHCP Snooping

DHCP Snooping：意为 DHCP 窥探，通过对 Client 和服务器之间的 DHCP 交互报文进行窥探，实现对用户 IP 地址使用情况的监控，同时 DHCP Snooping 起到一个 DHCP 报文过滤的功能，通过合理的配置实现对非法的 DHCP 服务的过滤。下边对 DHCP Snooping 内使用到的一些术语及功能进行解释：

1) **DHCP 请求报文**：DHCP 客户端发往 DHCP 服务器的报文。

2) **DHCP 应答报文**：DHCP 服务器发往 DHCP 客户端的报文。

3) **DHCP Snooping TRUST 口：**由于 DHCP 获取 IP 的交互报文是使用广播的形式，从而存在着非法的 DHCP 服务影响用户正常 IP 的获取，更有甚者通过非法的 DHCP 服务欺骗窃取用户信息的现象，为了防止非法的 DHCP 服务的问题，DHCP Snooping 把端口分为两种类型，TRUST 口和 UNTRUST 口，设备只转发 TRUST 口收到的 DHCP 应答报文，而丢弃所有来自 UNTRUST 口的 DHCP 应答报文，这样我们把合法的 DHCP Server 连接的端口设置为 TRUST 口，则其他口为 UNTRUST 口，就可以实现对非法 DHCP Server 的屏蔽。

4) **DHCP Snooping 报文过滤：**在对个别用户禁用 DHCP 报文的情况下，需要评估用户设备发出的任何 DHCP 报文，那么我们可以在端口模式下配置 DHCP 报文过滤功能，过滤掉该端口收到的所有 DHCP 报文。

5) **基于 VLAN 的 DHCP Snooping：**DHCP Snooping 功能生效是以 VLAN 为单位的，默认情况下打开 DHCP Snooping 功能，会在当前设备上的所有 VLAN 上使能 DHCP Snooping 功能，可以通过配置灵活的控制 DHCP Snooping 生效的 VLAN。

6) **DHCP Snooping 绑定数据库：**在 DHCP 环境的网络里经常会出现用户随意设置静态 IP 地址的问题，用户随意设置的 IP 地址不但使网络难以维护，而且会导致一些合法的使用 DHCP 获取 IP 的用户因为冲突而无法正常使用网络，DHCP Snooping 通过窥探 Client 和 Server 之间交互的报文，把用户获取到的 IP 信息以及用户 MAC、VID、PORT、租约时间等信息组成用户记录表项，从而形成 DHCP Snooping 的用户数据库，配合 ARP 检测功能或 ARP CHECK 功能的使用，进而达到控制用户合法使用 IP 地址的目的。

7) **DHCP Snooping 速率限制：**DHCP Snooping 需要对所有非信任端的 DHCP 请求报文进行检查，同时将合法的 DHCP 请求报文转发到信任口所在的网络。为了防止在非信任端出现 DHCP 请求报文攻击、控制流向信任网络的 DHCP 请求报文速率。DHCP Snooping 支持在端口对收到的 DHCP 报文进行速率限制，当接口收到的 DHCP 报文速率超过设定的限制时，丢弃超过限制速率的那部分 DHCP 报文。DHCP Snooping 的速率限制基于接口配置，可以选择通过 DHCP Snooping 的速率限制命令配置，也可以选择通过 NFPP 的速率限制命令配置，效果是一样的。对于支持 CPP 的产品来说，如果同时配置了 CPP 的 DHCP 报文速率限制和 DHCP Snooping 的报文速率限制，CPP 的配置将优先于 DHCP Snooping 的速率限制生效，因此为了确保 DHCP Snooping 速率限制生效，需要注意 CPP 的速率上限不小于 DHCP Snooping 的限制或者 NFPP 的限制。 CPP 的配置请查看配置指南《配置 CPU 保护》，NFPP 的配置请查看 NFPP 配置指导。

DHCP Snooping 通过对经过设备的 DHCP 报文进行合法性检查，丢弃不合法的 DHCP 报文，记录用户信息并生成 DHCP Snooping 绑定数据库供其他功能（如：ARP 检测功能）查询使用。以下几种类型的报文被认为是非法的 DHCP 报文：

- UNTRUST 口收到的 DHCP 应答报文，包括 DHCPACK、DHCPNACK、DHCPOFFER 等。
- UNTRUST 口收到的带有网关信息[giaddr]的 DHCP request 报文。
- 打开 mac 校验时，源 MAC 与 DHCP 报文携带的 chaddr 字段值为不同的报文。
- DHCPRELEASE 报文中的用户在 DHCP Snooping 绑定数据库中存在，但是 DHCPRELEASE 报文的接收端口和保存在 DHCP Snooping 绑定数据库中的端口不一致，那么这个 DHCPRELEASE 报文是非法的。

6.1.3 理解DHCP Snooping information option

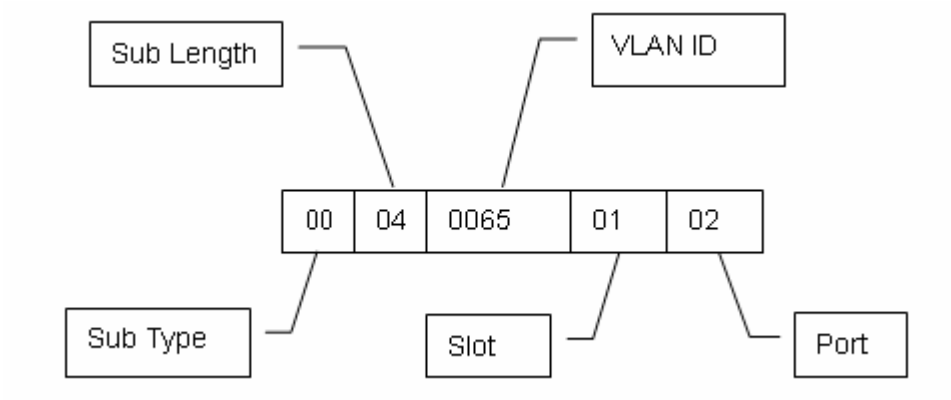
部分网络管理员在对当前的用户进行 IP 管理时，希望能够根据用户所处的位置来给用户分配 IP，即希望能够根据用户所连接的网络设备的信息进行用户的 IP 分配，从而交换机在进行 DHCP 窥探的同时把一些用户相关的设备信息以 DHCP option 的方式加入到 DHCP 请求报文中，根据 RFC3046，所使用的 option 选项号为 82。Option 82 选项最多可以包含 255 个子选项。若定义了 Option 82，则至少要定义一个子选项。目前设备只支持 Circuit ID（电路 ID 子选项）和 Remote ID（远程 ID 子选项）两个子选项。在 DHCP Server 服务器配置对 option82 内容的解析，这个服务器就可以通过 Option82 上传的内容，获取到更多用户的信息，从而更准确地给用户分配 IP。

- Circuit ID：

Circuit ID 的默认填充内容是接收到 DHCP 客户端请求报文的端口所属 VLAN 的编号以及端口索引（端口索引的取值为端口所在槽号和端口号），扩展填充内容是自定义的字符串。

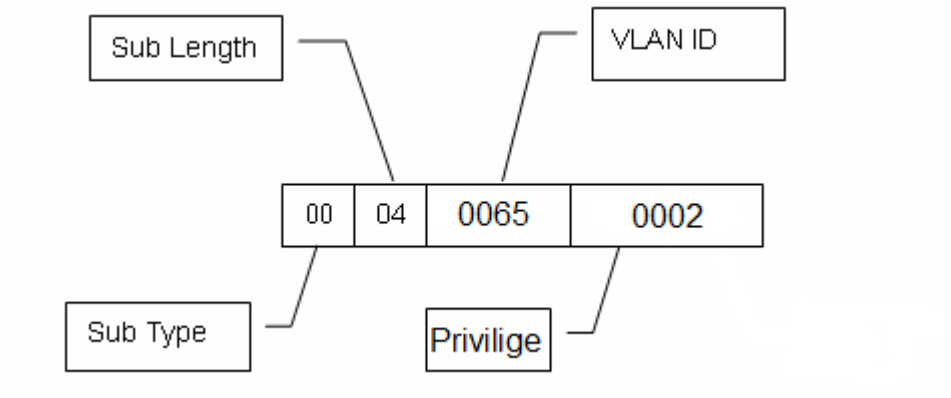
Circuit ID 填充格式有三种，第一种是标准填充格式，第二种是扩展填充格式，第三种是 DOT1X 扩展格式，在同一个网络域中，只能使用其中的一种，不能混合使用。标准填充格式时，Circuit ID 子选项只能填充默认的填充内容。标准和扩展填充格式如下所示：

图 11-2



DOT1X 填充格式如图 1-3 所示：

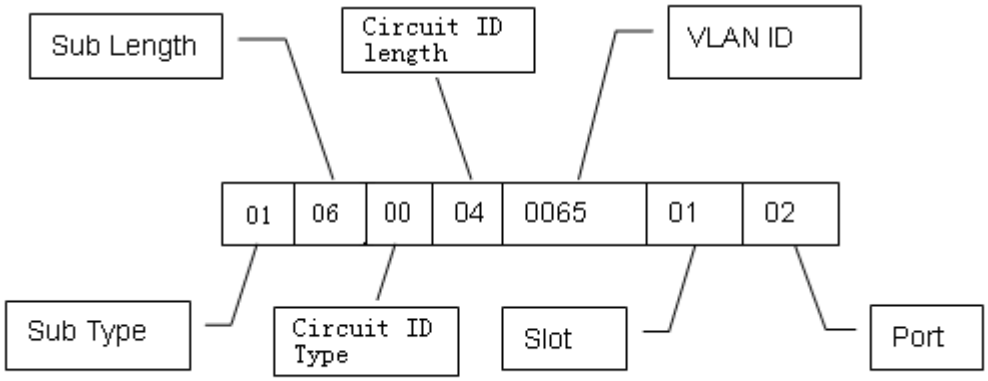
图 11-3



如果需要使用自定义的填充内容，那么可以使用扩展填充格式。扩展填充格式的填充内容可以是默认填充内容，也可以是扩展填充内容。为了区分填充内容的不同，在子选项长度后增加一个字节的内容类型字段和一个字节的内容长度字段，如果是默认填充内容，则设置内容类型为 0；如果是扩展填充内容，则设置内容类型为 1。

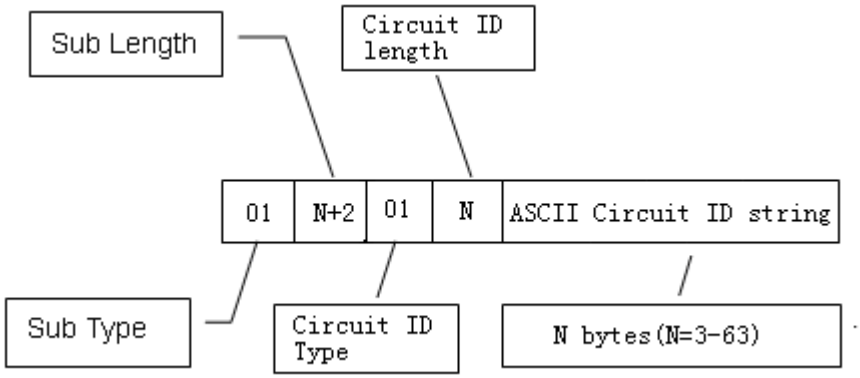
默认填充内容的格式如下：

图 11-4



扩展填充内容的格式如下：

图 11-5

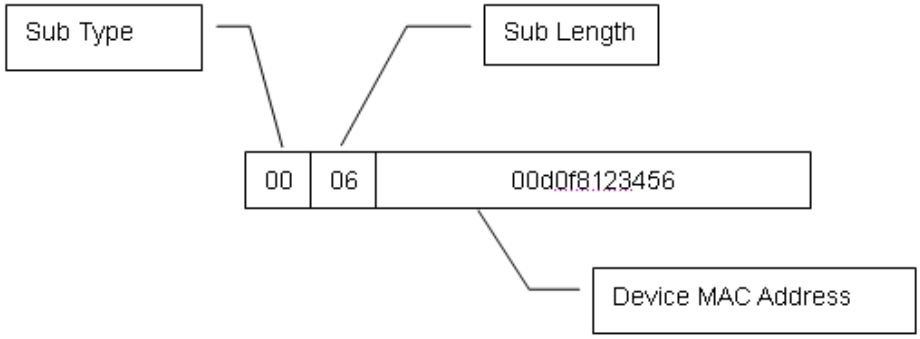


- Remote ID：

Remote ID 的默认填充内容是接收到 DHCP 客户端请求报文的 DHCP 中继设备的桥 MAC 地址。扩展填充内容是自定义的字符串。

Remote ID 填充格式有两种，一种是标准填充格式，一种是扩展填充格式，在同一个网络域中，只能使用其中的一种，不能混合使用。标准填充格式时，Remote ID 子选项只能填充默认的填充内容，如下所示：

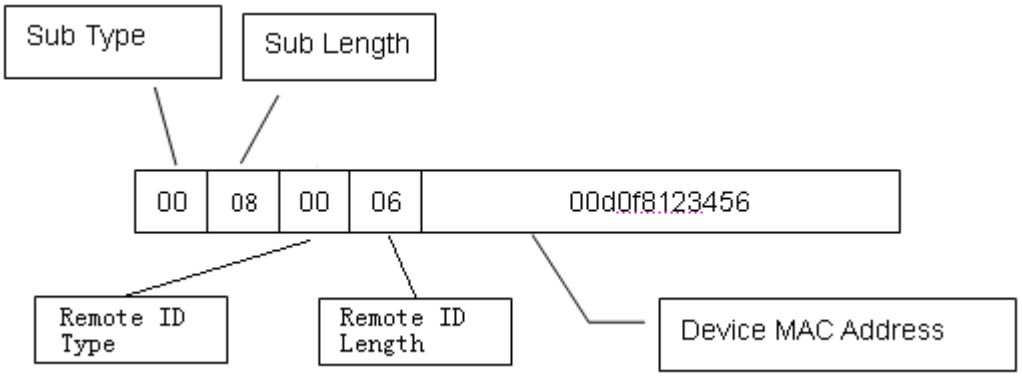
图 11-6



如果需要使用自定义的填充内容，那么可以使用扩展填充格式。扩展填充格式的填充内容可以是默认填充内容，也可以是扩展填充内容。为了区分填充内容的不同，在子选项长度后增加一个字节的内容类型字段和一个字节的内容长度字段，如果是默认填充内容，则设置内容类型为 0；如果是扩展填充内容，则设置内容类型为 1。

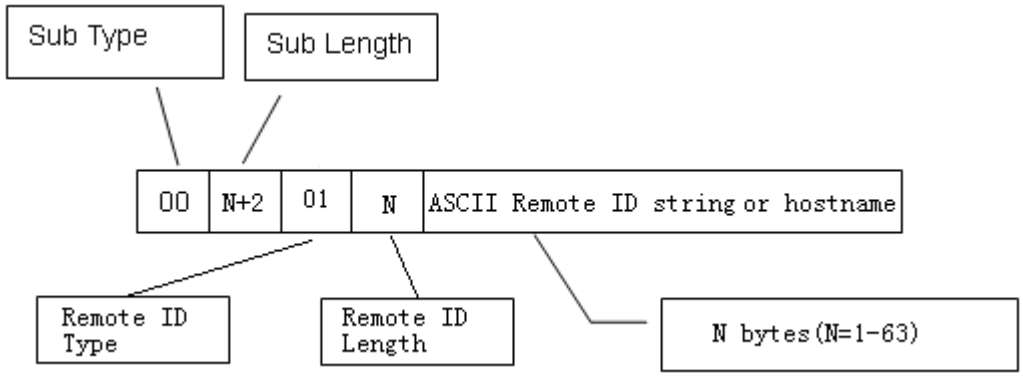
默认填充内容的格式如下：

图 11-7



扩展填充内容的格式如下：

图 11-8



Circuit ID 中端口索引的取值为端口所在槽号和端口号。其中端口号是指端口在槽上的序号，AP 口（聚合口）的端口号就是 AP 号。例如 Fa0/10，端口号就是 10，AP 11 的端口号就是 11。其中槽号是设备（堆叠认为是一台设备）上所有槽排序的序号，AP 口的槽号在最后。槽排序的序号从 0 开始，可用 show slots 命令查看。例如：

例 1：

```
Ruijie#show slots  （只列出 Dev、slot 示例）
  Dev Slot
  --- ----
  1   0    ------->槽号为 0
  1   1    ------->槽号为 1
  1   2    ------->槽号为 2
```

此时 AP 口的槽号为 3。

例 2：

```
Ruijie#show slots （只列出 Dev、slot 示例）
  Dev Slot
  --- ----
  1   0    ------>槽号为 0
  1   1    ------>槽号为 1
  1   2    ------>槽号为 2
  2   0    ------>槽号为 3
  2   1    ------>槽号为 4
  2   2    ------>槽号为 5
```

此时 AP 口的槽号为 6。

6.2 DHCP snooping的相关安全功能

在 DHCP 的网络环境中，管理员经常碰到的一个问题就是一些用户随意修改使用静态的 IP 地址，而不去使用动态获取的 IP 地址。这会导致一些使用动态获取 IP 的用户的无法正常使用网络，并且会使网络环境变复杂。因为 DHCP 动态绑定是设备在 DHCP snooping 的过程通过记录的合法用户的 IP 信息，所以对 DHCP 动态绑定进行相关的安全处理，可以解决用户随意使用静态 IP 地址的问题。当前的安全控制存在三种方式，一种是结合 IP Source Guard 功能对合法用户进行地址绑定，第二种就是使用软件的 DAI（动态 ARP 检测），通过对 ARP 的控制进行用户的合法性校验，第三种结合 ARP CHECK 的功能，来对合法用户的 ARP 报文进行绑定。

DHCP Snooping 模块和其他安全功能的优先级关系，可参考《锐捷新安全方案技术白皮书》。

> 结合 IP Source Guard 功能进行地址绑定时由于受硬件表项的限制，交换机能够支持的 DHCP 用户数目有限，当交换机上用户过多时，可能出现合法用户也无法添加硬件表项而不能正常使用网络的现象，而使用 DAI 功能时，由于所有的 ARP 报文都需要通过 CPU 转发和处理，所以会降低交换机的转发性能。

6.2.1 理解DHCP Snooping和IP Source Guard地址绑定的关系

IP Source Guard 功能维护一个 IP 源地址数据库，通过将数据库中的用户信息[VLAN、MAC、IP、PORT]设置为硬件过滤表项，只允许对应的用户使用网络，更多信息请参考《配置 IP Source Guard》。

DHCP Snooping 维护一个用户 IP 的数据库，并将该数据提供给 IP Source Guard 功能进行过滤，从而限制只有通过 DHCP 获取 IP 的用户才能够使用网络，这样就阻止了用户随意设置静态 IP。

6.2.2 DHCP Snooping和DAI的关系

DAI(Dynamic ARP Inspection,动态 ARP 检测)就是对经过设备的所有 ARP 报文进行检查。由于 DHCP 绑定过滤只针对 IP 报文，不能进行 ARP 报文的过滤，所以为了增加安全性，防止 ARP 欺骗等问题，对于 DHCP 绑定的用户进行 ARP 合法性检查，DHCP Snooping 提供数据库信息给 ARP 探测使用，在开启 DAI 功能的设备上，当开启 IP Source Guard 地址绑定的端口收到 ARP 报文时，DAI 模块就根据报文查询 DHCP snooping 的绑定数据库，只有当收到的 ARP 报文数据字段的源 MAC、源 IP 和端口信息都匹配时才认为收到的 ARP 报文是合法的，才进行相关的学习和转发操作，否则丢弃该报文，更多信息参考《DAI 配置指导》。

6.2.3 DHCP Snooping和ARP CHECK的关系

ARP CHECK 是对经过设备的所有 ARP 报文进行检查，DHCP Snooping 提供数据库信息供 ARP CHECK 使用，在开启 ARP CHECK 功能的设备上，当收到 ARP 报文时，ARP CHECK 模块就根据报文查询 DHCP snooping 的绑定数据库，只有当开启 IP Source Guard 地址绑定的端口收到的 ARP 报文数据字段的源 MAC、源 IP 和端口信息都匹配时才认为收到的 ARP 报文是合法的，才进行相关的学习和转发操作，否则丢弃该报文。

6.3 配置DHCP Snooping的其他注意事项

DHCP Snooping 功能与 DOT1x 的 DHCP Option 82 功能是互斥的，不能同时使用 DHCP Snooping 和 DHCP Option82。

DHCP Snooping 和 DAI 功能或 ARP CHECK 功能共用，可以控制用户必须使用 DHCP 分配的 IP 上网。

6.4 DHCP Snooping配置

6.4.1 配置打开和关闭DHCP Snooping

缺省情况下，设备的 DHCP Snooping 功能是关闭,当配置 **ip dhcp snooping** 命令后，设备就打开了 dhcp snooping 功能

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# [**no**] **ip dhcp snooping**	DHCP snooping 打开和关闭

下边是配置打开设备 DHCP snooping 功能：

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping
Ruijie(config)# end
Ruijie# show ip dhcp snooping
Switch DHCP snooping  status                    :   ENABLE
DHCP snooping  Verification of hwaddr status  :   DISABLE
DHCP snooping database write-delay time        :   0 seconds
DHCP snooping option 82 status                  :   DISABLE
DHCP snooping Support bootp bind status        :   DISABLE
Interface              Trusted           Rate limit (pps)
-----------------      ---------     ---------------
GigabitEthernet 0/1       YES                unlimited
```

6.4.2 配置端口DHCP报文过滤

缺省情况下，设备端口的 DHCP 请求报文过滤功能是关闭的。当不想对某个端口下的用户提供 DHCP 服务时，可配置此功能，配置后，就会对这个端口上来的 DHCP 请求报文进行过滤。

命令	作用

Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **interface** *interface*	进入接口配置模式
Ruijie(config-if)# [**no**] **ip dhcp snooping suppression**	配置接口过滤 DHCP 报文功能

下边是配置打开设备端口的 DHCP 请求报文过滤功能：

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# ip dhcp snooping suppression
```

6.4.3 配置DHCP Snooping功能生效的VLAN

缺省情况下，DHCP Snooping 功能对所有 VLAN 生效。如果要配置 DHCP Snooping 在某个 VLAN 上失效，将该 VLAN 从 DHCP Snooping 生效的 VLAN 范围中去除。

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# [**no**] **ip dhcp snooping vlan** {*vlan-rng* | {*vlan-min* [*vlan-max*]}}	配置 DHCP Snooping 功能生效的 VLAN

下边是配置 DHCP snooping 功能在 VLAN1000 上生效：

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping vlan 1000
Ruijie(config)# end
```

打开 DHCP Snooping 功能，默认情况下会在设备上的所有 VLAN 上打开 DHCP Snooping 功能，如果需要基于 VLAN 打开关闭 DHCP Snooping 功能，只需要在 DHCP Snooping 生效范围中添加/删除该 VLAN。

6.4.4 配置DHCP源MAC检查功能

配置此命令后，设备就会对 UNTRUST 口送上来的 DHCP Request 报文进行源 MAC 和 Client 字段的 MAC 地址校验检查，丢弃 MAC 值不相同的不合法的 DHCP 请求报文。默认不检查。

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# [**no**] **ip dhcp snooping verify mac-address**	打开和关闭源 MAC 检查功能

下边的是打开 DHCP 源 MAC 检查的功能

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping verify mac-address
Ruijie(config)# end
Ruijie# show ip dhcp snooping
Switch DHCP snooping  status                    :   ENABLE
DHCP snooping  Verification of hwaddr status   :   ENABLE
DHCP snooping database write-delay time         :   0 seconds
DHCP snooping option 82 status                  :   DISABLE
DHCP snooping Support bootp bind status         :   DISABLE
```

```
Interface              Trusted           Rate limit (pps)
-----------------      ---------     ---------------
GigabitEthernet 0/1       YES                unlimited
```

6.4.5 配置静态DHCP snooping information option

通过配置如下命令，在进行 DHCP 窥探转发时，给每个 DHCP 请求添加 option82 选项。缺省情况下该功能是关闭的。

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# [**no**] **ip dhcp snooping Information option** [*standard-format* | **dot1x-format**]	设置 DHCP snooping information option；standard-format：有此关键字时，填充的格式为标准格式；dot1x-format：有此关键字时填充的格式为 DOT1X 格式。
Ruijie(config)# [**no**] **ip dhcp snooping information option format remote-id** [**string** *ASCII-string* | **hostname**]	在扩展格式下配置 remote-id。 string：填充内容为自定义字符串； hostname：填充内容为主机名。
Ruijie(config)# **interface** *interface*	进入接口配置模式
Ruijie(config-if)# [**no**] **ip dhcp snooping vlan** *vlan-id* **information option format-type circuit-id string** *ASCII-string*	在扩展格式下配置 circuit-id 的自定义字符串。
Ruijie(config-if)# [**no**] **ip dhcp snooping vlan** *vlan-id* **information option change-vlan-to vlan** *vlan-id*	在扩展格式下配置 circuit-id 的 vlan 映射，和 Step 5 的命令互斥。

下边是配置打开 DHCP information option 功能：

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping information option
Ruijie(config)# end
Ruijie# show ip dhcp snooping
Switch DHCP snooping  status                    :   ENABLE
DHCP snooping  Verification of hwaddr status    :   ENABLE
DHCP snooping database write-delay time         :   0 seconds
DHCP snooping option 82 status                    :   ENABLE
DHCP snooping Support bootp bind status         :   DISABLE
Interface              Trusted           Rate limit (pps)
-----------------      ---------     ---------------
GigabitEthernet 0/1       YES                unlimited
```

当配置此功能后，DHCP relay 的 information option82 功能就会失效。

6.4.6 配置定时写DHCP Snooping数据库信息到flash

为了防止设备断电重启，设备上的 DHCP 用户信息丢失，而导致设备重启后，重启前已成功获取 IP 地址的用户不能通信，DHCP Snooping 提供可配置的定时把 DHCP Snooping 数据库信息写入 flash 的命令来保存 DHCP 用户信息。默认情况下，定时为 0，即不定时写 flash。

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# [**no**] **ip dhcp snooping database write-delay** [*time*]	设置 DHCP 延迟写 flash 的时间 *time*：600s--86400s.缺省为 0

下边的是设置 DHCP Snooping 延迟写 flash 的时间为 3600s：

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping database write-delay 3600
Ruijie(config)# end
Ruijie# show ip dhcp snooping
Switch DHCP snooping  status                    :   ENABLE
DHCP snooping  Verification of hwaddr status    :   ENABLE
DHCP snooping database write-delay time         :   3600 seconds
DHCP snooping option 82 status                    :   ENABLE
DHCP snooping Support bootp bind status         :   DISABLE
Interface              Trusted           Rate limit (pps)
-----------------      ---------     ---------------
GigabitEthernet 0/1       YES                unlimited
```

由于不停擦写 flash 会造成 flash 的使用寿命缩短，所以在设置延迟写 flash 时间时需要注意，设置时间较短有利于设备信息更有效的保存，设置时间较长能够减少写 flash 的次数，延长 flash 的使用寿命。

6.4.7 手动把DHCP snooping数据库信息写到flash

为了防止设备断电重启导致设备上的 DHCP 用户信息丢失而使用户不能上网，除了配置定时写 flash 外，也可以根据需要手动地把当前的 DHCP Snooping 绑定数据库信息写入 flash。

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **ip dhcp snooping database write-to-flash**	把 DHCP snooping 数据库信息写入 flash

下边的是手动的把 DHCP Snooping 数据库信息写入 flash：

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping database write-to-flash
Ruijie(config)# end
```

6.4.8 手动把flash中的信息导入DHCP snooping数据库

在开启 DHCP snooping 功能时，可以根据需要手动地把当前 flash 中的信息导入 DHCP Snooping 绑定数据库。

命令	作用
Ruijie# **renew ip dhcp snooping database**	把 flash 中信息导入 DHCP snooping 数据库。

下边的是手动的把 flash 中信息导入 DHCP Snooping 数据库：

```
Ruijie# renew ip dhcp snooping database
```

6.4.9 配置端口为TRUST口

用户通过配置此命令来设置一个端口为 TRUST 口，默认情况下所有端口全部为 UNTRUST 口：

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **interface** *interface*	进入接口配置模式
Ruijie(config-if)# [**no**] **ip dhcp snooping trust**	将端口设置为 trust 口

下边是配置设备的 1 端口为 TRUST 口：

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# ip dhcp snooping trust
Ruijie(config-if)# end
Ruijie# show ip dhcp snooping
Switch DHCP snooping  status                    :   ENABLE
DHCP snooping  Verification of hwaddr status    :   DISABLE
DHCP snooping database write-delay time         :   3600 seconds
DHCP snooping option 82 status                  :   DISABLE
DHCP snooping Support bootp bind status         :   DISABLE
Interface              Trusted           Rate limit (pps)
-----------------      ---------     ---------------
GigabitEthernet 0/1       YES                unlimited
```

打开 DHCP Snooping 后，只有配置为 TRUST 口连接的服务器发出的 DHCP 响应报文才能够被转发。

6.4.10 清空DHCP Snooping数据库动态用户信息

如果 DHCP Snooping 的数据库需要重新生成时，可用此命令删除当前的 DHCP Snooping 数据库的信息。

命令	作用
Ruijie# **clear ip dhcp snooping binding** [**vlan** *vlan-id* | *mac* | *ip* | **interface** *interface-id*]	清空当前数据库的信息，可基于 VLAN、MAC、IP、接口删除，并可组合使用。

下边的是手动清空当前数据库的信息：

```
Ruijie# clear ip dhcp snooping binding
```

6.5 DHCP snooping配置显示

6.5.1 显示DHCP snooping

您可以通过以下步骤显示 **ip dhcp snooping** 内容

命令	作用
show ip dhcp snooping	显示 dhcp snooping 的相关配置信息

例如：

```
Ruijie# show ip dhcp snooping
Switch DHCP snooping  status                    :   ENABLE
DHCP snooping  Verification of hwaddr status    :   ENABLE
DHCP snooping database write-delay time         :   3600 seconds
DHCP snooping option 82 status                  :   ENABLE
DHCP snooping Support bootp bind status         :   ENABLE
Interface              Trusted           Rate limit (pps)
-----------------      ---------     ---------------
GigabitEthernet 0/1       YES                unlimited
```

6.5.2 显示DHCP snooping 数据库信息

您可以通过以下步骤显示 **ip dhcp snooping** 数据库信息的相关内容

命令	作用
show ip dhcp snooping binding	查看 DHCP Snooping 绑定数据库的用户信息

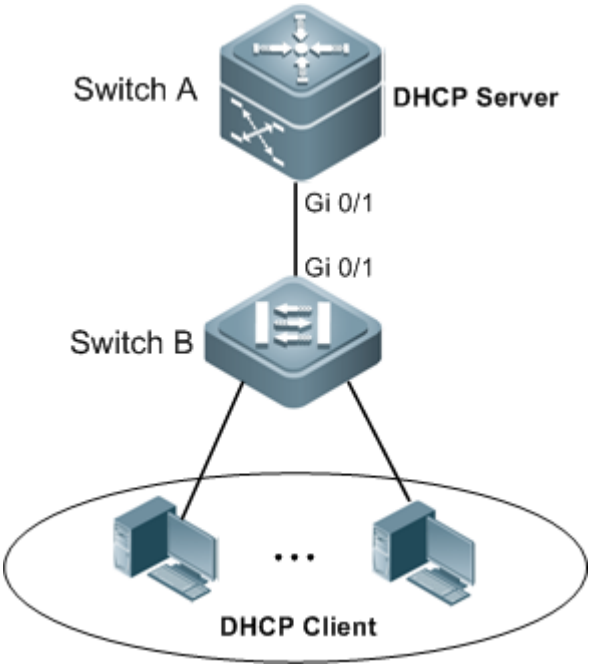
例如：

```
Ruijie# show ip dhcp snooping binding
Total number of bindings: 1
MacAddress         IpAddress       Lease(sec)   Type          VLAN  Interface
---------------- --------------- ------------ -------------
001b.241e.6775     192.168.12.9    7200        dhcp-snooping 1     GigabitEthernet 0/5
```

6.6 DHCP Snooping典型配置用例

拓扑图

图 11-9 DHCP Snooping 用例示意图



应用需求

1) DHCP 客户端用户通过合法 DHCP 服务器动态获取 IP 地址。

2) 避免其他用户私设 DHCP 服务器。

配置要点

在接入设备（本例为 Switch B）上开启 DHCP Snooping 功能，将上链口（本例为端口 Gi 0/1）设置为信任口。

配置步骤

- 配置 Switch B

第一步，打开 DHCP Snooping 功能。

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

第二步，配置上链口为信任口。

```
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#ip dhcp snooping trust
```

配置验证

第一步，确认 Switch B 的配置，关注点：是否开启 DHCP Snooping 功能、配置的 DHCP Snooping 信任口是否为上链口。

```
Ruijie#show running-config
!
```

```
ip dhcp snooping
!
interface GigabitEthernet 0/1
 ip dhcp snooping trust
```

第二步，查看 Switch B 的 DHCP Snooping 配置情况，关注点为信任口是否正确。

```
Ruijie#show ip dhcp snooping
Switch DHCP snooping  status                    :   ENABLE
DHCP snooping  Verification of hwaddr status    :   DISABLE
DHCP snooping database write-delay time         :   0 seconds
DHCP snooping option 82 status                  :   DISABLE
DHCP snooping Support bootp bind status         :   DISABLE
Interface                      Trusted       Rate limit (pps)
-------------------------      -------       ----------------
GigabitEthernet 0/1            YES           unlimited
```

第三步，查看 DHCP Snooping 地址绑定数据库信息（用户的 MAC 地址、动态分配的 IP 地址、地址租期、对应的 VLAN 和端口号等）。

```
Ruijie#show ip dhcp snooping binding
Total number of bindings: 1
MacAddress          IpAddress       Lease(sec)   Type           VLAN  Interface
------------------ --------------- ------------ ------------- ----- --------------------
0013.2049.9014      172.16.1.2      86207        dhcp-snooping 1     GigabitEthernet 0/11
```

7 动态 ARP 检测

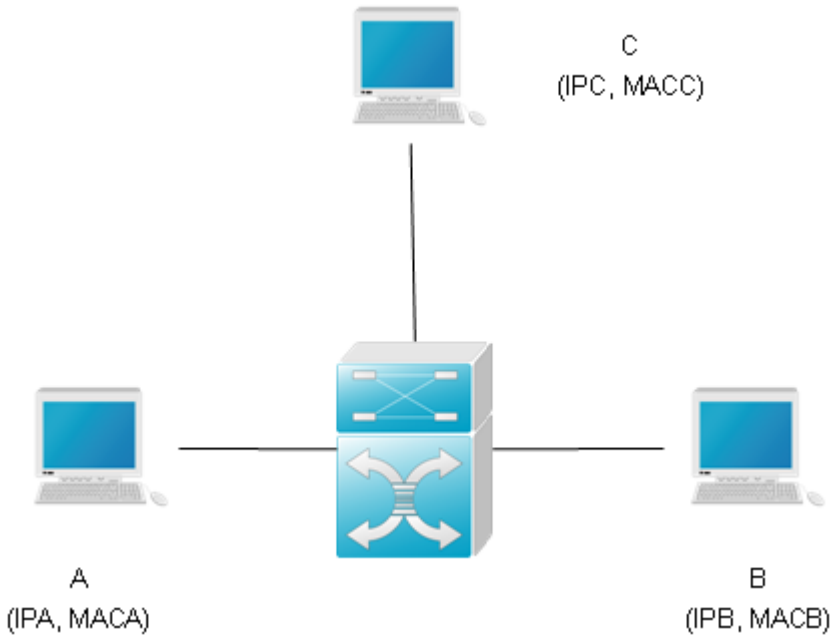
7.1 理解DAI

DAI 的全称是 Dynamic ARP Inspection，中文名为动态 ARP 检测。即对接收到的 ARP 报文进行合法性检查。不合法的 ARP 报文会被丢弃。

7.1.1 理解ARP 欺骗攻击

由于 ARP 协议本身的缺陷，ARP 协议不对收到的 ARP 报文进行合法性检查。这就造成了攻击者利用协议的漏洞轻易的进行 ARP 欺骗攻击。这其中，最典型的就是中间人攻击。中间人攻击描述如下：

图 12-1



如上图所示：设备 A、B、C 均连接在锐捷设备上，并且它们位于同一个子网。它们的 IP 和 MAC 分别表示为（IPA, MACA）(IPB, MACB) (IPC, MACC)。当设备 A 需要和设备 B 进行网络层通信时，设备 A 将会在子网内广播一个 ARP 请求，询问设备 B 的 MAC 值。当设备 B 接收到此 ARP 请求报文时，会更新自己的 ARP 缓存，使用的是 IPA 和 MACA,并发出 ARP 应答。设备 A 收到此应答后，会更新自己的 ARP 缓存，使用的是 IPB 和 MACB。

在这种模型下，设备 C 可以使设备 A 和设备 B 中的对应 ARP 表项对应关系不正确。使用的策略是，不断向网络中广播 ARP 应答。此应答使用的 IP 地址是 IPA 和 IPB，而 MAC 地址是 MACC，这样，设备 A 中就会存在 ARP 表项(IPB、MACC)，设备 B 中就会存在 ARP 表项(IPA, MACC)。这样，设备 A 和 B 之间的通信就变成了和设备 C 之间的通信，而设备 A、B 对此都一无所知。设备 C 充当了中间人的角色，只需要把发给自己的报文做合适的修改，转给另一方即可。这就是有名的中间人攻击。

7.1.2 理解DAI和ARP 欺骗攻击

DAI 确保了只有合法的 ARP 报文才会被设备转发。它主要执行以下几个步骤：

- 在打开 DAI 检查功能的 VLAN 所对应的非信任端口上拦截住所有 ARP 请求和应答报文
- 在做进一步相关处理之前，根据 DHCP 数据库的设置，对拦截住的 ARP 报文进行合法性检查。
- 丢弃没有通过检查的报文。
- 检查通过的报文继续做相应的处理，送给相应的目的地。
- ARP 报文是否合法的依据是 DHCP snooping binding 数据库，具体请参考《DHCP snooping 配置指导》。

7.1.3 接口信任状态和网络安全

基于设备上每一个端口的信任状态，对 ARP 报文作出相应的检查，从受信任端口接收到的报文将跳过 DAI 检查，被认为是合法的 ARP 报文； 而从非信任端口接收到的 ARP 报文，将严格执行 DAI 检查。

在一个典型的网络配置中，应该将连接到网络设备的二层端口设置为受信任端口，连接到主机设备的二层端口设置为非信任端口。

将一个二层端口错误的配置成非信任端口可能会影响到网络正常通信。

具体配置命令请参考 **ip arp inspection trust**，**show ip arp inspection interface**。

7.2 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（必须）
- 设置端口的 ARP 报文最大接收速率（可选）
- DHCP snooping database 相关配置（可选）

7.2.1 启用指定VLAN的DAI报文检查功能

如果没有启用了 VLAN vid 的 DAI 报文检查功能，vlan-id = vid 的 ARP 报文会跳过 DAI 相关的安全检查（不会跳过 ARP 报文限速）。

可以通过 **show ip arp inspection vlan** 查看所有 VLAN 是否启用了 DAI 报文检查功能

要配置 VLAN 的 DAI 报文检查功能，在接口配置模式中执行以下命令：

命令	作用
Ruijie(config)# **ip arp inspection vlan** *vlan-id*	启用 VLAN *vlan-id* 的 DAI 报文检查功能开关
Ruijie(config)# **no ip arp inspection vlan** [*vlan-id*]	关闭 VLAN *vlan-id* 的 DAI 报文检查功能开关。缺省情况下，所有 VLAN 的 DAI 报文检查功能是关闭的。 省略 *vlan-id* 时关掉所有 VLAN 的 DAI 报文检查功能

7.2.2 设置端口的信任状态

此功能应用在二层接口配置模式，且此二层接口为一个 SVI 的成员口。

如果端口是可信任的，ARP 报文将跳过进一步的检查，否则，会使用 DHCP snooping 数据库的信息来检查当前 ARP 报文的合法性

> 上联端口一般设置为信任口，下联端口一般设置为非信任口。因为上联设备不会主动申请 IP 地址，则不会形成上联设备对应的 DHCP snooping 数据库信息。

要设置端口信任状态，在接口配置模式中执行以下命令：

命令	作用
Ruijie(config-if)# **ip arp inspection trust**	设置端口是可信任的
Ruijie(config-if)# **no ip arp inspection trust**	设置端口是不可信任的。缺省情况下，所有二层端口都是不可信任的。

7.2.3 DHCP snooping database相关配置

参考《DHCP Snooping 配置指导》。

如果没有配置 DHCP Snooping database，则所有 ARP 报文通过检查

7.3 显示DAI

7.3.1 显示VLAN是否启用DAI功能

要显示各 VLAN 的启用状态，在全局配置模式中执行以下命令：

命令	作用
show ip arp inspection vlan	显示各 VLAN 的启用状态

7.3.2 显示各二层接口DAI配置状态

要显示各二层接口 DAI 配置状态，在全局配置模式中执行以下命令：

命令	作用

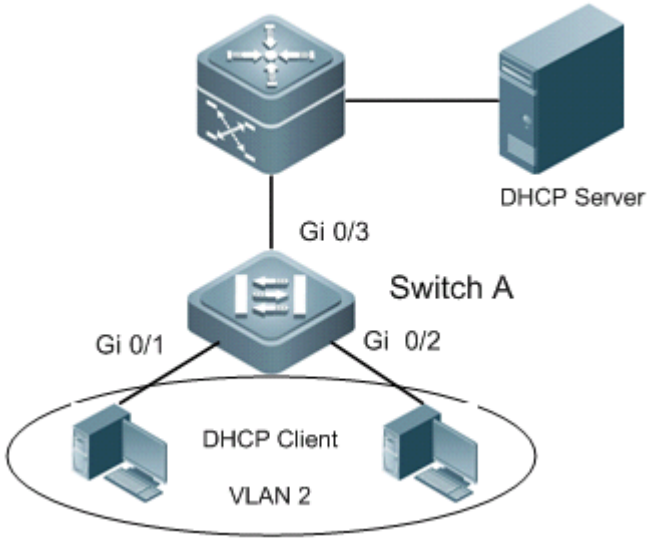
show ip arp inspection interface	显示各二层接口的 DAI 配置（包括信任状态，和速率限制）

支持 NFPP(网络基础保护策略)的产品，速率限制由 NFPP 完成，不再通过 DAI 进行设置，因此上述命令只显示接口的信任状态。

7.4 DAI典型配置用例

拓扑图

图 12-2



应用需求

如上图所示，用户 PC 的 IP 地址是 DHCP 服务器自动分配的，为了保证用户能够正常上网，有如下要求：

1) 用户 PC 只能从指定的 DHCP 服务器获取 IP 地址，不允许私设 DHCP 服务器。

2) 用户 PC 只能使用合法 DHCP 服务器分配的 IP 地址上网，不允许随意设置 IP 地址。

配置要点

- 在接入交换机（本例为 Switch A）上启用 DHCP Snooping 并将连接合法 DHCP 服务器的上链口（本例为 GigabitEthernet 0/3）设置为信任口可满足第一个需求。
- 在接入设备（本例为 Switch A）启用 DHCP Snooping 基础上再开启 DAI，可满足第二需求。

在汇聚或核心交换上如有其他 PC 接入并存在私设 DHCP 服务器可能，也需要开启 DHCP Snooping。

配置步骤

- 配置 Switch A

第一步，设置直连用户 PC 的端口的 VLAN。

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#interface range gigabitEthernet 0/1-2
Ruijie(config-if-range)#switchport access vlan 2
```

第二步，开启 DHCP SNOOPING 功能。

```
Ruijie(config-if-range)#exit
Ruijie(config)#ip dhcp snooping
```

第三步，在对应的 VLAN 上开启 DAI 功能。

```
Ruijie(config)#ip arp inspection vlan 2
```

第四步，将上链口设置为 DHCP SNOOPING 信任口

```
Ruijie(config)#interface gigabitEthernet 0/3
Ruijie(config-if-GigabitEthernet 0/3)#ip dhcp snooping trust
```

第五步，将上链口设置为 DAI 信任口。

```
Ruijie(config-if-GigabitEthernet 0/3)#ip arp inspection trust
```

配置验证

第一步，确认配置是否正确，关注点为 DHCP Snooping/DAI 是否启用，信任接口是否正确。

```
Ruijie#show running-config
ip dhcp snooping
!
ip arp inspection vlan 2
!
interface GigabitEthernet 0/1
 switchport access vlan 2
!
interface GigabitEthernet 0/2
 switchport access vlan 2
!
interface GigabitEthernet 0/3
ip dhcp snooping trust
 ip arp inspection trust
```

第二步，查看 DHCP SNOOPING 的使能状态以及对应的信任端口，关注点为上链口是否设置为可信任接口。

```
Ruijie#show ip dhcp snooping
Switch DHCP snooping  status                    :   ENABLE
DHCP snooping  Verification of hwaddr status    :   DISABLE
DHCP snooping database write-delay time         :   0 seconds
DHCP snooping option 82 status                  :   DISABLE
```

```
DHCP snooping Support bootp bind status         :   DISABLE
Interface                       Trusted       Rate limit (pps)
------------------------        -------       ----------------
GigabitEthernet 0/3             YES           unlimited
```

第三步，查看 DAI 状态，关注点为对应的 VLAN 的使能情况和上链口是否设置为可信任接口。

```
Ruijie#show ip arp inspection vlan
Vlan     Configuration
----     -------------
2         Enable
Ruijie#show ip arp inspection interface
       Interface         Trust State
---------------------    -----------
GigabitEthernet 0/1      Untrusted
GigabitEthernet 0/2      Untrusted
GigabitEthernet 0/3      Trusted
```

如果需要查看 DHCP Snooping 形成的数据库绑定信息，可以通过 **show ip dhcp snooping binding** 命令，在此不再列举。

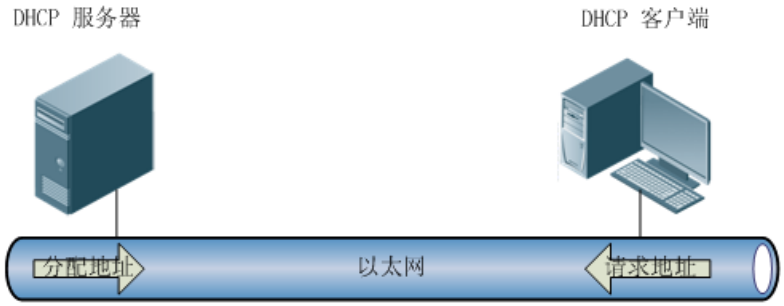
8 IP Source Guard

8.1 IP Source Guard简介

8.1.1 理解DHCP

在典型的 DHCP 环境中，DHCP 服务器负责网络中地址的管理和分配，网络中的主机如果想要使用网络资源，必须向 DHCP 服务器申请合法的网络地址，只有获得了合法地址的客户端才能正常使用网络；

图 13-1 正常的 DHCP 地址分配



然而仅仅依靠服务器/客户端这种模型完全无法保证网络中地址资源的有效管理，以及地址管理的安全性；来自客户端的攻击[非法报文]，以及网络中可能存在的各种伪装服务器，对传统的 DHCP 模型提出了更高的安全要求；

DHCP Snooping 的引入解决这一问题，在连接 DHCP 服务器与客户端的设备上开启 DHCP Snooping 功能，就可以解决传统 DHCP 模型中的大部分安全；DHCP Snooping 将网络分为两个部分：客户端网络-非信任网络，对来自该网络上的客户端请求进行安全检测；服务器网络-信任网络，将收到的合法的客户端请求转发到配置的信任服务器网络，由服务器完成地址的统一管理分配；通过这种方式，DHCP Snooping 解决了传统 DHCP 模型中的几个典型的安全问题：

图 13-2 存在伪装 DHCP 服务器的网络

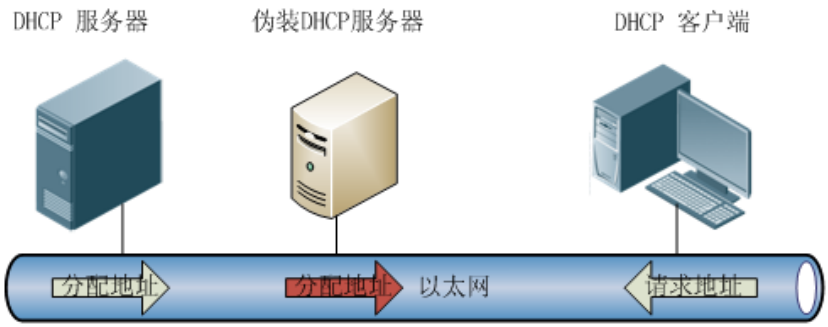


图 13-3 存在伪装 DHCP 客户端进行攻击的网络

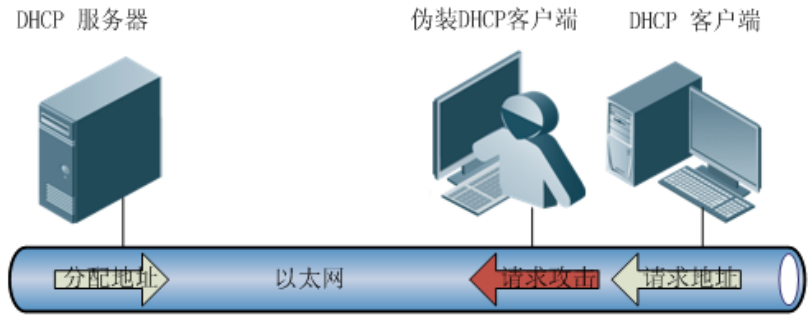
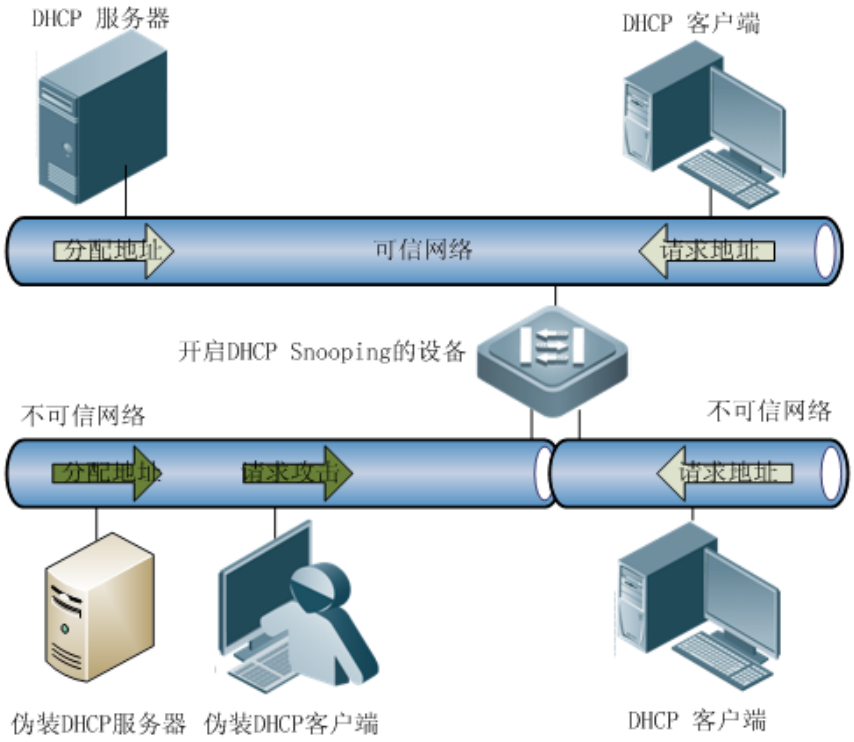


图 13-4 通过 DHCP Snooping 进行保护的网络



然而，虽然依靠 DHCP Snooping 的过滤，最大限度的过滤了来自客户端的攻击，杜绝了网络中的伪装服务器；但却无法对客户端网络中的非 DHCP 客户端进行有效的限制，也就是说无法检测有私设 IP 的客户端，这在一个纯 DHCP 的网络应用中，是无法接受的；为了防止这种 DHCP 网络中客户端私设 IP，可以在连接服务器与客户端网络之间的设备上开启 IP Source Guard 功能，IP Source Guard 是基于 DHCP Snooping 的，在 DHCP 模型中可以有效的保证网络中 DHCP 客户端能够正常使用网络。

8.1.2 理解IP Source Guard

IP Source Guard 维护一个 IP 源地址绑定数据库， IP Source Guard 可以在对应的接口上对主机报文进行基于源 IP、源 IP 加源 MAC 的报文过滤，从而保证只有 IP 源地址绑定数据库中的主机才能正常使用网络；

IP Source Guard 之所以在 DHCP 使用中能够有效的安全控制，这主要取决于 IP 源地址绑定数据库，IP Source Guard 会自动将 DHCP Snooping 绑定数据库中的合法用户绑定同步到 IP Source Guard 的 IP 源地址绑定数据库，这样 IP Source Guard 就可以在打开 DHCP Snooping 的设备上对客户端的报文进行严格过滤。

默认情况下，打开 IP Source Guard 功能的端口会过滤所有非 DHCP 的 IP 报文；只有当客户端通过 DHCP 从服务器获取到合法的 IP 或者管理员为客户端配置了静态的 IP 源地址绑定后，端口才允许和这个客户端匹配的 IP 报文通过。

IP Source Guard 支持基于 IP+MAC 或者基于 IP 的过滤，如果打开基于 IP+MAC 的过滤，IP Source Guard 会对所有报文的 MAC+IP 进行检测，仅仅允许 IP 源地址绑定表格中存在的用户报文通过；而基于 IP 的过滤，仅仅会对报文的源 IP 地址进行检测。

在支持 ARP Check 功能的交换机系统上，开启 IP Source Guard 功能和 ARP Check 功能后，交换机能使用 IP Source Guard 对 IP 报文进行 IP＋MAC 或仅源 IP 过虑， ARP Check 功能对 ARP 报文中的 Sender IP+Sender MAC 或仅对 Sender IP 检查过虑。

IP Source Guard 的相关过滤功能都是基于硬件实现的，接口上的 IP Source Guard 过滤规则可以理解为基于接口的可以动态改变的 ACL，各系列产品的过滤表容量存在差异，因此在规划 IP Source Guard 应用之前请参看相关产品规格说明。

8.1.3 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。

8.2 IP Source Guard配置

8.2.1 配置接口IP Source Guard功能

缺省情况下，接口的 IP Source Guard 功能是关闭的，接口下联的所有用户都可以使用网络；打开接口 IP Source Guard 功能之后，将会根据 IP 源地址绑定数据库对接口下联客户端进行过滤

命令	作用
Ruijie(config)# **interface interface**	进入接口配置模式
Ruijie(config-if-*type ID*)# [**no**] **ip verify source** [*port-security*]	打开接口上的 IP Source Guard 功能 默认为基于仅 IP 的过虑 port-security 将配置基于 IP+MAC 的过滤

下边是配置打开接口 1 的 IP Source Guard 功能：

```
Ruijie(config)# interface FastEthernet 0/1
Ruijie(config-if)# ip verify source
Ruijie(config-if)# end
```

- IP Source Guard 功能和 DHCP Snooping 功能结合应用，该功能仅仅在 DHCP Snooping 控制范围的接口上生效;
- IP Source Guard 功能仅仅在 DHCP Snooping 控制的非信任口上生效。
- IP Source Guard 支持在 AP 口上配置，但不支持在 AP 成员端口上配置。

8.2.2 配置静态IP源地址绑定用户

在某些应用情况下，某些端口下的用户希望能够静态使用某些 IP，就可以通过添加静态用户信息到 IP 源地址绑定数据库中来实现

命令	作用
Ruijie(config)# [**no**] **ip source binding mac-address vlan** *vlan_id ip-address* [**interface** *interface-id* **| ip-mac | ip-only**]	配置静态的 IP 源地址绑定用户到数据库。当没有接口选项时，绑定表项在 VLAN 内的所有绑定端口上生效。 **interface**：绑定到接口； **ip-mac**：全局绑定为 IP+MAC 绑定； **ip-only**：全局绑定为仅 IP 绑定。

下边是添加一个静态的用户到设备的 9 端口：

```
Ruijie# configure terminal
Ruijie(config)# ip source binding 00d0.f801.0101 vlan 1 192.168.4.243 interface FastEthernet 0/9
```

端口必需在 **vlan** *vlan_id* 参数所指定的 VLAN 中，否则无法进行有效的用户绑定。

8.3 IP Source Guard配置显示

8.3.1 显示IP Source Guard过滤表项

您可以通过以下步骤显示 IP Source Guard 过滤表项

命令	作用
show ip verify source [**interface** *interface*]	显示 IP Source Guard 过滤表项

例如：

```
Ruijie # show ip verify source
Interface       Filter-type Filter-mode Ip-address  Mac-address  VLAN
---------------   ---------   -----------  ----------  ----------- ------
FastEthernet 0/3  ip       active     3.3.3.3                1
FastEthernet 0/3  ip       active     deny-all
FastEthernet 0/4    ip+mac     active        4.4.4.4    0000.0000.0001    1
FastEthernet 0/4    ip+mac     active        deny-all
```

8.3.2 显示IP源地址绑数据库信息

您可以通过以下步骤显示 IP 源地址数据库信息的相关内容

命令	作用

show ip source binding [*ip-address*] [*mac-address*] [**dhcp-snooping**] [**static**] [**vlan** *vlan-id*] [**interface** *interface-id*]	查看 IP 源地址绑定数据库

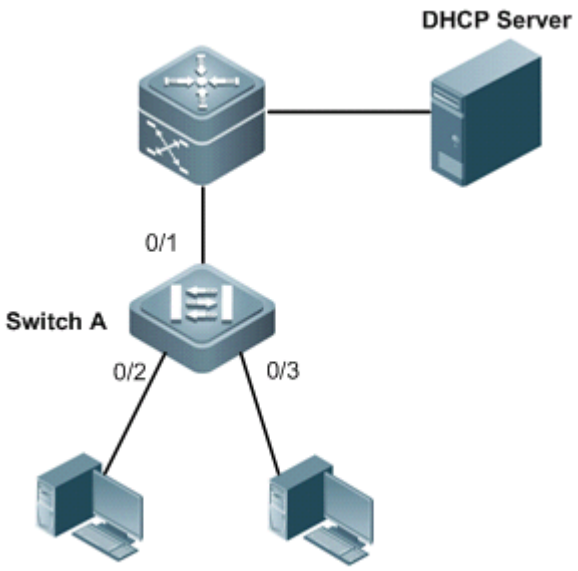
例如：

```
Ruijie# sh ip source binding
MacAddress      IpAddress     Lease(sec)  Type       VLAN  Interface
-----------     ----------    ----------  -------    ----  ------
0000.0000.0001  1.0.0.1       infinite     static    1     FastEthernet2/1
Total number of bindings: 1
```

8.4 IP Source Guard配置用例

拓扑图

图 13-5 DHCP 部署环境



应用需求

用户只能使用合法 DHCP 服务器动态分配或管理员静态分配的 IP 地址访问网络，源 IP 地址与交换机硬件过滤列表中的 IP 地址不匹配的 IP 报文被阻断，保证网络安全

配置要点

在接入设备（本例为 Switch A）上配置 IP Source Guard 和 DHCP Snooping 组合功能可满足需求：

1) 设置上链口（本例为 GigabitEthernet 0/1）为信任口，避免 DHCP 服务器欺骗

2) 在直连 PC 的端口上（本例为 GigabitEthernet 0/2 、GigabitEthernet 0/3）启用 IP Source Guard 功能

3) 管理员指定 IP 地址的用户可通过 IP Source Guard 静态绑定来实现（本例静态绑定 IP 地址为 192.168.216.4、MAC 地址为 0000.0000.0001）

配置步骤

- 配置 Swtich A

第一步，开启 DHCP Snooping 功能。

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

第二步，将上链口设置为 DHCP SNOOPING 信任口。

```
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#ip dhcp snooping trust
Ruijie(config-if-GigabitEthernet 0/1)#exit
```

第三步，在直连 PC 的端口上开启 IP Source Guard 功能

```
Ruijie(config)#interface range gigabitEthernet 0/2-3
Ruijie(config-if-range)#ip verify source port-security
Ruijie(config-if-range)#exit
```

第四步，配置静态绑定用户

```
Ruijie(config)#ip source binding 0000.0000.0001 vlan 1 192.168.216.4 interface gigabitEthernet 0/2
```

配置验证

第一步，查看 Switch A 的配置情况，关注点：是否开启 DHCP Snooping、是否将上链口配置为信任口、是否在直连用户的端口上开启 IP Source Guard 功能以及静态绑定用户的表项是否正确

```
Ruijie#show running-config
ip dhcp snooping
!
ip source binding 0000.0000.0001 vlan 1 192.168.216.1 interface GigabitEthernet 0/2
!
interface GigabitEthernet 0/1
 ip dhcp snooping trust
!
interface GigabitEthernet 0/2
 ip verify source port-security
!
interface GigabitEthernet 0/3
 ip verify source port-security
```

第二步，查看 DHCP Snooping 用户绑定数据库

```
Ruijie#show ip dhcp snooping binding
Total number of bindings: 2
MacAddress          IpAddress       Lease(sec)   Type           VLAN  Interface
------------------ --------------- ------------ -------------
0013.2049.9014      192.168.216.4   86233        dhcp-snooping 1     GigabitEthernet 0/3
00e0.4c70.b7e2      192.168.216.3   86228        dhcp-snooping 1     GigabitEthernet 0/2
```

第三步，查看通过 DHCP Snooping 用户绑定数据库和静态绑定用户共同生成的 IP 硬件过滤库：

```
Ruijie#show ip source binding
MacAddress          IpAddress       Lease(sec)   Type           VLAN  Interface
------------------ --------------- ------------ -------------
0000.0000.0001      192.168.216.4   infinite     static         1     GigabitEthernet 0/2
0013.2049.9014      192.168.216.4   86176        dhcp-snooping 1     GigabitEthernet 0/3
00e0.4c70.b7e2      192.168.216.3   86171        dhcp-snooping 1     GigabitEthernet 0/2
Total number of bindings: 3
```

第四步，查看 IP Source Guard 过滤表项如下：

```
Ruijie#show ip verify source
Interface            Filter-type Filter-mode Ip-address      Mac-address    VLAN
-------------------- ----------- ----------- --------------- -------------- --------
GigabitEthernet 0/2  ip+mac      active      192.168.216.4   0000.0000.0001  1
GigabitEthernet 0/2  ip+mac      active      192.168.216.3   00e0.4c70.b7e2  1
GigabitEthernet 0/2  ip+mac      active      deny-all        deny-all
GigabitEthernet 0/3  ip+mac      active      192.168.216.4   0013.2049.9014  1
GigabitEthernet 0/3  ip+mac      active      deny-all        deny-all
```

9 防网关 ARP 欺骗

9.1 概述

在交换机上，默认情况下 ARP 报文是在本 VLAN 内广播的，因此这就为针对网关的 ARP 欺骗提供了机会。

针对网关的 ARP 欺骗是指用户 A 发送 ARP 报文请求网关的 MAC 地址，这时处于同一 VLAN 的用户 B 也会收到该 ARP 报文，因此用户 B 可以发送 ARP 响应报文，将报文的源 IP 填为网关 IP，而源 MAC 填为自己的 MAC 地址。用户 A 收到该 ARP 响应后，就会认为用户 B 的机器就是网关，因此用户 A 通讯中发往网关的报文都将发往用户 B， 这样用户 A 的通讯实际上都被截取了，造成 ARP 欺骗的效果。

因此我们可以在交换机的逻辑端口(包括物理端口与及 AP 口)上配置防网关 ARP 欺骗来防止针对网关的 ARP 欺骗。防网关 ARP 欺骗配置后，可以在逻辑端口上检查 ARP 报文的源 IP 是否是我们配置的网关 IP，如果是，则将该报文丢弃，防止用户收到错误的 ARP 响应报文。 这样只有交换机上连设备能够下发网关的 ARP 报文，其它 PC 发送的假冒网关 ARP 响应报文将被交换机过滤。

9.2 配置防网关ARP欺骗

9.2.1 设置防网关ARP欺骗

设置防网关 ARP 欺骗地址。

命令	作用
Ruijie(config-if)# **anti-arp-spoofing ip** *ip-address*	在逻辑端口下配置防网关 ARP 欺骗，网关 IP 地址为指定 IP。

你可以在端口配置模式下通过命令 **no anti-arp-spoofing ip** *ip-address* 来将防网关 ARP 配置清除。

在上链口上不能配置防网关 ARP 欺骗。

9.2.2 查看防网关ARP欺骗信息

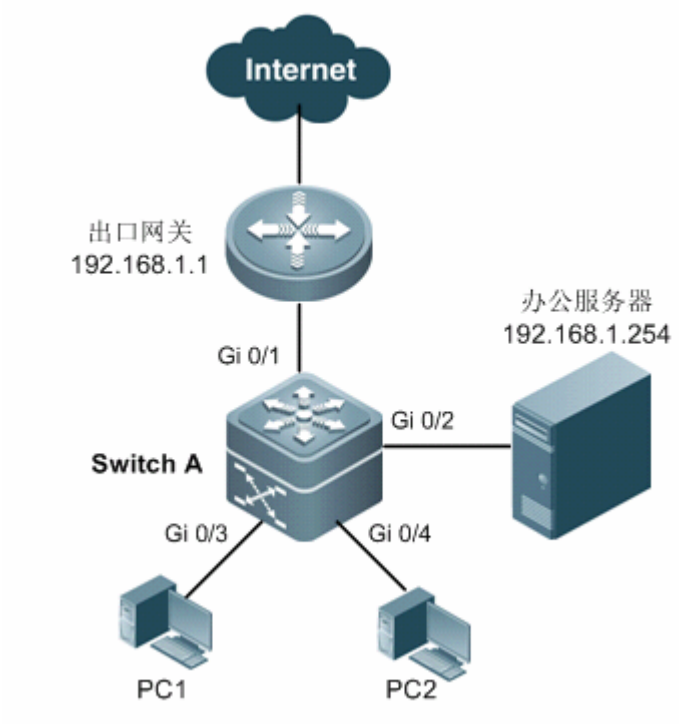
查看交换机的防网关 ARP 欺骗信息。

命令	作用
show anti-arp-spoofing	显示所有接口下的防网关 arp 欺骗信息

9.3 配置举例

拓扑图

图 16-1 防网关 ARP 欺骗典型拓扑



应用需求

上图为中小型公司或单位的简化典型网络拓扑，PC 用户通过接入设备 Switch A 访问办公服务器，以及通过网关设备连接外网。如果存在非法用户冒充网关 IP 地址或服务器 IP 地址进行 ARP 欺骗，将导致其它用户无法正常上网以及访问服务器。

基于以上应用分析，组网需求如下：

- 阻断伪造网关和内网服务器 ARP 欺骗报文，保证用户能正常上网

配置要点

在接入交换机（本例为 Switch A）直连 PC 的端口(本例为 Gi 0/3, Gi 0/4)上启用防网关欺骗，网关地址为内网网关地址和内网服务器地址。

上链口、连接出口网关或服务器的端口不能启用防网关欺骗，否则将导致源地址为网关 IP 或服务器 IP 的 ARP 报文被阻断，造成网络不通

如果端口不够，需在接入交换机下挂一台 8 口的 hub（集线器），也可在接入交换机上开启防网关欺骗，缺陷是同一台 hub 上的电脑之间的网关 ARP 欺骗无法阻断。

配置步骤

第一步，在直连电脑的端口上启用防网关欺骗

```
SwitchA# configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)#interface range gigabitEthernet 0/2-4
SwitchA(config-if-range)# anti-arp-spoofing ip 192.168.1.1
SwitchA(config-if-range)# anti-arp-spoofing ip 192.168.1.254
```

配置验证

第一步，确认配置是否正确，关注点：是否启用防网关欺骗、网关地址是否正确、上链口是否启用防网关欺骗

```
SwitchA (config-if)#show running-config
interface GigabitEthernet 0/1
!
interface GigabitEthernet 0/2
 anti-arp-spoofing ip 192.168.1.1
 anti-arp-spoofing ip 192.168.1.254
!
interface GigabitEthernet 0/3
 anti-arp-spoofing ip 192.168.1.1
 anti-arp-spoofing ip 192.168.1.254
!
interface GigabitEthernet 0/4
 anti-arp-spoofing ip 192.168.1.1
 anti-arp-spoofing ip 192.168.1.254
!
```

第二步，查看防网关欺骗状态，再次确认。关注点同第一步

```
SwitchA#show anti-arp-spoofing
Anti-arp-spoofing
port           ip
-------        -------
Gi 0/2         192.168.1.1
Gi 0/2         192.168.1.254
Gi 0/3         192.168.1.1
Gi 0/3         192.168.1.254
Gi 0/4         192.168.1.1
Gi 0/4         192.168.1.254
```

第三步，如果可能，将 PC1 的 IP 地址配置为网关的 IP 地址，然后观察网关是否报告 IP 地址冲突，PC2 是否能正常上网。

如果一切正常，说明防网关欺骗配置生效。

10 NFPP

10.1 概述

网络基础保护策略 (Network Foundation Protection Policy)，简称 NFPP。

10.1.1 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。

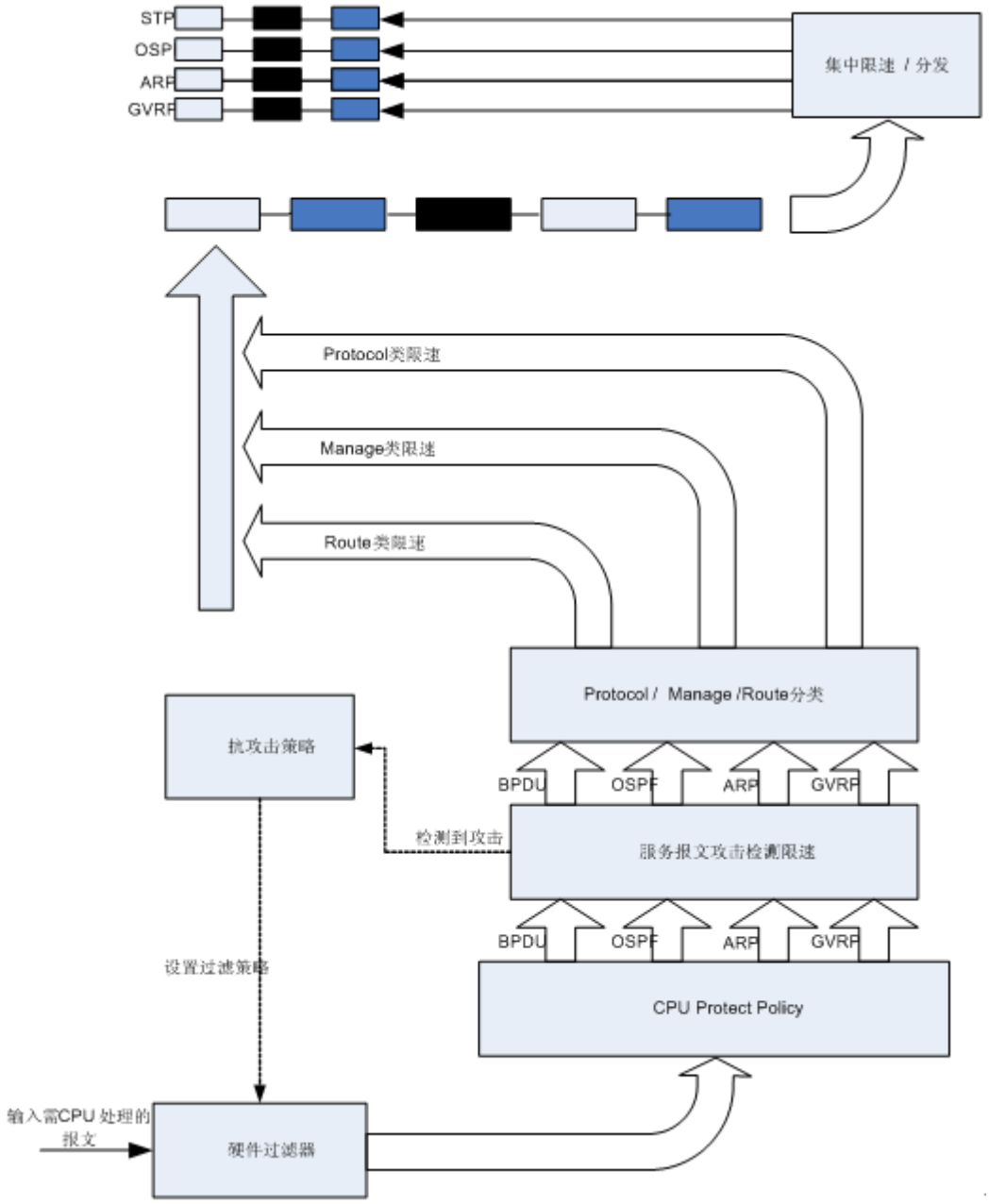
10.1.2 NFPP的原理

如下图所描述的，NFPP 系统处理数据流时，需要经过硬件过滤、CPU Protect Policy（简称 CPP）、报文攻击检测/限速、Protocol/Manage/route 流分类和集中限速等几个流程，并最终交给各个应用模块处理。

首先，需要进行 CPP 的分类和限速，这样 CPU 处理的数据流不仅根据 CPP 的服务分类原则进行了分类，而且这些服务报文还经过了硬件和软件的限速，从而避免了不同的服务报文之间相互抢占带宽，有效地解决了某一种服务报文的大流量攻击情况下，其他服务报文无法及时得到处理的问题。例如设备中同时存在 OSPF 服务报文和 BPDU 服务报文时，当其中某一个服务报文需要消耗大量 CPU 带宽的情况下，可以保证另一个服务报文的接收不受影响。

> 为了最大限度地利用 NFPP 中抗攻击功能，请根据具体的应用环境修改 CPU Protect Policy 中各种服务的限速值，也可以使用系统提供的推荐配置，这些推荐值可以通过命令 **show cpu-protect summary** 查看。

图 17-1 NFPP 系统的数据流向图



然后，针对报文所属的服务类型，对具体的报文服务类型实施不同的监控方式和策略，NFPP 提供各种服务监控水线和策略的配置，管理员可以根据具体的网络环境灵活配置某一个服务报文的告警水线和限速水线，这些水线的设置可以基于端口，也可以基于网络中的主机，这里的告警水线是指当端口或者某台主机的某种服务报文接收速率达到需要向管理员发出警告或者进行隔离的阈值；限速水线是指当端口或者某台主机的某种服务报文接收速率达到需要进行限速的阈值。告警或者隔离动作是在检测到攻击后交由抗攻击策略执行的。如果是隔离，抗攻击策略会利用硬件的过滤器实现，这样保证该攻击报文不会再被送到 CPU 处理，从而保证了设备正常运行。

- NFPP 在检测到某种服务的某个具体报文的攻击后，可以向管理员发出告警信息，但是为了防止告警信息频繁出现，如果攻击流持续存在，NFPP 在发出告警后的连续 60 秒时间内不再重复告警。
- 防止频繁打印日志消耗 CPU 资源，NFPP 把攻击检测的日志信息写到缓冲区，然后以指定速率从缓冲区取出来打印。NFPP 对 TRAP 没有限速。

监控后的服务报文再经过 Protocol/Manage/Route 流分类，这里的分类是指将 CPP 中定义的各种服务按照管理类(Manage) 、转发类(Route)和协议类(Protocol)的原则进行的分类（具体分类如表 1 所列），每一类都拥有独立的带宽，不同类别之间的带宽不能共享，超过带宽阈值的流将被丢弃。这样将不同的服务区分类别后，可以保证属于某类的各种服务报文在设备上得到优先处理。NFPP 允许管理员根据实际的网络环境灵活分配三类报文的带宽，从而保障 protocol 类和 manage 类能得到优先处理，protocol 类的优先处理保证了协议的正确运行，而 manage 类的优先处理保证了管理员能够实施正常管理，从而保障了设备的各种重要功能的正常运行，提高设备的抗攻击能力。

三种属性分类	CPU Protect Policy 中定义服务类型 （服务类型具体含义参见 CPU Protect Policy 配置指南）
Protocol	tp-guard，dot1x，rldp，rerp，slow-packet，bpdu，isis dhcps，gvrp，ripng，dvmrp，igmp，mpls，ospf, pim， rip，vrrp，ospf3，dhcp-relay-s，dhcp-relay-c，option82，tunnel-bpdu，tunnel-gvrp
Route	unknown-ipmc， 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。

10.2 配置NFPP

10.2.1 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。

10.2.2 配置每类报文允许的最大带宽

在配置模式下，按如下步骤设置每类报文的流量带宽：

命令	作用
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**cpu-protect sub-interface { manage | protocol|route} pps** *pps_vaule*	设置报文对应的队列的限速水线，*pps* 为整数。有效值范围是 1-8192
Ruijie(config)#**end**	退回到特权模式。
Ruijie#**show running-config**	查看全局配置
Ruijie#**copy running-config startup-config**	保存配置。

10.2.3 配置每类报文占用队列的最大百分比

在配置模式下，按如下步骤设置每种类型报文占用队列的百分比：

命令	作用
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**cpu-protect sub-interface { manage | protocol | route} percent** *percent_vaule*	设置报文对应的类型所占的队列的百分比，*percent _vaule* 为整数。有效值范围是 1-100
Ruijie(config)#**end**	退回到特权模式。
Ruijie#**show running-config**	查看全局配置
Ruijie#**copy running-config startup-config**	保存配置。

配置某类型所占百分比的有效值区间，必须小于等于百分之百减去其它两种类型百分比之和的差值。

10.3 ARP抗攻击

10.3.1 ARP抗攻击简介

在局域网中，通过 ARP 协议把 IP 地址转换为 MAC 地址。ARP 协议对网络安全具有重要的意义。通过网络向网关发送大量非法的 ARP 报文，造成网关不能为正常主机提供服务，这就是基于 ARP 的拒绝服务攻击。对于这种攻击，防范措施是一方面对 ARP 报文限速，另一方面检测出攻击源，对攻击源头采取隔离措施。

ARP 攻击识别分为基于主机和基于物理端口两个类别。基于主机又细分为基于源 IP 地址/VLAN ID/物理端口和基于链路层源 MAC 地址/ VLAN ID /物理端口。每种攻击识别都有限速水线和告警水线。当 ARP 报文速率超过限速水线时，超限报文将被丢弃。当 ARP 报文速率超过告警水线时，将打印警告信息，发送 TRAP，基于主机的攻击识别还会对攻击源头采取隔离措施。

ARP 抗攻击还能检测出 ARP 扫描。ARP 扫描是指链路层源 MAC 地址固定而源 IP 地址变化，或者链路层源 MAC 地址和源 IP 地址固定而目标 IP 地址不断变化。由于存在误判的可能，对检测出有 ARP 扫描嫌疑的主机不进行隔离，只是提供给管理员参考。

需要说明的是，ARP 抗攻击只是针对攻击交换机本身的 ARP 拒绝服务服务攻击，而不是针对 ARP 欺骗或者是解决网络中的 ARP 攻击问题。

10.3.2 打开ARP抗攻击功能

您可以在 **nfpp** 配置模式或者接口配置模式下打开 ARP 抗攻击功能，缺省情况下是打开的。

命令	作用
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**nfpp**	进入 NFPP 配置模式。
Ruijie(config-nfpp)#**arp-guard enable**	全局打开 ARP 抗攻击功能，缺省情况下打开。
Ruijie(config-nfpp)#**end**	退回到特权模式。
Ruijie#**configure terminal**	进入全局配置模式。

Ruijie(config)#**interface** *interface-name*	进入接口配置模式。
Ruijie(config-if)#**nfpp arp-guard enable**	在端口上打开 ARP 抗攻击功能，缺省情况是端口没有配置局部开关，采用全局开关。
Ruijie(config-if)#**end**	退回到特权模式。
Ruijie#**show nfpp arp-guard summary**	核对配置参数
Ruijie#**copy running-config startup-config**	保存配置。

当关闭 ARP 抗攻击功能时，系统将自动清除受监控的主机和扫描主机。

10.3.3 设置对攻击者的隔离时间

对攻击者的隔离时间分为全局隔离时间和基于端口的隔离时间（即局部隔离时间）。对于某个端口，如果没有配置基于端口的隔离时间，那么采用全局隔离时间；否则，采用基于端口的隔离时间。

命令	作用
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**nfpp**	进入 NFPP 配置模式
Ruijie(config-nfpp)#**arp-guard isolate-period** [*seconds* | **permanent**]	配置对攻击者的全局隔离时间。 取值范围为 0 秒，30 秒到 86400 秒（即一天），缺省值为 0 秒，表示不隔离；**permanent** 表示永久隔离。
Ruijie(config-nfpp)#**end**	返回特权模式
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**interface** *interface-name*	进入接口配置模式。
Ruijie(config-if)#**nfpp arp-guard isolate-period** [*seconds* | **permanent**]	在端口上配置对攻击者的隔离时间。 取值范围为 0 秒，180 秒到 86400 秒（即一天），缺省情况是没有配置局部隔离时间，采用全局隔离时间。0 秒表示不隔离；**permanent** 表示永久隔离。
Ruijie(config-if)#**end**	退回到特权模式。
Ruijie#**show nfpp arp-guard summary**	核对配置参数
Ruijie#**copy running-config startup-config**	保存配置。

如果要把全局隔离时间恢复成缺省值，在 **nfpp** 配置模式执行命令“**no arp-guard isolate-period**”。如果一个端口原来配置了局部隔离时间，现在想采用全局隔离时间，那么在端口配置模式下执行命令“**no nfpp arp-guard isolate-period**”把局部隔离时间配置删除。

10.3.4 设置对攻击者的监控时间

如果隔离时间为 0（即不隔离），防攻击模块将自动根据配置的监控时间对攻击者进行软件监控，提供当前系统中存在哪些攻击者的信息。当把隔离时间配置成非零值后，防攻击模块将自动对软件监控的主机采取硬件隔离。

命令	作用
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**nfpp**	进入 NFPP 配置模式

Ruijie(config-nfpp)#**arp-guard monitor-period** *seconds*	配置对攻击者的监控时间。 取值范围为 180 秒到 86400 秒（即一天），缺省值为 600 秒。
Ruijie(config-nfpp)#**end**	退回到特权模式。
Ruijie#**show nfpp arp-guard summary**	核对配置参数
Ruijie#**copy running-config startup-config**	保存配置。

如果要把监控时间恢复成缺省值，在 nfpp 配置模式执行命令“**no arp-guard monitor-period**”。

检测出攻击者的时候，如果隔离时间为 0，将对攻击者进行软件监控，超时为监控时间。在软件监控过程中，当隔离时间被配置为非零值时，将自动对软件监控的攻击者采取硬件隔离，并且把超时设置为隔离时间。监控时间在隔离时间为 0 的情况下才有意义。

如果把隔离时间从非零值改成零，将直接把相关端口的攻击者删除，而不是进行软件监控。

10.3.5 设置受监控主机的最大数目

命令	作用
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**nfpp**	进入 NFPP 配置模式。
Ruijie(config-nfpp)#**arp-guard monitored-host-limit** *number*	配置受监控主机的最大数目。 取值范围为 1 到 4294967295，缺省情况下受监控主机的最大数目为 1000 个。
Ruijie(config-nfpp)#**end**	退回到特权模式。
Ruijie#**show nfpp arp-guard summary**	核对配置参数
Ruijie#**copy running-config startup-config**	保存配置。

如果要把配置的受监控主机数恢复成缺省值，在 nfpp 配置模式执行命令“**no arp-guard monitored-host-limit**”。

如果受监控主机数已经达到默认的 1000 个，此时管理员把受监控主机的最大数目设置成小于 1000，不会删除已有的受监控主机，而是打印信息“%ERROR： The value that you configured is smaller than current monitored hosts 1000（配置的受监控主机数），please clear a part of monitored hosts.”来提醒管理员配置没有生效，需要删除部分已经被监控的主机。

当受监控主机表满时，打印日志“% NFPP_ARP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000（配置的受监控主机数） monitored hosts.”提醒管理员。

10.3.6 基于主机限速和识别攻击

识别主机有源 IP/VLAN ID/端口和链路层源 MAC/VLAN ID/端口两种识别方法。每台主机都有限速水线和攻击阈值（也称为告警水线），限速水线必须低于攻击阈值。当单台主机的 ARP 报文速度超过限速水线时，将丢弃这些超出限速水线的报文；如果单台主机的 ARP 报文速度超过攻击阈值，将采取隔离措施，记录到日志中，发送 TRAP。

支持识别 ARP 扫描，单位时间是 10 秒，缺省值是 15，如果 10 秒钟收到 15 个及以上 ARP 报文，链路层源 MAC 地址固定而源 IP 地址变化，或者链路层源 MAC 地址和源 IP 地址固定而目标 IP 地址不断变化，就认为有扫描嫌疑，将记录到日志中，发送 TRAP。

当检测到攻击行为时，打印的日志信息格式如下：

```
%NFPP_ARP_GUARD-4-DOS_DETECTED: Host<IP=N/A,MAC=0000.0000.0004,port=Gi4/1,VLAN=1> was
detected.(2009-07-01 13:00:00)
```

日志内容最后面括号中的时间是检测到攻击的时间。

发送的 TRAP 报文的数据中包含如下描述信息：

```
ARP DoS attack from host<IP=N/A,MAC=0000.0000.0004,port=Gi4/1,VLAN=1> was detected.
```

如果管理员把隔离时间配置成非零值，当硬件隔离成功时，打印的日志信息格式如下所示：

```
%NFPP_ARP_GUARD-4-ISOLATED:Host <IP=N/A,MAC=0000.0000.0004,port=Gi4/1,VLAN=1> was isolated.
(2009-07-01 13:00:00)
```

发送的 TRAP 报文的数据包含如下描述信息：

```
Host<IP=N/A,MAC=0000.0000.0004,port=Gi4/1,VLAN=1> was isolated.
```

当硬件隔离失败（原因通常是内存不足或者硬件资源不足）时，打印的日志信息格式如下所示：

```
%NFPP_ARP_GUARD-4-ISOLATE_FAILED: Failed to isolate host <IP=N/A,MAC=0000.0000.0004,port=Gi4/1,VLAN=1>.
(2009-07-01 13:00:00)
```

发送的 TRAP 报文的数据包含如下描述信息：

```
Failed to isolate host<IP=N/A,MAC=0000.0000.0004,port=Gi4/1,VLAN=1>.
```

当检测到 ARP 扫描时，打印的日志信息格式如下所示：

```
%NFPP_ARP_GUARD-4-SCAN: Host<IP=1.1.1.1,MAC=0000.0000.0004,port=Gi4/1,VLAN=1> was detected.
(2009-07-01 13:00:00)
```

发送的 TRAP 报文的数据包含如下描述信息：

```
ARP scan from host< IP=1.1.1.1,MAC=0000.0000.0004,port=Gi4/1,VLAN=1> was detected.
```

ARP 扫描表只保存最新的 256 条记录。当 ARP 扫描表满的时候，会打印日志提醒管理员：

```
%NFPP_ARP_GUARD-4-SCAN_TABLE_FULL: ARP scan table is full.
```

当管理员配置的限速水线大于攻击阈值时，打印命令提示信息“%ERROR：rate limit is higher than attack threshold 500pps(配置的攻击阈值).”提醒管理员。

当管理员配置的攻击阈值小于限速水线时，打印命令提示信息“%ERROR：attack threshold is smaller than rate limit 300pps(配置的限速水线).”提醒管理员。

- 对攻击者进行隔离，会设置一条策略到硬件中，但是硬件资源有限，当硬件资源耗尽的时候，会打印日志提醒管理员。
- 当无法为检测到的攻击者分配内存时，打印日志“%NFPP_ARP_GUARD-4-NO_MEMORY: Failed to alloc memory..”提醒管理员。
- ARP 扫描表只记录最新的 256 条记录。当 ARP 扫描表满了以后，最新记录将覆盖最旧记录。

管理员可以在 **nfpp** 配置模式和接口配置模式下进行配置。

命令	作用
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**nfpp**	进入 NFPP 配置模式
Ruijie(config-nfpp)#**arp-guard rate-limit {per-src-ip | per-src-mac}** *pps*	全局对每台主机的 ARP 报文速度进行限制。 取值范围是 1 到 9999，缺省值为 4 个。 “**per-src-ip**”是基于源 IP/VID/端口识别主机，“**per-src-mac**”是基于链路层源 MAC/VID/端口识别主机。
Ruijie(config-nfpp)#**arp-guard attack-threshold {per-src-ip | per-src-mac}** *pps*	全局配置攻击阈值。当某台主机的 ARP 报文超过攻击阈值时，就认为是在进行攻击，立即对这台主机采取隔离措施，记录到日志，发送 TRAP。 取值范围是 1 到 9999，缺省值为 8 个。 “**per-src-ip**”是基于源 IP/VID/端口识别主机，“**per-src-mac**”是基于链路层源 MAC/VID/端口识别主机。
Ruijie(config-nfpp)#**arp-guard scan-threshold** *pkt-cnt*	全局配置 ARP 扫描阈值，取值范围是 1 到 9999，缺省值为 15 个。单位值是 10 秒。如果 10 秒钟收到 15 个以上 ARP 报文，链路层源 MAC 地址固定而源 IP 地址变化，或者链路层源 MAC 地址和源 IP 地址固定而目标 IP 地址不断变化，就认为有扫描嫌疑。 ARP 扫描的特征是链路层源 MAC 地址固定而源 IP 地址变化，或者链路层源 MAC 地址和源 IP 地址固定而目标 IP 地址不断变化。
Ruijie(config-nfpp)#**end**	退回到特权模式。
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**interface** *interface-name*	进入接口配置模式。
Ruijie(config-if)#**nfpp arp-guard policy {per-src-ip | per-src-mac}** *rate-limit-pps attack-threshold-pps*	配置局部的限速水线和攻击水线，只在该配置所属端口上生效。 *rate-limit-pps* 是限速水线，取值范围是 1 到 9999，缺省是没配置基于端口的速率，采用全局的速率。 *attack-threshold-pps* 是攻击水线，取值范围是 1 到 9999。 缺省情况是端口没有自己的限速水线和攻击水线，采用全局的限速水线和限速水线。 “**per-src-ip**”是基于源 IP/VID/端口识别主机，“**per-src-mac**”是基于链路层源 MAC/VID/端口识别主机。
Ruijie(config-if)#**nfpp arp-guard scan-threshold** *pkt-cnt*	在每个端口上配置 ARP 扫描阈值，取值范围是 1 到 9999，缺省是没配置基于端口的 ARP 扫描阈值，采用全局 ARP 扫描阈值。单位值是 10 秒。
Ruijie(config-if)#**end**	退回到特权模式。
Ruijie#**show nfpp arp-guard summary**	核对配置参数
Ruijie#**copy running-config startup-config**	保存配置。

10.3.7 基于端口限速和识别攻击

每个端口都有限速水线和攻击阈值，限速水线必须低于攻击阈值。当某个端口的 ARP 报文速度超过限速水线时，就丢弃 ARP 报文。如果某个端口的 ARP 报文速度超过攻击阈值，将记录到日志中，发送 TRAP。

当端口遭受 ARP 拒绝服务攻击时，打印的警告信息格式如下：

```
%NFPP_ARP_GUARD-4-PORT_ATTACKED: ARP DoS attack was detected on port Gi4/1. (2009-07-01 13:00:00)
```

发送的 TRAP 报文的数据包含如下描述信息：

```
ARP DoS attack was detected on port Gi4/1.
```

管理员可以在 **nfpp** 配置模式和接口配置模式下进行配置。

命令	作用
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**nfpp**	进入 NFPP 配置模式
Ruijie(config-nfpp)#**arp-guard rate-limit per-port** *pps*	对每个端口的 ARP 报文速度进行限制。 取值范围是 1 到 9999，缺省值为 100 个。
Ruijie(config-nfpp)#**arp-guard attack-threshold per-port** *pps*	配置攻击阈值，当某个端口的 ARP 报文超过阈值时，记录到日志，发送 TRAP。 取值范围是 1 到 9999，缺省值为 200 个。
Ruijie(config-nfpp)#**end**	退回到特权模式。
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**interface** *interface-name*	进入接口配置模式。
Ruijie(config-if)#**nfpp arp-guard policy per-port** *rate-limit-pps attack-threshold-pps*	配置局部的限速水线和攻击水线，只在该配置所属端口上生效。 *rate-limit-pps* 是限速水线，取值范围是 1 到 9999。 *attack-threshold-pps* 是攻击水线，取值范围是 1 到 9999。 缺省情况是端口没有自己的限速水线和攻击水线，采用全局的限速水线和攻击水线。
Ruijie(config-if)#**end**	退回到特权模式。
Ruijie#**show nfpp arp-guard summary**	核对配置参数
Ruijie#**copy running-config startup-config**	保存配置。

- 基于 MAC 地址限速的优先级高于基于 IP 地址限速，而基于 IP 地址限速又高于基于端口限速。
- 为了使 ARP 抗攻击得到最佳的防攻击效果，建议管理员配置基于主机的限速水线和告警水线时遵循以下原则：
- 基于 IP 地址的限速水线 < 基于 IP 地址的告警水线 < 基于源 MAC 地址的限速水线 < 基于源 MAC 地址的告警水线。
- 配置端口限速水线时，可以参考这个端口上的主机数量，比如某个端口上有 500 台主机，那么可以把端口的限速水线设置成 500。

10.3.8 清除受监控主机

已被隔离的主机在一段时间后自动恢复，如果管理员要手动清除该主机，可以在特权模式下用以下命令清除。

命令	作用
Ruijie#**clear nfpp arp-guard hosts** [**vlan** *vid*] [**interface** *interface-id*] [*ip-address*	*mac-address*]	不带参数表示清除所有已被检测到攻击的主机，带参数表示清除符合条件的主机。

10.3.9 清除ARP扫描表

如果管理员要手动清除 ARP 扫描表，可以在特权模式下用以下命令清除。

命令	作用
Ruijie#**clear nfpp arp-guard scan**	清空 ARP 扫描表

10.3.10 查看ARP抗攻击的配置参数

使用 **show nfpp arp-guard summary** 查看 ARP 抗攻击的配置参数：

命令	作用
show nfpp arp-guard summary	查看 ARP 抗攻击配置参数

下面是一个例子：

```
Ruijie# show nfpp arp-guard summary
 (Format of column Rate-limit and  Attack-threshold is per-src-ip/per-src-mac/per-port.)
Interface  Status  Isolate-period Rate-limit Attack-threshold Scan-threshold
Global      Enable  300             4/5/60     8/10/100          15
G 0/1       Enable  180             5/-/-       8/-/-              -
G 0/2       Disable 200             4/5/60     8/10/100          20

Maximum count of monitored hosts: 1000
Monitor period：300s
```

字段 Interface 为 Global 表示全局配置。

字段 Status 表示是否打开抗攻击功能。

字段 Rate-limit 的格式为（对源 IP 地址的限速水线/对源 MAC 地址的限速水线/端口的限速水线值），字段 Attack-threshold 的显示格式类似。“-”表示没有配置。举例说明：

“4/5/60”表示对源 IP 地址的限速水线是 4，对源 MAC 地址的限速水线是 5，对每个端口的限速水线是 60。

G 0/1 这一行的字段 Rate-limit 为“5/-/-”，表示端口 G 0/1 对源 IP 地址的限速水线是 5，没有配置对源 MAC 地址的限速水线和端口的限速水线。

10.3.11 查看受监控主机的信息

命令	作用

show nfpp arp-guard hosts statistics	查看受监控主机表的统计信息，包括主机总数、隔离成功的主机数量和隔离失败的主机数量。
show nfpp arp-guard hosts [**vlan** *vid*] [**interface** *interface-id*] [*ip-address* |*mac-address*]	查看已被检测到攻击的主机。 不带参数表示显示所有已被检测到攻击的主机，带参数则只显示符合条件的主机。

```
Ruijie#show nfpp arp-guard hosts statistics
success    fail    total
-------    ----    -----
100          20        120
```

意思是：“总共有 120 台主机被隔离，其中 100 台主机隔离成功，20 台主机隔离失败”。

```
Ruijie# show nfpp arp-guard hosts
If column 1 shows '*', it means "hardware do not isolate user".
VLAN  interface IP address   MAC address      remain-time(s)
----  --------  ---------    -----------      -------------
1      Gi0/1       1.1.1.1      -                  110
2      Gi0/2       1.1.2.1      -                  61
*3     Gi0/3       -              0000.0000.1111   110
4      Gi0/4       -              0000.0000.2222    61
Total: 4 hosts

Ruijie# show nfpp arp-guard hosts vlan 1 interface G 0/1 1.1.1.1
If column 1 shows '*', it means "hardware do not isolate user".
VLAN  interface IP address   MAC address      remain-time(s)
---- --------  ---------     -----------      -------------
1     Gi0/1       1.1.1.1       -                  110
Total: 1 host
```

上述几个字段分别表示 VLAN 号、端口、IP 地址、MAC 地址，以及隔离剩余时间。

如果某一行的第一列显示“*”， 表示这台主机目前只是软件监控或者硬件因为资源不足而隔离失败。

如果“MAC address”栏显示“-”，表示这台主机是以源 IP 地址标识的；如果“IP address”栏显示“-”，表示这台主机是以源 MAC 地址标识的。

10.3.12 查看ARP扫描表

命令	作用
show nfpp arp-guard scan statistic	查看 ARP 扫描表的记录条数
show nfpp arp-guard scan [**vlan** *vid*] [**interface** *interface-id*] [*ip-address*] [*mac-address*]	查看 ARP 扫描表的记录 不带参数表示查看整张 ARP 扫描表，带参数表示只查看符合条件的表项。

```
Ruijie# show nfpp arp-guard scan statistics
```

```
ARP scan table has 4 record(s).
```

意思是：“ARP 扫描表总共有 4 条记录”。

```
Ruijie# show nfpp arp-guard scan
VLAN    interface   IP address   MAC address      timestamp
----    --------    ----------  -----------      ----------
1        Gi0/1       N/A           0000.0000.0001   2008-01-23 16:23:10
2        Gi0/2       1.1.1.1      0000.0000.0002   2008-01-23 16:24:10
3        Gi0/3       N/A           0000.0000.0003   2008-01-23 16:25:10
4        Gi0/4       N/A           0000.0000.0004   2008-01-23 16:26:10
Total：4 record(s)
```

“timestamp”记录的是检测出 ARP 扫描的时间，如“2008-01-23 16:23:10”表示在 2008 年 1 月 23 日 16 点 23 分 10 秒检测出 ARP 扫描。

```
Ruijie# show nfpp arp-guard scan vlan 1 interface G 0/1 0000.0000.0001
VLAN    interface   IP address   MAC address      timestamp
----    --------    ----------    -----------      ----------
1        Gi0/1       N/A           0000.0000.0001   2008-01-23 16:23:10
Total：1 record(s)
```

10.4 ICMP抗攻击

10.4.1 ICMP抗攻击简介

ICMP 协议作为诊断网络故障的常用手段，它的基本原理是主机发出 ICMP 回音请求报文（ICMP echo request），路由器或者交换机接收到这个请求报文后会回应一个 ICMP 回音应答（ICMP echo reply）报文。在上述这个处理过程中需要设备的 CPU 进行处理，这样就必然需要消耗 CPU 的一部分资源。如果攻击者向目标设备发送大量的 ICMP 回音请求，这样势必会导致设备的 CPU 资源被大量消耗，严重的情况可能导致设备无法正常工作，这种攻击方式也被人们命名为“ICMP 洪水”。对于这种攻击，防范措施是一方面对 ICMP 报文限速，另一方面检测出攻击源，对攻击源头采取隔离措施。

ICMP 攻击识别分为基于主机和基于物理端口两个类别。基于主机方式是采用源 IP 地址/虚拟局域网号/端口三者结合来识别的。每种攻击识别都有限速水线和告警水线。当 ICMP 报文速率超过限速水线时，将被丢弃。当 ICMP 报文速率超过告警水线时，将打印警告信息，发送 TRAP，基于主机的攻击识别还会对攻击源头采取隔离措施。

10.4.2 打开ICMP抗攻击功能

管理员可以在 **nfpp** 配置模式或者接口配置模式下打开 ICMP 抗攻击功能，缺省情况下就是打开的。

命令	作用
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**nfpp**	进入 NFPP 配置模式。
Ruijie(config-nfpp)#**icmp-guard enable**	打开 ICMP 抗攻击功能，缺省情况下启动。
Ruijie(config-nfpp)#**end**	退回到特权模式。

Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**interface** *interface-name*	进入接口配置模式。
Ruijie(config-if)#**nfpp icmp-guard enable**	在端口上打开 ICMP 抗攻击功能，缺省情况是端口没有配置局部开关，采用全局开关。
Ruijie(config-if)#**end**	退回到特权模式。
Ruijie#**show nfpp icmp-guard summary**	核对配置参数
Ruijie#**copy running-config startup-config**	保存配置。

当关闭 ICMP 抗攻击功能时，系统将自动清除已经被监控的主机。

10.4.3 设置对攻击者的隔离时间

对攻击者的隔离时间分为全局隔离时间和基于端口的隔离时间（即局部隔离时间）。对于某个端口，如果没有配置基于端口的隔离时间，那么采用全局隔离时间；否则，采用基于端口的隔离时间。

命令	作用
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**nfpp**	进入 NFPP 配置模式
Ruijie(config-nfpp)#**icmp-guard isolate-period** [*seconds* | **permanent**]	配置对攻击者的全局隔离时间。 取值范围为 0 秒，30 秒到 86400 秒（即一天），缺省值为 0 秒，表示不隔离；**permanent** 表示永久隔离。
Ruijie(config-nfpp)#**end**	退回到特权模式。
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**interface** *interface-name*	进入接口配置模式。
Ruijie(config-if)#**nfpp icmp-guard isolate-period**[*seconds* | **permanent**]	在端口上配置对攻击者的隔离时间。 取值范围为 0 秒，180 秒到 86400 秒（即一天），缺省情况是没有配置局部隔离时间，采用全局隔离时间。0 秒表示不隔离；**permanent** 表示永久隔离。
Ruijie(config-if)#**end**	退回到特权模式。
Ruijie#**show nfpp icmp-guard summary**	核对配置参数
Ruijie#**copy running-config startup-config**	保存配置。

如果要把全局隔离时间恢复成缺省值，在 **nfpp** 配置模式执行命令“**no icmp-guard isolate-period**”。如果一个端口原来配置了局部隔离时间，现在想采用全局隔离时间，那么在接口配置模式下执行命令“**no nfpp icmp-guard isolate-period**”把局部隔离时间配置删除。

10.4.4 设置对攻击者的监控时间

如果不配置全局隔离时间和基于端口的隔离时间（包括端口隔离时间配置成 0 秒），这种情况下，防攻击模块将自动采用监控时间对攻击者进行软件监控，提供当前系统中存在哪些攻击用户的信息。当配置全局隔离时间或者基于端口的隔离时间后，防攻击模块将自动对软件监控的用户采取硬件隔离。

命令	作用

Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**nfpp**	进入 NFPP 配置模式
Ruijie(config-nfpp)#**icmp-guard monitor-period** *seconds*	配置对攻击者的监控时间。 取值范围为 180 秒到 86400 秒（即一天），缺省值为 600 秒。
Ruijie(config-nfpp)#**end**	退回到特权模式。
Ruijie#**show nfpp icmp-guard summary**	核对配置参数
Ruijie#**copy running-config startup-config**	保存配置。

如果要把监控时间恢复成缺省值，在 nfpp 配置模式执行命令“**no icmp-guard monitor-period**”。

检测出攻击者的时候，如果隔离时间为 0，将对攻击者进行软件监控，超时为监控时间。在软件监控过程中，当隔离时间被配置为非零值时，将自动对软件监控的攻击者采取硬件隔离，并且把超时设置为隔离时间。监控时间在隔离时间为 0 的情况下才有意义。

如果把隔离时间从非零值改成零，将直接把相关端口的攻击者删除，而不是进行软件监控。

10.4.5 设置受监控主机的最大数目

命令	作用
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**nfpp**	进入 NFPP 配置模式。
Ruijie(config-nfpp)#**icmp-guard monitored-host-limit** *number*	配置受监控主机的最大数目。 取值范围为 1 到 4294967295 个，缺省情况下受监控主机的最大数目为 1000 个。
Ruijie(config-nfpp)#**end**	退回到特权模式。
Ruijie#**show nfpp icmp-guard summary**	核对配置参数
Ruijie#**copy running-config startup-config**	保存配置。

如果要把配置的最大受监控主机数恢复成缺省值，在 nfpp 配置模式执行命令“**no icmp-guard monitored-host-limit**”。

如果受监控主机数已经达到默认的 1000 个，此时管理员把受监控主机的最大数目设置成小于 1000，不会删除已有的受监控主机，而是打印信息“%ERROR： The value that you configured is smaller than current monitored hosts 1000（配置的受监控主机数），please clear a part of monitored hosts.”来提醒管理员配置没有生效，需要删除部分已经被监控的主机。

当受监控主机满时，打印日志“% NFPP_ICMP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000（配置的受监控主机数） monitored hosts.”提醒管理员。

10.4.6 基于主机限速和识别攻击

识别主机的方法为源 IP/VID/端口。每个用户都有限速水线和攻击阈值（也称为告警水线），限速水线必须低于攻击阈值。当单台主机的 ICMP 报文速度超过限速水线时，就丢弃超限的 ICMP 报文。如果单台主机的 ICMP 报文速度超过攻击阈值，将采取隔离措施，记录到日志中，发送 TRAP。

如果检测到攻击行为，打印的日志信息格式如下：

```
%NFPP_ICMP_GUARD-4-DOS_DETECTED: Host<IP=1.1.1.1,MAC= N/A,port=Gi4/1,VLAN=1> was detected.
(2009-07-01 13:00:00)
```

发送的 TRAP 报文的数据包含如下描述信息：

```
ICMP DoS attack from host<IP=1.1.1.1,MAC= N/A,port=Gi4/1,VLAN=1> was detected.
```

如果管理员把隔离时间配置成非零值，当硬件隔离成功时，打印的日志信息格式如下所示：

```
%NFPP_ICMP_GUARD-4-ISOLATED:Host<IP=1.1.1.1, MAC= N/A ,port=Gi4/1,VLAN=1> was isolated. (2009-07-01 13:00:00)
```

发送的 TRAP 报文的数据包含如下描述信息：

```
Host<IP=1.1.1.1,MAC= N/A,port=Gi4/1,VLAN=1> was isolated.
```

当硬件隔离失败（原因通常是内存不足或者硬件资源不足）时，打印的日志信息格式如下所示：

```
%NFPP_ICMP_GUARD-4-ISOLATE_FAILED: Failed to isolate host<IP=1.1.1.1, MAC=
N/A ,port=Gi4/1,VLAN=1>.(2009-07-01 13:00:00)
```

发送的 TRAP 报文的数据包含如下描述信息：

```
Failed to isolate host<IP=1.1.1.1,MAC= N/A,port=Gi4/1,VLAN=1>.
```

当无法为检测到的攻击者分配内存时，打印日志“%NFPPP_ ICMP_GUARD -4-NO_MEMORY: Failed to alloc memory.”提醒管理员。

管理员可以在 **nfpp** 配置模式和接口配置模式下进行配置。

命令	作用
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**nfpp**	进入 NFPP 配置模式。
Ruijie(config-nfpp)#**icmp-guard rate-limit per-src-ip** *pps*	全局对每台主机的 ICMP 报文速度进行限制。 取值范围是 1 到 9999，缺省值是基于端口的全局限速水线（将在下一节说明）的一半。 “**per-src-ip**”是基于源 IP/VID/端口识别主机。
Ruijie(config-nfpp)#**icmp-guard attack-threshold per-src**-ip *pps*	配置攻击阈值。当某台主机的 ICMP 报文超过攻击阈值时，就认为是在进行攻击，立即对这台主机采取隔离措施，记录到日志，发送 TRAP。 取值范围是 1 到 9999，缺省值和基于源 IP 地址的缺省限速水线相同。 “**per-src-ip**”是基于源 IP/VID/端口识别主机。
Ruijie(config-nfpp)#**end**	退回到特权模式。
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**interface** *interface-name*	进入接口配置模式。

Ruijie(config-if)#**nfpp icmp-guard policy per-src-ip** *rate-limit-pps attack-threshold-pps*	配置局部的限速水线和攻击水线，只在该配置所属端口上生效。 *rate-limit-pps* 是限速水线，取值范围是 1 到 9999，缺省是没有配置基于端口的速率，采用全局速率。 *attack-threshold-pps* 是攻击水线，取值范围是 1 到 9999。 缺省情况是端口没有自己的限速水线和攻击水线，采用全局的限速水线和攻击水线。 “per-src-ip”是基于源 IP/VID/端口识别主机。
Ruijie(config-if)#**end**	退回到特权模式。
Ruijie#**show nfpp icmp-guard summary**	核对配置参数
Ruijie#**copy running-config startup-config**	保存配置。

10.4.7 基于端口限速和识别攻击

每个端口都有限速水线和攻击阈值，限速水线必须低于攻击阈值。当某个端口的 ICMP 报文速度超过限速水线时，就丢弃 ICMP 报文。如果某个端口的 ICMP 报文速度超过攻击阈值，将记录到日志中，发送 TRAP。

当端口遭受 ICMP 拒绝服务攻击时，打印的警告信息格式如下：

```
%NFPP_ICMP_GUARD-4-PORT_ATTACKED: ICMP DoS attack was detected on port Gi4/1. (2009-07-01 13:00:00)
```

发送的 TRAP 报文的数据包含如下描述信息：

```
ICMP DoS attack was detected on port Gi4/1.
```

管理员可以在 **nfpp** 配置模式和接口配置模式下进行配置。

命令	作用
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**nfpp**	进入 NFPP 配置模式。
Ruijie(config-nfpp)#**icmp-guard rate-limit per-port** *pps*	对每个端口的 ICMP 报文速度进行限制。 取值范围是 1 到 9999，缺省值因产品而异，本产品缺省值为 400。
Ruijie(config-nfpp)#**icmp-guard attack-threshold per-port** *pps*	配置攻击阈值，当某个端口的 ICMP 报文超过阈值时，记录到日志，发送 TRAP。 取值范围是 1 到 9999，缺省值和基于端口的缺省限速水线相同。
Ruijie(config-nfpp)#**end**	退回到特权模式。
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**interface** *interface-name*	进入接口配置模式。

Ruijie(config-if)#**nfpp icmp-guard policy per-port** *rate-limit-pps attack-threshold-pps*	配置局部的限速水线和攻击水线，只在该配置所属端口上生效。 *rate-limit-pps* 是限速水线，取值范围是 1 到 9999。 *attack-threshold-pps* 是攻击水线，取值范围是 1 到 9999。 缺省情况是端口没有自己的限速水线和攻击水线，采用全局的限速水线和攻击水线。
Ruijie(config-if)#**end**	退回到特权模式。
Ruijie#**show nfpp icmp-guard configuration**	核对配置参数
Ruijie#**copy running-config tartup-config**	保存配置。

基于源 IP 地址限速优先级高于基于端口限速。

10.4.8 设置不监控的可信主机

如果管理员希望对某台主机不进行监控，即对该主机表示信任，则可以通过该命令配置。该可信主机发往 CPU 的 ping 报文将被允许发往 CPU。

命令	作用
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**nfpp**	进入 NFPP 配置模式。
Ruijie(config-nfpp)#**icmp-guard trusted-host** *ip mask*	配置不进行监控的 IP 地址范围。 最多能够配置 500 条。
Ruijie(config-nfpp)#**end**	退回到特权模式。
Ruijie#**show nfpp icmp-guard trusted-host**	查看不监控的可信主机。
Ruijie#**copy running-config startup-config**	保存配置。

在 **nfpp** 配置模式下，可以使用该命令的 **no** 选项删除一条可信主机表项。使用命令的 **no** 和 **all** 选项可以删除所有可信主机。

例如删除所有可信主机：

```
Ruijie(config-nfpp)# no icmp-guard trusted-host all
```

或删除单条可信主机：

```
Ruijie(config-nfpp)# no icmp-guard trusted-host 1.1.1.1 255.255.255.255
```

当不监控的可信主机表满时，打印提示信息“%ERROR: Attempt to exceed limit of 500 trusted hosts.”提醒管理员。

当受监控主机表中存在与可信主机相匹配的表项（IP 地址相同）时，系统将自动删除此 IP 地址对应的表项。

当删除可信主机失败时，打印提示信息“%ERROR: Failed to delete trusted host 1.1.1.0 255.255.255.0（配置的可信主机）.”提醒管理员。

当添加可信主机失败时，打印提示信息“%ERROR: Failed to add trusted host 1.1.1.0 255.255.255.0（配置的可信主机）.”提醒管理员。

当添加的可信主机已经存在时，打印提示信息“%ERROR: Trusted host 1.1.1.0 255.255.255.0（配置的可信主机）has already been configured.”提醒管理员。

当要删除的可信主机不存在时，打印提示信息“%ERROR: Trusted host 1.1.1.0 255.255.255.0（配置的可信主机）is not found.”提醒管理员。

当无法为可信主机分配内存时，打印提示信息“%ERROR: Failed to alloc memory.”提醒管理员。

10.4.9 清除受监控主机

已被隔离的主机在一段时间后自动恢复，如果管理员要手动清除该主机，可以在特权模式下用以下命令清除。

命令	作用
Ruijie#**clear nfpp 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。

10.4.10 查看ICMP抗攻击的配置参数

使用 **show nfpp icmp-guard summary** 查看 ICMP 抗攻击的配置参数：

命令	作用
show nfpp icmp-guard summary	查看 ICMP 抗攻击配置参数

下面是一个例子：

```
Ruijie# show nfpp icmp-guard summary
 (Format of column Rate-limit and  Attack-threshold is per-src-ip/per-src-mac/per-port.)
Interface  Status  Isolate-period Rate-limit Attack-threshold
Global      Enable  300             4/-/60     8/-/100
G 0/1       Enable  180             5/-/-       8/-/-
G 0/2       Disable 200             4/-/60     8/-/100

Maximum count of monitored hosts: 1000
Monitor period：300s
```

字段 Interface 为 Global 表示全局配置。

字段 Status 表示是否打开抗攻击功能。

字段 Rate-limit 的格式为（对源 IP 地址的限速水线/对源 MAC 地址的限速水线/端口的限速水线值），字段 Attack-threshold 的显示格式类似。“-”表示没有配置。举例说明：

“4/-/60”表示对源 IP 地址的限速水线是 4，对每个端口的限速水线是 60。

G 0/1 这一行的字段 Rate-limit 为“5/-/-”，表示端口 G 0/1 对源 IP 地址的限速水线是 5，没有配置对端口的限速水线。

10.4.11 查看受监控主机的信息

命令	作用

show nfpp icmp-guard hosts statistics	查看受监控主机表的统计信息，包括主机总数、隔离成功的主机数量和隔离失败的主机数量。
show nfpp icmp-guard hosts [**vlan** *vid*] [**interface** *interface-id*] [*ip-address*]	查看已被检测到攻击的主机。 不带参数表示显示所有已被检测到攻击的主机，带参数则只显示符合条件的主机。

```
Ruijie#show nfpp icmp-guard hosts statistics
success    fail    total
-------    ----    -----
100         20       120
```

表示：“总共有 120 台主机被监控，其中 100 台主机隔离成功，20 台主机隔离失败”。

```
Ruijie# show nfpp icmp-guard hosts
If column 1 shows '*', it means "hardware failed to isolate host".
VLAN  interface IP address     remain-time(s)
----  --------   ---------     -------------
1     Gi0/1      1.1.1.1       110
2     Gi0/2      1.1.2.1       61
Total：2 host(s)
```

```
Ruijie# show nfpp icmp-guard hosts vlan 1 interface g 0/1 1.1.1.1
If column 1 shows '*', it means "hardware failed to isolate host".
VLAN  interface IP address     remain-time(s)
---- --------   ---------      -------------
1    Gi0/1      1.1.1.1        80
Total：1 host(s)
```

上述几个字段分别表示 VLAN 号、端口、IP 地址、MAC 地址，以及隔离剩余时间。

如果某一行的第一列显示“*”， 表示这台主机目前只是软件监控或者硬件因为资源不足而隔离失败。

10.4.12 查看不监控的可信主机

使用 **show nfpp icmp-guard trusted-host** 查看不受监控的可信主机：

命令	作用
show nfpp icmp-guard trusted-host	查看不受监控的可信主机。

下面是一个例子：

```
Ruijie# show nfpp icmp-guard trusted-host
IP address      mask
---------       ------
1.1.1.0         255.255.255.0
1.1.2.0         255.255.255.0
Total：2 record(s)
```

10.5 DHCP抗攻击

10.5.1 DHCP抗攻击简介

DHCP 协议被广泛地应用在局域网环境里来动态分配 IP 地址。DHCP 协议对网络安全起着非常重要的意义。目前，存在的最广泛的 DHCP 攻击就是称为“DHCP 耗竭”的攻击，这种攻击通过伪造的 MAC 地址来广播 DHCP 请求的方式进行。目前网络上存在多种这样的攻击工具都可以很容易地实现上述攻击。如果发出的 DHCP 请求足够多的话，网络攻击者就可以在一段时间内耗竭 DHCP 服务器所提供的地址空间，这样当一台合法的主机请求一个 DHCP IP 地址的时候无法成功，从而无法访问网络。对于这种攻击，防范措施是一方面对 DHCP 报文限速，另一方面检测出攻击源，对攻击源头采取隔离措施。

DHCP 攻击识别分为基于主机和基于物理端口两个类别。基于主机方式是采用链路层源 MAC 地址/虚拟局域网号/端口三者结合来识别的。每种攻击识别都有限速水线和告警水线。当 DHCP 报文速率超过限速水线时，超限的 DHCP 报文将被丢弃。当 DHCP 报文速率超过告警水线时，将打印警告信息，发送 TRAP，基于主机的攻击识别还会对攻击源头采取隔离措施。

10.5.2 打开DHCP抗攻击功能

管理员可以在 **nfpp** 配置模式或者接口配置模式下打开 DHCP 抗攻击功能，缺省情况下就是打开的。

命令	作用
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**nfpp**	进入 NFPP 配置模式。
Ruijie(config-nfpp)#**dhcp-guard enable**	打开 DHCP 抗攻击功能，缺省情况下就是打开的。
Ruijie(config-nfpp)#**end**	退回到特权模式。
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**interface** *interface-name*	进入接口配置模式。
Ruijie(config-if)#**nfpp dhcp-guard enable**	在端口上打开 DHCP 抗攻击功能，缺省情况是端口没有配置局部开关，采用全局开关。
Ruijie(config-if)#**end**	退回到特权模式。
Ruijie#**show nfpp dhcp-guard summary**	核对配置参数
Ruijie#**copy running-config startup-config**	保存配置。

当关闭 DHCP 抗攻击功能时，系统将自动清除已经被监控的主机。

10.5.3 设置对攻击者的隔离时间

对攻击者的隔离时间分为全局隔离时间和基于端口的隔离时间（即局部隔离时间）。对于某个端口，如果没有配置基于端口的隔离时间，那么采用全局隔离时间；否则，采用基于端口的隔离时间。

命令	作用
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**nfpp**	进入 NFPP 配置模块

Ruijie(config-nfpp)#**dhcp-guard isolate-period** [*seconds* | **permanent**]	配置对攻击者的全局隔离时间。 取值范围为 0 秒，30 秒到 86400 秒（即一天），缺省值为 0 秒，表示不隔离；**permanent** 表示永久隔离。
Ruijie(config-nfpp)#**end**	退回到特权模式。
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**interface** *interface-name*	进入接口配置模式。
Ruijie(config-if)#**nfpp dhcp-guard isolate-period** [*seconds* | **permanent**]	在端口上配置对攻击者的隔离时间。 取值范围为 0 秒，180 秒到 86400 秒（即一天），缺省情况是没有配置局部隔离时间，采用全局隔离时间。0 秒表示不隔离；**permanent** 表示永久隔离。
Ruijie(config-if)#**end**	退回到特权模式。
Ruijie#**show nfpp dhcp-guard summary**	核对配置参数
Ruijie#**copy running-config startup-config**	保存配置。

如果要把全局隔离时间恢复成缺省值，在 **nfpp** 配置模式执行命令“**no dhcp-guard isolate-period**”。如果一个端口原来配置了局部隔离时间，现在想采用全局隔离时间，那么在接口配置模式下执行命令“**no nfpp dhcp-guard isolate-period**”把局部隔离时间配置删除。

10.5.4 设置对攻击者的监控时间

如果隔离时间为 0（即不隔离），防攻击模块将自动根据配置的监控时间对攻击者进行软件监控，提供当前系统中存在哪些攻击者的信息。当把隔离时间配置成非零值后，防攻击模块将自动对软件监控的主机采取硬件隔离。

命令	作用
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**nfpp**	进入 NFPP 配置模式
Ruijie(config-nfpp)#**dhcp-guard monitor-period** *seconds*	配置对攻击者的监控时间。 取值范围为 180 秒到 86400 秒（即一天），缺省值为 600 秒。
Ruijie(config-nfpp)#**end**	退回到特权模式。
Ruijie#**show nfpp dhcp-guard summary**	核对配置参数
Ruijie#**copy running-config startup-config**	保存配置。

如果要把监控时间恢复成缺省值，在 nfpp 配置模式执行命令“**no dhcp-guard monitor-period**”。

检测出攻击者的时候，如果隔离时间为 0，将对攻击者进行软件监控，超时为监控时间。在软件监控过程中，当隔离时间被配置为非零值时，将自动对软件监控的攻击者采取硬件隔离，并且把超时设置为隔离时间。监控时间在隔离时间为 0 的情况下才有意义。

如果把隔离时间从非零值改成零，将直接把相关端口的攻击者删除，而不是进行软件监控。

10.5.5 设置受监控主机的最大数目

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

Ruijie(config)#**nfpp**	进入 NFPP 配置模式。
Ruijie(config-nfpp)#**dhcp-guard monitored-host-limit** *number*	配置受监控主机的最大数目。 取值范围为 1 到 4294967295，缺省情况下受监控主机的最大数目为 1000 个。
Ruijie(config-nfpp)#**end**	退回到特权模式。
Ruijie#**show nfpp dhcp-guard summary**	核对配置参数
Ruijie#**copy running-config startup-config**	保存配置。

如果要把配置的最大受监控主机数恢复成缺省值，在 nfpp 配置模式执行命令“**no dhcp-guard monitored-host-limit**”。

如果受监控主机数已经达到默认的 1000 个，此时管理员把受监控主机的最大数目设置成小于 1000，不会删除已有的受监控主机，而是打印信息“%ERROR：The value that you configured is smaller than current monitored hosts 1000（配置的受监控主机数），please clear a part of monitored hosts.”来提醒管理员配置没有生效，需要删除部分已经被监控的主机。

当受监控主机表满时，打印日志“% NFPP_DHCP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000（配置的受监控主机数） monitored hosts.”提醒管理员。

10.5.6 基于主机限速和识别攻击

识别主机的方法为链路层源 MAC/VID/端口。每台主机都有限速水线和攻击阈值（也称为告警水线），限速水线必须低于攻击阈值。当单台主机的 DHCP 报文速度超过限速水线时，就丢弃超限的 DHCP 报文。如果单台主机的 DHCP 报文速度超过攻击阈值，将采取隔离措施，记录到日志中，发送 TRAP。

如果检测到攻击行为，打印的日志信息格式如下：

```
%NFPP_DHCP_GUARD-4-DOS_DETECTED: Host<IP=N/A,MAC=0000.0000.0001,port=Gi4/1,VLAN=1> was detected.
(2009-07-01 13:00:00)
```

发送的 TRAP 报文的数据包含如下描述信息：

```
DHCP DoS attack from host<IP=N/A,MAC=0000.0000.0001,port=Gi4/1,VLAN=1> was detected.
```

如果管理员把隔离时间配置成非零值，当硬件隔离成功时，打印的日志信息格式如下所示：

```
%NFPP_DHCP_GUARD-4-ISOLATED:Host<IP=N/A, MAC=0000.0000.0001,port=Gi4/1,VLAN=1> was isolated.
(2009-07-01 13:00:00)
```

发送的 TRAP 报文的数据包含如下描述信息：

```
Host<IP=N/A, MAC=0000.0000.0001,port=Gi4/1,VLAN=1> was isolated.
```

当硬件隔离失败（原因通常是内存不足或者硬件资源不足）时，打印的日志信息格式如下所示：

```
%NFPP_DHCP_GUARD-4-ISOLATE_FAIL:Failed to isolate host<IP=N/A,
MAC=0000.0000.0001,port=Gi4/1,VLAN=1>.(2009-07-01 13:00:00)
```

发送的 TRAP 报文的数据包含如下描述信息：

```
Failed to isolate host<IP=N/A, MAC=0000.0000.0001,port=Gi4/1,VLAN=1>.
```

当无法为检测到的攻击者分配内存时,打印日志“%NFPP_DHCP_GUARD-4-NO_MEMORY: Failed to alloc memory.”提醒管理员。

管理员可以在 **nfpp** 配置模式和接口配置模式下进行配置。

命令	作用
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**nfpp**	进入 NFPP 配置模式。
Ruijie(config-nfpp)#**dhcp-guard rate-limit per-src-mac** *pps*	全局对每台主机的 DHCP 报文速度进行限制。 取值范围是 1 到 9999，缺省值为 5 个。 “**per-src-mac**”是基于链路层源 MAC/VID/端口识别主机。
Ruijie(config-nfpp)#**dhcp-guard attack-threshold per-src-mac** *pps*	配置攻击阈值。当某台主机的 DHCP 报文超过攻击阈值时，就认为是在进行攻击，立即对这台主机采取隔离措施，记录到日志，发送 TRAP。 取值范围是 1 到 9999，缺省值为 10 个。 “**per-src-mac**”是基于链路层源 MAC/VID/端口识别主机。
Ruijie(config-nfpp)#**end**	退回到特权模式。
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**interface** *interface-name*	进入接口配置模式。
Ruijie(config-if)#**nfpp dhcp-guard policy per-src-mac** *rate-limit-pps attack-threshold-pps*	配置局部的限速水线和攻击水线，只在该配置所属端口上生效。 *rate-limit-pps* 是限速水线，取值范围是 1 到 9999。 *attack-threshold-pps* 是攻击水线，取值范围是 1 到 9999。 缺省情况是端口没有自己的限速水线和攻击水线，采用全局的限速水线和攻击水线。 “per-src-mac”是基于链路层源 MAC/VID/端口识别主机。
Ruijie(config-if)#**end**	退回到特权模式。
Ruijie#**show nfpp dhcp-guard summary**	核对配置参数
Ruijie#**copy running-config startup-config**	保存配置。

10.5.7 基于端口限速和识别攻击

每个端口都有限速水线和攻击阈值，限速水线必须低于攻击阈值。当某个端口的 DHCP 报文速度超过限速水线时，就丢弃超限 DHCP 报文。如果某个端口的 DHCP 报文速度超过攻击阈值，将记录到日志中，发送 TRAP。

当端口遭受 DHCP 拒绝服务攻击时，打印的警告信息格式如下：

```
%NFPP_DHCP_GUARD-4-PORT_ATTACKED: DHCP DoS attack was detected on port Gi4/1. (2009-07-01 13:00:00)
```

发送的 TRAP 报文的数据包含如下描述信息：

```
DHCP DoS attack was detected on port Gi4/1.
```

管理员可以在 **nfpp** 配置模式和接口配置模式下进行配置。

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

Ruijie(config)#**nfpp**	进入 NFPP 配置模式。
Ruijie(config-nfpp)#**dhcp-guard rate-limit per-port** *pps*	对每个端口的 DHCP 报文速度进行限制。 取值范围是 1 到 9999，缺省值为 150 个。
Ruijie(config-nfpp)#**dhcp-guard attack-threshold per-port** *pps*	配置攻击阈值，当某个端口的 DHCP 报文超过阈值时，记录到日志，发送 TRAP。 取值范围是 1 到 9999，缺省值为 300 个。
Ruijie(config-nfpp)#**end**	退回到特权模式。
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**interface** *interface-name*	进入接口配置模式。
Ruijie(config-if)#**nfpp dhcp-guard policy per-port** *rate-limit-pps attack-threshold-pps*	配置局部的限速水线和攻击水线，只在该配置所属端口上生效。 *rate-limit-pps* 是限速水线，取值范围是 1 到 9999。 *attack-threshold-pps* 是攻击水线，取值范围是 1 到 9999。 缺省情况是端口没有自己的限速水线和攻击水线，采用全局的限速水线和攻击水线。
Ruijie(config-if)#**end**	退回到特权模式。
Ruijie#**show nfpp dhcp-guard summary**	核对配置参数
Ruijie#**copy running-config startup-config**	保存配置。

基于链路层源 MAC 地址限速优先于基于端口限速处理。

10.5.8 清除受监控主机

已被隔离的主机在一段时间后自动恢复，如果管理员要手动清除该主机，可以在特权模式下用以下命令清除。

命令	作用
Ruijie#**clear nfpp dhcp-guard hosts** [**vlan** *vid*] [**interface** *interface-id*] [*mac-address*]	不带参数表示清除所有已被检测到攻击的主机，带参数表示清除符合条件的主机。

10.5.9 查看DHCP抗攻击的配置参数

使用 **show nfpp dhcp-guard summary** 查看 DHCP 抗攻击的配置参数：

命令	作用
show nfpp dhcp-guard summary	查看 DHCP 抗攻击配置参数

下面是一个例子：

```
Ruijie# show nfpp dhcp-guard summary
 (Format of column Rate-limit and  Attack-threshold is per-src-ip/per-src-mac/per-port.)
Interface  Status  Isolate-period Rate-limit Attack-threshold
Global      Enable  300             -/5/150      -/10/300
G 0/1       Enable  180             -/6/-        -/8/-
G 0/2       Disable 200             -/5/30       -/10/50
```

```
Maximum count of monitored hosts: 1000
Monitor period：300s
```

字段 Interface 为 Global 表示全局配置。

字段 Status 表示是否打开抗攻击功能。

字段 Rate-limit 的格式为（对源 IP 地址的限速水线/对源 MAC 地址的限速水线/端口的限速水线值），字段 Attack-threshold 的显示格式类似。“-”表示没有配置。举例说明：

“-/5/150”表示对源 MAC 地址的限速水线是 5，对每个端口的限速水线是 150。

G 0/1 这一行的字段 Rate-limit 为“-/6/-”，表示端口 G 0/1 对源 MAC 地址的限速水线是 6，没有配置对端口的限速水线。

10.5.10 查看受监控主机的信息

命令	作用
show nfpp dhcp-guard hosts statistics	查看受监控主机表的统计信息，包括主机总数、隔离成功的主机数量和隔离失败的主机数量。
show nfpp dhcp-guard hosts [**vlan** *vid*] [**interface** *interface-id*] [*mac-address*]	查看已被检测到攻击的主机。 不带参数表示显示所有已被检测到攻击的主机，带参数则只显示符合条件的主机。

```
Ruijie# show nfpp dhcp-guard hosts statistics
success    fail    total
------     ----     -----
100          20         120
```

表示：“总共有 120 台主机被监控，其中 100 台主机隔离成功，20 台主机隔离失败”。

```
Ruijie# show nfpp dhcp-guard hosts
If column 1 shows '*', it means "hardware failed to isolate host".
VLAN  interface   MAC address      remain-time(s)
----  --------    -----------      -------------
*1      Gi0/1       0000.0000.0001  110
2       Gi0/2       0000.0000.2222   61
Total: 2 host(s)
```

```
Ruijie# show nfpp dhcp-guard hosts vlan 1 interface g 0/1 0000.0000.0001
If column 1 shows '*', it means "hardware failed to isolate host".
VLAN  interface   MAC address      remain-time(s)
---- --------     -----------      -------------
 *1     Gi0/1       0000.0000.0001  110
Total: 1 host(s)
```

上述几个字段分别表示 VLAN 号、端口、IP 地址、MAC 地址，以及隔离剩余时间。

如果某一行的第一列显示“*”， 表示这台主机目前只是软件监控或者硬件因为资源不足而隔离失败。

10.6 ND抗攻击

10.6.1 ND抗攻击简介

ND 的全称是 Neighbor Discovery，翻译成汉语是“邻居发现”。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 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。

10.6.2 打开ND抗攻击功能

管理员可以在 **nfpp** 配置模式或者接口配置模式下打开 ND 抗攻击功能，缺省情况下就是打开的。

命令	作用
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**nfpp**	进入 NFPP 配置模式。
Ruijie(config-nfpp)#**nd-guard enable**	打开 ND 抗攻击功能，缺省情况下就是打开的。
Ruijie(config-nfpp)#**end**	退回到特权模式。
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**interface** *interface-name*	进入接口配置模式。
Ruijie(config-if)#**nfpp nd-guard enable**	在端口上打开 ND 抗攻击功能，缺省情况是端口没有配置局部开关，采用全局开关。
Ruijie(config-if)#**end**	退回到特权模式。
Ruijie#**show nfpp nd-guard summary**	核对配置参数
Ruijie#**copy running-config startup-config**	保存配置。

10.6.3 基于端口限速和识别攻击

每个端口都有限速水线和攻击阈值，限速水线必须低于攻击阈值。当某个端口的 ND 报文速度超过限速水线时，就丢弃超限 ND 报文。如果某个端口的 ND 报文速度超过攻击阈值，将记录到日志中，发送 TRAP。

ND snooping 把端口划分为非信任端口和信任端口，非信任端口连接主机，信任端口连接网关。由于通常信任端口的流量大于非信任端口的流量，所以信任端口的限速水线应该高于非信任端口的限速水线，开启 ND snooping 功能时，对于信任端口，ND snooping 将通告 ND guard 把端口的三类报文限速水线都设置成每秒 800 个，把攻击水线都设置成每秒 900 个。

ND guard 同等对待 ND snooping 设置的限速水线和管理员配置的限速水线，后配置的值覆盖先配置的值。具体的说，就是：“如果管理员在该端口上先配置限速水线，然后 ND snooping 设置限速水线，那么 ND snooping 设置限速水线覆盖管理员配置的限速水线；如果 ND snooping 先设置限速水线，然后管理员在该端口上配置限速水线，那么管理员配置的限速水线覆盖 ND snooping 设置的限速水线。”

在管理员保存配置的时候，将把 ND snooping 设置的限速水线保存到配置文件中。

ND snooping 设置的攻击水线和管理员配置的攻击水线的关系类似。

当端口遭受邻居请求/公告拒绝服务攻击时，打印的警告信息格式如下：

```
%NFPP_ND_GUARD-4-PORT_ATTACKED: NS-NA DoS attack was detected on port Gi4/1. (2009-07-01 13:00:00)
```

发送的 TRAP 报文的数据包含如下描述信息：

```
NS-NA DoS attack was detected on port Gi4/1.
```

当端口遭受路由器请求拒绝服务攻击时，打印的警告信息格式如下：

```
%NFPP_ND_GUARD-4-PORT_ATTACKED: RS DoS attack was detected on port Gi4/1. (2009-07-01 13:00:00)
```

发送的 TRAP 报文的数据包含如下描述信息：

```
RS DoS attack was detected on port Gi4/1.
```

当端口遭受路由器公告/重定向报文拒绝服务攻击时，打印的警告信息格式如下：

```
%NFPP_ND_GUARD-4-PORT_ATTACKED: RA-REDIRECT DoS attack was detected on port Gi4/1. (2009-07-01 13:00:00)
```

发送的 TRAP 报文的数据包含如下描述信息：

```
RA-REDIRECT DoS attack was detected on port Gi4/1.
```

管理员可以在 **nfpp** 配置模式和接口配置模式下进行配置。

命令	作用
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**nfpp**	进入 NFPP 配置模式。
Ruijie(config-nfpp)#**nd-guard rate-limit per-port** [**ns-na** | **rs** | **ra-redirect**] *pps*	对每个端口的 ND 报文速度进行限制。 取值范围是 1 到 9999，缺省值为 15 个。
Ruijie(config-nfpp)#**nd-guard attack-threshold per-port** [**ns-na** | **rs** | **ra-redirect**] *pps*	配置攻击阈值，当某个端口的 ND 报文超过攻击阈值时，记录到日志，发送 TRAP。 取值范围是 1 到 9999，缺省值为 30 个。
Ruijie(config-nfpp)#**end**	退回到特权模式。
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**interface** *interface-name*	进入接口配置模式。

Ruijie(config-if)#**nfpp nd-guard policy per-port** [**ns-na** | **rs** | **ra-redirect**] *rate-limit-pps attack-threshold-pps*	配置局部的限速水线和攻击水线，只在该配置所属端口上生效。 *rate-limit-pps* 是限速水线，取值范围是 1 到 9999。 *attack-threshold-pps* 是攻击水线，取值范围是 1 到 9999。
Ruijie(config-if)#**end**	退回到特权模式。
Ruijie#**show nfpp nd-guard summary**	核对配置参数
Ruijie#**copy running-config startup-config**	保存配置。

10.6.4 查看ND抗攻击的配置参数

使用 **show nfpp nd-guard summary** 查看 ND 抗攻击的配置参数：

命令	作用
show nfpp nd-guard summary	查看 ND 抗攻击配置参数

下面是一个例子：

```
Ruijie# show nfpp nd-guard summary
 (Format of column Rate-limit and  Attack-threshold is NS-NA/RS/RA-REDIRECT.)
Interface  Status  Rate-limit Attack-threshold
Global      Enable  20/5/10     40/10/20
G 0/1       Enable  15/15/15    30/30/30
G 0/2       Disable -/5/30       -/10/50
```

字段 Interface 为 Global 表示全局配置。

字段 Status 表示是否打开抗攻击功能。

字段 Rate-limit 的格式为（对邻居请求/公告的限速水线/对路由器请求的限速水线/对路由器公告/重定向报文的限速水线），字段 Attack-threshold 的显示格式类似。“-”表示没有配置。

举例说明：“-/5/30”表示在端口 G 0/2 上没有配置邻居请求/公告的限速水线，对路由器请求的限速水线是 5，对路由器公告/重定向报文的限速水线是 30。

10.7 自定义抗攻击

10.7.1 自定义抗攻击简介

网络协议种类繁多，仅路由协议就有 OSPF、BGP、RIP 等。各种协议需要在不同设备之间进行报文交互，交互报文必须送 CPU 交由各个协议进行处理，网络设备一运行某种协议，就相当于开了一扇窗口，给了攻击者可趁之机。如果攻击者向网络设备发送大量的协议报文，将会导致设备的 CPU 资源被大量消耗，严重的情况可能导致设备无法正常工作。

考虑到网络协议多种多样，并且在持续发展中，不同的用户环境下需要使用不同的协议。为此，锐捷设备提供了自定义抗攻击的功能，允许用户自定义抗攻击的类型，灵活配置，以满足不同用户环境下的抗攻击需求。

10.7.2 自定义抗攻击策略

管理员可以在 nfpp 配置模式下自定义一种抗攻击类型。自定义抗攻击要求用户必须配置自定义报文的类型、限速水线、攻击水线及如何识别用户这些基本信息。基本信息配置完以后，才能使自定义抗攻击类型生效。

自定义报文的类型可以由以太网链路层类型字段 etype、源 MAC 地址 smac、目的 MAC 地址 dmac、IPv4 协议号 protocol、源 IPv4 地址 sip、目的 IPv4 地址 dip、源传输层端口 sport 和目的传输层端口 dport 这些字段组合而成。

自定义抗攻击必须配置如何对自定义类型报文速率进行分类统计。分类有基于源 IP/VID/端口、基于源 MAC/VID/端口的主机速率统计及基于端口的速率统计，可以是三者的任意组合。并且必须为这些分类配置相应的限速水线及攻击水线。只有配置了分类的限速水线和攻击水线，该分类才会生效。

命令	作用
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**nfpp**	进入 NFPP 配置模式。
Ruijie(config-nfpp)#**define** *name*	配置自定义抗攻击类型名称
Ruijie(config-nfpp-define)# **match** [**etype** *type*] [**src-mac** *smac* [**src-mac-mask** *smac_mask*]] [**dst-mac** *dmac* [**dst-mac-mask** *dst_mask*]] [**protocol** *protocol*] [**src-ip** *sip* [**src-ip-mask** *sip-mask*]] [**dst-ip** *dip* **[dst-ip-mask** *dip-mask*]] [**src-port** *sport*] [**dst-port** *dport*]	配置自定义抗攻击类型需要匹配的报文字段。 **src-mac-mask** 、 **dst-mac-mask** 、 **src-ip-mask** 、 **dst-ip-mask** 默认均为全 1。 **protocol** 仅在 **etype** 为 ipv4 才有效；**src-ip**、**dst-ip** 仅在 **etype** 为 ipv4 时有效； **src-port**、**dst-port** 仅在 **protocol** 为 tcp 或者 udp 时有效。
Ruijie(config-nfpp-define)# **global-policy** {**per-src-ip** | **per-src-mac** | **per-port**} *rate-limit-pps attack-threshold-pps*	配置基于主机或者基于端口的限速水线和攻击水线。 **per-src-ip** 表示基于源 IP/VID/端口识别主机进行速率统计。**per-src-mac** 表示基于源 MAC/VID/端口识别主机进行速率统计。**per-port** 表示基于每个报文接收的物理端口进行速率统计。**per-src-ip**、**per-src-mac** 和 **per-port** 三者至少要配置一个，否则策略无法生效。 **per-src-ip** 仅在 **etype** 为 ipv4 有效。 *rate-limit-pps* 是限速水线，取值范围是 1 到 9999，缺省是不需要进行速率限制。自定义报文超过限速水线后的报文将被丢弃。 *attack-threshold-pps* 是攻击水线，取值范围是 1 到 9999。 缺省是不需要进行速率限制。 攻击水线必须大于或者等于限速水线。
Ruijie#**show nfpp define summary** *name*	核对配置参数
Ruijie#**copy running-config startup-config**	保存配置。

如果要把自定义抗攻击类型删除，在 nfpp 配置模式下执行“**no define** *name*”。删除自定义抗攻击类型将会清除该自定义抗攻击的所有配置，包含全局和端口下的配置，及所有隔离主机及可信主机。

自定义抗攻击类型的名字不能重复，match 匹配的字段及值也不能完全相同，也不能与 arp、icmp、dhcp、ip 抗攻击类型相同。当配置类型重复时，将提示配置失败。

当自定义抗攻击类型的 match 字段及值与已存在的抗攻击类型完全一样时，打印提示信息：“%ERROR: the match type and value are the same with define name(已存在的的抗攻击类型名).”，提示管理员配置失败。

- 当 match 配置了 protocol，但 etype 不是 IPv4 时，打印提示信息： “%ERROR: protocol is valid only when etype is IPv4(0x0800).”
- 当 match 配置了 src-ip、dst-ip，但 etype 不是 IPv4 时，打印提示信息：“%ERROR: IP address is valid only when etype is IPv4(0x0800).”
- 当 match 配置了 src-port、dst-port，但 protocol 不是 TCP 或者 UDP 时，打印提示信息：“%ERROR: Port is valid only when protocol is TCP(6) or UDP(17).”

10.7.3 常用自定义抗攻击策略

下面列出一些常用的网络协议对应的抗攻击策略。其中对应的限速水线与攻击水线能满足大部分网络应用场景需求，仅供参考。网络管理员应该根据实际应用场景配置有效的限速水线与攻击水线。

协议名	match	policy per-src-ip	policy per-src-mac	policy per-port
BPDU	dst-mac 0180.c200.0000	不适用本策略	rate-limit 20 attatch-threshold 40	rate-limit 100 attatch-threshold 100
SNMP	etype 0x0800 protocol 17 dst-port 161	rate-limit 1000 attatch-threshold 1200	不适用本策略	rate-limit 2000 attatch-threshold 3000
RSVP	etype 0x0800 protocol 46	rate-limit 800 attatch-threshold 1200	不适用本策略	rate-limit 1200 attatch-threshold 1500

- 自定义抗攻击为了最大限度地包含已有的协议类型，同是便于新的协议类型的扩展，开放允许用户自由组合报文的类型字段。若是配置不当，则可能导致网络出现异常。因此要求网络管理员对网络协议有较好的掌握。常用自定义抗攻击策略列出了当前已知协议的有效配置，管理员可参照进行配置。对于表中未列出的其它协议，需要谨慎配置使用。

10.7.4 设置对攻击者的隔离时间

对攻击者的隔离时间默认为 0，即不对攻击者进行隔离。

命令	作用
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**nfpp**	进入 NFPP 配置模式
Ruijie(config-nfpp)#**define** *name*	进入自定义抗攻击配置模式
Ruijie(config-nfpp)#**isolate-period** {*seconds* | **permanent**}	配置对攻击者的隔离时间。 取值范围为 0 秒，30 秒到 86400 秒（即一天），缺省值为 0 秒，表示不隔离；**permanent** 表示永久隔离。
Ruijie(config-nfpp)#**end**	退回到特权模式。
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**interface** *interface-name*	进入接口配置模式。
Ruijie(config-if)# **nfpp define name isolate-period** {*seconds* | **permanent**}	在端口上配置对攻击者的隔离时间。 取值范围为 0 秒，180 秒到 86400 秒（即一天），缺省情况是没有配置局部隔离时间，采用全局隔离时间。0 秒表示不隔离；**permanent** 表示永久隔离。

Ruijie(config-if)#**end**	退回到特权模式。
Ruijie#**show nfpp define summary** *name*	核对配置参数
Ruijie#**copy running-config startup-config**	保存配置。

如果要把全局隔离时间恢复成缺省值，在 nfpp 自定义抗攻击配置模式执行命令“**no isolate-period**”。如果一个端口原来配置了局部隔离时间，现在想采用全局隔离时间，那么在接口配置模式下执行命令“**no nfpp define** *name***(**自定义抗攻击名字**) isolate-period**”把局部隔离时间配置删除。

配置了隔离时间就是打开了 NFPP 硬件隔离功能，若有用户攻击则会消耗硬件表项资源，与其它安全功能（如 Web 认证等）进行硬件资源的竞争。因此配置隔离时间将会打印如下日志提醒管理员：

```
%NFPP-4-RESOURCE_COMPETITION: NFPP isolation will compete for hardware resources with other security features.
```

10.7.5 设置对攻击者的监控时间

如果隔离时间为 0（即不隔离），防攻击模块将自动根据配置的监控时间对攻击者进行软件监控，提供当前系统中存在哪些攻击者的信息。当把隔离时间配置成非零值后，防攻击将自动对软件监控的主机采取硬件隔离。

命令	作用
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**nfpp**	进入 NFPP 配置模式
Ruijie(config-nfpp)#**define** *name*	进入自定义抗攻击配置模式
Ruijie(config-nfpp)# **monitor-period** *seconds*	配置对攻击者的监控时间。 取值范围为 180 秒到 86400 秒（即一天），缺省值为 600 秒。
Ruijie(config-nfpp)#**end**	退回到特权模式。
Ruijie#**show nfpp define summary** *name*	核对配置参数
Ruijie#**copy running-config startup-config**	保存配置。

如果要把监控时间恢复成缺省值，在 nfpp 自定义配置模式执行命令“**no monitor-period**”。

检测出攻击者的时候，如果隔离时间为 0，将对攻击者进行软件监控，超时为监控时间。在软件监控过程中，当隔离时间被配置为非零值时，将自动对软件监控的攻击者采取硬件隔离，并且把超时设置为隔离时间。监控时间在隔离时间为 0 的情况下才有意义。

如果把隔离时间从非零值改成零，将直接把相关端口的攻击者删除，而不是进行软件监控。

10.7.6 设置受监控主机的最大数目

命令	作用
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**nfpp**	进入 NFPP 配置模式。
Ruijie(config-nfpp)#**define** *name*	进入自定义抗攻击配置模式
Ruijie(config-nfpp)#**monitored-host-limit** *number*	配置受监控主机的最大数目。 取值范围为 1 到 4294967295，缺省情况下受监控主机的最大数目为 1000 个。

Ruijie(config-nfpp)#**end**	退回到特权模式。
Ruijie#**show nfpp define summary** *name*	核对配置参数
Ruijie#**copy running-config startup-config**	保存配置。

如果要把配置的最大受监控主机数恢复成缺省值，在 nfpp 自定义配置模式执行命令“**no monitored-host-limit**”。

如果受监控主机数已经达到默认的 1000 个，此时管理员把受监控主机的最大数目设置成小于 1000，不会删除已有的受监控主机，而是打印信息“%ERROR：The value that you configured is smaller than current monitored hosts 1000（配置的受监控主机数），please clear a part of monitored hosts.”来提醒管理员配置没有生效，需要删除部分已经被监控的主机。

- 当受监控主机表满时，打印日志“% NFPP_DEFINE_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of name(自定义抗攻击类型名字)'s 1000（配置的受监控主机数） monitored hosts.”提醒管理员。

10.7.7 设置不监控的可信主机

如果管理员希望对某台主机不进行监控，即对该主机表示信任，则可以通过该命令配置。该可信主机发往 CPU 的 IP 报文将被允许发往 CPU。必须在配置 match 规则后才能添加不监控的可信主机。

命令	作用
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**nfpp**	进入 NFPP 配置模式
Ruijie(config-nfpp)#**define** *name*	进入 NFPP 自定义抗攻击配置模式
Ruijie(config-nfpp-define)#**trusted-host** {*mac mac_mask* | *ip mask* }	配置不进行监控的主机。 最多能够配置 500 条。
Ruijie(config-nfpp-define)#**end**	退回到特权模式。
Ruijie# **show nfpp define trusted-host** *name*	查看配置的可信主机
Ruijie**#copy running-config startup-config**	保存配置。

在 nfpp 自定义抗攻击配置模式下，可以使用该命令的 **no** 选项删除一条可信主机表项。使用命令的 **no** 和 **all** 选项可以删除所有可信主机。

例如删除所有可信主机：

```
Ruijie(config-nfpp-define)# no trusted-host all
```

或删除单条可信主机表项：

```
Ruijie(config-nfpp-define)# no trusted-host 1.1.1.1 255.255.255.255
```

- 当还未配置 match 类型时，打印提示信息“%ERROR: Please configure match rule first.”
- 当添加 IPv4 可信主机，但 match 规则的 etype 不为 IPv4 时，打印提示信息“%ERROR: Match type can't support IPv4 trusted host.”
- 当不监控的可信主机表满时，打印提示信息“%ERROR: Attempt to exceed limit of 500 trusted hosts.”提醒管理员。
- 当受监控主机表中存在与可信主机相匹配的表项（IP 地址相同）时，系统将自动删除此 IP 地址对应的表项。
- 当删除可信主机失败时，打印提示信息“%ERROR: Failed to delete trusted host 1.1.1.0 255.255.255.0（配置的可信主机）.”提醒管理员。

- 当添加可信主机失败时，打印提示信息“%ERROR: Failed to add trusted host 1.1.1.0 255.255.255.0（配置的可信主机）.”提醒管理员。
- 当添加的可信主机已经存在时，打印提示信息“%ERROR: Trusted host 1.1.1.0 255.255.255.0（配置的可信主机）has already been configured.”提醒管理员。
- 当要删除的可信主机不存在时，打印提示信息“%ERROR: Trusted host 1.1.1.0 255.255.255.0（配置的可信主机）is not found.”提醒管理员。
- 当无法为可信主机分配内存时，打印提示信息“%ERROR: Failed to allocate memory.”提醒管理员。

10.7.8 基于主机限速和识别攻击

识别主机的方法根据配置的抗攻击策略而定，包含源 IP 地址/VID/端口(per-src-ip)识别主机和源 MAC/VID/端口(per-src-mac)识别主机，两种方法可以同时生效，也可以都不生效。识别主机的方法是否生效的依据是用户是否配置了该方法的限速水线和攻击水线。每台主机都有限速水线和攻击阈值（也称为告警水线），限速水线必须低于攻击阈值。当单台主机的自定义类型报文速度超过限速水线时，就丢弃超限的自定义类型报文。如果单台主机的自定义类型报文速度超过攻击阈值，将采取隔离措施，记录到日志中，发送 TRAP。

当检测到攻击行为时，打印的日志信息格式如下：

```
%NFPP_DEFINE_GUARD-4- DOS_DETECTED: Host<IP=1.1.1.1,MAC= N/A,port=Gi4/1,VLAN=1> was detected by name(自定义抗攻击名字). (2009-07-01 13:00:00)
```

发送的 TRAP 报文的数据中包含如下描述信息：

```
name(自定义抗攻击名字) DoS attack from host<IP=1.1.1.1,MAC= N/A,port=Gi4/1,VLAN=1> was detected.
```

如果管理员把隔离时间配置成非零值，当硬件隔离成功时，打印的日志信息格式如下所示：

```
%NFPP_DEFINE_GUARD-4-ISOLATED:Host<IP=1.1.1.1, MAC= N/A ,port=Gi4/1,VLAN=1> was isolated by name(自定义抗攻击名字). (2009-07-01 13:00:00)
```

发送的 TRAP 报文的数据包含如下描述信息：

```
Host<IP=1.1.1.1,MAC=N/A,port=Gi4/1,VLAN=1> was isolated by name(自定义抗攻击名字).
```

当硬件隔离失败（原因通常是内存不足或者硬件资源不足）时，打印的日志信息格式如下所示：

```
%NFPP_DEFINE_GUARD-4-ISOLATE_FAILED:Failed to isolate host<IP=1.1.1.1, MAC= N/A ,port=Gi4/1,VLAN=1> by name(自定义抗攻击名字).(2009-07-01 13:00:00)
```

发送的 TRAP 报文的数据包含如下描述信息：

```
Failed to isolate host<IP=1.1.1.1,MAC= N/A,port=Gi4/1,VLAN=1> by name(自定义抗攻击名字).
```

管理员可以在 **nfpp** 自定义配置模式下和接口配置模式下进行配置。

命令	作用

Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**nfpp**	进入 NFPP 配置模式。
Ruijie(config-nfpp)#**define** *name*	进入 nfpp 自定义抗攻击配置模式
Ruijie(config-nfpp-define)# **global-policy** {**per-src-ip** | **per-src-mac**} *rate-limit-pps attack-threshold-pps*	配置基于主机的限速和攻击水线。 **per-src-ip** 表示基于源 IP/VID/端口识别主机进行速率统计。**per-src-mac** 表示基于源 MAC/VID/端口识别主机进行速率统计。 *rate-limit-pps* 是限速水线，取值范围是 1 到 9999，缺省是不需要进行速率限制。自定义报文超过限速水线后的报文将被丢弃。 *attack-threshold-pps* 是攻击水线，取值范围是 1 到 9999。自定义报文超过攻击水线，将会认为存在攻击，打印日志，发送 trap，并根据配置的隔离时间对用户进行隔离。 缺省是不需要进行速率限制。 攻击水线必须大于或者等于限速水线。
Ruijie(config-nfpp)#**end**	退回到特权模式。
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**interface** *interface-name*	进入接口配置模式。
Ruijie(config-if)#**nfpp define** *name* **policy** {**per-src-ip** | **per-src-mac**} *rate-limit-pps attack-threshold-pps*	配置局部的限速水线和攻击水线，只在该配置所属端口上生效。 **per-src-ip** 表示基于源 IP/VID/端口识别主机进行速率统计。**per-src-mac** 表示基于源 MAC/VID/端口识别主机进行速率统计。 *rate-limit-pps* 是限速水线，取值范围是 1 到 9999，缺省是不需要进行速率限制。自定义报文超过限速水线后的报文将被丢弃。 *attack-threshold-pps* 是攻击水线，取值范围是 1 到 9999。自定义报文超过攻击水线，将会认为存在攻击，打印日志，发送 trap，并根据配置的隔离时间对用户进行隔离。 缺省是使用全局配置的限速水线和攻击水线。 攻击水线必须大于或者等于限速水线。
Ruijie(config-if)#**end**	退回到特权模式。
Ruijie**#show nfpp define summary** *name*	核对配置参数
Ruijie#**copy running-config startup-config**	保存配置。

- 基于源 MAC/VID/端口的限速优先级高于基于源 IP/VID/端口的限速。
- 自定义抗攻击的端口识别主机策略要与全局的保持一致。
- 若全局没配置 per-src-ip 策略，端口配置 per-src-ip 策略时，打印提示 “%ERROR: name(自定义抗攻击名字) has not per-src-ip policy.”，提醒管理员配置失败。
- 若全局没配置 per-src-mac 策略，端口配置 per-src-mac 策略时，打印提示 “%ERROR: name(自定义抗攻击名字) has not per-src-mac policy.”，提醒管理员配置失败。

当无法为检测到的攻击者分配内存时，打印日志“%NFPP_DEFINE_GUARD-4-NO_MEMORY: Failed to allocate memory.”提醒管理员。

10.7.9 基于端口限速和识别攻击

抗攻击策略可以设置端口的限速水线和攻击阈值，限速水线必须低于攻击阈值。当某个端口的自定义类型报文速度超过限速水线时，就丢弃超限的自定义类型报文。如果某个端口的自定义类型报文速度超过攻击阈值，将记录到日志中，发送 TRAP。

当端口遭受 ARP 拒绝服务攻击时，打印的警告信息格式如下：

```
%NFPP_DEFINE_GUARD-4-PORT_ATTACKED: name(自定义抗攻击名字) DoS attack was detected on port Gi4/1.
(2009-07-01 13:00:00)
```

发送的 TRAP 报文的数据包含如下描述信息：

```
name(自定义抗攻击名字) DoS attack was detected on port Gi4/1.
```

管理员可以在 **nfpp** 自定义配置模式下和接口配置模式下进行配置。

命令	作用
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**nfpp**	进入 NFPP 配置模式。
Ruijie(config-nfpp)#**define** *name*	进入 nfpp 自定义抗攻击配置模式
Ruijie(config-nfpp-define)# **global-policy per-port** *rate-limit-pps attack-threshold-pps*	配置基于主机的限速和攻击水线。 **per-port** 表示基于每个报文接收的物理端口进行速率统计。 *rate-limit-pps* 是限速水线，取值范围是 1 到 9999，缺省是不需要进行速率限制。自定义报文超过限速水线后的报文将被丢弃。 *attack-threshold-pps* 是攻击水线，取值范围是 1 到 9999。自定义报文超过攻击水线，将会认为存在攻击，打印日志，发送 trap，并根据配置的隔离时间对用户进行隔离。 缺省是使用全局配置的限速水线和攻击水线。 攻击水线必须大于或者等于限速水线。
Ruijie(config-nfpp)#**end**	退回到特权模式。
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**interface** *interface-name*	进入接口配置模式。

Ruijie(config-if)#**nfpp define** *name* **policy per-port** *rate-limit-pps attack-threshold-pps*	配置局部的限速水线和攻击水线，只在该配置所属端口上生效。 **per-port** 表示基于每个报文接收的物理端口进行速率统计。 *rate-limit-pps* 是限速水线，取值范围是 1 到 9999，缺省是不需要进行速率限制。自定义报文超过限速水线后的报文将被丢弃。 *attack-threshold-pps* 是攻击水线，取值范围是 1 到 9999。自定义报文超过攻击水线，将会认为存在攻击，打印日志，发送 trap。 缺省是不需要进行速率限制。 攻击水线必须大于或者等于限速水线。
Ruijie(config-if)#**end**	退回到特权模式。
Ruijie#**show nfpp define summary** *name*	核对配置参数
Ruijie#**copy running-config startup-config**	保存配置。

基于主机的限速优先级高于基于端口限速。

若自定义抗攻击全局没配置 per-port 策略，端口配置 per-port 策略时，打印提示“%ERROR: name(自定义抗攻击名字) has not per-port policy.”，提醒管理员配置失败。

10.7.10 应用自定义抗攻击功能

管理员可以在 **nfpp** 配置模式或者接口配置模式下应用自定义抗攻击功能，缺省情况下是关闭的。

命令	作用
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**nfpp**	进入 NFPP 配置模式。
Ruijie(config-nfpp)# **define** *name* **enable**	全局打开自定义抗攻击功能。默认情况下所有端口都打开自定义抗攻击功能。
Ruijie(config-nfpp)#**end**	退回到特权模式。
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**interface** *interface-name*	进入接口配置模式。
Ruijie(config-if)#**nfpp define** *name* **enable**	在端口上打开自定义抗攻击功能，缺省情况是端口没有配置局部开关，采用全局开关。
Ruijie(config-if)#**end**	退回到特权模式。
Ruijie#**show nfpp define summary** *name*	核对配置参数
Ruijie#**copy running-config startup-config**	保存配置。

如果要关闭抗功能功能，可以在 NFPP 配置模式下执行”**no define** *name* **enable**”命令关闭全局自定义抗攻击功能，或者在接口配置模式下执行”**no nfpp define** *name* **enable**”命令关闭接口下的自定义抗攻击功能。如果想恢复接口配置，使接口使用全局的自定义抗攻击功能开关，需要在接口配置模式下执行”**default nfpp define** *name* **enable**”。

当自定义抗攻击策略还没配置完全时，无法打开自定义抗攻击功能，并提示用户缺少相应的策略配置。

当自定义抗攻击名字不存在时，打印提示信息：“%ERROR: The name is not exist.”。

- 当自定义抗攻击未配置 match 类型时，打印提示信息：“%ERROR：name（自定义抗攻击类型名字）doesn’t match any type.”
- 当自定义抗攻击未配置 policy 策略时，打印提示信息：“%ERROR：name（自定义抗攻击类型名字）doesn’t specify any policy.”

10.7.11 清除受监控主机

已被隔离的主机在一段时间后自动恢复，如果管理员要手动清除该主机，可以在特权模式下用以下命令清除。

命令	作用
Ruijie# **clear nfpp define hosts** *name* [**vlan** *vid*] [**interface** *interface-id*] [*ip-address*] [*mac-address*]	带参数表示清除符合条件的主机。

10.7.12 查看自定义抗攻击的配置参数

使用 **show nfpp define summary** 查看自定义抗攻击的配置参数：

命令	作用
show nfpp define summary [*name*]	查看自定义抗攻击配置参数，不带 *name* 表示显示所有自定义抗攻击的配置信息。

下面是一个例子：

```
Ruijie# show nfpp define summary tcp
Define tcp summary:
match etype 0x800 protocol 6
Maximum count of monitored hosts: 1000
Monitor period：300s
 (Format of column Rate-limit and  Attack-threshold is per-src-ip/per-src-mac/per-port.)
Interface  Status  Isolate-period Rate-limit Attack-threshold
Global      Enable  300             -/5/150     -/10/300
G 0/1       Enable  180             -/6/-       -/8/-
G 0/2       Disable 200             -/5/30     -/10/50
```

10.7.13 查看受监控主机的信息

命令	作用
show nfpp define hosts *name* **[statistics** | **[vlan** *vid*] [**interface** *interface-id*] [*ip-address*] [*mac-address*]]]	查看已被检测到攻击的主机。 不带参数表示显示所有已被检测到攻击的主机，带参数则只显示符合条件的主机。

下面是一个例子：

```
Ruijie#show nfpp define hosts tcp statistics
```

```
Define tcp:
success    fail    total
-------    ----    -----
100         20       120
```

意思是：“总共有 120 台主机被隔离，其中 100 台主机隔离成功，20 台主机隔离失败”。

```
Ruijie#show nfpp define hosts tcp
Define tcp:
If column 1 shows '*', it means "hardware do not isolate host".
VLAN  interface    IP address  remain-time(s)
----    --------   ---------    -------------
1      Gi0/1         1.1.1.1     110
*2      Gi0/2         1.1.2.1     61
Total: 2 host(s)
```

上述几个字段分别表示 VLAN 号、端口、IP 地址、MAC 地址，以及隔离剩余时间。

如果某一行的第一列显示“*”， 表示这台主机目前只是软件监控或者硬件因为资源不足而隔离失败。

10.7.14 查看不监控的可信主机

使用 **show nfpp define trusted-host** 查看不受监控的可信主机：

命令	作用
show nfpp define trusted-host *name*	查看不受监控的可信主机。

下面是一个例子：

```
Ruijie# show nfpp define trusted-host tcp
Define tcp:
IP address      mask
---------       ------
1.1.1.0         255.255.255.0
1.1.2.0         255.255.255.0
Total: 2 record(s)
```

10.8 NFPP日志信息

10.8.1 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。

10.8.2 配置日志缓冲区容量

管理员可以在 **nfpp** 配置模式下配置日志缓冲区的容量。

命令	作用
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**nfpp**	进入 NFPP 配置模式。
Ruijie(config-nfpp)# **log-buffer entries** *number*	配置 NFPP 日志缓冲区大小（范围 0-1024），单位是日志条数，缺省值为 256。
Ruijie(config-nfpp)#**end**	退回到特权模式。
Ruijie# **show nfpp log summary**	核对配置参数。

10.8.3 配置生成系统消息的速率

管理员可以在 **nfpp** 配置模式下配置生成系统消息的速率。

命令	作用
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**nfpp**	进入 NFPP 配置模式。
Ruijie(config-nfpp)# **log-buffer logs** *number_of_message* **interval** *length_in_seconds*	配置从专用日志缓冲区取日志生成系统消息的速率。生成系统消息的速率为 *number_of_message /length_in_seconds*，生成系统消息的同时还会删除专用缓冲区中的对应信息 *number_of_message*，缺省值为 1，范围为 0-1024，0 表示日志全部记录在专用缓冲区，不生成系统消息。 *length_in_seconds*，缺省值为 30，范围为 0-86400s（1 天），0 表示日志立即生成系统消息。 *number_of_message* 和 *length_in_seconds* 都为 0 表示日志立即生成系统消息。
Ruijie(config-nfpp)#**end**	退回到特权模式。
Ruijie# **show nfpp log summary**	核对配置参数。

10.8.4 配置日志过滤

管理员可以对日志进行过滤，只记录指定 VLAN 或指定端口的日志信息。

命令	作用
Ruijie#**configure terminal**	进入全局配置模式。
Ruijie(config)#**nfpp**	进入 NFPP 配置模式。
Ruijie(config-nfpp)# **logging vlan** *vlan-range*	指定需要记录哪些 VLAN 的日志。 缺省情况是所有日志都记录。

Ruijie(config-nfpp)# **logging interface** *interface-id*	指定需要记录哪个端口的日志。 缺省情况是所有日志都记录。
Ruijie(config-nfpp)#**end**	退回到特权模式。
Ruijie# **show nfpp log summary**	核对配置参数。

10.8.5 清除日志

命令	作用
clear nfpp log	清空日志缓冲区。

10.8.6 显示日志

命令	作用
show nfpp log summary	查看 NFPP 日志信息配置。
show nfpp log buffer [**statistics**]	显示 NFPP 的日志缓冲区。 带参数 statistics 表示显示日志缓冲区中的日志条数。

查看 NFPP 日志信息配置。

```
Ruijie#show nfpp log summary
Total log buffer size : 10
Syslog rate : 1 entry per 2 seconds
Logging:
VLAN  1-3, 5
interface Gi 0/1
interface Gi 0/2
```

查看 NFPP 日志缓冲区中日志条数。

```
Ruijie#show nfpp log buffer statistics
There are 6 logs in buffer.
```

查看 NFPP 的日志缓冲区。

```
Ruijie#show nfpp log buffer
Protocol VLAN  Interface IP address MAC address     Reason          Timestamp
-------- ----  --------- ---------- -----------     ------          ---------
ARP   1      Gi0/1       1.1.1.1      -              DoS             2009-05-30 16:23:10
ARP   1      Gi0/1       1.1.1.1      -              ISOLATED        2009-05-30 16:23:10
ARP   1      Gi0/1       1.1.1.2      -              DoS             2009-05-30 16:23:15
ARP   1      Gi0/1       1.1.1.2      -              ISOLATE_FAILED 2009-05-30 16:23:15
ARP   1      Gi0/1       -          0000.0000.0001  SCAN            2009-05-30 16:30:10
ARP   -      Gi0/2       -          -                 PORT_ATTACKED   2009-05-30 16:30:10
```

Protocol 有以下取值：

- ARP（对应 ARP 抗攻击）
- IP（对应 IP 防扫描）
- ICMP（对应 ICMP 抗攻击）
- DHCP（对应 DHCP 抗攻击）
- NS-NA（对应 ND 抗攻击中的邻居请求和邻居公告）
- RS（对应 ND 抗攻击中的路由器请求）
- RA-REDIRECT（对应 ND 抗攻击中的路由器公告和重定向报文）
- name (自定义抗攻击的名称)

Reason 表示原因，有 5 种取值：

- DoS 表示检测到拒绝服务攻击
- ISOLATED 表示攻击者被硬件成功地隔离
- ISOLATE_FAILED 表示隔离攻击者失败
- SCAN 表示检测到扫描
- PORT_ATTACKED 表示端口被攻击

当日志缓冲区溢出时，后续的日志将被丢弃，同时在日志缓冲区中显示一条所有属性都为"-"的表项。管理员需要增加日志缓冲区容量或者提高生成系统消息的速率。

从日志缓冲区取日志生成的系统消息带有事件发生的时间戳，如下所示：

%NFPP_ARP_GUARD-4-DOS_DETECTED: Host<IP=N/A,MAC=0000.0000.0004,port=Gi4/1,VLAN=1> was detected.(2009-07-01 13:00:00)

配置指南-ACL&QOS

本分册介绍 ACL&QOS 配置指南相关内容，包括以下章节：

1. ACL
2. IP QOS

1 ACL

1.1 访问控制列表概述

作为锐捷产品安全解决方案的一部分，使用访问控制列表提供强大的数据流过滤功能。锐捷产品目前支持多种访问列表。您可以根据网络具体情况选择不同的访问控制列表对数据流进行控制。

1.1.1 访问控制列表简介

ACLs 的全称为接入控制列表(Access Control Lists)，也称为访问列表（Access Lists），俗称为防火墙，在有的文档中还称之为包过滤。ACLs 通过定义一些规则对网络设备接口上的数据报文进行控制：允许通过或丢弃。按照其使用的范围，可以分为安全 ACLs 和 QoS ACLs。

对数据流进行过滤可以限制网络中的通讯数据的类型，限制网络的使用者或使用的设备。安全 ACLs 在数据流通过网络设备时对其进行分类过滤，并对从指定接口输入或者输出的数据流进行检查，根据匹配条件(Conditions)决定是允许其通过(Permit)还是丢弃(Deny)。

总的来说，安全 ACLs 用于控制哪些数据流允许从网络设备通过，Qos 策略对这些数据流进行优先级分类和处理。

ACLs 由一系列的表项组成，我们称之为接入控制列表表项(Access Control Entry：ACE)。每个接入控制列表表项都申明了满足该表项的匹配条件及行为。

访问列表规则可以针对数据流的源地址、目标地址、上层协议，时间区域等信息。

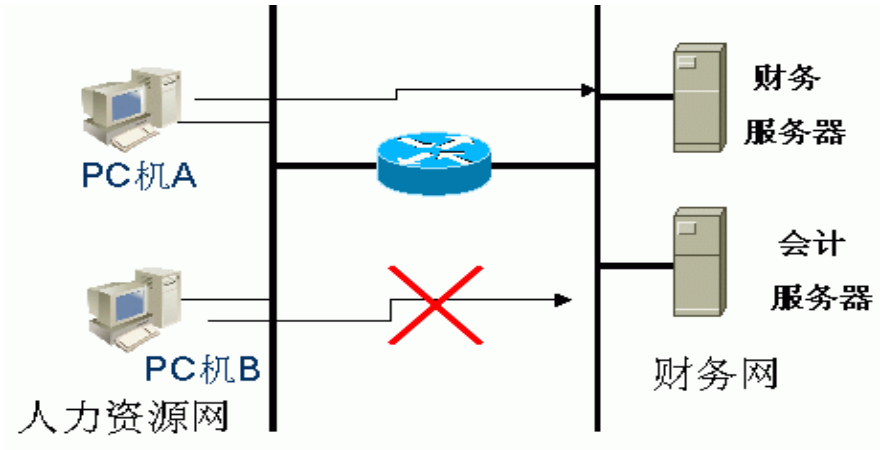
1.1.2 为什么要配置访问列表

配置访问列表的原因比较多，主要有以下一些：

- 限制路由更新：控制路由更新信息发往什么地方，同时希望在什么地方收到路由更新信息。
- 限制网络访问：为了确保网络安全，通过定义规则，可以限制用户访问一些服务（如只需要访问 WWW 和电子邮件服务，其他服务如 TELNET 则禁止），或者仅允许在给定的时间段内访问，或只允许一些主机访问网络等等。

下图是一个案例，在该案例中，只允许主机 A 访问财务网络，而主机 B 禁止访问。如下图所示。

图 1-1 使用访问列表控制网络访问



1.1.3 什么时候配置访问列表

您可以根据需要选择基本访问列表或动态访问列表。一般情况下，使用基本访问列表已经能够满足安全需要。但经验丰富的黑客可能会通过一些软件假冒源地址欺骗设备，得以访问网络。而动态访问列表在用户访问网络以前，要求通过身份认证，使黑客难以攻入网络，所以在一些敏感的区域可以使用动态访问列表保证网络安全。

通过假冒源地址欺骗设备即电子欺骗是所有访问列表固有的问题，使用动态列表也会遭遇电子欺骗问题：黑客可能在用户通过身份认证的有效访问期间，假冒用户的地址访问网络。解决这个问题的方法有两种，一种是尽量将用户访问的空闲时间设置小些，这样可以使黑客更难以攻入网络，另一种是使用 IPSEC 加密协议对网络数据进行加密，确保进入设备时，所有的数据都是加密的。

访问列表一般配置在以下位置的网络设备上：

- 内部网和外部网（如 INTERNET）之间的设备
- 网络两个部分交界的设备
- 接入控制端口的设备.

访问控制列表语句的执行必须严格按照表中语句的顺序，从第一条语句开始比较，一旦一个数据包的报头跟表中的某个条件判断语句相匹配，那么后面的语句就将被忽略，不再进行检查。

1.1.4 输入/输出ACL、过滤域模板及规则

输入 ACL 在设备接口接收到报文时，检查报文是否与该接口输入 ACL 的某一条 ACE 相匹配；输出 ACL 在设备准备从某一个接口输出报文时，检查报文是否与该接口输出 ACL 的某一条 ACE 相匹配。

在制定不同的过滤规则时，多条规则可能同时被应用，也可能只应用其中几条。只要是符合某条 ACE，就按照该 ACE 定义的处理报文(Permit 或 Deny)。ACL 的 ACE 根据以太网报文的某些字段来标识以太网报文的，这些字段包括：

二层字段(Layer 2 Fields)：

- 48 位的源 MAC 地址(必须申明所有 48 位)
- 48 位的目的 MAC 地址(必须申明所有 48 位)
- 16 位的二层类型字段

三层字段(Layer 3 Fields)：

- 源 IP 地址字段(可以申明全部源 IP 地址值，或申明您所定义的子网来定义一类流)
- 目的 IP 地址字段(可以申明全部目的 IP 地址值，或申明您所定义的子网来定义一类流)
- 协议类型字段

四层字段(Layer 4 Fields)：

- 可以申明一个 TCP 的源端口、目的端口或者都申明
- 可以申明一个 UDP 的源端口、目的端口或者都申明

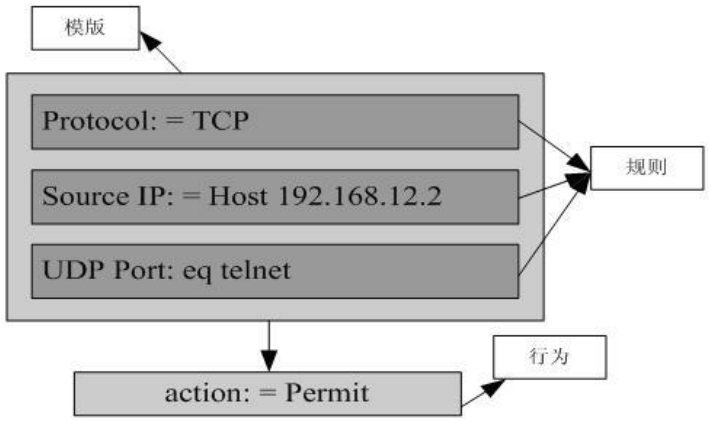
过滤域指的就是您在生成一条 ACE 时，根据报文中的哪些字段用以对报文进行识别、分类。过滤域模板就是这些字段组合的定义。比如，您在生成某一条 ACE 时希望根据报文的目的 IP 字段对报文进行识别、分类，而在生成另一条 ACE 时，希望根据的是报文的源 IP 地址字段和 UDP 的源端口字段，这样，这两条 ACE 就使用了不同的过滤域模板。

规则(Rules)，指的是 ACE 过滤域模板对应的值。 比如有一条 ACE 内容如下：

```
permit tcp host 192.168.12.2 any eq telnet
```

在这条 ACE 中，过滤域模板为以下字段的集合：源 IP 地址字段、IP 协议字段、目的 TCP 端口字段。对应的值(Rules)分别为：源 IP 地址＝Host 192.168.12.2；IP 协议＝TCP；TCP 目的端口＝Telnet。

图 1-2 对 ACE：permit tcp host 192.168.12.2 any eq telnet 的分析



过滤域模板可以是三层字段(Layer 3 Field)和四层字段(Layer 4 Field)字段的集合，也可以是多个二层字段(Layer 2 Field)的集合，但标准与扩展的 ACL 的过滤域模板不能是二层和三层、二层和四层、二层和三层、四层字段的集合。

OUT 方向 ACL 关联 SVI 的注意事项：支持 IP 标准，IP 扩展，MAC 扩展。

对 ACL 中匹配目的 IP 和目的 MAC 有一些限制，如果在 MAC 扩展中匹配目的 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。

应用 ACL 时，如果 ACL（包括 IP 访问列表）中的 ACE 匹配了非 L2 字段，比如 SIP，DIP 时，对于带标签的 MPLS 报文匹配是无效的。

1.1.5 ACL logging

为了让用户更好的掌握 ACL 在设备中的运行状态，在添加规则时可以根据需要决定是否指定报文匹配日志输出选项，如果指定了该选项，则在规则匹配到报文时会输出匹配日志信息。ACL logging 信息是基于 ACE 来打印 log 信息的，也即设备周期性的打印命中报文的 ACE 信息，以及该 ACE 命中的报文数量。如下：

```
*Sep  9 16:23:06: %ACL-6-MATCH: ACL 100 ACE 10 permit icmp any any, match 78 packets.
```

为合理控制 log 输出的数量和频率，ACL logging 支持配置 log 输出间隔的配置，并且分别配置 IPv4 ACL 的 log 输出间隔。

默认 ACL logging 的 log 输出间隔是 0，也即不输出 log。在为 ACE 指定了报文匹配日志输出选项后，若要输出相应的 log，需要配置 ACL logging 的输出间隔。

对于带 ACL logging 选项的 ACE，如果指定的时间间隔内没有匹配到任何报文，则不会输出与该 ACE 有关的报文匹配日志。如果指定的时间间隔内有匹配到报文，则时间间隔到期后，会输出与该 ACE 有关的报文匹配日志。其中的报文命中数目为该时间间隔内该 ACE 匹配到的报文总数，即为该 ACE 上一次输出 log 到本次输出 log 之间命中的报文数。

ACL logging 中的报文匹配计数只会输出安全 ACL 的匹配计数。如果非安全 ACL 如 QoS、PBR 等引用的 ACL 中有 ACE 带有 log 选项，log 选项不会对这些非安全 ACL 起作用，输出的报文匹配日志的计数也不会包含非安全 ACL 的报文匹配计数。

在 NBS200F 系列产品上，带 ACL logging 选项的 ACE 使用更多的硬件资源，如果配置的所有 ACE 都带有 ACL logging 选项，则会导致设备的 ACE 容量减半。

1.1.6 ACL报文匹配计数

由于网络管理的需要，有时用户可能会想知道某条 ACE 有没有匹配到报文，匹配了多少个。因此，ACL 提供了基于 ACE 的报文匹配计数，用户可以基于 ACL 开启和关闭该 ACL 下的所有的 ACE 的报文匹配计数功能，支持的 ACL 类型包括：IP 访问列表、MAC 访问列表。此外，用户可通过 ACL 的统计清除命令将 ACL 规则的报文匹配计数器清 0，以便重新统计。

ACL 报文匹配计数只针对安全 ACL，对于非安全 ACL 的报文匹配不会进行计数。

在 NBS200F 系列产品上开启 ACL 的报文匹配计数功能需要更多的硬件表项，极端情况下会使设备可以配置的 ACE 容量减半。

1.2 配置IP访问列表

要在设备上配置访问列表，必须为协议的访问列表指定一个唯一的名称或编号，以便在协议内部能够唯一标识每个访问列表。下表列出了可以使用编号来指定访问列表的协议以及每种协议可以使用的访问列表编号范围。

协议	编号范围
标准 IP	1-99，1300 - 1999
扩展 IP	100-199，2000 - 2699

1.2.1 IP访问列表配置指导

创建访问列表时，定义的规则将应用于设备上所有的分组报文，设备通过判断分组是否与规则匹配来决定是否转发或阻断分组报文。

基本访问列表包括标准访问列表和扩展访问列表，访问列表中定义的典型规则主要有以下：

- 源地址
- 目标地址
- 上层协议
- 时间区域

标准 IP 访问列表（编号为 1 - 99，1300 - 1999）主要是根据源 IP 地址来进行转发或阻断分组的，扩展 IP 访问列表（编号为 100 – 199，2000 - 2699）使用以上四种组合来进行转发或阻断分组的。其他类型的访问列表根据相关代码来转发或阻断分组的。

对于单一的访问列表来说，可以使用多条独立的访问列表语句来定义多种规则，其中所有的语句引用同一个编号或名字，以便将这些语句绑定到同一个访问列表。不过，使用的语句越多，阅读和理解访问列表就越来越困难。

隐含“拒绝所有数据流”规则语句

在每个访问列表的末尾隐含着一条“拒绝所有数据流”规则语句，因此如果分组与任何规则都不匹配，将被拒绝。

如下例：

```
Access-list 1 permit host 192.168.4.12
```

此列表只允许源主机为 192.168.4.12 的报文通过，其它主机都将被拒绝。因为这条访问列表最后包含了一条规则语句：access-list 1 deny any。

又如：

```
Access-list 1 deny host 192.168.4.12
```

如果列表只包含以上这一条语句，则任何主机报文通过该端口时都将被拒绝。

> 在定义访问列表的时候，要考虑到路由更新的报文。由于访问列表末尾“拒绝所有数据流”，可能导致所有的路由更新报文被阻断。

输入规则语句的顺序

加入的每条规则都被追加到访问列表的最后，语句被创建以后，就无法单独删除它，而只能删除整个访问列表。所以访问列表语句的次序非常重要。设备在决定转发还是阻断分组时，设备按语句创建的次序将分组与语句进行比较，找到匹配的语句后，便不再检查其他规则语句。

假设创建了一条语句，它允许所有的数据流通过，则后面的语句将不被检查。

如下例：

```
access-list 101 deny ip any any
access-list 101 permit tcp 192.168.12.0 0.0.0.255  eq  telnet any
```

由于第一条规则语句拒绝了所有的 IP 报文，所以 192.168.12.0/24 网络的主机 Telnet 报文将被拒绝，因为设备在检查到报文和第一条规则语句匹配，便不再检查后面的规则语句。

1.2.2 配置IP访问列表

基本访问列表的配置包括以下两步：

- 定义基本访问列表
- 将基本访问列表应用于特定接口

要配置基本访问列表，有以下两种方式：

方式一　在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)# **access-list** *id* {**deny	permit**} {src *src-wildcard*	**host** *src*	**any** } [**time-range** *tm-rng-name*] [**log**]	定义访问列表
Ruijie(config)# **interface** *interface*	选择要应用访问列表的接口
Ruijie(config-if)# **ip access-group** *id* { **in	out** }	将访问列表应用特定接口

方式二　在 ACL 配置模式下执行以下命令：

命令	作用
Ruijie(config)# **ip access-list** { **standard	extended** } { *id*	*name* }	进入配置访问列表模式
Ruijie (config-xxx-nacl)# [*sn*] { **permit	deny** } {src *src-wildcard*	**host** *src*	**any** } [**time-range** *tm-rng-name*] [**log**]	为 ACL 添加表项,具体内容请参见命令参考
Ruijie(config-xxx-nacl)# **exit**	退出访问控制列表模式
Ruijie(config)# **interface** *interface*	选择要应用访问列表的接口
Ruijie(config-if)# **ip access-group** *id* { **in	out** }	将访问列表应用特定接口

方式一只对数值 ACL 进行配置，方式二可以对命名和数值 ACL 进行配置，还可以指定表项的优先级(在支持 ACE 优先级的设备中)。

1.2.3 显示IP访问列表的配置

要监控访问列表，请在特权用户模式执行以下命令：

命令	作用
show access-lists [*id*	*name*]	可以查看基本访问列表

配置举例：

```
Ruijie #show access-lists
Extended IP access list 101
    10 deny ip any host 11.1.1.2 log (3 matches)
```

```
    20 permit ip any any log (10690 matches)
    30 deny ip host 192.168.21.59 any log (101 matches)
    40 permit tcp host 192.168.21.59 any eq ftp log
50 permit ip host 192.168.21.59 any log
```

1.3 配置MAC扩展访问列表

要在设备上配置 MAC 访问列表，必须给协议的访问列表指定一个唯一的名称或编号，以便在协议内部能够唯一标识每个访问列表。下表列出可以使用编号来指定 MAC 访问列表编号范围。

协议	编号范围
MAC 扩展访问列表	700-799

1.3.1 MAC扩展访问列表配置指导

创建 MAC 访问列表时，定义的规则将可以应用于所有的分组报文，通过判断分组是否与规则匹配来决定是否转发或阻断分组报文。

MAC 访问列表中定义的典型规则主要有以下：

- 源 MAC 地址
- 目标 MAC 地址
- 以太网协议类型
- 时间区

MAC 扩展访问列表（编号 700 -799）主要是根据源和目的 MAC 地址来进行转发或阻断分组的，也可以对以太网协议类型匹配。

对于单一的 MAC 访问列表来说，可以使用多条独立的访问列表语句来定义多种规则，其中所有的语句需引用同一个编号或名字，以便将这些语句绑定到同一个访问列表。

1.3.2 配置MAC扩展访问列表

MAC 访问列表的配置包括以下两步：

- 定义 MAC 访问列表
- 应用列表于特定接口

要配置 MAC 访问列表，有以下两种方式：

方式一，在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)# **access-list** *id* {**deny** | **permit**}{**any** | **host** *src-mac-addr*} {**any** | **host** *dst-mac-addr*} [*ethernet-type*] [**cos** *cos*]	定义访问列表,命令的具体内容请参见命令参考

Ruijie(config)# **interface** *interface*	选择选择要应用访问列表的接口
Ruijie(config-if)# **mac access-group** *id* { **in** | **out** }	将访问列表应用特定接口

方式二，在 ACL 配置模式下执行以下命令：

命令	作用
Ruijie(config)# **mac access-list extended** {*id* | *name*}	进入配置访问列表模式
Ruijie (config-mac-nacl)# [*sn*] { **permit** | **deny** }{**any** | **host** *src-mac-addr*} {**any** | **host** *dst-mac-addr*} [*ethernet-type*] [**cos** *cos*]	为 ACL 添加表项,命令的具体内容请参见命令参考
Ruijie(config-mac-nacl)# **exit**	退出访问控制列表模式
Ruijie(config)# **interface** *interface*	选择要应用访问列表的接口
Ruijie(config-if)# **mac access-group** {*id* | *name*} { **in** | **out**}	将访问列表应用特定接口

方式一只对数值 ACL 进行配置；方式二可以对命名和数值 ACL 进行配置，还可以指定表项的优先级（支持优先级 ACE 产品）。

1.3.3 显示MAC扩展访问列表的配置

要监控访问列表，请在特权模式执行以下命令：

命令	作用
show access-lists [*id* | *name*]	可以查看基本访问列表

1.4 配置全局安全ACL

1.4.1 理解全局安全ACL

由于安全部署上的需要，端口安全 ACL 常被配置作为病毒报文过滤及防范使用，用于过滤符合某些特征的报文，比如：TCP 攻击端口。各种病毒报文在全局网络环境中存在，且各端口下的病毒报文识别特征相同或相似，因此通常情况下会创建一个 ACL，添加匹配各种病毒特征的 deny ace 后，通过端口安全 ACL 将 ACL 应用到交换机各个端口，以达到病毒过滤的作用。

端口安全 ACL 用于病毒过滤等抗攻击场景时，存在较多不便，一是需要逐个端口配置，存在重复配置、操作性能低下及 ACL 资源过度消耗的情况；二是安全 ACL 的访问控制作用被弱化，由于被用于病毒过滤，安全 ACL 的限制路由更新、限制网络访问等基本功能无法正常使用。

针对上述情况，开发了全局安全 ACL 功能，主要用于交换机全局抗病毒部署及防御，避免对端口安全 ACL 的干扰。全局安全 ACL 在所有二层接口生效，避免了多个接口重复配置操作，且支持在各个接口独立关闭，以避免设备的某些接口不希望应用全局 ACL 时，比如：作为上联口的端口，不受全局 ACL 过滤影响。

当全局安全 ACL 与端口安全 ACL 同时配置时，两者共同生效，对于命中全局安全 ACL 的报文将被当作病毒报文直接过滤，对于没有命中全局安全 ACL 的报文将继续受端口安全 ACL 控制及检测。因此，不建议在全局安全 ACL 关联的 ACL 中配置强匹配条件的 ACE，如：deny 所有报文的 ACE、deny 所有 IP 报文的 ACE 等。

由于全局安全 ACL 主要用于病毒过滤，因此被关联于全局安全 ACL 的 ACL 中，只有 deny 类型的 ACE 会安装生效，permit 类型的 ACE 不会生效；

全局安全 ACL 没有缺省行为；

允许在物理端口和 AP 口上独立关闭全局安全 ACL 功能，不支持在 AP 成员口上关闭；

全局安全 ACL 只支持关联 IP 标准 ACL、IP 扩展 ACL；

全局安全 ACL 目前仅支持在接口的 IN 方向上生效。

1.4.2 缺省配置

缺省情况下，不存在全局安全 ACL 配置。

1.4.3 开启/关闭全局安全ACL

从特权模式开始，您可以通过以下步骤来配置一个全局安全 ACL

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# [**no**] **ip access-group id** { **in** | **out** }	开启/关闭全局安全 ACL

1.4.4 在指定端口上关闭全局安全ACL

从特权模式开始，您可以通过以下步骤关闭指定端口的全局安全 ACL 功能：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **interface** *interface-name*	进入接口模式
Ruijie(config-if)#**no global ip access-group**	关闭指定端口的全局安全 ACL 功能

1.5 其他相关配置

1.5.1 配置TCP Flag过滤控制

TCP Flag 过滤特性提供了一种灵活机制，当前 TCP Flag 过滤控制支持 Match-All 选项，接收到的报文匹配到有 TCP Flag 与 ACL 表项中定义的 TCP Flag 每一位均吻合，就由 ACL 规则来检验，使用者可以定义 TCP Flag 的任意组合，用来过滤某些具有特定 TCP Flag 的报文。当指定 established 选项时，如果接收到的报文中携带的 TCP Flag 带有 rst 或者 ack 标志，就表示符合 established 特征。

例如：

```
permit tcp any any match-all rst
```

允许 TCP Flag RST 置位，其他位为 0 的报文通过。

```
permit tcp any any  established
```

允许 TCP Flag 中的 RST 或 ACK 置位的报文通过，而不管其他位是否被置上。

这种过滤特性可以在命名 ACL,数值 ACL 配置协议号为 TCP 的情况下可选配置。MAC 扩展和 IP 标准没有此项功能。

请按照如下步骤配置 TCP Flag

命令	作用
Ruijie(config)# **ip access-list extended** { *id* | *name* }	进入配置访问列表模式
Ruijie(config-ext-nacl)# [*sn*] {**permit** | **deny**} **tcp** *source source-wildcard* [*operator port*] *destination destination-wildcard [operator port*] [**match-all** *flag-name* | **established**] [**precedence** *precedence*]	为 ACL 添加表项,命令的具体内容请参见命令参考
Ruijie(config-exp-nacl)# **exit**	退出访问控制列表模式，选择要应用访问列表的接口
或	
Ruijie(config)# **interface** *interface*	退出访问控制列表模式，选择要应用访问列表的接口
Ruijie(config-if)# **ip access-group** {*id* | *name*} {**in** | **out**}	将访问列表应用特定接口

下面的例子说明如何配置 TCP Flag

- enable 权限和密码

```
Ruijie> enable
Ruijie#
```

- 进入全局配置模式

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

- 进入 ACL 配置模式

```
Ruijie(config)# ip access-list extended test-tcp-flag
Ruijie(config-ext-nacl)#
```

- 添加 ACL 表项

```
Ruijie(config-ext-nacl)# permit tcp any any match-all rst
Ruijie(config-ext-nacl)# permit tcp host 1.1.1.1 any  established
```

- 添加 deny 表项

```
Ruijie(config-ext-nacl)# deny tcp any any match-all fin
```

- end

```
Ruijie(config-ext-nacl)# end
```

- 显示

```
Ruijie# show  access-list test-tcp-flag
ip access-lists extended test-tcp-flag
10 permit tcp any any match-all rst
20 permit tcp host 1.1.1.1 any established30 deny tcp any any match-all fin
```

1.5.2 按优先级配置ACL表项

为了体现 ACE 的优先级，对每个 ACL 列表提出标准，以规范该 ACL 列表下的 ACE 的编排方式，采用序号的起点-增量方式，具体描述如下：

- ACE 在链表中以序号自小至大方式排列；
- 以起点序号开始，如不指定序号均以前一 ACE 的序号为基础以增量递增。
- 指定序号时将该 ACE 以排序方式插入，增量保证了在两个相邻 ACE 之间能够插入新的 ACE。
- ACL 列表指定序号起点和序号增量。

提供 **ip access-list resequence** {*acl-id*| *acl-name*} *sn-start sn-inc* 命令，相关命令见命令参考。

每运行以上命令，便对 ACL list 下的 ace 重新排列，如名字为 tst_acl 的 ACL 下 ace 序号为：

初始时

```
ace1: 10
ace2: 20
ace3: 30
```

运行 **ip access-list resequence** *tst_acl 100 3*，ACE 的序号如下

```
Ruijie(config)# ip access-list resequence tst_acl 100 3
ace1: 100
ace2: 103
ace3: 106
```

不输入 sn-num 添加 ace4 时，序号如下

```
Ruijie(config-std-nacl)# permit 。。。
ace1: 100
ace2: 103
ace3: 106
ace4: 109
```

输入 seq-num = 105 添加 ace5 时，序号如下

```
Ruijie(config-std-nacl)# 105 permit 。。。
ace1: 100
ace2: 103
ace5: 105
ace3: 106
ace4: 109
```

序号的引用是为了实现优先级添加 ace 的方式。

删除 ACE

```
Ruijie(config-std-nacl)# no 106
ace1: 100
```

```
ace2: 103
ace5: 105
ace4: 109
```

如上序号也可以方便 ACE 的删除。

1.5.3 配置基于时间区的ACL

您可以使 ACL 基于时间运行，比如让 ACL 在一个星期的某些时间段内生效等。为了达到这个要求，您必须首先配置一个 Time-Range。

Time-Range 的实现依赖于系统时钟，如果您要使用这个功能，必须保证系统有一个可靠的时钟。

从特权模式开始，您可以通过以下步骤来设置一个 Time-Range：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **time-range** *time-range-name*	通过一个有意义的显示字符串作为名字来标识一个
Ruijie(config-time-range)# **absolute** [**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
Ruijie(config-time-range)# **periodic** *day-of-the-week time* **to** [*day-of-the-week*] *time*	设置周期时间(可选)
Ruijie# **show time-range**	验证您的配置
Ruijie# **copy running-config startup-config**	保存配置
Ruijie(config)# **ip access-list extended** *101*	进入 ACL 配置模式
Ruijie(config-ext-nacl)# **permit ip any any time-range** *time-range-name*	配置时间区的 ACE

Time Range 名字的长度为 1－32 个字符，不能包含空格；绝对的运行时间区间只能设置一个或不设置，基于 Time Range 的应用将仅在这个时间区间内有效；您可以设置一个或多个周期性运行的时间段。如果您已经为这个 Time Range 设置了一个运行时间区间，则将在时间区间内周期性的生效。

由于硬件表项资源有限，注意不要配置太多带时间区的 ACL 表项，否则当时间区生效时，可能会因为硬件资源不足而导致大量表项下发失败。对于带时间区的 ACL 表项，系统每隔 30 秒尝试将未下发的表项（包括之前未下发成功的表项）下发到硬件芯片。如果每次都有大量的表项因硬件资源限制而下发失败，尝试重新下发这些表项的过程中将会显著提高系统的 CPU 利用率，从而在这期间会使得控制台出现没响应的情况。

下面的例子以时间区 ACL 应用为例，说明如何在每周工作时间段内禁止 HTTP 的数据流：

```
Ruijie(config)# time-range no-http
Ruijie(config-time-range)# periodic weekdays 8:00 to 18:00
Ruijie(config)# end
Ruijie(config)# ip access-list extended limit-udp
Ruijie(config-ext-nacl)# deny tcp any any eq www time-range no-http
Ruijie(config-ext-nacl)# exit
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# ip access-group no-http in
```

```
Ruijie(config)# end
```

下面为 Time Range 的显示范例：

```
Ruijie# show time-range
time-range entry: no-http(inactive)
periodic Weekdays 8:00 to 18:00
time-range entry: no-udp
periodic Tuesday 15:30 to 16:30
```

1.5.4 配置注释

为了便于浏览和理解 ACL 配置，ACL 模块提供了针对 ACL 和 ACE 的注释功能。

一个 ACL 中最多配置 1 个 ACL 注释和 2048 条 ACE 注释。

每个注释长度为 100 字节，不允许一个 ACL 内出现 2 条相同内容的 ACE 注释。

从特权模式开始，您可以通过以下步骤给 ACL 配置注释：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **ip access-list standard** *id*	进入 ACL 配置模式(其他类型 ACL 类似)
Ruijie(config-std-nacl)# **list-remark** *comment*	给 ACL 配置注释

也可以通过以下步骤给 ACL 配置注释：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **access-list** *id* **list-remark** *comment*	直接给 ACL 配置注释(其他类型 ACL 类似)

从特权模式开始，您可以通过以下步骤给 ACE 配置注释：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **ip access-list standard** *id*	进入 ACL 配置模式(其他类型 ACL 类似)
Ruijie(config-std-nacl)# **remark** *comment*	给 ACL 配置一条 ACE 注释

也可以通过以下步骤给 ACE 配置注释：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **access-list** *id* **remark** *comment*	直接给 ACL 配置一条 ACE 注释(其他类型 ACL 类似)

下面的例子说明了如何配置 ACL 注释和 ACE 注释：

```
Ruijie(config)#ip access-list standard 1
Ruijie(config-std-nacl)#remark ace_remark_permit_62_start
Ruijie(config-std-nacl)#permit 192.168.197.62 0.0.0.0
Ruijie(config-std-nacl)#remark ace_remark_permit_62_end
```

```
Ruijie(config-std-nacl)#list-remark acl_remark_foo
Ruijie(config-std-nacl)#end
Ruijie#write
Ruijie#show access-lists 1
ip access-list standard 1
 remark ace_remark_permit_62_start
 10 permit host 192.168.197.62
 remark ace_remark_permit_62_end
list-remark acl_remark_foo
Ruijie#
```

1.5.5 配置ACL日志更新间隔

为了合理控制配置了 ACL logging 的 ACE 输出的 log 数量和频率，可以通过如下命令来设置 ACL 日志的更新间隔：

命令	作用
Ruijie(config)# **ip access-list log-update inerval** *time*	配置 ACL 日志更新间隔，其中 time 取范围为 [0, 1440]，默认值为 0，表示该无需输出 ACL logging，配置的间隔时间必须是 5 分钟的倍数。

如果要恢复 ACL 日志更新间隔的默认值，可用 **no ip access-list log-update interval** 全局配置命令设置。

配置举例：

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# ip access-list log-update interval 10
*Sep  9 16:23:06: %ACL-6-MATCH: ACL 120 ACE 10 permit icmp any any, match 78 packets.
*Sep  9 16:23:06: %ACL-6-MATCH: ACL 120 ACE 20 permit tcp any any, match 100 packets.
*Sep  9 16:33:06: %ACL-6-MATCH: ACL 120 ACE 10 permit icmp any any, match 345 packets.
*Sep  9 16:33:06: %ACL-6-MATCH: ACL 120 ACE 20 permit tcp any any, match 678 packets.
Ruijie(config)# no ip access-list log-update interval
```

1.5.6 配置、查看和清除ACL报文匹配计数

通过如下命令可以开启 ACL 报文匹配技术功能：

命令	作用
Ruijie(config)# { **mac** | **ip** } **access-list counter** { *id* | *name* }	开启指定 MAC ACL 或者 IPv4 ACL 下的所有 ACE 报文匹配计数功能

如果要取消 ACL 下的所有 ACE 的报文匹配技术功能，请使用 **no** { **mac | ip** } **access-list counter** { *id* | *name* }来设置。

使用 ACL 的查看命令可以看到 ACL 规则匹配到的报文计数，具体请参见相应类型访问列表的配置和显示章节。

对于如何清除 ACL 报文匹配计数，请按照如下步骤进行操作：

命令	作用

Ruijie# **clear counters access-list** [*id* | *name*]	清除 ACL 报文匹配计数

配置举例：

```
Ruijie(config)# ip access-list counter 101
Ruijie(config)# end
Ruijie #show ip access-lists
Extended IP access list 101
    10 deny ip any host 11.1.1.2 log (3 matches)
    20 permit ip any any log (10690 matches)
    30 deny ip host 192.168.21.59 any log (101 matches)
    40 permit tcp host 192.168.21.59 any eq ftp log
    50 permit ip host 192.168.21.59 any log
    (1080 packets filtered)
Ruijie# clear counters access-list
Ruijie #show ip access-lists
Extended IP access list 101
    10 deny ip any host 11.1.1.2 log
    20 permit ip any any log
    30 deny ip host 192.168.21.59 any log
    40 permit tcp host 192.168.21.59 any eq ftp log
    50 permit ip host 192.168.21.59 any log
```

使用 clear 相关的命令来清除 ACL 的报文匹配计数时，可能会造成该 ACL 丢失最多 1 秒钟到 5 秒的报文匹配计数，该 ACL 中带 logging 的 ACE 统计的匹配报文数也会受此影响。

如果有报文被上层软件 ACL 过滤掉，在显示 ACL 报文信息时，会将该 ACL 在软件上过滤掉的报文计数显示出来，这部分只会统计被 deny 的报文，不统计被 permit 的报文。注意，这里只会统计被软件 ACL 过滤掉的报文，不会统计被硬件 ACl 过滤掉的报文。

1.5.7 配置分片报文匹配模式

对于 IP 报文，在网络传输时中可能会被分片。报文发生分片时，只有首片报文带有四层信息，比如 TCP 或 UDP 端口号、ICMP 类型和 ICMP 编码等，其他的分片报文都不带有这些四层信息。默认情况下，如果 ACL 规则带有 fragment 标识，则只会去匹配非首片报文；如果 ACL 规则不带有 fragment 标识，则匹配所有报文，包括首片报文和后续的所有分片报文。除了这种默认的分片报文匹配模式外，锐捷交换机产品还提供了一种新的分片报文匹配方法，用户可以根据需要在指定的 ACL 上进行切换。新的分片报文匹配模式与默认的分片报文匹配模式的区别就在于：当 ACL 规则中不带有 fragment 标识时，如果报文被分片，首片报文会去匹配 ACL 规则中用户定义的所有匹配域(包括三层和四层信息)，而非首片报文则只会去匹配 ACL 规则中的非四层信息。

从特权模式开始，您可以通过以下步骤切换分片报文的匹配模式：

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

Ruijie(config)# **ip access-list new-fragment-mode** { *id* | *name* }	将 IPv4 ACL 的分片报文匹配模式从默认过滤模式切换到新匹配模式

使用 **no ip access-list new-fragment-mode** { *id* | *name* }命令来将指定 IPv4 ACL 的分片报文匹配模式切换回默认的过滤模式。

分片报文新匹配模式下，如果 ACL 规则不带 fragment 标识并且需要匹配报文的四层信息时，当匹配动作为 permit 时，ACL 规则会检查首片报文三层和四层信息，对于非首片报文只会检查报文的三层信息；当匹配动作为 deny 时，ACL 规则只会检查首片报文，不会去检查分片报文。

分片报文新匹配模式下，如果 ACL 规则带有 fragment 标识，不论 ACL 规则的匹配动作是 permit 还是 deny，都只检查非首片报文，而不会去检查首片报文。

分片报文新匹配模式下，如果 ACL 规则不带 fragment 标识，且匹配动作是 permit，这样的 ACL 规则需要使用更多的硬件表项，极端情况下会使得硬件表项容量减半；如果这样的 ACE 配置了 TCP flag 过滤控制的 established，则还会占用更多的硬件表项。

执行分片报文匹配模式切换时，会导致 ACL 的短时失效。

仅在 IP 扩展 ACL 上支持分片报文匹配模式的切换。不支持在 IP 标准 ACL 上进行分片报文匹配模式的切换。

配置举例：

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# access-list new-fragment-mode
```

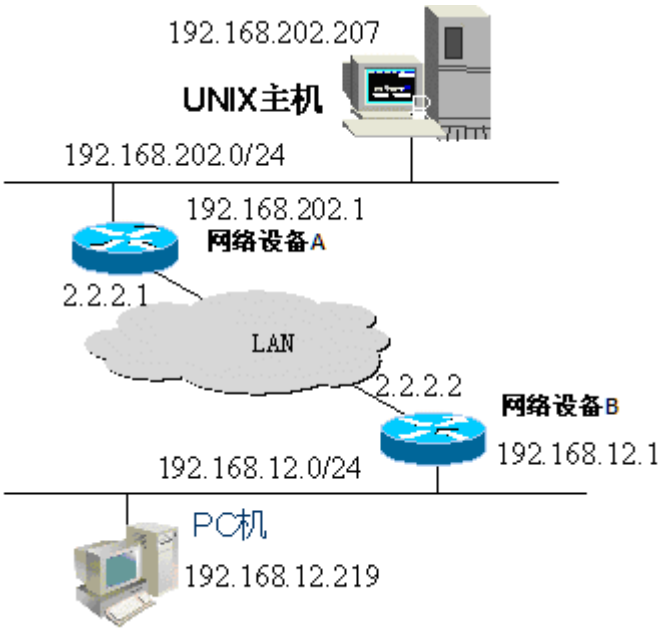
1.6 典型配置举例

1.6.1 IP访问列表示例

配置要求

有两台网络设备 A 和 B，如下图：

图 1-3 基本访问列表示例



要求通过在设备 B 上配置访问列表，实现以下安全功能：

192.168.12.0/24 网段的主机只能在正常上班时间访问远程 UNIX 主机 TELNET 服务，拒绝 PING 服务。

在设备 B 控制台上不能访问 192.168.202.0/24 网段主机的所有服务。

以上案例是银行系统应用的简化，即只允许分行或储蓄点局域网上的主机访问中心主机，不允许在设备上访问中心主机。

设备配置

设备 B 的配置：

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# ip address 192.168.12.1 255.255.255.0
Ruijie(config-if)# exit
Ruijie(config)# interface GigabitEthernet 0/2
Ruijie(config-if)# ip address 2.2.2.2 255.255.255.0
Ruijie(config-if)# ip access-group 101 in
Ruijie(config-if)# ip access-group 101 out
```

按照要求，配置一个编号为 101 的扩展访问列表

```
Ruijie(config)# access-list 101 permit tcp 192.168.12.0 0.0.0.255 any eq telnet time-range check
Ruijie(config)# access-list 101 deny icmp 192.168.12.0 0.0.0.255 any
Ruijie(config)# access-list 101 deny ip 2.2.2.0 0.0.0.255 any
Ruijie(config)# access-list 101 deny ip any any
```

配置 Time-Range 时间区

```
Ruijie(config)# time-range check
Ruijie(config-time-range)# periodic weekdays 8:30 to 17:30
```

访问列表 101 最后一条规则语句 access-list 101 deny ip any any 可以不要，因为访问列表最后隐含一条拒绝所有的规则语句。

设备 A 的配置：

```
A(config)# hostname Ruijie
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# ip address 192.168.202.1 255.255.255.0
Ruijie(config)# interface GigabitEthernet 0/2
Ruijie(config-if)# ip address 2.2.2.1 255.255.255.0
```

1.6.2 MAC扩展访问列表示例

要求通过配置 MAC 访问列表，实现以下安全功能：

- 使用 IPX 协议的主机 0013.2049.8272 不能访问设备 giga 0/1 端口
- 其他可以访问

```
Ruijie> enable
Ruijie# configure terminal
Ruijie(config)# mac access-list extended mac-list
Ruijie(config-mac-nacl)# deny host 0013.2049.8272 any ipx
Ruijie(config-mac-nacl)# permit any any
Ruijie(config-mac-nacl)# exit
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# mac access-group mac-list in
Ruijie(config-if)# end
Ruijie# show access-lists
mac access-list extended mac-list
deny host 0013.2049.8272 any ipx
permit any any
```

访问列表语句 permit any any 不能不要，因为访问列表最后隐含一条拒绝所有的规则语句。

1.6.3 配置TCP单向连接

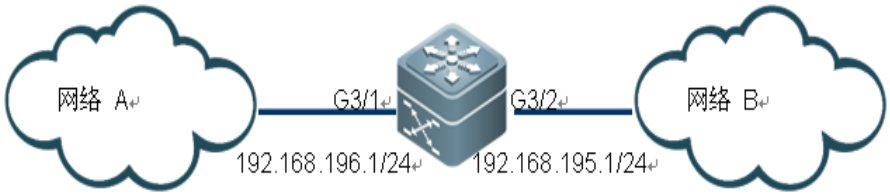
通过配置 TCP Flag 过滤实现单向 ACL 的功能。

配置要求

为了在一定程度上保证网络 A 的安全，要求只允许网络 A 的主机向网络 B 主机发起的 TCP 通信请求，但是不允许网络 B 的主机发起到网络 A 的 TCP 通信请求。

拓扑图

图 1-4 配置 TCP 单向连接



如上图所示，通过一台中间设备连接两个网络，网络 A 与设备的 G3/1 口相连，网络 B 与设备的 G3/2 口相连。

分析

环境要求阻止网络 B 的主机发起到网络 A 的 TCP 通信请求，只要过滤从网络 B 发起经过中间设备 G3/2 口转发的 TCP 连接请求报文即可。分析 TCP 连接过程可知，TCP 初始请求报文的 TCP 首部标志字段的 SYN 置位且 ACK 标志位为 0。因此，我们可以通过配置扩展访问控制列表的 Match-all 选项，在 G3/2 端口的入口方向，对 TCP 首部 SYN 标志位置 1 且 ACK 标志位为 0 的报文进行过滤，即可实现网络 A 单向访问网络 B 的应用。

配置步骤

1) 定义访问控制列表

进入配置模式

```
Ruijie# configure terminal
```

在配置模式下创建扩展访问列表 ACL101

```
Ruijie(config)# ip access-list extended 101
```

拒绝 TCP Flag 的 SYN=1，且其它（包含 ACK 标志位）标志位为 0 的报文通过

```
Ruijie(config-ext-nacl)# deny tcp any any match-all syn
```

允许其它 IP 报文通过

```
Ruijie(config-ext-nacl)# permit ip any any
```

2) 把访问控制列表应用在接口上

退出访问控制列表模式

```
Ruijie(config-ext-nacl)# exit
```

进入应用此访问列表的接口 G3/2

```
Ruijie(config)# interface gigabitEthernet 3/2
```

将 ACL 101 应用于 G3/2 入方向的包过滤

```
Ruijie(config-if)# ip access-group 101 in
```

3) 显示访问列表的配置

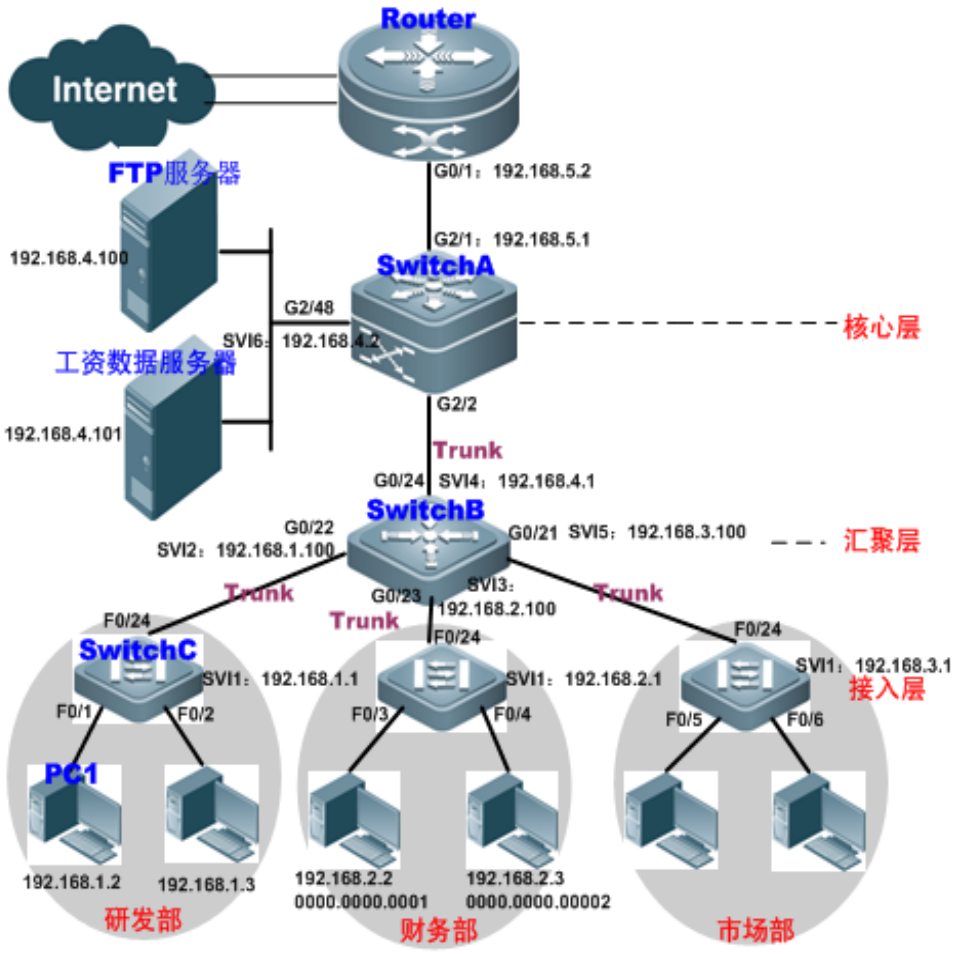
在特权模式下，使用 **show** 命令显示 ACL 相关配置

```
Ruijie# show access-lists 101
ip access-list extended 101
10 deny tcp any any match-all syn
20 permit ip any any
```

1.6.4 企业网ACL典型应用

组网图

图 1-5 企业网 ACL 应用场景拓扑图



上图是典型的企业网络拓扑：

接入层设备 C：连接各部门的 PC，通过千兆光纤(trunk 方式)连接汇聚层设备。

汇聚层设备 B：划分多个 VLAN，每个部门为一个 VLAN，通过万兆光纤(trunk 方式)上连核心层设备。

核心层设备 A：连接各种服务器，如 FTP，HTTP 服务器等，通过防火墙与 Internet 相连。

应用需求

上述企业网 ACL 应用场景主要有以下组网需求：

Internet 病毒无处不在，需要封堵各种病毒的常用端口，以保障内网安全。

只允许内部 PC 访问服务器，不允许外部 PC 访问服务器；

不允许非财务部门 PC 访问财务部 PC；不允许非研发部门 PC 访问研发部 PC

不允许研发部门人员在上班时间（即 9:00~18:00）使用 QQ、MSN 等聊天工具；

配置要点

- 通过在核心层设备（本例为设备 A）上联 Router 的端口（本例为 G2/1 口）上设置扩展 ACL 来过滤相关端口的数据包来达到防病毒的目的。
- 要求内部 PC 对服务器进行访问，不允许外部 PC 访问服务器，可以通过定义 IP 扩展 ACL 并应用到核心层设备（本例为设备 A）的下联汇聚层设备和服务器的接口（本例为 G2/2 口/SVI 2）上实现。
- 要求特定部门间不能互访，可通过定义 IP 扩展 ACL 实现（本例中分别在设备 B 的 G0/22、G0/23 上应用 IP 扩展 ACL）；
- 可通过配置时间 IP 扩展 ACL，限制研发部门在特定时间内使用 QQ/MSN 等聊天工具（本例中在设备 B 的 SVI 2 上应用时间 IP 扩展 ACL）。

配置步骤

- 配置核心层设备 A

第一步：定义阻断病毒访问控制列表 *Virus_Defence*

> 网络中的蠕虫病毒会在本地的 udp/69 端口上建立一个 tftp 服务器，用来向其它受侵害的系统上传送病毒的二进制程序。蠕虫选择目标 IP 地址的时候会首先选择受感染系统所在子网的 IP，然后再按照一定算法随机在互连网上选择目标攻击。一旦连接建立，蠕虫会向目标的 TCP 的 136、445、593、1025、5554、9995、9996，UDP 的 136、445、593、1433、1434，UDP/TCP 的 135、137、138、139 端口发送攻击数据。如果攻击成功，会监听目标系统的 TCP/4444 端口作为后门。然后蠕虫会连接到这个端口，发送 tftp 命令，回连到发起进攻的主机，将病毒文件传到目标系统上，然后运行它。中毒的服务器会向网络发送大量无效的数据包，浪费有效的网络带宽，甚至使网络设备死机，导致网络瘫痪。此时可以使用扩展访问列表来过滤这些端口的数据包来达到防病毒的目的。

```
A#configure terminal
A(config)#ip access-list extended Virus_Defence
```

！阻止来自内网外网可能被病毒利用的 TCP 端口报文

```
A(config-ext-nacl)#deny tcp any any eq 135
A(config-ext-nacl)#deny tcp any eq 135 any
A(config-ext-nacl)#deny tcp any any eq 136
A(config-ext-nacl)#deny tcp any eq 136 any
A(config-ext-nacl)#deny tcp any any eq 137
A(config-ext-nacl)#deny tcp any eq 137 any
```

……！中间的配置类似，此处省略说明

```
A(config-ext-nacl)#deny tcp any any eq 9996
A(config-ext-nacl)#deny tcp any eq 9996 any
```

！阻止来自内网外网可能被病毒利用的 UDP 端口报文

```
A(config-ext-nacl)#deny udp any any eq 69
A(config-ext-nacl)#deny udp any eq 69 any
A(config-ext-nacl)#deny udp any any eq 135
A(config-ext-nacl)#deny udp any eq 135 any
A(config-ext-nacl)#deny udp any any eq 137
A(config-ext-nacl)#deny udp any eq 137 any
```

……！中间的配置类似，此处省略说明

```
A(config-ext-nacl)#deny udp any any eq 1434
A(config-ext-nacl)#deny udp any eq 1434 any
```

！阻止 ICMP 报文

```
A(config-ext-nacl)#deny icmp any any
```

！允许其它所有 ip 数据包

```
A(config-ext-nacl)#permit ip any any
A(config-ext-nacl)#exit
```

第二步：将访问控制列表 *Virus_Defence* 应用在核心设备上联 Router 的接口上

```
A(config)#interface gigabitEthernet 2/1
A(config-if)#no switchport
A(config-if)#ip address 192.168.5.1 255.255.255.0
```

！将 ACL *Virus_Defence* 应用于 G2/1 入方向，阻断外网的病毒报文

```
A(config-if)#ip access-group Virus_Defence in
A(config-if)#exit
```

第三步，定义只允许内网 PC 访问服务器的访问控制列表 *access_server*

```
A(config)#ip access-list extended access_server
```

！只允许指定内网 IP 网段 PC 访问服务器(IP 地址为 192.168.4.100)

```
A(config-ext-nacl)#permit ip 192.168.2.0 0.0.0.255 host 192.168.4.100
A(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.255 host 192.168.4.100
A(config-ext-nacl)#permit ip 192.168.3.0 0.0.0.255 host 192.168.4.100
A(config-ext-nacl)#deny ip any any
```

第四步，将访问控制列表 *access_server* 应用在下联汇聚设备和服务器的接口上

```
A(config)#interface gigabitEthernet 2/2
A(config-if)#switch mode trunk
```

！应用于连接汇聚层设备接口的入方向

```
A(config-if)#ip access-group access_server in
A(config-if)#exit
```

！创建 vlan

```
A(config)#vlan 2
A(config-vlan)#exit
A(config)#interface gigabitEthernet 2/48
```

！连接服务器的接口 G2/48 属于 vlan2

```
A(config-if)#switch access vlan 2
A(config-if)#exit
```

！应用于连接服务器接口的入方向

```
A(config)#interface vlan 2
A(config-if-VLAN 2)# ip access-group access_server in
A(config-if-VLAN 2)# ip address 192.168.4.2 255.255.255.0
A(config-ext-nacl)#end
```

■ 配置汇聚设备 B

第一步，创建 vlan2-4

```
B#configure terminal
```

！创建 vlan2-4

```
B(config)#vlan range 2-4
B(config-vlan-range)#exit
```

第二步，定义访问控制列表

！定义 IP 扩展 ACL（vlan_access1 和 vlan_access2）

```
B(config)#ip access-list extended vlan_access1
```

！不允许财务部、市场部访问研发部

```
B(config-ext-nacl)#deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
B(config-ext-nacl)#deny ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
B(config-ext-nacl)#permit ip any any
B(config)#ip access-list extended vlan_access2
```

！不允许研发部、市场部访问财务部

```
B(config-ext-nacl)#deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
B(config-ext-nacl)#deny ip 192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255
B(config-ext-nacl)#permit ip any any
B(config-ext-nacl)#exit
```

第三步，将访问控制列表(vlan_access1 和 vlan_access2)应用在对应接口上

！配置 G0/22 口为 trunk 口，并应用 vlan_access1

```
B(config)#interface GigabitEthernet 0/22
B(config-if)#switchport mode trunk
```

```
B(config-if)#ip access-group vlan_access1 in
```

！配置 G0/23 口为 trunk 口，并应用 vlan_access2

```
B(config)# interface GigabitEthernet 0/23
B(config-if)# switchport mode trunk
B(config-if)# ip access-group vlan_access2 in
```

！配置 G0/24 为 trunk 口。

```
B(config)#interface GigabitEthernet 0/24
B(config-if)#switchport mode trunk
```

！配置 SVI2 的 IP 地址。

```
B(config)#interface vlan 2
B(config-if)#ip address 192.168.1.100 255.255.255.0
```

！配置 SVI3 的 IP 地址。

```
B(config)#interface vlan 3
B(config-if)#ip address 192.168.2.100 255.255.255.0
```

！配置 SVI4 的 IP 地址

```
B(config)#interface vlan 4
B(config-if)#ip address 192.168.4.1 255.255.255.0
```

第四步，定义时间段

！定义周一至周五的 9：00~18：00 的周期时间段

```
B#configure terminal
B(config)#time-range worktime
B(config-time-range)#periodic weekdays 9:00 to 18:00
```

第五步，定义研发部门数据流向规则

```
B#configure terminal
```

！在配置模式下创建扩展访问列表 ACL *yanfa*

```
B(config)#ip access-list extended yanfa
```

！禁止研发部的所有主机在工作日的 9：00 至 18：00 使用 QQ、MSN 等聊天工具。

```
B(config-ext-nacl)#deny tcp 192.168.1.0 0.0.0.255 eq 8000 any time-range worktime
B(config-ext-nacl)#deny tcp 192.168.1.0 0.0.0.255 eq 8001 any time-range worktime
B(config-ext-nacl)#deny tcp 192.168.1.0 0.0.0.255 eq 443 any time-range worktime
B(config-ext-nacl)#deny tcp 192.168.1.0 0.0.0.255 eq 1863 any time-range worktime
B(config-ext-nacl)#deny tcp 192.168.1.0 0.0.0.255 eq 4000 any time-range worktime
B(config-ext-nacl)#deny udp 192.168.1.0 0.0.0.255 eq 8000 any time-range worktime
B(config-ext-nacl)#deny udp 192.168.1.0 0.0.0.255 eq 1429 any time-range worktime
B(config-ext-nacl)#deny udp 192.168.1.0 0.0.0.255 eq 6000 any time-range worktime
```

```
B(config-ext-nacl)#deny udp 192.168.1.0 0.0.0.255 eq 6001 any time-range worktime
B(config-ext-nacl)#deny udp 192.168.1.0 0.0.0.255 eq 6002 any time-range worktime
B(config-ext-nacl)#deny udp 192.168.1.0 0.0.0.255 eq 6003 any time-range worktime
B(config-ext-nacl)#deny udp 192.168.1.0 0.0.0.255 eq 6004 any time-range worktime
```

！ 允许其它 IP 流量

```
B(config-ext-nacl)#permit ip any any
```

！ 将列表应用在 SVI2 的入方向上

```
B(config)#interface vlan 2
B(config-if)#ip access-group yanfa in
```

配置验证

第一步，确认 ACE 条目是否正确，关注点为配置项先后顺序是否正确和是否生效。

```
A#show access-lists
ip access-list extended Virus_Defence
 10 deny tcp any any eq 135
 20 deny tcp any eq 135 any
 30 deny tcp any eq 4444 any
 40 deny tcp any any eq 5554
 50 deny tcp any eq 5554 any
 60 deny tcp any any eq 9995
 70 deny tcp any eq 9995 any
 80 deny tcp any any eq 9996
 90 deny tcp any eq 9996 any
 100 deny udp any any eq tftp
 110 deny udp any eq tftp any
 120 deny udp any any eq 135
 130 deny udp any eq 135 any
 140 deny udp any any eq netbios-ns
 150 deny udp any eq netbios-ns any
 160 deny udp any any eq netbios-dgm
 170 deny udp any eq netbios-dgm any
 180 deny udp any any eq netbios-ss
 190 deny udp any eq netbios-ss any
 200 deny udp any any eq 445
 210 deny udp any eq 445 any
 220 deny udp any any eq 593
 230 deny udp any eq 593 any
 240 deny udp any any eq 1433
 250 deny udp any eq 1433 any
 260 deny udp any any eq 1434
 270 deny udp any eq 1434 any
```

```
 280 deny tcp any any eq 136
 290 deny tcp any eq 136 any
 300 deny tcp any any eq 137
 310 deny tcp any eq 137 any
 320 deny tcp any any eq 138
 330 deny tcp any eq 138 any
 340 deny tcp any any eq 139
 350 deny tcp any eq 139 any
 360 deny tcp any any eq 445
 370 deny tcp any eq 445 any
 380 deny tcp any any eq 593
 390 deny tcp any eq 593 any
 400 deny tcp any eq 1025 any
 410 deny tcp any any eq 4444
420 deny icmp any any
 430 permit tcp any any
 440 permit udp any any
 450 permit ip any any
ip access-list extended access_server
 10 permit ip 192.168.2.0 0.0.0.255 host 192.168.4.100
 20 permit ip 192.168.1.0 0.0.0.255 host 192.168.4.100
 30 permit ip 192.168.3.0 0.0.0.255 host 192.168.4.100
 40 deny ip any any
B#show access-lists
ip access-list extended vlan_access1
 10 deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
 20 deny ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
 30 permit ip any any
ip access-list extended vlan_access2
 10 deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
 20 deny ip 192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255
 30 permit ip any any
ip access-list extended yanfa
 10 deny tcp 192.168.1.0 0.0.0.255 eq 8000 any time-range worktime (active)
 20 deny tcp 192.168.1.0 0.0.0.255 eq 8001 any time-range worktime (active)
 30 deny tcp 192.168.1.0 0.0.0.255 eq 443 any time-range worktime (active)
 40 deny tcp 192.168.1.0 0.0.0.255 eq 1863 any time-range worktime (active)
 50 deny tcp 192.168.1.0 0.0.0.255 eq 4000 any time-range worktime (active)
 60 deny udp 192.168.1.0 0.0.0.255 eq 8000 any time-range worktime (active)
 70 deny udp 192.168.1.0 0.0.0.255 eq 1429 any time-range worktime (active)
 80 deny udp 192.168.1.0 0.0.0.255 eq 6000 any time-range worktime (active)
 90 deny udp 192.168.1.0 0.0.0.255 eq 6001 any time-range worktime (active)
 100 deny udp 192.168.1.0 0.0.0.255 eq 6002 any time-range worktime (active)
 110 deny udp 192.168.1.0 0.0.0.255 eq 6003 any time-range worktime (active)
 120 deny udp 192.168.1.0 0.0.0.255 eq 6004 any time-range worktime (active)
```

第二步，确认 ACL 配置是否完整，关注点为是否将正确的 ACL 应用到指定的接口上。

设备 A 配置：

```
A#show run
interface GigabitEthernet 2/1
 no switchport
 no ip proxy-arp
 ip access-group Virus_Defence in
 ip address 192.168.5.1 255.255.255.0
!
interface GigabitEthernet 2/2
 switchport mode trunk
 ip access-group access_server in
!
interface VLAN 2
 no ip proxy-arp
 ip access-group access_server in
 ip address 192.168.4.2 255.255.255.0
```

设备 B 配置：

```
B#show run
!
interface GigabitEthernet 0/22
 switchport mode trunk
 ip access-group vlan_access1 in
!
interface GigabitEthernet 0/23
 switchport mode trunk
 ip access-group vlan_access2 in
!
interface VLAN 2
 no ip proxy-arp
 ip access-group yanfa in
 ip address 192.168.1.100 255.255.255.0
```

2 IP QOS

2.1 QOS概述

随着 Internet 的飞速发展，人们对于在 Internet 上传输多媒体流的需求越来越大，一般说来，用户对不同的多媒体应用有着不同的服务质量要求，这就要求网络应能根据用户的要求分配和调度资源，因此，传统所采用的“尽力而为”转发机制，已经不能满足用户的要求。QOS 应运而生。

QOS（Quality of Service，服务质量）是用来评估服务方满足客户需求的能力。在因特网中，为了提高网络服务质量，引入 QOS 机制，用 QOS 评估网络投递分组的能力。我们通常所说的 QOS，是对分组投递过程中为延迟、抖动、丢包等核心需求提供支持的服务能力的评估。

2.1.1 QoS 基础框架

不支持 QoS 功能的设备不具有提供传输品质服务的能力，它同等对待所有的交通数据流，并不保证某一特殊的数据流会受到特殊的转发待遇。当网络带宽充裕的时候，所有的数据流都得到了较好的处理，而当网络拥塞发生的时候，所有的数据流都有可能被丢弃。这种转发策略被称做提供最佳效果服务，因为这时设备是尽最大能力转发数据，设备本身的交换带宽得到了充分的利用。

本设备支持 QoS 功能，能够提供传输品质服务。针对某种类别的数据流，您可以为它赋予某个级别的传输优先级，来标识它的相对重要性，并使用设备所提供的各种优先级转发策略、拥塞避免等机制为这些数据流提供特殊的传输服务。配置了 QoS 的网络环境，增加了网络的性能可预知性，并能够有效地分配网络带宽，更加合理地利用网络资源。

本设备的 QoS 实现以 IETF（Internet Engineering Task Force）的 DiffServ（Differentiated Servece Mode），差分服务模型） 体系为基础。DiffServ 体系规定网络中的每一个传输报文将被划分成不同的类别，分类信息被包含在了 IP 报文头中，DiffServ 体系使用了 IPv4 报文头中的 TOS（Type Of Service）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 字段的前 3 个比特，称作 IPprecedence value；或者携带在 IPv4 报文头中的 TOS 字段的前 6 个比特，称作 Differentiated Services Code Point (DSCP) value。

在遵循 DiffServ 体系的网络中，各设备对包含相同分类信息的报文采取相同的传输服务策略，对包含不同分类信息的报文采取不同的传输服务策略。报文的分类信息可以由网络上的主机、设备或者其它网络设备赋予。可以基于不同的应用策略或者基于报文内容的不同为报文赋予类别信息。识别报文的内容以便为报文赋予类别信息的做法往往需要消耗网络设备的大量处理资源，为了减少骨干网络的处理开销，一般这种赋予类别信息的方式都使用在网络边界。设备根据报文所携带的类别信息，为各种交通流提供不同的传输优先级，或者为某种交通流预留带宽，或者适当地丢弃一些优先级较低的报文、或者采取其他一些操作等等。这些独立设备的这种行为在 DiffServ 体系中被称作每跳行为（Per-hop Behavior）。

如果网络上的所有设备提供了一致的每跳行为，那么对于 DiffServ 体系来说，这个网络就可以构成 End-to-end QoSsolution。

2.1.2 QOS 处理流程

Classifying

Classifying 即分类，其过程是根据信任策略或者根据分析每个报文的内容来确定将这些报文归类到以 CoS 值来表示的各个数据流中，因此分类动作的核心任务是确定输入报文的 CoS 值。分类发生在端口接收输入报文阶段，当某个端口关联了一个表示 QoS 策略的 Policy-map 后，分类就在该端口上生效，它对所有从该端口输入的报文起作用。

对于一般非 IP 报文，设备将根据以下准则来归类报文：

- 如果报文本身不包含 QoS 信息，即报文的第二层报文头中不包含 User Priority bits，那么可以根据报文输入端口的缺省 CoS 值来获得报文的 QoS 信息。端口的缺省 CoS 值和报文的 User Priority bits 一样，取值范围为 0～7。
- 如果报文本身包含 QoS 信息，报文的第二层报文头中包含 User Priority bits，那么可以直接从报文中获得 CoS 值。

以上两种归类准则只有当端口的 QoS 信任模式打开的时候才起作用。打开端口的 QoS 的信任模式意味着不通过分析报文的内容，而直接从报文中或报文的输入端口上获得报文 QoS 信息。

如果端口关联的 Policy-map 中使用了基于 Mac access-list extended 的 ACLs 归类，那么在该端口上，将通过提取报文的源 MAC 地址、目的 MAC 地址以及 Ethertype 域来匹配关联的 ACLs，以确定报文的 DSCP 值。要注意的是，如果端口关联了某个 Policy-map，但又没有为其设置相应的 DSCP 值，则设备将按照缺省行为为符合这种归类的报文分配优先级：即根据报文第二层报文头中包含的优先级信息或端口的缺省优先级。

上面三种归类准则可能会同时作用于一个端口上。在这种情况下，上面三种归类准则按 3、2、1 的优先级起作用。即先根据 ACLs 归类，在归类失败的情况下，才有可能选择归类准则 2、1，在这个时候，如果端口的 QoS 信任模式打开，则根据准则 2 和 1 直接从报文中或者从端口上获得 QoS 信息；如果端口的 QoS 信任模式关闭，那么那些归类失败的报文将被赋予 DSCP 的缺省值 0。

对于 IP 报文，可以将根据以下准则来归类报文：

- 如果端口信任模式为 Trust ip-precedence，则直接从 IP 报文的 Ip precedence 字段（3 个比特）提取出来，填充到输出报文的 CoS 字段（3 个比特）。
- 如果端口信任模式为 Trust cos，则将报文的 CoS 字段（3 个比特）直接提取出来覆盖报文 Ip Precedence 字段（3 个比特）。这有两种情况，一是第二层报文头中不包含 User Priority bits，那么可以根据报文输入端口的缺省 CoS 值来获得报文的 CoS 值。另外一种是第二层报文头中包含 User Priority bits，则直接从报文头中取得 CoS 值。
- 如果端口关联的 Policy-map 中使用了基于 Ip access-list (Extended)的 ACLs 归类，那么该在该端口上，将通过提取报文的源 IP 地址、目的 IP 地址、Protocol 字段、以及第四层 TCP/UDP 端口字段来匹配相关联的 ACLs，以确定报文的 DSCP 值。要注意的是，如果端口关联了某个 Policy-map，但又没有为其设置相应的 DSCP 值，则设备将按照按照前面的规则 1、2 确定优先级。

和非 IP 报文归类准则一样，以上几种归类准则同样可以同时作用于一个端口上。在这种情况下，上面的归类准则按照 3、2、1 的优先级起作用。

有关上面提到的 CoS-to-DSCP map、IP-precedence-to-DSCP map 映射表的详细描述见随后描述。

Policing

Policing 即策略，发生在数据流分类完成后，用于约束被分类的数据流所占用的传输带宽。Policing 动作检查被归类的数据流中的每一个报文，如果该报文超出了作用于该数据流的 Police 所允许的限制带宽，那么该报文将会被做特殊处理，它或者要被丢弃，或者要被赋予另外的 DSCP 值。

在 QoS 处理流程中，Policing 动作是可选的。如果没有 Policing 动作，那么被分类的数据流中的报文的 DSCP 值将不会作任何修改，报文也不会在送往 Marking 动作之前被丢弃。

Marking

Marking 即标识，经过 Classifying 和 Policing 动作处理之后，为了确保被分类报文对应 DSCP 的值能够传递给网络上的下一跳设备，需要通过 Marking 动作将为报文写入 QoS 信息，可以使用 QoS ACLs 改变报文的 QoS 信息，也可以使用 Trust 方式直接保留报文中 QoS 信息，例如，选择 Trust DSCP 从而保留 IP 报文头的 DSCP 信息。

Queueing

Queueing 即队列，负责将数据流中报文送往端口的某个输出队列中，送往端口的不同输出队列的报文将获得不同等级和性质的传输服务策略。

每一个端口上都拥有 8 个输出队列，通过设备上配置的 DSCP-to-CoS Map 和 Cos-to-Queue Map 两张映射表来将报文的 DSCP 值转化成输出队列号，以便确定报文应该被送往的输出队列。

Scheduling

Scheduling 即调度，为 QoS 流程的最后一个环节。当报文被送到端口的不同输出队列上之后，设备将采用 WRR 或者其它算法发送 8 个队列中的报文。

可以通过设置 WRR 算法的权重值来配置各个输出队列在输出报文的时候所占用的每循环发送报文个数,从而影响传输带宽。或通过设置 DRR 算法的权重值来配置各个输出队列在输出报文的时候所占用的每循环发送报文字节数,从而影响传输带宽。

2.1.3 QOS 逻辑端口组

可以指定一系列端口为一个 QOS 逻辑端口组（这里端口可以是 AP，也可以是物理口，下文简称为逻辑端口组），并针对这个逻辑端口组关联 Policy-map 进行 QOS 处理，以限速为例，对符合限速条件的报文，在同一个逻辑端口组内所有的端口共享 Policy-map 所限定的带宽值。

加入逻辑端口组的成员必须是物理口或者是 Aggregate Port。

交换机逻辑端口组的支持数量为 128 个。

2.2 配置QOS

2.2.1 缺省 QOS 设置

用户在进行 QoS 配置之前，需要清楚和 QoS 有关的几点信息，如下：

- 一个接口最多关联 1 个 Policy-map
- 一个 Policy-map 可以拥有多个 Class-map

- 一个 Class-map 最多关联 1 个 ACL，该 ACL 的所有 ACE 必须具有相同过滤域模板
- 一个接口上关联的 ACE 的个数服从“配置安全 ACL”章节的限制

缺省情况下，QoS 功能是关闭的，即设备对所有的报文同等处理。但当您将一个 Policy Map 关联到某一个接口上，并设置了接口的信任模式时，该接口的 QoS 功能即被打开。要关闭该接口的 QoS 功能，您可以通过解除该接口的 Policy Map 设置，并将接口的信任模式设为 Off 即可。以下为 QOS 的缺省配置：

缺省 CoS 值	0
队列个数	8
队列轮转算法	WRR
QueueWeight	1:1:1:1:1:1:1:1
WRR Weight Range	1:254
DRR Weight Range	1:254
信任模式	No Trust

Cos 值到队列的默认映射表

CoS 值	0	1	2	3	4	5	6	7
队列	1	2	3	4	5	6	7	8

CoS to DSCP 默认映射表

CoS 值	0	1	2	3	4	5	6	7
DSCP 值	0	8	16	24	32	40	48	56

IP-Precedence to DSCP 默认映射表

IP-Precedence	0	1	2	3	4	5	6	7
DSCP	0	8	16	24	32	40	48	56

DSCP to CoS 的默认映射表

DSCP	0	8	16	24	32	40	48	56
CoS	0	1	2	3	4	5	6	7

2.2.2 配置接口的 Qos 信任模式

缺省情况下，接口的 Qos 信任模式是不信任

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **interface** *interface*	进入接口配置模式
Ruijie(config-if)# **mls qos trust {cos | ip-precedence | dscp}**	配置接口的 Qos 信任模式 cos，dscp 或 ip-precedence
Ruijie(config-if)# **no mls qos trust**	恢复接口默认 Qos 信任模式

以下命令将端口 interface GigabitEthernet 0/4 信任模式设置为 DSCP：

```
Ruijie(config)# interface gigabitEthernet 0/4
```

```
Ruijie(config-if)# mls qos trust dscp
Ruijie(config-if)# end
Ruijie# show mls qos interface g0/4
Interface: GigabitEthernet 0/4
Attached input  policy-map:
Default trust: trust dscp
Default COS: 0
Ruijie#
```

不支持在 SVI 口上配置 QoS 信任模式。

2.2.3 配置接口的缺省 CoS 值

您可以通过下面的设置步骤来配置每一个接口的缺省 CoS 值

缺省情况下，接口的缺省 CoS 值为 0

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **interface** *interface*	进入接口配置模式
Ruijie(config-if)# **mls qos cos default-cos**	配置接口的缺省 CoS 值, default-cos 为要设置的缺省 CoS 值, 取值范围为 0～7
Ruijie(config-if)# **no mls qos cos**	默认的缺省 CoS 值

下面的例子将接口 Interface g0/4 缺省 CoS 值设置为 6

```
Ruijie# configure terminal
Ruijie(config)# interface g 0/4
Ruijie(config-if)# mls qos cos 6
Ruijie(config-if)# end
Ruijie# show mls qos interface g 0/4
Interface: GigabitEthernet 0/4
Attached input  policy-map:
Default trust: trust dscp
Default COS: 6
Ruijie#
```

2.2.4 配置逻辑端口组

在接口配置模式下，请按如下步骤将端口加入逻辑端口组：

命令	作用
Ruijie(config-if)# [**no**] **virtual-group** *virtual-group-number*	将该接口加入一个逻辑端口组或退出一个逻辑端口组。*virtual-group-number* 表示逻辑端口组成员端口组的编号，即逻辑端口组号。

在接口配置模式下使用 **no virtual-group** *virtual-group-number* 命令将一个物理端口退出逻辑端口组。

下面的例子是将以太网接口 0/1 配置成逻辑端口组 5 的成员：

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

2.2.5 配置 Class Maps

您可以通过下面的设置步骤来创建并配置 Class Maps

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **ip access-list extended** {*id* | *name*} Ruijie(config)# **ip access-list standard** {*id* | *name*} Ruijie(config)# **mac access-list extended** {*id* | *name*} Ruijie(config)# **access-list** *id* […]	创建 ACL 请参见 ACL 章节
Ruijie(config)# [**no**] **class-map** *class-map-name*	创建并进入 class map 配置模式,class-map-name 是要创建的 class map 的名字 no 选项 删除一个已经存在的 class map
Ruijie(config-cmap)# [**no**] **match access-group** {*acl-num* | *acl-name* }	设置匹配 ACL, acl-name 为已经创建的 ACL 名字， acl-num 为已经创建的 ACL id，no 选项删除该匹配
Ruijie(config-cmap)# [**no**] **match ip dscp** *dscp-value1* [*dscp-value2* [*dscp-valueN*]]	设置要匹配的报文的 ip dscp 值，dscp-valueN 为要匹配的 DSCP 值，一次最多可以匹配 8 个不同的值。
Ruijie(config-cmap)# [**no**] **match ip precedence** *ip-pre-value1* [*ip-pre-value2* [*ip-pre-valueN*]]	设置要匹配的报文的 ip precedence 值，ip-pre-valueN 为要匹配的 EXP 值，一次最多可以匹配 8 个不同的值。

例如，以下设置步骤创建了一个名为 Class1 的 Class-map，它关联一个 ACL:acl_1。这个 Class-map 将分类所有端口号为 80 的 TCP 报文

```
Ruijie(config)# ip access-list extended acl_1
Ruijie(config-ext-nacl)# permit tcp any any eq 80
Ruijie(config-ext-nacl)# exit
Ruijie(config)# class-map class1
Ruijie(config-cmap)# match access-group acl_1
Ruijie(config-cmap)# end
```

2.2.6 配置 Policy Maps

您可以通过下面的设置步骤来创建并配置 Policy Maps

命令	作用
Ruijie# **configure terminal**	进入配置模式

Ruijie(config)# [**no**] **policy-map** *policy-map-name*	创建并进入 policymap 配置模式，policy-map-name 是要创建的 policymap 的名字 no 选项 删除一个已经存在的 policy map
Ruijie(config-pmap)# [**no**] **class** *class-map-name*	创建并进入数据分类配置模式，class-map-name 是已经创建的 class map 名字 no 选项 删除该数据分类
Ruijie(config-pmap-c)# [**no**] **set** { **ip dscp** *new-dscp* | **cos** *new-cos* [**none-tos**]}	为该数据流中的 IP 报文设置新的 ip dscp 值或者设置新的 cos 值；对于非 IP 报文，设置新的 ip dscp 不起作用； new-dscp 是要设置的新 DSCP 值，取值范围依产品不同而不同； new-cos 是要设置的新 CoS 值，取值范围为 0-7； none-tos 是代表设置新的 CoS 值，同时不修改报文的 DSCP 值。
Ruijie(config-pmap-c)# **police** *rate-bps burst-byte* [**exceed-action** {**drop** | **dscp** *dscp-value* | **cos** *cos-value* [**none-tos**]}]	限制该数据流的带宽和为带宽超限部分指定处理动作，rate-bps 是每秒钟带宽限制量(kbps)，burst-byte 猝发流量限制值(Kbyte)，drop 来丢弃带宽超限部分的报文，dscp dscp-value 改写带宽超限部分报文的 DSCP 值，dscp-value 取值范围依产品不同而不同，cos cos-value 改写带宽超限部分的报文的 CoS 值，cos-vlaue 取值范围为 0-7，none-tos 选项代表改写报文的 CoS 值时，不修改报文的 DSCP 值；
Ruijie(config-pmap-c)# **no police**	取消限制该数据流的带宽和为带宽超限部分指定处理动作

☑ NBS200F 系列设备不支持对带宽超限部分报文改写 DSCP 值。在 NBS200F 系列设备中，带宽超限部分报文只能被丢弃。

☑ NBS200F 系列设备同一个 policy map 应用于多个端口时，每个端口速率限制的带宽都是独立。

例如，以下的设置步骤创建了一个名为 Policy1 的 Policy-map，并将该 Policy-map 关联接口 Gigabitethernet 1/1

```
Ruijie(config)# policy-map policy1
Ruijie(config-pmap)# class class1
Ruijie(config-pmap-c)# set ip dscp 48
Ruijie(config-pmap-c)# exit
Ruijie(config-pmap)# exit
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# mls qos trust cos
Ruijie(config-if)# service-policy input policy1
```

2.2.7 配置接口应用 Policy Maps

您可以通过下面的设置步骤将 Policy Maps 应用到端口上

命令	作用

Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **interface** *interface*	进入接口配置模式
Ruijie(config-if)# [**no**] **service-policy** {**input** | **output**} *policy-map-name*	将创建的 Policy Map 应用到接口上；policy-map-name 是已经创建的 policy map 的名字，input 为输入,output 为输出

2.2.8 配置逻辑端口组应用 Policy Maps

您可以通过下面的设置步骤将 Policy Maps 应用到逻辑端口组上

命令	说明
Ruijie#**configure terminal**	进入配置模式
Ruijie(config)#**virtual-group** *virtual-group-number*	进入逻辑端口组配置模式
Ruijie(config)# [**no**] **service-policy** {**input | output**} **policy-map-name**	将创建的 Policy Map 应用到逻辑端口组上；policy-map-name 是已经创建的 policy map 的名字，input 为输入限速,output 为输出限速

目前 output 方向应用在逻辑端口组上未被支持。由于 class map 需要关联 acl，所以 acl 配置的所有限制均适用于 qos，具体请参考 acl 配置指南。

2.2.9 配置输出队列调度算法

您可以为端口的输出队列调度算法：WRR，SP，DRR，缺省情况下，输出队列算法为 WRR（带权重的队列轮转)

您可以通过以下步骤对端口优先级队列调度方式进行设置,详细算法请参照 QOS 概述。

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **mls qos scheduler** {**sp | wrr | drr** }	端口优先级队列调度方式，sp 为绝对优先级调度，wrr 为带帧数量权重轮转调度，drr 为带帧长度权重轮转调度
Ruijie(config)# **no mls qos scheduler**	恢复为缺省 wrr 调度

例如，以下的设置步骤将端口的输出轮转算法设置成 SP：

```
Ruijie# configure terminal
Ruijie(config)# mls qos scheduler sp
Ruijie(config)# end
Ruijie# show mls qos scheduler
Global Multi-Layer Switching scheduling
Strict Priority
Ruijie#
```

2.2.10 配置输出轮转权重

您可以通过以下步骤设置端口的输出轮转权重

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# {**wrr-queue | drr-queue**} **bandwidth weight1...weightn**	weight1...weightn 为指定的输出队列的权重值，个数及取值范围见缺省 QOS 设置
Ruijie(config)# **no** {**wrr-queue | drr-queue**} **bandwidth**	no 选项恢复权重的缺省值

☑ NBS200F 系列设备中，当（WRR/DRR）权重值设置为 0 时，表示此队列进行 SP 调度；同时队列调度优先级跟队列值一致，即队列 7-0 的调度优先级是从高到低的关系；为了保证调度准确，进行 WRR/DRR 调度的队列应该保持连续，而不应该中间插入 SP 调度，比如：wrr-queue bandwidth 1 2 3 0 4 5 6 7，3 队列配置了 SP 调度，这就会造成调度不准确。

下面的例子将 wrr 调度权重设置为 1:2:3:4:5:6:7:8

```
Ruijie# configure terminal
Ruijie(config)# wrr-queue bandwidth 1 2 3 4 5 6 7 8
Ruijie(config)# end
Ruijie# show mls qos queueing
Cos-queue map:
cos qid
--- ---
0   1
1   2
2   3
3   4
4   5
5   6
6   7
7   8
wrr bandwidth weights:
qid weights
--- -------
0   1
1   2
2   3
3   4
4   5
5   6
6   7
7   8
Ruijie(config)#
```

2.2.11 配置 Cos-Map

您可以通过设置 Cos-Map 来选择报文输出时进入哪个输出队列，Cos-Map 的缺省设置见缺省 QOS 配置

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **priority-queue Cos-Map** *qid cos0* [*cos1* [*cos2* [*cos3* [*cos4* [*cos5* [*cos6* [*cos7*]]]]]]]	qid 为队列 id,cos0..cos7 为指定和这个队列关联的 CoS 值。
Ruijie(config)# **no priority-queue cos-map**	Cos-Map 恢复成缺省值

下面是设置 CoS Map 的例子

```
Ruijie# configure terminal
Ruijie(config)# priority-queue Cos-Map 1 2 4 6 7 5
Ruijie(config)# end
Ruijie# show mls qos queueing
Cos-queue map:
cos qid
--- ---
0   1
1   2
2   1
3   4
4   1
5   1
6   1
7   1

wrr bandwidth weights:
qid weights
--- -------
0   1
1   2
2   3
3   4
4   5
5   6
6   7
7   8
```

2.2.12 配置 CoS-to-DSCP Map

CoS-to-DSCP Map 用于将报文的 CoS 值映射到内部 DSCP 值,您可以通过以下步骤对 CoS-to-DSCP Map 进行设置 ,CoS-to-DSCP Map 的缺省设置见缺省 QOS 配置

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **mls qos map cos-dscp** *dscp1...dscp8*	修改 CoS-to-DSCP Map 的设置,dscp1...dscp8 是对应于 CoS 值 0～7 的 DSCP 值,DSCP 取值范围依产品不同而不同
Ruijie(config)# **no mls qos map cos-dscp**	恢复缺省值

例如如下配置：

```
Ruijie# configure terminal
Ruijie(config)# mls qos map cos-dscp 56 48 46 40 34 32 26 24
Ruijie(config)# end
Ruijie# show mls qos maps cos-dscp
cos dscp
--- ----
0   56
1   48
2   46
3   40
4   34
5   32
6   26
7   24
```

2.2.13 配置 DSCP-to-CoS Map

DSCP-to-CoS 用于将报文的内部 DSCP 值映射到 CoS 值，以便为报文选择输出队列

DSCP-to-CoS Map 的缺省设置见缺省 QOS 配置，您可以通过以下步骤对 DSCP-to-CoS Map 进行设置:

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **mls qos map dscp-cos** *dscp-list* to *cos*	设置 DSCP to COS Map， *dscp-list* ：要设置的 DSCP 值的列表，DSCP 值之间用空格分隔，取值范围依产品不同而不同,*cos* ：对应 DSCP 值的 CoS 值，取值范围为：0～7；
Ruijie(config)# **no mls qos map dscp-cos**	设置为默认值

例如，以下的设置步骤将 DSCP 值 0、32、56 设置对应成 6：

```
Ruijie# configure terminal
Ruijie(config)# mls qos map dscp-cos 0 32 56 to 6
Ruijie(config)# show mls qos maps dscp-cos
dscp cos     dscp cos     dscp cos     dscp cos
---- ---     ---- ---     ---- ---     ---- ---
 0   6        1   0        2   0        3   0
 4   0        5   0        6   0        7   0
```

8	1	9	1	10	1	11	1
12	1	13	1	14	1	15	1
16	2	17	2	18	2	19	2
20	2	21	2	22	2	23	2
24	3	25	3	26	3	27	3
28	3	29	3	30	3	31	3
32	6	33	4	34	4	35	4
36	4	37	4	38	4	39	4
40	5	41	5	42	5	43	5
44	5	45	5	46	5	47	5
48	6	49	6	50	6	51	6
52	6	53	6	54	6	55	6
56	6	57	7	58	7	59	7
60	7	61	7	62	7	63	7

2.2.14 配置端口速率限制

您可以通过以下步骤对端口速率限制进行设置

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **interface** *interface*	进入接口配置模式
Ruijie(config-if)# **rate-limit** { **input | output** } *bps burst-size*	端口速率限制。input 为输入限速，output 为输出限速。 *bps* 是每秒钟的带宽限制量(kbps) *burst-size* 是猝发流量限制值(Kbyte)
Ruijie(config-if)# **no rate-limit**	取消端口限速

☑ NBS200F 系列产品的输出端口速率的限制指的是带宽的有效负荷，而不包含前导码和帧间隙所占去的负荷。（每个报文所附带的前导码和帧间隙所占的带宽为 20 字节，因此报文长度越大越准确）。

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/4
Ruijie(config-if)# rate-limit input 100 100
Ruijie(config-if)# end
Ruijie#
```

2.2.15 配置 IPpre to DSCP Map

IPpre-to-Dscp 用于将报文的 IPpre 值映射到内部 DSCP 值, IPpre-to-DSCP Map 的缺省设置见缺省 QOS 配置,您可以通过以下步骤对 IPpre-to-Dscp Map 进行设置:

命令	作用
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **mls qos map ip-prec-dscp** *dscp1...dscp8*	修改 IP-Precedence-to-Dscp Map 的设置,dscp1...dscp8 是对应于 IP-Precedence 值 0～7 的 DSCP 值

Ruijie(config)# **no mls qos map ip-prec-dscp**	恢复缺省配置。

例如如下配置：

```
Ruijie# configure terminal
Ruijie(config)# mls qos map ip-precedence-dscp 56 48 46 40 34 32 26 24
Ruijie(config)# end
Ruijie# show mls qos maps ip-prec-dscp
ip-precedence dscp
------------- ----
0      56
1      48
2      46
3      40
4      34
5      32
6      26
7      24
```

2.2.16 清除队列统计值

接口的输出队列的统计值可以通过特权模式命令 **show interfaces** 查看。您可通过特权模式下的 **clear counters** 命令清除接口的输出队列统计值。在支持显示接口输出队列统计值的设备上，清除接口的统计值的同时也会将接口上的输出队列统计值清零。清除接口统计值的命令请参考接口配置相关章节。

2.3 QOS显示

2.3.1 显示 class-map

您可以通过以下步骤显示 class-map 内容

命令	作用
show class-map [*class-name*]	显示 class map 实体的内容

例如：

```
Ruijie# show class-map
Class Map cc
Match access-group 1
Ruijie#
```

2.3.2 显示 policy-map

您可以通过以下步骤显示 Policy-map 内容

命令	作用
show policy-map [*policy-name* [**class** *class-name*]]	显示 QoS policy map，*policy-name* 为选定的 policy map 名，指定 class *class-name* 时显示相应 policy map 绑定的 class map。

例如：

```
Ruijie# show policy-map
Policy Map pp
Class cc
Ruijie#
```

2.3.3 显示 mls qos interface

您可以通过以下步骤显示所有端口 qos 信息

命令	作用
show mls qos interface [*interface*	*policers*]	显示接口的 QoS 信息，Policers 选项显示接口应用的 Policy map

例如：

```
Ruijie# show mls qos interface gigabitEthernet 0/4
Interface: GigabitEthernet 0/4
Attached input  policy-map: pp
Default trust: trust dscp
Default COS: 6
Ruijie# show mls qos interface policers
Interface: GigabitEthernet 0/4
Attached input  policy-map: pp
Ruijie#
```

2.3.4 显示 mls qos queueing

您可以通过以下步骤显示 qos 队列信息

命令	作用
show mls qos queueing	显示 QoS 队列信息，CoS-to-queue map，wrr weight 及 drr weight。

举例如下：

```
Ruijie# show mls qos queueing
Cos-queue map:
cos qid
--- ---
0   1
1   2
```

```
2   1
3   4
4   1
5   1
6   1
7   1
wrr bandwidth weights:
qid weights
---  -------
0   1
1   2
2   3
3   4
4   5
5   6
6   7
7   8
```

2.3.5 显示 mls qos scheduler

您可以通过以下步骤显示 QOS 调度方式

命令	作用
show mls qos scheduler	显示端口优先级队列调度方式

举例如下：

```
Ruijie# show mls qos scheduler
Global Multi-Layer Switching scheduling
Strict Priority
Ruijie#
```

2.3.6 显示 mls qos maps

您可以通过以下步骤显示 mls qos maps 对应表

命令	作用
show mls qos maps [**cos-dscp|dscp-cos| ip-prec-dscp**]	显示 dscp-cos maps；dscp-cos maps；ip-prec-dscp maps

举例如下：

```
Ruijie# show mls qos maps cos-dscp
cos dscp
---  ----
0   0
1   8
```

```
2    16
3    24
4    32
5    40
6    48
7    56
Ruijie# show mls qos maps dscp-cos
dscp cos     dscp cos     dscp cos     dscp cos
---- ---     ---- ---     ---- ---     ---- ---
0    6       1    0       2    0       3    0
4    0       5    0       6    0       7    0
8    1       9    1      10    1      11    1
12   1      13    1      14    1      15    1
16   2      17    2      18    2      19    2
20   2      21    2      22    2      23    2
24   3      25    3      26    3      27    3
28   3      29    3      30    3      31    3
32   6      33    4      34    4      35    4
36   4      37    4      38    4      39    4
40   5      41    5      42    5      43    5
44   5      45    5      46    5      47    5
48   6      49    6      50    6      51    6
52   6      53    6      54    6      55    6
56   6      57    7      58    7      59    7
60   7      61    7      62    7      63    7
Ruijie# show mls qos maps ip-prec-dscp
ip-precedence dscp
------------- ----
0       56
1       48
2       46
3       40
4       34
5       32
6       26
7       24
```

2.3.7 显示 mls qos rate-limit

您可以通过以下步骤显示端口速率限制信息

命令	作用
show mls qos rate-limit [**interface** *interface*]	显示[端口] 速率限制

举例：

```
Ruijie# show mls qos rate-limit
Interface: GigabitEthernet 0/4
rate limit input bps = 100 burst = 100
```

2.3.8 显示 show policy-map interface

您可以通过以下步骤显示端口 policymap 的配置

命令	作用
show policy-map interface *interface*	显示[端口] policymap 配置

举例：

```
Ruijie# show policy-map interface f0/1
FastEthernet 0/1  input (tc policy): pp
Class cc
set ip dscp 22
```

2.3.9 显示 virtual-group

在特权模式下，请按如下步骤显示 virtual-group 设置。

命令	作用
show virtual-group [*virtual-group-number*	**summary**]	显示逻辑端口组信息。

举例：

```
Ruijie#show virtual-group 1
  virtual-group        member
  -------------        -------------------------
  1                      Gi0/2 Gi0/3 Gi0/4 Gi0/5
                         Gi0/6 Gi0/7 Gi0/8 Gi0/9 Gi0/10
Ruijie#show virtual-group summary
  virtual-group        member
  -------------        -------------------------
  1                      Gi0/1 Gi0/2 Gi0/3 Gi0/4
                         Gi0/5 Gi0/6 Gi0/7 Gi0/8 Gi0/9
  2                      Gi0/11 Gi0/12 Gi0/13 Gi0/14
                         Gi0/15 Gi0/16 Gi0/17 Gi0/18 Gi0/19
```

2.3.10 显示队列统计值

您可在特权模式下通过以下命令来查看一个接口上的各个输出队列的统计值信息。

命令	作用
show interfaces [*interface-id*]	显示指定接口的全部状态和配置信息。

举例，显示接口 GigabitEthernet0/1 的队列统计值：

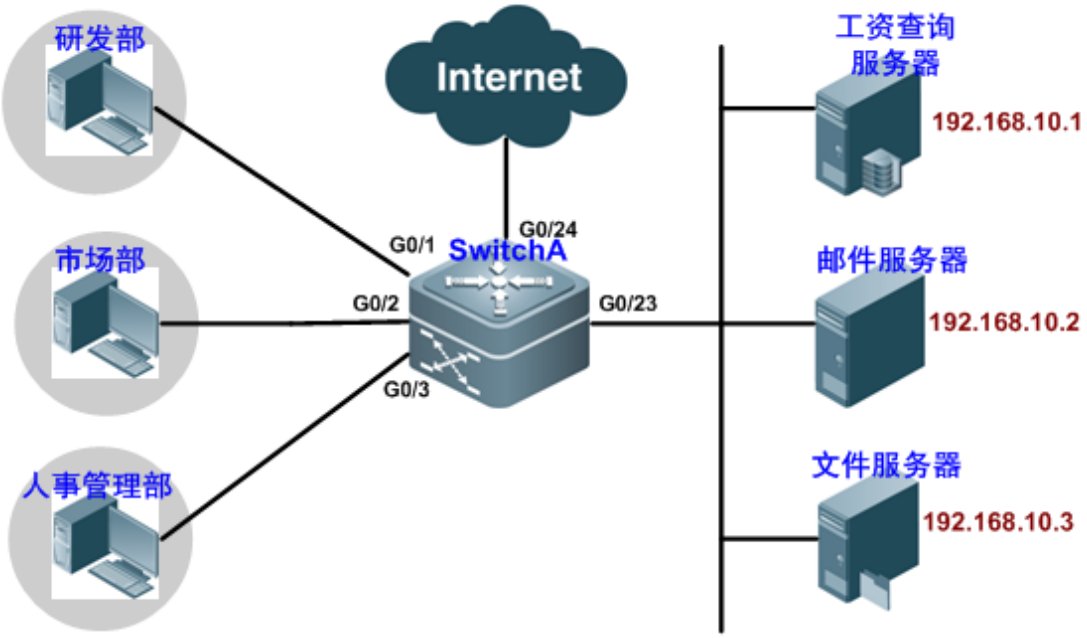
```
Ruijie#show interfaces gigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is DOWN  , line protocol is DOWN
Hardware is S5750E GigabitEthernet
Interface address is: no ip address
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Bridge, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  Rxload is 1/255, Txload is 1/255
  Queue:   Transmitted packets    Transmitted bytes      Dropped packets        Dropped bytes
    0                        0                    0                    0                    0
    1                        0                    0                    0                    0
    2                        0                    0                    0                    0
    3                        0                    0                    0                    0
    4                        0                    0                    0                    0
    5                        0                    0                    0                    0
    6                        0                    0                    0                    0
    7                        4                  288                    0                    0
  Switchport attributes:
    interface's description:""
    admin medium-type is Copper, oper medium-type is Copper
    lastchange time:0 Day: 0 Hour: 1 Minute:32 Second
    Priority is 0
    admin duplex mode is AUTO, oper duplex is Unknown
    admin speed is AUTO, oper speed is Unknown
    flow control admin status is OFF, flow control oper status is Unknown
    Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF
  Port-type: access
    Vlan id: 1
  5 minutes input rate 0 bits/sec, 0 packets/sec
  5 minutes output rate 0 bits/sec, 0 packets/sec
    4 packets input, 256 bytes, 0 no buffer, 0 dropped
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    4 packets output, 256 bytes, 0 underruns , 0 dropped
    0 output errors, 0 collisions, 0 interface resets
```

2.4 QOS典型配置用例

2.4.1 优先级重标记+队列调度应用

组网图

图 1-1 优先级重标记+队列调度应用图



某公司企业网通过交换机（本例为 SwitchA）实现业务互连。网络环境描述如下：

- 研发部、市场部和人事管理部分别接入 SwitchA 的端口 GigabitEthernet 0/1、GigabitEthernet 0/2 和 GigabitEthernet 0/3；
- 工资查询服务器、邮件服务器和文件服务器连接在 SwitchA 的端口 GigabitEthernet 0/23 下。

应用需求

配置优先级重标记和队列调度，实现下述需求：

- 当研发部和市场部访问服务器时，服务器报文的优先级为：邮件服务器> 文件服务器>工资查询服务器
- 无论人事管理部访问 Internet 或访问服务器，交换机都优先处理。
- 交换机在运行过程中，时常发现网络拥塞，为了保证业务顺利运转，要求使用 WRR 队列调度，使访问邮件数据库、访问文件数据库、访问工资查询数据库的 IP 数据报按照 6：2：1 的比例来调度。

配置要点

- 通过配置访问不同服务器数据流的 cos 值，实现设备处理访问各种服务器报文的优先级；
- 通过配置接口的缺省 CoS 值为特定值，实现设备优先处理人事管理部发出的报文；
- 通过配置 WRR 队列调度实现按特定个数比进行数据报文传输调度；

配置步骤

第一步，创建访问各类服务器的 ACL：

```
SwitchA(config)#ip access-list extended salary
SwitchA(config-ext-nacl)#permit ip any host 192.168.10.1
SwitchA(config-ext-nacl)#exit
SwitchA(config)#ip access-list extended mail
SwitchA(config-ext-nacl)#permit ip any host 192.168.10.2
SwitchA(config-ext-nacl)#exit
SwitchA(config)#ip access-list extended file
SwitchA(config-ext-nacl)#permit ip any host 192.168.10.3
```

第二步，创建匹配各类服务器 ACL 的 class-map：

```
SwitchA(config)#class-map salary
SwitchA(config-cmap)#match access-group salary
SwitchA(config-cmap)#exit
SwitchA(config)#class-map mail
SwitchA(config-cmap)#match access-group mail
SwitchA(config-cmap)#exit
SwitchA(config)#class-map file
SwitchA(config-cmap)#match access-group file
```

第三步，将 policy-map 关联相应的 class-map，并配置访问邮件服务器数据流的 cos 值访问文件服务器数据流的 cos 值访问工资查询服务器数据；流的 cos 值：

```
SwitchA(config)#policy-map toserver
SwitchA(config-pmap)#class mail
SwitchA(config-pmap-c)#set cos 4
SwitchA(config-pmap-c)#exit
SwitchA(config-pmap)#class file
SwitchA(config-pmap-c)#set cos 3
SwitchA(config-pmap-c)#exit
SwitchA(config-pmap)#class salary
SwitchA(config-pmap-c)#set cos 2
SwitchA(config-pmap-c)#end
```

第四步，将 policy-map 应用到相应端口,并配置端口的 Qos 信任模式

```
SwitchA(config)#interface gigabitEthernet 0/1
SwitchA(config-if-GigabitEthernet 0/1)#service-policy input toserver
SwitchA(config-if-GigabitEthernet 0/1)#mls qos trust cos
```

```
SwitchA(config-if-GigabitEthernet 0/1)#exit
SwitchA(config)#interface gigabitEthernet 0/2
SwitchA(config-if-GigabitEthernet 0/2)#service-policy input toserver
SwitchA(config-if-GigabitEthernet 0/2)#mls qos trust cos
SwitchA(config-if-GigabitEthernet 0/2)#exit
```

第五步，配置设备的端口优先级队列调度方式为绝对优先级调度：

```
SwitchA(config)#mls qos scheduler sp
```

第六步，配置下联人事管理部接口的缺省 CoS 值为 7，优先保障人事管理部发出的报文，并配置端口的 Qos 信任模式：

```
SwitchA(config)#interface gigabitEthernet 0/3
SwitchA(config-if-GigabitEthernet 0/3)#mls qos cos 7
SwitchA(config-if-GigabitEthernet 0/3)#mls qos trust cos
```

第七步，配置 WRR 队列调度的输出轮转权重：

```
SwitchA(config)#wrr-queue bandwidth 1 1 1 2 6 1 1 1
```

第八步，配置设备的端口优先级队列调度方式为 WRR 调度：

```
SwitchA(config)#mls qos scheduler wrr
```

配置验证

第一步，确认 class-map 的内容是否配置正确：

```
SwitchA(config)#show class-map
 Class Map salary
   Match access-group salary
 Class Map mail
   Match access-group mail
 Class Map file
   Match access-group file
```

第二步，确认 policy-map 的内容是否配置正确：

```
SwitchA(config)#show policy-map
 Policy Map toserver
    Class mail
      set cos 4
    Class file
      set cos 3
    Class salary
      set cos 2
```

第三步，确认对应端口的 QOS 信息是否正确：

```
SwitchA(config)#show mls qos interface gigabitEthernet 0/1
Interface: GigabitEthernet 0/1
```

```
Attached input  policy-map: toserver
Attached output policy-map:
Default trust: cos
Default cos: 0
SwitchA(config)#show mls qos interface gigabitEthernet 0/2
Interface: GigabitEthernet 0/2
Attached input  policy-map: toserver
Attached output policy-map:
Default trust: cos
Default cos: 0
```

第四步，确认 QOS 队列信息

```
SwitchA(config)#show mls qos queueing
Cos-queue map:
cos qid
--- ---
0   1
1   2
2   3
3   4
4   5
5   6
6   7
7   8

wrr bandwidth weights:
qid weights
--- -------
1   1
2   1
3   1
4   2
5   6
6   1
7   1
8   1

drr bandwidth weights:
qid weights
--- -------
1   1
2   1
3   1
4   1
5   1
```

6 1
7 1
8 1

配置指南-可靠性

本分册介绍可靠性配置指南相关内容，包括以下章节：

1. RLDP
2. TPP
3. RNS&Track
4. GRTD
5. SEM

1 RLDP

1.1 概述

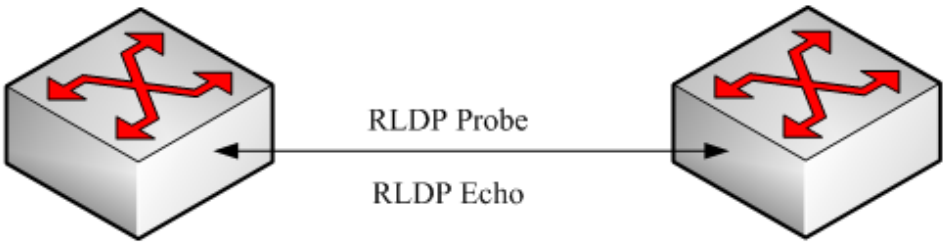
RLDP 全称是 Rapid Link Detection Protocol，是锐捷网络自主开发的一个用于快速检测以太网链路故障的链路协议。

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。

RLDP 是利用在链路两端交换 RLDP 报文来实现检测的，如下图所示：

图 3-1

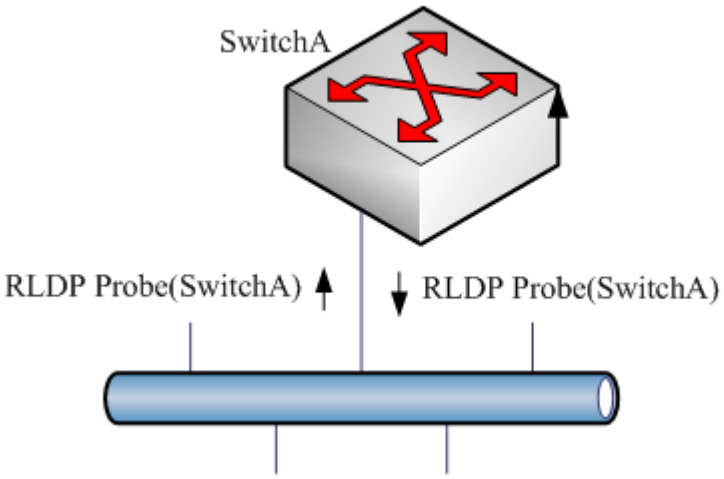


RLDP 定义了两种协议报文：探测报文(Probe)和探测响应报文(Echo)。RLDP 会在每个配置了 RLDP 并且是 linkup 的端口周期性地发送本端口的 Probe 报文，并期待邻居端口响应该探测报文，同时也期待邻居端口也发送自己的 Probe 报文。如果一条链路在物理和逻辑上都是正确的，那么一个端口应该能收到邻居端口的探测响应报文以及邻居端口的探测报文。否则链路将被认定是异常的。

要使用 RLDP 的单向检测和双向检测功能，必须保证链路两端的端口都打开了 RLDP，并且不允许一个开启了 RLDP 的端口下连多个邻居端口，否则 RLDP 无法检测出每个邻居的链路健康状况。

1.1.1 环路检测

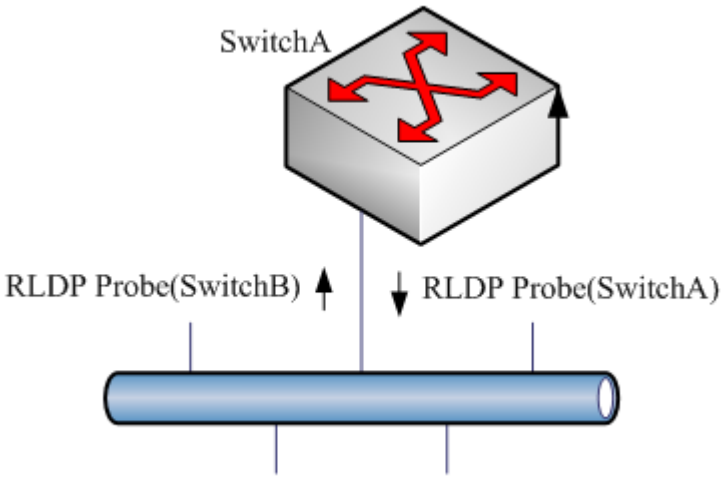
图 3-2 环路检测



所谓的环路故障是指端口连接的链路上出现了环路。如上图所示，RLDP 在某个端口上收到了本机发出的 RLDP 报文，则该端口将被认为是出现了环路故障，于是 RLDP 会根据用户的配置对这种故障做出处理，包括警告、设置端口违例、关闭端口所在的 svi、关闭端口学习转发等。

1.1.2 单向链路检测

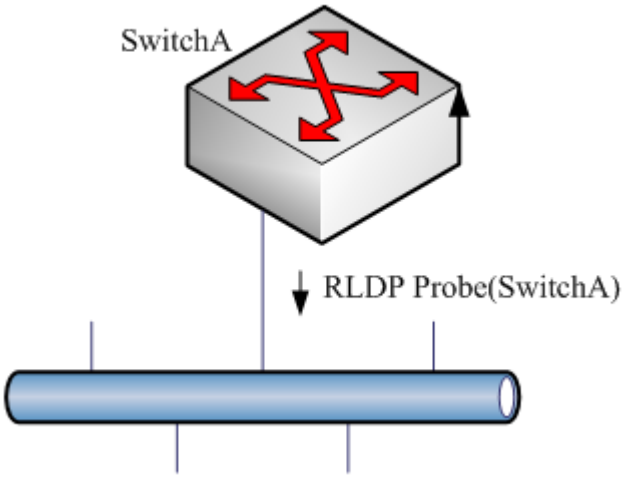
图 3-3 单向链路检测



所谓单向链路故障是指端口连接的链路只能接收报文或者只能发送报文（比如由于光纤接收线对接错误导致的单向接收或单向发送）。如上图所示，RLDP 在某个端口上只收到邻居端口的探测报文则该端口将被认为单向链路故障，于是 RLDP 会根据用户的配置对这种故障做出处理。另外如果端口无法收到任何 RLDP 检测报文，也会被认为是发生了单向链路故障。

1.1.3 双向链路检测

图 3-4 双向链路检测



所谓双向链路故障是指链路两端的帧收发都出现了故障。如上图所示，设备的端口在发出 RLDP 探测报文后，就一直无法接收到响应报文或邻居的探测报文，那么该链路将被认为是双向故障的。从故障性质上讲，双向故障实际上包含了单向故障。

如果链路两端有某一方未开启 RLDP 也会被诊断为双向或单向链路故障，因此配置双向链路检测或单向链路检测时需要管理员保证链路两端都开启了 RLDP，以避免出现错误的诊断信息。

10.4(3)软件版本，RLDP 协议缺省情况下只发送 SNAP 格式的报文（SNAP 封装中，DSAP 和 SSAP 字段固定为 0xAA，Control 字段固定为 0x03，通过 PID 字段来区分标识协议，对于 RLDP，PID 字段取值为 0x0788）。当收到 Ethernet II 格式的协议报文时，迁移到只发送 Ethernet II 格式的协议报文与邻居交互。因此，版本兼容的前提是需要能收到邻居的协议报文。这样，当 10.4(3)软件版本与非 10.4(3)软件版本互连时，如果对端已检测出链路故障，建议先恢复链路的错误状态。

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	3S
最大探测次数	2 次

RLDP 只能基于物理端口进行配置，包括 ap 成员口(支持 L2 和 L3 的 AP 成员口)，但无法在 SVI 上配置。对于 AP 口的配置是发散到该 AP 的每个成员口生效。

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
Ruijie(config)# **rldp enable**	打开全局的 RLDP 功能开关。
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
Ruijie(config)# **interface** *interface-id*	进入接口模式
Ruijie(config-if)# **rldp port** { **unidirection-detect | bidirection-detect | loop-detect** } { **warning | shutdown-svi | shutdown-port | block** }	端口打开 RLDP，同时配置诊断类型和故障处理方法。
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。

例：在 AP 成员口 GigabitEthernet 0/5 上配置 RLDP 并指定多个诊断类型和故障处理方法

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/5
Ruijie(config-if)# port-group 1
Ruijie(config-if)# rldp port unidirection-detect shutdown-svi
Ruijie(config-if)# rldp port bidirection-detect warning
Ruijie(config-if)# rldp port loop-detect block
Ruijie(config-if)# end
Ruijie# show rldp interface gigabitEthernet 0/5
port state      : normal
local bridge    : 00d0.f822.33ac
neighbor bridge : 0000.0000.0000
neighbor port   :
unidirection detect information:
action : shutdown svi
```

```
state  : normal
bidirection detect information :
action : warnning
state  : normal
loop detect  information       :
action : block
state  : normal
```

注意事项

配置端口检测有以下注意事项：

- 路由口不支持 shutdown-svi 的错误处理方法，因此该方法在路由口发生检测错误时将不被执行。
- 配置环路检测时要求端口下连的邻居设备不能开启 RLDP 检测，否则该端口将无法做出正确的检测。
- 如果 RLDP 检测出链路错误，则会发出警告信息。用户可以通过配置 log 功能将这些警告信息发到 log 服务器，记录 log 的级别至少要保证可以记录 3 级日志。
- 由于产品特性的不同，某些产品对于 block 的端口仍然会将报文送 cpu, 这就导致在配置诊断类型为环路检测、故障处理方法为 block 时，当设备检测出环路并将端口 block 处理后，仍会有大量的报文送 cpu,这样就未能达到环路检测的效果，所以建议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 故障处理方法中的 block 功能需要和 STP 互斥。也就是说如果用户配置了端口的故障处理方法为 block，则建议关闭 STP，否则由于 STP 无法识别单向链路，可能会出现 STP 允许端口转发，但 RLDP 却设置端口 block 的情况。如果要和 STP 共用，我们建议将错误处理方法配置为”shutdown-port”。
- 对于 AP 成员口上的 RLDP 配置，如果是配置环路检测，则会同步配置到该 AP 的所有成员口，如果是配置单向链路检测和双向链路检测，则直接在 AP 成员口生效。
- 对于物理口加入 AP 的情况，新加入的 AP 成员口的环路检测配置需要和该 AP 现有的成员口的环路检测配置一致。这里分 3 种情况：1）、如果新加入的 AP 成员口没有配置环路检测，而该 AP 现有的成员口有配置环路检测，则新加入的 AP 成员口同步环路检测的配置和检测结果。2）如果新加入的 AP 成员口有配置环路检测，而该 AP 现在的所有成员口都没有配置环路检测，则新加入的 AP 成员口清除环路检测配置并加入 AP。3）、如果新加入的 AP 成员口的环路检测配置和该 AP 现有的成员口的环路检测配置不一致，则新加入的 AP 成员口同步环路检测的配置和检测结果。
- AP 成员口配置 RLDP 时，故障处理方法只能配置为”shutdown-port”，如果故障处理方法配置为非”shutdown-port”时，将转换成”shutdown-port”的配置并生效。

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
Ruijie(config)# **rldp detect-interval** *interval*	配置探测间隔，interval 取值范围是 2-15s,默认是 3s。
Ruijie(config)# **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
Ruijie(config)# **rldp detect-max** *num*	配置最大探测次数，num 取值范围是 2-10,默认是 2 次。
Ruijie(config)# **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。

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
Ruijie# **rldp reset**	使所有 RLDP 检测失败的端口重新开始检测。

用户也可以在全局配置模式下使用 **errdisable recover** 命令来即时或定时重新启动被 rlp 设置成违例的端口的 RLDP 检测。

1.2.6 查看RLDP信息

查看所有端口的 RLDP 状态

在特权模式下使用如下命令查看 RLDP 的全局配置和所有配置了 rldp 检测的端口的检测信息：

命令	作用
Ruijie# **show rldp**	查看 RLDP 的全局配置和所有配置了 rldp 检测的端口的检测信息。

以下例子使用 **show rldp** 命令查看 rldp 所有端口的检测信息：

```
Ruijie# show rldp
rldp state          : enable
rldp hello interval : 3
rldp max hello      : 2
```

```
rldp local bridge   : 00d0.f8a6.0134
-----------------------------------------------
interface GigabitEthernet 0/1
port state:normal
neighbor bridge : 00d0.f800.41b0
neighbor port   : GigabitEthernet 0/2
unidirection detect information:
action : shutdown svi
state  : normal
interface GigabitEthernet 0/24
port state:error
neighbor bridge : 0000.0000.0000
neighbor port   :
bidirection detect information :
action : warnning
state  : error
```

从上述信息可以看到，端口 GigabitEthernet 0/1 配置了单向检测，并且当前未检测到错误，端口状态为正常(normal)。端口 GigabitEthernet 0/24 配置了双向检测，并且检测到了双向故障。

查看指定端口的 RLDP 状态

在特权模式下使用如下命令查看指定端口的 RLDP 检测信息：

命令	作用
show rldp interface *interface-id*	查看 *interface-id* 的 rldp 检测信息。

以下例子使用 show rldp interface GigabitEthernet *0/1* 命令查看 fas0/1 端口的 rldp 检测信息：

```
Ruijie# show rldp int GigabitEthernet 0/1
port state      : error
local bridge    : 00d0.f8a6.0134
neighbor bridge : 00d0.f822.57b0
neighbor port   : GigabitEthernet 0/1
unidirection detect information:
action: shutdown svi
state : normal
bidirection detect information :
action : warnning
state : normal
loop detect  information    :
action: shutdown svi
state : error
```

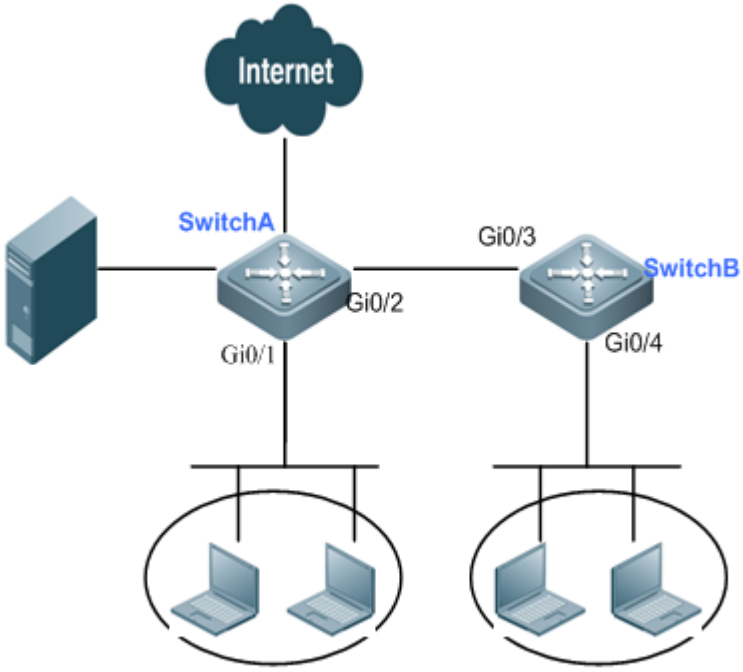
从上述信息可以看到，端口 GigabitEthernet 0/1 配置了三种检测类型：单向检测、双向检测、环路检测,故障时的错误处理分别为关闭端口所在的 svi、产生警告信息、关闭端口所在的 svi，其中环路检测发现了错误，使得当前的端口状态为 error，相应的，该端口所属的 svi 也被 shutdown。

1.3 配置举例

1.3.1 RLDP故障检测与处理

拓扑图

图 3-5 RLDP 应用拓扑图



应用需求

如上图所示，企业各部门用户通过设备 Switch A、Switch B 接入网络。由于链路中断或者用户人为造成网络环路等非设备因素造成网络中断，通过配置 RLDP 环路检测以及单双向链路检测功能，能迅速定位并处理故障，从而及时恢复网络，降低网络中断给企业带来的业务损失。主要需求有：

- 一旦检测到环路故障或者单双向链路故障，则根据配置的故障处理方法作故障处理；
- 若配置了 shutdown-port 故障处理的端口出现故障，要求主动恢复其 RLDP 检测，并使所有 RLDP 检测失败的端口重新开始检测。

配置要点

- 配置全局 RLDP 后再配置端口 RLDP，同时配置诊断类型和故障处理方法。
- 在特权模式下，使用 **rldp reset** 命令使所有 RLDP 检测失败的端口重新开始检测。

对环路检测来说，下联端口（在企业各部门用户或服务器上连接设备的端口）不能开启 RLDP；对单双向链路检测来说，设备对接端口 RLDP 都需开启。若端口为路由口，则只能用 warning、block 或 shutdown-port 故障处理方法，不支持 shutdown-svi 故障处理方法。

配置步骤

第一步，在设备上开启 RLDP。

！在 Switch A 上开启全局 RLDP。

```
SwitchA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)#rldp enable
```

！Switch B 的配置同上。

第二步，在设备端口上配置诊断类型与故障处理方法。

！在 Switch A 上开启端口 RLDP，并在端口 Gi0/1 上配置环路检测及故障处理方法 block，在端口 Gi0/2 上配置单向链路检测及故障处理方法 warning。

```
SwitchA(config)#interface gigabitEthernet 0/1
SwitchA(config-if)#rldp port loop-detect block
SwitchA(config-if)#exit
SwitchA(config)#interface gigabitEthernet 0/2
SwitchA(config-if)#rldp port unidirection-detect warning
SwitchA(config-if)#exit
```

！在 Switch B 上开启端口 RLDP，并在端口 Gi0/4 上配置环路检测及故障处理方法 block，在端口 Gi0/3 上配置双向链路检测及故障处理方法 shutdown-port。

```
SwitchB(config)#interface gigabitEthernet 0/4
SwitchB(config-if)#rldp port loop-detect block
SwitchB(config-if)#exit
SwitchB(config)#interface gigabitEthernet 0/3
SwitchB(config-if)#rldp port bidirection-detect shutdown-port
SwitchB(config-if)#exit
```

第三步，恢复端口 RLDP 检测。

！在 Switch A 上执行 **rldp reset** 命令。

```
SwitchA#rldp reset
```

！Switch B 的配置同上。

配置验证

查看设备所有端口的 RLDP 信息。

！ Switch A 所有端口的 RLDP 信息

```
SwitchA#show rldp
rldp state         : enable
rldp hello interval: 3
rldp max hello     : 2
rldp local bridge  : 00d0.f822.33aa
-----------------------------------
Interface GigabitEthernet 0/2
port state      : normal
neighbor bridge : 00d0.f800.41b0
neighbor port   : GigabitEthernet 0/3
unidirection detect information:
     action: warning
     state : normal

Interface GigabitEthernet 0/1
port state      : normal
neighbor bridge : 0000.0000.0000
neighbor port   :
loop detect information   :
     action: block
     state : normal
```

！ Switch B 所有端口的 RLDP 信息

```
SwitchB#show rldp
rldp state         : enable
rldp hello interval: 3
rldp max hello     : 2
rldp local bridge  : 00d0.f800.41b0
-----------------------------------
Interface GigabitEthernet 0/3
port state      : normal
neighbor bridge : 00d0.f822.33aa
neighbor port   : GigabitEthernet 0/2
bidirection detect information:
     action: shutdown-port
     state : normal

Interface GigabitEthernet 0/4
```

```
port state      : normal
neighbor bridge : 0000.0000.0000
neighbor port   :
loop detect information    :
     action: block
     state : normal
```

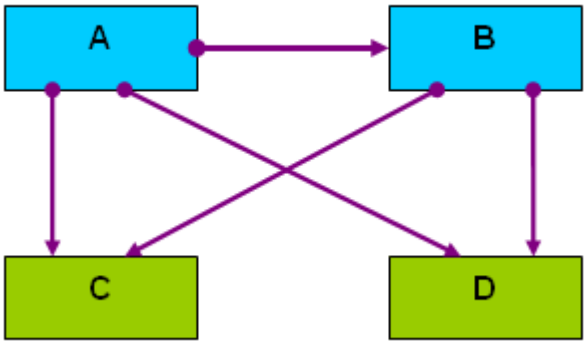
2 TPP

2.1 概述

TPP(Topology Protection Protocol，拓扑保护协议)是一个拓扑稳定保护协议。网络拓扑比较脆弱，当网络中存在非法攻击时，可能造成网络设备的 CPU 利用率异常、帧通路堵塞等现象，这些现象很容易引起网络拓扑的振荡。拓扑防护主要通过检测本地的异常现象（CPU 利用率异常、帧缓冲异常等）和检测邻居设备的异常现象来达到稳定网络拓扑的目的。与邻居设备的交互是通过发送特定的异常通告报文来实现的，该功能拥有较高的运行优先级，可以有效防止网络的拓扑振荡。

拓扑防护主要是针对 MSTP 或 VRRP 以及其他分布式网络协议可能造成的网络拓扑振荡而产生的。MSTP 或 VRRP 等协议均使用定时报文通告机制来自动维护网络拓扑结构，自动适应网络中的拓扑变化。这也造成了网络拓扑易受攻击，当受到人为的网络攻击时，因 CPU 利用率过高或帧通路阻塞等原因，可能造成定时报文的短暂中断，从而造成网络拓扑发生错误的振荡，这给网络的正常通信造成极大危害。而拓扑防护功能正是为了最大限度的防止这种不必要的网络振荡，它与其他分布式协议（MSTP、VRRP 等）协同工作，从而使网络更加稳定、可靠。

图 5-1

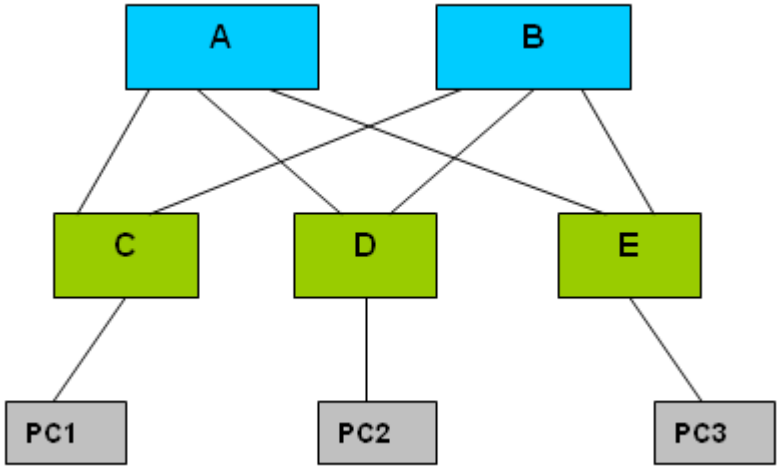


如上图的双核心拓扑，图中 A、B 为三层汇聚设备，C、D 为二层接入设备。A 为 MSTP 的根桥，各个网络设备的拓扑防护功能均开启。

三层汇聚设备 A 因遭受网络攻击造成 CPU 异常繁忙，从而导致 BPDU 报文不能正常发送。这时，拓扑防护功能检测到异常后，会向邻居设备发送异常通告报文，图中二层接入设备 C、D 的和三层汇聚设备 B 均接收到异常通告，这时，设备 C、D 的和设备 B 会根据异常通告信息，进行相应的防振荡处理。

设备 B 因遭受大量报文攻击造成 CPU 异常繁忙，这时造成收发包不正常，检测到异常后，它会向所有的邻居设备发送异常通告。设备 A 收到异常报文后，根据来源，发现异常对其没有影响，不会进一步处理。而下游的二层接入设备 C、D 接收到异常报文后，发现异常会影响其拓扑的计算，因此做进一步的防御处理，从而保证网络拓扑保持稳定。

图 5-2



如上图，A、B 为三层汇聚设备，C、D 和 E 为二层接入设备。

三层汇聚设备 A、B 和二层接入设备 C、D 和 E 均开启 MSTP，同时两台三层汇聚设备开启 VRRP 协议。拓扑防护功能使 MSTP 和 VRRP 运行更加稳定，避免网络拓扑发生不必要的振荡。

对于三层汇聚设备 A、B 使能全局拓扑防护功能，同时使能各个端口的拓扑防护功能。对于各台二层接入设备 C、D 和 E 使能全局拓扑防护功能。

2.2 配置TPP

TPP 配置包括全局功能配置和端口功能配置。全局功能配置用于使能设备的拓扑防护功能，默认情况下，全局拓扑防护功能使能，这时它会检测本地和邻居设备的运行情况，对产生的异常情况进行处理。不过它不会向邻居设备通告本地的运行情况。端口功能配置用于使能端口的拓扑防护功能，端口的拓扑防护功能使能时，表示对端的邻居设备关心本地设备的运行情况，因此当本地设备发生异常时，将通告该端口的对端邻居设备。默认情况下，所有端口的拓扑防护功能关闭。

> 拓扑防护功能适用于点对点链路的网络，且相邻网络设备都必须使能拓扑防护功能。另外，部署 TPP 功能时，通常需要通过 cpu topology-limit 命令配置 cup 利用率检测的阀值，当设备的 cpu 利用率超过该值时，系统会产生拓扑防护通告。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该切换的时候由于 TPP 的报警而不切换，如果该值太高，则可能系统已经繁忙到无法产生 TPP 告警，导致 TPP 功能失效。

2.2.1 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
Ruijie# **config terminal**	进入全局配置模式
Ruijie(config)# **topology guard**	使能全局拓扑防护

使用 **no topology guard** 禁止设备的全局拓扑防护功能

2.2.2 配置端口拓扑防护

配置命令如下：

命令	作用
Ruijie# **config terminal**	进入全局配置模式
Ruijie(config)# **interface** *interface-id*	进入接口配置模式
Ruijie(config-if)# **tp-guard port enable**	使能端口拓扑防护功能

使用 **no tp-guard port enable** 禁止端口的拓扑防护，该命令只适用于二层交换口和路由口。不适用于 AP 成员口。

全局拓扑防护作为拓扑防护的全局开关，当全局拓扑防护使能时，设备会检测本设备的运行参数，同时监听各个邻居设备的运行参数，但当本地出现异常现象时，它不会向邻居设备发送异常通告报文进行通告。端口的拓扑防护功能使能时，当本地出现异常现象时，会向该端口对端的邻居设备发送异常通告报文进行异常通告。

2.2.3 查看设备的TTP配置及状态

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
Ruijie# **show tpp**	查看设备的 TPP 配置及状态。

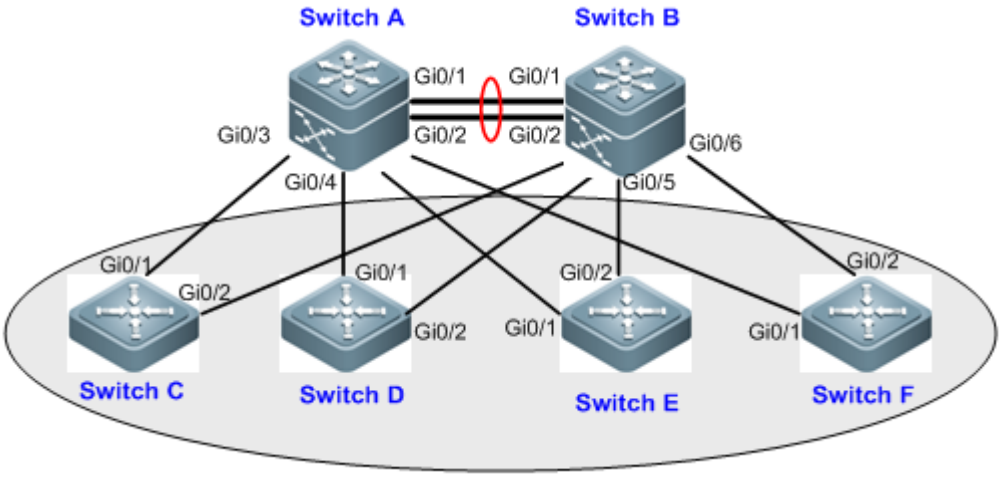
例：

```
Ruijie #show tpp
tpp state         : enable
tpp local bridge  : 00d0.f822.35ad
```

2.3 配置举例

拓扑图

图 5-3 TPP 典型应用拓扑图



应用需求

如上图所示，某园区网络的核心层采用典型的 MSTP+VRPP 双核心拓扑结构。当网络中存在非法攻击时，可能造成网络设备的 CPU 利用率异常、帧通路堵塞等现象，很容易引起网络拓扑的振荡。

通过应用 TPP 功能，使 MSTP 和 VRRP 的运行能较为稳定，避免网络拓扑发生不必要的振荡。

配置要点

在三层核心设备（Switch A/B）和二层接入设备（Switch C/D/E/F）上配置以下功能：

- 使能全局拓扑防护功能。该功能默认开启。
- 使能连接设备的接口的拓扑防护功能，在本机出现异常时能及时通告邻居保持拓扑稳定。
- 在每台设备上配置 CPU 利用率检测的阈值，当设备的 CPU 利用率超过该值时，系统会产生拓扑防护通告。

建议该值设置在一个中等偏上的位置比较合适，比如 50-70，这时 TPP 能够较为准确地对网络情况进行判断。如果该值太低，则可能导致网络拓扑该切换的时候由于 TPP 的报警而不切换，如果该值太高，则可能系统已经繁忙到无法产生 TPP 告警，导致 TPP 功能失效。

配置步骤

以下仅列举设备上的 TPP 功能配置，对于 MSTP+VRPP 的相关配置说明可参见手册的《MSTP 配置》和《VRRP 配置》部分。

- Switch A/B 上的配置

第一步，全局拓扑防护功能功能默认开启。如果被关闭，可以使用以下命令开启。

```
Ruijie# config terminal
Ruijie(config)# topology guard
```

第二步，开启接口拓扑防护功能

！开启核心设备间 AP 口的拓扑防护功能

```
Ruijie(config)#interface aggregateport 1
Ruijie(config-if-AggregatePort 1)#tp-guard port enable
```

！开启下联设备接口的端口拓扑防护功能

```
Ruijie(config)#interface range gigabitEthernet 0/3-6
Ruijie(config-if-range)#tp-guard port enable
```

第三步，配置 CPU 利用率检测的阈值

！在设备 cpu 利用率超过百分之六十时，系统会产生拓扑防护通告

```
Ruijie(config)#cpu topology-limit 60
```

- Switch C/D/E/F 上的配置

第一步，全局拓扑防护功能功能默认开启。如果被关闭，可以使用以下命令开启。

```
Ruijie# config terminal
Ruijie(config)# topology guard
```

第二步，开启接口拓扑防护功能

```
Ruijie(config)#interface range gigabitEthernet 0/1-2
Ruijie(config-if-range)#tp-guard port enable
```

第三步，配置 CPU 利用率检测的阈值

！在设备 CPU 利用率超过百分之六十时，系统会产生拓扑防护通告

```
Ruijie(config)#cpu topology-limit 60
```

验证结果

- TPP 功能配置查看

以 Swtich A 为例，查看 TPP 的配置；关注点：TPP 状态，接口 TPP 信息。

```
Ruijie#show tpp
tpp state         : enable       //全局 TPP 功能默认开启
tpp local bridge  : 00d0.f822.33aa
----------------------------------
interface GigabitEthernet 0/3
port tpp state       : enable
interface GigabitEthernet 0/4
port tpp state       : enable
interface GigabitEthernet 0/5
port tpp state       : enable
interface GigabitEthernet 0/6
port tpp state       : enable
```

```
interface AggregatePort 1
port tpp state       : enable
```

■ TPP 功能生效性验证

生成树拓扑稳定时，SwitchA 为根桥， Swtich C 的 Gi0/2 口处于 Block 状态。

第一步，为了模拟 Swtich C 由于受到下连非法用户的攻击。在验证中，将 Swtich B 的 Gi0/3 口配置 BPDU Filter 功能，使得 Swtich C 的 Gi0/2 口收不到 BPDU 报文；在未配置 TPP 的情况下，Swtich C 的 Gi0/2 口转变成 Forwarding 状态。拓扑改变。

```
Ruijie#show spanning-tree sum
Spanning tree enabled protocol mstp
MST 0 vlans map : 1-9, 11-19, 21-29, 31-39, 41-4094
  Root ID    Priority    4096
             Address     00d0.f834.56f0
             this bridge is root
             Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

  Bridge ID  Priority    32768
             Address     00d0.f822.33aa
             Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

Interface   Role   Sts   Cost    Prio   Type   OperEdge
---------   ----   ---   -----   ----   ----   --------
Gi0/2       Desg   FWD   20000   128    P2p    True
Gi0/1       Root   FWD   20000   128    P2p    False

MST 1 vlans map : 10, 20
  Region Root Priority   4096
             Address     00d0.f834.56f0
             this bridge is region root

  Bridge ID  Priority    32768
             Address     00d0.f822.33aa

Interface   Role   Sts   Cost    Prio   Type   OperEdge
---------   ----   ---   -----   ----   ----   --------
Gi0/2       Desg   FWD   20000   128    P2p    True
Gi0/1       Root   FWD   20000   128    P2p    False
```

第二步，在 Swtich C 按本例的配置步骤完成 TPP 的相关配置后，模拟 Swtich C 受到下连非法用户的攻击，向 Swtich C 发送大量 ARP 报文，导致 CPU 利用率超过限定值。此时再将 Swtich B 的 Gi0/3 口配置 BPDU Filter 功能，使得 Swtich C 的 Gi0/2 口收不到 BPDU 报文；查看 Swtich C 生成树接口的状态，发现接口仍然维持在 Block 状态。TPP 功能生效。

```
Ruijie#show spanning-tree summary
Spanning tree enabled protocol mstp
```

```
MST 0 vlans map : 1-9, 11-19, 21-29, 31-39, 41-4094
  Root ID    Priority    4096
             Address     00d0.f834.56f0
             this bridge is root
             Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

  Bridge ID  Priority    32768
             Address     00d0.f822.33aa
             Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

Interface   Role   Sts   Cost    Prio   Type   OperEdge
---------   ----   ---   -----   ----   ----   --------
Gi0/2       Altn   BLK   20000   128    P2p    False
Gi0/1       Root   FWD   20000   128    P2p    False

MST 1 vlans map : 10, 20
  Region Root Priority   4096
             Address     00d0.f834.56f0
             this bridge is region root

  Bridge ID  Priority    32768
             Address     00d0.f822.33aa

Interface   Role   Sts   Cost    Prio   Type   OperEdge
---------   ----   ---   -----   ----   ----   --------
Gi0/2       Altn   BLK   20000   128    P2p    False
Gi0/1       Root   FWD   20000   128    P
```

3 Rns & track

3.1 概述

rns 是 ruijie network service 的缩写，rns 通过探测对端设备是否有响应报文发出，来监控端到端连接的完整性。利用 rns 的探测结果，用户可以对网络故障进行诊断和定位。目前锐捷实现了 icmp-echo 和 dns 两种探测类型。

为了提高通信的可靠性，一些应用模块需要及时跟踪接口链路状态或网络可达性。负责接口链路状态和网络可达性的监测模块与应用模块之间增加 track 模块，可以屏蔽不同监测模块的差异，简化应用模块的处理。一个 track 对象可以跟踪一个 IP 地址是否可达，也可以跟踪一个接口是否是 up 的。track 功能分离了要跟踪的对象和对这个对象状态感兴趣的应用模块。当 track 对象状态变化时，应用模块采取动作。

3.2 配置rns

配置一个 rns 对象用来发送 icmp echo 报文。

命令	作用
Ruijie# **configure terminal**	进入全局配置模式
Ruijie(config)# **ip rns** *operation-number*	进入 ip rns 配置模式
Ruijie(config-ip-rns)# **icmp-echo** *destination-hostname* [**source-ipaddr** *ip-address*]	配置一个 ip rns 对象用来发送 icmp 报文

举例如下：

```
Ruijie> enable
Ruijie# configure terminal
Ruijie(config)# ip rns 1
Ruijie(config-ip-rns)# icmp-echo 10.1.1.1
```

显示 rns 对象的配置信息：

```
Ruijie# show ip rns configuration
Ip rns id:1
Type of operation to perform: icmp-echo
Target address/Source address:10.1.1.1/0.0.0.0
Operation timeout (milliseconds):1000
Vrf Name:
Operation frequency (milliseconds):1000
```

显示 rns 对象的统计信息：

```
Ruijie# show ip rns statistics
IP rns index    1
Number of successes:0
Number of failures:174
```

```
Round-trip min/avg/max = 0/0/0 ms
```

3.3 配置track

3.3.1 跟踪一个接口的链路状态

执行这个任务可以跟踪一个接口的链路状态。对于一个二层口，只要端口上电就认为是 up 的；对于三层口，只要三层口所包括的二层口有 up 的，就认为是 up；对于像 loopback 口这样的逻辑口，只要没有 shutdown 认为是 up 的。

配置步骤：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式
Ruijie(config)# **track** *object-number* **interface** *type number* **line-protocol**	跟踪一个接口的状态，并且进入 track 模式
Ruijie(config-track)# **delay** { **up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds* }	（可选）指定一段时间，当接口状态变化时，经过这段时间后才会改变 track 对象的状态，默认没有延迟。
Ruijie(config-track)# **show track** [*object-number*]	（可选）显示 track 对象的信息。可以使用这个命令来验证配置是否正确。

举例如下：

```
Ruijie> enable
Ruijie# configure terminal
Ruijie(config)# track 3 interface FastEthernet 1/0 line-protocol
Ruijie(config-track)# delay up 30
Ruijie(config-track)# show track 3
```

配置了一个 track 对象用来跟踪一个接口的状态，下面的例子显示了相关信息：

```
Ruijie# show track 3
Track 3
interface FastEthernet 1/0
The state is Up
1 change,current state last:11 secs
Delay up 10 secs,down 10 secs
```

3.3.2 跟踪一个rns对象的状态

我们用一个 track 对象来跟踪一个 rns 对象的状态，如果 rns 对象发送的报文有收到响应报文，则 track 对象状态为 up，相反 track 对象状态为 down。

> 当用 track 对象跟踪一个不存在的 rns 对象时,该 track 对象的状态是 up 的。

过程如下：

1) 配置一个 IP RNS 对象（略）

2) 配置一个 track 对象，跟踪 IP RNS 对象的状态。配置步骤如下：

命令	作用
Ruijie(config)# **track** *object-number* **rns** *entry-number*	跟踪一个 ip rns 对象的状态，并且进入 track 模式。
Ruijie(config-track)# **delay** { **up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds* }	（可选）指定一段时间，当 track 对象的状态变化时，经过这段时间后才会改变状态，默认没有延迟。
Ruijie(config-track)# **exit**	退到全局配置模式。

举例如下：

```
Ruijie(config)# track 123 rns 1
Ruijie(config-track)# delay up 30
Ruijie(config-track)# exit
```

显示 trackc 对象的状态：

```
Track 2
Ruijie Network Service 1
The state is Down
1 change,current state last:7 secs
Delay up 30 secs,down 0 secs
```

4 GRTD

4.1 概述

GRTD(Generic Real-Time Detections，通用实时检测)子系统提供一种实时故障检测功能。有了实时故障检测功能，用户可以在设备入网运行前或设备入网运行时检测设备是否存在硬件故障。

GRTD 提供四种硬件故障诊断方式：后台监控检测、系统启动自检、订制时间检测及 CLI 命令行检测。硬件检测功能主要检测系统管理链路及数据转发链路上各硬件组件是否正常，以确保系统在管理平面和数据转发平面无硬件故障。GRTD 的故障检测项分为影响系统正常运行的检测项及不影响系统正常运行的检测项：诸如端口环回测试、详尽的存储器测试等为影响系统正常运行的测试项；而 VSU 系统设备间通道测试等为不影响系统正常运行的检测项。

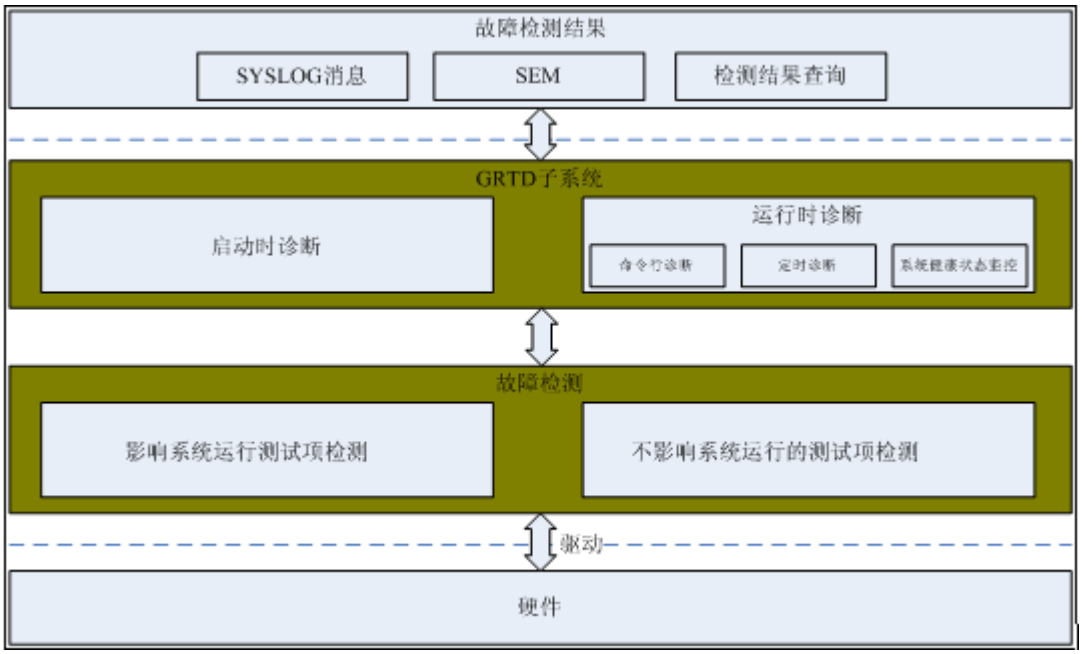
4.1.1 诊断范围

GRTD 可以检测以下几个方面问题：

- 各硬件组件
- 接口（以太网端口等）
- 连接器（VSU 系统设备间的连接器等）
- 存储器（内存、flash、芯片外挂存储器等）

4.1.2 工作原理

图 8-1 GRTD 框架图



由 GRTD 框架图中可以知道，GRTD 主要分三部分：

- 故障检测：根据设备硬件结构产生的具体检测项，主要分为影响系统正常运行检测项及不影响系统正常运行检测项。
- GRTD 子系统：检测功能核心模块，主要提供四种方式的检测功能。
- 故障检测结果：检测结果处理功能模块，主要用于故障检测结果的处理，包括产生 SYSLOG、与 SEM 模块的联动及结果查询。

GRTD 子系统提供四种检测方式：

- 启动时诊断：运行于系统初始化阶段，用于检测设备在使用前是否已经存在故障。
- 命令行诊断：利用 CLI 根据故障实行按需检测。
- 定时诊断：在用户指定时间进行检测项的检测。
- 监控检测：运行于系统后台，只有不影响系统正常运行的测试项能作为后台监控测试项。

实时诊断是网络高可靠性的要求之一，利用实时诊断降低设备异常给网络运行带来的一系列影响。网络高可靠性非常重要的一部分就是当设备在网络中运行时能实时检测硬件故障并根据硬件故障采取相应措施以降低硬件故障给网络带来的影响。GRTD 完成的就是这部分功能。

4.1.3 检测方式

GRTD 有以下四种检测方式。

启动自检

在设备初始化过程中对各硬件组件进行自检测试。启动自检分三个级别：最大限度自检测试、最小限度自检测试及不进行自检测试。最大限度自检测试与最小限度自检测试的区别在于参与启动自检测试的测试项数目不同，且最大限度自检测试包含

最小限度自检测试。可以通过命令 **show diagnostic content** 命令查询哪些测试项参与最大限度自检测试，哪些测试项参与最小限度自检测试。比如执行 **show diagnostic content** 命令的现实结果如下：

```
PortLoopbackTest--------------->  MPDX*******  not config     N/A
MacSelfTest-------------------->  C*DX*******  not config     N/A
```

PortLoopbackTest 其中一个属性为 M，则表示它将参与最小限度启动自检测试；MacSelfTest 其中一个属性为 C，则表示它将参与最大限度启动自检测试。如果当前系统配置的启动自检测试等级为最大限度自检测试，则在系统初始化过程中会执行 PortLoopbackTest 和 MacSelfTest 两项检测；如果当前系统配置的启动自检测试等级为最小限度自检测试，则在系统初始化过程中只会执行 PortLoopbackTest 这一项检测。

命令行检测

命令行检测是指根据需要利用 CLI 对某一测试项进行测试。测试完后该测试项的检测结果需输入命令进行查询。

监控检测

监控检测运行于系统后台，所有不影响系统正常运行的测试项都可以作为监控测试项。监控测试项测试失败，可以设置产生 SYSLOG 消息。对于监控测试项，可以设置激活或禁止其监控测试，可以设置其监控时间间隔，可以设置该监控测试项持续测试失败的次数。

> 影响系统正常运行的测试不能作为监控测试，监控测试的最小时间间隔为 1 秒。

计划测试

计划测试指根据用户配置好的时间启动相应测试项的测试，支持三种测试时间配置：

- on: 某一明确时间点进行测试
- daily: 每天的某一时间点进行测试
- weekly: 每周中某一天的某一时间点进行测试

> 不能配置同一时间点的不同测试方式，如已经为某一测试项配置在某一天的 12:00 进行计划测试，则无法再为其设置 daily 12:00 测试计划表。

4.1.4 检测项

使用 **show diagnostic content** 命令查看 GRTD 支持的检测项。

> 支持的检测项如下。

```
**************************************************************************
*Diagnostic test suite attributes:
M/C*/-Minimal bootup level test / Complete bootup level test / NA
P/V*/-Per port test / Per device test / NA
D/N*/-Disruptive test / Non-disruptive test / NA
```

```
  X*/-Not a health monitoring test / NA
  F*/-Fixed monitoring interval test / NA
  E*/-Always enabled monitoring test / NA
A/I*/-Monitoring in active / Monitoring in inactive / NA
Y/O*/-Key test / Non-key test / NA
  B*/-Basic ondemand test / NA
  R*/-Power-down line cards and need reload mainbord / NA
  K*/-Require resetting the line card after the test completed / NA
**************************************************************************
                                            test interval  Thre-
ID   Test Name                      Attributes  day hh:mm:ss   shold
===  ============================== ==========  ============   ====
 1)  PortLoopbackTest-------------->  MPDX*******  not config     N/A
 2)  MacSelfTest------------------->  C*DX*******  not config     N/A
 3)  TestCpld---------------------->  C*DX*******  not config     N/A
 4)  TestNandFlash----------------->  **DX*******  not config     N/A
 5)  TestNorFlash------------------>  **DX*******  not config     N/A
 6)  TestI2C----------------------->  C*DX*******  not config     N/A
 7)  TestPCI----------------------->  C*DX*******  not config     N/A
 8)  TestDdr----------------------->  **DX****B**  not config     N/A
```

测试项属性	说明
M / C	参与最小限度启动自检测试 / 参与最大限度启动自检测试
P / V	端口级测试 / 设备级测试
D / N	影响系统正常运行的测试 / 不影响系统正常运行的测试
X	不能作为监控测试项
F	监控测试间隔固定的监控测试
E	监控检测状态总是激活的监控测试
A / I	监控检测状态为激活 / 监控检测状态为禁止
Y / O	关键测试 / 非关键测试
B	只用于命令行测试
R	检测项测试完后需要重启设备及 VSU 系统
K	检测项测试完后需要重启设备

下文将对各检测项进行详细说明。

端口环回帧交换测试(PortLoopbackTest)

端口环回帧交换测试是指对设备上端口先进行环回操作（自环头环回或设置芯片 MAC/PHY 环回），然后对该端口进行包交换测试。如果测试失败，需要检查相应的硬件是否存在故障。测试前需要先指定所要测试的端口 ID 及这些端口的环回模式，如果不指定，默认被测端口 ID 为该设备上的所有端口且这些端口都为 MAC 环回。

可先对端口进行自环头环回测试，如果测试成功则表明端口无硬件故障，如果测试失败，可设置端口为 PHY 环回再进行测试，此时如果测试通过，则说明 PHY 与 RJ45 间存在故障，如果测试失败，需要继续将端口设置为 MAC 环回进行测试，如果测试成功，则说明 MAC 与 PHY 间存在硬件故障，而如果测试还是失败，则 CPU 到 MAC 间的硬件链路存在故障。

主要应用场景举例：在实际使用设备过程中，如果出现端口不通故障，可以利用此检测功能初步判断端口是否存在硬件故障。

MAC 芯片自检测试(MacSelfTest)

MAC 芯片自检测试是指 MAC 芯片类型自检测试以及 MAC 芯片与 MAC 外置包缓存(如 SDRAM，SSRAM，TCAM)之间的通道是否正常，同时测试 MAC 外置包缓存是否正常。

主要应用场景举例：在实际使用设备过程中，可能出现数据包无法正常转发现象，这种情况下可以利用此功能初步检测是否 PCI 总线对 MAC 芯片读写存在故障及对于存在外扩存储器的 MAC 芯片其对外扩存储器的读写访问是否正常。

> 对于不带外扩存储器的 MAC 芯片自检测试不会影响设备的正常运行，但如果 MAC 芯片带有外扩存储器，则此测试会导致数据包无法正常转发。

CPLD 自检测试(TestCpld)

主要测试 CPU 与 CPLD 之间的通道是否正常，即测试 CPU 是否能正常访问 CPLD。如果测试失败，说明 CPU 与 CPLD 间通道异常，可能导致 CPU 与 CPLD 间无法正常交互，以致 CPLD 的功能无法正常实现，如指示灯显示异常等故障。

主要应用场景举例：在实际使用设备过程中，如果发现设备指示灯异常，设备无法正常重启等现象，可以利用此功能初步定位 CPLD 是否存在故障。

> 由于在对 CPLD 进行测试时，会对 CPLD 的寄存器进行读写操作，所以可能导致 CPLD 功能异常。

PCI/PCIE 总线自检测试(TestPCI)

用于检测 PCI 和 PCIE 总线上的故障。PCI/PCIE 总线自检测试失败，可能导致挂接在 PCI/PCIE 总线上的器件信息无法读取，带外、带内数据通道异常等。

主要应用场景举例：在实际使用设备过程中，如果出现总线扫描不到设备，总线奇偶检验错误、PCIE 没有办法 Link 等现象，可以利用此功能初步定位 PCI/PCIE 总线是否存在故障。

串行 flash 检测(TestNandFlash)

主要用于检测串行 flash 是否存在故障。flash 故障检测包含两个方面内容：一是 flash 数据线和地址线的检测；二是 flash 内部存储空间的扫描测试。一般在测试 flash 时会先进行数据线与地址线的测试。由于 flash 内部存储空间测试通常需要花费很长时间，目前实现不支持 flash 全部空间的扫描测试。

并行 flash 检测(TestNorFlash)

主要用于检测并行 flash 是否存在故障。

> 在执行并行 flash 测试时，不允许设备掉电，如果设备掉电，可能导致并行 flash 中保存的信息丢失。

I2C 自检测试(TestI2C)

用于检测 I2C 总线上的故障。I2C 如果测试失败，可能导致挂接在 I2C 上的器件信息无法正常读取，比如温度，光模块信息等无法正常读取。

主要应用场景举例：在实际使用设备过程中，如果出现温度无法读取，光模块信息无法获取，监控模块的信息无法获取等现象，可以利用此功能初步定位 I2C 总线是否存在故障。

> 对于 BOX 设备的 I2C 测试，在利用命令行进行检测时需要先确认扩展插槽上是否插有扩展模块（不包括堆叠模块），如果插槽上没有插扩展模块，测试将失败。

内存测试(TestDdr)

用于检测内存数据线及地址线、内存内部空间读写是否存在故障。

主要应用场景举例：设备无法启动或设备无故异常重启，需要排除是否由于内存硬件故障导致。

> 由于内存测试需要重启设备，故内存测试只能进行单独的 CLI 测试，如果将内存测试设置为计划测试或者与其余测试项一起进行 CLI 测试，内存测试将被略过，此时可以通过命令 `show diagnostic event` 查看。而且内存测试是在 BOOT 中执行的，在进行内存测试前需确认 BOOT 版本是否支持内存测试。如果 BOOT 版本不支持内存测试，该功能将失效，请将 BOOT 版本升级到支持内存测试的版本，而如果 BOOT 为双 BOOT，当内存测试重启时如果设备从从 BOOT 启动，也不进行内存测试。

```
Diagnostic events <storage for 500 events, 27 events recorded>
Event Type (ET): I - Info, W - Warning, E - Error
Time Stamp           ET  Slot  Event Message
-------------------  --  ----  --------------------------
2010-08-27 09:03:24  I   1/0   Diagnostic Pass
2010-08-27 09:49:02  I   1/0   PortLoopbackTest Pass
2010-08-27 09:49:02  I   1/0   MacSelfTest Pass
2010-08-27 09:49:02  E   1/0   TestCpld Fail
2010-08-27 09:49:02  I   1/0   TestNandFlash Pass
2010-08-27 09:49:04  I   1/0   TestNorFlash Pass
2010-08-27 09:49:04  I   1/0   TestI2C Pass
2010-08-27 09:49:04  I   1/0   TestPCI Pass
2010-08-27 09:49:04  I   1/0   TestDdr Escape
```

4.1.5 检测结果处理

GRTD 提供命令行查询所有测试项的检测结果。检测结果有以下三种处理方式：

- 如果测试项测试失败，产生 SYSLOG 消息。主要用于监控测试，可以配置是否需要产生该消息。
- 产生测试事件，总测试事件条数可配置。测试事件有三种类型：
  info：测试信息，通常为测试通过。

warning：警告信息，测试执行超时及监控测试错误时产生警告信息。

error：出错信息，除了监控测试项外的其余检测项测试错误时产生错误信息。

目前所有检测项都是针对硬件进行的检测，一旦检测到故障，说明某硬件组件存在问题，详细维修手段请咨询锐捷技术支持工程师。

- 检测项结果与 SEM 的联动

  severity-major 级别：目前支持的测试项检测到错误都为 severity-major 级别。

  severity-minor 级别：目前版本测试项暂无此错误级别。

  severity-normal 级别：目前版本测试项暂无此错误级别。

4.2 配置GRTD

本节命令中，仅在 VSU 系统下支持 slot 参数。

功能特性	缺省值
GRTD 启动自检测试等级	minimal: 最小限度自检测试
GRTD 计划测试时间配置	无
GRTD 监控测试激活配置	根据测试项不同默认值不同，目前 ping 测试为默认激活。
GRTD 监控时间间隔配置	根据测试项不同默认值不同，目前 ping 测试默认间隔为 30 秒。
GRTD 监控测试 SYSLOG 配置	默认监控测试失败产生 SYSLOG。
GRTD 监控测试失败持续次数配置	默认为 10 次
诊断事件记录条数	默认为 500 条

4.2.1 配置GRTD启动自检测试等级

GRTD 启动自检测试等级默认为 minimal，可以配置为 complete、minimal 及 bypass，complete 为执行最大限度的启动自检测试，minimal 为执行最小限度的启动自检测试，bypass 为不执行启动自检测试。配置步骤如下：

命令	作用
Ruijie# **configure terminal**	进入全局模式
Ruijie(config)# **diagnostic bootup level { complete | minimal | bypass }**	配置启动自检测试等级

如果要恢复 GRTD 默认启动自检测试等级，在全局模式下使用 **no diagnostic bootup level** 命令进行设置。

例：配置 GRTD 启动自检测试为最大限度自检测试。

```
Ruijie#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#diagnostic bootup level complete
```

配置完后可以通过命令 **show diagnostid bootup level** 命令查看配置结果，这个配置对系统上所有设备都起作用，且当前配置只能在系统下次复位启动时生效。由于该配置会被写进系统环境变量，因此在配置文件丢失情况下其默认值为环境变量中记录的值（并不是 minimal）

```
Ruijie#show diagnostic bootup level
Current bootup diagnostic level: complete
```

4.2.2 配置GRTD命令行测试

命令行诊断指利用 CLI 执行某个或某些测试项，由于部分测试项执行后会影响其它测试项的执行结果，故命令行检测需要注意测试项测试顺序问题，比如必须在存储器测试前进行通道测试。

命令行测试必须严格遵循如下测试顺序：

1) 先执行不影响系统正常运行的测试项，可以通过命令 **show diagnostic content** 获取测试项的属性。

2) 执行端口环回测试、通道测试等这一类测试，这一类测试项属于影响系统正常运行的测试项，但不会对其后续的测试项测试结果产生影响。

3) 执行 PCI/PCIE 等总线测试、CPLD 测试、MAC 自检测试等。

4) 最后执行详尽的存储器测试。

执行详尽存储器测试后，需要复位对应的设备。不能在没有进行复位操作后直接进行其余测试项的测试。

命令	作用
Ruijie# **diagnostic start** [**slot** *slot_id* [**sub_sysytem** *subsys_id*]] **test** { **all** | **range** *test_range* | *test_id* }	开始测试
Ruijie# **diagnostic stop** [**slot** slot_id [**sub_sysytem** *subsys_id*]]	结束测试
Ruijie# **show diagnostic result** [**slot** *slot_id* [**sub_sysytem** *subsys_id*]] [**test** { **all** | **range** *test_range* | *test_id* }]	查询测试结果

例：VSU 系统下，对设备 1 执行命令行测试

```
Ruijie# diagnostic start slot 1 test range 4,5  //开始测试
Ruijie# diagnostic stop slot 1  //结束测试
Ruijie# show diagnostic result slot 1 test all  //查询测试结果
Current bootup diagnostic level: complete
Overall Diagnostic Result for Module 1: PASS
Test result: (P = Pass, F = Fail, U = Untested)
Switch#sho dia re sl 1/0 t a
Current bootup diagnostic level: minimal
Overall Diagnostic Result for Module: PASS
Test result: (P = Pass, F = Fail, U = Untested)
 1) PortLoopbackTest(loop mode: Mac):
    slot 0 port    1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
                   P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P
                  26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48
                   P  P  P  P  P  P  P  P  P  P  P  P  P  P  U  P  P  P  P  U  U  U  U
 2) MacSelfTest----------------------------------------> U
 3) TestCpld-------------------------------------------> U
```

```
4) TestNandFlash----------------------------------> U
5) TestNorFlash-----------------------------------> U
6) TestI2C----------------------------------------> U
7) TestPCI----------------------------------------> U
8) TestDdr----------------------------------------> U
```

4.2.3 配置GRTD计划测试

可以为测试项设置某一特定时间点、每天的某一特定时间点或每周某一天的某一特定时间点进行测试。配置步骤如下：

命令	作用
Ruijie# **configure terminal**	进入全局模式
Ruijie(config)# **diagnostic schedule** [**slot** *slot_id* [**sub_sysytem** *subsys_id*]] **test** { **all** | **range** *test_range* | *test_id* } { **daily** *hh:mm* | **on year** *month day_of_month hh:mm* | **weekly** *day_of_week hh:mm* }	配置计划测试时间。

如果需要删除已经配置的测试计划时间，在全局模式下使用 **no diagnostic schedule** 命令进行设置。

例：VSU 系统下，对设备 1 所有测试项配置在每天的 12:00 进行测试。

```
Ruijie#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#diagnostic schedule slot 1/0 test all daily 12:00
Scheduling test(s) [1 2 3 6 ] may disrupt normal system operation
```

配置完后可以利用 **show diagnostic schedule** 命令显示设置结果

```
Ruijie#*May  4 18:04:57: %SYS-5-CONFIG_I: Configured from console by console
Ruijie#show diagnostic schedule slot 1/0
Schedule #1:
    To be run on daily 12:0
    Test ID(s) to be executed : 1 2 3 4 5 6
```

删除测试项 1、2 在每天 12:00 的测试计划

```
Ruijie#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#no diagnostic schedule slot 1/0 test range 1,2 daily 12:00
```

显示设置结果

```
Ruijie#*May  4 18:04:57: %SYS-5-CONFIG_I: Configured from console by console
Ruijie#show diagnostic schedule slot 1/0
Schedule #1:
    To be run on daily 12:0
    Test ID(s) to be executed : 3 4 5 6
```

一旦已经配置了某一时间点的测试计划，就不能再配置同一时间点其它方式的测试计划，如:

```
Ruijie#show diagnostic schedule slot 1/0
Schedule #1:
To be run on daily 12:00
Test ID(s) to be executed : 3 4 5 6
Ruijie#
Ruijie#configure terminal
Ruijie(config)# diagnostic schedule slot 1/0 test all on 2010 5 20 12:00
Schedule time (12:00) is conflict
Ruijie(config)#
```

4.2.4 激活GRTD监控测试

对于某一监控测试项，可以激活或禁止其监控测试状态。

命令	作用
Ruijie# **configure terminal**	进入全局模式
Ruijie(config)# **diagnostic monitor active**	激活监控测试
Ruijie(config)# **diagnostic monitor active** [**slot** *slot_id* [**sub_sysytem** *subsys_id*]] **test** { **all** | **range** *test_range* | *test_id* }	激活某些监控测试项

如果需要禁止某些测试项的监控测试，在全局模式下使用 **no diagnostic monitor active** 命令进行设置。

例：VSU 系统下，激活设备 1 所有测试项的监控测试。

```
Ruijie#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#diagnostic monitor active slot 1 test all
The test[1] can not be used as health monitoring test
The test[2] can not be used as health monitoring test
The test[3] can not be used as health monitoring test
The test[6] can not be used as health monitoring test
```

测试项能否作为监控测试项，可以通过 **show diagnostic content** 命令查询。比如执行 **show diagnostic content** 命令的显示结果如下：

```
OutbandSelfTest--------> M**D*********  not config     NA
InbandSelfTest---------> C**D*********  not config     NA
InBandChannelTest------> ***N*********  0    00:00:10   10
```

只要测试项带有属性 D，则表示该测试项为影响系统正常运行的测试项，不能作为监控测试项。而如果测试项其中一个属性为 N，则表示该测试项可以作为监控测试项。

4.2.5 配置GRTD监控测试时间间隔

配置监控测试时间间隔需要执行如下命令：

命令	作用
Ruijie# **configure terminal**	进入全局模式
Ruijie(config)# **diagnostic monitor interval**	进入设置监控测试时间间隔
Ruijie(config)# **diagnostic monitor interval** [**slot** *slot_id* [**sub_sysytem** *subsys_id*]] **test** { **all** | **range** *test_range* | *test_id* } *hh:mm:ss* ***day*** *day_count*	设置监控测试时间间隔

对于有默认监控时间间隔的测试项，如果需要恢复默认的监控间隔，可以在全局模式下使用 **no diagnostic monitor interval** 进行设置。

例：VSU 系统下，为设备 1 所有测试项设置监控测试时间间隔为 10 秒。

```
Ruijie#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#diagnostic monitor interval slot 1 test all 00:00:10 day 0
The test[1] can not be used as health monitoring test
The test[2] can not be used as health monitoring test
The test[3] can not be used as health monitoring test
The test[6] can not be used as health monitoring test
```

监控测试的监控时间间隔最小单位为秒，但可以设置监控间隔为 0，当监控测试项的监控间隔为 0 时，该测试项将无法进行监控测试。

4.2.6 配置GRTD监控测试最大持续失败次数

监控测试最大持续失败次数是指当某监控测试项测试失败次数达到这个最大值后，将不再进行监控测试。

命令	作用
Ruijie# **configure terminal**	进入全局模式
Ruijie(config)# **diagnostic monitor threshold**	进入设置监控测试最大持续测试失败次数
Ruijie(config)# **diagnostic monitor threshold** [**slot** *slot_id* [**sub_sysytem** *subsys_id*]] **test** { **all** | **range** *test_range* | *test_id* } **failure-count** *threshold_value*	设置监控测试最大持续测试失败次数

对于有默认监控测试最大持续测试失败次数的测试项，如果需要恢复默认的最大持续测试失败次数，可以在全局模式下使用 **no diagnostic monitor threshold** 进行设置。

例：VSU 系统下，为设备 1 所有测试项设置监控测试最大持续测试失败次数为 6 次。

```
Ruijie#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#diagnostic monitor threshold slot 1 test all failure-count 6
The test[1] can not be used as health monitoring test
```

```
The test[2] can not be used as health monitoring test
The test[3] can not be used as health monitoring test
The test[6] can not be used as health monitoring test
```

监控测试最大持续测试失败次数最小为 1，最大为 99。

4.2.7 配置GRTD监控测试SYSLOG

指当监控测试失败时是否产生 SYSLOG 信息。

命令	作用
Ruijie# **configure terminal**	进入全局模式
Ruijie(config)#**diagnostic monitor syslog**	设置监控测试失败时产生 SYSLOG 消息。

当需要取消该 SYSLOG 消息时，在全局模式下使用 **no diagnostic monitor syslog** 命令进行取消。

4.2.8 配置GRTD诊断事件记录条数

配置诊断事件记录条数。

命令	作用
Ruijie# **configure terminal**	进入全局模式
Ruijie(config)# **diagnostic event-log size** *size_value*	配置诊断记录条数，范围 1 到 1000。

当需要恢复默认诊断事件记录条数时，在全局模式下使用 **no diagnostic event-log size** 命令完成。

4.3 配置举例

4.3.1 启动自检测试等级举例

配置要点

配置后系统上所有启动自检测试等级都为配置的值。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# diagnostic bootup level complete
```

显示验证

```
Ruijie# show diagnostic bootup level
Current bootup diagnostic level: complete
```

4.3.2 配置监控测试举例

配置要点

如果需要开始某项监控测试，需先配置好该监控测试项的监控测试时间间隔和最大监控测试持续失败次数后激活该监控测试项。只有不影响系统正常运行的测试项能作为监控测试项。

1) VSU 系统下，显示设备 1 所有测试项信息，用以确认哪些测试项为不影响系统正常运行的测试项。

```
Ruijie# show diagnostic content slot 1
======================================================================
*Diagnostic test suite attributes:
M/C*/-Minimal bootup level test / Complete bootup level test / NA
P/V*/-Per port test / Per device test / NA
D/N*/-Disruptive test / Non-disruptive test / NA
  X*/-Not a health monitoring test / NA
  F*/-Fixed monitoring interval test / NA
  E*/-Always enabled monitoring test / NA
A/I*/-Monitoring in active / Monitoring in inactive / NA
Y/O*/-Key test / Non-key test / NA
  B*/-Basic ondemand test / NA
  R*/-Power-down line cards and need reload mainbord / NA
  K*/-Require resetting the line card after the test completed / NA
======================================================================
                                          test interval  Thre-
ID   Test Name                      Attributes  day hh:mm:ss   shold
===  ============================== ==========  ============   ====
 1)  InBandChannelTest------------>  **N*F*I****  0   00:00:30   10
 2)  OutBandChannelTest----------->  **N*F*I****  0   00:00:30   10
 3)  OutbandSelfTest-------------->  **DX*******  not config     N/A
 4)  InbandSelfTest--------------->  **DX*******  not config     N/A
 5)  MacSelfTest------------------>  C*DX*******  not config     N/A
 6)  TestCpld--------------------->  C*DX*******  not config     N/A
 7)  TestNandFlash---------------->  **DX*******  not config     N/A
 8)  TestNorFlash----------------->  **DX*******  not config     N/A
 9)  TestI2C---------------------->  C*DX*******  not config     N/A
10)  TestPCI---------------------->  C*DX*******  not config     N/A
11)  TestDdr---------------------->  **DX****B**  not config     N/A
```

2) 1 和 2 测试项为不影响系统正常运行的测试项，为 1、2 项设置监控测试时间间隔及最大持续失败次数（如果想更方便的操作，也可以为所有测试项设置监控测试时间间隔及最大持续失败次数，如果是影响系统运行的测试项，会提示这些测试项不能作为监控测试，当然也不会进行相应的设置）。

```
Ruijie(config)# diagnostic monitor interval slot 1 test range 1,2 00:00:20 day 0
The test[1] is used as fixed interval test
```

```
The test[2] is used as fixed interval test
Ruijie(config)# diagnostic monitor threshold slot 1 test range 1,2 failure-count 6
Ruijie(config)# diagnostic monitor active slot 1 test range 1,2
```

3) 配置监控测试失败时产生 SYSLOG。

```
Ruijie(config)# diagnostic monitor syslog
```

显示验证

```
Ruijie# show diagnostic content slot 1
**************************************************************************
*Diagnostic test suite attributes:
M/C*/-Minimal bootup level test / Complete bootup level test / NA
P/V*/-Per port test / Per device test / NA
D/N*/-Disruptive test / Non-disruptive test / NA
  X*/-Not a health monitoring test / NA
  F*/-Fixed monitoring interval test / NA
  E*/-Always enabled monitoring test / NA
A/I*/-Monitoring in active / Monitoring in inactive / NA
Y/O*/-Key test / Non-key test / NA
  B*/-Basic ondemand test / NA
  R*/-Power-down line cards and need reload mainbord / NA
  K*/-Require resetting the line card after the test completed / NA
**************************************************************************
                                          test interval  Thre-
ID   Test Name                      Attributes  day hh:mm:ss   shold
===  ============================== ==========  ============   ====
 1)  InBandChannelTest------------>  **N*F*I****  0   00:00:30   6
 2)  OutBandChannelTest----------->  **N*F*I****  0   00:00:30   6
 3)  OutbandSelfTest-------------->  **DX*******  not config     N/A
 4)  InbandSelfTest--------------->  **DX*******  not config     N/A
 5)  MacSelfTest------------------->  C*DX*******  not config     N/A
 6)  TestCpld---------------------->  C*DX*******  not config     N/A
 7)  TestNandFlash----------------->  **DX*******  not config     N/A
 8)  TestNorFlash------------------>  **DX*******  not config     N/A
 9)  TestI2C----------------------->  C*DX*******  not config     N/A
10)  TestPCI----------------------->  C*DX*******  not config     N/A
11)  TestDdr----------------------->  **DX****B**  not config     N/A
```

4.3.3 命令行测试举例

测试要点

需严格按照如下顺序进行命令行测试：

1) 进行命令行测试前先禁止所有后台监控测试及删除所有计划测试。

2) 先执行不影响系统正常运行的测试项，可以通过命令 **show diagnostic content** 获取所有测试项的属性。

3) 执行端口环回测试、通道测试等这一类测试，这一类测试项属于影响系统正常运行的测试项，但不会对其后续的测试项测试结果产生影响。

4) 执行 PCI/PCIE 等总线测试、CPLD 测试、MAC 自检测试等。

5) 最后执行详尽的存储器测试。

```
Ruijie# show diagnostic content
******************************************************************
*Diagnostic test suite attributes:
M/C*/-Minimal bootup level test / Complete bootup level test / NA
P/V*/-Per port test / Per device test / NA
D/N*/-Disruptive test / Non-disruptive test / NA
  X*/-Not a health monitoring test / NA
  F*/-Fixed monitoring interval test / NA
  E*/-Always enabled monitoring test / NA
A/I*/-Monitoring in active / Monitoring in inactive / NA
Y/O*/-Key test / Non-key test / NA
  B*/-Basic ondemand test / NA
  R*/-Power-down line cards and need reload mainbord / NA
  K*/-Require resetting the line card after the test completed / NA
******************************************************************
                                            test interval  Thre-
ID   Test Name                      Attributes  day hh:mm:ss   shold
===  ============================== ==========  ============   ====
 1)  PortLoopbackTest-------------->  MPDX*******  not config     N/A
 2)  MacSelfTest------------------->  C*DX*******  not config     N/A
 3)  TestNandFlash----------------->  **DX*******  not config     N/A
 4)  TestNorFlash------------------>  **DX*******  not config     N/A
 5)  TestI2C----------------------->  C*DX*******  not config     N/A
 6)  TestPCI----------------------->  C*DX*******  not config     N/A
 7)  TestDdr----------------------->  **DX****B**  not config     N/A
```

先测试不影响系统正常运行的测试项

```
Ruijie# diagnostic start test all
Running test[7] may reload system
Running test(s) [1 2 3 4 5 6] may disrupt normal system operation
Do you want to continue? [no]:y
Ruijie# *Oct  8 12:53:34: %GRTD-6-TEST_RUNNING: Running PortLoopbackTest{ID=1}...
*Oct  8 12:53:35: %GRTD-6-TEST_OK:  PortLoopbackTest{ID=1} completed successfully.
*Oct  8 12:53:35: %GRTD-6-TEST_RUNNING: Running MacSelfTest{ID=2}...
```

```
*Oct  8 12:53:35: %GRTD-6-TEST_OK:  MacSelfTest{ID=2} completed successfully.
*Oct  8 12:53:35: %GRTD-6-TEST_RUNNING: Running TestNandFlash{ID=3}...
*Oct  8 12:53:35: %GRTD-6-TEST_OK:  TestNandFlash{ID=3} completed successfully.
*Oct  8 12:53:35: %GRTD-6-TEST_RUNNING: Running TestNorFlash{ID=4}...
*Oct  8 12:53:38: %GRTD-6-TEST_OK:  TestNorFlash{ID=4} completed successfully.
*Oct  8 12:53:38: %GRTD-6-TEST_RUNNING: Running TestI2C{ID=5}...
*Oct  8 12:53:38: %GRTD-3-TEST_ERR:  TestI2C{ID=5} completed error.
*Oct  8 12:53:38: %GRTD-6-TEST_RUNNING: Running TestPCI{ID=6}...
*Oct  8 12:53:38: %GRTD-6-TEST_OK:  TestPCI{ID=6} completed successfully.
*Oct  8 12:53:38: %GRTD-5-TEST_ESCAPE: Ddr test should be done alone.
```

显示验证

```
Ruijie# show diagnostic result test all
Current bootup diagnostic level: complete
Overall Diagnostic Result for Module: FAIL
Test result: (P = Pass, F = Fail, U = Untested)
 1) PortLoopbackTest(loop mode: Mac):
    slot 0 port    1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
                   P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P
                  25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48
                   P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P  P
 2) MacSelfTest----------------------------------------> P
 3) TestNandFlash--------------------------------------> P
 4) TestNorFlash---------------------------------------> P
 5) TestI2C--------------------------------------------> F
 6) TestPCI--------------------------------------------> P
 7) TestDdr--------------------------------------------> U
```

对于较为耗时的检测，可以下命令 **show diagnostic status** 查看当前系统的检测状态。如:

4.3.4 配置计划测试时间表举例

配置要点

一旦已经配置了某一时间点的测试计划，就不能再配置同一时间点其它方式的测试计划，因此需要注意测试计划时间是否冲突。如果是某一特定时间点的计划测试，还需要确认年月日是合法的。

- VSU 系统下，设备 1 所有测试项配置每天 12:00 进行计划测试。

```
Ruijie(config)# diagnostic schedule slot 1 test all daily 12:00
Scheduling test(s) [1 2 3 6] may disrupt normal system operation
Ruijie(config)#
```

- VSU 系统下，设备 1 所有测试项配置每周星期三 3:00 进行计划测试。

```
Ruijie(config)# diagnostic schedule slot 1 test all weekly  Wednesday 3:00
Scheduling test(s) [1 2 3 6] may disrupt normal system operation
```

- VSU 系统下，设备 1 所有测试项配置在 2010 年 8 月 1 号 00:00 进行计划测试

```
Ruijie(config)# diagnostic schedule slot 1 test all on 2010  August 1 00:00
Scheduling test(s) [1 2 3 6] may disrupt normal system operation
```

显示验证

```
Ruijie# show diagnostic schedule slot 1
Diagnostic for 1:
Schedule #1:
    To be run on daily 12:00
    Test ID(s) to be executed : 1 2 3 4 5 6
Schedule #2:
    To be run on August 1 2010 00:00
    Test ID(s) to be executed : 1 2 3 4 5 6
Schedule #3:
    To be run on Wednesday 03:00
    Test ID(s) to be executed : 1 2 3 4 5 6
```

5 SEM

5.1 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。

5.1.1 基本概念

事件

用户关心的事件，由用户配置，附属于策略，可以是一个也可以是多个。每种事件都由特定的检测器负责检测。当事件条件符合时，由事件检测器触发事件。比如，用户需要检测到特权模式下包含 **shutdown** 的命令，需要使用命令 **event tag** *example* **cli pattern** *shutdown* **mode** *exec* 配置事件给命令行事件检测器。

行动

用户在事件发生以后所要采取的行动，由用户配置，附属于策略，可以是一个也可以是多个。每种行动都对应不同的行动配置。当策略的事件发生以后，策略依次运行行动。比如，用户在某事件发生以后，需要重新启动设备，需要使用命令 **action** *example* **reload**。

策略

组织事件与事件、事件与行动的关系。需要在配置好以后提交策略配置，当策略的事件符合预定规则时触发策略，并依次运行策略的行动。

事件检测器

嵌入到具体的业务中，按照用户的配置监控业务，并在业务运行至符合用户配置的时候触发事件。将事件消息通知给智能管理服务器。

智能管理服务器

接收事件检测器的事件通知，并根据事件发生情况判断是否触发策略运行。一旦策略被触发，由智能管理服务器运行策略管理中的策略。

策略管理器

管理 SEM 的策略信息，并在策略被智能管理服务器触发以后，运行策略中的行动。

SEM 环境变量

在 SEM 运行过程中被策略行动所使用的变量。SEM 中环境变量有三种：

- 全局变量
- 系统局部变量
- 用户局部变量

在策略中使用变量时，“$”符号往后直到第一个不是字母、数字或下划线的字符之间的单词符号作为要被置换的变量的名字。全局变量可以在所有策略中使用。系统局部变量和用户局部变量都是局部变量，只能在具体的策略中使用，系统局部变量是只读类型，不可以被改写。用户局部变量在策略运行过程中被策略中的行动定义。所以系统局部变量一般以“_”开头，防止与用户局部变量冲突。

SEM 特定应用事件

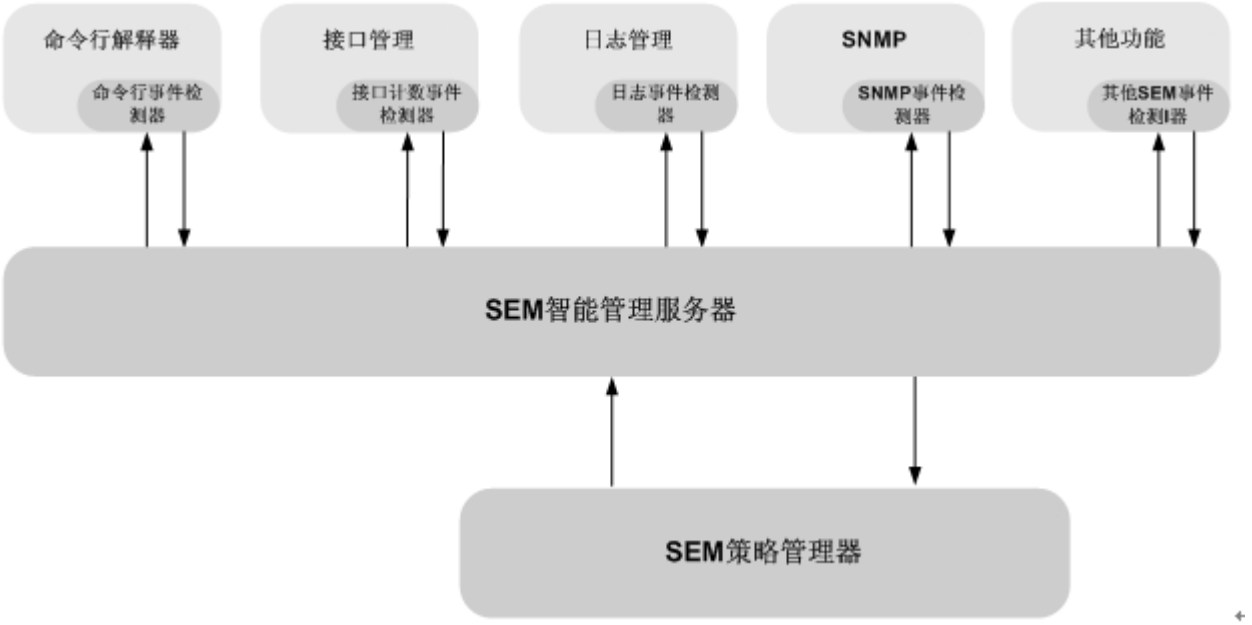
SEM 支持 SEM 系统内部使用特定应用事件，用于执行中的策略触发其他策略运行。为了方便区别不同的特定应用事件，使用子集和类型作为事件的标示。SEM 特定应用事件由特定应用事件检测器按照子集和类型进行检测，由策略运行中的特定应用事件行动项发布特定应用事件。当有策略行动发布了某子集和类型的特定应用事件时，正在检测的对应的子集和类型的事件被触发。举例见《SEM 典型配置举例章》中《SEM 检测特定应用事件》节。

SEM 命名计数器

SEM 支持一种 SEM 系统内部使用的命名计数器，由 SEM 计数事件检测器检测 SEM 命名计数器的变化，由策略运行中的 SEM 计数器行动项操作 SEM 命名计数器的值。SEM 命名计数器可以用于策略触发累计，数值统计等多种情况。举例见《SEM 典型配置举例章》中《SEM 检测计数器》节。

5.1.2 工作原理

图 9-1 SEM 结构图



SEM 提供了各种不同的事件检测器，这些事件检测器被嵌入到各种不同的业务中，实时的监控业务运行。检测器根据用户配置产生事件的条件与业务运行事件进行匹配，一旦匹配则事件检测器通知智能管理服务器事件发生。

智能管理服务器根据策略中的事件配置判断事件是否可以触发策略运行，当事件发生达到策略触发条件时，智能管理服务器运行策略管理器中的策略。

策略管理器中的策略按照用户的配置被依次运行预定的行动。

5.1.3 SEM支持的事件检测器

SEM 支持丰富的事件检测器，各种事件检测器嵌入到各个业务中。在业务运行过程中进行检测，决定事件是否发生。目前支持的检测器类型如下：

命令行事件检测器

命令行事件检测器检测用户的命令行输入。进行检测的用户命令行必须为通过命令行格式检查。将用户输入的命令的扩展形式进行正则匹配。一旦匹配通过，则触发命令行事件。命令行事件触发时支持两种等待模式：

- 同步模式：命令行事件被触发以后，命令行进入同步等待，等待策略运行结束。策略执行结束以后，由策略的执行结果决定用户输入的命令是否执行。
- 异步模式：命令行事件被触发后，不必等待策略运行结束。该模式下支持忽略命令执行的配置。当配置忽略时，命令行在触发完命令行事件以后，忽略对命令的执行。

计数事件检测器

计数事件检测器检测 SEM 内部的命名计数器，当命令计数器超过指定的阈值时触发计数器事件。当计数器事件被触发以后，该计数器事件检测将暂时失效，直到计数器达到其恢复阈值时其检测功能才可恢复。命名计数器的值由运行中的计数器行动改变，因此可以由其他策略将计数器的数值累加，当达到阈值后，计数器事件触发，计数器事件触发策略运行，在本策略运行过程中将计数器的值重置，以此达到循环的效果。

特定应用事件检测器

特定应用事件检测器检测 SEM 内部的特定应用事件，SEM 的内部事件由运行过程中的特定应用事件行动发布。当 SEM 发布的特定应用事件与当前特定应用事件的子集和类型相同，则特定应用事件触发。

接口计数事件检测器

接口计数事件检测器检测设备的接口统计计数。通过定期的采集和统计，判断接口的计数是否超过阈值，当接口统计超过阈值以后，接口计数事件被触发。当接口计数事件被触发以后，该接口计数事件检测将暂时失效，直到接口技术达到其恢复阈值时或者失效时间超过其恢复周期以后，其检测功能才能恢复。

空事件检测器

空事件检测器并非进行实际的检测，而是由 SEM 的 **smart manager run** 命令主动触发。该命令的参数为包含空事件的策略的名字。当该命令被执行成功以后，对应策略的空事件被触发。空事件被触发时支持两种等待模式：

- 同步模式：空事件被触发以后，命令行进入同步等待，待策略运行结束以后才能释放。
- 异步模式：空事件被触发以后直接释放，不进行等待。

热插拔事件检测器

VSU 系统支持热插拔。热插拔事件检测器检测 VSU 系统的成员热插拔，当有热插拔操作时热插拔事件触发。热插拔事件检测器支持两种事件种类：

- 插入
- 拔出

SNMP 事件检测器

SNMP 事件检测器分为以下 3 种类型：

- SNMP MIB 检测器：获取并统计检测设备的 SNMP MIB 对象值，当有 SNMP MIB 对象值超过事件设定阈值以后，SNMP MIB 事件被触发。当 SNMP MIB 事件被触发以后，该 SNMP MIB 事件检测器将暂时失效，直到 SNMP MIB 对象值达到其恢复阈值或者失效事件超过了事件的恢复周期以后，其检测功能才能恢复。
- SNMP Trap 检测器：检测 SNMP Trap 信息，当有 SNMP Trap 符合事件配置时，SNMP 事件触发。
- SNMP Object 检测器： 检测 SNMP 操作，当有 SNMP 操作符合事件配置时，SNMP 事件触发。SNMP Object 检测器支持同步和异步两种等待模式。并可以与 SNMP Object 行动配合完成自定义的 SNMP 回复。

Syslog 事件检测器

Syslog 事件检测器检测设备的日志信息，对设备发生的日志信息进行正则匹配，如果日志正则匹配通过，则 Syslog 事件触发。

定时器事件检测器

定时器事件检测器检测与时间有关的事件。主要有以下 4 种类型：

- 绝对时间定时器事件：定时器时间为未来某一时刻，当该时刻到达时，定时器事件触发。
- 倒计时定时器事件：定时器时间为从策略生效起的秒数，当到达该秒数时，定时器事件触发。
- 看门狗定时器事件：定时器时间为在策略生效起每经过设定的秒数，每当这些时刻到达时，就触发定时器事件一次。
- cron 定时器事件：cron (来源于希腊单词 chronos，意为“时间”)，广泛应用于 Unix 类操作系统中，用于设置周期性被执行的指令。SEM 支持 cron 方式的时间检测，当 cron 定时器事件 cron 串所描述的时间点到达时，定时器事件触发。

看门狗系统事件检测器

看门狗系统事件检测器检测设备的系统资源。当系统或任务的资源使用超过事件设定的阈值时，看门狗系统事件触发。目前支持的系统资源检测项目有如下：

- 设备的 CPU 资源
- 任务的 CPU 资源
- 设备的内存使用
- 设备的内存剩余
- 任务的内存使用

CPP 事件检测器

CPP 事件检测器检测检测 CPP（CPU Protect）功能的统计信息，当 CPP 的统计信息超过事件设定的阈值时，CPP 事件触发。CPP 事件检测器支持各种不同类型的报文检测：ARP，DHCP，IGMP，PIM，OSPF 等等。同时支持检测报文 pps，报文总数，报文丢弃数量。

GRTD 事件检测器

GRTD 事件检测器检测 GRTD（Generic Real-Time Diagnostics，通用实时诊断）发生的诊断结果，针对硬件相关组件以及组件间通信通道进行检测。当 GRTD 检测到的故障与事件设定的事件匹配时，GRTD 事件触发。

5.1.4 SEM支持的策略行动项

SEM 支持丰富的行动类型，在事件触发策略以后运行。可以执行收集信息和纠正设备或网络的问题，SEM 目前支持的行动项类型如下：

- 执行 CLI 命令：执行用户设定的命令。
- 发送 Syslog：发生指定的日志消息。

- 操作命名计数器：操作 SEM 内部的命名计数器。
- 切换至备机：VSU 系统中进行主备倒换。
- 复位设备：将设备复位。
- 触发特定应用事件：发布 SEM 内部的特定应用事件。
- 使策略执行等待：使策略执行过程中等待一段时间。

5.1.5 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。

5.1.6 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。

5.2 配置SEM

在设备上使用 SEM 需要一定的前提，大部分前提都是因为策略行动的执行需要，如下：

- 配置 Syslog 行动项之前，需要通过 **logging** 命令打开 Syslog 功能。
- 配置 VSU 系统下切换至备机行动之前，设备需要配备正常运行的备机。

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。具体要求请参考《SEM 命令参考》。

5.2.1 创建策略

命令	作用
Ruijie# **configure terminal**	进入全局模式
Ruijie(config)# **smart manager applet** *applet-name* [**class** *class-options*]	创建策略并进入 SEM 配置模式，*applet-name* 参数制定策略的名字，class 参数指定策略的类别（默认为 default 类别）

如果要删除策略，在全局模式下使用 **no smart manager applet** *applet-name* 命令进行设置。

例：在设备上配置名为 policy_a 的策略，创建好策略以后，将进入 SEM 配置模式。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# smart manager applet policy_a
Ruijie(sem-applet)#
```

新创建和正在被修改的策略不会立即生效，需要在配置好事件和行动以后，由 **commit** 命令提交才能正式生效，未提交的策略配置可以通过 **rollback** 命令回退。

一个完整的策略包括事件和行动，如果策略没有配置事件，则提交过程中将会导致错误，提交不成功。如果策略没有配置行动，提交会成功，但是会给与提示，一旦策略被触发运行，则什么都不做，直接结束。

5.2.2 配置事件

命令	作用
Ruijie# **configure terminal**	进入全局模式
Ruijie(config)# **smart manager applet** *applet-name* [**class** *class-options*]	进入 SEM 配置模式，*applet-name* 参数制定策略的名字，class 参数指定策略的类别（默认为 default 类别）
Ruijie(sem-applet)# **event tag event-name** [**correlate** { **andnot | and | or** }] **syslog pattern** *regular-expression* [**priority** *priority-level*] [**occurs** *num-occurrences*] [**period** *period-value*] [**skip** { **yes | no** }]	每种事件检测都对应一个 event 命令，此处以 syslog 事件为例，介绍配置事件的方法。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 event tag** *event-name* 命令进行设置。

例：为名为 policy_a 的策略配置名为 event_a 的 syslog 事件，检测内容包含“shutdown”的日志

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# smart manager applet policy_a
Ruijie(sem-applet)# event tag event_a syslog pattern "shutdown"
```

如果不配置事件就提交策略配置，则策略不会被注册，依然处于编辑状态。

一个策略中可以配置多个事件，事件的顺序按照策略的 tag 参数字符排序进行排列。

5.2.3 配置行动

命令	作用
Ruijie# **configure terminal**	进入全局模式
Ruijie(config)# **smart manager applet** *applet-name* [**class** *class-options*]	进入 SEM 配置模式，*applet-name* 参数制定策略的名字，class 参数指定策略的类别（默认为 default 类别）
Ruijie(sem-applet)# **action** *label* **syslog** [**priority** *priority-level*] **msg** *msg-text* **facility** *string*	每种行动都对应一个 action 命令，此处以 syslog 行动为例，介绍配置行动的方法。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"
```

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。

5.2.4 配置描述

命令	作用
Ruijie# **configure terminal**	进入全局模式
Ruijie(config)# **smart manager applet** *applet-name* [**class** *class-options*]	进入 SEM 配置模式，*applet-name* 参数制定策略的名字，class 参数指定策略的类别（默认为 default 类别）
Ruijie(sem-applet)# **description** *string*	设置描述信息

如果要删除策略描述信息，在 SEM 配置模式下使用 no **description** 命令进行设置。

例：为名为 policy_a 的策略配置描述信息，信息内容为“policy_for_test”。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# smart manager applet policy_a
Ruijie(sem-applet)# description "policy_for_test"
```

对描述信息的修改将立即生效，无须提交。

5.2.5 配置触发参数

命令	作用
Ruijie# **configure terminal**	进入全局模式
Ruijie(config)# **smart manager applet** *applet-name* [**class** *class-options*]	进入 SEM 配置模式，*applet-name* 参数制定策略的名字，class 参数指定策略的类别（默认为 default 类别）
Ruijie(sem-applet)# **trigger** [**occurs-value** *occurs-value*] [**occurs-period** *occurs-period-value*] [**correlate-start** *period-start-value*] [**correlate-period** *correlate-period-value*] [**delay** *delay-value*] [**maxrun** *maxruntime-number*]	设置策略触发参数

如果要恢复策略触发参数为默认，在 SEM 配置模式下使用 **no trigger** 命令进行设置。

例：为名为 policy_a 的策略配置触发参数，配置其触发以后延迟 5 秒运行，策略最大运行事件为 15 秒。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# smart manager applet policy_a
Ruijie(sem-applet)# trigger delay 5 maxrun 15
```

5.2.6 配置CLI行动项输出记录

命令	作用
Ruijie# **configure terminal**	进入全局模式
Ruijie(config)# **smart manager applet** *applet-name* [**class** *class-options*]	进入 SEM 配置模式，*applet-name* 参数制定策略的名字，class 参数指定策略的类别（默认为 default 类别）
Ruijie(sem-applet)# **policy record**	设计在 CLI 行动项运行时产生的输出记录到文件

如果要停止记录 CLI 行动项的输出记录，在 SEM 配置模式下使用 **no policy record** 命令进行设置。

例：为名为 policy_a 的策略配置 CLI 行动输出记录，单次策略运行产生的记录文件不大于 500K，policy_a 产生的所有记录文件不大于 2M。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# smart manager applet policy_a
Ruijie(sem-applet)# action action_1 cli command "enable"
Ruijie(sem-applet)# action action_2 cli command "show arp"
```

```
Ruijie(sem-applet)# policy record per-instance 500 per-policy 2000
```

5.2.7 显示当前策略配置

命令	作用
Ruijie# **configure terminal**	进入全局模式
Ruijie(config)# **smart manager applet** *applet-name* [**class** *class-options*]	进入 SEM 配置模式，*applet-name* 参数制定策略的名字，class 参数指定策略的类别（默认为 default 类别）
Ruijie(sem-applet)# **list-config**	显示当前策略配置

例：显示策略 policy_a 的策略配置。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# smart manager applet policy_a
Ruijie(sem-applet)# list-config
smart manager applet policy_a
 description "policy_for_test"
 event tag event_a syslog pattern "shutdown"
 trigger delay 5 maxrun 15
 action label syslog priority informational msg "action running"
Ruijie(sem-applet)#
```

当策略处于编辑状态而没有提交时，list-config 显示内容当前编辑中没有提交的配置，显示内容中不包含 commit 命令。当策略已经提交时，则显示提交策略的配置，显示内容中包含 commit 命令。

5.2.8 提交配置

命令	作用
Ruijie# **configure terminal**	进入全局模式
Ruijie(config)# **smart manager applet** *applet-name* [**class** *class-options*]	进入 SEM 配置模式，*applet-name* 参数制定策略的名字，class 参数指定策略的类别（默认为 default 类别）
Ruijie(sem-applet)# **commit**	提交策略配置

例：提交策略 policy_a 的策略配置。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# smart manager applet policy_a
Ruijie(sem-applet)# commit
```

提交过程中会进行策略配置合法性检查，如果检查不通过，则策略配置提交失败，策略不会被注册，依然处于编辑状态。比如策略没有配置事件，则提交检查不会通过。

可以被提交的策略分为两种：新创建的策略和被编辑的已经注册的策略。其他情况的策略，比如，已经注册的策略且没有被编辑，则不会被提交，会给出相应的提示信息。

以上两种可以提交的策略，在提交之前，如果用户希望放弃以做出的策略配置变化，通过 rollback 将策略配置回退。

5.2.9 查看注册策略

命令	作用
Ruijie# **show smart manager policy registered** [**policy** *policy-name*] [**event-type** *event-name*] [**class** *class-options*] [**time-ordered** | **name-ordered**]	显示已经注册的策略信息

例：提交策略 policy_a 的策略配置。

```
Ruijie# show smart manager policy registered
No.   Class    Event Type    Time Registered             Secu    Name
1     applet   syslog        Wed Mar 10 10:49:03 2010    none    policy_a
 event_a: syslog: pattern {shutdown}
 trigger delay 5.000
 maxrun 15.000
 action label syslog priority informational msg "action running"
```

5.2.10 回退配置

命令	作用
Ruijie# **configure terminal**	进入全局模式
Ruijie(config)# **smart manager applet** *applet-name* [**class** *class-options*]	进入 SEM 配置模式，*applet-name* 参数制定策略的名字，class 参数指定策略的类别（默认为 default 类别）
Ruijie(sem-applet)# **rollback**	回退策略配置

例：回退策略 policy_a 的策略配置。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# smart manager applet policy_a
Ruijie(sem-applet)# rollback
```

有两种情况下用户可以选择回退策略配置：新配置的策略，但尚未提交；配置了已经提交注册的策略，但尚未将变化提交。

以上两种情况用户可以通过 rollback 命令将未提交的策略配置回退掉。

5.2.11 配置多事件触发

命令	作用

Ruijie# **configure terminal**	进入全局模式
Ruijie(config)# **smart manager applet** *applet-name* [**class** *class-options*]	进入 SEM 配置模式，*applet-name* 参数制定策略的名字，class 参数指定策略的类别（默认为 default 类别）
Ruijie(sem-applet)# **event tag event-name** [**correlate** { **andnot** | **and** | **or** }] **syslog pattern** *regular-expression* [**priority** *priority-level*] [**occurs** *num-occurrences*] [**period** *period-value*] [**skip** { **yes** | **no** }]	配置首个事件
Ruijie(sem-applet)# **event tag event-name** [**correlate** { **andnot** | **and** | **or** }] **syslog pattern** *regular-expression* [**priority** *priority-level*] [**occurs** *num-occurrences*] [**period** *period-value*] [**skip** { **yes** | **no** }]	配置其他事件

例：配置策略 policy_a，并配置两个事件，首要事件检测日志中是否包含“need reload”，其他事件为是否有板卡插入。而且要求二者发生的间隔需要小于 180 秒。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# smart manager applet policy_a
Ruijie(sem-applet)# event tag event_a syslog pattern "need reload"
Ruijie(sem-applet)# event tag event_b correlate and oir type plugin "shutdown"
Ruijie(sem-applet)# trigger correlate-period 180
```

- 在配置多个事件的时候，SEM 会按照 tag 的字母排序自动为事件排序。建议对采用有排序规律的命名方法，如：01_cli ，02_timer ，03_counter ...。
- 事件之间的关系为：当前事件与其前边所有事件组合之间的关联系。只有首个事件被触发时，才检查策略是否触发。
- 除首个事件以外其他事件要配置并列关系，默认的并列关系为 and，首个事件配置的并列关系将被忽略。

5.2.12 配置和使用变量

命令	作用
Ruijie# **configure terminal**	进入全局模式
Ruijie# **smart manager environment** *variable-name string*	配置 SEM 全局变量
Ruijie(config)# **smart manager applet** *applet-name* [**class** *class-options*]	进入 SEM 配置模式，*applet-name* 参数制定策略的名字，class 参数指定策略的类别（默认为 default 类别）
Ruijie(sem-applet)# **action** *label* **set** *variable-name variable-value*	设置 SEM 局部变量
Ruijie(sem-applet)# **action** *label* **syslog** [**priority** *priority-level*] **msg** *msg-text* [**facility** *string*]	使用 SEM 变量 （多种行动中都支持使用变量，此处以 Syslog 为例，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"
```

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。

5.2.13 挂起/恢复调度器

命令	作用
Ruijie# **configure terminal**	进入全局模式
Ruijie(config)# **smart manager scheduler suspend**	将 SEM 策略调度器挂起

如果要恢复调度器运行，在全局配置模式下使用 **no smart manager scheduler suspend** 命令进行设置。

例：将 SEM 调度器挂起

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# smart manager scheduler suspend
```

将 SEM 调度器挂起仅为将调度功能挂起，已经被调度运行的线程不会因为调度器的挂起而停止运行。

5.2.14 暂停/恢复策略执行

命令	作用
Ruijie# **smart manager scheduler hold** { **all** | **policy** *job-id* | **class** *class-options* }	将执行中的策略暂停
Ruijie# **smart manager scheduler release** { **all** | **policy** *policy-id* | **class** *class-options* }	将暂停的策略恢复执行

例：将类别为 A 的的策略执行挂起

```
Ruijie# smart manager scheduler hold class a
```

例：将类别为 A 的的策略恢复执行

```
Ruijie# smart manager scheduler release class a
```

只有没有被调度器调度运行的线程可以被暂停，一旦被调度器调度运行，则无法被暂停。

暂停和恢复的参数中 class 和 all，是将指定的类别和所有类别暂停，类别的后续线程也将被暂停。而参数 policy 则只是将一个特定的类别暂停，类别中其他策略不受影响。

5.2.15 强制中止策略执行

命令	作用
Ruijie# **smart manager scheduler clear** { **all | policy** *job-id* | **class** *class-options*]	强制中止策略执行

例：强制中止策略运行 ID 为 150 的策略。

```
Ruijie# smart manager scheduler clear policy 150
```

5.2.16 显示SEM历史信息

命令	作用
Ruijie# **show smart manager history events**	显示 SEM 历史信息

例：显示 SEM 历史信息

```
Ruijie# show smart manager history events
No.   Job Id   Proc Status    Time of Event             Event Type   Name
1     1        Actv success   Tue Mar 9 00:00:00 2010   timer cron   applet: policy_a
```

5.2.17 显示SEM检测器信息

命令	作用
Ruijie# **show smart manager detector** [**all** | *detector-name*] [**detailed** | **statistics**]	显示 SEM 检测器信息

例：显示 SEM 检测器详细信息

```
Ruijie# show smart manager detector syslog detailed
No.   Name      Version
1     syslog    01.00
Applet Configuration Syntax:
event tag event-name [correlate {andnot | and | or }] syslog pattern regular-expression [occurs num-occurrences]
[period period-value] [priority priority-level]
Applet Built-in Environment Variables:
$_event_id
$_event_type
$_event_type_string
$_event_pub_time
$_event_pub_sec
$_event_pub_msec
$_syslog_msg
$_syslog_priority
```

例：显示 SEM 检测器统计信息

```
Ruijie# show smart manager detector syslog statistics
```

```
Syslog Detecotr Statistics:
Policy     Event     Detect   NoPri   PriPass   PriDeny   PatternPass   trigge
policy_a   event_a   1000     100     400       500       10            4
```

5.2.18 显示SEM版本信息

命令	作用
Ruijie# **show smart manager version**	显示 SEM 版本信息

例：显示 SEM 版本信息

```
Ruijie# show smart manager version
Smart Embedded Manager Version 1.0
Event Detectors:
name                 version
application          1.0
syslog               1.0
cli                  1.0
counter              1.0
cpp                  1.0
grtd                 1.0
interface            1.0
none                 1.0
oir                  1.0
snmp                 1.0
snmp-object          1.0
snmp-notification    1.0
sysmon               1.0
timer                1.0
```

5.3 配置举例

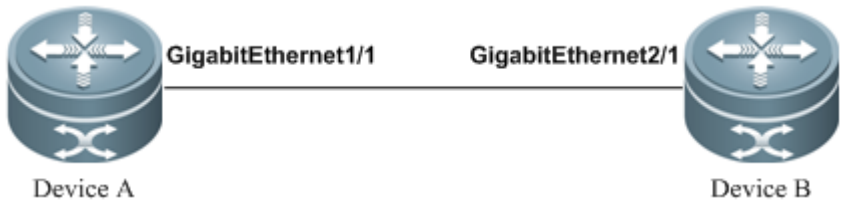
5.3.1 SEM检测接口计数

组网需求

Device A 和 Device B 直接相连，Device A 的 GigabitEthernet1/1 与 Device B 的 GigabitEthernet2/1 相连。因为线路或者 Device B 的问题，Device A 会经常突然接收到来自 Device B 的大量持续错帧，影响通信。将 Device A 的 GigabitEthernet1/1 shutdown 再恢复可以将问题修复。

组网拓扑

图 9-2 接口计数检测举例拓扑



配置要点

- 创建策略
- 配置接口事件
- 配置命令行行动
- 提交策略配置

配置步骤

配置 Device A

1) 给 Device A 配置策略取名为 policy_a。

2) 给 policy_a 配置名为 event_1 的事件，类型为 interface 类型。其具体的参数如下：
配置检测接口计数类型的参数“parameter input_errors_frame”，其含义为检测接口的输入错帧的数量；
配置被检测接口接口名字的参数“name GigabitEthernet 1/1”用于指定被检测的接口；
配置检测阈值的参数“entry-type value entry-op ge entry-val 2000”，其含义为检测计数的绝对值，当绝对值大于等于 2000 的时候为检测通过；
配置检测频率的参数“poll-interval 5”，其含义为检测接口计数的时间间隔为 5 秒钟一次；
计数检测通过以后恢复事件检测的条件参数为“exit-type value exit-op ge exit-val 2000 exit-time 60 exit-comb and”，其“exit-type value exit-op ge exit-val 2000”部分的选项与量值都与前边的检测阈值相同，即事件触发以后，量值检查立即满足恢复的条件，其“exit-time 60 exit-comb and”表示恢复时间与恢复检查为与关系，既然恢复检查在事件触发以后就立即满足，则一旦触发事件超过 60 秒，恢复的另一个条件恢复时间也得到满足，事件检测得到恢复。

3) 给 policy_a 配置多个行动，具体如下：
命令行进入 GigabitEthernet 1/1 的接口模式；
命令行将接口 shutdown；
命令行将接口 no shutdown；
命令行进入特权模式；
命令行清除接口 GigabitEthernet 1/1 的接口统计计数；

4) 保存 cli 行动项的输入命令和输出信息，通过配置 policy record 实现，缺省是不保存.

5) 将策略提交

6) 退出策略编辑

```
Ruijie# configure terminal
```

```
Ruijie(config)# smart manager applet policy_a
Ruijie(sem-applet)# event tag event_1 interface parameter input_errors_frame name GigabitEthernet 1/1 entry-type value entry-op ge entry-val 2000 poll-interval 5 exit-type value exit-op ge exit-val 2000 exit-time 60 exit-comb and
Ruijie(sem-applet)# action action_1 cli command "enable"
Ruijie(sem-applet)# action action_2 cli command "configure terminal"
Ruijie(sem-applet)# action action_3 cli command "interface GigabitEthernet 1/1"
Ruijie(sem-applet)# action action_4 cli command "shutdown"
Ruijie(sem-applet)# action action_5 cli command "no shutdown"
Ruijie(sem-applet)# action action_6 cli command "exit"
Ruijie(sem-applet)# action action_7 cli command "exit"
Ruijie(sem-applet)# action action_8 cli command "clear counters GigabitEthernet 1/1" pattern "y"
Ruijie(sem-applet)# policy record
Ruijie(sem-applet)# commit
Ruijie(sem-applet)# exit
Ruijie(config)#
```

显示验证

- 显示注册的 SEM 策略

```
Ruijie# show smart manager policy registered
No.  Class     Event Type          Time Registered           Secu   Name
1    applet    interface           Mon Mar 8 16:19:15 2010   none   policy_a
 event_1: interface: name GigabitEthernet 1/1 parameter input_errors_frame entry_op ge entry_val 2000 entry_type value exit_comb and exit_op ge exit_val 2000 exit_type value exit_time 60.000 poll_interval 5.000
 maxrun 20.000
 action action_1 cli command "enable"
 action action_2 cli command "configure terminal"
 action action_3 cli command "interface GigabitEthernet 1/1"
 action action_4 cli command "shutdown"
 action action_5 cli command "no shutdown"
 action action_6 cli command "exit"
 action action_7 cli command "exit"
 action action_8 cli command "clear counters GigabitEthernet 1/1" pattern "y"
```

- 在策略被执行之后，查看 CLI 行动输出记录

```
Ruijie# more /sem_record/policy_a/2010-05-08_16-21-15_1001.txt
                        SEM CLI RECORD FILE
SEM policy name: policy_a
SEM policy trigger id :1
SEM policy cli record time : Mon Mar 8 16:21:15 2010
================================================
Ruijie#enable
```

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#interface GigabitEthernet 1/1
Ruijie(config-GigabitEthernet 1/1)#shutdown
Ruijie(config-GigabitEthernet 1/1)#no shutdown
Ruijie(config-GigabitEthernet 1/1)#exit
Ruijie(config)#exit
Ruijie#clear counters GigabitEthernet 1/1
Ruijie#
```

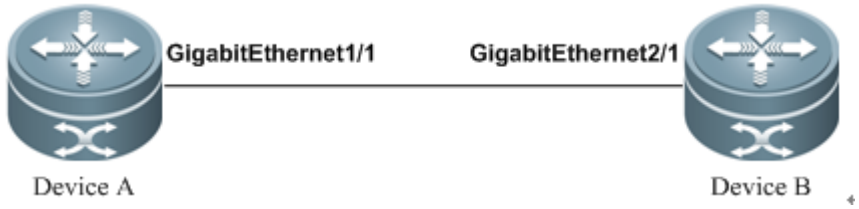
5.3.2 SEM检测特定应用事件

组网需求

Device A 和 Device B 直接相连，Device A 的 GigabitEthernet1/1 与 Device B 的 GigabitEthernet2/1 相连。因为线路或者 Device B 的问题，Device A 会经常突然接收到来自 Device B 的大量持续错帧，影响通信。将 Device A 的 GigabitEthernet1/1 shutdown 再恢复 可以将问题修复。而且 Device A 在执行事件过程中，如果一个小时内发生了五次，则需要发送日志和告警，以确定问题的时间分布。

组网拓扑

图 9-3 特定应用事件检测举例拓扑



配置要点

- 创建接口检测策略，配置接口计数事件，命令行行动，特定应用行动
- 创建特定应用事件检测策略，配置特定应用事件，Syslog 行动。

配置步骤

- 配置 Device A

1) 给 Device A 配置策略取名为 policy_a。

2) 给 policy_a 配置名为 event_1 的事件，类型为 interface 类型。其具体的参数如下：
配置检测接口计数类型的参数“parameter input_errors_frame”，其含义为检测接口的输入错帧的数量；
配置被检测接口接口名字的参数“name GigabitEthernet 1/1”用于指定被检测的接口；

配置检测阈值的参数“entry-type value entry-op ge entry-val 2000”，其含义为检测技术的绝对值，当绝对值大于等于 2000 的时候为检测通过；
配置检测频率的参数“poll-interval 5”，其含义为检测接口计数的时间间隔为 5 秒钟一次；
计数检测通过以后恢复事件检测的条件参数为“exit-type value exit-op ge exit-val 2000 exit-time 60 exit-comb and”，其“exit-type value exit-op ge exit-val 2000”部分的选项与量值都与前边的检测阈值相同，即事件触发以后，量值检查立即满足恢复的条件，其“exit-time 60 exit-comb and”表示恢复时间与恢复检查为与关系，既然恢复检查在事件触发以后就立即满足，则一旦触发事件超过 60 秒，恢复的另一个条件恢复时间也得到满足，事件检测得到恢复。

3) 给 policy_a 配置多个行动，具体如下：
命令行进入 GigabitEthernet 1/1 的接口模式；
命令行将接口 shutdown；
命令行将接口 no shutdown；
命令行进入特权模式；
命令行清除接口 GigabitEthernet 1/1 的接口统计计数；
发布 SEM 特定应用事件，其事件参数为：子集 100，类型 50

4) 将策略提交

5) 退出策略编辑

```
Ruijie# configure terminal
Ruijie(config)# smart manager applet policy_a
Ruijie(sem-applet)# event tag event_1 interface parameter input_errors_frame name GigabitEthernet 1/1 entry-type value entry-op ge entry-val 2000 poll-interval 5 exit-type value exit-op ge exit-val 2000 exit-time 60 exit-comb and
Ruijie(sem-applet)# action action_1 cli command "enable"
Ruijie(sem-applet)# action action_2 cli command "configure terminal"
Ruijie(sem-applet)# action action_3 cli command "interface GigabitEthernet 1/1"
Ruijie(sem-applet)# action action_4 cli command "shutdown"
Ruijie(sem-applet)# action action_5 cli command "no shutdown"
Ruijie(sem-applet)# action action_6 cli command "exit"
Ruijie(sem-applet)# action action_7 cli command "exit"
Ruijie(sem-applet)# action action_8 cli command "clear counters GigabitEthernet 1/1" pattern "y"
Ruijie(sem-applet)# action action_9 publish-event subset 100 type 50
Ruijie(sem-applet)# commit
Ruijie(sem-applet)# exit
Ruijie(config)#
```

■ 配置 Device A

1) 给 Device A 配置策略取名为 policy_b。

2) 给 Device A 配置名为 event_1 的事件(不同的策略中事件可以重名)，其类型为特定应用事件类型，子集和类型与上边 policy_a 中的 action_9 完全一致。检测 policy_a 中 action_9 发布的事件，当 policy_a 中 action_9 发布事件 100，50 以后，event_1 被触发。

3) 给 policy_b 配置行动发送日志

4) 将策略提交

5) 退出策略编辑

```
Ruijie# configure terminal
Ruijie(config)# smart manager applet policy_b
Ruijie(sem-applet)# event tag event_1 application subset 100 type 50
Ruijie(sem-applet)# action action_1 syslog msg "shutdown and no shutdown 5 times" priority 5
Ruijie(sem-applet)# trigger occurs 5 occurs-period 3600
Ruijie(sem-applet)# commit
Ruijie(sem-applet)# exit
Ruijie(config)#
```

显示验证

```
Ruijie# show smart manager policy registered
No.  Class    Event Type         Time Registered           Name
1    applet   interface          Mon Mar 8 21:07:21 2010   policy_a
 event_1: interface: name GigabitEthernet 1/1 parameter {input_errors_frame} entry_op ge entry_val 2000
entry_type value exit_comb and exit_op ge exit_val 2000 exit_type value exit_time 60.000 poll_interval 5.000
 maxrun 20.000
 action action_1 cli command "enable"
 action action_2 cli command "configure terminal"
 action action_3 cli command "interface GigabitEthernet 1/1"
 action action_4 cli command "shutdown"
 action action_5 cli command "no shutdown"
 action action_6 cli command "exit"
 action action_7 cli command "exit"
 action action_8 cli command "clear counters GigabitEthernet 1/1" pattern "y"
 action action_9 publish-event subset 100 type 50 arg1 "tmp"
2    applet   user application   Mon Mar 8 21:08:11 2010   policy_b
 event_1: application: sub_system 100 type 50
 trigger occurs 5 period 3600.000
 maxrun 20.000
 action action_1 syslog priority notifications msg "shutdown and no shutdown 5 times"
```

5.3.3 SEM检测计数器

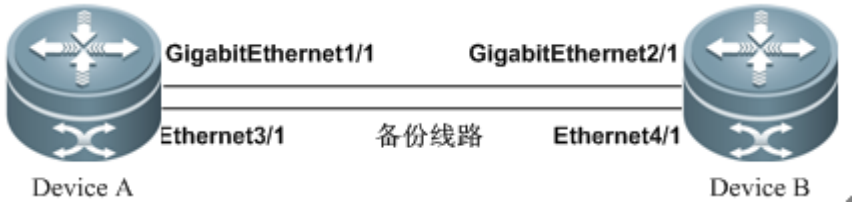
组网需求

Device A 和 Device B 直接相连，Device A 的 GigabitEthernet1/1 与 Device B 的 GigabitEthernet2/1 相连。另外在 Device A 的 Ethernet3/1 到 Device B 的 Ethernet4/1 有两设备的低带宽备份线路。因为线路或者 Device B 的问题，Device A 在接口 GigabitEthernet1/1 会经常突然接收到来自 Device B 的大量持续错帧，影响通信。将 Device A 的 GigabitEthernet1/1

shutdown 再恢复 可以将问题修复。当事件被触发总数超过 50 次以后，永久 shutdonw 接口 GigabitEthernet1/1，使用备份线路。

组网拓扑

图 9-4 计数器事件检测举例拓扑



配置要点

- 创建接口检测策略，配置接口计数事件，命令行行动，计数器行动
- 创建特定应用事件检测策略，配置计数器事件，命令行行动。

配置步骤

- 配置 Device A

1) 给 Device A 配置策略取名为 policy_a。

2) 给 policy_a 配置名为 event_1 的事件，类型为 interface 类型。其具体的参数如下：
配置检测接口计数类型的参数“parameter input_errors_frame”，其含义为检测接口的输入错帧的数量；
配置被检测接口接口名字的参数“name GigabitEthernet 1/1”用于指定被检测的接口；
配置检测阈值的参数“entry-type value entry-op ge entry-val 2000”，其含义为检测技术的绝对值，当绝对值大于等于 2000 的时候为检测通过；
配置检测频率的参数“poll-interval 5”，其含义为检测接口计数的时间间隔为 5 秒钟一次；
计数检测通过以后恢复事件检测的条件参数为“exit-type value exit-op ge exit-val 2000 exit-time 60 exit-comb and”，其“exit-type value exit-op ge exit-val 2000”部分的选项与量值都与前边的检测阈值相同，即事件触发以后，量值检查立即满足恢复的条件，其“exit-time 60 exit-comb and”表示恢复时间与恢复检查为与关系，既然恢复检查在事件触发以后就立即满足，则一旦触发事件超过 60 秒，恢复的另一个条件恢复时间也得到满足，事件检测得到恢复。

3) 给 policy_a 配置多个行动，具体如下：
命令行进入 GigabitEthernet 1/1 的接口模式；
命令行将接口 shutdown；
命令行将接口 no shutdown；
命令行进入特权模式；
命令行清除接口 GigabitEthernet 1/1 的接口统计计数；
计数器行动，给名为 counter_a 的 SEM 命令计数器的值增加 1

4) 将策略提交

5) 退出策略编辑

```
Ruijie# configure terminal
Ruijie(config)# smart manager applet policy_a
Ruijie(sem-applet)# event tag event_1 interface parameter input_errors_frame name GigabitEthernet 1/1 entry-type value entry-op ge entry-val 2000 poll-interval 5 exit-type value exit-op ge exit-val 2000 exit-time 60 exit-comb and
Ruijie(sem-applet)# action action_1 cli command "enable"
Ruijie(sem-applet)# action action_2 cli command "configure terminal"
Ruijie(sem-applet)# action action_3 cli command "interface GigabitEthernet 1/1"
Ruijie(sem-applet)# action action_4 cli command "shutdown"
Ruijie(sem-applet)# action action_5 cli command "no shutdown"
Ruijie(sem-applet)# action action_6 cli command "exit"
Ruijie(sem-applet)# action action_7 cli command "exit"
Ruijie(sem-applet)# action action_8 cli command "clear counters GigabitEthernet 1/1" pattern "y"
Ruijie(sem-applet)# action action_9 counter name counter_a op inc value 1
Ruijie(sem-applet)# commit
Ruijie(sem-applet)# exit
Ruijie(config)#
```

- 配置 Device A

1) 给 Device A 配置策略取名为 policy_b。

2) 给 Device A 配置名为 event_1 的事件(不同的策略中事件可以重名)，事件的类型为 SEM 计数器类型，具体参数如下：
检测的 SEM 计数器的名字为 counter_a，与策略 policy_a 中 action_9 操作的计数器名字相同；
计数器的检测参数为“entry-op ge entry-val 50”，其含义为当 SEM 计数器的值大于等于 50 的时候事件触发。
计数器的恢复参数为“exit-op ge exit-val 50”，其配置的类型与值都与检测参数相同，则表示计数器事件通过以后，立即恢复事件检测。

3) 给 policy_b 配置行动，具体如下：
命令行动进入 GigabitEthernet 1/1 的接口模式；
命令行动将接口永久 shutdown；

4) 将策略提交

5) 退出策略编辑

```
Ruijie# configure terminal
Ruijie(config)# smart manager applet policy_b
Ruijie(sem-applet)# event tag event_1 counter name counter_a entry-op ge entry-val 50 exit-op ge exit-val 50
Ruijie(sem-applet)# action action_1 cli command "enable"
Ruijie(sem-applet)# action action_2 cli command "configure terminal"
Ruijie(sem-applet)# action action_3 cli command "interface GigabitEthernet 1/1"
Ruijie(sem-applet)# action action_4 cli command "shutdown"
Ruijie(sem-applet)# action action_5 cli command "exit"
Ruijie(sem-applet)# commit
Ruijie(sem-applet)# exit
Ruijie(config)#
```

显示验证

```
Ruijie# show smart manager policy registered
No.   Class    Event Type     Time Registered           Name
1     applet   interface      Mon Mar 8 22:21:26 2010   policy_a
 event_1: interface: name GigabitEthernet 0/1 parameter input_errors_frame entry_op ge entry_val 2000 entry_type
value exit_comb and exit_op ge exit_val 2000 exit_type value exit_time 60.000 poll_interval 5.000
 maxrun 20.000
 action action_1 cli command "enable"
 action action_2 cli command "configure terminal"
 action action_3 cli command "interface GigabitEthernet 1/1"
 action action_4 cli command "shutdown"
 action action_5 cli command "no shutdown"
 action action_6 cli command "exit"
 action action_7 cli command "exit"
 action action_8 cli command "clear counters GigabitEthernet 1/1" pattern "y"
 action action_9 counter name counter_a value 1 op inc
2     applet   user counter   Mon Mar 8 22:23:26 2010   policy_b
 event_1: counter: name {counter_a} entry_val 50 entry_op ge exit_val 50 exit_op ge
 maxrun 20.000
 action action_1 cli command "enable"
 action action_2 cli command "configure terminal"
 action action_3 cli command "interface GigabitEthernet 1/1"
 action action_4 cli command "shutdown"
 action action_5 cli command "exit"
```

5.3.4 SEM检测热插拔

组网需求

VSU 系统在线状态插入新的成员设备后，由于软件故障，新插入的设备路由信息不完整，导致转发异常。通过命令 **clear ip route *** 重新刷路由可以解决问题。

配置要点

- 创建策略
- 配置热插拔事件
- 配置行动
- 提交策略配置

配置步骤

配置 Device A

1) 给 Device A 配置策略取名为 policy_a。

2) 给 policy_a 配置名为 event_1 的事件，类型为热差拔事件类型，操作类型为插入。

3) 给 policy_a 配置多个行动，具体如下：
执行命令进入特权模式；
执行命令 **clear ip route ***刷新路由

4) 将策略提交

5) 退出策略编辑

```
Ruijie# configure terminal
Ruijie(config)# smart manager applet policy_a
Ruijie(sem-applet)# event tag event_1 oir type plugin
Ruijie(sem-applet)# action action_1 cli command "enable"
Ruijie(sem-applet)# action action_2 cli command "clear ip route *"
Ruijie(sem-applet)# delay 60
Ruijie(sem-applet)# commit
Ruijie(sem-applet)# exit
Ruijie(config)#
```

显示验证

```
Ruijie# show smart manager policy registered
No.  Class    Event Type          Time Registered           Secu   Name
1    applet   oir                 Mon Mar 8 16:45:17 2010   none   policy_a
 event_1: oir: type{plugin}
 maxrun 20.000
 delay 60.000
 action action_1 cli command "enable"
 action action_2 cli command "clear ip route *"
```

5.3.5 SEM定时器事件

组网需求

Device A 与 Tftp Server 相连，Devie A 需要每天零点自动将日志文件归档到 Tftp Server 上，并将原有日志文件删除。

组网拓扑

图 9-5 定时器检测举例拓扑

配置要点

- 创建策略
- 配置定时器事件
- 配置行动
- 提交策略配置

配置步骤

配置 Device A

1) 给 Device A 配置策略取名为 policy_a。

2) 给 policy_a 配置名为 event_1 的事件，类型为 cron 定时器类型，指示时间为每日的零点整。

3) 给 policy_a 配置多个行动，具体如下：
执行命令进入特权模式；
执行 **copy** 命令归档日志

4) 将策略提交

5) 退出策略编辑

```
Ruijie# configure terminal
Ruijie(config)# smart manager applet policy_a
Ruijie(sem-applet)# event tag event_1 timer cron cron-entry "0 0 * * *"
Ruijie(sem-applet)# action action_1 cli command "enable"
Ruijie(sem-applet)# action action_2 cli command "copy flash: logfile.txt
tftp://172.16.0.2/device_a/log_$_event_pub_time"
Ruijie(sem-applet)# action action_3 cli command "delete flash: logfile.txt"
Ruijie(sem-applet)# commit
Ruijie(sem-applet)# exit
Ruijie(config)#exit
```

显示验证

```
Ruijie# show smart manager policy registered
No.   Class    Event Type          Time Registered           Secu    Name
```

```
1   applet   timer cron          Mon Mar 8 17:25:47 2010   none   policy_a
 event_1: timer cron: cron entry “0 0 * * *”
 maxrun 20.000
 action action_1 cli command "enable"
 action action_2 cli command "copy flash:logfile.txt tftp://172.16.0.2/device_a/log_$_event_pub_time"
 action action_3 cli command "delete flash:logfile.txt"
```

5.3.6 SEM检测CPP计数

组网需求

Device A 与 用户相连，时而会有来自网络的不明攻击，导致设备 CPU 长期占用率高。如果能够发现攻击，并降低攻击报文的优先级，可缓解攻击造成的影响。

组网拓扑

图 9-6 CPP 计数检测举例拓扑

配置要点

- 准备工作
- 创建策略
- 配置 CPP 计数事件
- 配置行动
- 提交策略配置

配置步骤

配置 Device A

1) 将报文优先级小于 1 的都调整为 1，这样发现有攻击类型的报文，就将其优先级设定为 0，小于正常报文，保证设备正常工作。

2) 给 Device A 配置策略取名为 policy_a。

3) 给 policy_a 配置名为 event_1 的事件，类型为 cpp 类型，其参数如下：
配置检测所有类型的 CPP 报文，使用参数“parameter any”；
配置检测 CPP 报文的丢弃量“type drop op ge value 1000”，指示当指定类型的 CPP 报文丢弃量大于等于 1000 个时事件触发；
配置检测的时间检测“poll-interval 15”，指示检测的时间间隔为 15 秒

4) 给 policy_a 配置多个行动，具体如下：
执行命令进入全局模式；
执行命令 **cpu-protect type $_type pri 0** 将检测到攻击的 CPP 报文类型的优先级降低，其中“$_type”为环境变量，由 CPP 事件检测器设定。运行时被具体的 CPP 报文的类型所替换。

5) 将策略提交

6) 退出策略编辑

```
Ruijie# configure terminal
Ruijie(config)# cpu-protect type tp-guard pri 1
Ruijie(config)# cpu-protect type arp pri 1
Ruijie(config)# cpu-protect type dhcps pri 1
Ruijie(config)# cpu-protect type dot1x pri 1
Ruijie(config)# cpu-protect type gvrp pri 1
Ruijie(config)# cpu-protect type rip pri 1
Ruijie(config)# cpu-protect type unknow-ipmc pri 1
Ruijie(config)# cpu-protect type err-ttl pri 1
Ruijie(config)# cpu-protect type dhcp_relay_client pri 1
Ruijie(config)# cpu-protect type dhcp_realy_server pri 1
Ruijie(config)# cpu-protect type dhcp_option82 pri 1
Ruijie(config)# smart manager applet policy_a
Ruijie(sem-applet)# event tag event_1 cpp parameter any type drop op ge value 1000 poll-interval 15
Ruijie(sem-applet)# action action_1 cli command "enable"
Ruijie(sem-applet)# action action_2 cli command "configure terminal"
Ruijie(sem-applet)# action action_3 cli command "cpu-protect type $_type pri 0"
Ruijie(sem-applet)# commit
Ruijie(sem-applet)# exit
Ruijie(config)#
```

显示验证

```
Ruijie# show smart manager policy registered
No.  Class    Event Type          Time Registered           Name
1    applet   cli                 Mon Mar 8 19:30:00 2010   policy_a
 event_1: cpp: parameter any type drop op ge value 1000 poll-interval 15
 maxrun 20.000
 action action_1 cli command "enable"
 action action_2 cli command " configure terminal "
 action action_3 cli command " cpu-protect type $_type pri 0"
```

5.3.7 SEM检测命令行

组网需求

Device A 与 Tftp Server 相连，Devie A 每次执行 **copy running-config startup-config** 命令之前，都需要将旧配置备份到 Tftp Server。

组网拓扑

图 9-7 命令行检测举例拓扑

配置要点

- 创建策略
- 配置命令行事件
- 配置行动
- 提交策略配置

配置步骤

配置 Device A

1) 给 Device A 配置策略取名为 policy_a。
2) 给 policy_a 配置名为 event_1 的事件，类型为命令行类型，检测包含“copy running-config startup-config”内容的命令；并且执行策略使用同步方式，即使用参数“sync yes”
3) 给 policy_a 配置多个行动，具体如下：
   执行命令进入特权模式；
   执行 **copy** 命令归档配置文件；
4) 将策略提交
5) 退出策略编辑

```
Ruijie# configure terminal
Ruijie(config)# smart manager applet policy_a
Ruijie(sem-applet)# event tag event_1 cli pattern "copy running-config startup-config" sync yes
```

```
Ruijie(sem-applet)# action action_1 cli command "enable"
Ruijie(sem-applet)# action action_2 cli command "copy startup-config
tftp://172.16.0.2/device_a/conf_$_event_pub_time"
Ruijie(sem-applet)# action action_3 exit 1
Ruijie(sem-applet)# commit
Ruijie(sem-applet)# exit
Ruijie(config)#
```

显示验证

```
Ruijie# show smart manager policy registered
No.   Class    Event Type          Time Registered           Name
1     applet   cli                 Mon Mar 8 19:30:00 2010   policy_a
 event_1: cli: pattern “copy running-config startup-config” sync yes
 maxrun 20.000
 action action_1 cli command "enable"
 action action_2 cli command "copy startup-config tftp://172.16.0.2/device_a/conf_$_event_pub_time"
 action action_3 exit 1
```

5.3.8 SEM检测SNMP事件

组网需求

网管工作站通过以太网与 Device A 互联，Device A 上启用 SNMP 服务，网管工作站可以通过网络管理 Device A。出于兼容性考虑，get OID 1.3.6.1.2.1.2.1 的值的 SNMP 操作需要被阻止。

组网拓扑

图 9-8 SNMP 事件检测举例拓扑

配置要点

- 创建策略
- 配置 SNMP Object 事件
- 配置行动

- 提交策略配置

配置步骤

配置 Device A

1) 给 Device A 配置策略取名为 policy_a。

2) 给 policy_a 配置名为 event_1 的事件，类型为 SNMP Object 类型，参数如下：
检测 snmp 操作的 OID 参数“oid 1.3.6.1.2.1.2.1”；
OID 不可以是表类型参数“istable no”；
OID 的类型为 int 类型，使用参数“type int”；
触发策略的执行方式为异步方式，忽略 SNMP Object 操作，使用参数“skip yes”；

3) 给 policy_a 配置行动，记录到日志 snmp 操作被取消。

4) 将策略提交

5) 退出策略编辑

```
Ruijie# configure terminal
Ruijie(config)# smart manager applet policy_a
Ruijie(sem-applet)# event tag event_1 snmp-object oid 1.3.6.1.2.1.2.1 istable no type int skip yes
Ruijie(sem-applet)# action action_1 syslog msg "cancel snmp operate" priority 5
Ruijie(sem-applet)# commit
Ruijie(sem-applet)# exit
Ruijie(config)#
```

显示验证

```
Ruijie# show smart manager policy registered
No.   Class    Event Type          Time Registered           Secu   Name
1     applet   snmp-object         Tue Mar 9 17:46:01 2010   none   policy_a
 event_1: snmp-object: oid 1.3.6.1.2.1.2.1 type int skip yes istable no
 maxrun 20.000
 action action_1 syslog msg "cancel snmp operate"
```

5.3.9 SEM检测空事件

组网需求

Device A 安装调试过程中，需要反复的清理路由表，ARP 表。需要一种简单的方法实现批量操作

配置要点

- 创建策略

- 配置空事件
- 配置行动
- 提交策略配置

配置步骤

配置 Device A

1) 给 Device A 配置策略取名为 policy_a。

2) 给 policy_a 配置名为 event_1 的事件，类型为空类型，通过命令行手动触发。

3) 给 policy_a 配置多个行动，具体如下：
执行命令进入特权模式；
执行 **clear arp-cache**，清除 ARP 缓存；
执行 **clear ip route ***，刷新 ipv4 路由；

4) 将策略提交

5) 退出策略编辑

```
Ruijie# configure terminal
Ruijie(config)# smart manager applet policy_a
Ruijie(sem-applet)# event tag event_1 none
Ruijie(sem-applet)# action action_1 cli command "enable"
Ruijie(sem-applet)# action action_2 cli command "clear arp-cache"
Ruijie(sem-applet)# action action_3 cli command "clear ip route *"
Ruijie(sem-applet)# 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 *"
```

5.3.10 SEM检测Syslog事件

组网需求

Device A 在发生内存不足的情况下会发送日志，发现该日志的时候需要对设备进行主备倒换操作。

配置要点

- 创建策略
- 配置 Syslog 事件
- 配置行动
- 配置策略触发参数
- 提交策略配置

配置步骤

配置 Device A

1) 给 Device A 配置策略取名为 policy_a。
2) 给 policy_a 配置名为 event_1 的事件，类型 Syslog 类型，检测级别为 2 内容包含“No-memory”的日志。
3) 给 policy_a 配置 switchover 行动。
4) 将策略提交
5) 退出策略编辑

```
Ruijie# configure terminal
Ruijie(config)# smart manager applet policy_a
Ruijie(sem-applet)# event tag event_1 syslog pattern "No-memory" priority critical
Ruijie(sem-applet)# action action_1 reload
Ruijie(sem-applet)# commit
Ruijie(sem-applet)# exit
Ruijie(config)#
```

显示验证

```
Ruijie# show smart manager policy registered
No.   Class    Event Type          Time Registered           Secu   Name
1     applet   syslog              Tue Mar 9 18:38:23 2010   none   policy_a
 event_1: syslog: pattern “No-memory” priority critical
maxrun 20.000
action action_1 switchover
```

5.3.11 SEM检测看门狗系统事件

组网需求

Device A 可能存在业务突发导致内存不足或者内存泄漏，当内存耗尽时设备出现故障。为了不因内存问题导致业务受影响，目前需要在内存使用量达到 95%时将设备主备倒换。

配置要点

- 创建策略
- 配置看门狗系统事件
- 配置行动
- 配置策略触发参数
- 提交策略配置

配置步骤

配置 Device A

1) 给 Device A 配置策略取名为 policy_a。
2) 给 policy_a 配置名为 event_1 的事件，类型为看门狗系统事件类型，检测的类型参数为“type memory scope system-use percent”，含义位检测系统内存使用百分比；检测的阈值参数为“entry-op ge entry-val 95”，含义位超过 95%是事件触发。
3) 给 policy_a 配置行动将设备主备倒换。
4) 将策略提交
5) 退出策略编辑

```
Ruijie# configure terminal
Ruijie(config)# smart manager applet policy_a
Ruijie(sem-applet)# event tag event_1 sysmon type memory scope system-use percent entry-op ge entry-val 95
Ruijie(sem-applet)# action action_1 switchover
Ruijie(sem-applet)# commit
Ruijie(sem-applet)# exit
Ruijie(config)#
```

显示验证

```
Ruijie# show smart manager policy registered
No.  Class    Event Type          Time Registered           Secu   Name
1    applet   sysmon              Tue Mar 9 18:38:23 2010   none   policy_a
 event_1: sysmon: type memory scope system-use percent entry-op ge entry-val 95
 maxrun 20.000
 action action_1 switchover
```

5.3.12 SEM检测GRTD事件

组网需求

Device A 的 GRTD 监控诊断发现严重问题时，为方式诊断出的问题影响业务正常运行，将设备主备倒换。

配置要点

- 创建策略
- 配置 GRTD 事件
- 配置行动
- 配置策略触发参数
- 提交策略配置

配置步骤

配置 Device A

1) 给 Device A 配置策略取名为 policy_a。
2) 给 policy_a 配置名为 event_1 的事件，类型为 GRTD 类型，检测所有槽位监控测试出严重问题，参数“slot all testing-type monitoring severity-major”；
3) 给 policy_a 配置行动将设备主备倒换
4) 将策略提交
5) 退出策略编辑

```
Ruijie# configure terminal
Ruijie(config)# smart manager applet policy_a
Ruijie(sem-applet)# event tag event_1 grtd slot all testing-type monitoring severity-major
Ruijie(sem-applet)# action action_1 switchover
Ruijie(sem-applet)# commit
Ruijie(sem-applet)# exit
Ruijie(config)#
```

显示验证

```
Ruijie# show smart manager policy registered
No.   Class    Event Type         Time Registered           Secu   Name
1     applet   grtd               Tue Mar 9 18:38:23 2010   none   policy_a
 event_1: grtd: slot all testing-type monitoring level severity-major
 maxrun 20.000
```

```
action action_1 switchover
```

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. SNMP
2. RMON
3. NTP
4. SNTP
5. SPAN
6. RSPAN

1 SNMP

1.1 SNMP相关知识

1.1.1 概述

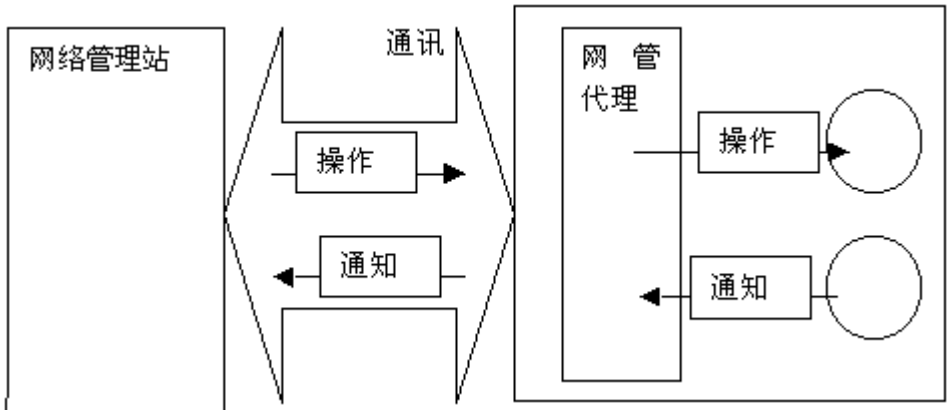
SNMP 是 Simple Network Management Protocol（简单网络管理协议）的缩写，在 1988 年 8 月就成为一个网络管理标准 RFC1157。到目前，因众多厂家对该协议的支持，SNMP 已成为事实上的网管标准，适合于在多厂家系统的互连环境中使用。利用 SNMP 协议，网络管理员可以对网络上的节点进行信息查询、网络配置、故障定位、容量规划，网络监控和管理是 SNMP 的基本功能。

SNMP 是一个应用层协议，为客户机/服务器模式，包括三个部分：

- SNMP 网络管理器
- SNMP 代理
- MIB 管理信息库
- SNMP 网络管理器，是采用 SNMP 来对网络进行控制和监控的系统，也称为 NMS (Network Management System)。
- SNMP 代理（SNMP Agent）是运行在被管理设备上的软件，负责接受、处理并且响应来自 NMS 的监控和控制报文，也可以主动发送一些消息报文给 NMS。

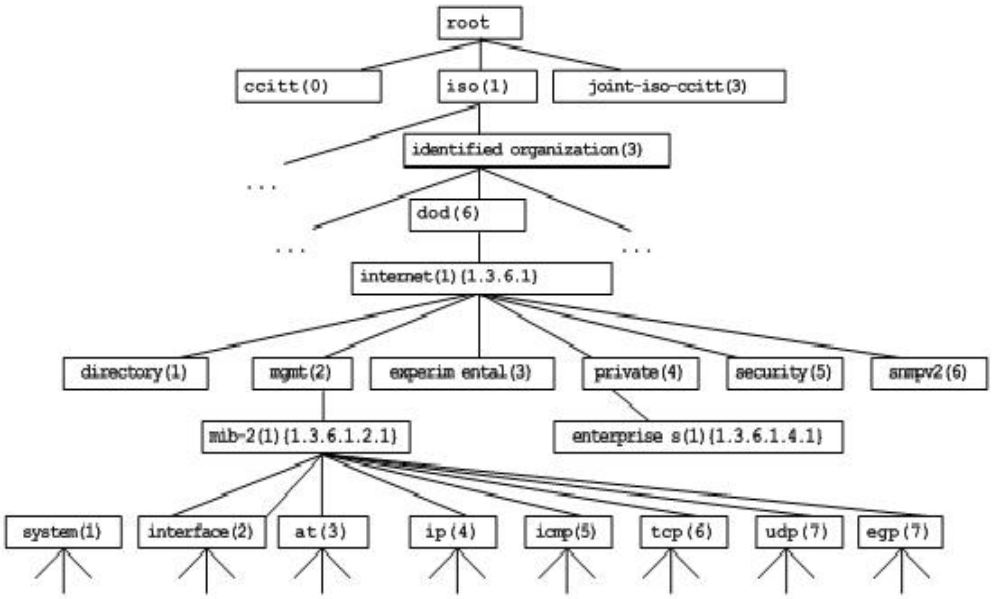
NMS 和 Agent 的关系可以用如下的图来表示：

图 1-1 网络管理站（NMS）与网管代理（Agent）的关系图



MIB（Management Information Base）是一个虚拟的网络管理信息库。被管理的网络设备中包含了大量的信息，为了能够在 SNMP 报文中唯一的标识某个特定的管理单元，MIB 采用树形层次结构来描述网络设备中的管理单元。树的节点表示某个特定的管理单元。如下图 MIB 对象命名树，为了唯一标识网络设备中的某个管理单元 System，可以采用一串的数字来表示，如{1.3.6.1.2.1.1}这一串数字即为管理单元的 Object Identifier（单元标识符），MIB 则是网络设备的单元标识符的集合。

图 1-2 MIB 树形层次结构



1.1.2 SNMP协议版本

目前 SNMP 支持以下版本：

- SNMPv1 ：简单网络管理协议的第一个正式版本，在 RFC1157 中定义。
- SNMPv2C：基于共同体（Community-Based）的 SNMPv2 管理架构，在 RFC1901 中定义的一个实验性协议。
- SNMPv3 ：通过对数据进行鉴别和加密，提供了以下的安全特性：

1) 确保数据在传输过程中不被篡改；

2) 确保数据从合法的数据源发出；

3) 加密报文，确保数据的机密性；

SNMPv1 和 SNMPv2C 都采用基于共同体（Community-based）的安全架构。通过定义主机地址以及认证名(Community String)来限定能够对代理的 MIB 进行操作的管理者。

SNMPv2C 增加了 Get-bulk 操作机制并且能够对管理工作站返回更加详细的错误信息类型。Get-bulk 操作能够一次性地获取表格中的所有信息或者获取大批量的

数据，从而减少请求-响应的次数。SNMPv2C 错误处理能力的提高包括扩充错误代码以区分不同类型的错误，而在 SNMPv1 中这些错误仅有一种错误代码。现在通过错误代码可以区分错误类型。由于网络上可能同时存在支持 SNMPv1 和 SNMPv2C 的管理工作站，因此 SNMP 代理必须能够识别 SNMPv1 和 SNMPv2C 报文，并且能返回相应版本的报文。

1.1.3 SNMP管理操作

SNMP 协议中的 NMS 和 Agent 之间的交互信息，定义了 6 种操作类型：

1) Get-request 操作：NMS 从 Agent 提取一个或多个参数值。

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；

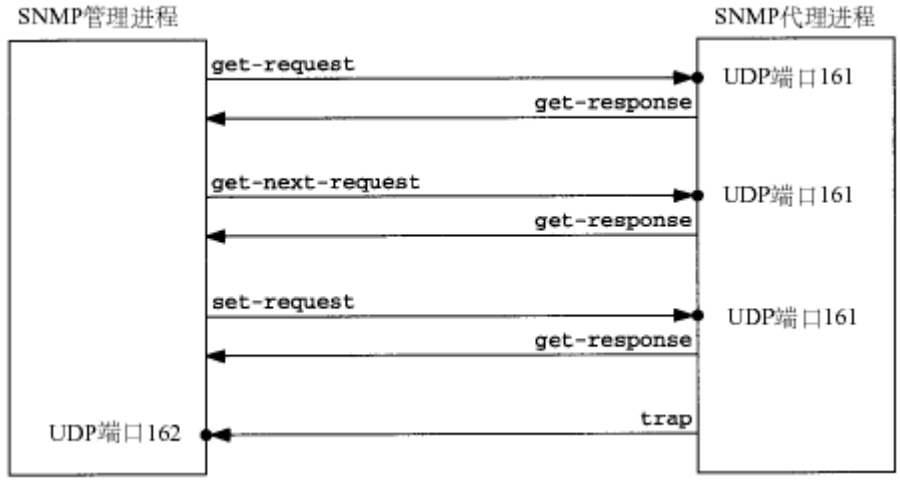
4) Set-request 操作：NMS 设置 Agent 的一个或多个参数值。

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）。下图描述了这几种种操作。

图 1-3 SNMP 的报文类型



NMS 向 Agent 发出的前面 3 种操作和 Agent 的应答操作采用 UDP 的 161 端口。Agent 发出的 Trap 操作采用 UDP 的 162 端口。

1.1.4 SNMP安全

SNMPv1 和 SNMPv2 版本使用认证名用来鉴别是否有权使用 MIB 对象。为了能够管理设备，网络管理系统 (NMS)的认证名必须同设备中定义的某个认证名一致。

一个认证名可以有以下属性：

- 只读(Read-only)：为被授权的管理工作站提供对所有 MIB 变量的读权限。
- 读写(Read-write)：为被授权的管理工作站提供对所有 MIB 变量的读写权限。
- 在 SNMPv2 的基础上，SNMPv3 通过安全模型以及安全级别来确定对数据采用哪种安全机制进行处理；目前可用的安全模型有三种类别：SNMPv1、SNMPv2C、SNMPv3。
- 下表为目前可用的安全模型以及安全级别

安全模型	安全级别	鉴别	加密	说明
SNMPv1	noAuthNoPriv	认证名	无	通过认证名确认数据的合法性
SNMPv2c	noAuthNoPriv	认证名	无	通过认证名确认数据的合法性

SNMPv3	noAuthNoPriv	用户名	无	通过用户名确认数据的合法性
SNMPv3	authNoPriv	MD5 或者 SHA	无	提供基于 HMAC-MD5 或者 HMAC-SHA 的数据鉴别机制
SNMPv3	authPriv	MD5 或者 SHA	DES	提供基于 HMAC-MD5 或者 HMAC-SHA 的数据鉴别机制提供基于 CBC-DES 的数据加密机制

1.1.5 SNMP 引擎标识

引擎标识用于唯一标识一个 SNMP 引擎。由于每个 SNMP 实体仅包含一个 SNMP 引擎，它将在一个管理域中唯一标识一个 SNMP 实体。因此，作为一个实体的 SNMPv3 代理器必须拥有一个唯一的引擎标识，即 SnmpEngineID。

引擎标识为一个 OCTET STRING，长度为 5～32 字节长。在 RFC3411 中定义了引擎标识的格式：

- 前 4 个字节标识厂商的私有企业号（由 IANA 分配），用 HEX 表示。
- 第 5 个字节表示剩下的字节如何标识：
- 0：保留
- 1：后面 4 个字节是一个 Ipv4 地址。
- 2：后面 16 个字节是一个 Ipv6 地址。
- 3：后面 6 个字节是一个 MAC 地址。
- 4：文本，最长 27 个字节，由厂商自行定义。
- 5：16 进制值，最长 27 个字节，由厂商自行定义。
- 6-127：保留。
- 128-255：由厂商特定的格式。

1.2 SNMP的配置

SNMP 的配置工作在网络设备的全局配置模式下完成，在进行 SNMP 配置前，请先进入全局配置模式。

1.2.1 设置认证名及访问权限

SNMPv1/SNMPv2C 采用基于共同体（Community-based）的安全方案，SNMP 代理只接受来自相同认证名（Community-String）的管理操作，与网络设备的认证名不符的 SNMP 报文将不被响应，直接丢弃。认证名相当于 NMS 和 Agent 之间的密码。

可以设置访问列表关联，只有指定的 IP 地址的 NMS 可以管理；

可以设定该共同体的操作权限，是 ReadOnly（只读）还是 ReadWrite（读写）；

指定视图的名称，用于基于视图的管理。默认没有指定视图，即允许访问 所有 MIB 对象；

可以指明能够使用该认证名的管理者的 IP。 若不指明，则表示不限制使用该认证名的管理者的 IP 地址。缺省为不限制使用该认证名的管理者的 IP 地址；

要配置 SNMP 认证名，在全局配置模式下执行如下命令：

命令	作用
Ruijie(config)# **snmp-server community** [**0**|**7**] *string* [view *view-name*] **[ro | rw] [host** *host-ip*] [*aclnum* | *aclname*]	设置认证名和权限。

可以配置一条或者多条指定，来指定多个不同的共同体名称，使得网络设备可以供不同的权限的 NMS 的管理，要删除共同体名称和权限，在全局配置模式下，执行 **no snmp-server community** [**0**|**7**] *string* 命令。

关键字“**0**”和“**7**”代表团体名字符串的加密类型。团体名字符串之前使用关键字“**0**”代表输入的团体名为明文，使用关键字“**7**” 代表输入的团体名为密文，不使用加密类型团体名默认为明文。配置 **service password-encryption** 命令后，团体名字符串（Community-String）将进行加密的显示和存放。此时取消 **service password-encryption** 配置后，团体字符串仍然以密文显示和存放，不会恢复为明文。

1.2.2 设置SNMP协议端口

SNMP 协议默认使用 161 UDP 端口接收 SNMP 报文；基于安全考虑，用户可自定义使用的 UDP 端口。

要配置 SNMP 协议端口号，在全局配置模式下执行如下命令：

命令	作用
Ruijie(config)# **snmp-server udp-port** *port-num*	设置 SNMP 协议接收报文的 UDP 端口号。

使用 **no snmp-server udp-port** 命令恢复使用默认端口。

1.2.3 配置MIB视图和组

可以使用基于视图的访问控制模型来判定一个操作关联的管理对象是否在视图允许之内或被排除在外，只有在视图允许之内的管理对象才被允许访问。在进行控制时，一般是将某些用户和一个组关联，再将某个组与某个视图关联。一个组内的用户具有相同的访问权限。

可以设置包含视图和排除视图；

可以为一组用户设置只读的视图和可写的视图；

如果是 SNMPv3 的用户，可以为其指定使用的安全级别，是否需要进行认证、是否需要进行加密；

要配置 MIB 视图和组，在全局配置模式下执行如下命令：

命令	作用
Ruijie(config)# **snmp-server view** *view-name oid-tree* {**include** | **exclude**}	创建一个 MIB 视图，包含或排除关联的 MIB 对象。
Ruijie(config)# **snmp-server group** *groupname* {**v1** | **v2c** |**v3** {**auth** | **noauth** | **priv**}} [**read** *readview*] [**write** *writeview*] [**access** { [*aclnum* | *aclname*] }]	创建一个组，并和视图关联。

使用 **no snmp-server view** *view-name* 命令来删除一个视图，或者使用 **no snmp-server view** *view-name oid-tree* 命令在一个视图中删除一棵子树。也可以使用 **no snmp-server group** *groupname* {**v1 | v2c | v3** }命令来删除一个组。

1.2.4 配置SNMP用户

可以使用基于用户的安全模型来进行安全管理，基于用户的管理必须事先配置用户的信息，NMS 只有使用合法的用户才能同代理进行通信。

对于 SNMPv3 用户，可以指定安全级别、认证算法（MD5 或 SHA）、认证口令、加密算法（目前只有 DES）和加密口令；

要配置 SNMP 用户，在全局配置模式下执行如下命令：

命令	作用
Ruijie(config)# **snmp-server user** *username roupname* {**v1	v2c	v3 [encrypted] [auth { md5|sha }** *auth-password*] [**priv des56** *priv-password*] } [**access** { [*aclnum*	*aclname*] }]	设置用户信息。

通过 **no snmp-server user** *username groupname* {**v1 | v2c | v3** } 删除指定用户。

1.2.5 配置SNMP主机地址

Agent 在特定的情况下，也会主动的向 NMS 发送消息，要配置 Agent 主动发送消息的 NMS 主机地址，在全局配置模式下，执行如下指令：

命令	作用
Ruijie(config)# **snmp-server host** *host-addr* [**vrf** *vrfname*] [**traps**] [**version** { **1	2c	3** { **auth	noauth	priv** }] *community-string* [**udp-port** *port-num*] [*notification-type*]	设置 SNMP 主机地址，主机端口，vrf 选项，消息类型，认证名（在 SNMPv3 下是用户名）、安全级别（仅 SNMPv3 支持）等

1.2.6 设置SNMP代理参数

可以对 SNMP 的 Agent 的基本参数进行配置，设置设备的联系方式、设备的网元编码信息、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
Ruijie(config)# **snmp-server contact** *text*	设置系统的联系方式
Ruijie(config)# **snmp-server location** *text*	设置系统的位置
Ruijie(config)# **snmp-server net-id** *text*	设置设备的网元编码信息
Ruijie(config)# **snmp-server chassis-id** *number*	设置系统的序列码

1.2.7 定义SNMP代理最大数据报文长度

为了减少对网络带宽的影响，可以定义 SNMP 代理的数据包的最大长度。在全局配置模式下，执行如下指令：

命令	作用
Ruijie(config)# **snmp-server packetsize** *byte-count*	设置最大代理数据包大小

1.2.8 屏蔽SNMP代理

SNMP 代理服务是锐捷产品提供的一个服务，默认是启动的，在不需要代理服务的时候，可以通过如下方式屏蔽 snmp 代理功能以及相关配置信息；屏蔽 snmp 代理功能，在全局配置模式下，执行如下指令：

命令	作用
Ruijie(config)# **no snmp-server**	屏蔽 SNMP 代理服务

1.2.9 关闭SNMP代理

不同于屏蔽命令，锐捷产品提供了关闭 snmp 代理的命令，该命令会直接关闭 snmp 所有服务（相当于 snmp 代理功能被禁用了，不接收报文、不发送响应报文及 trap），但是不会屏蔽代理的配置信息；要关闭 SNMP 代理服务，在全局配置模式下，执行如下指令：

命令	作用
Ruijie(config)# **no enable service snmp-agent**	关闭 SNMP 代理服务

1.2.10 配置Agent主动向NMS发送Trap消息

Trap 是 Agent 不经请求主动向 NMS 发送的消息，用于报告一些紧急而重要的事件的发生。缺省是不允许 Agent 主动发送 Trap 消息，如果要允许，在全局配置模式下，执行如下指令：

命令	作用
Ruijie(config)# **snmp-server enable traps** [*type*] [*option*]	允许 Agent 主动发送 Trap 消息
Ruijie(config)# **no snmp-server enable traps** [*type*] [*option*]	禁止 Agent 主动发送 Trap 消息

1.2.11 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
Ruijie(config)# **interface** *interface-id*	进入端口配置模式
Ruijie(config-if)# [**no**] **snmp trap link-status**	打开或者关闭发送该接口 link trap 的功能.

下面配置将配置接口为不发送 Link trap:

```
Ruijie(config)# interface gigabitEthernet 1/1
Ruijie(config-if)# no snmp trap link-status
```

1.2.12 配置发送消息操作的参数

可以指定 Agent 发送 Trap 消息的一些参数，执行如下指令来设置：

命令	作用
Ruijie(config)# **snmp-server trap-source** *interface*	指定发送 Trap 消息的源接口
Ruijie(config)# **snmp-server queue-length** *length*	指定每个 Trap 消息报文的队列长度
Ruijie(config)# **snmp-server trap-timeout** *seconds*	指定发送 Trap 消息的时间间隔

1.2.13 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，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
Ruijie(config)# **snmp-server trap-format private**	配置 TRAP 消息携带私有字段
Ruijie(config)# **no snmp-server trap-format private**	取消 TRAP 消息携带私有字段

当使用 SNMP v1 的版本发送 Trap 消息时，该配置不生效。

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: 8000131103000000000000
storage-type: permanent     active
Security level: auth priv
Auth protocol: SHA
Priv protocol: DES
Group-name: g1
```

1.3.4 查看SNMP视图和组

在特权用户模式下，执行 **show snmp group** 来查看当前代理上配置的组。

```
Ruijie# show snmp group
groupname: g1
securityModel: v3
securityLevel:authPriv
readview: default
writeview: default
notifyview:
```

```
groupname: public
securityModel: v1
securityLevel:noAuthNoPriv
readview: default
writeview: default
notifyview:
groupname: public
securityModel: v2c
securityLevel:noAuthNoPriv
readview: default
writeview: default
notifyview:
```

在特权用户模式下，执行 show snmp view 来查看当前代理上配置的视图。

```
Ruijie# show snmp view
default(include) 1.3.6.1
test-view(include) 1.3.6.1.2.1
```

1.3.5 查看用户配置的主机信息

在特权用户模式下，执行 **show snmp host** 来查看当前代理上用户配置的主机信息。

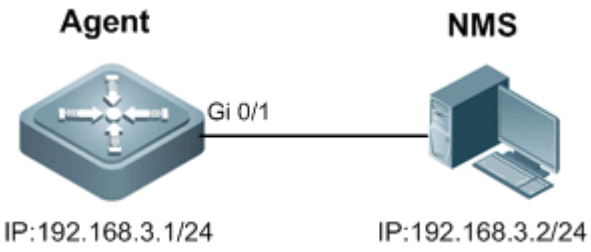
```
Ruijie# show snmp host
Notification host: 192.168.64.221
udp-port: 162   type: trap
user: public    security model: v1
Notification host: 2000:1234::64
udp-port: 162   type: trap
user: public    security model: v1
```

1.4 SNMP典型配置用例

1.4.1 SNMP v1/v2 配置用例

拓扑图

图 1-4 SNMP v1/2 应用拓扑



应用需求

1) 网管工作站（NMS）基于共同体认证模式对网络设备（Agent）进行管理，网络设备能够控制共同体访问指定 MIB 对象的操作权限（可读或可写），例如：某共同体“user1”只能读写 System（1.3.6.1.2.1.1）节点下的对象。

2) 网络设备仅允许特定 IP（例如：192.168.3.2/24）的网管工作站对网络设备进行管理。

3) 网络设备能够主动向网管工作站发送消息。

4) 网管工作站能够获取设备的基本系统信息，如系统的联系方式、位置、序列码。

配置要点

1) 通过创建 MIB 视图，并关联设置认证名（Community）及访问权限（Read 或 Write），即可实现第一个应用需求。

2) 在设置认证名及访问权限的同时，设置访问控制列表关联或指明使用该认证名的管理者的 IP，即可实现第二个应用需求（本例采用关联访问控制列表）。

3) 配置 SNMP 主机地址，并使能 Agent 主动发送 Trap 消息的功能。

4) 配置 SNMP 代理的参数信息。

配置步骤

第一步，配置 MIB 视图和访问控制列表。

！创建一个 MIB 视图名“v1”，包含关联的 MIB 对象（1.3.6.1.2.1.1）。

```
Ruijie(config)#snmp-server view v1 1.3.6.1.2.1.1 include
```

！创建访问控制列表名“a1”，允许 IP 地址为 192.168.3.2/24。

```
Ruijie(config)#ip access-list standard a1
Ruijie(config-std-nacl)#permit host 192.168.3.2
Ruijie(config-std-nacl)#exit
```

第二步，配置认证名及访问权限。

！配置 Community 为“user1”，关联 MIB 视图“v1”可写，以及关联访问控制列表“a1”。

```
Ruijie(config)#snmp-server community user1 view v1 rw a1
```

第三步，配置 Agent 主动向 NMS 发送消息。

！配置 SNMP 主机地址为 192.168.3.2，消息格式为 Version 2c，认证名为“user1”。

```
Ruijie(config)#snmp-server host 192.168.3.2 traps version 2c user1
```

！使能 Agent 主动发送 Trap 消息。

```
Ruijie(config)#snmp-server enable traps
```

第四步，配置 SNMP 代理参数。

！配置系统所处的位置。

```
Ruijie(config)#snmp-server location fuzhou
```

！配置系统的联系方式。

```
Ruijie(config)#snmp-server contact ruijie.com.cn
```

！配置系统的序列码。

```
Ruijie(config)#snmp-server chassis-id 1234567890
```

第五步，配置 Agent 的 IP 地址。

！配置 Gi 0/1 的接口地址为 192.168.3.1/24。

```
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-gigabitEthernet 0/1)#ip address 192.168.3.1 255.255.255.0
Ruijie(config-if-gigabitEthernet 0/1)#exit
```

验证结果

第一步，查看设备的配置信息。

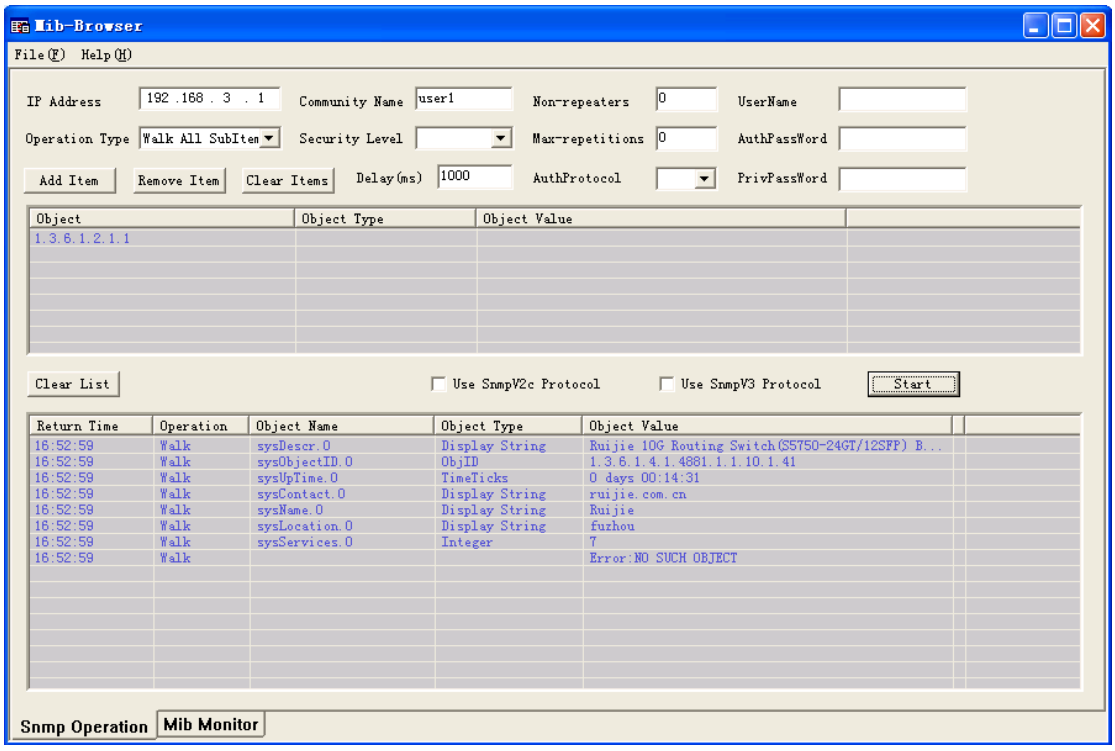
```
Ruijie# show running-config
!
ip access-list standard a1
 10 permit host 192.168.3.2
!
interface gigabitEthernet 0/1
 no ip proxy-arp
 ip address 192.168.3.1 255.255.255.0
!
snmp-server view v1 1.3.6.1.2.1.1 include
snmp-server location fuzhou
snmp-server host 192.168.3.2 traps version 2c user1
snmp-server enable traps
snmp-server contact ruijie.com.cn
snmp-server community user1 view v1 rw a1
snmp-server chassis-id 1234567890
```

第二步，查看 SNMP 视图和组的信息。

```
Ruijie#show snmp view
v1(include) 1.3.6.1.2.1.1                    //自定义 MIB 对象“v1”
default(include) 1.3.6.1                     //系统缺省定义 MIB 对象
Ruijie#show snmp group
groupname: user1                        //配置 Community 默认为 SNMP 组
securityModel: v1
securityLevel:noAuthNoPriv
readview: v1
writeview: v1
notifyview:
groupname: user1
securityModel: v2c
securityLevel:noAuthNoPriv
readview: v1
writeview: v1
notifyview:
```

第三步，安装 MIB-Browser，在 IP Address 中输入设备的 IP 地址：192.168.3.1，在 Community Name 中输入“user1”，点击 add item 按钮，选择要查询的 MIB 的具体管理单元，比如下图的 System。点击 Start 按钮，便开始对网络设备进行 MIB 的查询了，具体的查询结果见对话框的最下面的窗口：

图 1-5



1.4.2 SNMP v3 配置用例

拓扑图

图 1-6 SNMPv3 应用拓扑

应用需求

1) 网络工作站（NMS）基于用户的认证加密模式对网络设备（Agent）进行管理。例如：使用用户名“user1”，认证方式为 MD5，认证密码为 123，加密算法为 DES56，加密密码为 321。

2) 网络设备能够控制用户访问 MIB 对象的操作权限。例如：用户“user1”可以对 System（1.3.6.1.2.1.1）节点下的 MIB 对象进行读操作，其中只能对 SysContact（1.3.6.1.2.1.1.4.0）节点下的 MIB 对象进行写操作。

3) 网络设备能够主动向网管工作站发送验证加密的消息。

配置要点

- 创建 MIB 视图，并指定包含或排除的 MIB 对象。
- 创建 SNMP 组，设置该组的版本号为“v3”，并指定该组使用的安全级别，同时需要设置该组对相应视图的读写权限。
- 创建用户名，同时关联对应的 SNMP 组名，即可以设置用户访问 MIB 对象的操作权限，同时需要配置版本号为“v3”，以及相应的认证方式、认证密码、加密算法、加密密码。
- 配置 SNMP 主机地址，同时需要配置版本号为“3”，并设置使用的安全级别。

配置步骤

第一步，配置 MIB 视图和组。

！创建一个 MIB 视图 “view1”，包含关联的 MIB 对象（1.3.6.1.2.1.1）；再创建一个 MIB 视图“view2”，包含关联的 MIB 对象（1.3.6.1.2.1.1.4.0）。

```
Ruijie(config)#snmp-server view view1 1.3.6.1.2.1.1 include
Ruijie(config)#snmp-server view view2 1.3.6.1.2.1.1.4.0 include
```

！创建一个组“g1”，选择版本号为“v3”，配置安全级别为认证加密模式“priv”，并可读视图“view1”，可写视图“view2”。

```
Ruijie(config)#snmp-server group g1 v3 priv read view1 write view2
```

第二步，配置 SNMP 用户。

！创建用户名“user1”，属于组“g1”，选择版本号为“v3”，配置认证方式为“md5”，认证密码为“123”，加密方式为“DES56”，加密密码为“321”。

```
Ruijie(config)#snmp-server user user1 g1 v3 auth md5 123 priv des56 321
```

第三步，配置 SNMP 主机地址。

！配置主机地址为 192.168.3.2，选择版本号为“3”，配置安全级别为认证加密模式“priv”，关联对应的用户名“user1”。

```
Ruijie(config)#snmp-server host 192.168.3.2 traps version 3 priv user1
```

！ 使能 Agent 主动向 NMS 发送 Trap 消息。

```
Ruijie(config)#snmp-server enable traps
```

第四步，配置 Agent 的 IP 地址。

！ 配置 Gi0/1 的接口地址为 192.168.3.1/24。

```
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-gigabitEthernet 0/1)#ip address 192.168.3.1 255.255.255.0
Ruijie(config-if-gigabitEthernet 0/1)#exit
```

验证结果

第一步，查看设备的配置信息。

```
Ruijie# show running-config
!
interface gigabitEthernet 0/1
 no ip proxy-arp
 ip address 192.168.3.1 255.255.255.0
!
snmp-server view view1 1.3.6.1.2.1.1 include
snmp-server view view2 1.3.6.1.2.1.1.4.0 include
snmp-server user user1 g1 v3 encrypted auth md5 7EBD6A1287D3548E4E52CF8349CBC93D priv des56
D5CEC4884360373ABBF30AB170E42D03
snmp-server group g1 v3 priv read view1 write view2
snmp-server host 192.168.3.2 traps version 3 priv user1
snmp-server enable traps
```

第二步，查看 SNMP 用户

```
Ruijie# show snmp user
User name: user1
Engine ID: 800013110300d0f8221120
storage-type: permanent     active
Security level: auth priv
Auth protocol: MD5
Priv protocol: DES
Group-name: g1
```

第三步，查看 SNMP 视图

```
Ruijie#show snmp view
view1(include) 1.3.6.1.2.1.1
```

```
view2(include) 1.3.6.1.2.1.1.4.0
default(include) 1.3.6.1
```

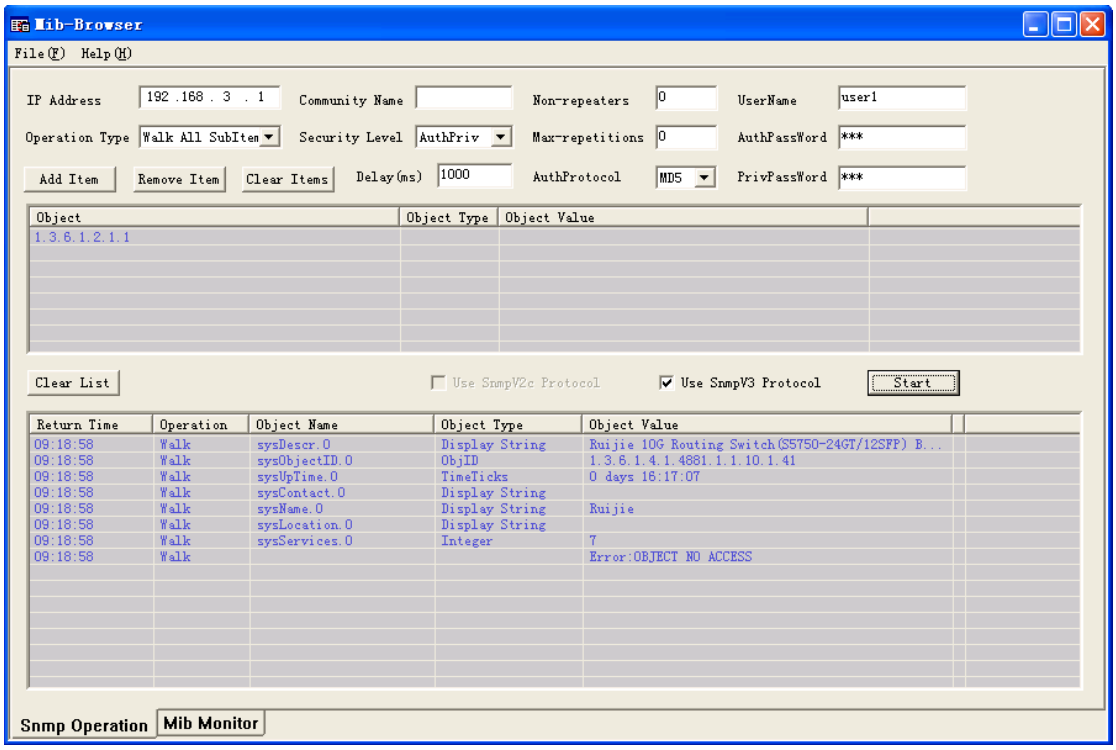
第四步，查看 SNMP 组

```
Ruijie# show snmp group
groupname: g1
securityModel: v3
securityLevel:authPriv
readview: view1
writeview: view2
notifyview:
```

第五步，查看用户配置的主机信息

```
Ruijie#show snmp host
Notification host: 192.168.3.2
udp-port: 162
type: trap
user: user1
security model: v3 authPriv
```

第六步，安装 MIB-Browser，在 IP Address 中输入设备的 IP 地址：192.168.3.1，在 UserName 中输入“user1”，在 Security Level 中选择“AuthPriv”，在 AuthPassWord 中输入“123”，在 AuthProtocol 中选择“MD5”，在 PrivPassWord 中输入“321”。点击 add item 按钮，选择要查询的 MIB 的具体管理单元，比如下图的 System。点击 Start 按钮，便开始对网络设备进行 MIB 的查询了，具体的查询结果见对话框的最下面的窗口：



2 RMON

2.1 概述

RMON（Remote Monitoring，远程监视）是 IETF(Internet Engineering Task Force，Internet 工程专门小组)标准的监控规范，这个规范可以让各种网络监控器和控制台系统之间交换网络监控数据。RMON 在网络节点上放置探测器，网络管理平台决定这些探测器汇报哪些信息，如被监视的统计信息，收集历史信息所使用的时间段等等。例如交换机和路由器等网络设备，在网络上相当一个网络节点，通过 RMON 功能，可以监视当前所处节点位置的信息。

RMON 的发展经历了三个阶段，第一阶段是以太网远程监视；第二阶段增加了令牌环的功能，称为令牌环远程监视模块；第三阶段被称为 RMON2，从而使 RMON 功能发展到协议监视的更高层次。

第一阶段的 RMON（下称 RMON1）包含九个组，所有的组都是可选择性（而非强制性）的，但有些组的使用必须有其他组的支持。

交换机实现其中的第 1，2，3，9 组的内容：统计组、历史组、警告组、事件组。

2.1.1 统计组

统计组是 RMON 中的第 1 组，统计组统计被监控的每个子网的基本统计信息。目前只能对网络设备的以太网接口进行监控、统计。该组包含一个以太网统计表，统计的内容包括丢弃的数据包、广播数据包、CRC 错误、大小块、冲突等。

2.1.2 历史组

历史组(History)是 RMON 中的第 2 组，历史组定期地收集网络统计信息，并记录下来以便日后处理。它包含两个小组：

- HistoryControl 组用来设置采样间隔时间、采样数据源等控制信息。
- EthernetHistory 组为管理员提供有关网段流量、错误包、广播包、利用率以及碰撞次数等其他统计信息的历史数据。

2.1.3 警告组

警报组(Alarm)是 RMON 中的第 3 组，以指定的时间间隔监控一个特定的 MIB(Management Information Base，管理信息库)对象，当这个 MIB 对象的值超过一个设定的上限值或低于一个设定的下限值时，会触发警报。警报被当作事件来处理，处理事件的方式可以是记录日志或发送 SNMP Trap 的方式。

2.1.4 事件组

事件组(Event)是 RMON 中的第 9 组，决定由于警报而产生事件时，处理行为是产生一个日志记录表项还是一个 SNMP Trap。

2.2 配置RMON

2.2.1 配置统计组

您可以使用如下命令添加一个统计表项。

命令	作用
Ruijie(config-if)# **rmon collection stats** *index* [**owner** *ownername*]	添加一个统计项
Ruijie(config-if)# **no rmon collection stats** *index*	删除一个统计项

☑ 我司产品当前版本只支持以太网接口的统计。

索引值应该是一个 1-65535 之间的整数，目前可最多同时配置 100 条统计项

2.2.2 配置历史控制组

你可以使用如下命令添加一条历史控制表项：

命令	作用
Ruijie(config-if)# **rmon collection history** *index* [**owner** *ownername*] [**buckets** *bucket-number*] [**interval** *seconds*]	添加一个历史控制表项
Ruijie(config-if)# **no rmon collection history** *index*	删除一个历史控制表项

☑ 我司产品当前版本只支持以太网的记录。

索引值应该在 1-65535 之间，最多可以配置 10 条控制表项。

Bucket-number：控制项指定了采用的数据源、时间间隔。每个采样区间，都进行一次采样。采样的结果保存下来，Bucket-number 指定了保存采样的最大数目，当采样纪录达到最大值时，则新纪录覆盖最早的纪录。Bucket-number 取值范围是 1-65535，默认值是 10。

Interval：采样的时间间隔。默认值是 1800 秒，取值在 1-3600 之间。

2.2.3 配置警告组和事件组

你可以使用如下命令配置警告表：

命令	作用

Ruijie(config)# **rmon alarm** *number variable interval* {**absolute** | **delta**} **rising-threshold** *value* [*event-number*] **falling-threshold** *value* [*event-number*] [**owner** *ownername*]	添加一个历史控制表项
Ruijie(config)# **rmon event** *number* [**log**] [**trap** *community*] [**description** *description-string*] [**owner** *ownername*]	添加一个事件组表项
Ruijie(config)# **no rmon alarm** *number*	删除一个警告组
Ruijie(config)# **no rmon event** *number*	删除一个事件组

number：警告表(事件表)的索引，范围 1-65535。

variable：警告表监控的变量。变量必须是整数类型。

interval：采样的时间间隔。范围<1-4294967295>

关键字 Absolute 表示拿每次采样得到的值和上限、下限比较，关键字 Delta 表示利用和上次采样的差值和上限、下限比较。

value 定义了上限、下限的值。

event-number：当超过了上限或者下限的时候，触发事件组索引为 Event-number 的事件。

关键字 Log 表示事件触发的动作是：纪录事件

关键字 Trap 表示事件触发后的动作是：发送 Trap 消息到管理站。

community：发送 Trap 时的认证名。

description-string：事件的描述。

ownername：警告组或事件组的所有者。

2.2.4 显示RMON状态

命令	作用
show rmon alarm	显示警告组
show rmon event	显示事件组
show rmon history	显示历史组
show rmon statistics	显示统计组

2.3 RMON配置实例

2.3.1 配置统计组实例

如果您希望统计以太端口 3，使用如下命令：

```
Ruijie(config)# interface gigabitEthernet 0/3
```

```
Ruijie(config-if)# rmon collection stats 1 owner zhangsan
```

2.3.2 配置历史组实例

如果您希望每隔 10 分钟统计以太网端口 3 的历史信息，使用如下命令：

```
Ruijie(config)# interface gigabitEthernet 0/3
Ruijie(config-if)# rmon collection history 1 owner zhangsan interval 600
```

2.3.3 配置警告组和事件组实例

如果您希望配置对一个可统计的 MIB 变量的报警功能。下面的例子说明了对 MIB-II 中 IfEntry 表中实例 ifInNUcastPkts.6(端口 6 上收到的非单播帧的个数，实例的标识符为 1.3.6.1.2.1.2.2.1.12.6)设置报警功能。具体功能为：交换机每隔 30 秒检查端口 6 上收到的非单播帧的个数的变化，如果收到的非单播帧的个数比上次检查时(30 秒前)增加了 20 个或 20 个以上，或者比上次只增加 10 个或 10 以下，则警报被触发，同时警报将触发事件 1 进行相应的操作(记录到日志中，并发送认证名为”rmon”的 Trap，事件的描述为“ifInNUcastPkts is too much”)。警报和事件表项的拥有者均为 zhangsan。

```
Ruijie(config)# rmon alarm 10 1.3.6.1.2.1.2.2.1.12.6 30 delta rising-threshold 20 1 falling-threshold 10 1 owner
zhangsan
Ruijie(config)# rmon event 1 log trap rmon description "ifInNUcastPkts is too much " owner zhangsan
```

2.3.4 显示rmon状态实例

show rmon alarm

```
Ruijie# show rmon alarm
rmon alarm table:
                    index: 10,
                    interval: 30,
                    oid = 1.3.6.1.2.1.2.2.1.12.6
                    sampleType: 2,
                    alarmValue: 0,
                    startupAlarm: 3,
                    risingThreshold: 20,
                    fallingThreshold: 10,
                    risingEventIndex: 1,
                    fallingEventIndex: 1,
                    owner: zhangesan,
                    stats: 1,
```

show rmon event

```
Ruijie# show rmon event
rmon event table:
                    index = 1
```

```
                    description = ifInNUcastPkts
                    type = 4
                    community = rmon
                    lastTimeSent = 0 d:0 h:0 m:0 s
                    owner = zhangsan
                    status = 1
```

show rmon history

```
Ruijie# show rmon history
rmon history control table:
                    index = 1
                    interface = FastEthernet 0/1
                    bucketsRequested = 10
                    bucketsGranted = 10
                    interval = 1800
                    owner = zhangsan
                    stats = 1

rmon history table:
                    index = 1
                    sampleIndex = 198
                    intervalStart = 0d:14h:0m:47s
                    dropEvents = 0
                    octets = 67988
                    pkts = 726
                    broadcastPkts = 502
                    multiPkts = 189
                    crcAllignErrors = 0
                    underSizePkts = 0
                    overSizePkts = 0
                    fragments = 0
                    jabbers = 0
                    collisions = 0
                    utilization = 0
```

show rmon statistics

```
Ruijie#  show rmon statistics
ether statistic table:
                    index = 1
                    interface = FastEthernet 0/1
                    owner = zhangsan
                    status = 0
                    dropEvents = 0
                    octets = 1884085
                    pkts = 3096
```

```
broadcastPkts = 161
multiPkts = 97
crcAllignErrors = 0
underSizePkts = 0
overSizePkts = 1200
fragments = 0
jabbers = 0
collisions = 0
packets64Octets = 128
packets65To127Octets = 336
packets128To255Octets = 229
packets256To511Octets = 3
packets512To1023Octets = 0
packets1024To1518Octets = 1200
```

3 NTP

3.1 理解NTP

Network Time Protocol（NTP）是用来使网络设备时间同步化的一种协议，它可以使网络设备对其服务器或时钟源做同步化，它可以提供高精准度的时间校正（LAN 上与标准时间差小于 1 毫秒，WAN 上几十毫秒），且可使用加密确认的方式来防止攻击。

NTP 提供准确时间，首先要有准确的时间来源，这一时间应该是国际标准时间 UTC。 NTP 获得 UTC 的时间来源可以是原子钟、天文台、卫星，也可以从 Internet 上获取。这样就有了准确而可靠的时间源。

为防止对时间服务器的恶意破坏，NTP 使用了识别(Authentication)机制，检查时间同步信息是否是真正来自所宣称的服务器并检查资料的返回路径，以提供对抗干扰的保护机制。

目前我司设备支持 NTP 的客户端与服务器功能，即设备既可以从时间服务器上同步时间，也能够作为时间服务器对其他设备进行时间同步。在作为服务器工作时设备仅支持单播 Server 模式。

3.2 配置NTP

3.2.1 配置NTP全局安全识别机制

锐捷的 NTP 客户端支持与服务器进行加密通信，加密方式为密钥加密机制。

配置 NTP 客户端通过加密方式与服务器通信分两步：第一，对 NTP 客户端进行全局安全识别以及全局密钥相关设置；第二，设置通信服务器的信任密钥；NTP 全局安全设置机制属于第一个设置步骤，但是要真正发起与服务器之间的加密通信，还要对对应的服务器设置认证密钥。

在缺省情况下，客户端不使用全局安全识别机制。如果未使用安全识别机制则不对通信进行加密处理。但是仅仅设置了全局安全标志，并不代表一定采用了加密方式完成服务器与客户端的通信，还必须完成其他全局密钥配置并设置服务器加密密钥才可能发起和服务器的加密通信。

要配置全局安全识别机制，在全局配置模式中执行以下命令：

命令	作用
Ruijie(config)#**ntp authenticate**	配置 NTP 全局安全识别机制。
Ruijie(config)#**no ntp authenticate**	关闭 NTP 全局安全识别机制。

报文的验证是通过 **ntp authentication-key**、**ntp trusted-key** 指定的信任密钥进行验证的。

3.2.2 配置NTP全局认证密钥

进行 NTP 安全认证全局配置，接下来的配置就是设置全局认证密钥。

配置全局认证密钥，每个密钥有一个唯一的 key-id 标识，客户可以用 **ntp trusted-key** 将该 key-id 对应的密钥设置为全局信任密钥。

要配置全局认证密钥，在全局配置模式中执行以下命令：

命令	作用
Ruijie(config)#**ntp authentication-key** *key-id* **md5** *key-string* [*enc-type*]	配置 NTP 全局认证密钥。 key-id：1-4294967295 key-string：长度范围任意 enc-type：有 0 和 7 两种类型。
Ruijie(config)#**no ntp authentication-key** *key-id*	删除 NTP 全局认证密钥。

配置了全局认证密钥并不说明该密钥一定有效，在使用该密钥之前必须将该密钥配置成为全局信任密钥。

☑ 锐捷目前的版本只支持最大 1024 认证密钥，每个服务器允许设置唯一一个密钥进行安全通信。

3.2.3 配置NTP全局信任密钥ID

进行全局安全认证配置的最后一个阶段，就是将一个全局密钥配置成全局信任密钥。通过该信任密钥，用户才可以发送加密数据并检验收到数据报文的合法性。

要指定全局信任密钥，在全局配置模式中执行以下命令：

命令	作用
Ruijie(config)#**ntp trusted-key** *key-id*	配置 NTP 全局信任密钥 ID。
Ruijie(config)#**no ntp trusted-key** *key-id*	删除 NTP 全局信任密钥 ID。

以上三步设置仅仅是完成安全认证机制的第一个步骤，真正发起与客户服务器的加密通信必须对相应的服务器设置信任密钥。

直接删除全局认证密钥，则该密钥对应的信任信息也会被删除。

3.2.4 配置NTP服务器

在缺省情况下，没有配置 NTP 服务器。锐捷的客户端系统支持最多同时与 20 个 NTP 服务器交互，（在全局认证以及密钥相关设置完成后）可以为每一个服务器设置一个认证密钥，发起与服务器的加密通信。

与服务器的默认通信版本为 NTP 版本 3，同时可以配置发送 NTP 报文的源接口，并只在发送接口上接收对应服务器的 NTP 报文。

配置一个 NTP 服务器，在全局配置模式下执行以下命令：

命令	作用

Ruijie(config)#**ntp server** *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
Ruijie(config)#**no ntp server** *ip-addr*	删除 NTP 服务器

只有完成了全局安全识别以及密钥设置机制，这时候设置服务器通信的信任密钥，才能发起与服务器的加密通信，而加密通信的完成需要服务器端信任相同的密钥。

3.2.5 关闭接口接收NTP报文

该命令的功能是关闭对应接口上接收 NTP 报文。

在缺省情况下，任意接口上接收的 NTP 报文都可以提供给客户端进行时钟调整，通过设置这个功能，可以屏蔽对应接口上收到的 NTP 报文。

能够进行该功能命令配置的接口肯定是能够配置 IP 收发报文的接口，在其他接口上没有该命令。

在接口配置模式下执行以下命令，配置关闭接口接收 NTP 报文：

命令	作用
Ruijie(config-if)#**interface** *interface-type number*	进入接口配置模式
Ruijie(config-if)#**ntp disable**	关闭接口接收 NTP 报文的功能。

要打开接口接收 NTP 报文的功能，在接口模式下使用 **no ntp disable** 命令。

3.2.6 NTP功能开关

no ntp 命令的功能是关闭 NTP 同步服务，停止时间同步，同时清空相关的 NTP 配置信息。

在缺省情况下，NTP 功能是关闭的，但只要配置了 NTP 服务器或 NTP 安全识别机制，NTP 功能就会被打开。

要关闭 NTP，在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)#**ntp authenticate** 或 **ntp server** *ip-addr* [**version** *version*][**source** *if-name number*][**key** *keyid*][**prefer**]	打开 NTP 功能
Ruijie(config)#**no ntp**	关闭 NTP 功能。

3.2.7 配置NTP更新硬件时钟

使用此功能可以让 NTP 客户端使用从外部时钟源同步得来的时钟值更新设备的硬件时钟。

在全局配置模式下执行以下命令配置更新硬件时钟：

命令	作用
Ruijie(config)#**ntp update-calendar**	配置更新硬件时钟
Ruijie(config)#**no ntp update-calendar**	取消配置更新硬件时钟

在缺省情况下没有配置 NTP 更新硬件时钟。配置之后，NTP 客户端会在每次与外部时钟源同步成功时也同时更新设备的硬件时钟。一般情况下建议启用此功能，使设备的硬件时钟也能同时保持精准。

3.2.8 设置NTP主时钟

该功能用来设置本地时钟作为 NTP 主时钟（本地时钟参考源可靠），为其它设备提供同步时间。

在通常情况下，本地系统都会直接或间接地与外部的时钟源进行同步。但若由于网络连接故障等原因而导致本地系统无法与外部时钟源同步时，可以通过该命令设置本地时钟参考源可靠，为其他设备提供同步时间。

一旦进行了此设置，系统便不会与比其时钟层数数值更高的时钟源进行同步。

NTP 使用“层数（stratum）”的概念来描述设备距离权威时钟源的“跳数（hops）”。一个层数为 1 的时间服务器应当有个直连的原子钟或电波钟；层数为 2 的时间服务器就从层数为 1 的服务器获取时间；层数为 3 的服务器就从层数为 2 的获取时间……如此递推。因此时钟层数数值更低的时钟源即被认为拥有更高的时钟精度。

在全局配置模式下执行以下命令配置 NTP 主时钟功能：

命令	作用
Ruijie(config)#**ntp master** [*stratum*]	设置本地时钟作为 NTP 主时钟并指定相应时钟层数。时钟层数取值范围为 1～15；若不指定该参数则默认值为 8。
Ruijie(config)#**no ntp master**	取消 NTP 主时钟设置

如下可以设置本地时钟参考源可靠，并设置其时钟层数为 12。

```
Ruijie(config)# ntp master 12
```

使用此命令时必须特别小心。将本地时钟设置为主时钟（尤其是指定了较低的时钟层数值时）很有可能将真正的有效时钟源覆盖。如果对同一网络中的多个设备都使用了该命令，则可能由于设备之间的时钟差异导致网络的时钟同步不稳定。

另外，使用该命令前若系统从未与外部时钟源同步过，则有可能需要手动校准系统时钟以保证其不会有过大的偏差（关于如何手动校准系统时钟请参考《交换机基础管理配置指南》中的系统时间配置部分）

3.2.9 配置NTP服务的访问控制权限

NTP 服务的访问控制功能提供了一种最小限度的安全措施（更安全的方法是使用 NTP 身份验证机制）。系统在缺省情况下未配置任何 NTP 访问控制规则。

在全局配置模式下执行以下命令配置 NTP 服务的访问控制权限：

命令	作用

Ruijie(config)#**ntp access-group { peer | serve | serve-only | query-only }** *access-list-number* | *access-list-name*	设置对本地服务的访问控制权限
Ruijie(config)#**no ntp access-group { peer | serve | serve-only | query-only }** *access-list-number* | *access-list-name*	取消对本地服务的访问控制权限的设置

其中：

- **peer**：既允许对本地 NTP 服务进行时间请求和控制查询，也允许本地设备与远程系统同步时间（完全访问权限）。
- **serve**：允许对本地 NTP 服务进行时间请求和控制查询，但不允许本地设备与远程系统同步时间。
- **serve-only**：仅允许对本地 NTP 服务进行时间请求。
- **query-only**：仅允许对本地 NTP 服务进行控制查询。
- *access-list-number*：IP 访问控制列表标号；范围为 1～99 和 1300～1999。关于如何创建 IP 访问控制列表请参考《访问控制列表配置指南》中的相关描述。
- *access-list-name*：IP 访问控制列表名。关于如何创建 IP 访问控制列表请参考《访问控制列表配置指南》中的相关描述。

当一个访问请求到达时，NTP 服务按照从最小访问限制到最大访问限制的顺序依次匹配规则，以第一个匹配到的规则为准。匹配顺序为 peer、serve、serve-only、query-only。

> 目前系统暂未支持控制查询功能（用于通过网络管理设备对 NTP 服务器进行控制，如设置闰秒标记或监控其工作状态等）。虽然是按照上述顺序进行规则匹配，但涉及到与控制查询相关的请求都无法支持。

如果未配置任何访问控制规则，则所有访问都是允许的。但一旦配置了访问控制规则，则仅有规则中所允许的访问才能进行。

可以如下配置以允许第 1 号访问列表中的对端设备对本地设备进行时间请求、查询控制和时间同步；并限制第 2 号访问列表中的对端设备仅能对本地设备进行时间请求：

```
Ruijie(config)# ntp access-group peer 1
Ruijie(config)# ntp access-group serve-only 2
```

3.3 显示NTP信息

3.3.1 调试NTP

要进行 NTP 功能调试，可以通过该命令输出必要的调试信息，进行故障诊断和排除。

调试 NTP 功能，在特权模式下执行以下命令：

命令	作用
debug ntp	打开调试功能。
no debug ntp	关闭调试功能。

3.3.2 显示NTP信息

在特权模式下，您可以使用 **show ntp status** 命令来显示当前的 NTP 信息。

显示 NTP 状态信息，在特权模式下执行以下命令：

命令	作用
show ntp status	显示当前的 NTP 信息

只有在配置了相关的通信服务器之后该命令才能打印出显示信息。

```
Ruijie# show ntp status
Clock is synchronized,stratum 9,reference is 192.168.217.100
nominal freq is 250.0000 Hz,actual freq is 250.0000 Hz,precision is 2**18
reference time is AF3CF6AE.3BF8CB56(20:55:10.000 UTC Mon Mar 1 1993)
clock offset is 32.97540 sec,root delay is 0.00000 sec
root dispersion is 0.00003 msec,peer dispersion is 0.00003 msec
```

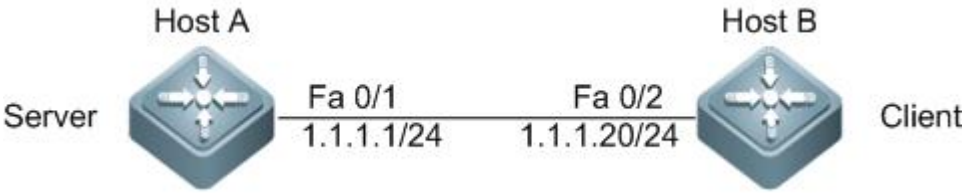
stratum 代表当前时钟的等级，reference 为同步服务器的地址，frep 当前系统时钟频率，precision 为当前系统时钟精度，reference time 为同步服务器参考时钟的 UTC 时间值，clock offset 为当前时钟偏移， root delay 为当前时钟延迟，root dispersion 为顶级服务器精度，peer dispersion 为同步服务器精度。

3.4 NTP典型配置举例

3.4.1 配置NTP客户端/服务器模式

拓扑图

图 1-1 NTP 客户端/服务器模型



应用需求

- Host A 设置本地时钟作为 NTP 主时钟，其时钟层数为 12
- Host B 配置为 NTP 客户端，指定 Host A 为 NTP 服务器
- Host B 的硬件时钟也能保持同步

配置要点

1) NTP 服务器

- 在通常情况下，本地系统都会直接或间接地与外部的时钟源进行同步。但若由于网络连接故障等原因而导致本地系统无法与外部时钟源同步时，可以通过 **ntp master** 命令设置本地时钟作为 NTP 主时钟，为其他设备提供同步时间。

2) NTP 客户端

- 配置指定的 NTP 服务器
- 通过配置 NTP 的硬件时钟更新功能，让 NTP 客户端使用从外部时钟源同步得来的时钟值更新设备的硬件时钟，使设备的硬件时钟也能同时保持精准

配置步骤

- NTP 服务器端的配置

！设置 NTP 主时钟。将本地时钟作为可信基准时钟源，时钟层数为 12

```
HostA(config)# ntp master 12
```

- NTP 客户端的配置

！设置 Host A 为 NTP 服务器

```
HostB(config)# ntp server 1.1.1.1
```

！配置 NTP 硬件时钟更新功能

```
HostB(config)# ntp update-calendar
```

配置验证

- 配置 NTP 同步之前，查看时间

！查看基准时钟源的时间

```
HostA# show clock
17:12:48 UTC Tue, Sep 8, 2009
```

！查看未同步前客户端的时间

```
HostB# show clock
12:01:10 UTC Sat, Jan 1, 2000
```

！查看未同步前客户端 NTP 状态

```
HostB(config)# show ntp status
Clock is unsynchronized, stratum 16, no reference clock
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**0
reference time is 0.0 (00:00:00.000 UTC Thu, Jan 1, 1970)
clock offset is 0.00000 sec, root delay is 0.00000 sec
root dispersion is 0.00000 msec, peer dispersion is 0.00000 msec
```

由以上显示可以看出，此时未同步；

- 配置 NTP 同步之后，查看 NTP 配置。关注点：NTP 服务器地址、层数。

CLI 界面打印如下日志信息：

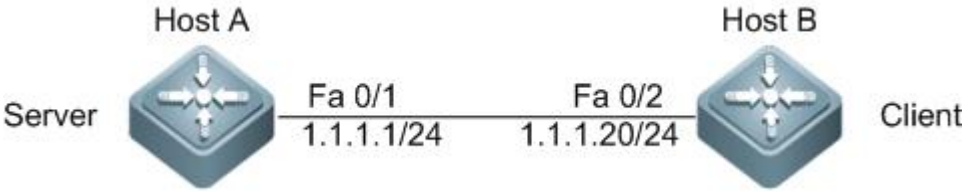
```
*Sep  8 18:10:37: %SYS-6-CLOCKUPDATE: System clock has been updated to 18:10:37 UTC Tue Sep  8 2009.
HostB# show ntp status
Clock is synchronized, stratum 13, reference is 1.1.1.1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**24
reference time is CE511CC9.37EB5B2D (18:11:21.000 UTC Tue, Sep 8, 2009)
clock offset is -0.00107 sec, root delay is 0.00000 sec
root dispersion is 0.00002 msec, peer dispersion is 0.00002 msec
```

由以上显示信息可以看出，NTP 客户端同服务器建立了连接，Host B 与 Host A 时间同步，且比 Host A 层数大 1，为 13。

3.4.2 配置带身份认证的NTP客户端/服务器模式

拓扑图

图 1-2 NTP 客户端/服务器模型



应用需求

- Host A 设置本地时钟作为 NTP 主时钟，其时钟层数为 12
- Host B 配置为 NTP 客户端，指定 Host A 为 NTP 服务器
- 启用身份认证机制，防止非法用户对时间服务器的恶意破坏

配置要点

配置 NTP 服务器/客户端的身份认证功能包括以下几个步骤：

- 使能 NTP 全局安全识别机制
- 配置 NTP 全局认证密钥及其对应的密钥 ID
- 指定 NTP 全局信任密钥 ID

NTP 客户端同指定 NTP 服务器之间的通信认证密钥及对应密钥的 ID 值一致。

配置步骤

■ NTP 服务器端的配置

第一步，设置本地 NTP 主时钟。将本地时钟作为可信基准时钟源，层数为 12

```
HostA(config)# ntp master 12
```

第二步，配置 NTP 身份认证

！使能 NTP 全局安全识别机制

```
HostA(config)# ntp authenticate
```

！配置 NTP 全局认证密钥为“helloworld”，其对应的密钥 ID 为“6”

```
HostA(config)# ntp authentication-key 6 md5 helloworld
```

！指定“6”为 NTP 全局信任密钥 ID

```
HostA(config)# ntp trusted-key 6
```

■ NTP 客户端的配置

第一步，配置 NTP 身份认证

！使能 NTP 全局安全识别机制

```
HostB(config)# ntp authenticate
```

！配置 NTP 全局认证密钥为“helloworld”，其对应的密钥 ID 为“6”

```
HostB(config)# ntp authentication-key 6 md5 helloworld
```

！指定“6”为 NTP 全局信任密钥 ID

```
HostB(config)# ntp trusted-key 6
```

！设置 Host A 为 NTP 服务器，并设置同该服务器通信的密钥 ID 为“6”

```
HostB(config)# ntp server 1.1.1.1 key 6
```

配置验证

■ 查看 NTP 服务器端的配置信息。关注点：NTP 主时钟设置、NTP 服务器 IP 地址、认证相关功能配置。

```
HostA#show run
!
interface fastEthernet 0/1
ip address 1.1.1.1 255.255.255.0
!
ntp authentication-key 6 md5 07360623191d300a004609 7
ntp authenticate
ntp trusted-key 6
ntp master 12
!
```

■ 查看 NTP 客户端的配置信息。关注点：指定 NTP 服务器的 IP 地址及密钥 ID、认证相关功能配置。

```
HostB #show run
!
interface fastEthernet 0/2
ip address 1.1.1.20 255.255.255.0
!
ntp authentication-key 6 md5 141a4f012d1d3c23174905 7
ntp authenticate
ntp trusted-key 6
ntp server 1.1.1.1 key 6
!
```

正确配置后，CLI 打印如下日志信息：

```
*Sep  9 11:31:29: %SYS-6-CLOCKUPDATE: System clock has been updated to 11:31:29 UTC Wed Sep  9 2009.
```

以上日志信息说明 NTP 客户端 HostB 的时钟已经被更新。

■ 查看 NTP 服务器端的 NTP 状态信息

```
HostA #show ntp status
Clock is synchronized, stratum 12, reference is 127.127.1.1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**24
reference time is CE521261.E52DECA2 (11:39:13.000 UTC Wed, Sep 9, 2009)
clock offset is 0.00000 sec, root delay is 0.00000 sec
root dispersion is 0.00002 msec, peer dispersion is 0.00002 msec
```

■ 查看 NTP 客户端的 NTP 状态信息；关注点：NTP 服务器地址、层数。

```
HostB# show ntp status
Clock is synchronized, stratum 13, reference is 1.1.1.1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**24
reference time is CE5212A1.E5D712A0 (11:40:17.000 UTC Wed, Sep 9, 2009)
clock offset is -0.00005 sec, root delay is 0.00000 sec
root dispersion is 0.00002 msec, peer dispersion is 0.00002 msec
```

由以上显示信息可以看出，NTP 客户端同服务器成功建立了连接，Host B 与 Host A 时间同步，且比 Host A 层数大 1，为 13。

4 SNTP

4.1 概述

目前，因特网上普遍采用了通讯协议来实现网络时间同步，即 NTP（Network Time Protocol--网络时间协议），还有一种协议是 NTP 协议的简化版，即 SNTP（Simple Network Time Protocol，简单网络时间协议）。

NTP 协议可以跨越各种平台和操作系统，用非常精密的算法，因而几乎不受网络的延迟和抖动的影响，可以提供 1-50 ms 精度。NTP 同时提供认证机制，安全级别很高。但是 NTP 算法复杂，对系统要求较高。

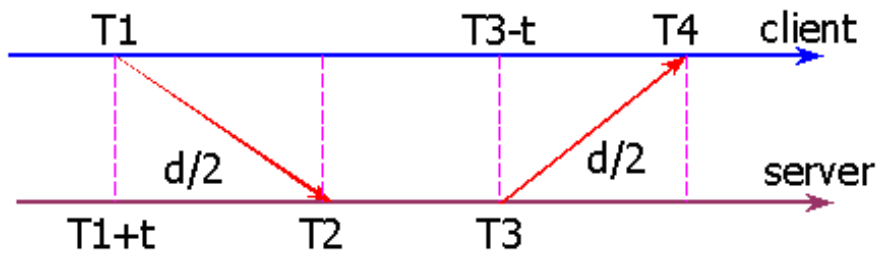
SNTP（简单网络时间协议）是 NTP 的简化版本，在实现时，计算时间用了简单的算法，性能较高。而精确度一般也能达到 1 秒左右，也能基本满足绝大多数场合的需要。

由于 SNTP 的报文和 NTP 的报文是完全一致的，所以本设备实现的 SNTP Client 能完全兼容 NTP Server。

4.2 SNTP原理

SNTP 协议采用客户机/服务器工作方式，服务器通过接收 GPS 信号或自带的原子钟作为系统的时间基准，客户机通过定期访问服务器提供的时间服务获得准确的时间信息，并调整自己的系统时钟，达到网络时间同步的目的。

图 1-1



Originate Timestamp	T1	time request sent by client
Receive Timestamp	T2	time request received at server
Transmit Timestamp	T3	time reply sent by server
Destination Timestamp	T4	time reply received at client

T1：客户机发送查询请求时间（以客户机时间系统为参照），标记为 Originate Timestamp；

T2：服务器收到查询请求时间（以服务器时间系统为参照），标记为 Receive Timestamp；

T3：服务器回复时间信息包时间（以服务器时间系统为参照），标记为 Transmit Timestamp；

T4：客户机收到时间信息包时间（以客户机时间系统为参照），标记为 Destination Timestamp；

T：服务器和客户机之间的时间偏差；

d：两者之间的往返时间；

时间求解过程：

因为

T2 = T1 + t + d / 2;

所以

T2 - T1 = t + d / 2;

又因为

T4 = T3 – t + d / 2;

所以

T3 - T4 = t – d / 2;

求得

d = (T4 - T1) - (T3 - T2);

t = ((T2 - T1) + (T3 - T4)) / 2;

求出了 t 和 d，SNTP Client 就可据此算出当前的时间。

即，当前时间为 T4 + t

4.3 配置SNTP

4.3.1 缺省的SNTP设置

缺省情况下，SNTP 的配置如下：

功能特性	缺省值
SNTP 状态	Disable，关闭 SNTP 服务
NTP Server 的 IP 地址	0
SNTP 的同步时间的间隔	1800s
本地时区	+8，即东八区

4.3.2 打开SNTP

进入特权模式，按以下步骤打开 SNTP：

1) 进入全局配置模式。

```
Ruijie# config
```

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”时间间隔请勿小于 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。

4.3.3 配置SNTP Server的地址

由于 SNTP 的报文和 NTP 的报文是完全一致的，所以 SNTP Client 能完全兼容 NTP Server。网络上存在着较多的 NTP Server，您可以选择一个网络延迟较少的一个作为设备上的 SNTP Server。

具体的 NTP server 地址可以登录 http://www.time.edu.cn/或 http://www.ntp.org/上获取。

如 192.43.244.18(time.nist.gov)。

进入特权模式，按以下步骤配置 SNTP Server IP 地址：

1) 进入全局配置模式。

```
Ruijie# config
```

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
```

4.3.4 配置SNTP同步时钟的间隔

SNTP Client 需要设置一定的时间间隔定期访问 NTP Server，以便定时校正时钟。以下步骤将配置设备和 NTP Server 同步时钟的间隔：

1) 进入全局配置模式。

```
Ruijie# config
```

2) 设置定时同步时钟的间隔，单位为秒。范围为 60 秒-65535 秒，缺省值为 1800 秒。

```
Ruijie(config)# sntp interval <seconds>
```

3) 退回到特权模式

```
Ruijie(config)# End
```

4) 显示当前配置

```
Ruijie# show running-config
```

5) 保存配置。

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

这里设置的时间间隔不会立即生效，如果要立即生效，请配置完时间间隔后执行 sntp enable 命令。

4.3.5 配置本地时区

通过 SNTP 协议通讯后获取的时间都是格林威治标准时间 (GMT)，为了准确的获取本地时间，需要设置本地时区来对标准时间进行调正。

1) 进入全局配置模式。

```
Ruijie# config
```

2) 配置时区。

<timezone-name>：时区名称，范围 2 至 10 个字符。

<time-zone>：时区，范围为-23 至 23，负数表示西区，正数表示东区。如 8 表示东八区，-8 表示西 8 区，0 表示格林威治标准时间。默认时区名为“UTC”，缺省值为 0。

```
Ruijie(config)# clock timezone <time-zone>
```

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 timezone** 来恢复缺省值。

4.4 显示SNTP

步骤如下：

1) 查看 SNTP 的相关参数

```
Ruijie# show sntp
```

2) 使用 **show sntp** 查看 SNTP 的配置参数：

```
Ruijie# show sntp
SNTP state                  : ENABLE                                  //SNTP 是否打开
SNTP server                 : 192.168.4.12                              //SNTP Server
SNTP sync interval          : 60                                    //定时同步的时间间隔
Time zone                    : +8                                           //本地时区
```

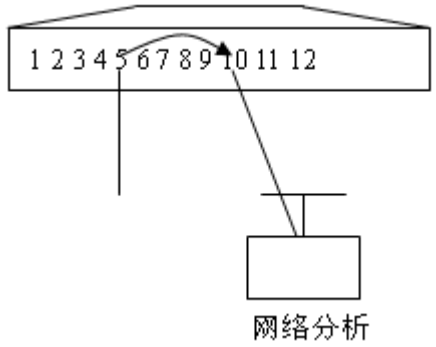
5 SPAN

5.1 SPAN概述

用户可以利用端口镜像(SPAN)提供的功能，将指定端口的报文复制到交换机上另一个连接有网络监测设备的端口，进行网络监控与故障排除。

通过 SPAN 可以监控所有进入和从源端口输出的报文。例如，在图 1 中，端口 5 上的所有报文都被映射到了端口 10，连接在端口 10 上的的网络分析仪虽然没有和端口 5 直接相连，但是可以接收通过端口 5 上的所有报文。

图 1-1 SPAN 配置实例



SPAN 并不影响源端口和目的端口的报文交换，只是将所有进入和从源端口输出的报文原样复制了一份到目的端口。但是在镜像流量超过目的端口带宽的情况下，例如 100Mbps 目的端口监控 1000Mbps 源端口的流量，可能导致报文被丢弃。

5.2 SPAN基本概念

5.2.1 SPAN会话

SPAN 会话是镜像源端口与目的端口之间的数据流，可以监控单个或多个端口的输入、输出、双向的报文。Switched port、Routed port 和 AP 等类型的端口都可以配置为 SPAN 会话的源端口和目的端口。端口加入 SPAN 会话后并不影响交换机的正常操作。

用户可以在处于关闭状态的端口上配置 SPAN 会话，但是该 SPAN 会话是非活动的，只有相关的端口被打开后，SPAN 会话才会变为活动状态。另外，SPAN 会话在交换机上电后并不立即生效，直到目的端口处于可操作状态后，SPAN 会话才处于活动状态。用户可以通过 **show monitor** [**session** *session_num*]命令查看 SPAN 会话的操作状态。

5.2.2 镜像数据流

数据流方向

SPAN 会话包含以下三种方向的数据流：

- 输入数据流：所有源端口上接收到的报文都将被复制一份到目的端口。在一个 SPAN 会话中，用户可以监控一个或多个源端口的输入报文。由于某些原因(如端口安全)，从源端口输入的报文可能被丢弃，但这不影响 SPAN 功能，该报文仍然会镜像到目的端口。
- 输出数据流：所有从源端口发送的报文都将复制一份到目的端口。在一个 SPAN 会话中，用户可以监控一个或多个源端口的输出报文。若由于某些原因，从别的端口发送到源端口的报文可能被丢弃，同样，该报文也不会发送到目的端口。由于某些原因从源端口输出的报文的格式可能改变，例如源端口输出经过路由之后的报文，报文的源 MAC、目的 MAC、VLAN ID 以及 TTL 发生变化，同样，拷贝到目的端口的报文的格式也会变化。
- 双向数据流：包括上面所说的两种数据流。在一个 SPAN 会话中，用户可监控一个或多个源端口的输入和输出方向的数据流。

SPAN Traffic

使用 SPAN 可以监控所有网络通讯，包括多播帧，BPDU 帧等。

5.2.3 源端口

源端口也被称为被监控口，在 SPAN 会话中，源端口上的数据流被监控，用于网络分析或故障排除。在单个 SPAN 会话中，用户可以监控输入、输出和双向数据流，且源端口的最大个数没有限制。

源端口具有以下特性：

- 源端口可以是 switched port，routed port 或 AP。
- 源端口不能同时作为目的端口。
- 源端口和目的端口可以属于同一 VLAN，也可以属于不同 VLAN。

5.2.4 目的端口

SPAN 会话有一个目的端口(也被称为监控口)，用于接收源端口的报文拷贝。

目的端口具有以下特性：

- 目的端口可以是 switched port、routed port 或 AP。
- 目的端口不能同时作为源端口。

☑ NBS200F 系列产品不支持 AP(Aggregate Port)口作为输出端口。

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

5.3.1 SPAN缺省状态

功能特性	缺省值
SPAN 状态	关闭

5.3.2 创建SPAN会话并指定目的端口和源端口

用户可以按照以下步骤创建 SPAN 会话并指定目的端口(监控口)和源端口(被监控口)：

命令	作用
Ruijie(config)# **monitor session** *session_num* **source interface** *interface-id* [**,| -**] {**both	rx	tx**}	指定源端口。对于 *interface-id*，请指定相应的接口号。
Ruijie(config)# **monitor session** *session_num* **destination interface** *interface-id* [**switch**]	指定目的端口。对于 *interface-id*，请指定相应的接口号，添加 switch 参数将支持镜像目的端口交换功能。

想要删除 SPAN 会话，可以使用 **no monitor session** *session_num* 全局配置命令。想要删除所有 SPAN 会话，可以使用 **no monitor session all** 全局配置命令。使用 **no monitor session** *session_num* **source interface** *interface-id* 全局配置命令或 **no monitor session** *session_num* **destination interface** *interface-id* 可删除源端口或目的端口。

下面这个例子说明如何创建一个 SPAN 会话：会话 1。首先，将当前会话 1 的配置清除掉，然后设置端口 gigabitEthernet 3/1 的报文镜像到端口 gigabitEthernet 3/8。**Show monitor session** 特权命令用于确认配置是否成功。

```
Ruijie(config)# no monitor session 1
Ruijie(config)# monitor session 1 source interface
gigabitEthernet 3/1 both
Ruijie(config)# monitor session 1 destination interface
gigabitEthernet 3/8
Ruijie(config)# end
Ruijie# show monitor session 1
sess-num: 1
src-intf:
GigabitEthernet 3/1 frame-type Both
dest-intf:
GigabitEthernet 3/8
```

5.3.3 从SPAN会话中删除一个口

用户可以按照以下步骤从一个 SPAN 会话中删除源端口。

命令	作用
Ruijie(config)# **no monitor session** *session_num* **source interface** *interface-id* [，**| -**] [**both	rx	tx**]	指定需删除的源端口。对于 interface-id，请指定相应的接口号。

使用 **no monitor session** *session_num* **source interface** *interface-id* 全局配置命令可以从一个 SPAN 会话中删除源端口。下面这个例子显示如何将端口 gigabitEthernet 1/1 从会话 1 中删除并确认配置是否成功。

```
Ruijie(config)# no monitor session 1 source interface
gigabitethernet 1/1 both
Ruijie(config)# end
Ruijie# show monitor session 1
sess-num: 1
dest-intf:
GigabitEthernet 3/8
```

5.3.4 配置基于流的镜像

在全局配置模式下，按照以下步骤可以设置基于流的镜像。

命令	作用
Ruijie(config)# **[no] monitor session** *session_num* **source interface** *interface-id* **rx acl** *name*	设定需要镜像的流所匹配的 acl name,以及镜像源端口和目的端口

☑ 只支持入口镜像。

5.3.5 其他注意事项

1) 请将网络分析仪连接到监控口。

2) 当 SPAN 处于使能状态，配置的变更有以下结果：

- 如果改变了源端口的 VLAN 配置，配置将马上生效。
- 如果改变了目的端口的 VLAN 配置，配置马上生效。
- 如果禁用了源端口或目的端口，SPAN 将不起作用。
- 如果将源端口或目的端口加入 AP，源端口或目的端口将退出 SPAN 会话。

5.4 显示SPAN状态

使用 **show monitor** 特权命令可显示当前 SPAN 配置的状态,下面这个例子说明了如何通过 **show monitor** 特权命令显示 SPAN 会话 1 的当前状态

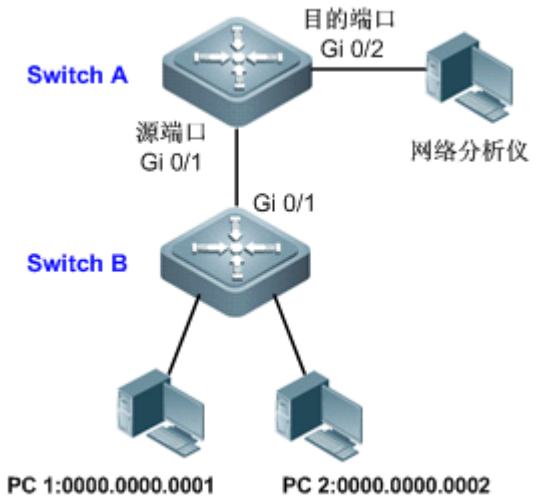
```
Ruijie# show monitor session 1
sess-num: 1
src-intf:
GigabitEthernet 3/1 frame-type Both
dest-intf:
GigabitEthernet 3/8
```

5.5 SPAN典型配置用例

5.5.1 基于流的镜像配置用例

拓扑图

图 1-2 SPAN 简单应用拓扑



应用需求

网络分析仪能够监控 Switch A 转发给 Switch B 的所有数据流，监控来自 Switch B 的特定数据流（如来自 PC1 和 PC2 的数据流）。

配置要点

1、在连接网络分析仪的设备上（本例为 Switch A）配置 SPAN 功能，将连接 Switch B 的端口（本例为 Gi 0/1）设置 SPAN 的源端口，将直连网络分析仪的端口（本例为 Gi 0/2）设置为 SPAN 的目的端口。

2、配置 SPAN 源端口（本例为 Gi 0/1）基于流的镜像（仅允许 PC1 和 PC2 的数据流）

配置步骤

第一步，配置互联设备的连接口。

！配置 Switch A 的端口 Gi 0/1 为 Trunk Port。

```
SwitchA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)#interface gigabitEthernet 0/1
SwitchA(config-if-GigabitEthernet 0/1)#switchport mode trunk
```

```
SwitchA(config-if-GigabitEthernet 0/1)#exit
```

第二步，配置 ACL。

！在 Switch A 上创建 MAC 扩展访问列表“ruijie”，允许源 MAC 为 0000.0000.0001 和 0000.0000.0002。

```
SwitchA(config)#mac access-list extended ruijie
SwitchA(config-mac-nacl)#permit host 0000.0000.0001 any
SwitchA(config-mac-nacl)#permit host 0000.0000.0002 any
SwitchA(config-mac-nacl)#exit
```

第三步，创建 SPAN 会话，并指定源端口和目的端口。

！在 Switch A 上，创建 Session 1，并指定 Gi 0/1 为源端口，镜像双向数据流，并配置基于流的入口镜像。

```
SwitchA(config)#monitor session 1 source interface gigabitEthernet 0/1 tx
SwitchA(config)#monitor session 1 source interface gigabitEthernet 0/1 rx acl ruijie
```

！在 Switch A 指定端口 Gi 0/2 为 Session 1 的镜像目的端口

```
SwitchA(config)#monitor session 1 destination interface gigabitEthernet 0/2
```

验证结果

第一步，查看设备的配置信息。

```
SwitchA#show running-config
!
mac access-list extended ruijie
 10 permit host 0000.0000.0001 any etype-any
 20 permit host 0000.0000.0002 any etype-any
!
interface GigabitEthernet 0/1
 switchport mode trunk
!
monitor session 1 destination interface GigabitEthernet 0/2
monitor session 1 source interface GigabitEthernet 0/1 tx
monitor session 1 source interface GigabitEthernet 0/1 rx acl ruijie
!
```

第二步，查看设备的 SPAN 状态。

```
SwitchA#show monitor session 1
sess-num: 1                              //SPAN Session
span-type: LOCAL_SPAN                   //本地镜像
src-intf:                                 //SPAN 源端口信息
GigabitEthernet 0/1         frame-type Both
rx acl id 2900                          //基于流的镜像
acl name ruijie
dest-intf:                                //SPAN 目的端口信息
```

GigabitEthernet 0/2

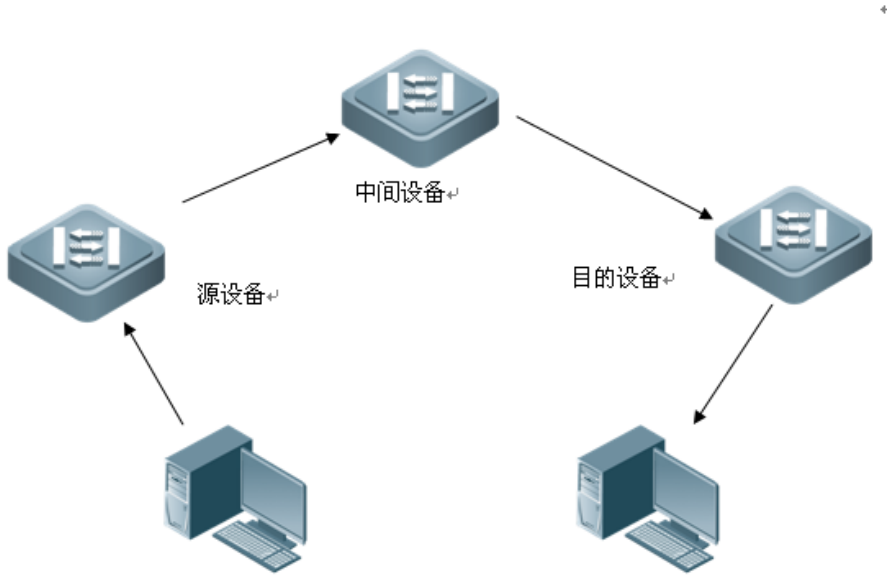
6 RSPAN

6.1 概述

远程端口镜像(RSPAN)是本地端口镜像(SPAN)的扩展，远程端口镜像突破了源端口和目的端口必须在同一台设备上的限制，使源端口和目的端口之间可以跨越多个网络设备。这样网络管理员就可以坐在中心机房通过分析仪观测远端被镜像端口的数据报文。

RSPAN 实现的功能是将所有的被镜像报文通过一个特殊的 RSPAN VLAN(称为 Remote VLAN)传递到远端镜像设备的目的端口，典型应用拓扑如下所示：

图 1-1 RSPAN 典型应用拓扑图



图中各设备的角色分为三种：

- 源交换机：远程镜像源端口所在的交换机，负责将源端口的报文复制一份从源交换机的输出端口输出，通过 Remote VLAN 进行转发，传输给中间交换机或目的交换机。
- 中间交换机：网络中处于源交换机和目的交换机之间的交换机，通过 Remote VLAN 把镜像报文传输给下一个中间交换机或目的交换机。如果源交换机与目的交换机直接相连，则不存在中间交换机。
- 目的交换机：远程镜像目的端口所在的交换机，将从 Remote VLAN 接收到的镜像报文通过镜像目的端口转发给监控设备。

各个交换机上参与 RSPAN 的端口如下所示。

交换机	参与镜像的端口	作用
源交换机	源端口(Source Port)	被监测的用户端口，通过本地端口镜像把用户数据报文复制到指定的输出端口，源端口可以有多个
	输出端口	将镜像报文发送到中间交换机或者目的交换机

中间交换机	普通端口	将镜像报文发送到目的交换机。 建议中间交换机上配置两个 Trunk 端口，和两侧的设备相连
目的交换机	源端口	接收远程镜像报文
	镜像目的端口(Destination port)	远程镜像报文的监控端口

为了实现远程端口镜像功能，需要定义一个特殊的 VLAN，称之为 Remote VLAN。这个 VLAN 只传输镜像报文，不能用来承载正常的业务数据。所有被镜像的报文通过该 VLAN 从源交换机传递到目的交换机的指定端口，实现在目的交换机上对源交换机的远程端口的报文进行监控的功能。

- 在源交换机、中间交换机和目的交换机上，RSPAN 与本地 SPAN 功能可以共存，互不冲突。
- 远程镜像 Remote VLAN 内的报文不影响设备的 CPU 利用率
- 支持指定镜像目的口允许或不允许对外通讯，默认不允许对外通讯。
- Remote VLAN 不能是 VLAN 1，也不能是 Private VLAN。
- Remote VLAN 不参与 GVRP。

6.2 配置RSPAN

- 配置准备
- 源交换机上的配置
- 中间交换机上的配置
- 目的交换机上的配置
- 基于流的 RSPAN 配置
- 配置举例

6.2.1 配置准备

- 确定源交换机、中间交换机、目的交换机
- 确定镜像源端口、镜像目的端口、Remote VLAN
- 通过配置保证 Remote VLAN 内从源交换机到目的交换机的二层互通性
- 确定被监控报文的方向
- 启用 Remote VLAN

6.2.2 源交换机上的配置

- RSPAN 会话
- 源端口

- 输出端口
- Remote VLAN
- VSPAN 配置
- 配置步骤

RSPAN 会话

RSPAN 会话具有本地 SPAN 会话相同的特性，具体见 SPAN 配置指南。

源端口

源端口也被称为被监控口，在 RSPAN 会话中，源端口上的数据流被监控，用于网络分析或故障排查。在单个 RSPAN 会话中，用户可以监控输入、输出或双向数据流，且源端口的个数没有限制。

源端口具有以下特性：

- 源端口可以是 switched port，routed port 或 AP(Aggregate Port)；
- 支持将源设备上的多个源端口镜像到指定的输出端口；
- 源端口与输出端口不能为同一端口；
- 当镜像源端口为三层接口时，监控的报文包括二层报文和三层报文；
- 在双向监控多个端口的情况下，一份报文由一个端口进入，从另外一个端口输出，只要有监控到一份报文视为正确；
- 当启用 STP 的端口处于 block 状态时，该端口输入、输出的报文能够被监控到；
- 源端口和目的端口可以属于同一 VLAN，也可以属于不同 VLAN。

输出端口

RSPAN 镜像数据流从源设备的输出端口向中间设备广播出去，输出端口具有以下特性：

- 输出端口可以是 switched port，routed port 或 AP(Aggregate Port)。
- 输出端口只能属于一个 RSPAN 会话。

Remote VLAN

RSPAN 镜像的数据流通过 Remote VLAN 进行广播，这个 VLAN 只传输镜像报文，不能用来承载正常的业务数据。所有被镜像的报文通过该 VLAN 从源交换机传递到目的交换机的指定端口，实现在目的交换机上对源交换机的远程端口的报文进行监控的功能。

Remote VLAN 具有以下特性：

- Remote VLAN 不能是 VLAN 1，也不能是 Private VLAN。
- 一个 Remote VLAN 对应一个 RSPAN session。

VSPAN 配置

VSPAN 是 VLAN SPAN 的简称，是指将某些 VLAN 的数据流作为数据源镜像到目的设备的目的端口。

VSPAN 具有以下特性：

- 可以指定某个 VLAN 作为镜像的数据源，这个 VLAN 不能是 Remote VLAN。配置命令为 **monitor session** *session-num* **source vlan** *vlan-id* [rx | tx | both]。
- 可以指定某些 VLAN 作为镜像的数据源，这些 VLAN 不能是 Remote VLAN。配置命令为 **monitor session** *session-num* **filter vlan** *vlan-id-list*。

源交换机上的配置步骤

源设备的配置步骤如下所示：

命令	作用
Ruijie# **configure**	进入全局配置模式
Ruijie(config)# **vlan** *vlan-id*	进入 Vlan 配置模式
Ruijie(config-Vlan)# **remote-span**	设置 Vlan 为 remote-span Vlan
Ruijie(config-Vlan)# **exit**	退到全局配置模式
Ruijie(config)# **monitor session** *session_num* **remote-source**	配置远程源镜像
Ruijie(config)# **monitor session** *session-num* **source interface** *interface-name*[**rx | tx | both**]	配置远程镜像源端口(源口的 rx，tx 可以配置到同一个目的口，也可以配置到不同的目的口，但每一个只能配置到一个目的口)
Ruijie(config)#**monitor session** *session_num* **destination remote vlan** *remote_vlan-id* **interface** *interface-name* [**switch**]	配置远程源镜像组的 Remote VLAN **switch** 关键字表示目的口参与交换
Ruijie(config)# **monitor session** *session_number* **source interface** *interface-id* **rx acl** *name*	设定需要镜像的流所匹配的 **acl** *name*

建议不要将普通端口加入 Remote VLAN。

不要在与中间交换机或目的交换机相连的端口上配置镜像源端口，否则可能引起网络内的流量混乱。

6.2.3 中间交换机上的配置

RSPAN 会话的中间设备确保远程镜像 VLAN 内的报文的透传，配置过程如下：

命令	作用
Ruijie# **configure**	进入全局配置模式
Ruijie(config)# **vlan** *vlan-id*	进入 vlan 配置模式
Ruijie(config-vlan)# **remote-span**	设置 vlan 为 remote-span Vlan
Ruijie(config-vlan)# **exit**	退到全局配置模式

6.2.4 目的交换机上的配置

目的端口

RSPAN 远程设备将 Remote VLAN 接收到的镜像报文通过目的端口转发给监控设备。目的端口具有如下特性：

目的端口可以是 switched port，routed port 或 AP(Aggregate Port)。

用户可以指定镜像目的端口允许或不允许对外通讯，默认状态是不允许对外通讯。目的端口处于不允许通讯状态下时，既不允许转发其他端口的数据报文，也不允许转发 CPU 发出的报文。

☑ NBS200F 系列产品不支持 AP(Aggregate Port)口作为输出端口。

配置步骤

命令	作用
Ruijie# **configure**	进入全局配置模式
Ruijie(config)# **vlan** *vlan-id*	进入 vlan 配置模式
Ruijie(config-vlan)# **remote-span**	设置 vlan 为 remote-span vlan
Ruijie(config-vlan)# **exit**	退到全局配置模式
Ruijie(config)# **monitor session** *session_num* **remote-destination**	配置远程目的镜像
Ruijie(config)# **monitor session** *session-num* **destination remote** vlan *vlan-id* **interface** *interface-name* [**switch**]	配置 Remote VLAN 和远程镜像目的端口 **switch** 关键字表示目的口参与交换
Ruijie(config)# **interface** *interface-name*	进入远程镜像目的端口
Ruijie(config-if)# **switchport access vlan** *vid* | **switchport trunk native vlan** *vid*	vid 表示 remote-span vlan 的 vid 如果目的口是 access 口，则把它加入 remote-span vlan 如果目的口是 trunk 口，则把它加入 remote-span vlan，并且将 remote-span vlan 设置成它的 native vlan

6.2.5 基于流的RSPAN配置

RSPAN 是对本地 SPAN 的扩展，因此 RSPAN 同样也支持基于流的镜像(具体配置见镜像的配置指南)。

基于流的 RSPAN 不影响正常通讯。

用户可以在 RSPAN 源设备上配置源端口的 in 方向的 ACL，支持标准 ACL、扩展 ACL、MAC ACL、自定义 ACL。

用户可以在 RSPAN 源设备上配置源端口的 in 方向的端口 ACL，可以在 RSPAN 目的设备上配置目的端口 out 方向的端口 ACL。

用户可以在 RSPAN 源交换机上基于 Remote VLAN 应用 out 方向的 ACL，在 RSPAN 目的交换机上基于 Remote VLAN 应用 in 方向的 ACL。

6.2.6 显示RSPAN会话

命令	作用
show monitor	显示镜像

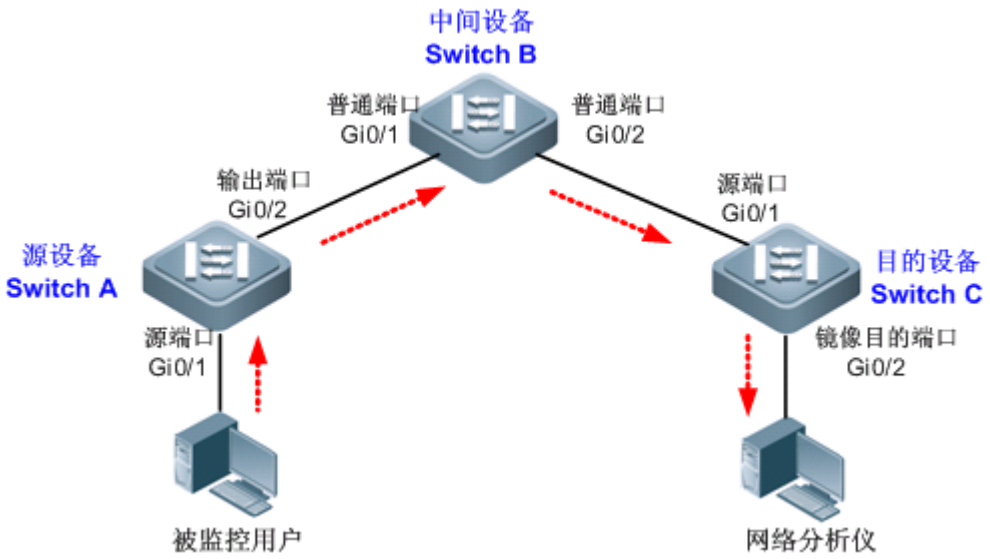
示例：

```
Ruijie# show monitor
sess-num: 1
src-intf:
GigabitEthernet 0/4 frame-type Both
dest-intf:
GigabitEthernet 0/6
remote vlan 3
```

6.3 RSPAN典型配置用例

拓扑图

图 1-2 RSPAN 的应用拓扑



应用需求

- 网络分析仪可以通过远程镜像监控用户。
- 设备之间均能正常交换数据。

配置要点

- 在源设备（本例为 Switch A）、中间设备（本例为 Switch B）、目的设备（本例为 Switch C）上配置 Remote VLAN。
- 在源设备上，配置直连用户的端口（本例为 Gi 0/1）为源端口，与中间设备相连的端口（本例为 Gi 0/2）为输出端口，并配置输出端口可交换功能。
- 在中间设备上，与源设备、目的设备相连的端口（本例为 Gi 0/1 和 Gi 0/2）仅需配置为普通端口。
- 在目的设备上，与中间设备相连的端口（本例为 Gi 0/1）作为源端口，仅需配置为普通端口，与网络分析仪相连的端口（本例为 Gi 0/2）配置为镜像目的端口，并配置镜像目的端口可交换功能。

通过源设备的输出端口转发的镜像数据流，可以在 Remote VLAN 中广播，则除源设备外的任意设备端口加入 Remote VLAN，便可对源端口进行监控，实现一对多远程镜像。如果在目的设备上指定一个镜像目的端口，则镜像数据流仅转发到该目的端口。

配置步骤

第一步，配置 Remote VLAN。

！在 Switch A 上创建 VLAN 7，设置为 Remote VLAN。

```
SwitchA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)#vlan 7
SwitchA(config-vlan)#remote-span
SwitchA(config-vlan)#exit
```

！在 Switch B、C 上配置同上。

第二步，配置 RSPAN 源设备。

！在 Switch A 上，配置端口 Gi 0/2 为 Trunk Port，用于连接 Switch B。

```
SwitchA(config)#interface gigabitEthernet 0/2
SwitchA(config-if-GigabitEthernet 0/2)#switchport mode trunk
SwitchA(config-if-GigabitEthernet 0/2)#exit
```

！在 Switch A 上，创建 RSPAN Session 1，设置为源设备，并设置端口 Gi 0/1 为源端口，端口 Gi 0/2 为输出端口。

```
SwitchA(config)#monitor session 1 remote-source
SwitchA(config)#monitor session 1 source interface gigabitEthernet 0/1 both
SwitchA(config)#monitor session 1 destination remote vlan 7 interface gigabitEthernet 0/2 switch
```

第三步，配置 RSPAN 中间设备

！在 Switch B 上，配置端口 Gi 0/1 和 Gi 0/2 为 Trunk Port。

```
SwitchB(config)#interface range gigabitEthernet 0/1-2
SwitchB(config-if-range)#switchport mode trunk
```

第四步，配置 RSPAN 目的设备

！在 Switch C 上，配置端口 Gi 0/1 为 Trunk Port，用于连接 Switch B 作为源端口。

```
SwitchC(config)#interface gigabitEthernet 0/1
SwitchC(config-if-GigabitEthernet 0/1)#switchport mode trunk
```

！在 Switch C 上，创建 RSPAN Session，设置为目的设备，并设置端口 Gi 0/2 为镜像目的端口。

```
SwitchC(config)#monitor session 1 remote-destination
SwitchC(config)#monitor session 1 destination remote vlan 7 interface gigabitEthernet 0/2 switch
```

验证结果

第一步，查看设备配置信息。

！Switch A 的配置

```
SwitchA#show running-config
!
vlan 7
 remote-span
!
interface GigabitEthernet 0/2
 switchport mode trunk
!
monitor session 1 remote-source
monitor session 1 destination remote vlan 7 interface GigabitEthernet 0/2 switch
monitor session 1 source interface GigabitEthernet 0/1 both
!
```

！Switch B 的配置

```
SwitchB#show running-config
!
vlan 7
 remote-span
!
interface GigabitEthernet 0/1
 switchport mode trunk
!
interface GigabitEthernet 0/2
 switchport mode trunk
```

！Switch C 的配置

```
SwitchC#show running-config
!
vlan 7
 remote-span
!
interface GigabitEthernet 0/1
 switchport mode trunk
```

```
!
monitor session 1 remote-destination
monitor session 1 destination remote vlan 7 interface GigabitEthernet 0/2 switch
```

第二步，查看设备的 RSPAN 信息

！查看 Switch A

```
SwitchA#show monitor
sess-num: 1                                          //RSPAN Session
span-type: SOURCE_SPAN                               //RSPAN 源设备
src-intf:                                            //RSPAN 源端口信息
GigabitEthernet 0/1         frame-type Both
dest-intf:                                           //RPSAN 输出端口信息
GigabitEthernet 0/2
remote vlan 7
mtp_switch on                                  //允许输出端口正常交换数据
```

！查看 Switch C

```
SwitchC#show monitor
sess-num: 1                                          //RSPAN Session
span-type: DEST_SPAN                                 //RSPAN 目的设备
dest-intf:                                           //RSPAN 目的端口信息
GigabitEthernet 0/2
remote vlan 7
mtp_switch on                                  //允许目的端口正常交换数据
```