配置手册

RG-S2300 系列
安全接入交换机
RGOS 10.2(5)

版权声明

免责声明

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

前 言

版本说明

本手册对应的软件版本为：RGOS®10.2(5)版。

读者对象

本书适合下列人员阅读

- 网络工程师
- 技术推广人员
- 网络管理员

本书约定

1. 通用格式约定

宋体：正文采用 5 号宋体。

注意、说明等提示内容前后增加线条与正文隔离。

终端信息显示格式：英文用 `Courier New` ，中文用宋体，文字大小 5 号，表示屏幕输出信息。信息中夹杂的用户从终端输入的信息，采用**加粗**字体表示。

2. 命令行格式约定

命令行字体采用用 Arial，具体相关格式意义如下：

粗体：命令行关键字（命令中保持不变必须照输的部分）采用加粗字体表示。

斜体：命令行参数（命令中必须由实际值进行替代的部分）采用斜体表示

[ ] ：表示用[ ] 括起来的部分，在命令配置时是可选的。

{ x | y | ... }：表示从两个或多个选项中选取一个。

[x | y | ...]：表示从两个或多个选项中选取一个或者不选。

//：由双斜杠开始的行表示为注释行。

3. 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： 注意、警告、提醒操作中应注意的事项。

说明： 说明、提示、窍门、对操作内容的描述进行必要的补充

说明：

1) 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

2) 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。

3) 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。

第1章 命令行界面配置

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。

本章节主要包括以下内容：

- 命令模式
- 获得帮助
- 简写命令
- 使用命令的 **no** 和 **default** 选项
- 理解 CLI 的提示信息
- 使用历史命令
- 使用编辑特性
- CLI 输出信息的过滤和查找
- 访问 CLI

1.1. 命令模式

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

在命令提示符下输入问号键（?）可以列出每个命令模式支持使用的命令。

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

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

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

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

命令模式概要：

命令模式	访问方法	提示符	离开或访问下一模式	关于该模式
User EXEC（用户模式）	访问网络设备时首先进入该模式。	Ruijie>	输入 **exit** 命令离开该模式。 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. 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	说明
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

注意：

对于所有的命令，如果遇到 word/string 和关键字都允许执行的情况下，优先匹配关键字，和具体的功能无关。比如：

Ruijie(config)#aaa domain ?
 WORD　Specific domain configure
 default　Default domain configure
 enable　Domain enable configure

这时，执行 aaa domain d 命令，将优先匹配关键字 default，此时执行的命令是 aaa domain default 。

1.3. 简写命令

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

例如 **show configuration** 命令可以写成：

```
Ruijie# show conf
```

1.4. 使用命令的 no 和 default 选项

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

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

1.5. 理解 CLI 的提示信息

下表列出了用户在使用 CLI 管理网络设备时可能遇到的错误提示信息。

常见的 CLI 错误信息：

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

1.6. 使用历史命令

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

从历史命令记录重新调用输入过的命令，执行下表中的操作：

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

注意:

标准的终端支持方向键，例如 VT100 系列。

1.7. 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。包括：

- 编辑快捷键
- 命令行滑动窗口

1.7.1.编辑快捷键

下表列出编辑快捷键：

功能	快捷键	说明
在编辑行内移动光标。	左方向键或 Ctrl-B	光标移到左边一个字符。
	右方向键或 Ctrl-F	光标移到右边一个字符。
	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	删除光标所在的字符。
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。

1.7.2.命令行滑动窗口

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

编辑命令行时光标移动操作如下表：

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

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

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

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

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

注意:

默认的终端行宽是 80 个字符。

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

1.8. CLI 输出信息的过滤和查找

1.8.1. Show 命令的查找和过滤

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

命令	说明
Ruijie# **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。

注意：

1) 支持在任意模式下执行 **Show** 命令

2) 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	说明
Ruijie# **show** *any-command* | **exclude** *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。
Ruijie# **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。

注意：

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

1.9. 使用命令别名

系统提供命令别名功能，可以指定任意单词作为命令的别名，例如：将单词

"mygateway"定义为"ip route 0.0.0.0 0.0.0.0 192.1.1.1"的别名，

则输入这个单词就相当于输入后面的整个字符串。

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

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

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

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

**command-alias=original-command*

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

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

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

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

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

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

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

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

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

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

命令别名在使用时必须完整输入，否则不能被识别。

使用 **show aliases** 命令可以查看系统中的别名设置。

1.9.1.访问 CLI

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

第2章 交换机基础管理配置

2.1. 概述

本章描述对我司产品的一些管理操作：

- 通过命令的授权控制用户访问
- 登录认证控制
- 系统时间配置
- 定时重启
- 系统名称和命令提示符
- 标题配置
- 查看系统信息
- 控制台速率配置
- 在网络设备上使用 telnet
- 连接超时设置
- 批处理执行文件中的命令
- 服务开关设置

说明：

有关本节引用的 CLI 命令的详细使用信息及说明，请参照《配置交换机管理命令》。

2.2. 通过命令的授权控制用户访问

2.2.1. 概述

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

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

2.2.2.缺省的口令和特权级别配置

缺省没有设置任何级别的口令，缺省的级别是 15 级。

2.2.3.设置和改变各级别的口令

我司产品提供下面的命令用于设置和改变各级别的口令。

命令	目的
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# **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。

2.2.4.配置多个特权级别

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

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

2.2.4.1. 命令授权配置

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

你可以使用如下命令对命令进行授权：

命令	目的
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。**level** 1 是普通用户级别，**level** 15 是特权用户级别，在各用户级别间切换可以使用 **enable/disable** 命令。 *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。

2.2.4.2. 命令授权配置实例

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

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

进入 1 级，可以看见命令和子命令：

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

```
<cr>
```

下面是将 reload 命令及其子命令的权限恢复为默认值的配置过程：

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

进入 1 级，命令权限已经被收回：

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

2.2.5.配置线路（line）口令保护

我司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	目的
Ruijie(config-line)# **password** *password*	指定 **line** 线路口令
Ruijie(config-line)# **login**	启用 **line** 线路口令保护

说明：

如果没有配置登录认证，即使配置了 **line** 口令，登录时，**line** 层口令认证会被忽略。登录认证在下一节介绍。

2.2.6.支持会话锁定

我司产品支持通过 **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：

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

2.3. 登录认证控制

2.3.1. 概述

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

利用 RADIUS 服务器对用户登录时的用户名和密码进行控制，这样网络设备不再用本地保存的密码信息进行认证，而是将加密后的用户信息发送到 RADIUS 服务器上进行验证，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。

2.3.2. 配置本地用户

我司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）

2.3.3. 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**	非 AAA 模式下，设置线路登录进行本地认证
Ruijie(config-line)# **login authentication** {**default** | *list-name*}	AAA 模式下，设置线路登录进行 AAA 认证。认证时使用 AAA 方法列表中的认证方法，包括 Radius 认证、本地认证、无认证等。

说明：

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

2.4. 系统时间配置

2.4.1. 概述

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

2.4.2. 设置系统时间

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

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

命令	作用
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 2008-1-30，05:54:43

```
Ruijie# clock set 05:54:43 1 30 2008        //设置系统时间和日期
Ruijie# show clock                          //确认修改系统时间生效
05:54:43 CHN-BJ Wed 2008-01-30
```

2.4.3. 查看系统时间

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

下：

```
Ruijie# sh clock                                    //显示当前系统时间
05:54:43 CHN-BJ Wed 2008-01-30
```

2.4.4.硬件时钟更新

一些平台使用硬件时钟（calendar）来补充软件时钟，硬件时钟是不间断持续运转的，因为硬件时钟是走电池的，即使设备关闭或重启状态下也在运转。
如果硬件时钟和软件时钟不同步，软件时钟是比较精确的，采用该命令将软件时钟的日期和时间复制给硬件时钟。

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

命令	作用
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
```

2.5.定时重启

2.5.1.概述

本节描述如何使用 **reload** [modifiers]命令制定重启计划（scheme），以实现系统定时重启。定时重启功能，它在某些场合下(比如出于测试目的或其它需要)可以为用户提供操作上的便利。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：

1. **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*。

2. **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*。

3. **reload cancel**

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

说明:

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

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

2.5.2.指定系统在某个时间重启

在特权模式下，通过如下命令，可以指定系统在将来的某个时间重启：

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

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

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

2.5.3.指定系统一段时间后重启

在特权模式下，使用如下命令指定系统一段时间后重启：

命令	作用
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.
```

2.5.4.直接重启

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

2.5.5.删除已设置的重启策略

在特权模式下，使用如下命令删除已设置的重启计划：

命令	作用
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，则用户会看到错误操作的提示信息。

2.6.系统名称和命令提示符

2.6.1.概述

为了管理的方便，你可以为一台网络设备配置系统名称(System Name)来标识它。同时如果你还没有为 CLI 配置命令提示符，则系统名称（如果系统名称超过

32 个字符，则截取其前 32 个字符)将作为默认的命令提示符，提示符将随着系统名称的变化而变化。默认情况下，以具体的设备名称作为系统名称，例如”S2924G”、”R2692”等。

2.6.2.配置系统名称

我司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 255 个字节。

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

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

2.6.3.配置命令提示符

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

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

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

2.7. 标题配置

2.7.1. 概述

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

2.7.2. 配置每日通知

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

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

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

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

2.7.3. 配置登录标题

您可以通过以下全局配置模式的命令来设置登录标题信息：

命令	作用

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

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

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

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

2.7.4.显示标题

标题的信息将在你登录网络设备时显示，下面是一个标题显示的例子：

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

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

2.8.查看系统信息

2.8.1.概述

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

2.8.2.查看系统、版本信息

系统信息主要包括系统描述，系统上电时间，系统的硬件版本，系统的软件版本，系统的 Ctrl 层软件版本，系统的 Boot 层软件版本，产品序列号（仅对于有烧写过序列号的设备）。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
Ruijie# **show version**	显示系统、版本信息

2.8.3.显示硬件实体信息

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

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

2.8.4.查看系统默认启动的主程序名

你可以在命令行使用 **show mainfile** 命令来显示系统默认启动的主程序名，显示的格式如下：

```
Ruijie# show mainfile
MainFile name: rgos.bin.
```

2.9.控制台速率配置

2.9.1.概述

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

设备的终端的速率设置必须和网络设备的控制台的速率一致。

2.9.2.设置控制台速率

在线路配置模式下，您可以使用以下命令来设置控制台的速率：

命令	作用
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
```

2.10. 在网络设备上使用 telnet

2.10.1. 概述

Telnet 在 TCP/IP 协议族中属于应用层协议，它给出了通过网络提供远程登录和虚拟终端通讯功能的规范。Telnet Client 服务为已登录到本网络设备上的本地用户

或远程用户提供使用本网络设备的 Telnet Client 程序访问网上其他远程系统资源的服务。如下图所示用户在微机上通过终端仿真程序或 Telnet 程序建立与网络设备 A 的连接后，可通过输入 telnet 命令再登录设备 B，并对其进行配置管理。

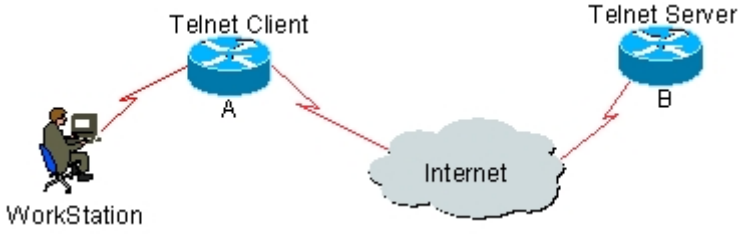


图 1

2.10.2. 使用 Telnet Client

您可以通过网络设备上的 **telnet** 命令登录到远程设备上去：

命令	作用
Ruijie# **telnet** *host-ip-address*	通过 **telnet** 登录到远程设备，可以是主机名或 IP 地址。

下面的例子是如何建立 **Telnet** 会话并管理远程网络设备，远程网络设备的 ip 地址是 192.168.65.119：

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

2.11. 连接超时设置

2.11.1. 概述

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

2.11.2. 连接超时

当前已接受的连接，在指定时间内，没有任何输入信息，服务器端将中断此连接。

我司产品提供 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** *20*	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。

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
```

2.11.3. 会话超时

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

我司产品提供 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** *20*	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。

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

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

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

说明：

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

2.13. 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（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**	打开 Http Server

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

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

2.14. 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。以下例子在交换机上打开 Http Server，设置服务端口为 8080，并采用本地用户名进行登录认证：

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

第3章 LINE 模式配置

3.1. 概述

本章描述对 LINE 的一些操作：

- 进入 LINE 模式
- 增加/减少 LINE VTY 数目
- 配置 LINE 下可以通讯的协议

3.2. LINE 模式配置

3.2.1. 进入 LINE 模式

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

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

3.2.2. 增加/减少 LINE VTY 数目

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

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

3.2.3. 配置 Line 下的可通讯协议

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

协议进行通讯。

命令	说明
configure terminal	进入配置模式
Line vty *line number*	进入 Line 配置模式
transport input {**all** | **ssh** | **telnet** | **none**}	配置对应 Line 下可以通讯的协议
no transport input	配置 LINE 下不允许任何协议通讯
default transport input	恢复 LINE 下的通讯协议为默认配置

3.2.4.配置 Line 下的访问控制列表

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

命令	说明
configure terminal	进入配置模式
Line vty *line number*	进入 Line 配置模式
access-class *access-list-number* {**in | out**}	配置对应 Line 下的访问控制列表
no access-class *access-list-number* {**in |out**}	取消 Line 下配置的访问控制列表

第4章 系统升级维护配置

4.1. 概述

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

4.2. 升级维护方法

我们将从以下几个小节描述如何升级维护设备的文件

- 通过 TFTP 协议传输文件
- 通过 XMODEM 协议传输文件

4.2.1. 通过 TFTP 协议传输文件

一种是从主机端下载文件到设备，另一种是从设备上传文件到主机端。

在 CLI 命令模式下，按如下步骤设置来完成文件的下载：

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

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

在 CLI 命令模式下，按如下步骤设置来完成文件的上传：

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

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

4.2.2.通过 XMODEM 协议传输文件

一种是从主机端下载文件到设备，另一种是从设备上传文件到主机端。

在 CLI 命令模式下，按如下步骤设置来完成文件的下载：

下载前，首先通过 Windows 超级终端登录到设备的带外管理界面；然后在特权模式下使用以下命令下载文件；而后在本地主机的 Windows 超级终端中，选择“传送”菜单中的“发送文件”功能，如图 1 所示：

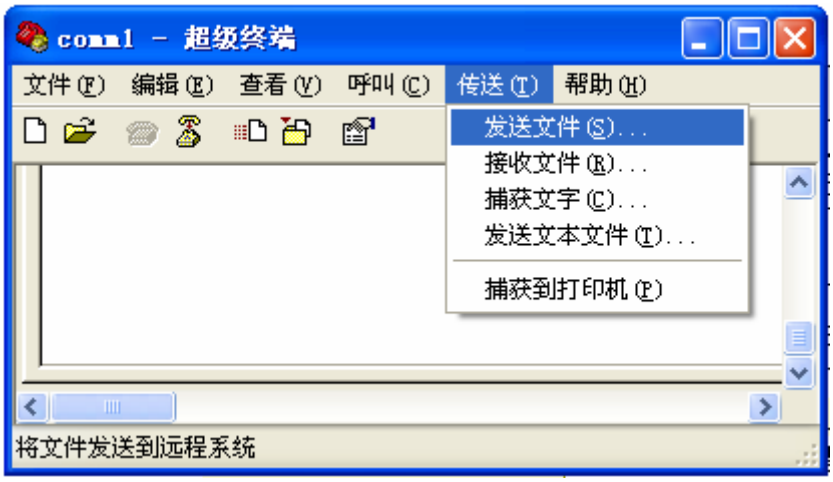


图 1

在弹出的对话框的文件名选择本地主机要下载的文件，协议选择“Xmodem”，点击“发送”，则 Windows 超级终端显示发送的进度以及数据包。如图 2 所示：

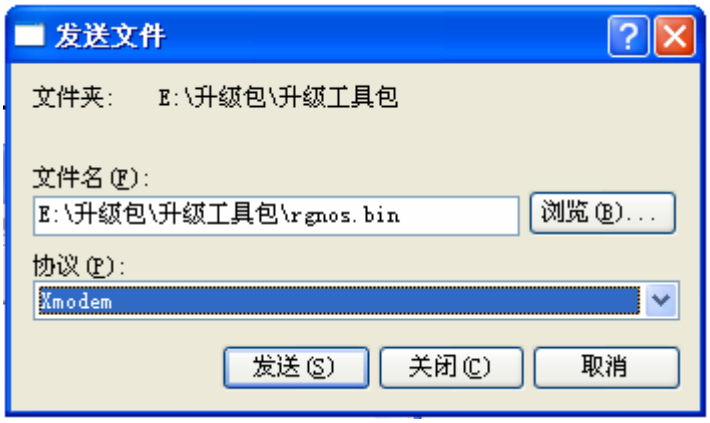


图 2

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

在 CLI 命令模式下，按如下步骤设置来完成文件的上传：

上传前，首先通过 Windows 超级终端登录到设备的带外管理界面；然后在特权模

式下使用以下命令上传文件；最后在本地主机的 Windows 超级终端中，选择“传送”菜单中的“接收文件”功能。如图 3 所示：

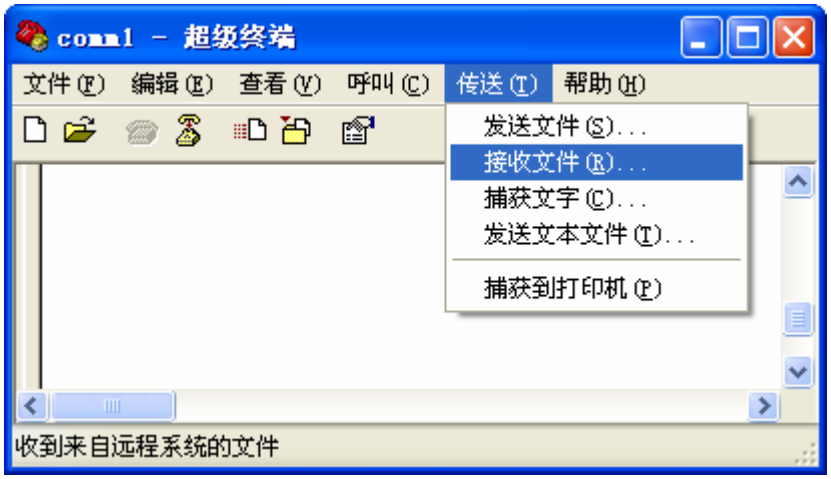


图 3

在弹出的对话框选择上传文件的存储位置，接收协议选择“Xmodem”，点击“接收”，超级终端会进一步提示用户本地存储文件的名称，点击“确认”后开始接收文件。如图 4 所示：

图 4

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

4.2.3.升级系统

不论是盒式设备还是机箱设备，使用都可以使用上述的 tftp 或者 xmodem 将升级文件传输到设备上。传输成功后，重新启动设备，升级文件就会自动完成当前系

统的检测和升级，这个过程不需要人工干预和介入。

升级文件在盒式设备和机箱设备上的升级动作有所不同：

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

2）机箱设备包含有管理板，线卡以及多业务卡，要通过一个升级文件完成整套系统的升级操作。首先待管理板端升级完毕，系统复位。机器再次启动时，版本自动同步功能会启动起来，完成线卡和多业务卡的系统升级。

自动升级功能：是运行于主管理板端的一个功能，会对系统中存在的从管理板，线卡和多业务卡进行版本一致性检查，当发现他们的版本和主管理板中对应的单板版本不一致时，就将他们的单板升级文件传送过去，完成他们的升级，以使整个系统的版本保持一致。

注意：

任何时候升级机箱设备的主管理板，都会同时升级从管理板，从而保持版本的一致性。升级线卡的操作会使整个系统中插入的线卡同时得到升级。在升级结束提示前不可断电，否则可能导致升级程序丢失。
在机箱设备升级未完成前，可通过**show version**检查所有线卡和管理板的软件版本是否与升级的目标版本一致的方式检查升级是否完成，不能进行主备切换（例如：**redundancy force-switchover**），否则会导致升级失败而退回原始版本。

- 通过升级文件来升级机箱设备：

1） 确认要载入的升级文件的文件名为 **rgos.bin**

2） 使用上述 **copy** 命令，将此文件下载到设备上

3） 如果设备上存在从管理板，需要等待主从管理板的主程序升级成功，成功时将有如下提示：

```
Upgrade Slave CM MAIN successful!!
Upgrade CM MAIN successful!!
```

1） 执行一次整机复位操作

2） 系统再次启动后，升级文件会开始运行，将会看到类似如下提示：

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

3） 在升级操作完成后，将会看到类似如下提示：

```
Installing process finished ......
Restart machine operation is permited now !!!!!!
```

4） 升级文件运行完毕后系统会自动复位，出现如下提示：

```
System restarting, for reason 'Upgrade product !'.
```

5） 系统再次启动后，管理板的整个系统会完成升级，然后加载管理板的单板升级文件运行，这还会有步骤 5 和 6 的提示信息，但不会有步骤 7 的提示信息，取而代之的是：

```
System load main program from install package ......
```

直接从升级文件中加载管理板的主程序运行

6） 主程序正常运行后，自动升级功能就会启动，如果机箱中有从管理板或者其他模块会看到如下提示：

```
A new card is found in slot [1].
System is doing version synchronization checking ......
Current software version in slot [1] is synchronous.
System needn't to do version synchronization for this card ......
```

或者如下提示：

```
System is doing version synchronization checking ......
Card in slot [3] need to do version synchronization ......
```

其他打印信息

```
Version synchronization begain ......
Keep power on, don't draw out the card and don't restart your
machine before finished !!!!!!
```

其他打印信息

```
Transmission is OK, now, card in slot [3] need restart ...
Software installation of card in slot [3] is in process ......
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!
Software installation of card in slot [3] has finished
successfully ......
The version synchronization of card in slot [3] get finished
successfully.
```

上述两种情况一种表示，线卡的版本已经是同步的不需要再次自动升级，另一种表示线卡的版本，还需要自动升级，然后做升级操作。

系统会依次对从板和每一个模块完成上述操作。

根据提示等待系统完成所有模块的版本一致检查和升级操作，系统便可正常工作了。

注意:

在升级或者自动升级过程中，会有不允许重启的提示，一旦出现类似提示，请务必不要断电或者复位系统，也不要随便插拔其他模块。

说明：

对于热插入的模块系统会有同样的自动升级检查操作。

- 通过升级文件来升级盒式设备：

盒式设备的升级只需要完成上述步骤的 1－7，然后系统自行复位后就会正常运行了。

第5章 网络通信检测工具

5.1. 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*]]	**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，如果应答数据包与请求数据包相匹配（如果数据部分长度不相等，取公共部分进行匹配），则显示‘!’符号；如果应答数据包与请求数据包不匹配，则显示‘C’符号；如果没有应答，则显示‘.’符号。最后输出一个统计信息。以下为普通 ping 的实例：

```
Ruijie# ping 192.168.5.1
Sending 5, 100-byte ICMP Echoes to 192.168.5.1, timeout is 2
seconds:
< press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10
ms
```

扩展的 Ping 功能，只能在特权用户模式下执行。在扩展 Ping 中，可以指定发送数据包的个数、长度、超时的时间等等。和普通的 Ping 功能一样，最后也输出一个统计信息， 以下为一个扩展 Ping 的实例：

```
Ruijie# ping 192.168.5.197 length 1500 ntimes 100 data ffff source
192.168.4.190 timeout 3
Sending 100, 1000-byte ICMP Echoes to 192.168.5.197, timeout
is 3 seconds:
  < press Ctrl+C to break >
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
Success rate is 100 percent (100/100), round-trip min/avg/max
= 2/2/3 ms
Ruijie#
```

5.2. 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，并送回一个地址不可达的错误数据包给源地址。根据这个规则，Traceroute 命令的执行过程是：首先给目的地址发送一个 TTL 为 1 的数据包，第一个网关便送回一个 ICMP 错误消息，以指明此数据包不能被发送，因为 TTL 超时，之后将数据包的 TTL 域加 1 后重新发送，同样第二个网关返回 TTL 超时错误，这个过程一直继续下去，直到到达目的地址，记录每一个回送 ICMP TTL 超时信息的源地址，便记录下了数据从源地址到达目的地址，IP 数据包所经历的整个完整的路径。

Traceroute 命令可以在普通用户模式和特权用户模式下执行，具体的命令格式如下：

命令	功能
Ruijie**# traceroute** [*protocol*] [*destination* [**probe** *probe*] [**ttl** *minimum maximum*] [**source** *source*] [**timeout** *seconds*]]	跟踪数据包发送网络路径

以下为应用 Traceroute 的两个例子，一个为网络连接畅通，一个为网络连接存在某些网关不通的情况。

1．网络畅通的 Traceroute 例子：

```
Ruijie# traceroute 61.154.22.36
  < press Ctrl+C to break >
Tracing the route to 61.154.22.36

1     192.168.12.1       0 msec  0 msec  0 msec
2     192.168.9.2        4 msec  4 msec 4 msec
3     192.168.9.1        8 msec  8 msec  4 msec
4     192.168.0.10       4 msec  28 msec  12 msec
5     202.101.143.130    4 msec  16 msec  8 msec
6     202.101.143.154   12 msec  8 msec  24 msec
7     61.154.22.36      12 msec  8 msec  22 msec
```

从上面的结果可以清楚地看到，从源地址要访问 IP 地址为 61.154.22.36 的主机，网络数据包都经过了哪些网关（1－6），同时给出了到达该网关所花费的时间，这对于网络分析，是非常有用的。

2．网络中某些网关不通的 Traceroute 例子：

```
Ruijie# traceroute 202.108.37.42
< press Ctrl+C to break >
Tracing the route to 202.108.37.42
1     192.168.12.1      0 msec  0 msec  0 msec
2     192.168.9.2       0 msec  4 msec 4 msec
3     192.168.110.1    16 msec  12 msec  16 msec
4     *  *  *
5     61.154.8.129      12 msec  28 msec  12 msec
6     61.154.8.17        8 msec  12 msec  16 msec
7     61.154.8.250      12 msec  12 msec  12 msec
8     218.85.157.222    12 msec  12 msec  12 msec
9     218.85.157.130    16 msec  16 msec  16 msec
10    218.85.157.77     16 msec  48 msec  16 msec
11    202.97.40.65      76 msec  24 msec  24 msec
12    202.97.37.65      32 msec  24 msec  24 msec
13    202.97.38.162     52 msec  52 msec  224 msec
14    202.96.12.38      84 msec  52 msec  52 msec
15    202.106.192.226   88 msec  52 msec  52 msec
16    202.106.192.174   52 msec  52 msec  88 msec
17    210.74.176.158   100 msec  52 msec  84 msec
18    202.108.37.42     48 msec  48 msec  52 msec
```

从上面的结果可以清楚地看到，从源地址要访问 IP 地址为 202.108.37.42 的主机，网络数据包都经过了哪些网关（1－17），并且网关 4 出现了故障。

第6章 接口配置

6.1. 接口类型概述

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

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

6.1.1. 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

6.1.1.1. 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。

6.1.1.1.1.Access Port

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

缺省 VLAN

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

帧的接收与发送

Access Port 发送出的数据帧是不带 TAG 的，且它只能接收以下三种格式的帧：

- Untagged 帧
- VID 为 Access Port 所属 VLAN 的 Tagged 帧

- VID 为 0 的 Tagged 帧

Untagged 帧

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

Tagged 帧

Access 端口接收到的数据帧带有 TAG 时，将按照以下条件进行处理：

- 当 TAG 的 VID（VLAN ID）与缺省 VLAN ID 相同时，接收该数据帧，并在发送时去掉 TAG 标志后发送。
- 当 TAG 的 VID（VLAN ID）为 0 时，接收该数据帧。在 TAG 中，VID＝0 用于识别帧优先级。
- 当 TAG 的 VID（VLAN ID）与缺省 VLAN ID 不同且不为 0 时，丢弃该帧。

6.1.1.1.2.Trunk Port

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

缺省 VLAN

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

注意:

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

帧的接收与发送

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

Untagged 帧

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

Tagged 帧

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

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

说明:

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

6.1.1.1.3.Hybrid 端口

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

6.1.1.2. 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。

注意:

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。

6.1.2.三层接口(L3 interface)

本节主要描述三层接口的类型及相关的定义

- SVI (Switch virtual interface)

6.1.2.1. SVI(Switch virtual interface)

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

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

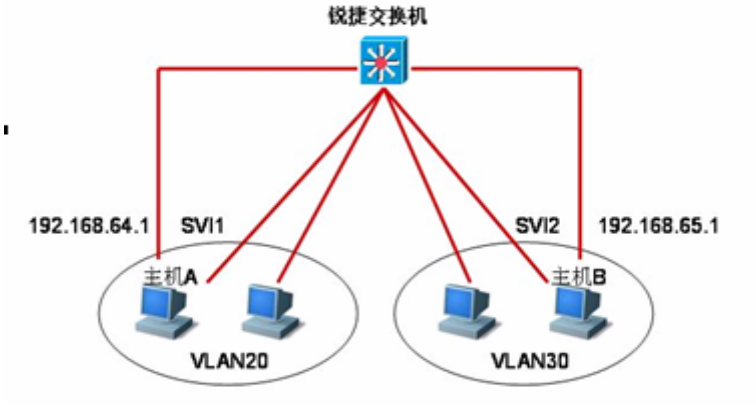


图 1

SVI 可用于二层设备做为 DHCP Client 的相关配置。

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

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

注意：

该系列产品支持 DHCP Client 功能，但不支持 DHCP Server 功能。

具体配置参见下述《配置 SVI》中的相关描述。

6.2. 配置接口

本节描述接口的缺省配置，配置指南，配置步骤，配置实例

6.2.1. 接口编号规则

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

对于 Aggregate Port，其编号的范围为 1－设备支持的 Aggregate Port 个数。

对于 SVI，其编号就是这个 SVI 对应的 VLAN 的 VID。

注意:

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

6.2.2. 接口配置命令的使用

您可在全局配置模式下使用 interface 命令进入接口配置模式。

命令	作用

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

下例给出了进入 Gigabitethernet 2/1 接口的示例：

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

在接口配置模式下您可配置接口的相关属性。

6.2.3.使用 interface range 命令

6.2.3.1. 配置一定范围的接口

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

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

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

有效的接口范围格式：

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

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

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

TenGigabitethernet *slot/{第一个 port} - {最后一个 port}*；

Aggregate Port Aggregate *port 号 - Aggregate port 号*, 范围 1～MAX；

在一个 **interface range** 中的接口必须是相同类型的，即或者全是 fastethernet，gigabitethernet 或者全是 Aggregate Port，或者全是 SVI。

下面的例子是在全局配置模式下使用 **interface range** 命令：

```
Ruijie# configure terminal
Ruijie(config)# interface range fastethernet 1/1 - 10
Ruijie(config-if-range)# no shutdown
Ruijie(config-if-range)#
```

下面的例子是如何使用分隔符号（,）隔开多个 range：

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

6.2.3.2. 配置和使用端口范围的宏定义

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

命令	作用
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
```

6.2.4.选择接口介质类型

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

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

此配置命令只对支持介质选择的端口有效。

配置为 Aggregate Port 成员口的端口，其介质类型必须一致，否则无法加入到 AP 中。Aggregate Port 成员口的端口类型不能改变。

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

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

```
Ruijie# config terminal
```

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

6.2.5.配置接口的描述和管理状态

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

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

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

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

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

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

下面的例子描述如何关闭接口 Gigabitethernet 1/2：

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

6.2.6.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。

以下配置命令只对 Switch 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。 注意： 1000 只对千兆口有效；
Ruijie(config-if)# **duplex** {**auto** | **full** | **half** }	设置接口的双工模式。
Ruijie(config-if)# **flowcontrol** {**auto** | **on** | **off** }	设置接口的流控模式。 注意：当 speed,duplex,flowcontrol 都设为非 auto 模式时，该接口关闭自协商过程

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
```

注意：

S2300 系列交换机，跨芯片和跨堆叠的流控不生效，配置流控时需要注意是否有跨芯片或跨堆叠。

S2300 系列产品光口只能支持千兆，百兆不能 Up

6.2.7.配置接口的 MTU

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

MTU 是指帧中有效数据段的长度，不包括以太网封装的开销。

端口的 MTU 检查只在输入时进行。输出时不会检查 MTU。端口收到的帧，如果长度超过设置的 MTU，将被丢弃。

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

此配置命令只对物理端口有效。SVI 接口暂时不支持 MTU 设置。

命令	作用

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

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

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

说明：

S2300 系列产品所支持的 MTU 是固定的，长度为 1528Bytes，手工配置无效。

接口的 MTU 配置只对硬件转发的报文起作用。

6.2.8.配置二层接口

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

二层接口的缺省配置如下表：

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

保护端口	关闭
端口安全	关闭

6.2.8.1. 配置 Switch Port

6.2.8.1.1.配置 access/trunk port

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

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

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

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

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

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

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

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

配置 trunk port 的 native VLAN

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

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

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

配置接口的端口安全，有关端口安全更详细的信息请参照“基于端口的流量控制”：

命令	作用
Ruijie(config-if)**# switchport port-security**	配置接口的端口安全。

下例显示如何打开 Gigabitethernet 2/1 的端口安全。。

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

配置接口的速度，双工，流控请参照“配置接口的速度，双工，流控”。

下例显示如何配置 Gigabitethernet 2/1 为 access port，所属 VLAN 为 100，速度，双工，流控为自协商模式，端口安全打开：

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

6.2.8.1.2.配置 Hybrid 端口

您可以通过以下步骤配置 Hybrid 端口：

命令	说明
configure terminal	进入配置模式

interface <*interface*>	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

```
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
```

6.2.8.2. 配置 L2 Aggregate Port

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

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

6.2.8.3. 清除接口的统计值并复位该接口

在特权模式下您可通过 **clear** 命令清除接口的统计值并复位该接口。该命令只对 Switch Port,L2 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
```

注意：

S23 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 2044(UNTAG，包含 FCS，,如果是 TAG 报文，不大于 2048)字节的报文，正常转发，对超出 2044(UNTAG，包含 FCS，如果是 TAG 报文，超出 2048)字节的报文丢弃。

6.2.9.配置三层接口

6.2.9.1. 配置 SVI

本节主要描述如何创建 SVI 及和 SVI 的一些相关配置。

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

SVI 的配置：

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

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

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

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

注意：

该系列设备最多支持创建一个 SVI 接口。

要配置 DHCP 客户端，使其通过 DHCP 获得动态分配的 IP 地址，在进入 SVI 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

监视和维护 DHCP 客户有两类命令，可以通过在客户端上进行以下操作：

1）调试（debug）命令，输出必要的调试信息，主要用于故障诊断和排除.

2）显示命令，显示 DHCP 相关信息。

要进行 DHCP 客户的调试，在命令执行模式中执行以下命令：

命令	作用
Ruijie# **debug ip dhcp client**	调试 DHCP 客户

要显示 DHCP 客户获得的租约信息，在命令执行模式中执行以下命令：

命令	作用
Ruijie# **show dhcp lease**	显示 DHCP 租约信息

6.3. 端口属性随端口类型变化的转化关系

功能	2，3 层口转化	加入，退出 ap
速率	状态不变	加入 AP，应用 AP 配置；退出 AP，还原端口配置。
双工	状态不变	加入 AP，应用 AP 配置；退出 AP，还原端口配置。
dot1x	不支持 3 层口；变成 3 层口后，状态关闭；还原成 2 层口，状态为默认值关闭。	不支持 ap；加入 ap 后，端口上的 dot1x 认证关闭；退出后，还原成默认状态关闭；
端口安全	不支持 3 层口；变成 3 层口，状态关闭；重新恢复成 2 层口，状态为默认值关闭。	不支持 ap；加入后关闭，退出 ap 后；还原成端口的加入 ap 前的配置。
arp check	状态不变	加入 AP，应用 AP 配置；退出 AP，还原端口配置。
带宽	状态不变	加入 AP，应用 AP 配置；退出 AP，还原端口配置。
Ip 地址	不支持 2 层口；变成 2 层口，ip 配置丢失；重新恢复成 3 层口，默认为没有配置 ip 地址；	加入 AP，应用 AP 配置；退出 AP，还原端口配置。

shutdown	状态不变	加入AP，应用AP配置；退出AP，还原端口配置。

2 层口不能加入 3 层 ap，3 层口不能加入 2 层 ap；2 层口，3 层口，2 层 ap，3 层 ap 和 SVI 都不能相互转化；

6.4. 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。

以下例子为显示接口 Gigabitethernet 1/1 的接口状态：

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

以下例子为显示接口 SVI 5 的接口状态和配置信息：

```
Ruijie# show interfaces vlan 5
```

```
VLAN   : V5
Description          : SVI 5
AdminStatus         : up
OperStatus          : down
Primary Internet address     :  192.168.65.230/24
Broadcast address         :  192.168.65.255
PhysAddress         : 00d0.f800.0001
LastChange          : 0:0h:0m:5s
```

以下例子为显示接口 Aggregate Port 3 的接口状态：

```
Ruijie# show interfaces aggregateport 3：
Interface   : 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
```

6.5. line-detect 线缆检测

管理员可以通过线缆检测命令来检测线缆的工作状况。在线缆处于短路、断路等异常状态时，线缆检测有助于正确判断线缆的工作状况。

此命令必须在接口模式下执行，具体配置如下：

命令	作用
Ruijie(config)# **interface** *interface*	进入接口模式
Ruijie(config-if)# **line-detect**	执行线缆检测

注意:

1. 只有电介质的物理口才支持线缆检测，光介质物理口、AP 口不支持线缆检测。

2. 在正常连接的接口执行线缆检测，会导致连接暂时断掉，然后再重新建立连接。

以下是利用此命令进行线缆检测的例子：

```
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#line-detect

Interface : GigabitEthernet 0/1
start cable-diagnoses,please wait...
cable-daignoses end!this is result:
4 pairs
pair state     length(meters)
---- ---------- --------------
A    Ok        1
pair state     length(meters)
---- ---------- --------------
B    Ok        2
pair state     length(meters)
---- ---------- --------------
C    Short     1
pair state     length(meters)
---- ---------- --------------
D    Short     1
```

显示项解释：

显示项	解释
pairs	是指线缆里面包含的线对数目，如双绞线是由四对线组合而成。
State	当前线对的状态，共有三个值：OK（正常），Short（短路），Open（断路）。正常情况下，百兆双绞线 A、B 两对为 OK，C、D 两对为 Short。千兆双绞线 A、B、C、D 四对均为 OK。
Length	线缆的长度，单位为米。只有 state 为 OK 的线对的长度才有效。另外，由于线缆长度是根据信号的传递时间来计算的，所以可能存在一定的误差。状态为 Short 或者 Open 对应的 length 是指端口到线缆故障点的长度。

6.6. LinkTrap 策略配置

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

6.6.1.配置命令

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

6.6.2.配置举例

下面配置将配置接口为不发送 Link trap:

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

第7章 Aggregate Port 配置

本章描述如何在锐捷设备的上配置 Aggregate Port。

7.1. 概述

7.1.1. 理解 Aggregate Port

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

当 AP 中的一条成员链路断开时，系统会将该成员链路的流量自动地分配到 AP 中的其它有效成员链路上去。AP 中一条成员链路收到的广播或者多播报文，将不会被转发到其它成员链路上。

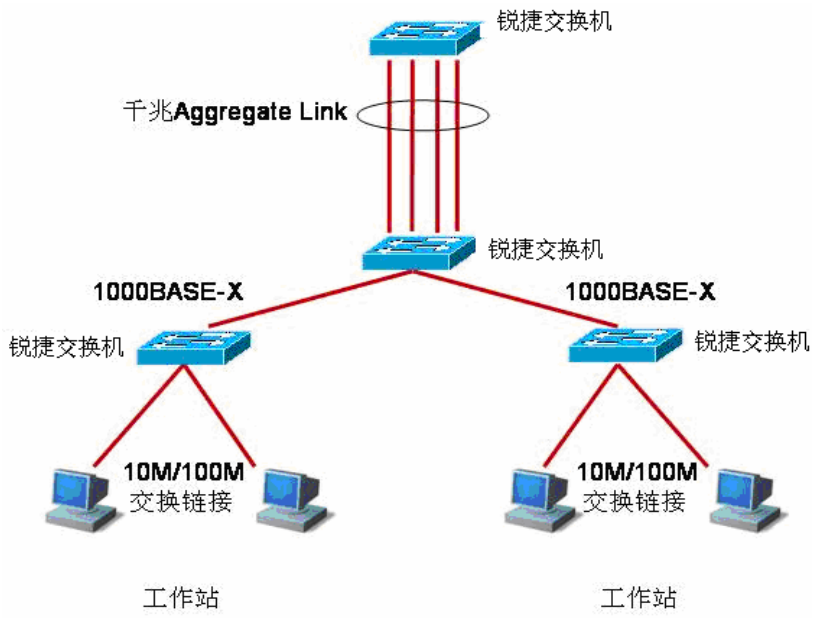


图 1 典型的 AP 配置

7.1.2. 理解流量平衡

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

方式。

源 MAC 地址流量平衡是根据报文的源 MAC 地址把报文分配到 AP 的各个成员链路中。不同源 MAC 的报文，转发的成员链路不同，相同源 MAC 的报文，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，从同一个成员链路转发，不同目的 MAC 的报文，从不同的成员链路转发。

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 地址的报文可能被分配到同一个 AP 的成员链路中。

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 的报文通过不同的成员链路转发，相同源 IP 或目的 IP 的报文则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，则自动根据二层报文的源 MAC 地址或目的 MAC 地址来进行流量平衡。

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，则自动根据二层报文 MAC 地址进行流量平衡。具有不同的源 IP+目的 IP 地址的报文可能被分配到同一个 AP 的成员链路中。

我们应根据不同的网络环境设置合适的流量分配方式，以便能把流量较均匀地分配到各个链路上，充分利用网络的带宽。

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

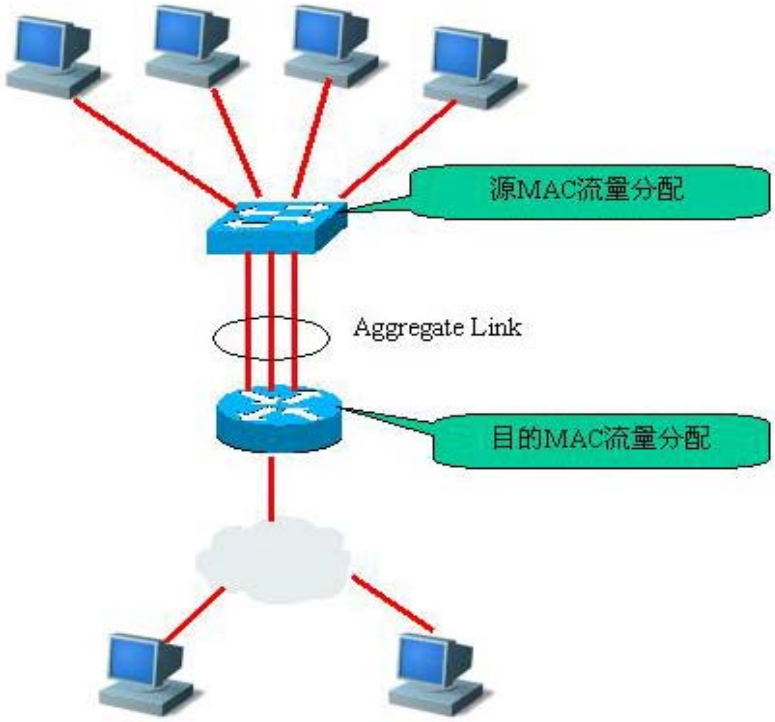


图 2　AP 流量平衡示意图

注意：

S2352 产品支持 6 个 Aggregate Port，其中 Aggregate Port 1 和 Aggregate Port 5 固定分配给百兆口使用，Aggregate Port 6 固定分配给千兆口用。（最多支持 8 个成员端口）。堆叠情况下， S2300 系列的交换机不支持跨设备的 Aggregate Port 功能。

7.2. 配置 Aggregate Port

7.2.1. 缺省的 Aggregate Port 配置

AP 的缺省配置如下表所示：

属性	缺省值
二层 AP 接口	无

流量平衡	根据输入报文的源 MAC 地址进行流量分配。

7.2.2.Aggregate Port 配置指导

AP 成员端口的端口速率必须一致。

二层端口只能加入二层 AP

AP 不能设置端口安全功能。

当把端口加入一个不存在的 AP 时，AP 会被自动创建。

一个端口加入 AP，端口的属性将被 AP 的属性所取代。

一个端口从 AP 中删除，则端口的属性将恢复为其加入 AP 前的属性。

注意:

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

7.2.3.配置 Aggregate Port

在接口配置模式下，请按如下步骤将端口加入 AP：

命令	作用
Ruijie(config-if-range)# **port-group** *port-group-number*	将该接口加入一个 AP(如果这个 AP 不存在，则同时创建这个 AP)。

在接口配置模式下使用 **no port-group** 命令将一个物理端口退出 AP。

下面的例子是将二层的以太网接口 0/1 配置成二层 AP 5 成员：

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

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

7.2.4.配置 Aggregate Port 的流量平衡

在配置模式下，请按如下步骤配置 AP 的流量平衡算法：

命令	作用
Ruijie(config)# **aggregateport load-balance** {**dst-mac** | **src-mac** | **src-dst-mac** }	设置 AP 的流量平衡，选择使用的算法： **dst-mac**：根据输入报文的目的 MAC 地址进行流量分配。在 AP 各链路中，目的 MAC 地址相同的报文被送到相同的成员链路，目的 MAC 不同的报文分配到不同的成员链路 **src-mac**：根据输入报文的源 MAC 地址进行流量分配。在 AP 各链路中，来自不同 MAC 地址的报文分配到不同的成员链路，来自相同的 MAC 地址的报文使用相同的成员链路 **src-dst-mac**：根据源 MAC 与目的 MAC 进行流量分配。不同的源 MAC——目的 MAC 对的流量通过不同的成员链路转发，同一源 MAC——目的 MAC 对通过相同的成员链路转发。

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。

7.3. 显示 Aggregate Port

在特权模式下，请按如下步骤显示 AP 设置。

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

```
Ruijie# show aggregateport load-balance
Load-balance : Source MAC address

Ruijie#show aggregateport 1 summary

AggregatePort MaxPorts SwitchPort Mode   Ports
------------- -------- ---------- ------
Ag1           8        Enabled    ACCESS
```

第8章 VLAN 配置

本章描述如何配置 IEEE802.1q VLAN

8.1. 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。

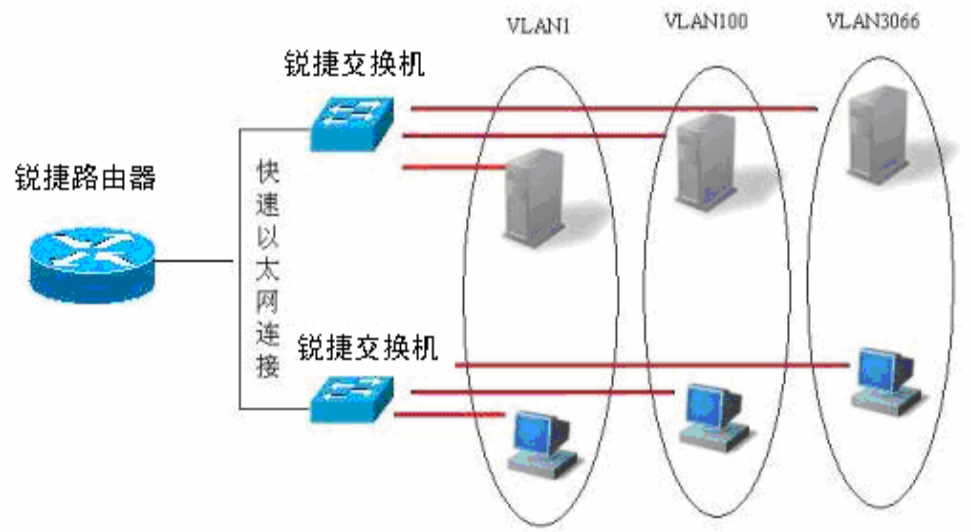


图 1

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（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。

8.1.1.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。

8.1.2.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：

VLAN 成员类型	VLAN 端口特征
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。

8.2. 配置 VLAN

一个 VLAN 是以 VLAN ID 来标识的。在设备中，您可以添加、删除、修改 VLAN 2-4094，而 VLAN 1 是由设备自动创建，并且不可被删除。

可以使用接口配置模式来配置一个端口的 VLAN 成员类型或加入、移出一个 VLAN。

8.2.1.VLAN 配置信息的保存

当您在特权命令模式下输入 **copy running-config startup-config** 命令后，VLAN 的配置信息便被保存进配置文件。要查看 VLAN 配置信息，可以使用 **show vlan** 命令。

8.2.2.缺省的 VLAN 配置

参数	缺省值	范围
VLAN ID	1	1－4093
VLAN Name	VLAN xxxx，xxxx 是 VLAN ID 数	无范围

VLAN State	Active	Active，Inactive

8.2.3.创建、修改一个 VLAN

在特权模式下，您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)# **name** *vlan-name*	（可选）为 VLAN 取一个名字。如果没有进行这一步，则设备会自动为它起一个名字 VLAN xxxx，其中 xxxx 是用 0 开头的四位 VLAN ID 号。比如，VLAN 0004 就是 VLAN 4 的缺省名字。

如果您想把 VLAN 的名字改回缺省名字，只需输入 **no name** 命令即可。

下面是一个创建 VLAN 888，将它命名为 Test888，并且保存进配置文件的例子：

```
Ruijie# configure terminal
Ruijie(config)# vlan 888
Ruijie(config-vlan)# name test888
Ruijie(config-vlan)# end
```

8.2.4.删除一个 VLAN

您不能删除缺省 VLAN（VLAN 1）。

在特权模式下删除一个 VLAN：

命令	作用
Ruijie(config)# **no vlan** *vlan-id*	输入一个 VLAN ID，删除它。

8.2.5.向 VLAN 分配 Access 口

如果您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。

在特权模式下，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 Ethernet 1/10 作为 Access 口加入了 VLAN20：

```
Ruijie# configure terminal
Ruijie(config)# interface fastethernet 1/10
Ruijie(config-if)# switchport mode access
Ruijie(config-if)# switchport access vlan 20
Ruijie(config-if)# end
```

下面这个例子显示了如何检查配置是否正确：

```
Ruijie(config)# show interfaces gigabitEthernet 3/1 switchport
Switchport is enabled
Mode is access port
Acsess vlan is 1,Native vlan is 1
Protected is disabled
Vlan lists is ALL
```

8.3. 配置 VLAN Trunks

8.3.1. 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。

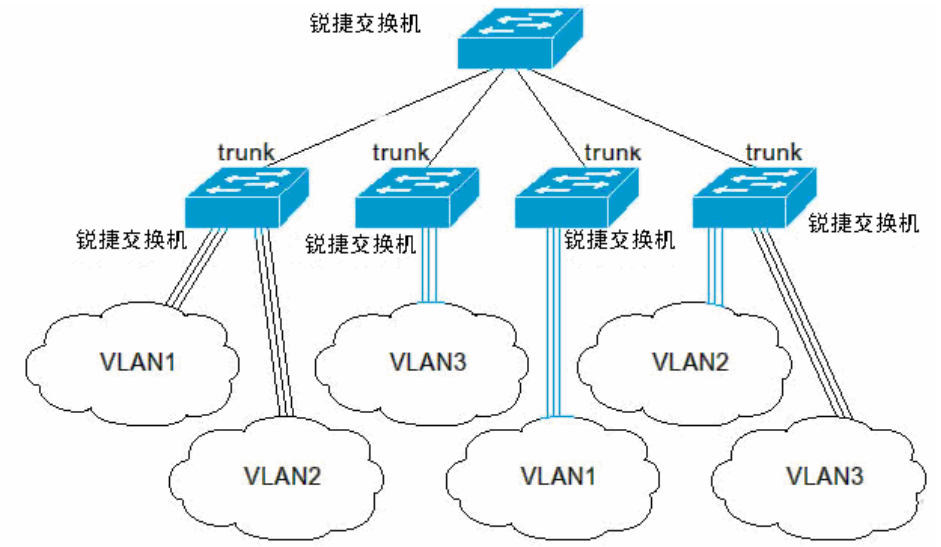


图 2

您可以把一个普通的以太网端口，或者一个 Aggregate Port 设为一个 Trunk 口（关于 Aggregate Port 的详细说明，请见配置 Aggregate Port）。

如果要把一个接口在 ACCESS 模式和 TRUNK 模式之间切换，请用 **switchport mode** 命令：

命令	作用
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 口定义一个 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 口属于相同的 Native VLAN。

8.3.2.配置一个 Trunk 口

8.3.2.1. Trunk 口基本配置

在特权模式下，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 trunk** 接口配置命令。

8.3.3.定义 Trunk 口的许可 VLAN 列表

一个 Trunk 口缺省可以传输本设备支持的所有 VLAN（1－4094）的流量。但是，您也可以通过设置 Trunk 口的许可 VLAN 列表来限制某些 VLAN 的流量不能通过这个 Trunk 口。

在特权模式下，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 1/15 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
Switchport is enabled
Mode is trunk port
Acsess vlan is 1,Native vlan is 1
Protected is disabled
Vlan lists is
1,3-4094
```

8.3.4.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。

在特权模式下，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。

当把一个接口的 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。

8.4.显示 VLAN

在特权模式下，才可以查看 VLAN 的信息。显示的信息包括 VLAN VID、VLAN 状态、VLAN 成员端口以及 VLAN 配置信息。以下罗列了相关的显示命令：

命令	作用
show vlan [**id** *vlan-id*]	显示所有或指定 VLAN 的参数

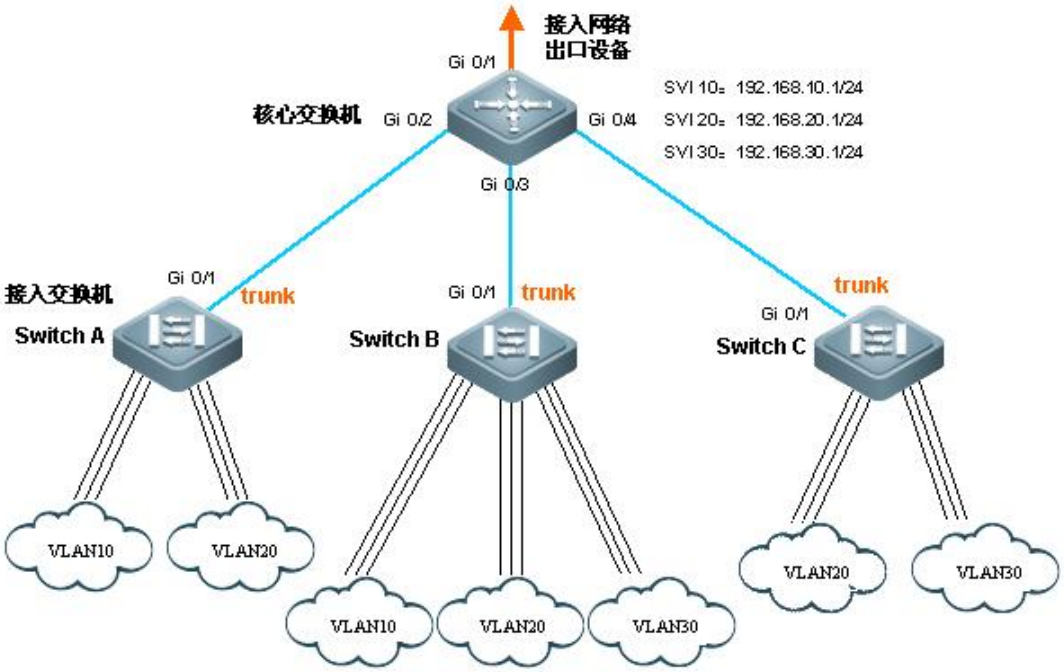
下面是一个显示 VLAN 的例子：

```
Ruijie# show vlan
VLAN[1] "VLAN0001"
GigabitEthernet 3/1
GigabitEthernet 3/2
GigabitEthernet 3/3
GigabitEthernet 3/4
GigabitEthernet 3/5
GigabitEthernet 3/6
GigabitEthernet 3/7
GigabitEthernet 3/8
GigabitEthernet 3/9
GigabitEthernet 3/10
GigabitEthernet 3/11
GigabitEthernet 3/12
```

```
VLAN[6] "VLAN0006"
GigabitEthernet 3/1

Ruijie# show vlan  id 1
VLAN[1] "VLAN0001"
GigabitEthernet 3/1
GigabitEthernet 3/2
GigabitEthernet 3/3
GigabitEthernet 3/4
GigabitEthernet 3/5
GigabitEthernet 3/6
GigabitEthernet 3/7
GigabitEthernet 3/8
GigabitEthernet 3/9
GigabitEthernet 3/10
GigabitEthernet 3/11
GigabitEthernet 3/12
```

8.5. VLAN 配置用例

8.5.1.组网拓扑



8.5.2.组网需求

如上图所示，某用户内网被划分为 VLAN 10、VLAN 20、VLAN 30，以实现相互间的 2 层隔离；3 个 VLAN 对应的 IP 子网分别为 192.168.10.0/24、192.168.20.0/24、192.168.30.0/24，3 个 VLAN 通过 3 层核心交换机的 IP 转发能力实现子网互连。

8.5.3.配置要点

本用例以核心交换机和 1 台接入交换机为例说明配置过程。要点如下：

1. 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；
2. 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；
3. 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。

8.5.4.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
```

第9章 Private VLAN 配置

9.1. Private VLAN 技术

服务提供商如果给每个用户一个 VLAN，则由于一台设备支持的 VLAN 数最大只有 4096 而限制了服务提供商能支持的用户数；在三层设备上，每个 VLAN 被分配一个子网地址或一系列地址，这种情况导致 IP 地址的浪费，一种解决方法就是应用 Private VLAN 技术。

私有 VLAN(Private VLAN)将一个 VLAN 的二层广播域划分成多个子域，每个子域都由一个私有 VLAN 对组成：主 VLAN(Primary VLAN)和辅助 VLAN(Secondary VLAN)。

一个私有 VLAN 域可以有多个私有 VLAN 对，每一个私有 VLAN 对代表一个子域。在一个私有 VLAN 域中所有的私有 VLAN 对共享同一个主 VLAN。每个子域的辅助 VLAN ID 不同。

一个私有 VLAN 域中只有一个主 VLAN，辅助 VLAN 实现同一个私有 VLAN 域中的二层隔离，有两种类型的辅助 VLAN：

- 隔离 VLAN(Isolated VLAN)：同一个隔离 VLAN 中的端口不能互相进行二层通信。一个私有 VLAN 域中只有一个隔离 VLAN。
- 群体 VLAN(Community VLAN)：同一个群体 VLAN 中的端口可以互相进行二层通信，但不能与其它群体 VLAN 中的端口进行二层通信。一个私有 VLAN 域中可以有多个群体 VLAN。

混杂端口（Promiscuous Port），属于主 VLAN 中的端口，可以与任意端口通讯，包括同一个私有 VLAN 域中辅助 VLAN 的隔离端口和群体端口。

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

群体端口(Community port)，属于群体 VLAN 中的端口，同一个群体 VLAN 的群体端口可以互相通讯，也可以与混杂通讯。不能与其它群体 VLAN 中的群体端口及隔离 VLAN 中的隔离端口通讯。

私有 VLAN 中，只有主 VLAN 可以创建 SVI 接口，辅助 VLAN 不可以创建 SVI。

私有 VLAN 中的端口可以为 SPAN 源端口，不可以为镜像目的端口。

9.2. 注意事项

S2300 系列产品不支持将 AP 设置为隔离口；在堆叠情况下，S2300 系列产品一个 Private VLAN 的成员 VLAN 及其端口不能跨设备。

9.3. Private VLAN 配置

9.3.1.缺省 Private VLAN 设置

缺省情况下，没有 Private VLAN 的配置

9.3.2.配置 VLAN 作为私有 VLAN

配置方法如下命令

命令	说明
configure terminal	进入配置模式
vlan *vid*	进入 VLAN 配置模式
private-vlan{community | isolated| primary}	配置私有 VLAN 类型
no private-vlan{community | isolated | primary}	取消私有 VLAN 配置
end	退出 VLAN 模式
show vlan private-vlan [*type*]	显示私有 VLAN

说明：

在 802.1Q Vlan 中具有成员口情况不能声明为私有 VLAN，VLAN 1 不能声明为私有 VLAN，对于具有 Trunk 口或 Uplink 口的 802.1Q VLAN 中，先将该 VLAN 从许可 VLAN 列表中删除，一对 Private VLAN 处于 ACTIVE 状态必须满足以下条件：

1) 具有 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
```

9.3.3.关联 Secondary VLAN 和 Primary VLAN

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

命令	说明
configure terminal	进入配置模式
vlan *p_vid*	进入 Primary VLAN 配置模式
private-vlan association {*svlist* | **add** *svlist* | **remove** *svlist*}	关联 Secondary VLAN
no private-vlan association	清除与所有 Secondary VLAN 的关联
end	退出 VLAN 模式
show vlan private-vlan [*type*]	显示私有 VLAN

举例如下：

```
Ruijie# configure terminal
Ruijie(config)# vlan 202
Ruijie(config-vlan)# private-vlan association 303-307,309,440
Ruijie(config-vlan)# end
Ruijie# show vlan private-vlan
VLAN Type  Status    Routed   Interface   Associated VLANs
---- ----  --------  ------   ---------   ------------------
202  prim  inactive  Disabled             303-307,309,440
303  comm  inactive  Disabled             202
304  comm  inactive  Disabled             202
305  comm  inactive  Disabled             202
306  comm  inactive  Disabled             202
307  comm  inactive  Disabled             202
309  comm  inactive  Disabled             202
440  comm  inactive  Disabled             202
```

说明：

该操作在声明为 Primary VLAN 的 VLAN 配置模式进行。

9.3.4.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
configure terminal	进入配置模式
interface vlan *p_vid*	进入 Primary VLAN 的接口模式
private-vlan mapping {*svlist* | **add** *svlist* | **remove** *svlist*}	映射 Secondary VLAN 到 Primary VLAN 的 SVI 三层交换。
end	退出接口模式

下面例子配置 Secondary VLAN 路由：

```
Ruijie# configure terminal
Ruijie(config)# interface vlan 202
Ruijie(config-if)# private-vlan mapping add 303-307,309,440
Ruijie(config-if)# end
Ruijie#
```

说明：

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

9.3.5.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
configure terminal	进入配置模式
interface <*interface*>	进入接口配置模式 *fastethernet*, *gigabitethernet*, *tengigabitethernet*

switchport mode private-vlan host	配置为二层交换模式
no switchport mode	清除私有 VLAN 配置
end	退出 SVI 接口模式
switchport private-vlan host-association *p_vid s_vid*	关联二层口与私有 VLAN
no switchport private-vlan host-association	清除关联

举例如下：

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/2
Ruijie(config-if)# switchport mode private-vlan host
Ruijie(config-if)# switchport private-vlan host-association
202 203
Ruijie(config-if)# end
Ruijie#
```

说明：

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

9.3.6.配置二层接口作为私有 VLAN 的混杂端口

配置二层接口作为私有 VLAN 的端口，通过以下操作命令：

命令	说明
configure terminal	进入配置模式
interface <*interface*>	进入接口配置模式 百兆,千兆，万兆
switchport mode private-vlan promiscuous	配置为私有 VLAN 二层交换模式
no switchport mode	删除端口私有 VLAN 配置
switchport private-vlan mapping *p_vid*{*svlist* | **add** *svlist* | **remove** *svlist*}	私有 VLAN 混杂端口选择所在 VLAN，及混杂的 secondary VLAN 列表
no switchport private-vlan mapping	取消混杂所有的的 seconary VLAN.

下面例子描述配置过程：

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/2
Ruijie(config-if)# switchport mode private-vlan promiscuous
Ruijie(config-if)# switchport private-vlan mapping 202 add 203
Ruijie(config-if)# end
Ruijie#
```

说明：

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

9.4. Private VLAN 显示

9.4.1. 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
```

第10章 MAC 地址配置

10.1. 管理 MAC 地址表

10.1.1. 概述

MAC 地址表包含了用于端口间报文转发的地址信息。MAC 地址表包含了动态、静态、过滤三种类型的地址，我们将从以下几个方面描述 MAC 地址表。

10.1.1.1. 动态地址

动态地址是设备通过接收到的报文自动学习到的 MAC 地址。当一个端口接收到一个包时，设备将把这个包的源地址和这个端口关联起来，并记录到地址表中，设备通过这种方式不断学习新的地址。

当设备收到一个包时，若该包的目的 MAC 地址是设备已学习到的动态地址，则这个包将直接转发到与这个 MAC 地址相关联的端口上，否则，这个包将向所有端口转发。

设备通过学习新的地址和老化掉不再使用的地址来不断更新其动态地址表。对于地址表中一个地址，如果较长时间(由地址老化时间决定)设备都没有收到以这个地址为源地址的包，则这个地址将被老化掉。您可以根据实际情况改变动态地址的老化时间。需要注意的是如果地址老化时间设置得太短，会造成地址表中的地址过早被老化而重新成为设备未知的地址，而设备再接收到以这些地址为目的地址的包时，会向 VLAN 中的其它端口发广播，这样就造成了一些不必要的广播流。如果老化时间设置得太长，则地址老化太慢，地址表容易被占满。当地址表加满后，新的地址将不能被学习，在地址表有空间来学习这个地址之前，这个地址就会一直被当作未知的地址 ，当设备收到以这些地址为目的地址的包时，同样向 VLAN 中的其它端口发广播，这样也会造成了一些不必要的广播流。

当设备复位后，设备学习到的所有动态地址都将丢失，设备需要重新学习这些地址。

在堆叠环境下，从机学习到的地址会通告给主机，但是若该地址对应的数据流没有经过某台从机，则对应的从机不会学习到该地址，这时该从机收到目的 mac 为上述 mac 的报文时，会广播到所有端口。

注意:

堆叠系统下各成员设备的地址表是不同步的。举例说明如下：

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

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

10.1.1.2. 静态地址

静态地址是手工添加的 MAC 地址。静态地址和动态地址功能相同，不过相对动态地址而言，静态地址只能手工进行配置和删除(不能学习和老化)，静态地址可以保存在配置文件中，即使设备复位，静态地址也不会丢失。

10.1.1.3. 过滤地址

过滤地址是手工添加的 MAC 地址。当设备接收到以过滤地址为源地址的包时将会直接丢弃。过滤地址永远不会被老化，只能手工进行配置和删除，过滤地址可以保存到配置文件中，即使设备复位，过滤地址也不会丢失。

如果您希望设备能屏蔽掉一些非法的用户，您可以将这些用户的 MAC 地址设置为过滤地址，这样这些非法用户将无法通过设备与外界通讯。

注意:

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。

10.1.1.4. MAC 地址和 VLAN 的关联

所有的 MAC 地址都和 VLAN 相关联，相同的 MAC 地址可以在多个 VLAN 中存在，不同 VLAN 中该地址可以关联不同的端口。每个 VLAN 都维护它自己的逻辑上的一份地址表。一个 VLAN 已学习的 MAC 地址，对于其他 VLAN 而言可能就是未知的，仍然需要学习。

10.1.2. 配置 MAC 地址

10.1.2.1. MAC 地址表的缺省配置

下表显示的地址表的缺省配置：

内容	缺省设置
地址表老化时间	300 秒
动态地址表	自动学习
静态地址表	没有配置任何静态地址
过滤地址表	没有配置任何过滤地址

注意：

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。

10.1.2.2. 设置地址老化时间

下表为设置地址老化时间：

命令	作用
Ruijie(config)# **mac-address-table aging-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。

您可以在全局配置模式下通过命令 **no mac-address-table aging-time** 来将地址老化时间恢复为缺省值。

10.1.2.3. 删除动态地址表项

在特权模式下，您可以使用命令 **clear mac-address-table dynamic** 删除设备上所有的动态地址；您可以使用命令 **clear mac-address-table dynamic address mac-address** 删除一个特定 MAC 地址；您可以使用命令 **clear mac-address-table dynamic interface** *interface-id* 删除一个特定物理端口或 Aggregate Port 上的所有动态地址；您也可以使用命令 **clear mac-address-table**

dynamic vlan *vlan-id* 删除指定 VLAN 上的所有动态地址。

您可以使用特权模式下的命令 **show mac-address-table dynamic** 来验证相应的动态地址是否已经被删除。

10.1.2.4. 增加和删除静态地址表项

如果您要增加一个静态地址，您需要指定 MAC 地址(包的目的地址)，VLAN(这个静态地址将加入哪个 VLAN 的地址表中)，接口(目的地址为指定 MAC 地址的包将被转发到的接口)。

添加一个静态地址：

命令	作用
Ruijie(config)# **mac-address-table static** *mac-add* **vlan** *vlan-id* **interface** *interface-id*	mac-addr：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-addr 指定的地址为目的地址的包时，这个包将被转发到 interface-id 指定的接口上。

您可以在全局配置模式下通过命令 **no mac-address-table static mac-addr vlan** *vlan-id* **interface** *interface-id* 来删除一个静态地址表项。

下面的例子说明了如何配置一个静态地址 00d0.f800.073c，当在 VLAN 4 中接受到目的地址为这个地址的包时，这个包将被转发到指定的接口 Gigabitethernet 1/3 上。

```
Ruijie(config)# mac-address-table static 00d0.f800.073c vlan
4 interface gigabitethernet 1/3
```

10.1.2.5. 增加和删除过滤地址表项

如果您要增加一个过滤地址，您需要指定希望设备过滤掉哪个 VLAN 内的哪个 MAC 地址，当设备在该 VLAN 内收到以这个 MAC 地址为源地址的包时，这个包都将被直接丢弃。

添加一个过滤地址：

命令	作用
Ruijie(config)# **mac-address-table filtering** *mac-addr* **vlan** *vlan-id*	mac-addr：指定设备需要过滤掉的 MAC 地址 vlan-id：指定该地址所属的 VLAN

您可以在全局配置模式下通过命令 **no mac-address-table filtering mac-addr**

vlan *vlan-id* 来删除一个过滤地址表项。

下面的例子说明了如何让设备过滤掉 VLAN 1 内源 MAC 地址为 00d0.f800.073c 的数据包：

```
Ruijie(config)# mac-address-table filtering 00d0.f800.073c vlan 1
```

注意：

S23系列交换机产品只支持基于源MAC地址过滤。即其只过滤源MAC地址是过滤地址的报文，不过滤仅目的MAC地址是过滤地址的报文。

10.1.3. 查看 MAC 地址信息

查看设备的 MAC 地址表信息：

命令	作用
Ruijie# **show mac-address-table**	显示所有类型的 MAC 地址信息(包括动态地址，静态地址和过滤地址)
Ruijie# **show mac-address-table aging-time**	显示当前的地址老化时间
Ruijie# **show mac-address-table dynamic**	显示所有动态地址信息
Ruijie# **show mac-address-table static**	显示所有静态地址信息
Ruijie# **show mac-address-table filtering**	显示所有过滤地址信息
Ruijie# **show mac-address-table interface** *接口 ID*	显示指定接口的所有类型的地址信息
Ruijie# **show mac-address-table vlan** *ID*	显示指定 VLAN 的所有类型的地址信息
Ruijie# **show mac-address-table count**	显示地址表中 MAC 地址的统计信息

下面是一些显示 MAC 地址信息的例子:

显示 MAC 地址表：

```
Ruijie# show mac-address-table dynamic
Vlan       MAC Address         Type     Interface
----------  ---------------------------------------------------
1          0001.960c.a740      DYNAMIC  gigabitethernet 1/1
1          0009.b715.d40c      DYNAMIC  gigabitethernet 1/1
1          0080.ad00.0000      DYNAMIC  gigabitethernet 1/1
```

显示地址表中 MAC 地址的统计信息：

```
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
```

显示地址老化时间的设置：

```
Ruijie# show mac-address-table aging-time
Aging time    : 300
```

10.2. MAC 地址变化通知

10.2.1. 概述

如果您需要了解对于设备而言网络中用户的变化情况，使用 MAC 地址通知功能是一种有效的手段。打开 MAC 地址通知的功能后，当设备学习到一个新的 MAC 地址或删除掉一个已学习到的 MAC 地址，一个反映 MAC 地址变化的通知信息就会产生，并以 SNMP Trap 的形式将通知信息发送给指定的 NMS(网络管理工作站)。如果一个 MAC 地址增加的通知产生，我们就知道一个新的用户(这个 MAC 地址标识的用户)开始使用设备，如果一个 MAC 地址删除(一个使用设备的用户，如果在地址老化时间指定的时间间隔内没有和设备进行任何通讯，用户对应 MAC 地址将从设备的地址表中删除)的通知产生，则表示一个用户已经停止使用设备了。

当使用设备的用户较多时，可能会出现在短时间内会有大量的 MAC 地址变化产生(比如设备上电时)，导致网络流量增加。为了减轻网络负担，您可以设置发送 MAC 地址通知的时间间隔。系统会将指定的时间间隔地址通知信息加以捆绑，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，这样就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。如果您没有配置接收 Trap 的 NMS 或您没有及时接收 MAC 地址变化的 Trap，您可以通过查看 MAC 地址通知历史记录表来了解最近 MAC 地址变化的消息。

MAC 地址通知功能是基于接口的，但 MAC 地址通知有一个全局开关。如果 MAC 地址通知全局开关关闭，则所有接口上均不会产生 MAC 地址通知。只有在全局开关打开并且接口上的 MAC 地址变化功能打开的情况下，这个接口才会产生 MAC 地址变化通知，而没有打开通知功能的接口上的 MAC 地址的变化将不会通知。您可以设置让接口仅仅发送地址增加或减少的通知，也可以设置两者都发。

注意：

MAC 地址通知仅针对动态地址，对于静态配置的地址的变化将不会产生通知信

息。

10.2.2. 配置 MAC 地址变化通知功能

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 Trap. community-string：指明发送的 Trap 上附带的认证名
Ruijie (config)**#snmp-server enable traps**	允许交换机发送 Trap
Ruijie(config)# **mac-address-table notification**	打开 MAC 地址通知功能的全局开关
Ruijie(config)# **mac-address-table notification** {**interval** *value* | **history-size** *value*}	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

您可以在全局配置模式下通过命令 **no snmp-server enable traps mac-notification** 来禁止设备发送 MAC 地址变化通知的 Trap，使用命令 **no mac-address-table notification** 来关闭 MAC 地址通知的全局开关，此外，您可以在接口配置模式下，使用命令 **no snmp trap mac-notification** {**added** | **removed**}来关闭指定接口的相应 MAC 地址通知功能。

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 1/3 上当 MAC 地址增加和减少时进行通知的功能：

```
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 1/3
Ruijie(config-if)# snmp trap mac-notification added
Ruijie(config-if)# snmp trap mac-notification removed
```

10.2.3. 查看 MAC 地址变化通知信息

在特权模式下，你可以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一些例子。

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
------------------- ------------- ---------------
Gi1/1              Disabled      Enabled
Gi1/2              Disabled      Disabled
Gi1/3              Enabled       Enabled
Gi1/4              Disabled      Disabled
Gi1/5              Disabled      Disabled
Gi1/6              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 Gi1/1
Removed     1    00d0.f808.0c0c Gi1/1
History Index:2
Entry Timestamp: 21891
MAC Changed Message :
```

```
Operation   VLAN MAC Address    Interface
----------- ---- ------------- -------------------
Added       1    00d0.f80d.1083 Gi1/1
```

10.3. IP 和 MAC 地址绑定

10.3.1. 概述

通过手动配置 IP 和 MAC 地址绑定功能，您可以对输入的报文进行过滤控制。如果您将一个指定的 IP 地址和一个 MAC 地址绑定，则交换机只接收源 IP 地址和 MAC 地址均匹配这个绑定地址的 IP 报文；否则该报文将被丢弃。

利用地址绑定这个特性，您可以严格控制设备的输入源的合法性校验。需要注意的是，通过地址绑定控制交换机的输入，将优先于 802.1X、端口安全以及 ACL 生效。

10.3.2. 配置地址绑定

在全局模式下，您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
Ruijie(config)**# address-bind install**	开启绑定生效功能

您可以在全局配置模式下使用 **no address-bind** *ip-address mac-address* 取消该 IP 地址和 MAC 地址的绑定。

通过 **no address-bind install** 命令可关闭绑定功能。

10.3.3. 查看地址绑定表

你可以在特权模式下使用 **show address-bind** 命令来显示设备中已经设置了的 IP 地址和 MAC 地址的绑定：

```
Ruijie# show address-bind
Total Bind Addresses in System : 2
IP Address      Binding MAC Addr
----------     ----------------------
3.3.3.3         00d0.f811.1112
3.3.3.4         00d0.f811.1117
```

10.3.4. 查看指定地址绑定状态

你可以在特权模式下使用 **show address-bin**d [ip-address *ip* | mac-address *mac*] 命令来查看指定 IP/MAC 地址的绑定状态。

```
Ruijie# show address-bind ip-address 3.3.3.3
IP Address      Binding MAC Addr
-----------     -----------------
3.3.3.3         00d0.f811.1112
```

10.3.5. 查看地址绑定表是否打开

你可以在特权模式下使用 **show address-bind summary** 命令来显示设备中地址绑定开关的状态以及绑定的地址个数

```
Ruijie# show address-bind summary
Total Bind Addresses in System : 0
Max Bind Addresses limit in System : 1000
System Address bind status:SUCCESS
```

注意:

System Address bind status 在系统中存在三种状态：SUCCESS，表示您已经使用了命令 address-bind install 命令成功打开地址绑定；FAIL，表示您已经使用了命令 address-bind install 命令，但由于设备硬件资源不足以绑定您配置的地址，所以绑定失败，这时您配置的所有绑定地址将不能生效，您可以删除部分配置的地址并再次绑定；Uninstall，表示您还没有打开地址绑定开关，这时您配置的所有绑定地址将不能生效。

10.3.6. 设置 IP 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 转发规则	IPV6 转发规则
严格	只允许符合 IPV4+MAC 条件的报文转发。	不允许任何 ipv6 报文转发（默认模式）。
宽松	只允许符合 IPV4+MAC 条件的报文转发。	允许所有的 IPV6 报文转发。
兼容	只允许符合 IPV4+MAC 条件的报文转发。	只允许源 MAC 为绑定地址的 MAC 地址的 IPV6 报文转发

IPV6 模式只对 IPV6 的转发有影响。

从特权模式开始，您可以通过以下步骤来设置 IP 地址的绑定模式：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式
Ruijie(config)# **address-bind ipv6-mode compatible**	设置 ipv6 模式为兼容模式
Ruijie(config)# **address-bind ipv6-mode loose**	设置 ipv6 模式为宽松模式
Ruijie(config)# **address-bind ipv6-mode strict**	设置 ipv6 模式为严格模式
Ruijie(config)# **no adress-bind ipv6-mode**	设置 ipv6 模式为默认模式（严格模式）。

例如，绑定 IP 地址为 192.168.5.2 用户的地址为 00d0.f822.33aa，并允许该用户相应的 IPV6 报文转发。

```
Ruijie# configure t
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# address-bind 00d0.f822.33aa ip 192.168.5.2
Ruijie(config)# address-bind ipv6-mode compatible
```

注意：

设置 IPV6 模式对 **DHCP Snooping** 的地址绑定，端口安全的 MAC+IP 等多种 MAC+IP 绑定功能同时生效。对于某些产品的端口安全等功能支持 IPV6 的安全地址，IPV6 模式下的转发规则，如下表所示：

模式	Ipv4 转发规则	IPV6 转发规则
严格模式	只允许符合 IPV4+MAC 条件的报文转发。	只允许符合 IPV6 安全地址配置的 IPV6 报文转发。
宽松模式	只允许符合 IPV4+MAC 条件的报文转发。	允许所有的 IPV6 报文转发。
兼容模式	只允许符合 IPV4+MAC 条件的报文转发。	只允许源 MAC 为绑定的 MAC 地址，或符合 IPV6 安全地址配置的 IPV6 报文转发。

10.3.7. 配置地址绑定例外口

如果您想地址绑定策略对某些特定口不生效，您可以将这些特定口配置为例外口，从特权模式开始，您可以通过以下步骤来设置地址绑定的例外口：

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

Ruijie(config)**# address-bind uplink** *intf-id*	配置地址绑定的例外口
Ruijie(config)**# address-bind install**	安装地址绑定例外口

你可以在全局配置模式下使用 **no address-bind uplink** *interface-id* 取消该例外口的设置或使用 **no address-bind install** 取消例外口的安装。

10.3.8. 查看地址绑定例外口

您可以在特权模式下使用 **show address-bind uplink** 命令来显示交换机中已经设置了的地址绑定例外口：

```
Ruijie# show address-bind uplink
Ports       State
------------ ------
Fa0/1       Enabled
Fa0/2       Disabled
Fa0/3       Disabled
Fa0/4       Disabled
Fa0/5       Disabled
Fa0/6       Disabled
Fa0/7       Disabled
Fa0/8       Disabled
Fa0/9       Disabled
Fa0/10      Disabled
```

第11章 DHCP Snooping 配置

11.1. DHCP Snooping 简介

11.1.1. 理解 DHCP

DHCP 协议被广泛用来动态分配可重用的网络资源，如 IP 地址。一次典型的 DHCP 获取 IP 的过程如下所示：

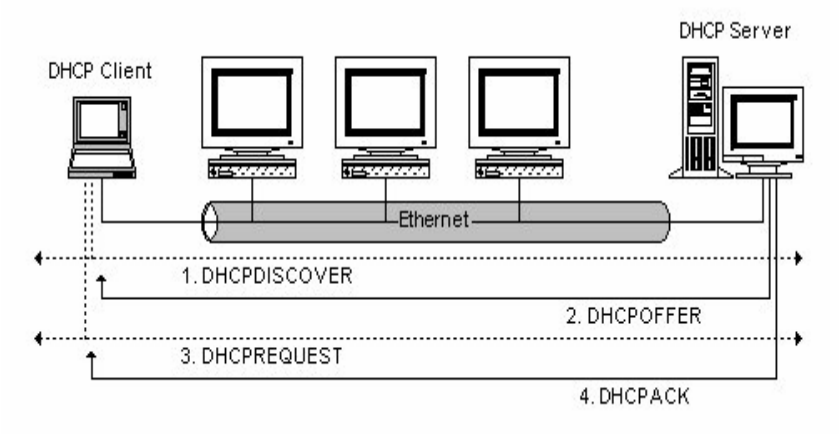


图 1

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 分配资源(如 IP 地址)，然后发出 DHCP OFFER 报文。

DHCP Client 收到 DHCP OFFER 报文后，发出 DHCP REQUEST 请求，请求获取服务器租约，并通告其他服务器已接受此服务器分配地址。

服务器收到 DHCP REQUEST 报文，验证资源是否可以分配，如果可以分配，则发送 DHCP ACK 报文；如果不可分配，则发送 DHCP NAK 报文。DHCP Client 收到 DHCP ACK 报文，就开始使用服务器分配的资源。如果收到 DHCP NAK，则重新发送 DHCP DISCOVER 报文。

11.1.2. 理解 DHCP Snooping

DHCP Snooping（即 DHCP 窥探）可以窥探客户端和服务器之间的 DHCP 交互报文，可以筛选合法的 DHCP 报文，屏蔽非法的 DHCP 服务器。以下解释了

DHCP Snooping 使用的术语及功能：

DHCP Snooping Trust 接口：由于 DHCP 获取 IP 的交互报文是使用广播的形式，因此可能存在非法服务器影响用户获取 IP 地址。为了防止非法服务器问题，将端口配置为两种类型，TRUST 口和 UNTRUST 口。对于 DHCP 客户端请求报文，仅将其转发到 TRUST 口。对于 DHCP 服务器响应报文，仅转发来自 TRUST 口的响应报文，而丢弃所有来自 UNTRUST 口的响应报文。通过将合法 DHCP 服务器连接的端口设置为 TURST 口，其他口设置为 UNTRUST 口，就可以实现对非法 DHCP 服务器的屏蔽。

DHCP Snooping 绑定数据库：在 DHCP 环境的网络里，经常出现用户私自设置 IP 地址的问题，难网络管理带来一定的困难。DHCP Snooping 通过窥探客户端和服务器之间的交互报文，把用户获取到的 IP 地址以及用户 MAC、VID、PORT、租约时间等信息组成一个用户表项，从而形成一个 DHCP Snooping 绑定数据库。

DHCP Snooping 功能对经过设备的 DHCP 报文进行合法性检查，丢弃不合法的 DHCP 报文，并记录用户信息生成 DHCP Snooping 绑定数据库。以下几种类型的报文被认为是非法的 DHCP 报文：

1. UNTRUST 口收到的 DHCP 服务器响应报文，包括 DHCPACK、DHCPNAK、DHCPOFFER 等。

2. 打开源 mac 校验功能时，链路层头部源 MAC 与 DHCP 报文携带的 DHCP Client 字段不相同的报文。

3. 与 DHCP Snooping 绑定数据库中用户信息不一致的 DHCPRELEASE 报文。

11.1.3. DHCP Snooping information option

部分网络管理员在对当前的用户进行 IP 地址管理时，希望能够根据用户所处的位置来确定给用户分配 IP 地址，即希望能够根据用户所连接的网络设备的信息进行分配。交换机在窥探 DHCP 报文的同时，可以把一些用户相关的设备信息以 DHCP option82 选项加入到 DHCP 请求报文中。通过 option82 选项的信息，服务器可以更准确的为用户分配 IP 地址。DHCP snooping 加入 option82 选项的格式如下：

Agent Circuit ID

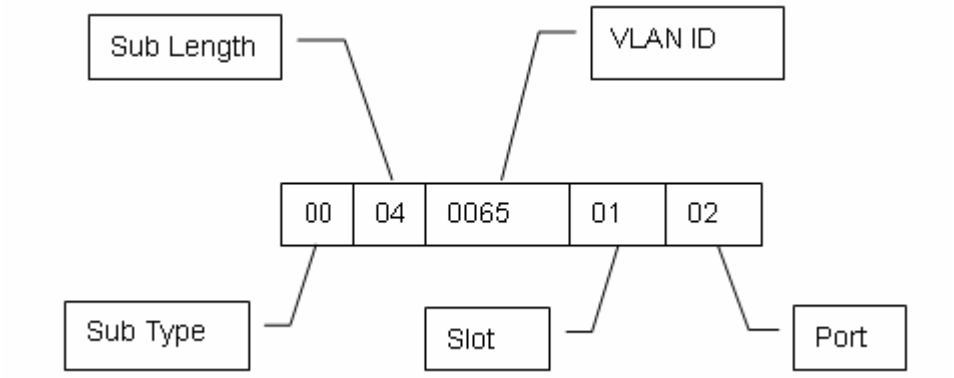


图 2

Agent Remote ID

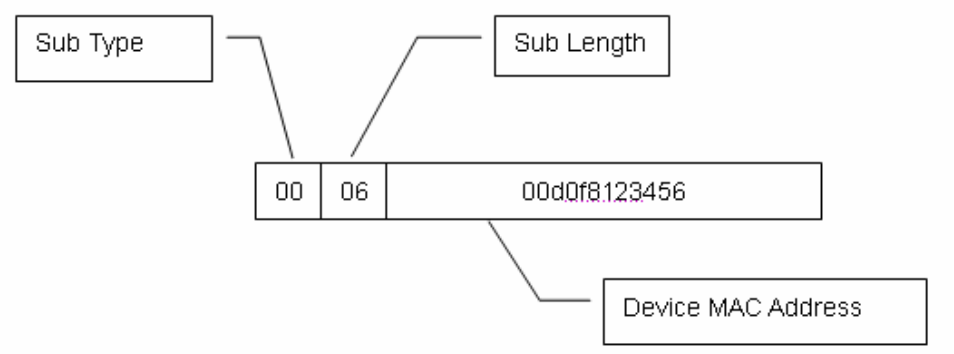


图 3

11.1.4. DHCP Snooping 地址绑定功能

DHCP snooping 地址绑定功能就是通过对 DHCP 报文交互过程进行窥探，将合法用户信息(IP 地址、MAC、VLAN、PORT、租约时间)，形成 DHCP snooping 数据库。将 DHCP snooping 数据库中的用户信息添加到 IP 报文硬件过滤表中，从而限制只有 DHCP snooping 数据库中的合法用户才能够发送 IP 报文，防止非法用户私设 IP 地址。

11.1.5. DHCP Snooping 支持 Bootp 用户绑定

DHCP Snooping 是基于 DHCP 协议设计的安全控制功能，对于 Bootp 应用的兼容性不足。主要是因为在 Bootp 报文中不存在 DHCP 相关 Option，如：报文类型、租约时间等选项。因此 DHCP Snooping 很难对 Bootp 应用环境中的用户进行有效控制。

针对市场日益增多的无盘工作站应用，我们对 DHCP Snooping 功能进行了扩展，增加了对 Bootp 协议的支持。DHCP Snooping 对 DHCP 报文交互进行窥探处理的同时，添加了对 Bootp 报文的处理，针对合法的 Bootp 用户，将会提取用户的 IP 地址、MAC 地址、端口及所属 VLAN 信息，添加一个静态绑定表项到 DHCP Snooping 数据库中。

Bootp 用户在 DHCP Snooping 数据库中相当于一个静态绑定用户，同手工配置的静态绑定用户相同。此用户在 Bootp 交互过程中动态生成，但是删除时同静态用户操作相同，需要管理员手动配置命令进行删除。

11.1.6. DHCP snooping 的相关安全功能

DHCP Snooping 地址绑定只是对 IP 报文进行过滤，不能对 ARP 报文进行过滤。

为了增加安全性，防止 ARP 欺骗等问题，需要对非法 ARP 报文进行过滤。（ARP 报文过滤，可以参考 ARP-CHECK、DAI 相关章节）

11.1.7. DHCP Snooping 配置的其他注意事项

1．DHCP Snooping 功能与 DHCP Relay Option 82 功能是互斥的，即不能同时打开 DHCP Snooping 和 DHCP Relay Option82 功能。

2．将端口配置为 TRUST 口后，不再对该端口下的用户进行安全控制。

3．开启 DHCP Snooping 功能后， 此时 DHCP 报文送 CPU 处理，不受安全策略控制影响。因此用户在配置时要注意：1）即使 DHCP 报文不符合所配置的安全策略，用户依然可以申请到 IP 地址；2）虽然用户可以申请到 IP 地址，但用户的 IP 报文可能会因为不满足安全策略而被丢弃，这种情况下用户会无法上网。

11.2. DHCP Snooping 配置

11.2.1. 配置打开和关闭 DHCP Snooping

缺省情况下，设备 DHCP Snooping 功能为关闭状态。配置该功能后，DHCP Snooping 开始对经过该设备的所有 DHCP 报文进行窥探。

命令	说明
Ruijie**# configure terminal**	进入配置模式
Ruijie(config)**# [no] ip dhcp snooping**	打开和关闭 DHCP snooping

下面是打开设备的 DHCP Snooping 功能：

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping
Ruijie(config)# end
Ruijie#
```

11.2.2. 配置 DHCP Snooping 支持 Bootp 用户绑定

缺省情况下，设备 DHCP Snooping 功能不支持 Bootp 用户绑定。配置该功能后，DHCP Snooping 开始对经过该设备的所有 Bootp 报文进行窥探，并将合法 Bootp 用户添加到 DHCP Snooping 数据库中。

命令	说明
Ruijie**# configure terminal**	进入配置模式

Ruijie(config)# [no] ip dhcp snooping bootp-bind	打开和关闭 DHCP snooping 支持 Bootp 绑定

下面是打开设备的 DHCP Snooping 功能：

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping bootp-bind
Ruijie(config)# end
Ruijie#
```

11.2.3. 配置源 MAC 检查功能

缺省情况下，源 MAC 检查功能为关闭状态。配置该功能后，DHCP Snooping 就会对 UNTRUST 口送上来的 DHCP 请求报文进行一致性检查。如果链路层头部源 MAC 字段和 DHCP 报文的 CLIENT MAC 字段相同，检查通过，则报文正常处理；否则检查失败，则丢弃该报文。

命令	说明
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

下面是打开源 MAC 检查功能：

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping verify mac-address
Ruijie(config)# end
Ruijie#
```

11.2.4. 配置静态绑定用户

缺省情况下，设备中不存在静态绑定用户。在某些应用情况下，用户希望配置静态 IP 地址访问网络，可以通过配置静态绑定用户功能来实现。

命令	说明
Ruijie# configure terminal	进入配置模式
Ruijie(config)# [no] ip dhcp snooping binding mac-addrees vlan *vlan_id* ip *ip-address* interface *interface-id*	配置 DHCP Snooping 静态绑定用户

下面是添加一个静态绑定用户：

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping binding 00d0.f801.0101 vlan
1 ip 192.168.1.1 interface fastethernet 0/9
```

```
Ruijie (config)# end
Ruijie#
```

注意：

1. 静态绑定用户并不会与动态用户相冲突。配置了静态绑定的用户，仍然可以动态获取 IP 地址。
2. Bootp 用户相当于静态绑定用户。删除 Bootp 用户与删除静态绑定用户，执行命令相同。

11.2.5. 配置 DHCP snooping information option

缺省情况下，此功能关闭。配置该功能后，DHCP Snooping 在进行报文转发时，会在所有 DHCP 请求报文中添加 option82 选项；同时将所有 DHCP 响应报文中的 option82 选项删除。

命令	说明
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# **[no] ip dhcp snooping Information option**	打开和关闭 DHCP snooping information option 功能

下面是配置打开 **DHCP Snooping information option** 功能：

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping information option
Ruijie(config)# end
Ruijie#
```

注意：

配置该功能后，在同一设备上配置的 DHCP relay option82 功能就会失效。

11.2.6. 配置端口地址绑定开关

缺省情况下，此功能关闭。在端口下，配置该功能后，将此端口下的所有 DHCP Snooping 用户，将设置到硬件绑定表中。通过硬件绑定表，对所有经过该设备的 IP 报文进行过滤，防止用户私设 IP 地址。

命令	说明
Ruijie# **configure terminal**	进入配置模式

Ruijie(config)# **interface fastethernet** *0/1*	进入接口配置模式
Ruijie(config-if)# [**no**] **ip dhcp snooping address-bind**	打开/关闭端口上的 DHCP snooping 地址绑定功能

下边是配置打开 DHCP snooping 地址绑定功能：

```
Ruijie# configure terminal
Ruijie(config)# interface fastethernet 0/1
Ruijie(config-if)# ip dhcp snooping address-bind
Ruijie(config)# end
Ruijie#
```

11.2.7. 配置定时将 DHCP Snooping 数据库写入 Flash 文件

缺省情况下，此功能关闭。为了防止设备重新启动后，DHCP Snooping 数据库中的动态用户信息丢失，DHCP Snooping 提供定时将数据库中所有动态用户信息写入 Flash 文件的功能。

命令	说明
Ruijie# **configure terminal**	进入配置模式
Ruijie(config)# [**no**] **ip dhcp snooping database write-delay** [*time*]	配置定时写 Flash 文件的时间间隔； *time*：600—86400(s)，缺省为 0，不定时写。

下面是配置 DHCP Snooping 定时写 Flash 文件的时间间隔为 3600s：

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping database write-delay 3600
Ruijie(config)# end
Ruijie#
```

注意：

由于不停擦写 flash，会造成 flash 的使用寿命缩短。所以在设置延迟写 flash 时间时需要注意，设置时间较短有利于设备信息更有效的保存；设置时间较长能够延长 flash 的使用寿命。

11.2.8. 配置手动将 DHCP Snooping 数据库写入 Flash 文件

管理员在重新启动设备前，可以手动将当前的DHCP Snooping用户绑定数据库写入 Flash 文件，保证设备重新启动，与之前状态一致。

命令	说明
Ruijie**# configure terminal**	进入配置模式
Ruijie(config)**# ip dhcp snooping database write-to-flash**	手动将 DHCP snooping 数据库实时写入 flash 文件

下面是配置实时将 DHCP Snooping 数据库写入 Flash 文件：

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping database write-to-flash
Ruijie(config)# end
```

11.2.9. 配置端口为 TRUST 口

缺省情况下，端口状态为 UNTRUST。通过配置此命令，将一个端口为配置为 TRUST 口，连接合法 DHCP 服务器。DHCP Snooping 功能仅转发 TRUST 口的 DHCP 响应报文，丢弃 UNTRUST 口的 DHCP 响应报文。

命令	说明
Ruijie**# configure terminal**	进入配置模式
Ruijie(config)**# interface fastethernet** *0/1*	进入接口配置模式
Ruijie(config-if)**# [no] ip dhcp snooping trust**	配置端口为 TRUST 口

下面是配置端口 **fastethernet** *0/1* 为 TRUST 口：

```
Ruijie# configure terminal
Ruijie(config)# interface fastethernet 0/1
Ruijie(config-if)# ip dhcp snooping trust
Ruijie(config-if)# end
Ruijie#
```

11.2.10. 清空 DHCP Snooping 数据库中所有动态用户信息

此命令用于删除 DHCP Snooping 用户绑定数据库中所有动态用户信息。

命令	说明
Ruijie**# clear ip dhcp snooping binding**	清空当前数据库中所有动态用户的信息

下边的是手动清空当前数据库中所有动态用户的信息：

```
Ruijie# clear ip dhcp snooping binding
```

11.3. DHCP snooping 其它配置

11.3.1. 显示 DHCP snooping

此命令用于显示 DHCP Snooping 功能当前的配置情况：

命令	说明
Ruijie# **show ip dhcp snooping**	显示 dhcp snooping 的相关配置信息

例：

```
Ruijie# show ip dhcp snooping

Switch DHCP snooping status : ENABLE
Verification of hwaddr field status : DISABLE
DHCP snooping database write-delay time: 0(not write)
DHCP snooping option 82 status: ENABLE
DHCP snooping Support Bootp bind status: ENABLE
Interface                    Trusted
-----------------------      -------
FastEthernet0/11             yes
```

11.3.2. 显示 DHCP snooping 数据库信息

此命令用于显示 DHCP Snooping 数据库中的用户信息：

命令	说明
Ruijie# **show ip dhcp snooping binding**	查看 DHCP Snooping 绑定数据库中的用户信息

例如：

```
Ruijie# show ip dhcp snooping binding

Total number of bindings: 1

MacAddress     IpAddress  Lease  Type  VLAN  Interface
-------------  ---------------  ----------  -------------
00d0.f801.0101 192.168.1.1   -   static 1  fastethernet 0/1
```

11.3.3. DHCP snooping 调试开关

此命令用于打开 DHCP Snooping 的调试信息开关。

命令	说明
Ruijie**# debug ip dhcp snooping {event | packet}**	打开/关闭 DHCP Snooping 调试信息开关

例如：

```
Ruijie# debug ip dhcp snooping event
Ruijie# debug ip dhcp snooping packet
```

第12章 IGMP Snooping 配置

12.1. 概述

12.1.1. 理解 IGMP

在理解 IGMP 之前，首先介绍 IP 组播的概念及作用。

在 Internet 上，诸如视频会议和视频点播等单点发送多点接收的多媒体业务正在成为信息传送的重要组成部分。点对点的单播传输方式不能适应这一类业务传输特性，因为服务器必须为每一个接收者提供一个相同内容的 IP 报文拷贝，同时网络上也重复地传输相同内容的报文，占用了大量资源，IP 广播同样不能满足该要求，虽然 IP 广播允许一个主机把一个 IP 报文发送给同一个网络的所有主机，但是由于不是所有的主机都需要这些报文，因而浪费了网络资源。在这种情况下组播（Multicast）应运而生，它的出现解决了一个主机向特定的多个接收者发送消息的方法。如下图所示。

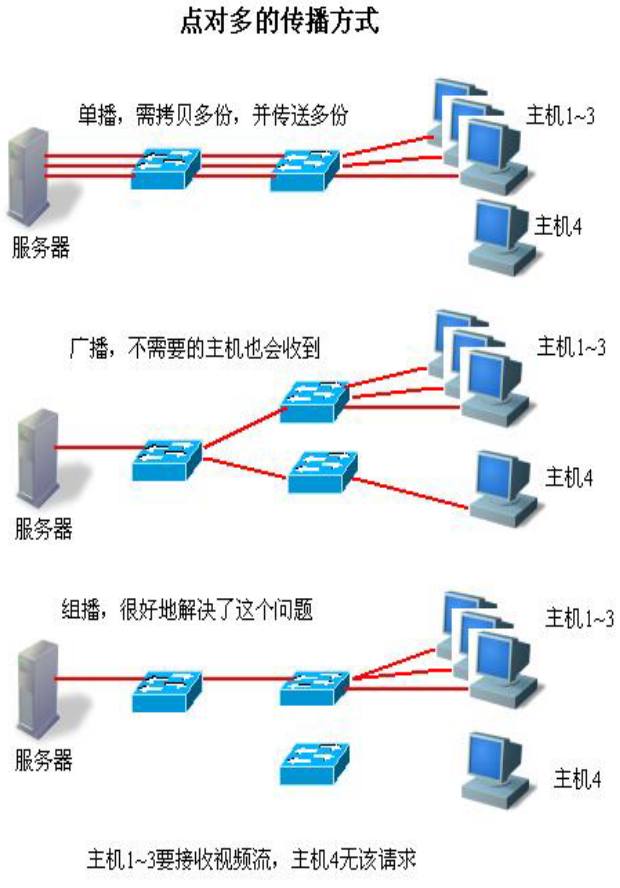


图 1

IP 组播是指一个 IP 报文向一个“主机组”的传送，这个包含 0 个或多个主机的主机组由一个单独的 IP 地址标识。

主机组地址也称为“组播地址”，又称为 D 类地址，即从 224.0.0.0 ~ 239.255.255.255。224.0.0.0~224.0.0.255 属于保留地址，其中：

- 224.0.0.1 － 网段中所有支持组播的主机
- 224.0.0.2 － 网段中所有支持组播的组播设备

第 2 层的组播地址（组播 MAC 地址）是从 IP 组播地址映射来的。把组播 IP 的后 23 位同 01-00-5e-00-00-00 进行或运算得到的结果便是组播 MAC 地址。如：组播 IP 地址为 224.255.1.1，其十六进制表示为 e0-ff-01-01，后 23 位为 7f-01-01，与 01-00-5e-00-00-00 进行或操作的结果为：01-00-5e-7f-01-01。01-00-5e-7f-01-01 即为组 224.255.1.1 的组播 MAC 地址。

IGMP(Internet Group Management Protocol)协议运行于主机和与主机直接相连的组播设备之间，主机通过此协议告诉本地组播设备希望加入并接受某个特定组播组的信息，同时路由设备通过此协议周期性地查询局域网内某个已知组的成员是否处于活动状态（即该网段是否仍有属于某个组播组的成员），实现所连接网络组成员关系的收集与维护。 。目前有三个版本的 IGMP：IGMPv1 在 RFC1112 中说明，IGMPv2 在 RFC 2236 中说明，IGMPv3 在 RFC3376 中说明。

下面，我们将分别简要介绍在 IGMPv1、IGMPv2 主机是如何加入或离开某一组播组的 （假设加入 224.1.1.1）。

IGMPv1 中，主机向组播设备上的某个接口发送 224.1.1.1 的 IGMP Report 报文，要求加入该组中。 组播设备收到该请求，则认为接收到请求的接口下存在组播成员，因而该接口转发对应组播组的报文。三层组播设备的接口定时发送 224.0.0.1（所有主机）的 IGMP Query 报文，若主机要继续接收该组报文，则应回应 IGMP Report 报文，如果某个接口收不到任何主机的 IGMP Report 报文，则认为该接口下不存在任何组播成员，因而不向该接口转发对应组的报文。

IGMPv2 向下兼容 v1，它对报文进行扩展——增加了 IGMP Leave 报文，以使主机可以主动要求离开组播组。在 IGMPv2 中，主机加入组中的过程同 v1 一致，主机发一个 IGMP Report 报文请求加入到某一组中。组播设备的查询者定时发送 224.0.0.1 的 IGMP Query 报文，若主机要接收该组报文，则应回应 IGMP Report 报文，若组播设备收不到任何主机的 IGMP Report 报文，将把该组注销。在 IGMPv2 中，主机还可以主动离开某一组。当主机不再需要某一组播流时，它主动朝组播设备发送 IGMP Leave 报文从该组中注销。组播设备的查询者收到 IGMP Leave 报文后，发出该组的 IGMP Query 报文来确定该组内是否还存在其他需要接收该组播消息的主机。这时若其它主机需要接收该组播，则将回应 IGMP Report 报文。若组播设备收不到任何主机的回应，将把该组注销。

在 IGMP v1/ v2 的基础上，IGMP v3 提供了额外的源过滤多播功能。IGMPv3 同组播路由设备的交互过程同 IGMPv2 相同。但是在 IGMP v1/ v2 中，主机只根据组地址来决定加入某个组并从任何一个源接收发给该组地址的组播流。而使用 IGMP v3 的主机不仅通告该主机所希望加入的多播组，同时还通告该主机所希望接收的多播源的地址。主机可以通过一个包括列表或一个排除列表来指明希望从

哪些源能接收多播流。同时 IGMP v3 带来的另外一个好处是节省带宽，避免不需要的、非法的组播数据流占用网络带宽，这尤其在多个多播源共用一个多播地址的网络环境中表现明显。

同 IGMPv2 对比，IGMPv3 的规定了以下两种报文类型：Membership Query 、Version 3 Membership Report。其中 Membership Query 分为三种：

- General Query：用于查询接口下所有多播成员信息；
- Group-Specific Query：用于查询接口下指定组的成员信息；
- Group-and-Source-Specific Query：该类型为 IGMPv3 中新增加的，用于查询接口下是否有成员需要接收指定源列表中的源所发出的特定组的多播流。

IGMP Version3 同时向下兼容 IGMP Version1 和 IGMP Version2。
要了解更多IP组播的相关知识，请查阅RFC 1112 、RFC 2236以及RFC 3376。

12.1.2. 理解 IGMP Snooping

在二层(Layer2)设备下，组播帧是作为广播转发的，这样容易造成组播流风暴，浪费网络带宽。网络上典型的组播帧是视频流，在某个 VLAN 中，如果有个用户注册了某组视频流，那么该 VLAN 中的所有成员都能收到这个视频流，无论他们是否想要。

IGMP Snooping 的作用便是解决这个问题的，它能使视频流只朝注册用户所在的端口转发，从而不会影响到其它的用户。

IGMP Snooping 是运行在以太网二层组播设备上的组播约束机制，监控组播路由设备和用户之间的 IGMP 报文，用于管理和控制组播组。IGMP Snooping 的中文含义是“窥探”，从这个词的含义我们就很容易理解它的工作过程：二层组播设备“窥探”用户主机与组播路由设备之间的交互报文，跟踪组信息及申请的端口。当二层组播设备“窥探”到主机朝组播路由设备发出的 IGMP report(请求)报文，二层组播设备便把该端口加入组播转发表中；当二层组播设备“窥探”到 IGMP Leave（离开）报文时，二层组播设备便把该端口从表中删除。组播路由设备会定时发IGMP Query报文，在收到IGMP Query报文后，如果在一定的时间段内没有收到主机的 IGMP Report 报文，便把该端口从表中删除。

12.1.3. 理解路由连接口

路由连接口就是连接三层组播设备的端口，如下图所示。

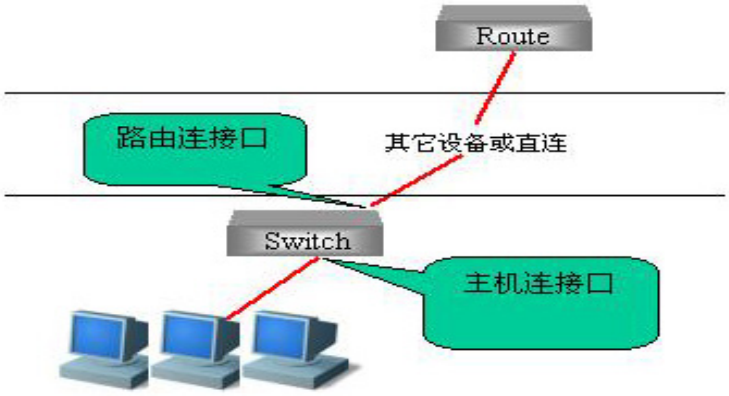


图 2

主机发出的 IGMP Report、IGMP Leave 等报文将从路由连接口转发向组播路由设备。只有从该端口收到的 IGMP Query 报文才被视为合法的报文转发向主机端口，从非路由连接口收到的 IGMP Query 报文将被丢弃。如何配置路由连接口请看配置路由连接口章节。

注意，在某些网络环境中，只要网络中不存在组播路由设备，就无需配置路由连接口，IGMP snooping 依然能正常运行。如下图：

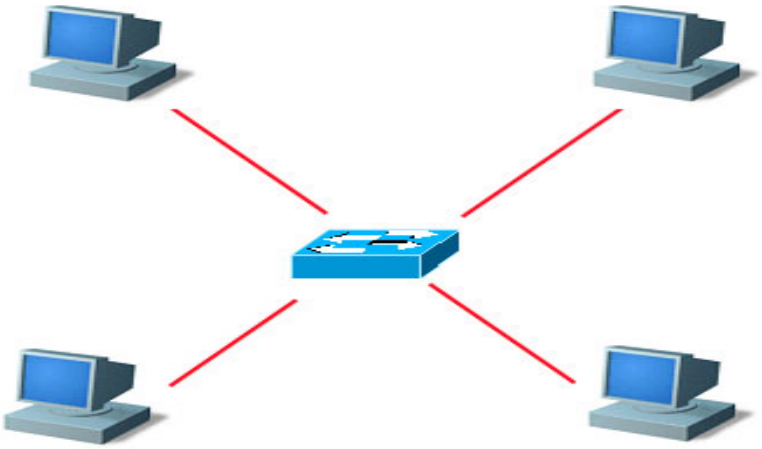


图 3

在这个网络环境中，没有组播路由设备，而这四台 PC 既可能是组播流的发送者，也可能是组播流的接收者，这时，中间的二层组播设备其实只要打开 IGMP snooping 就可满足需求，不必设置任何一个端口为路由连接口。

另外，路由连接口缺省就是要成为该 VLAN 内组播数据的接收者，如下图：

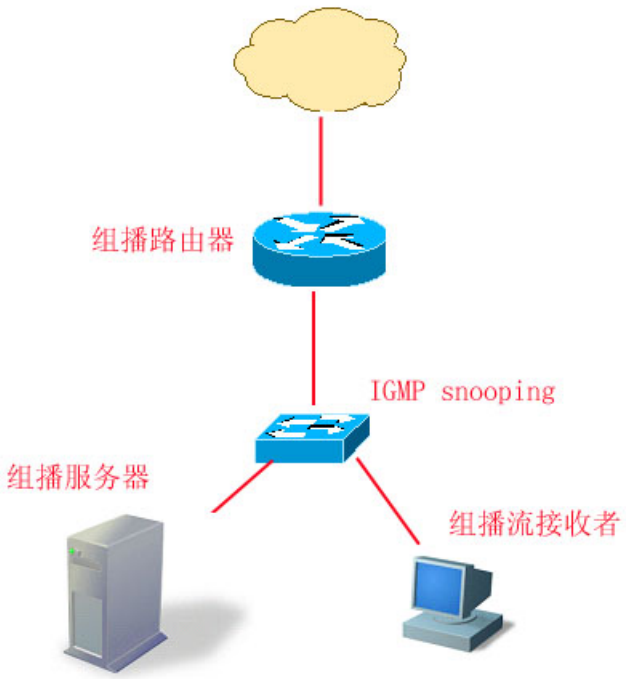


图 4

支持 IGMP Snooping 的二层组播设备不但要把组播数据转发给组播流的接收者，也要把组播数据转发给路由连接口，以便让组播路由设备将组播数据流转发给其他网络。但是有可能管理员不想把某一批组播数据让上级的组播路由设备知道，您可以在二层组播设备上配置路由连接口需要转发哪些组播数据、过滤哪些组播数据，以满足网络管理员的多种需求。

注意:

上图的网络拓朴中，如果没有“组播流接收者”，二层组播设备也会自动创建一条组播转发表项到组播路由设备，但这种由“组播数据流”产生的组播转发表项可能是不稳定的，路由连接口的变动将会删除组播数据流产生的组播转发表项；建议管理员直接配置一条静态的组播转发表项到路由连接口（请参见 配置IGMP snooping的静态成员），以保证组播流的稳定转发。

12.1.4. 理解 IGMP Snooping 的各种工作模式

DISABLE 模式：在该模式下，IGMP Snooping 不起作用，即二层组播设备不“窥探”主机与路由设备之间的 IGMP 报文，组播帧当广播在 VLAN 内转发。

IVGL 工作模式：在该模式下，各 VLAN 间的组播流是相互独立的。主机只能朝与自己处于同一个 VLAN 的路由连接口请求组播。

SVGL 工作模式：在该模式下，各 VLAN 的主机共享一组播流。主机可以跨 VLAN

申请组播流。指定一个 Multicast VLAN，在该 VLAN 收到的组播数据流可以向跨 VLAN 的其他主机转发。如下图所示：

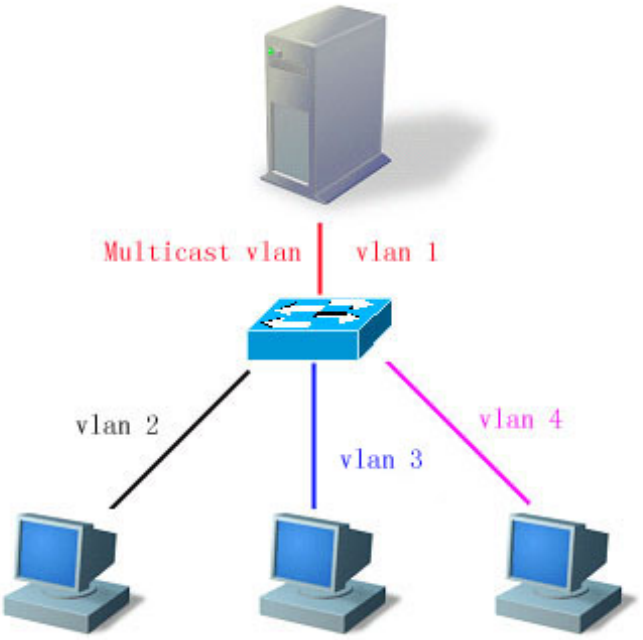


图 5

只要组播数据流的 VID 是 Multicast VLAN 的（或者 UNTAG 的数据流，接收端口的 native vlan 为 Multicast VLAN），都将转发给该组播地址的成员端口，无论该成员端口是不是这个 VLAN 内的。所形成的组播转发表的 VID 将是 Multicast VLAN 的。在 SVGL 模式下，除了路由连接口，其它端口只有有处于 Multicast VLAN 中，其发送的多播在才会 VLAN 中转发。

IVGL 和 SVGL 两种模式可以同时存在，您可以为划分一批组播地址范围给 SVGL，在这批组播地址内组播转发表（GDA 表）都是跨 VLAN 转发的，而其他的组播地址则使用 IVGL 模式。

锐捷二层组播设备实现的 IGMP Snooping 提供的 IVGL 模式与 SVGL 模式，增强了网络应用的灵活性，使之能适应不同的网络环境。

12.1.5. 理解 fast-leave

IGMP 协议对 Leave 报文的要求是“不能让端口马上离开组，应由组播路由设备发 IGMP Query 报文，主机无响应后，才能让端口离开该组”，但在特定环境中（如一个端口只连一个组播用户的环境中），IGMP Snooping 可以接收到 LEAVE 报文就直接离开，该功能称为 Fast Leave。

12.1.6. 理解 IGMP snooping suppression

对于启用 IGMP Snooping 的设备，每个组地址可能存在多个 IGMP 的用户，每个用户在加入组及收到 Query 报文时都会发送一个 Report 报文，而锐捷二层组播设备对于每一个 Report 报文都会转到组播路由设备，这样组播路由设备在发送一个 Query 到启用 Snooping 设备的端口时，会收到多个 Report 报文。为了减轻服务器处理 Report 报文的压力，当多台主机请求加入同一个多播组时，二层组播设备只把收到的第一个 Report 报文转发到路由口，其它的 Report 报文将被抑制。这种功能就是 IGMP Snooping Suppression.

由于 IGMP v3 Report 报文的特殊形式，IGMP Snooping Suppression 只支持 v1，v2 Report 报文的抑制。

12.1.7. 典型应用

组播的应用越来越大，最主要的是被应用于校园网与小区网中。组播技术可以应用于天气预报、新闻传送、视频点播等服务，目前最常见的是视频点播。普通的网络拓扑如下图所示。

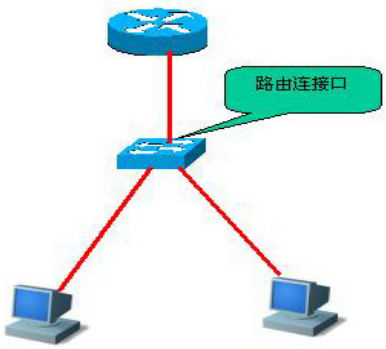


图 6

对设备的要求：二层组播设备支持 IGMP Snooping

需要的设置：

1. 打开 IGMP Snooping 功能
2. 设置上链为路由连接口

特点：

1. 配置简单
2. 能有效地减少广播风暴，提高网络带宽利用率

12.2. 配置 IGMP Snooping

我们将从以下几个章节描述如何配置 IGMP Snooping

- IGMP Snooping 的默认值
- 配置 IGMP Profiles
- 配置路由连接口
- 配置路由连接口转发组播帧的范围
- 配置 IVGL 模式
- 配置 SVGL 模式
- 配置 IVGL、SVGL 并存模式
- 配置 DISABLE 模式
- 配置 Query 报文的最长响应时间
- 配置 IGMP Snooping 的静态成员
- 配置 IGMP Filtering。

12.2.1. IGMP Snooping 的默认值

IGMP Snooping 状态	DISABLE 状态
路由连接口	所有的口均不是路由连接口，不进行动态学习。
源端口检查	关闭
IGMP Profile	表项为空，缺省行为是 Deny
SVGL 的 Multicast Vlan	VLAN 1
IGMP Filtering	无
IGMP Snooping 静态成员	无

注意:

您最好在配置好 VLAN、端口的 Access、Trunk、AP 属性后再进行 IGMP Snooping 的配置，否则就可能达不到您所预期的要求。因为以上这些属性都是二层组播设备的基本配置属性，如果在生成组播转发表后去修改这些属性，之后可能产生异常的转发效果。
另外，如果二层组播设备工作在 private vlan 模式下，则不支持 igmp snooping。

Igmp snooping 组播地址存在 Hash 冲突的可能性，如果某一时刻系统建立的组播个数还没有超过指标限制但添加新组播地址失败，那么很可能是 Hash 冲突了。

S23 系列产品在 Igmp snooping 开启后，目的 MAC 为多播地址的协议报文，如 OSPF 等会被当作未知名多播报文，当存在大量的管理报文或未知名多播报文时，就有可能导致这些协议报文无法被透传出去。

12.2.2. 配置 IGMP Profiles

这里要先介绍一个 IGMP Profile 表项，它可以定义一系列的组播地址范围，定义 permit/deny 动作，以提供后面的“SVGL 模式应用的组播地址范围”、“路由连接口过滤组播数据范围”、“IGMP Filtering 范围”各项功能使用。注意如果已经把一个 IGMP Profile 关联到一个功能应用上，再去修改它，会影响到该功能生成的组播转发表。

在配置模式下，按如下步骤设置一个 Profile：

命令	作用
Ruijie(config)**# ip igmp profile** *profile-number*	进入IGMP Profile模式，分配一个数字以供标识，该数字范围为 1－65535。
Ruijie (config-profile)**# permit | deny**	(可选)配置是要 permit 还是 deny 这一批组播地址范围，缺省值是 deny。这个行为表示：允许/禁止以下 range 内的这些组播地址，并禁止/允许其他的组播地址。
Ruijie(config-profile)**# range** *ip multicast-address*	添加组播地址范围，可添加多个。
Ruijie**# end**	退回到特权模式。

如果要删除其中一个 IGMP profile，可以用 **no ip igmp profile profile number** 来执行。

如果要删除 profile 里的一个 range，可以用 **no range ip multicast address** 来执行。

以下有个例子是表示 Profile 的配置过程：

```
Ruijie(config)# ip igmp profile 1
Ruijie(config-profile)# permit
Ruijie(config-profile)# range 224.1.1.1 225.1.1.1
Ruijie(config-profile)# range 226.1.1.1
Ruijie(config-profile)# end
Ruijie# show ip igmp profile 1
IGMP Profile 1
permit
```

```
range 224.1.1.1 225.1.1.1
range 226.1.1.1
```

按以上配置，这个 IGMP Profile 的规则就是 permit 224.1.1.1 到 225.1.1.1 的组播地址，以及 226.1.1.1 这个组播地址，其他的组播地址都被 deny。

12.2.3. 配置路由连接口

路由连接口是组播路由设备连接二层组播设备的端口（并不是指和视频流服务器连接的端口）。在源端口检查打开的情形下，只有从路由连接口进入的视频流才被转发，其它的将被丢弃。您可以静态地配置路由连接口，也可配置让二层组播设备动态的侦听 IGMP query/dvmrp 或 PIM 报文，以自动识别路由连接口。

在配置模式下，按如下步骤设置一个路由连接口：

命令	作用
Ruijie(config)**# ip igmp Snooping vlan** *vlan-id* **mrouter** {**interface** *interface-id* | **learnpim-dvmrp**}	设置接口为路由连接口，使用该命令的 **no** 选项删除一个路由连接口。您也可以配置让二层组播设备动态学习路由连接口；用相应的 **no** 命令来关闭动态学习，并清空所有动态学习到的路由连接口。缺省是不进行动态学习的。
Ruijie(config)**# end**	退回到特权模式

以下例子是设置以太网接口 1/1 为路由连接口，并配置自动学习路由连接口：

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping vlan 1 mrouter interface
gigabitEthernet 0/7
Ruijie(config)# ip igmp snooping vlan 1 mrouter learn pim-dvmrp
Ruijie(config)# end
Ruijie# show ip igmp snooping mrouter
Vlan    Interface        State       IGMP profile
----    ---------        ------      -------------
1   GigabitEthernet 0/7   static          0
1   GigabitEthernet 0/12  dynamic         0
Ruijie# show ip igmp snooping mrouter learn
Vlan   learn method
----   ------------------
1      pim-dvmrp
```

12.2.4. 配置路由连接口转发组播帧的范围

由于路由连接口缺省就要做为该 VLAN 内所有组播地址的成员，而转发组播数据流。但是有可能某些组播数据不希望转发给组播路由设备，管理员可以用 IGMP Profile 来过滤该路由连接口转发组播数据的范围。

在配置模式下，按如下步骤配置路由连接口转发组播帧的范围：

命令	作用
Ruijie(config)**# ip igmp snooping vlan** *vlan-id* **mrouter interface** *interface-id* **profile** *profile name*	设置该端口为这个路由连接口、并关联的 profile。符合该 profile 的组播流才会被转发到这个路由连接口上。
Ruijie(config)**# end**	退回特权模式。

您可以通过 **no ip igmp Snooping vlan** *vlan-id* **mrouter interface** *interface-id* **profile** 来删除与 profile 的关联。

以下是配置路由连接口转发组播帧的范围的实例：

```
Ruijie# configure terminal
Ruijie(config)# ip igmp Snooping vlan 1 mrouter interface
gigabitEthernet 0/7 profile 1
Ruijie(config)# end
Ruijie# show ip igmp Snooping mrouter
Vlan    Interface      State     IGMP profile
----    ---------      ------    -------------
1   GigabitEthernet 0/7    static        1
1   GigabitEthernet 0/12   dynamic       0
```

12.2.5. 配置动态学习的路由口的老化时间

在开启动态路由口学习时，动态学习的路由口会使用默认的 300s 作为老化时间，如果在老化时间内没有接收到新的学习 Mrtoue 口的报文，则会删除动态学到的路由口，而下边的命令则可以设置老化的时间，设置范围在 1-3600s。

在配置模式下，按如下步骤配置路由连接口转发组播帧的范围：

命令	作用
Ruijie(config)**# ip igmp snooping dyn-mr-aging-time** *time*	配置动态路由口老化时间，*time* ：<1-3600> 默认值为 300s。
Ruijie(config)**# end**	退回特权模式。

您可以通过 **no ip igmp snooping dyn-mr-aging-time** 来恢复老化时间为默认值。

以下是配置动态路由口老化时间为 100 的实例：

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping dyn-mr-aging-time 100
Ruijie(config)# end
```

12.2.6. 配置 IVGL 模式

在配置模式下，按如下步骤打开并设置 IGMP Snooping 为 IVGL 模式：

命令	作用
Ruijie(config)# **ip igmp Snooping ivgl**	打开并设置 IGMP Snooping 为 **IVGL** 模式。
Ruijie(config)# **end**	退回特权模式。

以下例子是打开并设置 IGMP Snooping 为 IVGL 模式：

```
Ruijie# configure Terminal
Ruijie(config)# IP igmp Snooping ivgl
Ruijie(config)# end
```

12.2.7. 配置 DISABLE 模式

在配置模式下，按如下步骤设置 IGMP Snooping 为 DISABLE 模式：

命令	作用
Ruijie(config)# **no ip igmp snooping**	关闭 IGMP Snooping
Ruijie(config)# **end**	退回特权模式。

12.2.8. 配置 Query 报文的最长响应时间

组播路由设备会定时发送 IGMP Query 报文来查询组播成员存不存在，如果在发出 Query 报文的一定时间内没有收到主机的 IGMP Report 报文，则会认为该端口不再接收组播流，二层组播设备会把该端口从组播转发表中删除。缺省时间为 10 秒

在配置模式下，按如下步骤设置 Query 报文的最长响应时间：

命令	作用
Ruijie(config)**# ip igmp snooping query-max-respone-time** *seconds*	设置 Query 报文的最长响应时间，范围为 1-65535，缺省时长为 10 秒
Ruijie(config)**# end**	退回特权模式。

使用 **no ip igmp Snooping query-max-respone-time** 命令恢复它的缺省值。

12.2.9. 配置 Fast-leave

在配置模式下，按如下步骤设置 **igmp snooping fast-leave** ：

命令	作用
Ruijie(config)**# ip igmp snooping fast-leave enable**	打开二层组播设备 fast-leave 功能能。
Ruijie(config)**# end**	退回特权模式。

使用 **no ip igmp snooping fast–leave enalbe** 命令关闭 fast-leave 功能。

以下例子是打开 fast–leave 功能：

```
Ruijie# configure Terminal
Ruijie(config)# ip igmp snooping fast–leave enalbe
Ruijie(config)# end
```

12.2.10. 配置 IGMP Snooping Suppression

在配置模式下，按如下步骤设置 **igmp snooping suppression**：

命令	作用
Ruijie(config)**# ip igmp snooping suppression enable**	打开二层组播设备 suppression 功能。
Ruijie(config)**# end**	退回特权模式。

使用 **no ip igmp snooping suppression enalbe** 命令关闭 Suppression 功能。

以下例子是打开 Suppression 功能：

```
Ruijie# configure Terminal
Ruijie(config)# ip igmp snooping suppression enalbe
Ruijie(config)# end
```

12.2.11. 配置 IGMP Snooping 的静态成员

您可以在 IGMP Snooping 打开的情况下，静态配置一个端口接收某个组播流，不受各种 IGMP 报文的影响。

在配置模式下，按如下步骤设置 IGMP Snooping 的静态成员：

命令	作用
Ruijie(config)# **ip igmp snooping ivgl**	打开并设置 IGMP Snooping 为 **IVGL** 模式。
Ruijie(config)# **ip igmp snooping vlan** *vlan-id* **static** *ip-addr* **interface** *interface-id*	静态配置一个端口接收某个组播流。 • *vlan-id*：组播流的 vid • *ip-addr*：组播地址 • *interface-id*： 端口号
Ruijie(config)# **end**	退回特权模式。

您可以用 **no ip igmp snooping vlan** *vlan-id* **static** *ip-addr* **interface** *interface-id* 删除组播成员的静态配置。

以下为配置 IGMP snooping 静态成员的实例：

```
Ruijie# configure Terminal
Ruijie(config)# ip igmp snooping vlan 1 static 224.1.1.1
interface GigabitEthernet 0/7
Ruijie(config)# end
Ruijie(config)# show ip igmp snooping gda
Abbr: M - mrouter
      D - dynamic
      S - static
VLAN  Address              Member ports
---- --------------   ----------------------------
1    224.1.1.1            GigabitEthernet 0/7(S)
```

12.2.12. 配置 IGMP Filtering

在某些情况下，您可能需要控制某个端口只能接收一批特定的组播数据流、控制该端口下最多允许动态加入多少组。IGMP Filtering 满足了这种需求。

您可以把某一个 IGMP Profile 应用在一个端口下，如果该端口收到 IGMP Report 报文，则二层组播设备就会查找这个端口所要加入的组播地址是否在 IGMP Profile 允许范围之内。若是，则允许加入，之后才进行后续处理。

您也可以在一个端口下配置最多允许加入的组的个数，超过范围，二层组播设备也不再接收、处理 IGMP Report 报文。

在配置模式下，按如下步骤配置 IGMP Filtering：

命令	作用
Ruijie(config)**# interface** *interface-id*	进入配置接口。
Ruijie(config-if)**# ip igmp snooping filter** *profile-number*	（可选）应用 Profile 于该端口，*profile number* 范围为 1- 65535.
Ruijie(config-if)**# ip igmp snooping max-groups** *number*	（可选）允许最多几个组动态的加入该端口,参数范围为 0 – 4294967294。
Ruijie(config-if)**# end**	退回特权模式。

12.3. 查看 IGMP Snooping 信息

我们提供的可查看的相关 IGMP snooping 的信息如下：

- 查看当前模式
- 查看路由连接口信息
- 查看动态转发表
- 查看源端口检查状态
- 查看 IGMP Profile
- 查看 IGMP Filtering

12.3.1. 查看当前模式

在特权模式下使用如下命令查看 IGMP Snooping 当前的工作模式及全局配置：

命令	作用
Ruijie**# show ip igmp snooping**	查看 IGMP Snooping 当前的工作模式及全局配置。

以下例子使用 **show ip igmp snooping** 命令查看 IGMP Snooping 配置信息：

```
Ruijie# show ip igmp snooping
Igmp-snooping mode    : IVGL
SVGL vlan-id          : 1
SVGL profile number    : 0
Source check port      : Disabled
Query max respone time : 10(Seconds)
```

12.3.2. 查看和清除 IGMP snooping 的统计值

在特权模式下使用如下命令查看和清除 IGMP Snooping 的统计值信息：

命令	作用
Ruijie**# show ip igmp snooping statistics** [**vlan** *vlan-id*]	查看 IGMP Snooping 的统计信息。
Ruijie**# clear ip igmp snooping statistics**	清除 IGMP Snooping 的统计信息

以下例子使用 **show ip igmp snooping statistics** 命令查看 IGMP Snooping 的路由连接口信息：

```
Ruijie# show ip igmp snooping statistics
GROUP    Interface    Last report       Last leave     Last
                        time          time         reporter
-------------- ----------- ------------  ------------   -
224.1.1.2 VL1:Gi4/2   0d:0h:0m:7s     ----    192.168.9.250
                        Report pkts: 1          Leave pkts: 0
```

12.3.3. 查看路由连接口信息

在特权模式下使用如下命令查看 IGMP Snooping 的路由连接口信息：

命令	作用
Ruijie**# show ip igmp snooping mrouter**	查看 IGMP Snooping 的路由连接口信息。

以下例子使用 **show ip igmp snooping** 命令查看 IGMP Snooping 的路由连接口信息：

```
Ruijie# show ip igmp snooping mrouter
Vlan    Interface       State     IGMP profile number
----     --------        -------     ------------------
1   GigabitEthernet 0/7    static        1
1   GigabitEthernet 0/12   dynamic       0
```

12.3.4. 查看动态转发表

在特权模式下使用如下命令查看各端口在组播组中的转发规则，即查看 GDA 表：

命令	作用

Ruijie**# show ip igmp snooping gda-table**	查看各端口在组播组中的转发规则表。

以下例子是查看 GDA 表的各组播组信息以及一个组播组的所有成员端口的信息：

```
Ruijie# show ip igmp snooping gda-table
Abbr: M - mrouter
      D - dynamic
      S - static
VLAN  Address            Member ports
------------------------------------------------------------
1      224.1.1.1          GigabitEthernet 0/7(S)
```

12.3.5. 查看 IGMP Profile

在特权模式下使用如下命令查看 IGMP Profile 信息：

命令	作用
Ruijie**# show ip igmp profile** *profile-number*	查看 IGMP Profile 信息。

12.3.6. 查看 IGMP Filtering

在特权模式下使用如下命令查看 IGMP Filtering 的配置信息：

命令	作用
Ruijie**# show ip igmp snooping interface** *interface-id*	查看 IGMP Filtering 的配置信息。

以下为查看 IGMP Filtering 的信息

```
Ruijie# show ip igmp snooping interface GigabitEthernet 0/7
Interface         Filter Profile number     max-groups
----------       ----------------------    -----------
GigabitEthernet 0/7          1               4294967294
```

12.4. 配置 IGMP Snooping 的其它限制

IGMP Snooping 的源端口检查要使用过滤域模板(Masks)，过滤域模板的定义详细参见《访问控制列表配置》章节。地址绑定、源端口检查和 ACL 这三种应用共享过滤域模板，可用的总模板数视不同产品而定。由于过滤域模板数量有限，所以这三种功能会相互影响。启用地址绑定功能需要占用两个模板，启用源端口检查占用两个模板，ACL 可用的模板取决于这两种功能是否启动。假设 ACL 在缺省

情况可使用 8 个模板，如果启用地址绑定和源端口检查其中任何一个功能，则 ACL 可使用的模板减少两个。如果同时启动地址绑定和源端口检查，则 ACL 可使用的模板数减少 4 个，只剩下 4 个。反过来，如果 ACL 使用了多个模板而使剩余模板数达不到这两种应用的要求时，则启用地址绑定、源端口检查功能时，系统会提示模板资源耗尽信息。当这三种功能的某个功能因为模板限制而无法正常运用时，可以通过减少其它两种功能的模板占用来实现该功能的正常应用。如三种功能同时启用时，打开源端口检查提示模板耗尽，则可以关闭地址绑定功能（删除所有地址绑定）或者删除占用多个模板的 ACL 的 ACE，源端口检查则可以正常启用。

在打开 IGMP Snooping 或者设置路由口时，如果打开源端口检查是打开的，则可能由于模板资源不足导致源端口检查功能失效，这时后系统提示：Source port check applying failed for hardware out of resources。这时候应该释放其它模板资源，重新关闭，然后打开源端口检查。

注意:

对于 S2300 系列组播设备，在打开 igmp snooping 的情况下，若 access 口收到非所在 vlan 的多播报文，并且该报文符合 igmp group 的转发规则，则组播设备还是会将报文转发到 igmp group 中注册的端口。

第13章 MSTP 配置

13.1. MSTP 概述

13.1.1. STP、RSTP

13.1.1.1. STP、RSTP 总述

本设备既支持 STP 协议，也支持 RSTP 协议，遵循 IEEE 802.1D 和 IEEE 802.1w 标准。

STP 协议是用来避免链路环路产生的广播风暴、并提供链路冗余备份的协议。

对二层以太网来说，两个 LAN 间只能有一条活动着的通路，否则就会产生广播风暴。但是为了加强一个局域网的可靠性，建立冗余链路又是必要的，其中的一些通路必须处于备份状态，如果当网络发生故障，另一条链路失效时，冗余链路就必须被提升为活动状态。手工控制这样的过程显然是一项非常艰苦的工作，STP 协议就自动地完成这项工作。它能使一个局域网中的设备起以下作用：

- 发现并启动局域网的一个最佳树型拓朴结构。
- 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）。

13.1.1.2. 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 都有了指定网桥（Designated Bridge），位于该 LAN 与根桥之间的最短路径中。指定网桥和 LAN 相连的端口称为指定端口（Designated Port）。
- 根口（Root port）和指定端口（Designated Port）进入 Forwarding 状态。
- 其他不在生成树中的端口就处于 Discarding 状态

13.1.1.3. Bridge ID

按 IEEE 802.1W 标准规定，每个网桥都要有单一的网桥标识（Bridge ID），生成树算法中就是以它为标准来选出根桥（Root Bridge）的。Bridge ID 由 8 个字节组成，后 6 个字节为该网桥的 mac 地址，前 2 个字节如果下表所示，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。

	Priority value				System ID											
Bit 位	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

值	32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

13.1.1.4. Spanning-Tree Timers（生成树的定时器）

以下描述影响到整个生成树性能的三个定时器。

- Hello timer：定时发送 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。

13.1.1.5. Port Roles and Port States

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

- 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

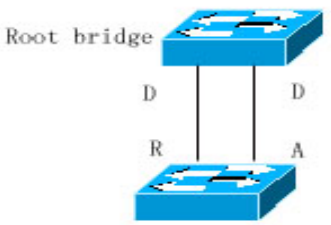


图 1

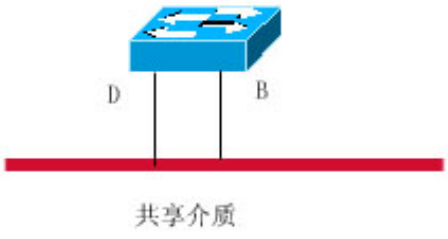


图 2

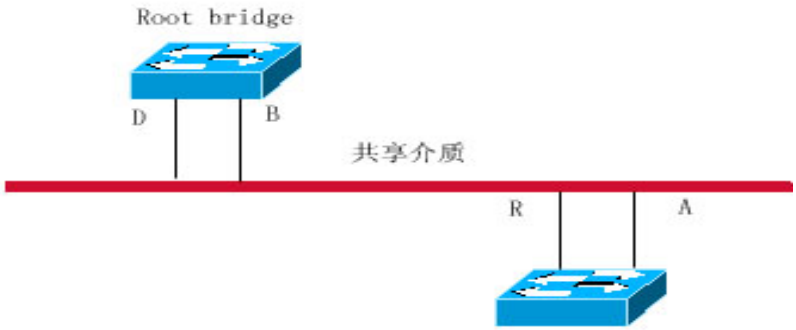


图 3

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。

13.1.1.6. 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 间为百兆链路，B 和 C 间为十兆链路。Switch A 做为该网络的骨干设备，对 Switch B 和 Switch C 都做了链路冗余，显然，如果让这些链路都生效是会产生广播风暴的。

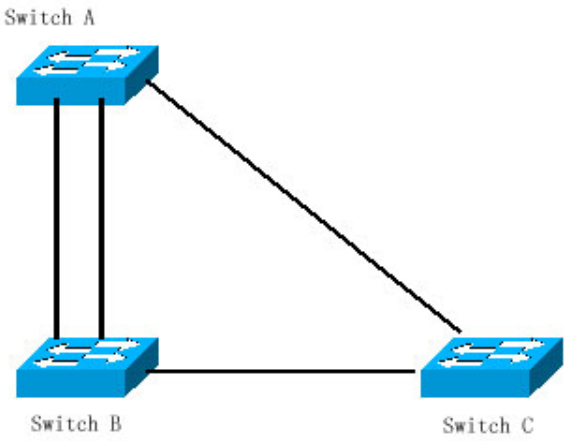


图 4

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。

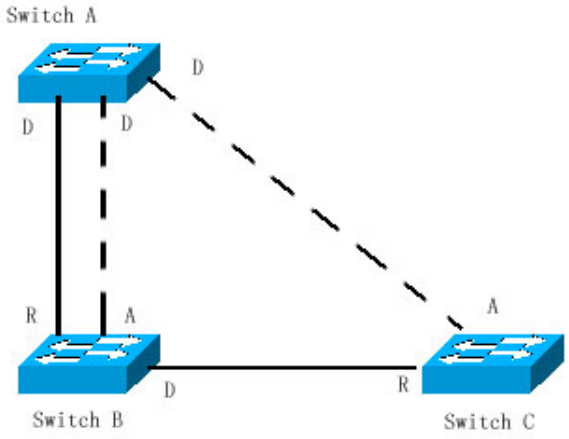


图 5

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。

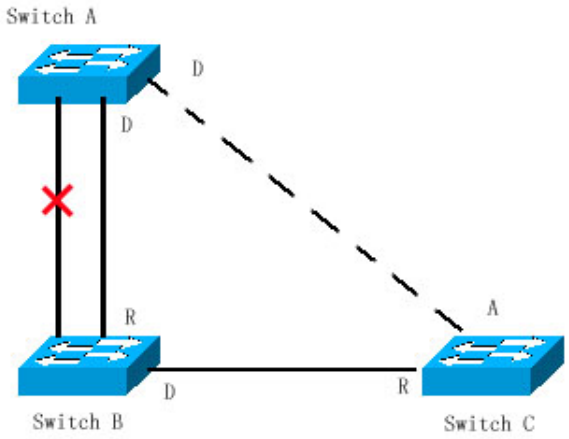


图 6

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。

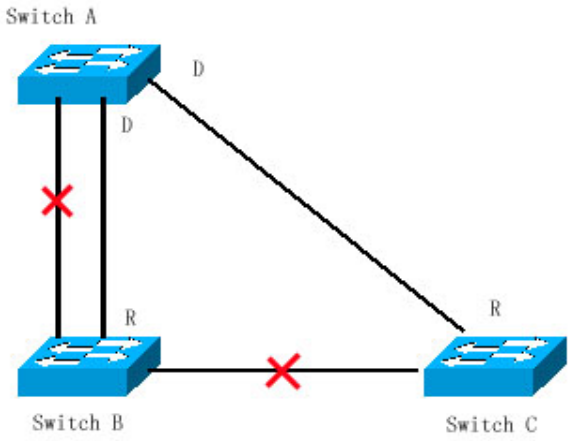


图 7

13.1.1.7. RSTP 的快速收敛

现在开始介绍 RSTP 所特有的功能，即能让端口“快速”的 Forwarding。

STP 协议是选好端口角色（Port Role）后等待 30 秒(为 Forward-Delay Time 的 2 倍，Forward-Delay Time 可配置，默认为 15 秒)后再 Forwarding 的，而且每当拓朴发生变化后，每个网桥的 Root Port 和 Designated Port 都要重新过 30 秒再 Forwarding，因此要等整个网络拓朴稳定为一个树型结构就大约需要 50 秒。

而 RSTP 端口的 Forwarding 过程就大不一样了，如图 8 所示，Switch A 发送 RSTP 特有“Proposal”报文，Switch B 发现 Switch A 的优先级比自身高，就选 Switch A 为根桥，收到报文的端口为 Root Port，立即 Forwarding，然后从 Root Port 向 Switch A 发送“Agree”报文。Switch A 的 Designated Port 得到“同意”，也就 Forwarding 了。然后 Switch B 的 Designated Port 又发送“Proposal”报文依次将生成树展开。因此在理论上，RSTP 是能够在网络拓朴发生变化的一瞬间恢复网络树型结构，达到快速收敛。

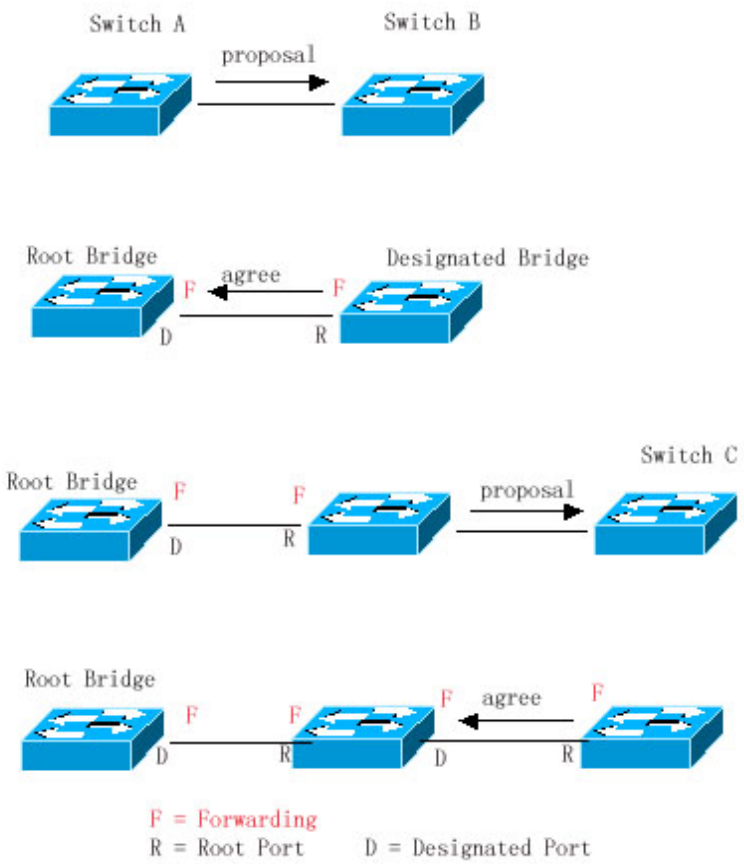


图 8

注意:

以上的“握手”过程是有条件的，就是端口间必须是“Point-to-point Connect（点对点连接）”。为了让您的设备发挥最大的功效，最好不要使设备间为非点对点连接。

本章中除图 9 外，其它示意图均为“点对点连接”，以下列出了“非点对点连接”的范例图。

非点对点连接范例：

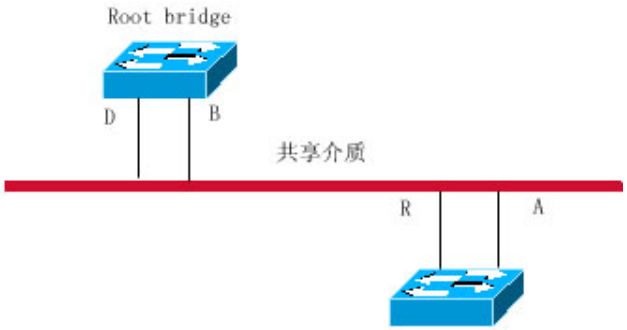


图 9

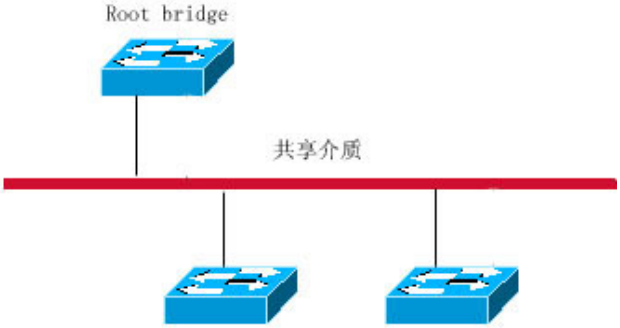


图 10

另外、下图为“点对点”连接，请用户注意区分

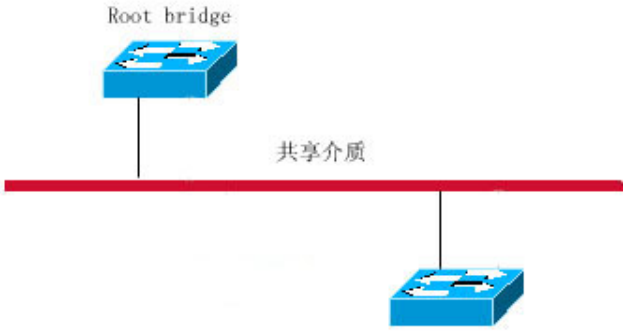


图 11

13.1.1.8. RSTP 与 STP 的兼容

RSTP 协议可以与 STP 协议完全兼容，RSTP 协议会根据收到的 BPDU 版本号来

自动判断与之相连的网桥是支持 STP 协议还是支持 RSTP 协议，如果是与 STP 网桥互连就只能按 STP 的 Forwarding 方法，过 30 秒再 Forwarding，无法发挥 RSTP 的最大功效。

另外，RSTP 和 STP 混用还会遇到这样一个问题。如图 12 所示，Switch A 是支持 RSTP 协议的，Switch B 只支持 STP 协议，它们俩互连，Switch A 发现与它相连的是 STP 桥，就发 STP 的 BPDU 来兼容它。但后来如果换了台 Switch C，它支持 RSTP 协议，但 Switch A 却依然在发 STP 的 BPDU，这样使 Switch C 也认为与之互连的是 STP 桥了，结果两台支持 RSTP 的设备却以 STP 协议来运行，大大降低了效率。

为此 RSTP 协议提供了 Protocol-migration 功能来强制发 RSTP BPDU(这种情况下，对端网桥必须支持 RSTP)，这样 Switch A 强制发了 RSTP BPDU，Switch C 就发现与之互连的网桥是支持 RSTP 的，于是两台设备就都以 RSTP 协议运行了，如图 13。

Protocol Migration

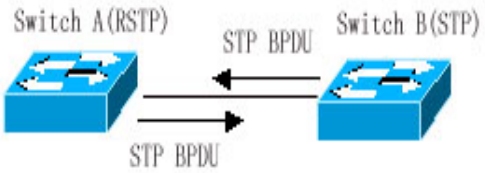


图 12

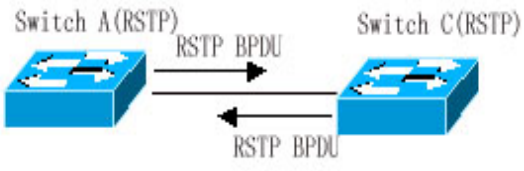


图 13

13.1.2. MSTP 概述

本设备支持 MSTP，MSTP 是在传统的 STP、RSTP 的基础上发展而来的新的生成树协议，本身就包含了 RSTP 的快速 FORWARDING 机制。

由于传统的生成树协议与 Vlan 没有任何联系，因此在特定网络拓朴下就会产生以下问题：

如图 14 所示，设备 A、B 在 Vlan1 内，设备 C、D 在 Vlan2 内，然后连成环路。

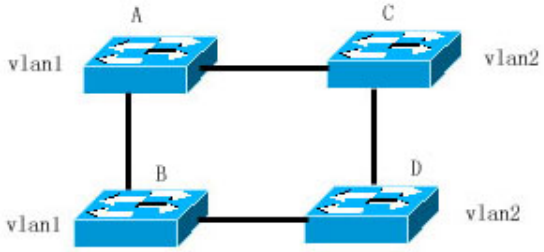


图 14

若从设备 A 依次通过设备 C、D 到达 B 的链路花费比从设备 A 直接到 B 的链路花费更少的情况下，会造成把设备 A 和 B 间的链路给 DISCARDING（如图 15 所示）。由于设备 C、D 不包含 Vlan1，无法转发 Vlan1 的数据包，这样设备 A 的 Vlan1 就无法与设备 B 的 Vlan1 进行通讯。

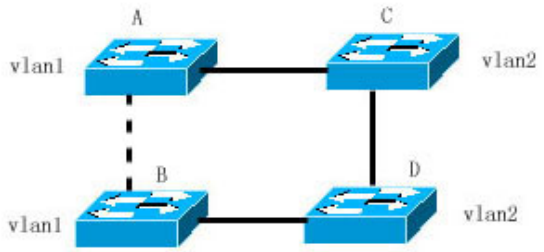


图 15

为了解决这个问题，MSTP 就产生了，它可以把一台设备的一个或多个 Vlan 划分为一个 Instance，有着相同 Instance 配置的设备就组成一个域（MST Region），运行独立的生成树（这个内部的生成树称为 IST，Internal Spanning-tree）；这个 MST region 组合就相当于一个大的设备整体，与其他 MST Region 再进行生成树算法运算，得出一个整体的生成树，称为 CST（Common Spanning Tree）。

按这种算法，以上网络就可以在 MSTP 算法下形成图 16 的拓朴：设备 A 和 B 都在 MSTP Region 1 内，MSTP Region 1 没有环路产生，所以没有链路 DISCARDING，同理 MSTP Region 2 的情况也是一样的。然后 Region 1 和 Region 2 就分别相当于两个大的设备，这两台“设备”间有环路，因此根据相关配置选择一条链路 DISCARDING。

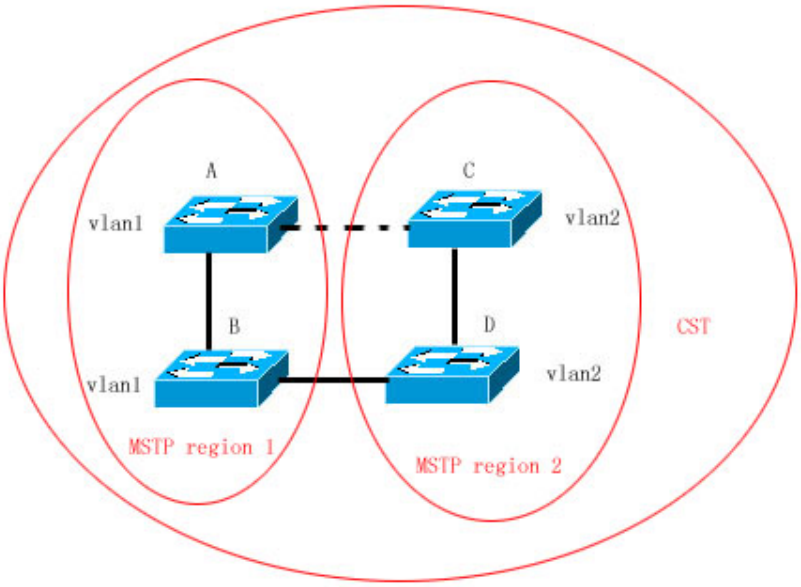


图 16

这样，既避免了环路的产生，也能让相同 Vlan 间的通讯不受影响。

13.1.2.1. 如何划分 MSTP Region

根据以上描述，很明显，要让 MSTP 产生应有的作用，首先就要合理地划分 MSTP Region，相同 MSTP Region 内的设备“MST 配置信息”一定要相同。

MST 配置信息包括：

- MST 配置名称（Name）：最长可用 32 个字节长的字符串来标识 MSTP Region。
- MST Revision Number：用一个 16bit 长的修正值来标识 MSTP Region。
- MST Instance—vlan 的对应表：每台设备都最多可以创建 64 个 Instance（id 从 1 到 64），Instance 0 是强制存在的，所以系统总共支持 65 个 Instance。用户还可以按需要分配 1-4094 个 Vlan 属于不同的 Instance（0－64），未分配的 Vlan 缺省就属于 Instance 0。这样，每个 MSTI（MST Instance）就是一个“Vlan 组”，根据 BPDU 里的 MSTI 信息进行 MSTI 内部的生成树算法，不受 CIST 和其他 MSTI 的影响。

您可在用 **spanning-tree mst configuration** 全局配置命令进入“MST 配置模式”配置以上信息。

MSTP BPDU 里附带以上信息，如果一台设备收到的 BPDU 里的 MST 配置信息和自身的一样，就会认为该端口上连着的设备和自己是属于同一个 MST Region，否则就认为是从另外一个 Region 来的。

建议：

建议在关闭 STP 的模式下配置 Instance—vlan 的对应表，配置好后再打开 MSTP，以保证网络拓朴的稳定和收敛。

13.1.2.2. MSTP region 内的生成树（IST）

划分好 MSTP Region 后，每个 Region 里就按各个 Instance 所设置的 Bridge Priority、Port Priority 等参数选出各个 Instance 独立的 Root Bridge，以及每台设备上各个端口的 Port Role，然后就 Port Role 指定该端口在该 Instance 内是 FORWARDING 还是 DISCARDING 的。

这样，经过 MSTP BPDU 的交流，IST(Internal Spanning Tree) 就生成了，而各个 Instance 也独立的有了自己的生成树（MSTI），其中 Instance 0 所对应的生成树与 CST 共同称为 CIST（Common Instance Spanning Tree）。也就是说，每个 Instance 都为各自的“vlan 组”提供了一条单一的、不含环路的网络拓朴。

如下图所示，在 Region 1 内，设备 A、B、C 组成环路。

在 CIST（Instance 0）中，如图 17，因 A 的优先级最高，被选为 Region Root，再根据其他参数，把 A 和 C 间的链路给 DISCARDING。因此，对 Instance 0 的“Vlan 组”来说，只有 A 到 B、B 到 C 的链路可用，打断了这个“Vlan 组”的环路。

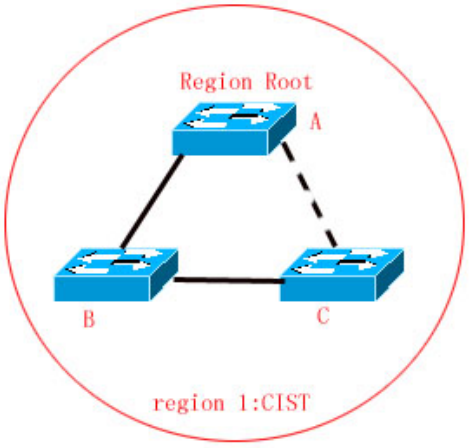


图 17

而对 MSTI 1（Instance 1）来说，如图 18，B 的优先级最高，被选为 Region Root，再根据其他参数，把 B 和 C 间的链路给 DISCARDING。因此，对 Instance 1 的“Vlan 组”来说，只有 A 到 B、A 到 C 的链路可用，打断了这个“Vlan 组”的环路。

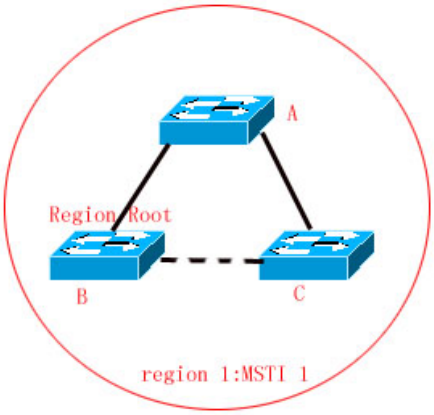


图 18

而对 MSTI 2（Instance 2）来说，图 19，C 的优先级最高，被选为 Region Root，再根据其他参数，把 A 和 B 间的链路给 DISCARDING。因此，对 Instance 2 的“Vlan 组”来说，只有 B 到 C、A 到 C 的链路可用，打断了这个“Vlan 组”的环路。

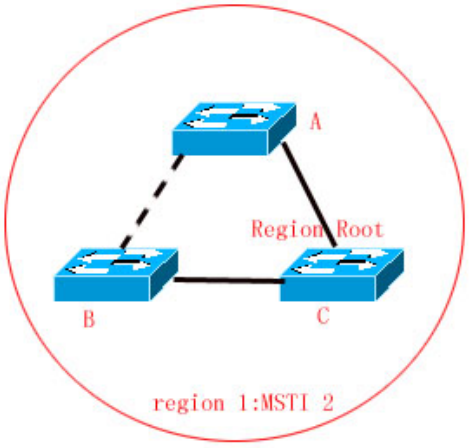


图 19

用户在这里要注意的是 MSTP 协议本身不关心一个端口属于哪个 Vlan，所以用户应该根据实际的 Vlan 配置情况来为相关端口配置对应的 Path Cost 和 Priority，以防 MSTP 协议打断了不该打断的环路。

13.1.2.3. MSTP region 间的生成树（CST）

每个 MSTP region 对 CST 来说可以相当于一个大的设备整体，不同的 MSTP Region 也生成一个大的网络拓朴树，称为 CST(Common Spanning Tree) 。如图 20 所示，对 CST 来说，Bridge ID 最小的设备 A 被选为整个 CST 的根(CST Root)，同时也是这个 Region 内的 CIST Regional Root。在 Region 2 中，由于设备 B 到 CST Root 的 Root Path Cost 最短，所以被选为这个 Region 内的 CIST Regional Root。同理，Region 3 选设备 C 为 CIST Regional Root。

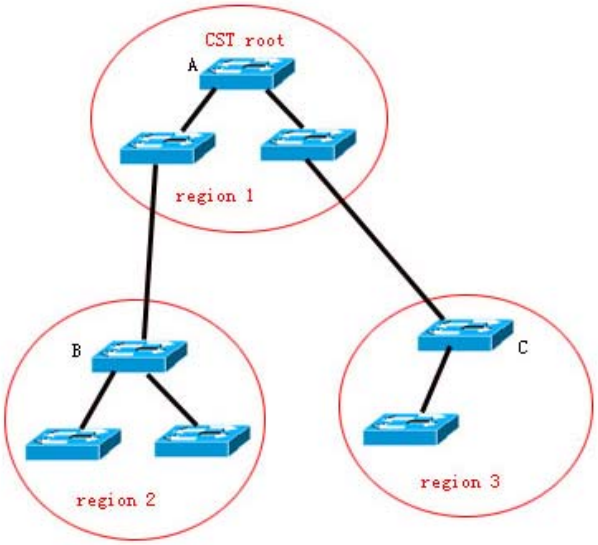


图 20

CIST Regional Root 不一定是该 Region 内 Bridge ID 最小的那台设备，它是指该 Region 内到 CST Root 的 Root Path Cost 最小的设备。

同时，CIST Regional Root 的 Root Port 对 MSTI 来说有了个新的 Port Role，为“Master port”，作为所有 Instance 对外的“出口”，它对所有 Instance 都是 FORWARDING 的。为了使拓朴更稳定，我们建议每个 Region 对 CST Root 的“出口”尽量只在该 Region 的一台设备上!

13.1.2.4. Hop Count

IST 和 MSTI 已经不用 Message Age 和 Max Age 来计算 BPDU 信息是否超时，而是用类似于 IP 报文 TTL 的机制来计算，它就是 Hop Count。

您可以用 **spanning-tree max-hops** 全局配置命令来设置。在 Region 内，从 Region Root Bridge 开始，每经过一个设备，Hop Count 就会减 1，直到为 0 则表示该 BPDU 信息超时，设备收到 Hops 值为 0 的 BPDU 就要丢弃它。

为了和 Region 外的 STP、RSTP 兼容，MSTP 依然保留了 Message Age 和 Max Age 的机制。

13.1.2.5. MSTP 和 RSTP、STP 协议的兼容

对 STP 协议来说，MSTP 会像 RSTP 那样发 STP BPDU 来兼容它，详细情况请参考“RSTP 与 STP 的兼容”章节。

而对 RSTP 协议来说，本身会处理 MSTP BPDU 中 CIST 的部分，因此 MSTP 不必专门的发 RSTP BPDU 以兼容它。

每台运行 STP 或 RSTP 协议的设备都是单独的一个 Region，不与任何一个设备组成同一个 Region。

13.2. MSTP 可选特性概述

13.2.1. 理解 Port Fast

如果设备的端口直连着网络终端，那么就可以设置该端口为 Port Fast，端口直接 Forwarding，这样可免去端口等待 Forwarding 的过程（如果不配置 Port Fast 的端口，就要等待 30 秒 Forwarding）。下图表示了一个设备的哪些端口可以配置为 Port Fast enable。

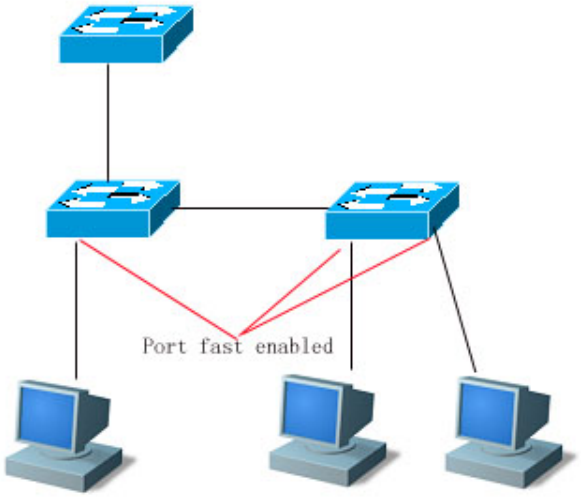


图 21

如果在设了 Port Fast 的端口中还收到 BPDU，则它的 Port Fast Operational State 为 Disabled。这时该端口会按正常的 STP 算法进行 Forwarding。

13.2.2. 理解边缘口的自动识别(AutoEdge 功能)

AutoEdge 功能是指当指定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不是一台网络设备，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。

您可以通过 **spanning-tree autoedge disabled** 命令取消边缘口的自动识别功能。

该功能是缺省打开的。

注意:

1) 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。

2) 该功能作用于指定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。同时如果指定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。

3) 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。

4) 该功能只适用与指定口。

5) AutoEdge 功能遵循 IEEE 802.1D 2004 版本的标准定义，在该版本中，Bridge Hello Time 参数的范围已修改为 1.0-2.0。所以在使用 AutoEdge 功能时请确认 Hello Time 时间在该范围内，超出了该范围可能会有临时环路的风险。如果确认需要将 Hello Time 值超出该范围，建议先将端口的 AutoEdge 功能关闭。

13.2.3. 理解 BPDU Guard

BPDU Guard 既能全局的 enable，也能针对单个 Interface 进行 enable。这两者有些细小的差别。

您可以在特权模式中用 **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 或者该端口自动标识为边缘端口，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。

您也可以在 Interface 配置模式下用 **spanning-tree bpduguard enable** 命令来打开单个 Interface 的 BPDU Guard（与该端口是否是边缘端口无关）。在这个情况下如果该 Interface 收到了 BPDU，就进入 Error-disabled 状态。

当接口因 BPDU Guard 功能生效而进入 Error-disabled 状态时，可以通过在全局配置模式下使用 **errdisable recover** 命令来将接口从错误状态中恢复过来。

13.2.4. 理解 BPDU Filter

BPDU Filter 既能全局的 enable，也能针对单个 Interface 进行 enable。这两者有些细小的差别。

您可以在特权模式中用 spanning-tree portfast bpdufilter default 命令打开全局的 BPDU Filter enabled 状态，在这种状态下，如果某个 Interface 打开了 Port Fast 或者该端口自动标识为边缘端口，则该接口将既不收 BPDU，也不发 BPDU，这样，直连端口的主机就收不到 BPDU。而如果边缘端口因收到 BPDU 而使 Port

Fast Operational 状态 disabled，BPDU Filter 也就自动失效。

您也可以在 Interface 配置模式下用 spanning-tree bpdufilter enable 命令设置单个 Interface 的 BPDU Filter enable（与该端口是否是边缘端口无关）。在这个情况下该 Interface 既不收 BPDU，也不发 BPDU，并且是直接 Forwarding 的。

13.2.5. 理解 TC Guard

网络中遇到 TC 报文攻击的时候会产生很多的地址删除操作，并且 TC 报文是可扩散的，将影响整个网络。使用 TC Guard 功能，我们允许用户在全局或者端口上禁止 TC 报文的扩散。当一个端口收到 TC 报文的时候，如果全局配置了 TC Guard 或者是端口上配置了 TC Guard，则该端口将屏蔽掉该端口接收或者是自己产生的 TC 报文，使得 TC 报文不会扩散到其它端口，这样能有效控制网络中可能存在的 TC 攻击，保持网络的稳定，尤其是在三层设备上，该功能能有效避免接入层设备的振荡引起核心路由中断的问题。

注意:

1) 错误的使用 tc-guard 功能会使网络之间的通讯中断。

2) 建议您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。

3) 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。

4) 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。

13.2.6. 理解 BPDU 源 MAC 检查

BPDU 源 MAC 检查是为了防止通过人为发送 BPDU 报文来恶意攻击交换机而使 MSTP 工作不正常。当确定了某端口点对点链路对端相连的交换机时，可通过配置 BPDU 源 MAC 检查来达到只接收对端交换机发送的 BPDU 帧，丢弃所有其他 BPDU 帧，从而达到防止恶意攻击。你可以在 interface 模式下来为特定的端口配置相应的 BPDU 源 MAC 检查 MAC 地址，一个端口只允许配置一个过滤 MAC 地址，通过 no bpdu src-mac-check 来禁止 BPDU 源 MAC 检查，此时端口接收任何 BPDU 帧。

13.2.7. 理解 BPDU 非法长度过滤

BPDU 的以太网长度字段超过 1500 时，该 BPDU 帧将被丢弃，以防止收到非法 BPDU 报文。

13.2.8. 理解 Root Guard 功能

在网络设计中常常将根桥和备份根桥划分在同一个域内，由于维护人员的错误配置或网络中的恶意攻击，根桥有可能收到优先级更高的配置信息，从而失去当前根桥的位置，引起网络拓扑的错误的变动。Root Guard 功能就是为了防止这种情况的出现。

启用 Root Guard 功能的接口，将强制其在所有实例上的端口角色为指定端口。当收到优先级更高的 BPDU 配置信息时，启用 Root Guard 功能的接口状态将被设置为 root-inconsistent (blocked)。

接口状态被 Root Guard 特性设置为 blocked 状态后，需要通过关闭 Root Guard 功能或关闭接口的保护功能（即在接口配置模式下使用 **spanning-tree guard none 命令**），使之恢复为正常状态。

注意:

1) 错误的使用 Root Guard 特性会导致二层网络通信中断。

2) 非指定端口在启用 Root Guard 功能后，会被强制为指定口，同时端口状态切换为 Blocked 状态。

3) 启用 Root Guard 特性的端口如果在 MST0 收到更优的 BPDU 配置消息，会强制其在所有的实例中的端口状态为 Blocked 状态。

4) 同一个端口不能同时启用 Root Guard 和 Loop Guard 特性。

5) 启用 Root Guar 特性后，边缘端口的自动识别功能将失效。

13.2.9. 理解 Loop Guard 功能

在 STP 中，交换机的根端口和其他阻塞端口的状态依靠不断接收上游交换机发送的 BPDU 来维持的。但是由于链路拥塞或者单向链路故障，这些端口可能因收不到上游设备的 BPDU 而变成指定端口，原本阻塞的端口会迁移到 Forwarding 状态，导致交换网络产生环路。Loop Guard 功能能够抑制这种环路的产生。

对于配置了 Loop Guard 功能的端口，当一定时间内接收不到上游设备发送的 BPDU 报文时，Loop Guard 功能随即生效，把端口状态设置为 loop-inconsistent (Block）这个过渡状态来抑制环路的产生。直到端口重新收到 BPDU 报文时，端口才会从 loop-inconsistent 状态中恢复，重新开始生成树计算。

注意:

1) 可基于全局或接口启用 Loop Guard 特性。

2) 同一个端口不能同时启用 Root Guard 和 Loop Guard 特性。

3) 启用 Loop Guard 特性后，边缘端口的自动识别功能将失效。

13.3. 配置 MSTP

13.3.1. 缺省的 Spanning Tree 设置

下面列出 Spanning Tree 的缺省配置

项目	缺省值
Enable State	Disable，不打开 STP
STP MODE	MSTP
STP Priority	32768
STP port Priority	128
STP port cost	根据端口速率自动判断
Hello Time	2 秒
Forward-delay Time	15 秒
Max-age Time	20 秒
Path Cost 的缺省计算方法	长整型
Tx-Hold-Count	3
Link-type	根据端口双工状态自动判断
Maximum hop count	20
vlan 与 实例 对应关系	所有 vlan 属于实例 0 只存在实例 0

您可通过 **spanning-tree reset** 命令让 Spanning Tree 参数恢复到缺省配置(不包括关闭 Span)

13.3.2. 打开、关闭 Spanning Tree 协议

打开 Spanning-tree 协议，设备即开始运行生成树协议，本设备缺省运行的是 MSTP 协议。

设备的缺省状态是关闭 Spanning-tree 协议。

进入特权模式，按以下步骤打开 Spanning Tree 协议：

命令	作用
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。

如果您要关闭 Spanning Tree 协议，可用 **no spanning-tree** 全局配置命令进行设置。

13.3.3. 配置 Spanning Tree 的模式

按 802.1 相关协议标准，STP、RSTP、MSTP 这三个版本的 Spanning Tree 协议本来就无须管理员再多做设置，版本间自然会互相兼容。但考虑到有些厂家不完全按标准实现，可能会导致一些兼容性的问题。因此我们提供这么一条命令配置，以供管理员在发现其他厂家的设备与本设备不兼容时，能够切换到低版本的 Spanning Tree 模式，以兼容之。

注意，当您从 MSTP 模式切换到 RSTP 或 STP 模式时，有关 MSTP Region 的所有的信息将被清空。

设备的缺省模式是 MSTP 模式。

进入特权模式，按以下步骤打开 Spanning Tree 协议：

命令	作用
Ruijie**# configure terminal**	进入全局配置模式。
Ruijie(config)**# spanning-tree mode mstp/rstp/stp**	切换 Spanning Tree 模式。
Ruijie(config)**# end**	退回到特权模式。
Ruijie**# show spanning-tree**	核对配置条目。
Ruijie**# copy running-config startup-config**	保存配置。

如果您要恢复 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。

13.3.4. 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。您可以给不同的 Instance 分配不同的设备优先级，各个 Instance 可根据这些值运行独立的生成树协议。对于不同 Region 间的设备，它们只关心 CIST（Instance 0）的优先级。

如 Bridge ID 所讲，优先级的设置值有 16 个，都为 4096 的倍数，分别是 0，4096，8192，12288，16384，20480，24576，28672，32768，36864，40960，45056，49152，53248，57344，61440。缺省值为 32768。

进入特权模式，按以下步骤配置设备优先级：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **spanning-tree** [**mst** *instance-id*] **priority** *priority*	针对不同的 instance 配置设备的优先级，当您不加 instance 参数时，即对 instance 0 进行配置。 *instance-id*，范围为 0－64 *priority*，取值范围为 0 到 61440，按 4096 的倍数递增，缺省值为 32768。
Ruijie(config)# **end**	退回到特权模式。
Ruijie# **show running-config**	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

您如果要恢复到缺省值，可用 **no spanning-tree mst** *instance-id* **priority** 全局配置命令进行设置。

13.3.5. 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。您可以在一个端口上给不同的 Instance 分配不同的端口优先级，各个 Instance 可根据这些值运行独立的生成树协议。

和设备的优先级一样，可配置的优先级值也有 16 个，都为 16 的倍数，分别是 0，16，32，48，64，80，96，112，128，144，160，176，192，208，224，240。缺省值为 128。

进入特权模式，按以下步骤配置端口优先级：

命令	作用

Ruijie**# configure terminal**	进入全局配置模式。
Ruijie(config)**# interface** *interface-id*	进入该 interface 的配置模式，合法的 interface 包括物理端口和 Aggregate Link。
Ruijie(config-if)**# spanning-tree** [**mst** *instance-id*] **port-priority** *priority*	针对不同的 instance 配置端口的优先级，当您不加 instance 参数时，即对 instance 0 进行配置。 *instance-id*，范围为 0－64 *priority*，配置该 interface 的优先级，取值范围为 0 到 240，按 16 的倍数递增，缺省值为 128
Ruijie(config-if)**# end**	退回到特权模式。
Ruijie**# show spanning-tree** [**mst** *instance-id*] **interface** *interface-id*	核对配置条目。
Ruijie**# copy running-config startup-config**	保存配置。

您如果要恢复到缺省值，可用 **no spanning-tree mst** *instance-id* **port-priority** 接口配置命令进行设置。

13.3.6. 配置端口的路径花费（Path Cost）

设备是根据哪个端口到根桥（Root Bridge）的 Path Cost 总和最小而选定 Root Port 的，因此 Port Path Cost 的设置关系到本设备 Root Port。它的缺省值是按 Interface 的链路速率（The Media Speed）自动计算的，速率高的花费小，如果管理员没有特别需要可不必更改它，因为这样算出的 Path Cost 最科学。您可以在一个端口上针对不同的 Instance 分配不同的路径花费，各个 Instance 可根据这些值运行独立的生成树协议。

进入特权模式，按以下步骤配置端口路径花费：

命令	作用
Ruijie**# configure terminal**	进入全局配置模式。
Ruijie(config)**# interface** *interface-id*	进入该 interface 的配置模式，合法的 interface 包括物理端口和 Aggregate Link。
Ruijie(config-if)**# spanning-tree** [**mst** *instance-id*] **cost** *cost*	针对不同的 instance 配置端口的优先级，当您不加 instance 参数时，即对 instance 0 进行配置。 *instance-id*，范围为 0－64 *cost* ，配置该端口上的花费，取值范围为 1 到 200,000,000。缺省值为根据 interface 的链路速率自动计算。
Ruijie(config-if)**# end**	退回到特权模式。

Ruijie# **show spanning-tree** [**mst** *instance-id*] **interface** *interface-id*	核对配置条目。
Ruijie# **copy running-config startup-config**	保存配置。

您如果要恢复到缺省值，可用 **no spanning-tree mst cost** 接口配置命令进行设置。

13.3.7. 配置 Path Cost 的缺省计算方法（path cost method）

当该端口 Path Cost 为缺省值时，设备会自动根据端口速率计算出该端口的 Path Cost。但 IEEE 802.1d 和 IEEE 802.1t 对相同的链路速率规定了不同 Path Cost 值，802.1d 的取值范围是短整型（short）（1—65535），802.1t 的取值范围是长整型（long）(1—200,000,000)。请管理员一定要统一好整个网络内 Path Cost 的标准。缺省模式为长整型模式（IEEE 802.1t 模式）。

下表列出两种方法对不同链路速率自动设置的 Path Cost。

端口速率	Interface	IEEE 802.1d（short）	IEEE 802.1t（long）
10M	普通端口	100	2000000
	Aggregate Link	95	1900000
100M	普通端口	19	200000
	Aggregate Link	18	190000
1000M	普通端口	4	20000
	Aggregate Link	3	19000

进入特权模式，按以下步骤配置端口路径花费的缺省计算方法：

命令	作用
Ruijie# **configure terminal**	进入全局配置模式。
Ruijie(config)# **spanning-tree pathcost method long/short**	配置端口路径花费的缺省计算方法，设置值为长整型（long）或短整型（short），缺省值为长整型（long）。
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。

13.3.8. 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。

13.3.9. 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。

13.3.10. 配置 Max-Age Time

配置 BPDU 报文消息生存的最长时间。缺省值为 20 秒。

进入特权模式，按以下步骤配置 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。

注意：

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，否则有可能导致拓朴不稳定。

13.3.11. 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。

13.3.12. 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。

13.3.13. 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

13.3.14. 配置 MSTP Region

要让多台设备处于同一个 MSTP Region，就要让这几台设备有相同的名称（Name）、相同的 Revision Number、相同的 Instance—Vlan 对应表。

你可以配置 0－64 号 Instance 包含哪些 Vlan，剩下的 Vlan 就自动分配给 Instance 0。一个 Vlan 只能属于一个 Instance。

我们建议您在关闭 STP 的模式下配置 Instance—Vlan 的对应表，配置好后再打开 MSTP，以保证网络拓朴的稳定和收敛。

进入特权模式，按以下步骤配置 MSTP Region：

命令	作用
Ruijie**# configure terminal**	进入全局配置模式。
Ruijie(config)**# spanning-tree mst configuration**	进入 MST 配置模式。
Ruijie(config-mst)**# instance** *instance-id* **vlan** *vlan-range*	把 vlan 组添加到一个 MST instance 中 *instance-id*，范围为 0－64 *vlan-range*，范围为 1－4094 举例来说： instance 1 vlan 2-200 就是把 vlan 2 到 vlan 200 都添加到 instance 1 中。 instance 1 vlan 2,20,200 就是把 vlan 2、vlan 20，vlan 200 添加到 instance 1 中。 同样，您可以用 **no** 命令把 vlan 从 instance 中删除，删除的 vlan 自动转入 instance 0。
Ruijie(config-mst)**# name** *name*	指定 MST 配置名称，该字符串最多可以有 32 个字节。
Ruijie(config-mst)**# revision** *version*	指定 MST revision number，范围为 0－65535。缺省值为 0
Ruijie(config-mst)**# show**	核对 MST 的配置条目。
Ruijie(config-mst)**# end**	退回到特权模式。
Ruijie**# copy running-config startup-config**	保存配置。

要恢复缺省的 MST Region Configuration 配置，您可以用 **no spanning-tree mst configuration** 全局配置命令。您也可以用 **no instance** *instance-id* 来删除该 instance。同样，**no name**、**no revision** 可以分别把 MST name、MST revision number 恢复到缺省值。

以下为配置实例：

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

```
Ruijie(config-mst)# instance 1 vlan 10-20
Ruijie(config-mst)# name region1
Ruijie(config-mst)# revision 1
Ruijie(config-mst)# show
Multi spanning tree protocol : Enable Name [region1]
Revision 1
Instance Vlans Mapped
-------- --------------------
0 1-9,21-4094
1 10-20
------------------------------
Ruijie(config-mst)# exit
Ruijie(config)#
```

注意:

在配置 vlan 和 instance 的映射关系前请务必确保所配置的 vlan 已经被创建，否则在部分产品上有可能会出现 vlan 和 instance 关联失败。

13.3.15. 配置 Maximum-Hop Count

配置 Maximum-Hop Count，指定了 BPDU 在一个 Region 内经过多少台设备后被丢弃。它对所有 Instance 有效。

进入特权模式，按以下步骤配置 Maximum-Hop Count：

命令	作用
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。

13.3.16. 配置接口的兼容性模式

配置接口的兼容性模式，可以使该端口发送 BPDU 时根据当前端口的属性有选择的携带不同的 MSTI 的信息，以实现与其它厂商之间的互连。

进入特权模式，按以下步聚配置接口的兼容性模式：

命令	作用
Ruijie**# configure terminal**	进入全局配置模式。
Ruijie(config)**#interface** *interface-id*	进入接口配置模式
Ruijie(config-if)**# spanning-tree compatible enable**	打开接口的兼容性模式
Ruijie(config-if)**# end**	退回到特权模式。
Ruijie**# show running-config**	核对配置条目。
Ruijie**# copy running-config startup-config**	保存配置。

您如果要取消该配置，可用 **no spanning-tree compatible enable** 接口配置命令进行设置。

13.4. 配置 MSTP 可选特性

13.4.1. 缺省的生成树可选特性设置

边缘口的自动识别功能(AutoEdge 功能)默认打开。
其它可选特性的缺省值默认都是关闭的。

13.4.2. 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。

13.4.3. 关闭边缘口的自动识别

如果在一定的时间范围内(为 3 秒)，如果指定口没有收到 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。

13.4.4. 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 bpduguard 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。

13.4.5. 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 bpdufilter 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。

13.4.6. 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。

13.4.7. 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。

13.4.8. 启用 Root Guard 特性

进入特权模式，按以下步骤启用接口的 Root Guard 特性

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，可配置的接口包括物理口和 Aggregate Link。
Ruijie(config-if)**# spanning-tree guard root**	启用 Root Guard 特性
Ruijie**# show running-config**	核对配置条目。
Ruijie**# copy running-config startup-config**	保存配置。

13.4.9. 启用 Loop Guard 特性

进入特权模式，按以下步骤全局启用 Loop Guard 特性

命令	作用
Ruijie**# configure terminal**	进入全局配置模式。
Ruijie(config)**# spanning-tree Loopguard default**	全局启用 Loop Guard 特性。
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，按以下步骤基于接口启用 Loop Guard 特性

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。可配置的接口包括物理口和 Aggregate Link。
Ruijie(config-if)**# spanning-tree guard loop**	启用 Loop Guard 特性。
Ruijie**# show running-config**	核对配置条目。
Ruijie**# copy running-config startup-config**	保存配置。

13.4.10. 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*	进入接口配置模式。可配置的接口包括物理口和 Aggregate Link。
Ruijie(config-if)**# spanning-tree guard none**	在接口模式下，关闭根防护或环路防护特性
Ruijie**# show running-config**	核对配置条目。
Ruijie**# copy running-config startup-config**	保存配置。

13.5. 显示 MSTP 配置和状态

MSTP 提供了如下的显示命令命令用于查看各种配置信息及运行时信息，各命令的功能说明如下：

命令	含义
Ruijie**# show spanning-tree**	显示 MSTP 的各项参数信息及生成树的拓扑信息

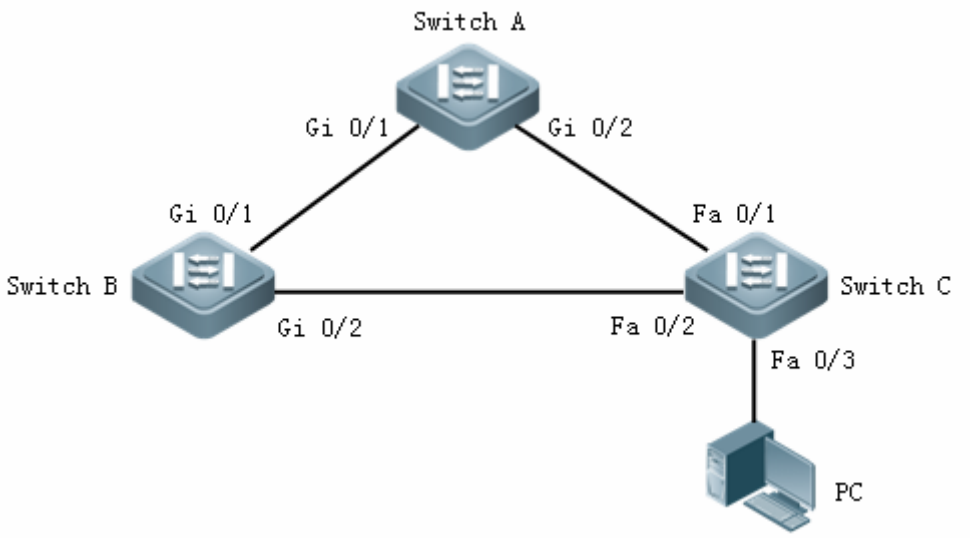
Ruijie# **show spanning-tree summary**	显示 MSTP 的各 instance 的信息及其端口转发状态信息
Ruijie# **show spanning-tree inconsistentports**	显示因根保护或环路保护而 block 的端口
Ruijie# **show spanning-tree mst configuration**	显示 MST 域的配置信息
Ruijie# **show spanning-tree mst** *instance-id*	显示该 instance 的 MSTP 信息
Ruijie# **show spanning-tree mst** *instance-id* **interface** *interface-id*	显示指定 interface 的对应 instance 的 MSTP 信息
Ruijie# **show spanning-tree interface** *interface-id*	显示指定 interface 的所有 instance 的 MSTP 信息
Ruijie# **show spanning-tree forward-time**	显示 forward-time
Ruijie# **show spanning-tree Hello time**	显示 Hello time
Ruijie# **show spanning-tree max-hops**	显示 max-hops
Ruijie# **show spanning-tree tx-hold-count**	显示 tx-hold-count
Ruijie# **show spanning-tree pathcost method**	显示 pathcost method

13.6. MSTP 典型配置用例

13.6.1. 组网需求

1) 将三台设备连接成三角环网，配置 MSTP 模式。
2) 在设备上配置相应的 Vlan-Instance 映射，以及 MST 配置名称、MST Revision Number，并指定相应设备的实例优先级
3) 查看 MSTP 配置信息
4) 全局开启 BPDU Guard 功能，在直连 PC 的端口上配置 Port Fast 功能。

13.6.2. 组网拓扑



13.6.3. 配置步骤

1) **配置 Switch A**

配置端口 Gi 0/1 和 Gi 0/2 属于 Trunk 口，创建 VLAN 2 和 VLAN 3。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
Ruijie(config)# interface gigabitEthernet 0/2
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
Ruijie(config)# vlan 2
Ruijie(config-vlan)# exit
Ruijie(config)# vlan 3
Ruijie(config-vlan)# exit
```

配置生成树为 MSTP 模式，并将 VLAN 2 映射到 Instance 1，将 VLAN 3 映射到 Instance 2，设置 MST 配置名称为 ruijie，MST Revision Number 为 1，查看 MST 配置信息，开启生成树协议。

```
Ruijie(config)# spanning-tree mode mstp
Ruijie(config)# spanning-tree mst configuration
Ruijie(config-mst)# instance 1 vlan 2
%Warning:you must create vlans before configuring instance-vlan
relationship
Ruijie(config-mst)# instance 2 vlan 3
%Warning:you must create vlans before configuring instance-vlan
relationship
```

```
Ruijie(config-mst)# name ruijie
Ruijie(config-mst)# revision 1
Ruijie(config-mst)# show
Multi spanning tree protocol : Enable
Name    : ruijie
Revision : 1
Instance  Vlans Mapped
--------  ------------------------------------------
0       : 1, 4-4094
1       : 2
2       : 3
---------------------------------------------------
Ruijie(config-mst)# exit
Ruijie(config)# spanning-tree
Enable spanning-tree.
```

在该设备上配置 Instance 0 的优先级为 4096

```
Ruijie(config)# spanning-tree mst 0 priority 4096
```

2） **配置 Switch B**

配置端口 Gi 0/1 和 Gi 0/2 属于 Trunk 口，创建 VLAN 2 和 VLAN 3。

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
Ruijie(config)# interface gigabitEthernet 0/2
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
Ruijie(config)# vlan 2
Ruijie(config-vlan)# exit
Ruijie(config)# vlan 3
Ruijie(config-vlan)# exit
```

配置生成树为 MSTP 模式，并将 VLAN 2 映射到 Instance 1，将 VLAN 3 映射到 Instance 2，设置 MST 配置名称为 ruijie，MST Revision Number 为 1，开启生成树协议。

```
Ruijie(config)# spanning-tree mode mstp
Ruijie(config)# spanning-tree mst configuration
Ruijie(config-mst)# instance 1 vlan 2
%Warning:you must create vlans before configuring instance-vlan
relationship
Ruijie(config-mst)# instance 2 vlan 3
%Warning:you must create vlans before configuring instance-vlan
relationship
Ruijie(config-mst)# name ruijie
Ruijie(config-mst)# revision 1
Ruijie(config-mst)# exit
Ruijie(config)# spanning-tree
Enable spanning-tree.
```

在该设备上配置 Instance1 的优先级为 4096
```
Ruijie(config)# spanning-tree mst 1 priority 4096
```

3) 配置 Switch C

配置端口 Fa 0/1 和 Fa 0/2 属于 Trunk 口，创建 VLAN 2 和 VLAN 3。
```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
Ruijie(config)# interface fastEthernet 0/2
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
Ruijie(config)# vlan 2
Ruijie(config-vlan)# exit
Ruijie(config)# vlan 3
Ruijie(config-vlan)# exit
```
配置生成树为 MSTP 模式，并将 VLAN 2 映射到 Instance 1，将 VLAN 3 映射到 Instance 2，设置 MST 配置名称为 ruijie，MST Revision Number 为 1，开启生成树协议。
```
Ruijie(config)# spanning-tree mode mstp
Ruijie(config)# spanning-tree mst configuration
Ruijie(config-mst)# instance 1 vlan 2
%Warning:you must create vlans before configuring instance-vlan
relationship
Ruijie(config-mst)# instance 2 vlan 3
%Warning:you must create vlans before configuring instance-vlan
relationship
Ruijie(config-mst)# name ruijie
Ruijie(config-mst)# revision 1
Ruijie(config-mst)# exit
Ruijie(config)# spanning-tree
Enable spanning-tree.
```
在该设备上配置 Instance 2 的优先级最高
```
Ruijie(config)# spanning-tree mst 2 priority 4096
```
全局开启 BPDU Guard 功能，并配置端口 Fa 0/3 为 Port Fast。
```
Ruijie(config)# spanning-tree portfast bpduguard default
Ruijie(config)# interface fastEthernet 0/3
Ruijie(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected
to a single host. Connecting hubs, Ruijiees, bridges to this
interface when portfast is enabled,can cause temporary loops.
Ruijie(config-if)# end
```
查看该设备的生成树配置信息
```
Ruijie# show spanning-tree
StpVersion : MSTP
SysStpStatus : ENABLED
MaxAge : 20
```

```
HelloTime : 2
ForwardDelay : 15
BridgeMaxAge : 20
BridgeHelloTime : 2
BridgeForwardDelay : 15
MaxHops: 20
TxHoldCount : 3
PathCostMethod : Long
BPDUGuard : enabled
BPDUFilter : Disabled
LoopGuardDef  : Disabled
###### mst 0 vlans map : 1, 4-4094
BridgeAddr : 00d0.f82a.aa8e
Priority: 32768
TimeSinceTopologyChange : 0d:0h:19m:44s
TopologyChanges : 1
DesignatedRoot : 1000.00d0.f822.33aa
RootCost : 0
RootPort : 1
CistRegionRoot : 1000.00d0.f822.33aa
CistPathCost : 200000
###### mst 1 vlans map : 2
BridgeAddr : 00d0.f82a.aa8e
Priority: 32768
TimeSinceTopologyChange : 0d:0h:1m:46s
TopologyChanges : 7
DesignatedRoot : 1001.00d0.f834.56f0
RootCost : 200000
RootPort : 2
###### mst 2 vlans map : 3
BridgeAddr : 00d0.f82a.aa8e
Priority: 4096
TimeSinceTopologyChange : 0d:0h:1m:44s
TopologyChanges : 5
DesignatedRoot : 1002.00d0.f82a.aa8e
RootCost : 0
RootPort : 0
# 查看端口 Fa 0/1 的生成树配置信息
Ruijie# show spanning-tree interface fastEthernet 0/1
PortAdminPortFast : Disabled
PortOperPortFast : Disabled
PortAdminAutoEdge : Enabled
PortOperAutoEdge : Disabled
PortAdminLinkType : auto
PortOperLinkType : point-to-point
PortBPDUGuard : Disabled
```

```
PortBPDUFilter : Disabled
PortGuardmode  : None
###### MST 0 vlans mapped :1, 4-4094
PortState : forwarding
PortPriority : 128
PortDesignatedRoot : 1000.00d0.f822.33aa
PortDesignatedCost : 0
PortDesignatedBridge :1000.00d0.f822.33aa
PortDesignatedPort : 8002
PortForwardTransitions : 1
PortAdminPathCost : 200000
PortOperPathCost : 200000
Inconsistent states : normal
PortRole : rootPort
###### MST 1 vlans mapped :2
PortState : discarding
PortPriority : 128
PortDesignatedRoot : 1001.00d0.f834.56f0
PortDesignatedCost : 0
PortDesignatedBridge :8001.00d0.f822.33aa
PortDesignatedPort : 8002
PortForwardTransitions : 5
PortAdminPathCost : 200000
PortOperPathCost : 200000
Inconsistent states : normal
PortRole : alternatePort
###### MST 2 vlans mapped :3
PortState : forwarding
PortPriority : 128
PortDesignatedRoot : 1002.00d0.f82a.aa8e
PortDesignatedCost : 0
PortDesignatedBridge :1002.00d0.f82a.aa8e
PortDesignatedPort : 8001
PortForwardTransitions : 1
PortAdminPathCost : 200000
PortOperPathCost : 200000
Inconsistent states : normal
PortRole : designatedPort
```

第14章 SPAN 配置

14.1. 概述

14.1.1. 理解 SPAN

您可以通过使用 SPAN 将一个端口上的帧拷贝到交换机上的另一个连接有网络分析设备或 RMON 分析仪的端口上来分析该端口上的通讯。SPAN 将某个端口上所有接收和发送的帧 MIRROR 到某个物理端口上来进行分析。

例如，在图 1 中，千兆端口 5 上的所有帧都被映射到了千兆端口 10，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，可接收通过端口 5 上的所有帧。

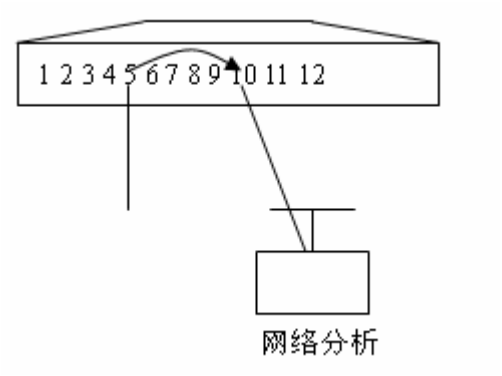


图 1 SPAN 配置实例

通过 SPAN 可以监控所有进入和从源端口输出的帧，包括路由输入帧。

SPAN 并不影响源端口和目的端口的交换，只是所有进入和从源端口输出的帧原样拷贝了一份到目的端口。然而一个流量过度的目的端口，例如一个 100Mbps 目的端口监控一个 1000Mbps 可能导致帧被丢弃。

14.1.2. 注意事项

- S2300 系列的交换机不支持垮设备镜像，即在堆叠情况下，如果镜像源端口和镜像目的口在不同的堆叠成员设备上，镜像将不生效。
- S2300 系列产品上，如果开启了 Igmp Snooping 功能，那么 Igmp 协议报文将无法镜像到指定端口，同时未知名组播报文也不能被镜像。
- 在 S2300 系列产品上，安全端口下源 MAC 地址不是安全地址的报文不能够被镜像到镜像目的口。

14.2. SPAN 概念和术语

该部分描述了和 SPAN 配置相关的一些概念和术语

14.2.1. SPAN 会话

一个 SPAN 会话是一个目的端口和源端口的组合。您可以监控单个或多个接口的输入，输出和双向帧。

您只能配置一个 SPAN 会话，Switched port、routed port 和 AP 都可以配置为源端口和目的端口。SPAN 会话并不影响交换机的正常操作。

您可以将 SPAN 会话配置在一个 disabled port 上，然而，SPAN 并不马上发生作用直到您使能目的和源端口。**Show monitor session session number** 命令显示了 SPAN 会话的操作状态。一个 SPAN 会话在上电后并不马上生效直到目的端口处于可操作状态。

14.2.2. 帧类型

SPAN 会话包含以下帧类型：

接收帧：所有源端口上接收到的帧都将被拷贝一份到目的口。在一个 SPAN 会话中，您可监控一个或几个源端口的输入帧。若由于某些原因，从源端口输入的帧可能被丢弃，如端口安全，但这不影响 SPAN 的功能，该帧仍然会发送到目的端口。

发送帧：所有从源端口发送的帧都将拷贝一份到目的端口。在一个 SPAN 会话中，您可监控一个或几个源端口的输出帧。若由于某些原因，从别的端口发送到源端口的帧可能被丢弃，同样，该帧也不会发送到目的端口。由于某些原因发送到源端口的帧的格式可能改变，例如源端口输出经过路由之后的帧，帧的源 MAC、目的 MAC、VLAN ID 以及 TTL 发生变化。同样，拷贝到目的端口的帧的格式也会变化。

双向帧：包括上面所说的两种帧。在一个 SPAN 会话中，您可监控一个或几个源端口的输入和输出帧。

14.2.3. 源端口

源端口(也叫被监控口)可以是一个 switched port、routed port 或 AP，该端口被监控用做网络分析。在单个的 SPAN 会话中，您可以监控输入，输出和双向帧，对于源端口的最大个数不做限制。

一个源端口有以下特性：

1) 它可以是 switched port，routed port 或 AP。

2) 它不可以同时为目的口。

3) 它可以指定被监控帧的输入或输出方向。

4) 源端口和目的端口可以处于一个 VLAN 或不处于一个 VLAN 中。

14.2.4. 目的端口

SPAN 会话有一个目的口(也叫监控口)，用于接收源端口的帧拷贝。

目的端口有以下特性：

- 它可以是 switched port、routed port 和 AP。

14.3. 配置 SPAN

本部分描述了如何在您的交换机上配置 SPAN，它包含以下配置:

14.3.1. SPAN 配置

功能	缺省配置
SPAN 状态	禁止

14.3.2. SPAN 配置指南

请遵循以下规则进行 SPAN 的配置。

请将网络分析仪连接到监控口

目的端口不能为源端口，源端口不能为目的端口。

您可以配置一个 disabled port 为目的端口或源端口，但此时 SPAN 功能并不起作用，直到目的端口和源端口被重新使能。

no monitor session *session_number* 全局配置命令可从 SPAN 会话中删除源或目的端口。

当 SPAN 处于使能状态，配置的变更有以下结果：

—如果您改变了源端口的 VLAN 配置，该配置将马上生效。

—如果您改变了目的端口的 VLAN 配置，该配置马上生效。

—如果您禁止了源端口或目的端口，SPAN 将不起作用。

—如果您将源端口或者目的端口加入到一个 AP 中，该配置将使 SPAN 的源端口或者目的端口被取消。

14.3.3. 创建一个 SPAN 会话并指定监控口和被监控口

创建一个 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_number* **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_number* **destination interface** *interface-id* {**encapsulation | switch**}	指定目的端口。对于 *interface-id*，请指定相应的接口号 添加 *encapsulation* 参数将支持镜像口封装功能,添加 *switch* 参数将支持镜像目的口交换功能。

想要删除 SPAN 会话，可使用 **no monitor session** *session_number* 全局配置命令。想要删除所有 SPAN 会话，可使用 **no monitor session all** 全局配置命令。使用 **no monitor session session_number source interface** *interface-id* 全局配置命令或 **no monitor session** *session_number* **destination interface** *interface-id* 可删除源端口或目的端口

下面这个例子说明了如何创建一个 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 1 的帧 MIRROR 到端口 8。**Show monitor session** 特权命令用于确认配置。

```
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
```

14.3.4. 从 SPAN 会话中删除一个口

从一个 SPAN 会话中删除源端口。

命令	作用
Ruijie(config)**# no monitor session** *session_number* **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_number* **source interface** *interface-id* 全局配置命令可从一个 SPAN 会话中删除源端口。下面这个例子显示了如何将端口 1 从会话 1 中删除并确认配置

```
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
```

14.3.5. 配置基于流的镜像

在特权模式下，遵循以下步骤可设置基于流的镜像。

命令	作用
Ruijie(config)**# [no] 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, 以及镜像源端口和目的端口

只支持入口镜像。

Acl 配置命令参见相关配置指南。

14.4. 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
```

第15章 IP 地址配置

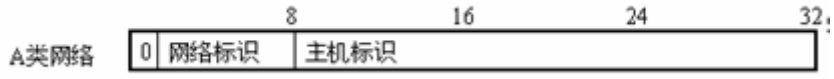
15.1. IP 地址配置

15.1.1. IP 地址简介

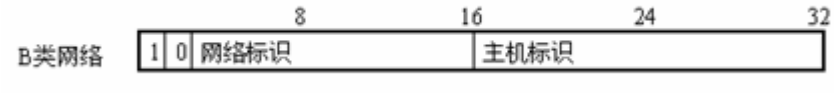
IP 地址由 32 位二进制组成，为了书写和描述方便，一般用十进制表示。十进制表示时，分为四组，每组 8 位，范围从 0~255，组之间用“.”号隔开，比如“192.168.1.1”就是用十进制表示的 IP 地址。

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

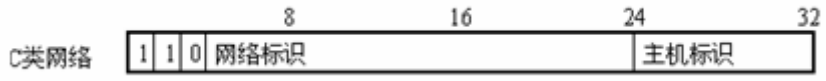
A 类地址，最高比特位为“0”，有 7 个比特位表示网络号，24 个比特位表示本地地址。这样总共有 128 个 A 类网络。



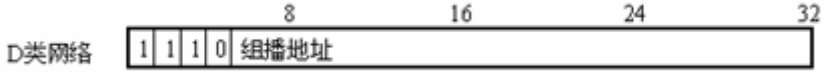
B 类地址，前两个最高比特位为“10”，有 14 个比特位表示网络号，16 个比特位表示本地地址。这样总共有 16,348 个 B 类网络。



C 类地址，前三个最高比特位为“110”，有 22 个比特位表示网络号，8 个比特位表示本地地址。这样总共有 2,097,152 个 C 类网络。



D 类地址，前四个最高比特位为“1110”，其余比特位为组播地址。



说明：

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

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

下表为保留与可用的地址列表：

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

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

类别	IP 地址范围	网络数
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。

15.1.2. IP 地址配置任务

15.1.2.1. 地址解析协议（ARP）配置

在局域网中，每个 IP 网络设备都有两个地址：1）本地地址，由于它包含在数据链路层的帧头中，更准确地说应该是数据链路层地址，但实际上对本地地址进行处理的是数据链路层中的 MAC 子层，因此习惯上称为 MAC 地址，MAC 地址在局域网上代表着 IP 网络设备；2）网络地址，在互联网上代表着 IP 网络设备，同时它也说明了该设备所属的网络。

局域网上两台 IP 设备之间需要通信，必须要知道对方的 48 比特的 MAC 地址。根据 IP 地址来获知 MAC 地址的过程称为地址解析（ARP）。而根据 MAC 地址获知 IP 地址的过程称为反向地址解析（RARP）。地址解析的方式有两类：1）地址解析协议（ARP）；2）代理地址解析协议（Proxy ARP）。关于 ARP 、Proxy ARP、RARP，分别在 RFC 826，RFC 1027，RFC 903 文当中描述。

ARP 是用来绑定 MAC 地址和 IP 地址的，以 IP 地址作为输入，ARP 能够知道其关联的 MAC 地址。一旦知道了 MAC 地址，IP 地址与 MAC 地址对应关系就会保存在设备的 ARP 缓冲中。有了 MAC 地址，IP 设备就可以封装链路层的帧，然后将数据帧发送到局域网上去。缺省配置下，以太网上 IP 和 ARP 的封装为 Ethernet II 类型，也可以封装成其它类型的以太网帧类型如 SNAP。

RARP 的工作原理与 ARP 类似，不过 RARP 是以 MAC 地址作为输入，然后得到关联的 IP 地址。RARP 通常应用在无盘工作站上。

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

- 静态配置 ARP
- ARP 封装设置

15.1.2.1.1. 静态配置 ARP

ARP 协议提供了 IP 地址和 MAC 地址动态映射的功能，通常情况下不需要进行静态配置。我司产品通过配置静态 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

15.1.2.1.2. ARP 封装设置

目前 ARP 封装只支持 Ethernet II 类型，在我司产品中也表示为 ARPA 关键字。

15.1.3. 监视和维护 IP 地址

要监视和维护网络，根据以下任务描述，根据实际需要进行操作。

- 清除 ARP 缓冲内容
- 显示系统和网络状态

15.1.3.1. 清除 ARP 缓冲内容

您可以删除 arp 缓冲的全部内容：

命令	作用
Ruijie# **clear arp-cache**	清除 ARP 缓冲

15.1.3.2. 显示系统和网络状态

您可以查看 ARP 缓冲的所有内容，通过这些信息对网络故障的排除十分有帮助。通过测试本地设备网络的可达到性，您可以知道数据包在离开本设备后将往那条路径发送。

要显示系统和网络统计量，在特权用户模式中执行以下命令：

命令	作用
Ruijie# **show arp**	显示 ARP 缓冲表
Ruijie# **show ip arp**	显示 IP ARP 缓冲表

Ruijie**# show ip interface** [*interface-type interface-number*]	显示接口 IP 信息
Ruijie**# ping** *ip-address* [**length** *bytes*] [**ntimes** *times*] [**timeout** *seconds*]	测试网络可达性

15.1.4. 配置默认网关

如果在设备中不知道将数据包发送到哪一个目标地址时，将该数据保发送到默认网关，使用 **show ip redirects** 命令查看设置。

如果需要配置默认网关，则在全局配置模式下执行下面命令，该命令的 no 形式是删除默认网关。

命令	说明
ip default-gateway *ip-address*	设置默认网关

如果需要查看配置的默认网关，执行如下命令。

命令	说明
show ip redirects	显示默认网关

本命令只在二层设备上支持。

第16章 DHCP Relay 配置

16.1. 概述

16.1.1. 理解 DHCP

DHCP 协议被广泛用来动态分配可重用的网络资源，如 IP 地址。

DHCP Client 发出 DHCP DISCOVER 广播报文给 DHCP Server。DHCP Server 收到后 DHCP DISCOVER 报文后，根据一定的策略来给 Client 分配资源,如 IP 地址，发出 DHCP OFFER 报文。DHCP Client 收到 DHCP OFFER 报文后，验证资源是否可用。如果资源可用发送 DHCP REQUEST 报文；如果不可用，重新发送 DHCP DISCOVER 报文。服务器收到 DHCP 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 DHCP ACK 报文；如果不可分配，则发送 DHCP NAK 报文。DHCP Client 收到 DHCP ACK 报文，就开始使用服务器分配的资源；如果收到 DHCP NAK，则可能重新发送 DHCP DISCOVER 报文再次请求另一个 IP 地址。

16.1.2. 理解 DHCP 中继代理（DHCP Relay Agent）

DHCP 请求报文的目的 IP 地址为 255.255.255.255，这种类型报文的转发局限于子网内，不会被设备转发。为了实现跨网段的动态 IP 分配，DHCP Relay Agent 就产生了。它把收到的 DHCP 请求报文封装成 IP 单播报文转发给 DHCP Server，同时，把收到的DHCP响应报文转发给DHCP Client。这样DHCP Relay Agent 就相当于一个转发站，负责沟通位于不同网段的 DHCP Client 和 DHCP Server。这样就实现了只要安装一个 DHCP Server 就可对所有网段的动态 IP 管理，即 Client—Relay Agent—Server 模式的 DHCP 动态 IP 管理。

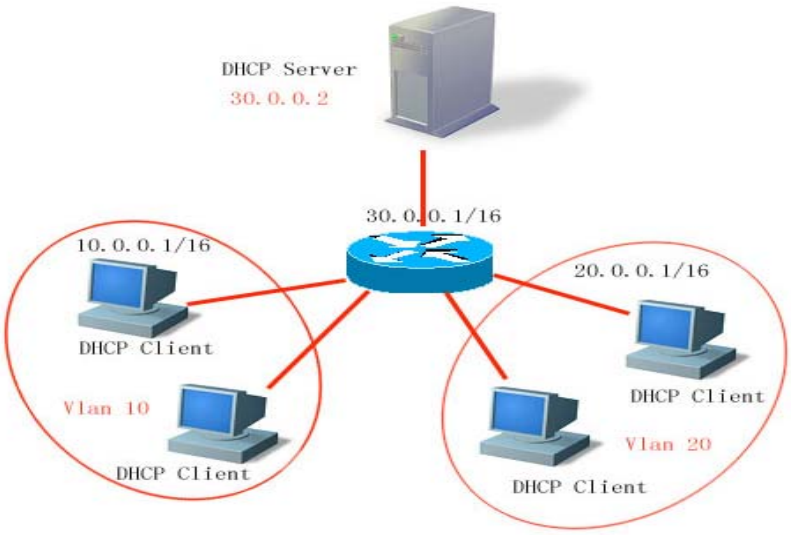


图 1

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 Server 在 30.0.0.1/16 的网络上，30.0.0.2 的 DHCP Server 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 Relay Agent，并指定 DHCP Server IP 为 30.0.0.2 就可以了

16.1.3. 理解 DHCP Relay Agent Information(option 82)

根据 RFC3046 的定义，中继设备进行 DHCP relay 时，可以通过添加一个 option 的方式来详细的标明 DHCP client 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 option82，该 option 可以继续分解成多个子选项，现阶段经常使用的子选项有 Circuit ID 和 Remote ID。本公司实现的 relay agent information 现阶段存在两种，一种是与 802.1x/SAM 应用方案结合 relay agent information option dot1x，另一种是结合用户所属的端口 vid，slot，port，以及设备 mac 信息的 relay agent information option82，下边对两种方案应用时 option 携带的内容及格式以及一些典型的应用方案进行一些说明：

1. relay agent information option dot1x：此种应用方案需要结合 802.1x 认证以及我司产品 RG-SAM。通过 RG-SAM 在 802.1x 认证过程中给设备下放不同的 IP 权限，结合 DHCP client 所属的 vid 组合成 Circuit ID 子选项。在 DHCP relay 上传到 DHCP server 时，结合 DHCP server 的配置，就可以实现给不同权限用户分配不同权限 IP 的应用。组合成 Circuit ID 格式如下，其中 priviliage 和 vid 字段各占两个字节：

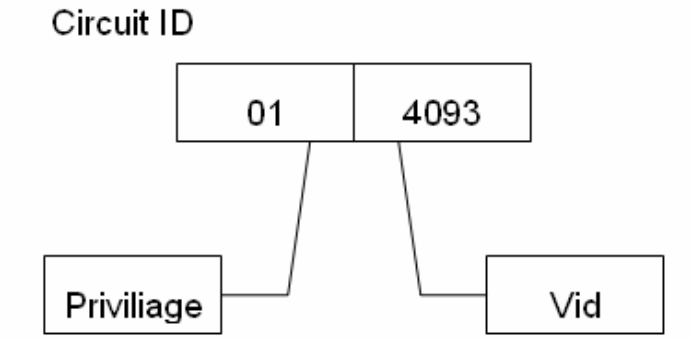


图 2

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，设备在 DHCP relay 的过程中，根据收到 DHCP 请求的实体端口，以及设备自身的物理地址信息，组合构成 option82 信息上传到服务器，option 选贤得格式如下：

Agent Circuit ID

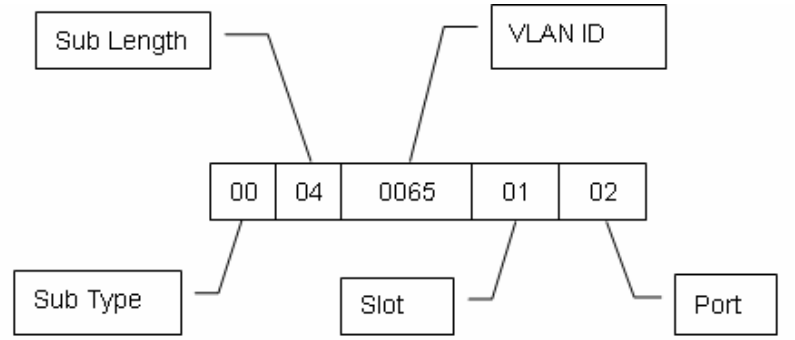


图 3

Agent Remote ID

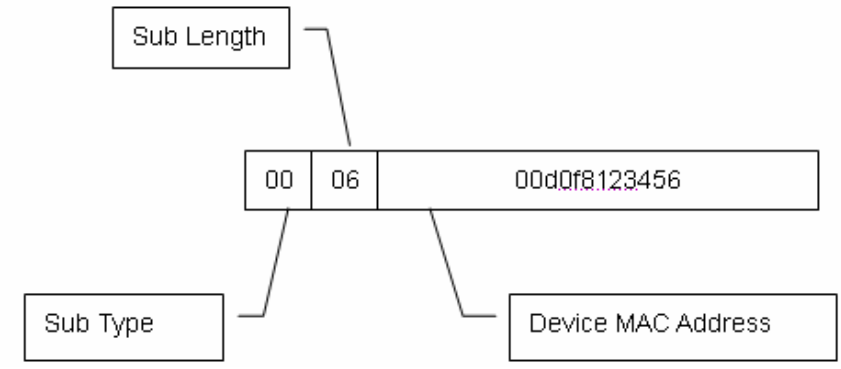


图 4

16.1.4. 理解 DHCP relay Check Server-id 功能

在 DHCP 应用时，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 client 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 server，而不是发送给每一个配置的 DHCP server，上述就是 DHCP check server-id 功能

16.2. 配置 DHCP

16.2.1. 配置 DHCP 中继代理

在全局配置模式下，请按如下步骤配置 DHCP 中继代理：

命令	作用
Ruijie (config)**# service dhcp**	启用 DHCP 代理
Ruijie(config)**# no service dhcp**	关闭 DHCP 代理。

16.2.2. 配置 DHCP Server 的 IP 地址

在配置 DHCP Server 的 IP 地址后，设备所收到的 DHCP 请求报文将转发给它，同时，收到的来自 Server 的 DHCP 响应报文也会转发给 Client。

DHCP server 地址可以全局配置，也可以在三层接口上配置，每种配置模式都可以配置多个服务器地址最多可以配置 20 个服务器地址，。在某接口收到 DHCP 请求，则首先使用接口 DHCP 服务器；如果接口上面没有配置服务器地址，则使用全局配置的 DHCP 服务器。

DHCP 中继支持基于 vrf 的中继功能，配置方法就是在对应的服务器地址前面添加 vrf 参数。配置 DHCP 服务器地址请按如下方式进行：

命令	作用
Ruijie(config)**# IP helper-address** [**vrf**] *A.B.C.D*	添加一个全局的 DHCP 服务器地址
Ruijie(config-if)**# IP helper-address** [**vrf**] *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设置。
Ruijie(config)**# no IP helper-address** [**vrf**] *A.B.C.D*	删除一个全局的 DHCP 服务器地址
Ruijie(config-if)**# no IP helper-address** [**vrf**] *A.B.C.D*	删除一个接口的 DHCP 服务器地址

16.2.3. 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 relay 的 option dot1x 功能，当打开此功能时，设备在进行 relay 时就会结合 802.1x 添加对应的 option 信息到服务器，配置此功能时需要和 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。

注意：

该功能主要在如下场景中使用：

配合 802.1x 功能且 1x 认证口下连多用户，需要支持

1.用户不需要认证就可以获取 IP 访问受限网络资源，比如只能访问内网

2.用户认证后可以不受限制访问网络资源，比如可以访问 Internet

为了满足上述要求，交换机允许用户未认证前可以从 DHCP 服务器获取一个低权限的 IP 地址。同时管理员需要在 SAM 认证服务器上为用户配置一个 IP 权限，这样用户认证通过后就可以根据这个权限从 DHCP 服务器分配到一个具有更高访问权限的IP地址。而为了控制不同IP访问不同网络资源，通常是在网关上部署PBR功能。

该功能仅限于 802.1X 功能配合 SAM 服务器进行部署,不支持其他安全方案,比如 WEB 认证。

16.2.4. 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# config
Ruijie(config)# ip access-list extended DenyAccessEachOther
OfUnauthrize
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 0.0.0.255 192.1
68.3.0 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。

16.2.5. 配置 DHCP option 82

当配置命令 **ip dhcp relay information option82** 命令时，设备就会在 DHCP relay 的过程中添加如理解 **DHCP Relay Agent Information** 中所述格式的 **option** 到服务器。

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。

16.2.6. 配置 DHCP relay check server-id

当配置命令 **ip dhcp relay check** *server-id* 后，设备在收到 DHCP relay 时就会去解析 DHCP SERVER-ID option，如果此选项不为空，则只对此 server 发送请求，而不对其他配置的服务器发送请求。

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

16.2.7. 配置 DHCP relay suppression

当配置命令 **ip dhcp relay suppression** 后，配置了 DHCP realy suppression 的接口不把收到的 DHCP 广播请求转为单播 relay 出去，而对于端口收到的广播报文的正常广播转发不做抑制。

在接口配置模式下，请按如下步骤功能：

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。

16.2.8. DHCP 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 relay 功能
Ruijie(config)# ip helper-address 192.18.100.1  //添加全局服务器地址
Ruijie(config)# ip helper-address192.18.100.2   //添加全局服务器地址
Ruijie(config)# interface GigabitEthernet 0/3
Ruijie(config-if)# ip helper-address 192.18.200.1  //添加接口服务器地址
Ruijie(config-if)# ip helper-address 192.18.200.2  //添加接口服务器地址
Ruijie(config-if)# end
```

16.3. 配置 DHCP relay 的其他注意事项

对于二层的网络设备来说，需要实现跨管理 vlan relay 功能时就必须打开 option dot1x、动态地址绑定和option82 的至少一个功能，否则在二层设备上只能实现管理 vlan 的 relay 功能。

16.3.1. 配置 DHCP option dot1x 需要的注意事项

1. 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。
2. 在应用此方案时需要启用 802.1x 的 DHCP 模式的 IP 授权。
3. 此命令与 **dhcp option82** 命令互斥，不能同时使用。
4. 在启用了 802.1x 的 DHCP 模式的 IP 授权的模式下，也会设置 MAC + IP 的绑定，所以不能与 DHCP 动态绑定功能不能同时启用。

16.3.2. 配置 DHCP option82 需要的注意事项

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

16.4. 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 RGOS 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
```

16.5. DHCP 典型配置用例

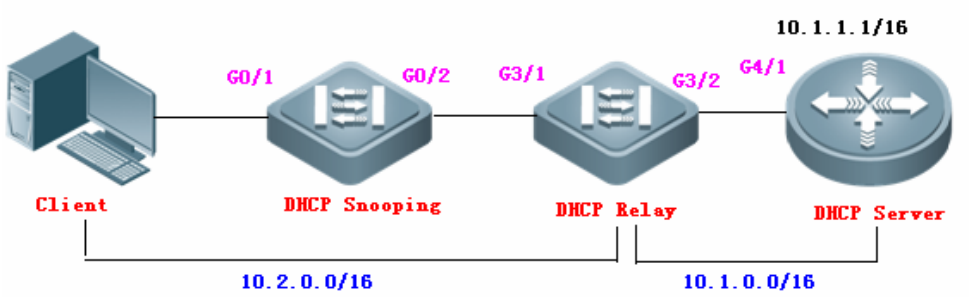
16.5.1. 跨网段的用户申请 IP 上网

16.5.1.1. 配置要求

1、要求用户跨网段可以获取 IP 地址进行正常上网；

2、防止非法的用户私自设置 IP 地址进行上网。

16.5.1.2. 拓扑图



16.5.1.3. 分析

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

16.5.1.4. 配置过程

按上述拓扑图搭建环境，按下述配置步骤进行配置：

- DHCP Snooping 的配置：

开启 DHCP Snooping 功能

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

配置与服务器相连的 Gi0/2 为可信任口

```
Ruijie(config)# interface gigabitEthernet 0/2
Ruijie(config-if)# ip dhcp snooping trust
```

配置 Gi0/2 为 ARP 检测信任口

```
Ruijie(config-if)# ip arp inspection trust
Ruijie(config-if)# exit
```

启用指定 VLAN 的 DAI 报文检查功能

```
Ruijie(config)# ip arp inspection vlan 1
```

配置设备的 IP 地址（SVI1）

```
Ruijie(config)# interface vlan 1
Ruijie(config-if)# ip address 10.2.0.1 255.255.0.0
```

配置到另一个网段（10.1.0.0/16）的静态路由

```
Ruijie(config)# ip route 10.1.0.0 255.255.0.0 10.2.1.1
```

- DHCP Relay 的配置

启用 DHCP 中继代理

```
Ruijie(config)# server dhcp
```

添加一个全局的 DHCP 服务器的地址

```
Ruijie(config)# ip helper-address 10.1.1.1
```

配置与 Snooping 设备连接的端口的 IP 地址

```
Ruijie(config)# interface gigabitEthernet 3/1
Ruijie(config-if)# no switchport
Ruijie(config-if)# ip address 10.2.1.1 255.255.0.0
```

配置与 Server 设备连接的端口的 IP 地址

```
Ruijie(config)# interface gigabitEthernet 3/2
Ruijie(config-if)# no switchport
Ruijie(config-if)# ip address 10.1.0.1 255.255.0.0
```

- DHCP Server 上的配置：

为连接 Relay 设备的端口配置 IP 地址

```
Ruijie(config)# interface gigabitEthernet 4/1
Ruijie(config-if)# no switchport
Ruijie(config-if)# ip address 10.1.1.1 255.255.0.0
```

启用 DHCP 服务器

```
Ruijie(config)# service dhcp
```

配置 DHCP 排斥地址，这些地址不会被分配给客户端

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

配置地址池名并进入地址池配置模式

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

```
# 配置客户端缺省网关
Ruijie(dhcp-config)# default-router 10.2.1.1
# 配置 DHCP 地址池的网络号和掩码
Ruijie(dhcp-config)# network 10.2.0.0  255.255.0.0
# 配置到另一个网段（10.2.0.0/16）的静态路由
Ruijie(config)# ip route 10.2.0.0  255.255.0.0  10.1.0.1
```

第17章 DNS 配置

17.1. 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。

17.2. 配置域名解析

17.2.1. 缺省的 DNS 配置

DNS 的缺省配置如下表：

属性	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

17.2.2. 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
```

17.2.3. 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。

17.2.4. 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。

17.2.5. 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** [*word*]	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。

17.2.6. 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
Ruijie# **show hosts**	查看 DNS 的相关参数

```
Ruijie# show hosts
DNS name server    :
192.168.5.134    static
    host                type          address
www.163.com             static       192.168.5.243
www.ruijie.com          dynamic      192.168.5.123
```

17.2.7. 应用举例

Ping 指定域名的主机：

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

第18章 简单网络时间协议(SNTP)

18.1. 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。

18.1.1. SNTP 原理

SNTP 协议采用客户/服务器工作方式，服务器通过接收 GPS 信号或自带的原子钟作为系统的时间基准，客户机通过定期访问服务器提供的时间服务获得准确的时间信息，并调整自己的系统时钟，达到网络时间同步的目的。

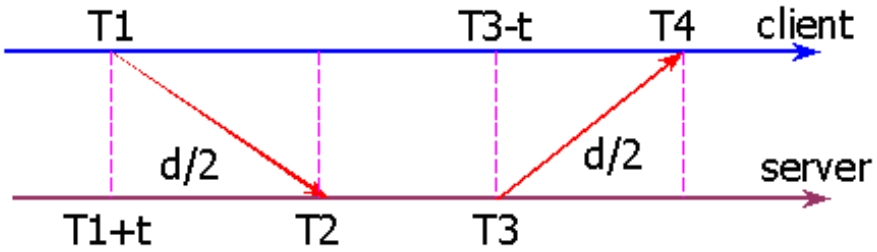


图 1

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：客户方发送查询请求时间(以客户方时间系统为参照)，标记为 Originate Timestamp；

T2：服务器收到查询请求时间(以服务器时间系统为参照)，标记为 Receive Timestamp；

T3：服务器回复时间信息包时间(以服务器时间系统为参照)，标记为 Transmit Timestamp；

T4：客户方收到时间信息包时间(以客户方时间系统为参照)，标记为 Destination Timestamp；

T：服务器和客户端之间的时间偏差；

d：两者之间的往返时间；

时间求解过程：

因为

T2 = T1 + t + d / 2;

所以

T2 - T1 = t + d / 2;

又因为

T4 = T3 – t + d / 2;

所以

T3 - T4 = t – d / 2;

求得

d = (T4 - T1) - (T3 - T2);

t = ((T2 - T1) + (T3 - T4)) / 2;

求出了 t 和 d，SNTP Client 就可据此算出当前的时间。

即，当前时间为 T4 + t

18.2. 配置 SNTP

本章节将介绍如何配置 SNTP

18.2.1. 缺省的 SNTP 设置

缺省情况下，SNTP 的配置如下：

项目	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

18.2.2. 打开 SNTP

进入特权模式，按以下步骤打开 SNTP：

1) 进入全局配置模式。

```
Ruijie# config
```

2) 打开 SNTP，即时同步一次时钟。后续如果输入这个命令， 都会“即时同步”时钟，不必等待定时同步。(为了避免频繁地同步时间，每两次的“即时同步”时间请勿小于 5 秒)。

```
Ruijie(config)# sntp enable
```

3) 退回到特权模式

```
Ruijie(config)# End
```

4) 显示当前配置

```
Ruijie# show running-config
```

5) 保存配置。

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

您如果要关闭 SNTP，可以用 **no sntp enable** 全局配置命令来关闭 SNTP。

18.2.3. 配置 NTP Server 的地址

由于 SNTP 的报文和 NTP 的报文是完全一致的，所以 SNTP Client 能完全兼容 NTP Server。网络上存在着较多的 NTP Server，您可以选择一个网络延迟较少的一个做为交换机上的 NTP Server。

具体的NTP server地址可以登录 http://www.time.edu.cn/或 http://www.ntp.org/上获取。

如 192.43.244.18(time.nist.gov)。

进入特权模式，按以下步骤配置 SNTP Server IP 地址：

1) 进入全局配置模式。

```
Ruijie# config
```

2) 设置 SNTP Server 的 IP 地址。

```
Ruijie(config)# sntp server <ip-addr>
```

3) 退回到特权模式

```
Ruijie(config)# End
```

4) 显示当前配置

```
Ruijie# show running-config
```

5) 保存配置。

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

18.2.4. 配置SNTP同步时钟的间隔

SNTP Client 需要设置一定的时间间隔定期访问 NTP Server，以便定时校正时钟。以下步骤将配置交换机和 NTP Server 同步时钟的间隔：

1) 进入全局配置模式。

```
Ruijie# config
```

2) 设置定时同步时钟的间隔，单位为秒。范围为 60 秒-65535 秒，缺省值为 1800 秒。

```
Ruijie(config)# sntp interval <seconds>
```

3) 退回到特权模式

```
Ruijie(config)# End
```

4) 显示当前配置

```
Ruijie# show running-config
```

5) 保存配置。

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

18.2.5. 配置本地时区

通过 SNTP 协议通讯后获取的时间都是格林威治标准时间 (GMT)，为了准确的获取本地时间，需要设置本地时区来对标准时间进行调正。

1） 进入全局配置模式。

```
Ruijie# config
```

2） 配置时区，范围为-23 至 23，负数表示西区，正数表示东区。如 8 表示东八区，-8 表示西 8 区，0 表示格林威治标准时间。缺省值为北京时间东八区。

```
Ruijie(config)# clock time-zone <time-zone>
```

3） 退回到特权模式

```
Ruijie(config)# End
```

4） 显示当前配置

```
Ruijie# show running-config
```

5） 保存配置

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

您可以通过 **no clock time-zone** 来恢复缺省值。

18.3. 显示 SNTP

步骤如下：

1) 查看 SNTP 的相关参数

```
Ruijie# show sntp
```

2) 使用 **show sntp** 查看系统保护的配置参数：

```
Ruijie# show sntp
SNTP state                : ENABLE              //SNTP 是否打开
SNTP server               : 192.168.4.12          //NTP Server
SNTP sync interval        : 60             //定时同步的时间间隔
Time zone             : +8                          //本地时区
```

第19章 NTP 配置

19.1. 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，检查来对时的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。

SNTP 是 NTP 的简化版本，其报文信息格式是完全相同的。所不同的是 SNTP 简化了时间校正的算法，忽略了许多可能导致误差的因素，因此 SNTP 在精度上远不如 NTP。SNTP 不支持安全识别机制。目前设备支持 NTP 的客户端功能，即可以从时间服务器上同步时间。

19.2. 配置 NTP

本章介绍怎样在我们的系统实现中配置 NTP 客户端。

- 配置 NTP 全局安全识别机制
- 配置 NTP 全局认证密钥
- 配置 NTP 全局信任密钥 ID
- 配置 NTP 服务器
- 关闭接口接收 NTP 报文
- NTP 功能开关
- 配置 NTP 实时同步

19.2.1. 配置 NTP 全局安全识别机制

锐捷的 NTP 客户端支持与服务器进行加密通信，加密方式为密钥加密机制。

配置NTP客户端通过加密方式与服务器通信分两步：第一，对NTP客户端进行全局安全识别以及全局密钥相关设置；第二，设置通信服务器的信任密钥设置；NTP 全局安全设置机制属于第一个设置步骤，但是要真正发起与服务器之间的加密通信，还要对对应的服务器设置认证密钥。

在缺省情况下，客户端不使用全局安全识别机制。如果未使用安全识别机制则不对通信进行加密处理。但是仅仅设置了全局安全标志，并不代表一定采用了加密方式完成服务器与客户端的通信，还必须完成其他全局密钥配置并设置服务器加密密钥才可能发起和服务器的加密通信。

要配置全局安全识别机制，在全局配置模式中执行以下命令：

命令	作用
ntp authenticate	配置 NTP 全局安全识别机制。
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。

19.2.2. 配置 NTP 全局认证密钥

进行 NTP 安全认证全局配置，接下来的配置就是设置全局认证密钥。

配置全局认证密钥，每个密钥有一个唯一的 key-id 标示，客户可以用 **ntp trusted-key** 将该 key-id 对应的密钥设置为全局信任密钥。

要配置全局认证密钥，在全局配置模式中执行以下命令：

命令	作用
ntp authentication-key *key-id* **md5** *key-string* [*enc-type*]	配置 NTP 全局认证密钥。 key-id：1-4294967295 key-string：长度范围任意 enc-type：有 0 和 7 两种类型。
no ntp authentication-key *key-id* **md5** *key-string* [*enc-type*]	删除 NTP 全局认证密钥。

配置了全局认证密钥并不说明该密钥一定有效，在使用该密钥之前必须将该密钥配置成为全局信任密钥。

注意：

我司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。

19.2.3. 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
ntp trusted-key *key-id*	配置 NTP 全局信任密钥 ID。
no ntp trusted-key *key-id*	删除 NTP 全局信任密钥 ID。

以上三步设置仅仅是完成安全认证机制的第一个步骤，真正发起与客户服务器的加密通信必须对相应的服务器设置信任密钥。

注意:

直接删除全局认证密钥，则该密钥对应的信任信息也会被删除。

19.2.4. 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
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
no ntp server *ip-addr*	删除 NTP 服务器

只有完成了全局安全识别以及密钥设置机制，这时候设置服务器通信的信任密

钥，才能发起于服务器的加密通信，而加密通信的完成需要服务器端信任相同的密钥。

19.2.5. 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。

注意:

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
interface *interface-type number*	进入接口配置模式
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

19.2.6. 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
no ntp	关闭 NTP 功能。
ntp authenticate 或 **ntp server** *ip-addr* [**version** *version*][**source** *if-name number*][**key** *keyid*][**prefer**]	打开 NTP 功能

19.2.7. 配置 NTP 实时同步

为了提高精确度，在第一次通过的过程中客户端会和服务器连续进行 8 个报文的交互，在接下来的同步过程中，NTP 同步的时间间隔为 1 分钟，即本此同步完成到自动发起下一次时钟同步，当用户要手动进行实时同步的时候可以使用该命令。

进行 NTP 实时同步，在全局配置模式下执行以下命令：

命令	作用
ntp synchronize	进行实时同步
no ntp synchronize	关闭实时同步

锐捷的客户端系统设置为每次同步完成之后间隔 30 分钟进行下一次同步，添加新的服务器也会触发实时同步，当 NTP 客户端停止同步的时候使用该命令也会进行实时同步，在同步过程中使用该命令不会有任何效果。

关闭实时同步的命令和关闭 NTP 的命令都可以停止时钟同步（同步过程中）或者关闭同步功能（同步过程间），不同的是，关闭 NTP 的命令不仅仅会关闭 NTP 同步功能，而且会清除相关的 NTP 配置信息。

19.3. NTP 信息显示

19.3.1. 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。

19.3.2. 显示 NTP 信息

在特权模式下，您可以使用 **show ntp status** 命令来显示当前的 NTP 信息。

显示 NTP 状态信息，在特权模式下执行以下命令：

命令	作用
show ntp status	显示当前的 NTP 信息

只有在配置了相关的通信服务器之后该命令才能打印出显示信息。

```
Ruijie# show ntp status
Clock is synchronized, stratum 9, reference is 192.168.217.100
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision
is 2**18
reference time is AF3CF6AE.3BF8CB56 (20:55:10.000 UTC Mon Mar
1 1993)
clock offset is 32.97540 sec, root delay is 0.00000 sec
root dispersion is 0.00003 msec, peer dispersion is 0.00003 msec
```

注：starum 代表当前时钟的等级，reference 为同步服务器的地址，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。

19.4. 配置范例

在以下配置中，网络中有一个指定为 master 的 NTP 服务器，并打开了相应的认证机制，配置了一个 key-id 为 6、key-string 为 wooooop 的密钥，并设置该密钥为服务器信任密钥；为了配置锐捷的客户机可以和网络上的 NTP 服务器进行时间同步，我们将对客户进行如下配置，启动安全认证，并配置一个和 NTP 服务器端一样的密钥，然后将我们的同步服务器设定为网络上的这个 NTP 服务器，开始时间同步。

```
Ruijie(config)# no ntp
Ruijie(config)# ntp authentication-key 6 md5 wooooop
Ruijie(config)# ntp authenticate
Ruijie(config)# ntp trusted-key 6
Ruijie(config)# ntp server 192.168.210.222 key 6
Ruijie(config)# ntp synchronize
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# ntp disable
Ruijie(config-if)# no ntp disable
```

第20章 SNMP 配置

20.1. SNMP 相关知识

20.1.1. 概述

SNMP 是 Simple Network Manger 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)。常用的运行在 NMS 上的网管平台有 HP OpenView 、CiscoView、CiscoWorks 2000，锐捷网络针对自己的网络设备，开发了一套网管软件－－Star View。这些常用的网管软件可以方便的对网络设备进行监控和管理。

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：

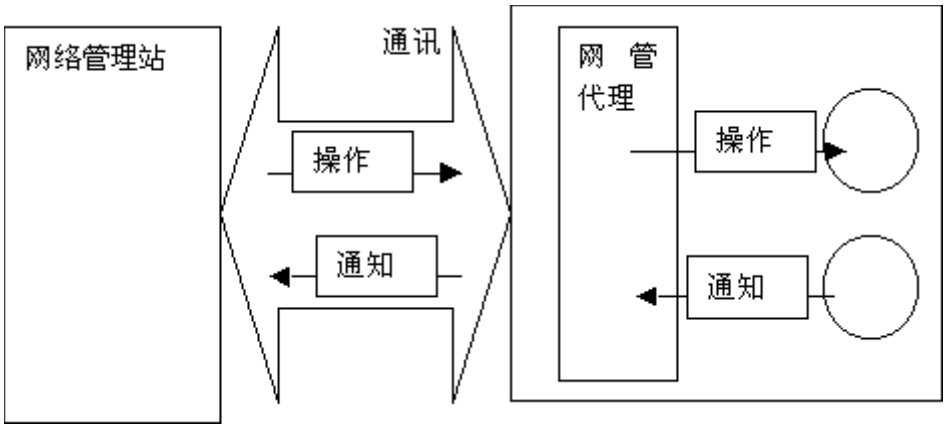


图 1 网络管理站（NMS）与网管代理（Agent）的关系图

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。

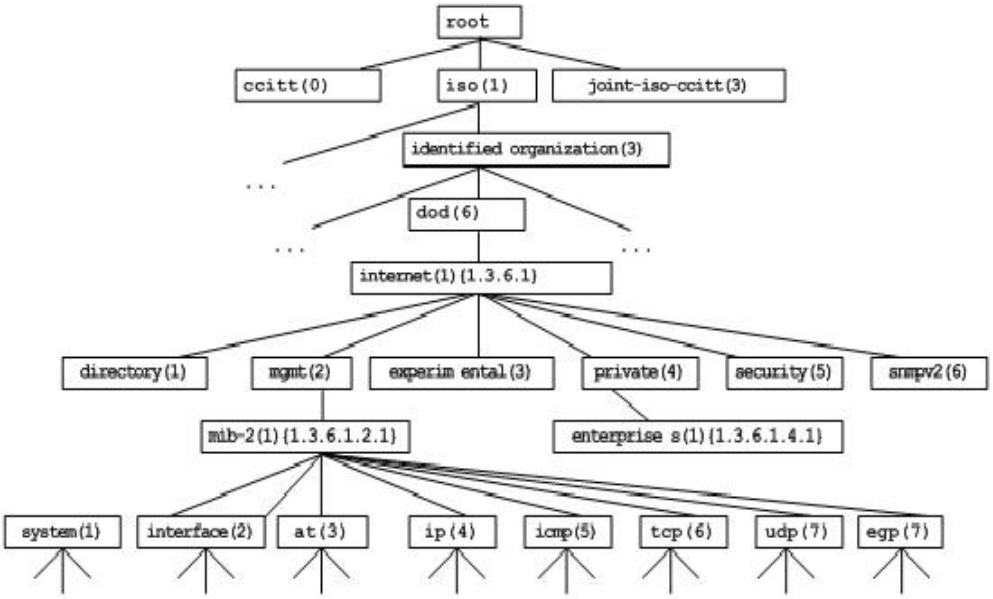


图 2　MIB 树形层次结构

20.1.2.　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(Commumity 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。

20.1.3. 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。

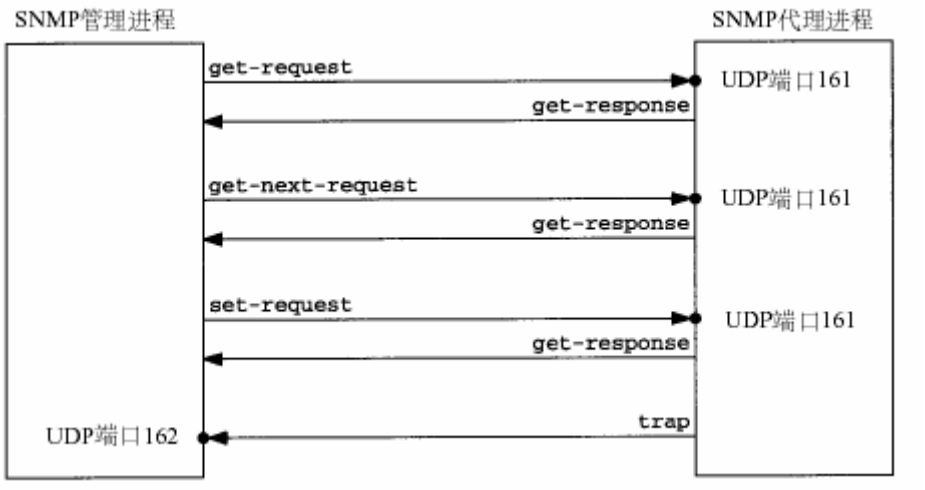


图 3 SNMP 的报文类型

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。

20.1.4. 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， SNMPv 3 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

20.1.5. 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。

20.2. 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。

20.2.1. 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** *string* [**view** *view-name*] [**ro** | **rw**] [**host** *host-ip*] [*num*]	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** 命令。

20.2.2. 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** {*num* | *name*}]	创建一个组，并和视图关联。

使用 **no snmp-server view** *view-name* 命令来删除一个视图，或者使用 **no snmp-server view** *view-name oid-tree* 命令在一个视图中删除一棵子树。也可以使用 **no snmp-server group** *groupname* 命令来删除一个组。

20.2.3. 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** | **v2** | **v3** [**encrypted**] [**auth** { **md5**|**sha** } *auth-password*] [**priv des56** *priv-password*] } [**access** {*num* | *name*}]	设置用户信息。

通过 **no snmp-server user** *username groupname* 删除指定用户。

20.2.4. 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* **traps** [**vrf** *vrfname*] [**version** {**1**|**2c** |**3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port-num*] [**type**]	设置 SNMP 主机地址，主机端口，vrf 选项，消息类型，认证名（在 SNMPv3 下是用户名）、安全级别（仅 SNMPv3 支持）等

20.2.5. 设置 SNMP 代理参数

可以对 SNMP 的 Agent 的基本参数进行配置，设置设备的联系方式、设备位置、序列号的信息，NMS 通过访问设备的这些参数，便可以得知设备的联系人，设备所在的物理位置等信息。

要配置 SNMP 代理参数，在全局配置模式下，执行如下指令：

命令	作用
Ruijie(config)# **snmp-server contact** *text*	设置系统的联系方式
Ruijie(config)# **snmp-server location** *text*	设置系统的位置
Ruijie(config)# **snmp-server chassis-id** *number*	设置系统的序列码

20.2.6. 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

20.2.7. 屏蔽 SNMP 代理

SNMP 代理服务是我司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

20.2.8. 关闭 SNMP 代理

不同于屏蔽命令，我司产品提供了关闭 snmp 代理的命令，该命令会直接 snmp 所有服务，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

20.2.9. 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

20.2.10. 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
```

20.2.11. 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

20.3. SNMP 的监控与维护

20.3.1. 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，我司产品提供了 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
Contact: wugb@i-net.com.cn
Location: fuzhou
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

20.3.2. 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
snmpInBadVersions
snmpInBadCommunityNames
snmpInBadCommunityUses
snmpInASNParseErrs
snmpInTooBigs
snmpInNoSuchNames
snmpInBadValues
snmpInReadOnlys
snmpInGenErrs
snmpInTotalReqVars
snmpInTotalSetVars
snmpInGetRequests
snmpInGetNexts
snmpInSetRequests
snmpInGetResponses
snmpInTraps
snmpOutTooBigs
snmpOutNoSuchNames
snmpOutBadValues
snmpOutGenErrs
snmpOutGetRequests
snmpOutGetNexts
snmpOutSetRequests
snmpOutGetResponses
snmpOutTraps
snmpEnableAuthenTraps
snmpSilentDrops
snmpProxyDrops
entPhysicalEntry
entPhysicalEntry.entPhysicalIndex
entPhysicalEntry.entPhysicalDescr
entPhysicalEntry.entPhysicalVendorType
entPhysicalEntry.entPhysicalContainedIn
entPhysicalEntry.entPhysicalClass
entPhysicalEntry.entPhysicalParentRelPos
entPhysicalEntry.entPhysicalName
entPhysicalEntry.entPhysicalHardwareRev
entPhysicalEntry.entPhysicalFirmwareRev
entPhysicalEntry.entPhysicalSoftwareRev
entPhysicalEntry.entPhysicalSerialNum
entPhysicalEntry.entPhysicalMfgName
entPhysicalEntry.entPhysicalModelName
entPhysicalEntry.entPhysicalAlias
entPhysicalEntry.entPhysicalAssetID
entPhysicalEntry.entPhysicalIsFRU
```

```
entPhysicalContainsEntry
entPhysicalContainsEntry.entPhysicalChildIndex
entLastChangeTime
```

20.3.3. 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
```

20.3.4. 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
```

20.4. SNMP 配置举例

20.4.1. 典型配置实例

- 配置要求

如图，网络设备和网管工作站 NMS 通过以太网连接，NMS 的 IP 地址为 192.168.12.181，网络设备的 IP 地址为 192.168.12.1，在网管工作站上运行了网管软件（以 HP OpenView 为例）。

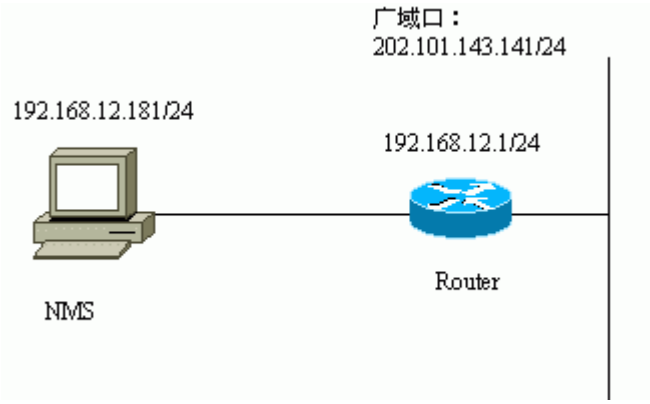


图 5　SNMP 典型配置组网图

- 网络设备具体配置

启动 SNMP 代理服务：

```
Ruijie(config)# snmp-server community public RO
```

只需要在全局配置模式下，配置以上指令，网络设备便启动了 SNMP 代理服务功能，这时 NMS 便可以对网络设备进行 SNMP 的监控了，不过只配置了只读权限，不能修改网络设备的配置，只能是监控网络设备。其他的配置都是可选的。

如果需要有读写的功能，可以采用如下的配置：

```
Ruijie(config)# snmp-server community private RW
```

以下是配置网络设备 SNMP 的一些代理基本参数，NMS 可以通过这些参数得知网络设备的一些基本系统信息，该配置为可选配置：

```
Ruijie(config)# snmp-server location fuzhou
Ruijie(config)# snmp-server contact wugb@i-net.com.cn
Ruijie(config)# snmp-server chassis-id 1234567890
0987654321
```

以下的配置，是允许网络设备主动向 NMS 发送一些 Trap 消息，该配置为可选配置：

```
Ruijie(config)# snmp-server enable traps
Ruijie(config)# snmp-server host 192.168.12.181 public
```

通过如上配置，网络设备的SNMP代理已经配置完毕，NMS便可以对网络设备进行监控和管理了，以 HP OpenView 为例，可以产生网络拓扑结构图，如下图：

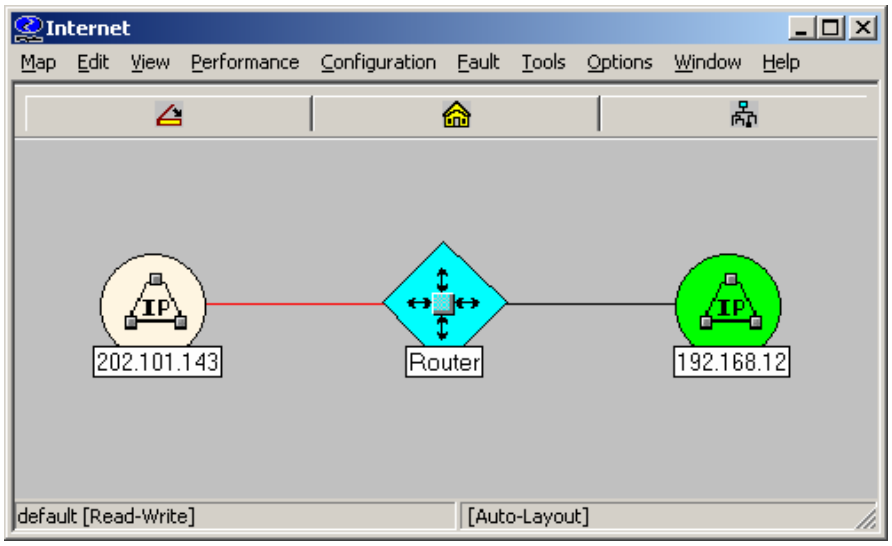


图 6　网络拓扑结构图

您可以对网络设备中的管理单元进行查询和设置，点击 HP OpenView 的 TOOL->SNMP MIB Brower 菜单，出现如下的对话框，在 Name 中输入 IP 地址 192.168.12.1，在 Community Name 中输入 Public，选择要查询的 MIB 的具体管理单元，比如下图的 System。点击 Start Query，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 MIB Values 窗口：

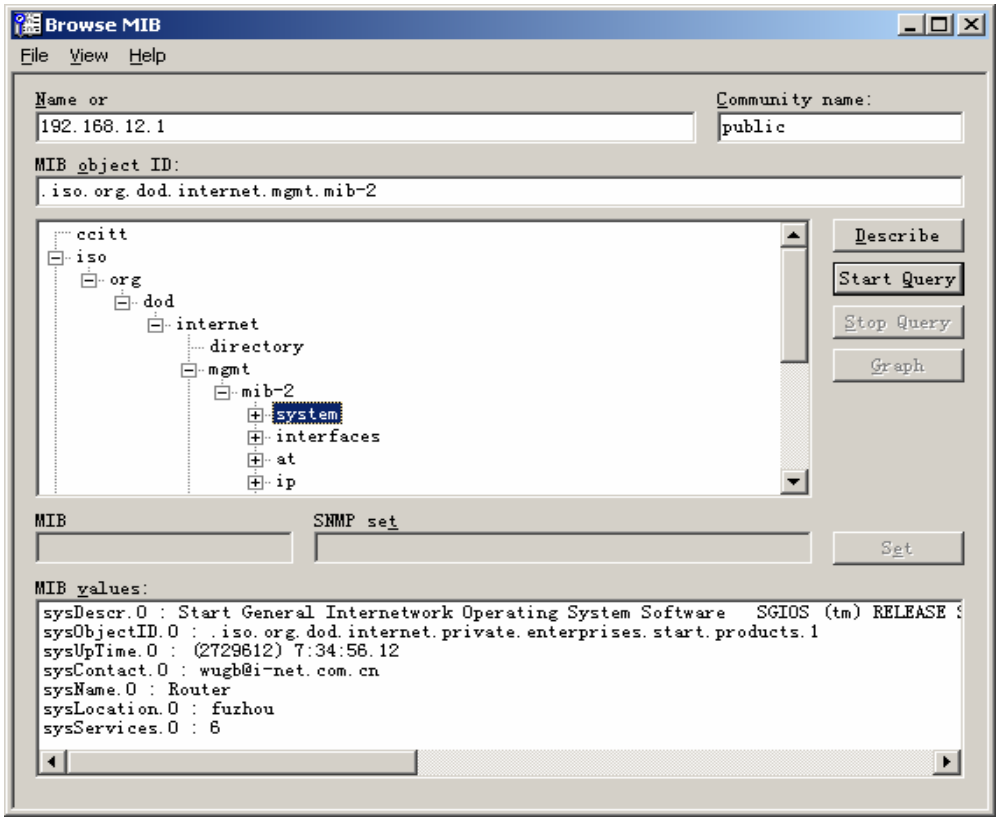


图 7　MIB 查询界面

HP OpenView 有很强大的网络管理的功能，比如，还可以用图表示出网络接口的流量统计图，其他的具体的各项 SNMP 的功能，见网管软件的文档，这里不在详述：

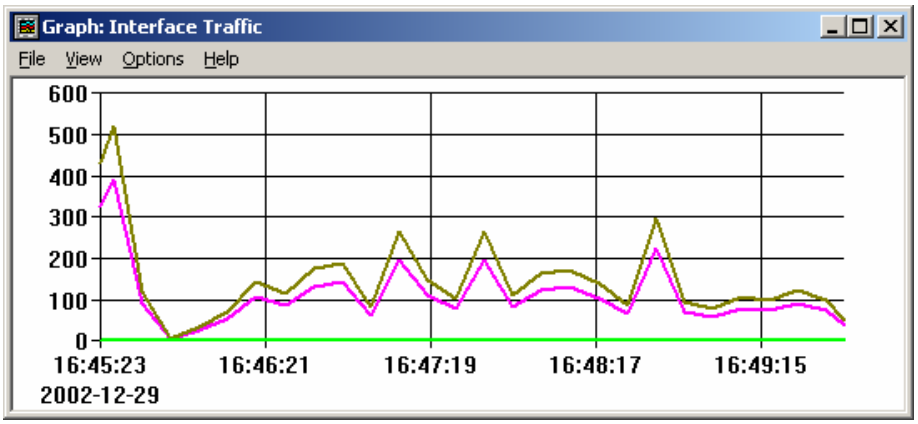


图 8　接口流量统计图

20.4.2.　SNMP 访问列表关联控制实例

我司产品可以设置访问列表关联的方式，只要访问列表中允许的 NMS 才可以利用 SNMP 对 Agent 进行监控和管理，限制 NMS 对网络设备的访问，提高 SNMP 的

安全性。

在全局配置模式下：

```
Ruijie(config)# access-list 1 permit 192.168.12.181
Ruijie(config)# snmp-server community public RO 1
```

通过如上配置，只有 IP 地址为 192.168.12.181 的主机才能利用 SNMP 对网络设备进行监控和管理了。

20.4.3. SNMPv3 相关配置实例

以下的配置允许 SNMPv3 的管理者采用认证＋加密模式通过用户名 v3user 对 MIB-2(1.3.6.1.2.1)节点下的管理变量进行设置和查看。采用的认证模式为 MD5，使用的认证密码为 MD5-Auth，采用 DES 加密，加密密钥为 DES-Priv。同时允许向 192.168.65.199 以 SNMPv3 格式发送 Trap。发送 Trap 使用的用户名为 v3user, 采用认证＋加密模式发送，采用的认证模式为 MD5，使用的认证密码为 MD5-Auth，采用 DES 加密，加密密钥为 DES-Priv。

```
Ruijie(config)# snmp-server view v3userview 1.3.6.1.2.1 include
Ruijie (config)# snmp-server group v3usergroup v3 priv read
v3userview write v3userview
Ruijie (config)# snmp-server user v3user v3usergroup v3 auth
md5 md5-auth priv des56 des-priv
Ruijie (config)# snmp-server host 192.168.65.199 traps version
3 priv v3user
```

第21章 RMON 配置

21.1. 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。

21.1.1. 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。

21.1.2. 历史组

历史组(History)是 RMON 中的第 2 组，历史组定期地收集网络统计信息，并记录下来以便日后处理。它包含两个小组：

1. HistoryControl 组用来设置采样间隔时间、采样数据源等控制信息。

2. EthernetHistory 组为管理员提供有关网段流量、错误包、广播包、利用率以及碰撞次数等其他统计信息的历史数据。

21.1.3. 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。

21.1.4. 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。

21.2. RMON 配置任务列表

21.2.1. 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

注意：

我司产品当前版本只支持以太网接口的统计。索引值应该是一个 1-65535 之间的整数，目前可最多同时配置 100 条统计项。

21.2.2. 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

注意：

我司产品当前版本只支持以太网的纪录。索引值应该在 1-65535 之间，最多可以配置 10 条控制表项。

Bucket-number：控制项指定了采用的数据源、时间间隔。每个采样区间，都进行一次采样。采样的结果保存下来，Bucket-number 指定了保存采样的最大数目，当采样纪录达到最大值时，则新纪录覆盖最早的纪录。Bucket-number 取值范围是 1-65535，默认值是 10。

Interval：采样的时间间隔。默认值是 1800 秒，取值在 1-3600 之间。

21.2.3. 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*]	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

21.2.4. 显示 RMON 状态

命令	作用
Ruijie(config)# **show rmon alarm**	显示警告组
Ruijie(config)# **show rmon event**	显示事件组
Ruijie(config)# **show rmon history**	显示历史组
Ruijie(config)# **show rmon statistics**	显示统计组

21.3. RMON 配置实例

21.3.1. 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
```

21.3.2. 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
```

21.3.3. 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 "ifIn
NUcastPkts is too much " owner zhangsan
```

21.3.4. 显示 rmon 状态实例

21.3.4.1. show rmon alarm

```
Ruijie# show rmon alarm
Alarm : 1
Interval : 1
Variable : 1.3.6.1.2.1.4.2.0
Sample type : absolute
Last value : 64
Startup alarm : 3
Rising threshold : 10
Falling threshold : 22
Rising event : 0
Falling event : 0
Owner : zhangsan
```

21.3.4.2. show rmon event

```
Ruijie# show rmon event
Event : 1
Description : firstevent
Event type : log-and-trap
Community : public
Last time sent : 0d:0h:0m:0s
Owner : zhangsan
Log : 1
Log time : 0d:0h:37m:47s
Log description : ipttl
Log : 2
Log time : 0d:0h:38m:56s
Log description : ipttl
```

21.3.4.3. show rmon history

```
Ruijie# show rmon history
Entry : 1
Data source : Gi1/1
Buckets requested : 65535
```

```
Buckets granted : 10
Interval : 1
Owner : zhangsan
Sample : 198
Interval start : 0d:0h:15m:0s
DropEvents : 0
Octets : 67988
Pkts : 726
BroadcastPkts : 502
MulticastPkts : 189
CRCAlignErrors : 0
UndersizePkts : 0
OversizePkts : 0
Fragments : 0
Jabbers : 0
Collisions : 0
Utilization : 0
```

21.3.4.4. show rmon statistics

```
Ruijie# show rmon statistics
Statistics : 1
Data source : Gi1/1
DropEvents : 0
Octets : 1884085
Pkts : 3096
BroadcastPkts : 161
MulticastPkts : 97
CRCAlignErrors : 0
UndersizePkts : 0
OversizePkts : 1200
Fragments : 0
Jabbers : 0
Collisions : 0
Pkts64Octets : 128
Pkts65to127Octets : 336
Pkts128to255Octets : 229
Pkts256to511Octets : 3
Pkts512to1023Octets : 0
Pkts1024to1518Octets : 1200
Owner : zhangsan
```

第22章 基于端口的流控制配置

22.1. 风暴控制

22.1.1. 概述

当 LAN 中存在过量的广播、多播或未知名单播包时，就会导致网络变慢和报文传输超时几率大大增加。这种情况我们称之为 LAN 风暴。协议栈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。当接口接收到的广播、多播或未知名单播包的速率超过所设定的阀值时，设备将只允许通过所设定阀值带宽的报文，超出阀值部分的报文将被丢弃，直到数据流恢复正常，从而避免过量的泛洪报文进入 LAN 中形成风暴。

22.1.2. 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。

您可以在接口配置模式下通过命令 **no storm-control broadcast ,no storm-control multicast , no storm-control unicast** 来关闭接口相应的风暴控制功能。

下面的例子打开 GigabitEthernet 0/1 上的多播风暴控制功能，并且设置允许的速率为 4M。

```
Ruijie# configure terminal
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# storm-control multicast 4096
Ruijie(config-if)# end
```

说明：

1. 缺省情况下， S2300 系列产品针对多播的风暴控制功能被关闭， S2300 系列产品针对广播和未知名单播的风暴控制功能被打开，风暴控制的缺省值为端口带宽的百分之一。

注意：

1. 设备基于 level 的风暴控制，带宽基准值直接采用设置风暴控制的物理口支持的最大带宽值，不采用物理口实际工作时的带宽值进行换算。
2. 如果仅使能风暴控制功能，如配置 storm-control broadcast，这时风暴控制采用缺省设置，缺省设置值为端口带宽的百分之一。

22.1.3. 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
Ruijie# **show storm-control** [*interface-id*]	显示风暴控制信息。

下面的例子为显示接口 Gi0/3 的风暴控制功能的使能状态：

```
Ruijie# show storm-control gigabitEthernet 0/3
Interface   Broadcast Control   Multicast Control   Unicast
Control action
GigabitEthernet 0/3 Disabled  Disabled   Disabled    none
```

您也可以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
```

22.2. Protected Port

22.2.1. 概述

有些应用环境下，要求一台设备上的有些端口之间不能互相通讯。在这种环境下，这些端口之间的通讯，不管是单址帧，还是广播帧，以及多播帧，都不能在保护口之间进行转发。您可以通过将某些端口设置为保护口(Protected Port)来达到目的。

当您将某些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转发，但允许保护口之间进行三层路由，第二种是既阻断保护口之间的二层转发又阻断三层路由；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。

当您将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将按照 SPAN 的设置发到 SPAN 目的端口。因此您最好不要将 SPAN 目的端口设为保护口(这样您还可以节约系统资源)。

设备支持将 Aggregated Port 设置为保护口，当您将一个 Aggregated Port 设置为保护口时，Aggregated Port 的所有成员口都被设置为保护口。

22.2.2. 配置 Protected Port

将一个端口设置为保护口：

命令	作用
Ruijie(config-if)**# switchport protected**	将该接口设置为保护口

您可以通过命令 **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
```

注意：

S23 系列产品的保护口功能不支持垮设备，即堆叠情况下如果保护口分布在不同的堆叠成员设备上，那么不同设备上保护口之间还是可以通信，同一设备上的保护口之间不能通信。

22.2.3. 显示 Protected Port 配置

命令	作用
Ruijie(config-if)**# show interfaces switchport**	显示交换口配置

您可以通过命令 **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
```

22.3. 端口安全

22.3.1. 概述

端口安全功能通过报文的源 MAC 地址或者源 MAC+源 IP 或者仅源 IP 来限定报文是否可以进入交换机的端口，您可以静态设置特定的MAC地址，静态IP+MAC绑定或者仅 IP 绑定，或者动态学习限定个数的 MAC 地址来控制报文是否可以进入端口，使能端口安全功能的端口称为安全端口。只有源MAC地址为端口安全地址表中配置或者配置绑定的IP+MAC地址，或者配置的仅IP绑定地址，或者学习到的MAC地址的报文才可以进入交换机通信，其他报文将被丢弃。

为了增强安全性，您可以将 MAC 地址和 IP 地址绑定起来作为安全地址。当然您也可以只指定 MAC 地址而不绑定 IP 地址。

您可以使用下面几种方式加满端口上的安全地址：

- 通过使用接口配置模式下的命令来手工配置端口的所有安全地址。
- 让该端口自动学习地址，这些自动学习到的地址将变成该端口上的安全地址，直到达到最大个数。需要注意的是，自动学习的安全地址均不会绑定 IP 地址，如果在一个端口上，您已经配置了绑定 IP 地址的安全地址，则将不能再通过自动学习来增加安全地址。
- 手工配置一部分安全地址，剩下的部分让设备自己学习。

如果一个端口被配置为一个安全端口，当其安全地址的数目已经达到允许的最大个数后，如果该端口收到一个源地址不属于端口上的安全地址的包时，一个安全违例将产生。当安全违例将产生时，您可以设置下面几种针对违例的处理模式：

protect：当安全地址个数满后，安全端口将丢弃未知名地址（不是该端口的安全地址的任何一个）的包。该处理模式为缺省的对违例的处理模式。

restrict：当违例产生时，将发送一个 Trap 通知。

shutdown：当违例产生时，将关闭端口并发送一个 Trap 通知。

22.3.2. 配置端口安全

22.3.2.1. 端口安全的缺省配置

下表显示的端口安全的缺省配置：

内容	缺省设置
端口安全开关	所有端口均关闭端口安全功能

最大安全地址个数	128
安全地址	无
违例处理方式	保护(protect)

22.3.2.2. 端口安全配置指导

配置端口安全时有如下一些限制：

- 一个安全端口不能是一个 Aggregate Port
- 一个安全端口不能是 SPAN 的目的端口
- 一个安全端口只能是一个 Access Port

802.1x 认证功能和端口安全功能互斥使能。802.1x 认证功能和端口安全功能都可以保证网络使用者的合法性，使能其一就可以达到控制端口接入的目的。

同时 IP+MAC 绑定和仅 IP 绑定的安全地址与 ACLs 共享系统的硬件资源，因此当您在某一个安全端口上应用了 ACLs，则该端口上所能设置的 IP+MAC 绑定和仅 IP 绑定的安全地址个数将会减少。

一个安全端口上的安全地址的格式必须保持一致，即一个端口上的安全地址要么全是绑定了 IP 地址的安全地址，要么都是不绑定 IP 地址的安全地址。如果一个安全端口同时包含这两种格式的安全地址，则不绑定 IP 地址的安全地址将失效(绑定 IP 地址的安全地址优先级更高)。

22.3.2.3. 配置安全端口及违例处理方式

在接口配置模式下，请使用如下命令配置安全端口及违例处理方式：

命令	作用
Ruijie(config-if)# **switchport port-security**	打开该接口的端口安全功能
Ruijie(config-if)# **switchport port-security maximum** *value*	设置接口上安全地址的最大个数，范围是 1－1000，缺省值为 128。

Ruijie(config-if)# **switchport port-security violation{protect | restrict | shutdown}**	设置处理违例的方式： **protect**：保护端口，当安全地址个数满后，安全端口将丢弃未知名地址(不是该端口的安全地址中的任何一个)的包 **restrict**：当违例产生时，将发送一个 Trap 通知 **shutdown**：当违例产生时，将关闭端口并发送一个 Trap 通知。当端口因为违例而被关闭后，您可以在全局配置模式下使用命令 **errdisable recovery** 来将接口从错误状态中恢复过来。

在接口配置模式下，您可以使用命令 **no switchport port-security** 来关闭一个接口的端口安全功能。使用命令 **no switchport port-security maximum** 来恢复为缺省个数。使用命令 **no switchport port-security violation** 来将违例处理置为缺省模式。

下面的例子说明了如何使能接口 gigabitethernet 0/3 上的端口安全功能，设置最大地址个数为 8，设置违例方式为 protect

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitethernet 0/3
Ruijie(config-if)# switchport mode access
Ruijie(config-if)# switchport port-security
Ruijie(config-if)# switchport port-security maximum 8
Ruijie(config-if)# switchport port-security violation protect
Ruijie(config-if)# end
```

说明：

1，如果安全端口上配置了仅 Ip 或者 Ip+Mac 绑定的的安全地址，当端口学习的 Mac 地址达到并超出设置的安全地址个数时，并不会产生违例事件。

2，只在首次端口违例产生才发出 trap 及 log 信息。

3，二层端口安全的违例产生到处理完成的生效时间大约在 1 秒内。

22.3.2.4. 配置安全端口上的安全地址

在接口配置模式下，请使用如下命令为安全端口添加安全地址：

命令	作用

Ruijie(config-if)# **switchport port-security mac-address** *mac-address* [**ip-address** *ip-address*]	手工配置接口上的安全地址。**ip-address**(可选)： 为这个安全地址绑定的 IP 地址。

在接口配置模式下，您可以使用命令 **no switchport port-security mac-address** *mac-address* 来删除该接口的安全地址。

下面的例子说明了如何为接口 gigabitethernet 0/3 配置一个安全地址：00d0.f800.073c，并为其绑定一个 IP 地址：192.168.12.202。

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitethernet 0/3
Ruijie(config-if)# switchport mode access
Ruijie(config-if)# switchport port-security
Ruijie(config-if)# switchport port-security mac-address 00d0.f800.073c ip-address 192.168.12.202
Ruijie(config-if)# end
```

22.3.2.5. 配置安全地址的老化时间

您可以为一个接口上的所有安全地址配置老化时间。打开这个功能，您需要设置安全地址的最大个数，这样，您就可以让设备自动的增加和删除接口上的安全地址。

在接口配置模式下，请使用如下命令配置安全地址老化时间：

命令	作用
Ruijie(config-if)#**switchport port-security aging**{**static** | **time** *time* }	**static**：加上这个关键字，表示老化时间将同时应用于手工配置的安全地址和自动学习的地址，否则只应用于自动学习的地址。 **Time** ：表示这个端口上安全地址的老化时间，范围是 0－1440，单位是分钟。如果您设置为 0，则老化功能实际上被关闭。老化时间按照绝对的方式计时，也就是一个地址成为一个端口的安全地址后，经过 Time 指定的时间后，这个地址就将被自动删除。*Time* 的缺省值为 0。

您可以在接口配置模式下使用命令 **no switchport port-security aging time** 来关闭一个接口的安全地址老化功能，使用命令 **no switchport port-security aging static** 来使老化时间仅应用于动态学习到的安全地址。

下面的例子说明了如何配置一个接口 gigabitethernet 0/3 上的端口安全的老化时间，老化时间设置为 8 分钟，老化时间同时应用于静态配置的安全地址：

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitthernet 0/3
Ruijie(config-if)# switchport port-security aging time 8
Ruijie(config-if)# switchport port-security aging static
Ruijie(config-if)# end
```

22.3.3. 查看端口安全信息

在特权模式下，您可以通过如下命令来查看端口安全的信息：

命令	作用
Ruijie**#show port-security interface** [*interface-id*]	查看接口的端口安全配置信息。
Ruijie**#show port-security address**	查看安全地址信息。
Ruijie**# show port-security address** [*interface-id*]	显示某个接口上的安全地址信息
Ruijie**# show port-security**	显示所有安全端口的统计信息，包括最大安全地址数，当前安全地址数以及违例处理方式等。

下面的例子显示了接口 Gigabitethernet 0/3 上的端口安全配置：

```
Ruijie# show port-security interface gigabitethernet 0/3
Interface : Gi0/3
Port Security: Enabled
Port status : down
Violation mode:Shutdown
Maximum MAC Addresses:8
Total MAC Addresses:0
Configured MAC Addresses:0
Aging time : 8 mins
SecureStatic address aging : Enabled
```

下面的例子显示了系统中的所有安全地址

```
Ruijie# show port-security address
Vlan Mac Address IP Address Type Port Remaining Age(mins)
-----------------------------------------------------------
1  00d0.f800.073c   192.168.12.202    Configured   Gi0/3    8
1  00d0.f800.3cc9   192.168.12.5      Configured   Gi0/1    7
```

您也可以只显示一个接口上的安全地址，下面的例子显示了接口 gigabitstethernet 0/3 上的安全地址

```
Ruijie# show port-security address interface gigabitethernet
0/3
```

```
Vlan Mac Address IP Address Type Port Remaining Age(mins)
---- -------------- --------- ------ -----------------
1    00d0.f800.073c  192.168.12.202 Configured Gi0/3    8
```

下面的例子显示的是安全端口的统计信息

```
Ruijie# show port-security
Secure Port MaxSecureAddr(count) CurrentAddr(count) Security
Action
----------  -----------------  -----------------  -------
Gi0/1       128                 1                 Restrict
Gi0/2       128                 0                 Restrict
Gi0/3       8                    1                 Protect
```

22.4. ARP-CHECK

22.4.1. 概述

ARP 报文检查（ARP-CHECK）基于全局或者端口上的 MAC+IP 绑定安全功能，例如 DHCP Snooping，端口安全或者全局地址绑定等。通过丢弃非法用户的 ARP 报文来有效防止欺骗 ARP，防止非法信息点冒充网络关键设备的 IP（如服务器），造成网络通讯混乱。

ARP-CHECK 有三种模式：打开，关闭和自动模式，缺省为自动模式。

在打开模式下，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。

在关闭模式下，不检查端口上的 ARP 报文。

在自动模式下，在端口上没有合法用户的情况下，不检查 ARP 报文；在有合法用户的情况下，检查 ARP 报文。

ARP 报文检查的限制：

1. 打开端口安全地址的 ARP 报文检查会使所有端口的绑定 IP 的安全地址最大数目减少一半。

2. 打开端口安全地址的 ARP 报文检查对已经存在的安全地址不生效。如果您要使以前设置的安全地址生效，可以重新关闭，再打开该端口的安全地址。端口 ARP 报文检查使用了策略管理模块，和其它策略管理模块共享硬件资源。如果硬件资源不足时，可能出现部分安全地址的 ARP 报文检查不生效的现象。

3. 当 MAC+IP 的安全地址表项比较多时，打开 ARP Check Cpu，对 CPU 性能影响比较大,会降低 CPU 效率。

22.4.2. 配置 ARP-CHECK

从特权模式下开始配置 ARP-CHECK

命令	作用
Ruijie**# configure t**	进入配置模式
Ruijie(config)**#interface** *interface-id*	进入接口模式
Ruijie(config-if)**# arp-check**	打开 arp 报文检查
Ruijie(config-if)**# no arp-check**	关闭 arp 报文检查
Ruijie(config-if)**# arp-check auto**	还原成缺省配置

例如在端口上添加合法用户 mac 地址 00d0.f822.33ab，IP 地址为 192.168.2.5 时，端口上的 ARP 报文检查会自动启用。

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# interface fastEthernet 0/5
Ruijie(config-if)# switchport port-security
Ruijie(config-if)# switchport port-security mac-address
00d0.f822.33ab ip-address 192.168.2.5
```

ARP 报文检查自动启用了，如果你想关闭 ARP 报文检查。

```
Ruijie(config-if)# no arp-check
```

说明:

1. ARP-CHECK 功能对 ARP 报文内容的检查由于产品的不同而略有不同，S23 系列产品检查 ARP 协议内部的 Sender Mac 和 Sender Ip 字段。

第23章 802.1X 配置

本章节描述基于 AAA 服务配置的相关内容。802.1x 用于控制用户对网络访问的认证，并对其提供授权与记帐功能。

本节包含如下内容：

- 概述
- 配置 802.1x
- 查看 802.1x 的配置及当前的统计值
- 配置 802.1x 其它注意事项

说明：

有关本节引用的 CLI 命令的详细使用信息及说明，请参照《配置 802.1X 命令》

23.1. 概述

IEEE 802 LAN 中，用户只要能接到网络设备上，不需要经过认证和授权即可直接使用。这样，一个未经授权的用户，他可以没有任何阻碍地通过连接到局域网的设备进入网络。随着局域网技术的广泛应用，特别是在运营网络的出现，对网络的安全认证的需求已经提到了议事日程上。如何在以太网技术简单、廉价的基础上，提供用户对网络或设备访问合法性认证，已经成为业界关注的焦点。IEEE 802.1x 协议正是在这样的背景下提出的。

IEEE802.1x（Port-Based Network Access Control）是一个基于端口的网络存取控制标准，为 LAN 提供点对点式的安全接入。这是 IEEE 标准委员会针对以太网的安全缺陷而专门制定的标准，能够在利用 IEEE 802 LAN 优势的基础上，提供一种对连接到局域网设备的用户进行认证的手段。

IEEE 802.1x 标准定义了一种基于“客户端——服务器”（Client-Server）模式实现了限制未认证用户对网络的访问。客户端要访问网络必须先通过服务器的认证。

在客户端通过认证之前，只有 EAPOL 报文（Extensible Authentication Protocol over LAN）可以在网络上通行。在认证成功之后，正常的数据流便可在网络上通行。

应用 802.1x 我司的设备提供了 Authentication，Authorization，and Accounting 三种安全功能，简称 AAA。

- Authentication： 认证，用于判定用户是否可以获得访问权，限制非法用户
- Authorization： 授权，授权用户可以使用哪些服务，控制合法用户的权限
- Accounting： 计账，记录用户使用网络资源的情况，为收费提供依据

我们将从以下几个方面阐述 802.1x

- 设备的角色
- 认证的发起及认证过程中的报文交互
- 已认证用户及未认证用户的状态
- 典型应用的拓扑结构

23.1.1. 设备的角色

IEEE802.1x 标准认证体系由恳请者、认证者、认证服务器三个角色构成，在实际应用中，三者分别对应为：工作站（Client）、设备(network access server，NAS)、Radius-Server。

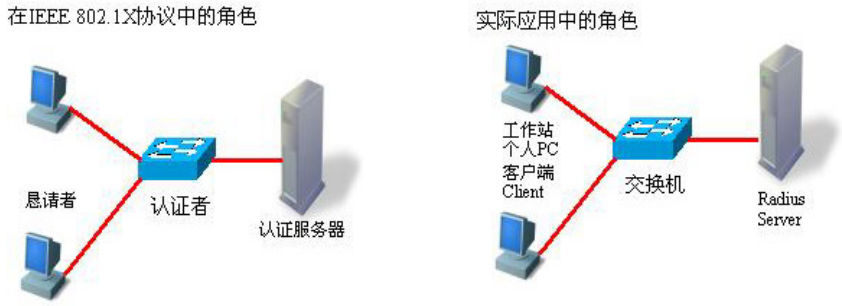


图 1

- 恳请者

恳请者是最终用户所扮演的角色，一般是个人 PC。它请求对网络服务的访问，并对认证者的请求报文进行应答。恳请者必须运行符合 IEEE 802.1x 客户端标准的软件，目前最典型的就是 WindowsXP 操作系统自带的 IEEE802.1x 客户端支持，另外，我司也已推出符合该客户端标准的 Ruijie Supplicant 软件。

- 认证者

认证者一般为交换机等接入设备。该设备的职责是根据客户端当前的认证状态控制其与网络的连接状态。在客户端与服务器之间，该设备扮演着中介者的角色：从客户端要求用户名，核实从服务器端的认证信息，并且转发给客户端。因此，设备除了扮演 IEEE802.1x 的认证者的角色，还扮演 RADIUS Client 角色，因此我们把设备称作 network access server(NAS)，它要负责把从客户端收到的回应封装到 RADIUS 格式的报文并转发给 RADIUS Server，同时它要把从 RADIUS Server 收到的信息解释出来并转发给客户端。

扮演认证者角色的设备有两种类型的端口：受控端口（controlled Port）和非受控端口（uncontrolled Port）。连接在受控端口的用户只有通过认证才能访问网络资源；而连接在非受控端口的用户无须经过认证便可以直接访问网络资源。我们把用户连接在受控端口上，便可以实现对用户的控制；非受控端口主要是用来连接认证服务器，以便保证服务器与设备的正常通讯。

- 认证服务器

认证服务器通常为 RADIUS 服务器，认证过程中与认证者配合，为用户提供认证服务。认证服务器保存了用户名及密码，以及相应的授权信息，一台服务器可以对多台认证者提供认证服务，这样就可以实现对用户的集中管理。认证服务器还负责管理从认证者发来的记帐数据。锐捷网络科技公司实现 802.1x 的设备完全兼容标准的 Radius Server，如 MicroSoft win2000 Server 自带的 Radius Server 及 Linux 下的 Free Radius Server。

23.1.2. 认证的发起及认证过程中的报文交互

恳请者和认证者之间通过 EAPOL 协议交换信息，而认证者和认证服务器通过 RADIUS 协议交换信息，通过这种转换完成认证过程。EAPOL 协议封装于 MAC 层之上，类型号为 0x888E。同时，标准为该协议申请了一个组播 MAC 地址 01-80-C2-00-00-03，用于初始认证过程中的报文传递。

下图是一次典型的认证过程中，三个角色设备的报文交互过程

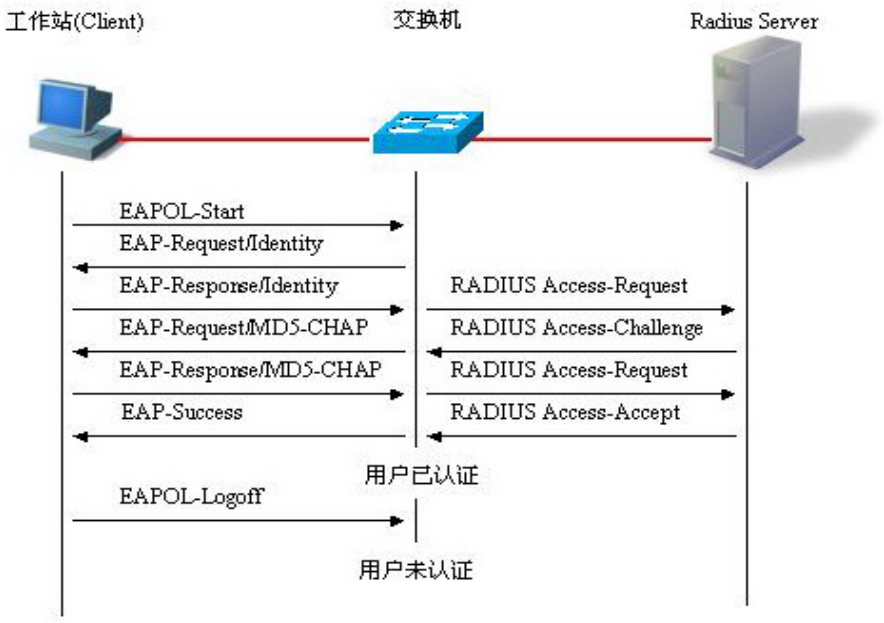


图 2

该过程是一个典型的由用户发起的认证过程(在一些特殊的情形下，设备也可能主动发出认证请求，过程与该图一致，只是少了用户主动发出请求这一步）。

23.1.3. 已认证用户及未认证用户的状态

802.1x 中根据端口的认证状态来决定该端口上的用户是否允许访问网络，由于我们对 802.1X 进行扩展，是基于用户的，所以，我们是根据一个端口下的用户的认证状态来决定该用户是否允许访问网络资源。一个非受控端口下的所有用户均可使用网络资源，而一个受控端口下的用户只有处于已认证状态（Authorized）才能访问网络资源。一个用户刚发起认证时，状态处于未认证状态（unauthorized），这时它不能访问网络，在认证通过后，该用户的状态会变为已认证状态（authorized），此时该用户便可以使用网络资源。

如果工作站不支持 802.1x，而该机器连接在受控端口下，当设备请求该用户的用户名时，由于工作站不支持导致没对该请求做出响应。这就意味着该用户仍然处于未认证状态（unauthorized），不能访问网络资源。

相反地，如果工作站支持 802.1x，而所连的设备不支持 802.1x。用户发出的 EAPOL-START 帧无人响应，用户在发送一定数目的 EAPOL-START 帧仍未收到回应的情形下，将认为自己所连的端口是非受控端口，而直接使用网络资源。

在支持 802.1x 的设备下，所有端口的默认设置是非受控端口，我们可以把一个端口设置成受控端口，从而要求这个端口下的所有用户都要进行认证。

当用户通过了认证（设备收到了从 RADIUS Server 服务器发来的成功报文），该用户便转变成已认证状态(authorized)，该用户可以自由使用网络资源。如果用户认证失败以至仍然处于未认证状态，可以重新发起认证。如果设备与 RADIUS server 之间的通讯有故障，那么该用户仍然处于未认证状态（unauthorized），网络对该用户来说仍然是不可使用的。

当用户发出 EAPOL-LOGOFF 报文后，该用户的状态由已认证(authorized)转向未认证状态(unauthorized)。

当设备的某个端口变为 LINK-DOWN 状态，该端口上的所有用户均变为未认证(unauthorized)状态。

当设备重新启动，该设备上的所有用户均变为未认证状态(unauthorized)。

如果您要强制一个用户通过认证，可以通过添加静态 MAC 地址来实现。

23.1.4. 典型应用的拓扑结构

A、带 802.1x 的设备作为接入层设备

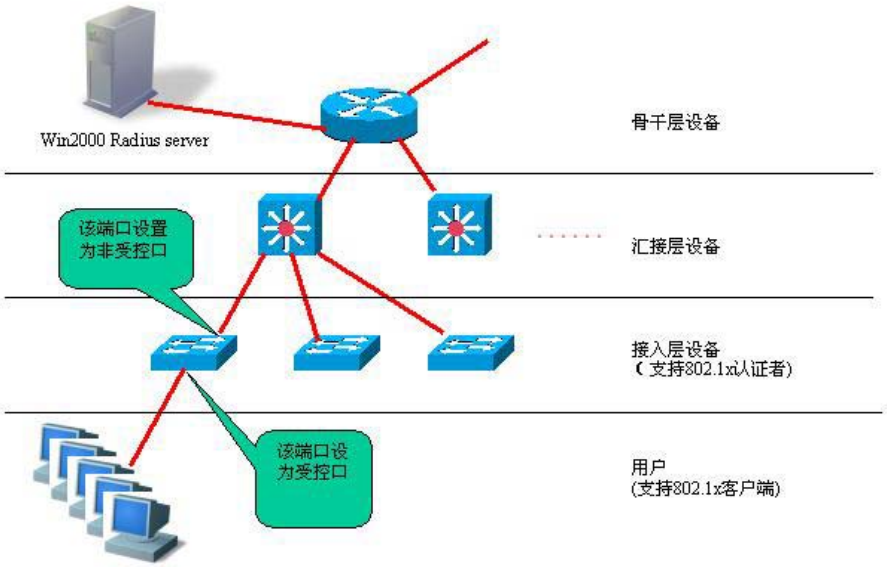


图 3

该方案的说明：

- 该方案的要求：

1. 用户支持 802.1x，即要装有 802.1x 的客户端软件（windowXp 自带，Ruijie-supplicant 或其他符合 IEEE802.1x 标准的客户端软件）。

2. 接入层设备支持 IEEE 802.1x

3. 有一台（或多台）支持标准 RADIUS 的服务器作为认证服务器

- 该方案的配置要点：

1. 与 Radius Server 相连的口及上联口，配置成非受控口，以便设备能正常地与服务器进行通讯，以及使已认证用户能通过上联口访问网络资源

2. 与用户连接的端口要设置为受控口，以实现对接入用户的控制，用户必须通过认证才能访问网络资源。

- 该方案的特点：

1. 每台支持 802.1x 的设备所负责的客户端少，认证速度快。各台设备之间相互独立，设备的重启等操作不会影响到其它设备所连接的用户。

2. 用户的管理集中于 Radius Server 上，管理员不必考虑用户连接在哪台设备上，便于管理员的管理

3. 管理员可以通过网络管理接入层的设备

B、带 802.1x 的设备作为汇接层设备

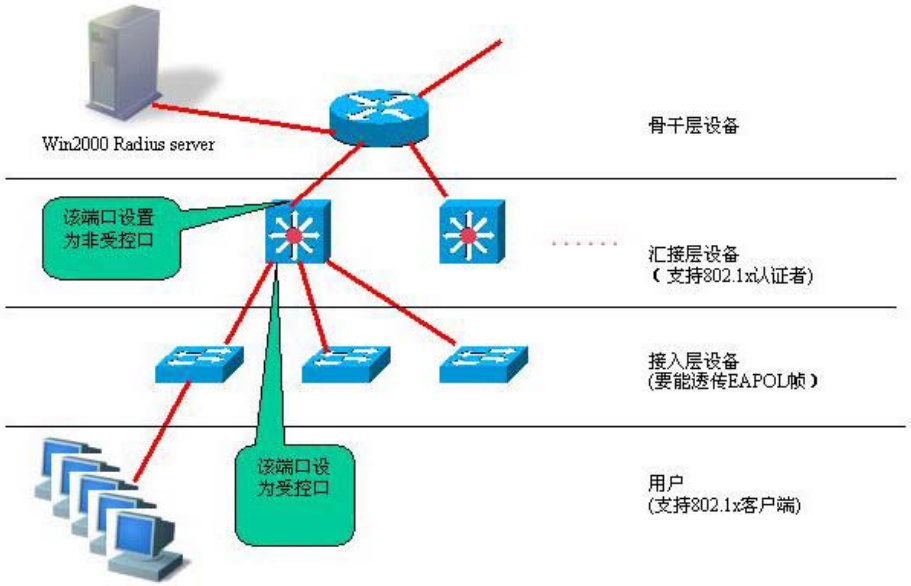


图 4

该方案的说明：

- 该方案的要求：

1. 用户支持 802.1x，即要装有 802.1x 的客户端软件（windowXp 自带，Ruijie-supplicant 或其他符合 IEEE802.1x 标准的客户端软件）。

2. 接入层设备支持要能透传 IEEE 802.1x 帧(EAPOL)

3. 汇接层设备支持 802.1x（扮演认证者角色）

4. 有一台（或多台）支持标准 RADIUS 的服务器作为认证服务器

- 该方案的配置要点：

1. 与 Radius Server 相连的口及上联口，配置成非受控口，以便设备能正常地与服务器进行通讯，以及使已认证用户能通过上联口访问网络资源

2. 与接入层设备连接的端口要设置为受控口，以实现对接入用户的控制，用户必须通过认证才能访问网络资源。

- 该方案的特点：

1. 由于是汇接层设备，网络规模大，下接用户数多，对设备的要求高，若该层设备发生故障，将导致大量用户不能正常访问网络。

2. 用户的管理集中于 Radius Server 上，管理员无需考虑用户连接在哪台设备上，便于管理员的管理

3. 接入层设备可以使用较廉价的非网管型设备（只要支持 EAPOL 帧透传）

4. 管理员不能通过网络直接管理接入层设备

23.2. 配置 802.1X

我们将通过以下章节说明如何配置 802.1x

- 802.1x 的默认配置
- 802.1x 的配置注意事项
- 配置设备与 RADIUS SERVER 之间的通讯
- 设置 802.1X 认证的开关
- 打开/关闭一个端口的认证
- 打开定时重认证
- 打开/关闭 过滤非我司 supplicant 功能的开关
- 改变 QUIET 时间
- 设置报文重传间隔
- 设置最大请求次数
- 设置最大重认证次数
- 设置 Server-timeout
- 配置设备主动发起 802.1x 认证
- 配置 802.1x 记帐
- 配置 IP 授权模式
- 发布广告信息
- 某端口下的可认证主机列表
- 授权
- 配置认证方式
- 配置备份认证服务器
- 对在线用户的配置及管理
- 实现用户与 IP 的捆绑
- 基于端口的流量记费
- 实现端口的 VLAN 自动跳转及控制开关
- 代理服务器屏蔽和拨号屏蔽
- 配置客户端在线探测
- 配置 EAPOL 帧带 TAG 的选项开关

23.2.1. 802.1x 的默认配置

下表列出 802.1x 的一些缺省值

内容	默认值
认证 Authentication	关闭 DISABLE
记帐 Accounting	关闭 DISABLE
认证服务器(Radius Server) *服务器 IP 地址(ServerIp) *认证 UDP 端口 *密码(Key)	*无缺省值 *1812 *无缺省值
记帐服务器(Accounting Server) *记帐服务器 IP 地址 *记帐 UDP 端口	*无缺省值 *1813
所有端口的类型	非受控端口（所有端口均无须认证便可直接通讯）
定时重认证 re-authentication	关闭
定时重认证周期 reauth_period	3600 秒
认证失败后允许再次认证的间隔	10 秒
重传时间间隔	3 秒
最大重传次数	3 次
客户端超时时间	3 秒，在该段时间内没有收到客户端的响应便认为这次通讯失败
服务器超时时间	5 秒，在该段时间内没有收到服务器的回应，便认为这次通讯失败
某端口下可认证主机列表	无缺省值

23.2.2. 802.1X 的配置注意事项

- 只有支持 802.1x 的产品，才能进行以下设置。
- 802.1x 既可以在二层下又可以在三层下的设备运行。
- 要先设置认证服务器 IP 地址，radius－server 认证方式才可以正常工作。
- 打开端口安全的端口不允许打开 1X 认证。
- Aggregate Port 不允许打开 1X 认证。
- 交换机只要有一个端口打开了 1x 功能，所有的端口都会将 1x 协议报文送到 cpu。

23.2.3. 配置设备与 RADIUS SERVER 之间的通讯

Radius Server 维护了所有用户的信息：用户名、密码、该用户的授权信息以及该用户的记帐信息。所有的用户集中于 Radius Server 管理，而不必分散于每台设备，便于管理员对用户的集中管理。

设备要能正常地与 RADIUS SERVER 通讯，必须进行如下设置：

Radius Server 端：要注册一个 Radius Client。注册时要告知 Radius Server 设备的 IP、认证的 UDP 端口（若记帐还要添记帐的 UDP 端口）、设备与 Radius Server 通讯的约定密码，还要选上对该 Client 支持 EAP 扩展认证方式）。对于如何在 Radius Server 上注册一个 Radius Client，不同软件的设置方式不同，请查阅相关的文档。

设备端：为了让设备能与 Server 进行通讯，设备端要做如下的设置：设置 Radius Server 的 IP 地址，认证（记帐）的 UDP 端口，与服务器通讯的约定密码。

在特权模式下，按如下步骤设置设备与 Radius Server 之间的通讯：

命令	作用
configure terminal	进入全局配置模式
aaa new-model	打开 AAA 开关
radius-server host *ip-address* [**auth-port** *port*] [**acct-port** *port*]	配置 RADIUS 服务器
Radius-server key *string*	配置 RADIUS Key
end	退出到特权模式
write	保存配置
show radius server	显示 RADIUS 服务器

使用 **no radius-server host** *ip-address* **auth-port** 命令将 Radius Server 认证 UDP 端口恢复为缺省值。使用 **no radius-server key** 命令删除 Radius Server 认证密码。以下例子是设置 server ip 为 192.168.4.12、认证 Udp 端口为 600、以明文方式设置约定密码：

```
Ruijie# configure terminal
Ruijie(config)# radius-server host 192.168.4.12
Ruijie(config)# radius-server host 192.168.4.12 auth-port 600
Ruijie(config)# radius-server key MsdadShaAdasdj878dajL6g6g
a
Ruijie(config)# end
```

- 官方约定的认证的 UDP 端口为 1812
- 官方约定的记帐的 UDP 端口为 1813
- 设备与 Radius Server 约定的密码的长度建议不少于 16 个字符

- 设备与 Radius Server 连接的端口要设置成非受控口

23.2.4. 设置 802.1X 认证的开关

当打开 802.1x 认证时，设备会主动要求受控端口上的主机进行认证，未通过认证的主机不允许访问网络。

在特权模式下，按如下步骤打开 1x 认证：

命令	作用
configure terminal	进入全局配置模式
aaa new-model	打开 AAA 开关
radius-server host *ip-address* [**auth-port** *port*] [**acct-port** *port*]	配置 RADIUS 服务器
radius-server key string	配置 RADIUS Key
aaa authentication dot1x *auth* **group radius**	配置 dot1x 认证方法列表
dot1x authentication *auth*	dot1x 应用认证方法列表
end	退出到特权模式
write	保存配置
show running-config	显示配置

注意：

在基于域名的 AAA 服务开关打开情况下，也即配置命令 **aaa domain enable** 时，**dot1x authentication** 命令选择的认证方法列表将不会被使用，而使用用户所在的域配置的认证方法列表。具体配置参考“配置基于域名的 AAA 服务”。

以下例子是打开 802.1x 认证：

```
Ruijie# configure terminal
Ruijie(config)# aaa new-model
Ruijie(config)# radius-server host 192.168.217.64
Ruijie(config)# radius-server key starnet
Ruijie(config)# aaa authentication dot1x authen group radius
Ruijie(config)# dot1x authentication authen
Ruijie(config)# end
Ruijie# show running-config
!
aaa new-model
!
aaa authentication dot1x authen group radius
```

```
!
username ruijie password 0 starnet
!
radius-server host 192.168.217.64
radius-server key 7 072d172e071c2211
!
!
!
dot1x authentication authen
!
interface VLAN 1
 ip address 192.168.217.222 255.255.255.0
 no shutdown
!
!
line con 0
line vty 0 4
!
end
```

802.1x 在应用 RADIUS 认证方法时，先配置 Radius Server 的 IP 地址，并确保设备与 Radius Server 之间的通讯正常。若没有 Radius Server 的配合，设备无法完成认证功能。如何设置 Radius Server 与设备之间的通讯请见上一章节。

23.2.5. 打开/关闭一个端口的认证

在 802.1x 打开的情形下，打开一个端口的认证，则该端口成为受控口，连接在该端口下的用户要通过认证才能访问网络，然而，在非受控端口下的用户可以直接访问网络。

在特权模式下，按如下步骤设置一个端口的认证状态。

命令	作用
configure terminal	进入全局配置模式
interface *interface*	进入接口设置模式,指定要配置的接口
dot1x port-control auto	设置该接口为受控接口（打开接口认证功能）。使用该命令的 no 选项关闭该接口的认证功能
end	退出到特权模式
write	保存配置
show dot1x port-control	查看 802.1x 接口认证配置

使用该命令的 **no dot1x port-control** 命令关闭接口的认证功能。以下例子是设

置以太网接口 1/1 为受控接口：

```
Ruijie# configure terminal
Ruijie(config)# interface f 1/1
Ruijie(config-if)# dot1x port-control auto
Ruijie(config)# end
```

当接口被设置为受控口的时候，只允许 EAP 报文过，往 CPU 的报文也在受控范围内。

注意：

如果希望 cpu 不收到任何来自受控口的非 EAP 报文，可以将交换机设置为管理 vlan，与用户 vlan 分开。

23.2.6. 打开定时重认证

802.1x 能定时主动要求用户重新认证，这样可以防止已通过认证的用户不会被其他用户冒用，还可以检测用户是否断线，使记费更准确。除了可以设定重认证的开关，我们还可以定义重认证的间隔。默认的重认证间隔是 3600 秒。在根据时常进行记费的场合下，要根据具体的网络规模确定重认证间隔，使之既有足够时间完成一次认证又尽可能精确。

在特权模式下，按如下步骤打开/关闭重认证状态，并且设置重认证时间间隔。

命令	作用
configure terminal	进入全局配置模式
dot1x re-authentication	打开定时重认证功能
dot1x timeout re-authperiod *seconds*	设置重认证时间间隔
end	退出到特权模式
write	保存配置
show dot1x	显示 dot1x 配置

使用 **no dot1x re-authentication** 命令关闭定时重认证功能，使用 **no dot1x timeout re-authperiod** 命令将重认证时间间隔恢复为缺省值。

以下例子是打开定时重认证功能，并设置重认证时间间隔为 1000 秒：

```
Ruijie# configure terminal
Ruijie(config)# dot1x re-authentication
Ruijie(config)# dot1x timeout re-authperiod 1000
```

```
Ruijie(config)# end
Ruijie# show dot1x
802.1X Status:       Disabled
Authentication Mode:  EAP-MD5
Authed User Number:   0
Re-authen Enabled:    Enabled
Re-authen Period:     1000 sec
Quiet Timer Period:   10 sec
Tx Timer Period:      3 sec
Supplicant Timeout:   3 sec
Server Timeout:       5 sec
Re-authen Max:        3 times
Maximum Request:      3 times
Filter Non-RG Supp:   Disabled
Client Oline Probe:   Disabled
Eapol Tag Enable:     Disabled
Authorization Mode:   Disabled
```

若打开重认证，请注意重认证间隔的合理性。要根据具体的网络规模而设置。

23.2.7. 打开/关闭 过滤非我司 supplicant 功能的开关

当选用我司的 supplicant 产品作为 802.1x 认证的客户端时，如果用户同时也使用了其它的一些802.1x 认证客户端(比如打开了 WindowsXP 自带的802.1x 认证功能选项)，则有可能会使认证失败。

这时可以通过打开本功能，将非我司 supplicant 发出的 802.1x 报文过滤掉，来保证 supplicant 的认证不受其它 802.1x 客户端的影响。默认情况下，该功能是关闭的。

在特权模式下，按如下步骤打开、关闭过滤功能：

命令	作用
configure terminal	进入全局配置模式
dot1x private-supplicant-only	打开过滤功能
end	退出到特权模式
write	保存配置
show dot1x	显示 dot1x 配置

以下例子是打开我司 supplicant 功能的开关的配置：

```
Ruijie# configure terminal
Ruijie(config)# dot1x private-supplicant-only
Ruijie(config)# end
```

```
Ruijie# show dot1x
802.1X Status:       enable
Authentication Mode:  eap-md5
Total User Number:    0(exclude dynamic user)
Authed User Number:   0(exclude dynamic user)
Dynamic User Number:  0
Re-authen Enabled:    enable
Re-authen Period:     2 sec
Quiet Timer Period:   10 sec
Tx Timer Period:      3 sec
Supplicant Timeout:   3 sec
Server Timeout:       5 sec
Re-authen Max:        3 times
Maximum Request:      3 times
Private supplicant only:   enable
Client Online Probe:  disable
Eapol Tag Enable:     disable
Authorization Mode:   disable
```

使用 **no dot1x private-supplicant-only** 命令关闭功能。

23.2.8. 改变 QUIET 时间

当用户认证失败时，设备将等待一段时间后，才允许用户再次认证。Quiet Period 的时间长度便是允许再认证的时间间隔。该值的作用是避免设备受恶意攻击。Quiet Period 的默认间隔为 10 秒，

我们可以通过设定较短的 Quiet Period 使用户可以更快地进行再认证。

在特权模式下，按如下步骤设置 Quiet Period 的值

命令	作用
configure terminal	进入全局配置模式
dot1x timeout quiet-period *seconds*	设置 Quiet Period 值
end	退出到特权模式
write	保存配置
show dot1x	显示 dot1x 配置

使用 **no dot1x timeout quiet-period** 命令将 Quiet Period 恢复为缺省值。以下例子是设置 QuietPeriod 值 500 秒：

```
Ruijie# configure terminal
Ruijie (config)# dot1x timeout quiet-period 500
Ruijie(config)# end
```

23.2.9. 设置报文重传间隔

设备发 EAP-request/identity 之后，若在一定的时间内没有收到用户的回应，设备将重传这个报文。该值的默认值为 3 秒，要根据具体的网络规模进行调整。

在特权模式下，按如下步骤设置报文重传间隔

命令	作用
configure terminal	进入全局配置模式
dot1x timeout tx-period *seconds*	设置报文重传间隔
end	退出到特权模式
write	保存配置
show dot1x	显示 dot1x 配置

使用 **no dot1x timeout tx-period** 命令将报文重传间隔恢复为缺省值。以下例子是设置报文重传间隔为 100 秒：

```
Ruijie# configure terminal
Ruijie(config)# dot1x timeout tx-period 100
Ruijie(config)# end
```

23.2.10. 设置最大请求次数

设备在 RadiusServer 发出认证请求后，若在 ServerTimeout 时间内没收到 Radius Server 的回应，将重传该报文。最大请求次数指的是设备重传请求的最大数，超过该次数设备将认为本次认证失败。默认的重传次数为 3 次，我们要根据具体的网络环境进行调整。

在特权模式下，按如下步骤设置报文重传次数

命令	作用
configure terminal	进入全局配置模式
dot1x max-req *count*	设置报文重传次数
end	退出到特权模式
write	保存配置
show dot1x	显示 dot1x 配置

```
Ruijie#show dot1x
```

使用 **no dot1x max-req** 命令将报文重传次数恢复为缺省值。以下例子是设置报文重传次数为 5 次：

```
Ruijie# configure terminal
Ruijie(config)# dot1x max-req 5
Ruijie(config)# end
```

23.2.11. 设置最大重认证次数

当用户认证失败后，设备会尝试再次与用户进行认证。在认证次数超过最大重认证次数之后，设备就认为这个用户已经断线，结束认证过程。系统默认的次数是 3 次，我们可以重新设置这个值。

在特权模式下，按如下步骤设置最大重认证次数：

命令	作用
configure terminal	进入全局配置模式
dot1x reauth-max *count*	设置最大重认证次数
end	退出到特权模式
write	保存配置
show dot1x	显示 dot1x 配置

使用 **no dot1x reauth-max** 命令将最大重认证次数恢复为缺省值。以下例子是设置最大重认证次数为 3 次：

```
Ruijie# configure terminal
Ruijie(config)# dot1x reauth-max 3
Ruijie(config)# end
```

23.2.12. 设置 Server-timeout

该值指的是 Radius Server 的最大响应时间，若在该时间内，设备没有收到 Radius Server 的响应，将认为本次认证失败。

在特权模式下，按如下步骤设置 Server-timeout、恢复为默认值

命令	作用
configure terminal	进入全局配置模式
dot1x timeout server-timeout *seconds*	设置服务器最大响应时间，使用该命令的 no 选项将其恢复为缺省值
end	退出到特权模式
write	保存配置
show dot1x	显示 dot1x 配置

注意:

实际应用中如果选择 radius 作为 802.1X 的网络认证方法，同时又配置了其它方法作为备用方法，比如配置了 aaa authentication dot1x default group radius none 希望在 radius 服务器超时不响应情况下可以通过 none 方法实现免认证，则需要注意 radius 的超时时间和 802.1X 超时时间的关系。

802.1X 的默认超时是 5 秒，而 radius 由于有超时重传，默认就是 3*5，也就是 15 秒超时。显然这种情况下 802.1X 会先出现超时导致认证失败，从而无法达到用户的配置期望。因此实际使用中请注意调整参数，保证：

radius 的每次超时时间 *重传次数 < 802.1X 的 server-timeout。

23.2.13. 配置设备主动发起 802.1x 认证

802.1x 是基于端口的安全访问认证，用户要访问网络，就必须先进行认证，绝大多数情况下，认证是由用户端通过发出 EAPOL-START 报文来发起的。关于认证过程中报文的交互，请参考“认证的发起及认证过程中的报文交互”。

但是在某些特殊情况下，认证却需要由设备来发起。比如设备复位、认证端口状态由 linkdown 变为 linkup，这时候为了保证已认证的用户能够继续使用网络，就需要设备主动发起认证。另外，如果用户使用了一些不会主动发起认证请求的 802.1x 客户端软件来进行认证（比如使用 WindowsXP 自带的 802.1x 客户端软件），这时候就需要设备能够主动发起认证，设备通过发出 EAP-request/identity 组播报文来强制要求认证端口下的所有用户进行认证。

以下将介绍如何配置设备主动发起 802.1x 认证，以及在不同的应用环境下用户应该如何合理地进行配置。

打开/关闭设备主动发起认证的开关

当该功能关闭时，设备只在复位和认证端口状态改变的时候发起一次认证请求，这是为了保证在线用户能够继续认证使用网络，其它任何时候设备都不会主动发起认证请求。当该功能打开后， 用户可以配置主动发起认证请求的次数、发送认证请求的间隔、用户认证通过后是否要停止发送请求等附属功能。

进入特权模式，按以下步骤打开主动认证功能：

命令	作用
configure terminal	进入全局配置模式
dot1x auto-req	打开主动认证功能。该功缺省认情况下是关闭的
end	退出到特权模式

write	保存配置
show dot1x	显示 dot1x 配置

使用该命令的 **no** 选项可以关闭该功能，只有该功能打开的情况下，后面的设置才能起作用，设置设备主动发送认证请求的次数，用户可以设置设备主动发起认证请求的次数，这个值可根据实际的网络环境设定。

进入特权模式，按以下步骤设置发送报文的次数：

命令	作用
configure terminal	进入全局配置模式
dot1x auto-req packet-num *num*	设备主动发送 num 个 802.1x 认证请求报文,如果 num 为 0，则设备将持续地发送该报文。缺省值是 0（无限个）
end	退出到特权模式
write	保存配置
show dot1x auto-req	显示配置

使用该命令的 **no** 选项恢复为默认值，下面配置报文发送间隔

进入特权模式，按以下步骤设置主动发送报文的间隔：

命令	作用
configure terminal	进入全局配置模式
dot1x auto-req req-interval *interval*	设置报文发送间隔
end	退出到特权模式
write	保存配置
show dot1x auto-req	显示配置

使用该命令的 **no** 选项恢复为默认值，由于发出认证请求组播报文会导致认证口下的所有用户进行重认证，所以发送间隔不要太小，否则会影响认证效率。

设置在发现用户认证通过后是否停止发送请求报文，在某些应用需求下(比如一个端口下面只接一个用户)，我们可以指定设备在发现用户认证通过后，停止向对应端口发送认证请求，如果用户下线，则继续发送。

进入特权模式，按以下步骤设置：

命令	作用
configure terminal	进入全局配置模式
dot1x auto-req user-detect	端口有认证用户停止发送报文。该功能缺省打开

end	退出到特权模式
write	保存配置
show dot1x auto-req	显示配置

使用该命令的 **no** 选项关闭该功能，用户在设置该功能时要仔细考虑当前的网络应用环境。

应用示例以上三个命令为用户提供了灵活的应用策略，用户可以根据具体的网络应用环境来选择合适的配置命令。为了方便用户进行配置，我们建立了如下的应用配置表，用户可参考该表来进行配置：

	方案 1	**方案 2**	**方案 3**
用户环境	一端口对任意用户	一端口对单用户	一端口对多用户
是否要求使用我司的 supplicant 作为认证客户端	是	否	否
建议采用的配置命令	不必打开 dot1x auto-req 功能	**dot1x auto-req** **dot1x auto-req packet-num** *num* **dot1x auto-req req-interval** *interval* **dot1x auto-req user-detect**	**dot1x auto-req** **dot1x auto-req packet-num** *0* **dot1x auto-req req-interval** *interval* **no dot1x auto-req user-detect**

23.2.14. 配置 802.1x 记帐

锐捷网络公司的 802.1x 实现了记帐功能。该记帐是基于时长的，也就是说 802.1x 记录了用户第一次认证通过到用户主动退出或设备检测到用户中断的时间长度。

在用户第一次认证通过之后，设备会向服务器发一个记帐开始请求，当用户主动离线或设备检测到用户已离线或用户的物理连接已中断，设备将向服务器发一个记帐结束请求。服务器组将会把这些信息记录在服务器组的数据库上。网管便可以根据这些信息提供记帐的依据。

锐捷网络公司的 802.1x 十分重视记帐的可靠性，为了避免记帐服务器的意外情况，特别支持记帐备份服务器。当一个服务器由于各种原因而不能提供记帐服务，设备将自动把记帐信息转发给另一台备份服务器，这大大提高了记帐可靠性。

在用户主动退出的情形下，记帐的时长是精确的；在用户意外中断的情形下，用户记帐的精度以重认证的间隔为准（设备通过重认证检测一个用户是否意外中

断）。

要打开设备的记帐工作需对设备做如下的设置：

1. 在 Radius Server 注册这台设备为 Radius Client，如认证时的操作
2. 设置记帐服务器的 IP 地址
3. 设置记帐的 UDP 端口
4. 在 802.1x 打开的前提下，打开记帐服务

在特权模式下，按如下步骤设置记帐服务

命令	作用
configure terminal	进入全局配置模式
aaa new-model	打开 AAA 功能
aaa group server radius *gs*	配置记帐服务器组
server *192.168.4.12* **acct-port** *11*	向服务器组添加服务器
exit	退回全局配置模式
aaa accounting network *acct* **start-stop group** *gs*	配置记账方法列表
dot1x accounting *acct*	为 802.1X 应用记账方法列表
end	退出到特权模式
write	保存配置
show running-config	显示配置

使用 **no aaa accounting network** 命令的将删除记账方法列表。使用 **no dot1x accounting** 命令使用默认的 dot1x 记帐方法。以下例子是设置记帐服务器的 IP 地址为 192.168.4.12、设置备份记帐服务器的 IP 地址为 192.168.4.13、设置记帐服务器的 UDP 端口为 1200、应用 802.1x 记帐功能：

```
Ruijie# configure terminal
Ruijie(config)# aaa new-model
Ruijie(config)# aaa group server radius acct-use
Ruijie(config-gs-radius)# server 192.168.4.12 acct-port 1200
Ruijie(config-gs-radius)# server 192.168.4.13 acct-port 1200
Ruijie(config-gs-radius)# exit
Ruijie(config)# aaa accounting network acct-list start-stop
group acct-use
Ruijie(config)# dot1x accounting acct-list
Ruijie(config)# end
Ruijie# write memory
```

```
Ruijie# show running-config
```

注意:

1) 与 Radius Server 的约定记帐密码与认证相同

2) 必须在 AAA 打开的前提下才能打开记帐

3) 802.1X 认证通过后才能进行记账

4) 802.1x 的记帐功能在默认的情形下是关闭的

5) 记帐的数据库格式请见相关的 Radius Server 文档

6) 在基于域名的 AAA 服务开关打开情况下，也即配置命令 **aaa domain enable** 时，**dot1x accounting** 命令选择的记帐方法列表将不会被使用，而使用用户所在的域配置的记账方法列表。具体配置参考“配置基于域名的 AAA 服务”。

同时我们支持计费更新功能 ，在 NAS 设备上设定了计费更新包的周期后，NAS 设备即定时定期的向 Radius Server 发送计费更新包，Radius Server 上可以定义，如果多少次（几个周期）没有收到 NAS 设备发过来的某用户的计费更新包时，即认为该 NAS 或该用户不在线，Radius Server 即可停止相关用户的计费，从在线用户表中将其删除等等操作。

在特权模式下，按如下步骤设置记帐更新功能服务

命令	作用
configure terminal	进入全局配置模式
aaa new-model	打开 AAA 功能
aaa accounting update	设置记帐计费更新功能
end	退出到特权模式
write	保存配置
show running-config	显示配置

用 **no aaa accounting update** 可以关闭记账更新功能服务

```
Ruijie# configure terminal
Ruijie(config)# aaa accounting update
Ruijie(config)# end
Ruijie# write memory
Ruijie# show running-config
```

以下章节为锐捷网络产品特有的功能：

为了方便宽带运营商及其他特殊场合的用途，锐捷对 802.1x 的功能在标准的基

础上进行了扩展（该扩展是完全基于标准之上，没有任何的与 IEEE 802.1x 不兼容）。

23.2.15. 配置 IP 授权模式

锐捷网络实现的 802.1x，可以强制要求已认证的用户使用固定的 IP。管理员通过配置 IP 授权模式来限定用户获得 IP 地址的方式。IP 授权模式有四种：DISABLE 模式、DHCP SERVER 模式、RADIUS SERVER 模式、SUPPLICANT 模式。下面分别介绍这四种工作模式的特性：

DISABLE 模式（默认）：在该模式下，设备不对用户的 IP 做限制，用户只需认证通过便可以使用网络。

DHCP SERVER 模式：用户的 IP 通过指定的 DHCP SERVER 获得，只有指定的 DHCP SERVER 分配的 IP 才是合法的 IP，对于 DHCP 模式可以使用 DHCP relay option82 实现 802.1X 的更为灵活的 IP 分配策略。典型的方案图如下：

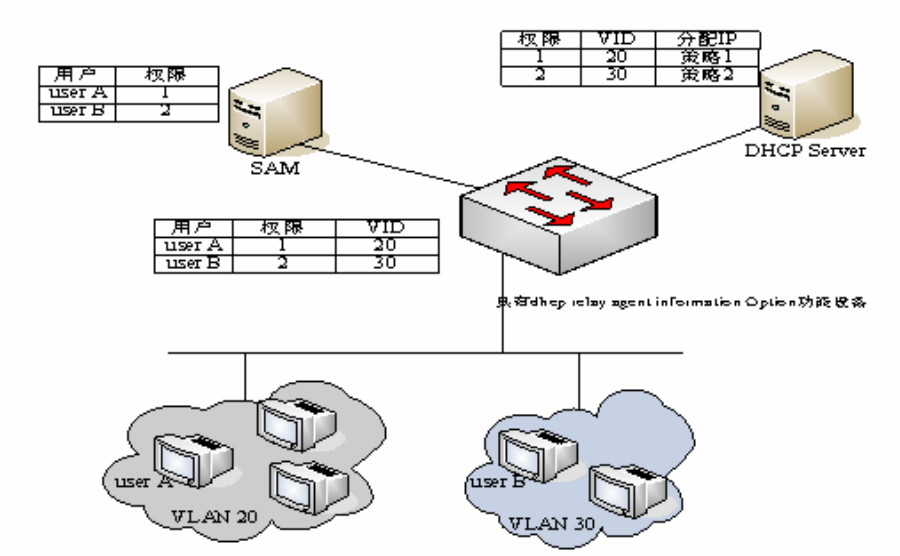


图 5

各用户通过 DHCP Client 发起 IP 请求，具有 dhcp relay option82 的网络设备融合 SAM 服务器上的用户权限，构造 option82 字段封装于 DHCP 请求报文，该 option82 字段由“vid + 权限”组成。DHCP Server 由 option82 字段选择不同的分配策略。

此种模式下需要对 DHCP Relay 及相应的 option82 进行配置，如打开 DHCP relay 功能，并选择 option82 策略，相应的配置见 DHCP Relay 配置指南和命令参考。

RADIUS SERVER 模式：用户的 IP 通过 RADIUS SERVER 指定。用户只能用 RADIUS SERVER 指定的 IP 访问网络。

SUPPLICANT 模式：所绑定用户的 IP 为 SUPPLICANT 认证时 PC 的 IP。认证后，用户只能用该 IP 访问网络，不可随意更改 IP。

四种模式下的应用模型：

- DISABLE 模式：适合不对用户限定 IP 的场合。用户只需通过认证便可以访问网络。
- DHCP SERVER 模式：用户 PC 通过 DHCP 获得 IP 地址，管理员通过配置设备的 DHCP RELAY 来限定用户访问的 DHCP SERVER，这样，只有指定的 DHCP SERVER 分配的 IP 才是合法的。
- RADIUS SERVER 模式：用户 PC 使用固定的 IP，RADIUS SERVER 配置了<用户—IP>的对应关系，并通过 RADIUS 的 Framed-IP-Address 属性告知设备，用户只能用该 IP 才能访问网络。
- SUPPLICANT 模式：用户 PC 使用固定的 IP，SUPPLICANT 将该信息告知设备，用户只能用认证时的 IP 才能访问网络。

注意：

用户切换模式时会导致已经认证的用户全部下线，所以建议在用户使用前就配置好认证模式。

s2352g/s2328g 不支持 dot1x option 82.

在特权模式下，如下配置 IP 授权模式：

命令	作用
configure terminal	进入全局配置模式
aaa new-model	打开 AAA 功能
aaa authorization ip-auth-mode {disabled | dhcp-server | radius-server | supplicant }	配置 IP 授权模式
end	退出到特权模式
write	保存配置
show running-config	显示配置

以下例子是把配置 IP 授权模式为 RADIUS-SERVER 模式：

```
Ruijie# configure terminal
Ruijie(config)# aaa authorization ip-auth-mode radius-serve
r
Ruijie(config)# end
Ruijie# show running-config
!
aaa new-model
!
aaa authorization ip-auth-mode radius-server
```

```
!
Ruijie# write memory
```

23.2.16. 发布广告信息

锐捷网络实现的 802.1x，可以在 Radius Server 端配置 Reply-Message 字段，当认证成功后，该字段的信息可以在锐捷网络推出的 802.1x 客户端 Star-Supplicant 上显示出来，便于运营商发布一些信息。

该消息只有在用户第一次认证时显示，重认证时不会显示，这样就避免了对用户的频繁打扰。

广告信息的显示窗口支持 HTML，会自动把消息中的 http://XXX.XXX.XX 转换成可直接跳转的连接，便于用户查看详细的信息。

广告信息的发布：

1) 运行商在 Radius Server 端，配置 Reply Message 属性的内容

2) 只有锐捷的客户端 Ruijie-supplicant 才支持（对本公司设备的用户免费），其它的客户端看不到信息但不影响使用

3) 在设备端无需设置

23.2.17. 某端口下的可认证主机列表

为了增强 802.1x 的安全性，我们在不影响 IEEE 802.1x 的基础上进行了扩展，网管可以限定某个端口的认证的主机列表。如果一个端口下的可认证主机列表为空，则任何用户均可认证；若可认证主机列表不为空，那么只有列表中的主机允许认证。允许认证的主机用 MAC 标识。

添加某一端口下的可认证主机、删除某一端口下的可认证主机

命令	作用
configure terminal	进入全局配置模式
dot1x auth-address-table address *mac-addr* **interface** *interface*	设置可认证主机列表
end	退出到特权模式
write	保存配置
show running-config	显示配置

注意：

若主机列表为空，该端口允许任何主机认证。

23.2.18. 授权

为了方便运营商，我司的产品可以对不同类型的用户提供不同质量的服务，如：提供给用户的最大带宽不同。而这些信息集中于 Radius Server 上，管理员不必对每台设备进行配置。

由于 Radius 没有标准的属性来表示最大数据率。我们只能通过厂商自定义属性来传递授权信息。

定义的通用格式如下：

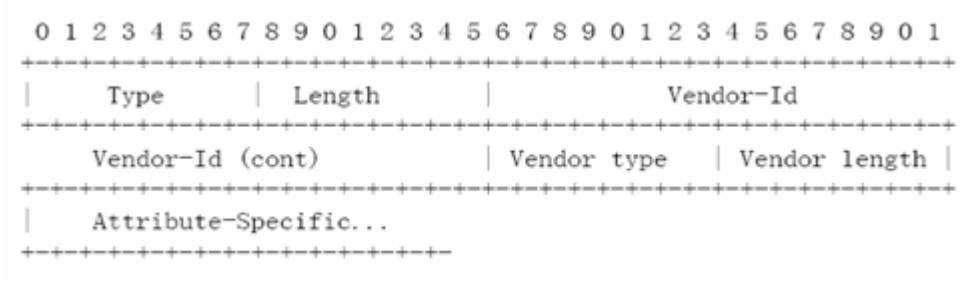


图 6

对于最大数据率应填的值如下：

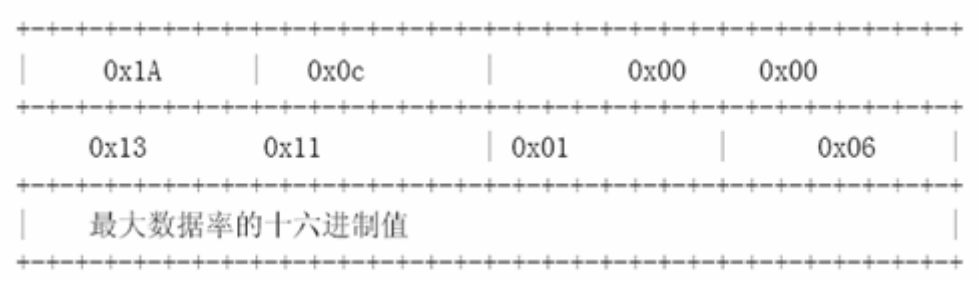


图 7

最大数据率的单位：kbps

对于最大数据率为 10M 的用户应填如下：

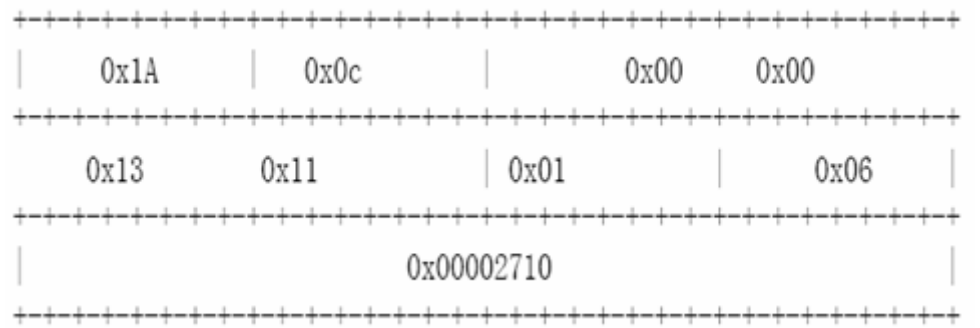


图 8

自定义的头按照以上格式填，最大数据率为 10M，即 10000kbsp，转换成 16 进制则 0x00002710，填在相应的字段上即可。

该功能无须设置设备端。只要设备端支持授权便可。

23.2.19. 配置认证方式

在标准中，802.1x 是通过 EAP-MD5 进行认证。锐捷网络科技公司实现的 802.1X，不但可以通过 EAP-MD5 方式认证（默认），还可以采用 CHAP 和 PAP 方式认证。采用 CHAP 的好处是可以减少一次设备与 RADIUS SERVER 的通讯，减轻 RADIUS SERVER 的压力。和 CHAP 方式一样，PAP 和 RADIUS SERVER 间的通讯也只有一次，虽然 PAP 认证方式由于其在安全方面存在很大缺陷，所以不建议使用，但是在某些情况下还是可以满足用户的特殊需求，比如当用户使用的安全服务器只支持 PAP 认证模式时，选择 PAP 认证模式就能够充分地利用现有的资源，保护用户的投资。

在特权模式下，按如下步骤设置 802.1x 的认证方式：

命令	作用
configure terminal	进入全局配置模式
dot1x auth-mode mode	配置认证模式
end	退出到特权模式
write	保存配置
show dot1x	显示配置

以下例子是配置成 CHAP 模式的例子：

```
Ruijie# configure terminal
Ruijie (config)# dot1x auth-mode CHAP
Ruijie(config)# end
Ruijie# show dot1x
802.1X Status:       Disabled
Authentication Mode:  CHAP
Authed User Number:   0
Re-authen Enabled:    Disabled
Re-authen Period:     3600 sec
Quiet Timer Period:   10 sec
Tx Timer Period:      3 sec
Supplicant Timeout:   3 sec
Server Timeout:       5 sec
Re-authen Max:        3 times
Maximum Request:      3 times
```

```
Filter Non-RG Supp:   Disabled
Client Oline Probe:   Disabled
Eapol Tag Enable:     Disabled
Authorization Mode:   Group Server
```

23.2.20. 配置备份认证服务器

我司基于 802.1x 的认证系统，可以支持备份服务器。当主服务器因各种原因当机之后，设备将自动向方法列表服务器组下一个服务器提交认证请求。当配置多个服务器时，第一个配置的服务器就是主服务器，后面配置的都是备份服务器。

在特权模式下，按如下方式设置备份认证服务器。

命令	作用
configure terminal	进入全局配置模式
aaa new-model	打开 aaa 开关
aaa group server radius *gs-name*	配置服务器组
server *sever*	配置服务器
end	退出到特权模式
write	保存配置
show dot1x	显示配置

以下例子是配置 192.168.4.12 为备份服务器的例子：

```
Ruijie# configure terminal
Ruijie# aaa new-model
Ruijie(config)# aaa group server radius auth-ll
Ruijie(config-gs-radius)# server 192.168.4.1
Ruijie(config-gs-radius)# server 192.168.4.12
Ruijie(config-gs-radius)# end
Ruijie#
```

23.2.21. 对在线用户的配置及管理

锐捷设备提供了通过 SNMP 对已认证用户进行管理的功能。管理员可以通过 SNMP 查看已认证用户的信息，还可以强制使一个用户下线。被强制下线的用户必须再次认证才能使用网络资源。

该功能无需配置设备。

23.2.22. 实现用户与 IP 的捆绑

用锐捷网络公司提供的客户端，以及对 Radius Server 的正确配置，可以实现用户与 IP 的唯一绑定。某个用户必须以管理员分配的 IP 进行认证，否则将不能认证成功。

该功能无需配置设备，用户需用锐捷网络公司提供的客户端软件，管理员需配置 Radius Server。

23.2.23. 基于端口的流量记费

锐捷网络设备除了提供针对时长的记费外，在设备的每个端口只接入一个用户的情形下，设备还可以提供针对流量的记费功能。

该功能无需配置设备，但需 Radius server 支持。

23.2.24. 配置 802.1X 端口动态 VLAN 自动跳转

动态 VLAN 自动跳转功能需要在远端 RADIUS 服务器上设置针对用户的下传 VLAN 属性，RADIUS 服务器通过相应定义的 RADIUS 属性封装下传 VLAN 信息。接入认证设备收到封装在 RADIUs 报文中的下传 vlan 信息，并在用户认证通过后自动把通过该用户认证的端口加入到下传 VLAN 中。

通过 **show dot1x summary** 命令可在接入认证设备端验证认证端口所接入的真实 VLAN。通过 **show dot1x user id** 命令可查看 RADIUS 服务器下传 VLAN 信息。

锐捷网络产品可通过锐捷私有 RADIUS 属性及 RADIUS 标准属性两种方式封装下传 VLAN 信息。

RADIUS 服务器使用锐捷私有属性封装下传 VLAN 信息时，服务器将私有属性封装在 26 号 RADIUS 标准属性中，私有厂商 ID 为十六进制数 0x00001311，默认情况下该私有属性类型号为 4。可通过命令 **radius attribute 4 vendor-type** *type* 设置在接入设备上可的下传 vlan 私有属性类型。配置命令可参见“配置 RADIUS”。

锐捷网络产品同时支持 RADIUS 服务器使用 RADIUS 标准属性封装下传 VLAN 信息，包括以下属性组合：

64 号属性 Tunnel-Type

65 号属性 Tunnel-Medium-Type

81 号属性 Tunnel-Private-Group-ID

分别取值如下：

Tunnel-Type=VLAN (13)

Tunnel-Medium-Type=802（6）

Tunnel-Private-Group-ID=VLANID(封装为字符串)

接入认证设备接收到下传 VLAN 属性后，先将下传 VLAN 属性作为 VLAN 名称，查找接入认证设备上配置的相同名称的VLAN，若存在相同名称的VLAN，认证端口自动跳转至该 VLAN；若不存在相同名称的 VLAN，则将下传 VLAN 属性作为 VLAN ID，若 Tunnel-Private-Group-ID 属性封装的 vlan ID 字符串合法（在接入认证设备支持的VLAN ID 范围内），认证端口自动跳转至该VLAN，否则认证失败。

锐捷网络产品支持在 ACCESS 和 TRUNK 端口模式下的启用 802.1X 认证，包括如下 VLAN 自动跳转模式：

1，ACCESS 模式认证端口下的 VLAN 自动跳转

在接入认证设备上未配置下传 VLAN 信息时，若下传 VLAN 属性设置为 VLAN ID，接入认证设备可创建相应 VLAN，并使认证端口跳转到该 VLAN 中；若下传 VLAN 属性指定为 VLAN 名称，认证将无法通过。

在接入认证设备上配置下传 VLAN 后，若该 vlan 在接入认证设备上被设置为私有 VLAN 或 Super VLAN，则认证端口下的用户将无法通过认证；

2，TRUNK 的端口模式下的 Native VLAN 自动跳转

由于 TRUNK 端口同时属于多个 VLAN，因此 trunk 端口实现的是 Native vlan 的自动跳转。在设接入认证设备上配置下传 vlan 后，若下传 VLAN 属性指定为 VLAN ID，可认证端口的 Native VLAN 将跳转到下传 VLAN；若下传 VLAN 属性指定为 VLAN 名称，端口下用户将无法通过认证。

在接入认证设备上配置下传 VLAN 后，若该 vlan 在接入认证设备上被设置为私有 VLAN 或 Super VLAN，则认证端口下的用户将无法通过认证；

可以通过以下步骤设置启用端口 vlan 自动跳转：

1，启用 AAA 服务

命令	作用
configure terminal	进入全局配置模式
aaa new-model	启用 AAA 服务

有关 AAA 的配置具体参见“配置 AAA”章节。

2，配置 RADIUS 服务器相关信息

命令	作用
configure terminal	进入全局配置模式
radius-server host *host-ip*	配置 RADIUS 服务器 IP 地址
radius-server key *text*	配置接入认证设备与 RADIUS 服务器之间通信时使用的共享密钥

有关 AAA 的配置具体参见“配置 AAA”章节。

3，配置方法列表

命令	作用
configure terminal	进入全局配置模式
aaa authentication dot1x *list1* **group radius**	配置 AAA dot1x 认证方法列表 list1
aaa accounting network *list2* **start-stop group radius**	配置 AAA 记账方法列表 list2

有关 AAA 的配置具体参见“配置 AAA”章节。

4，选择 802.1X AAA 服务方法列表

命令	作用
configure terminal	进入全局配置模式
dot1x authentication *list1*	选择已预先配置 dot1x 认证方法列表 list1
dot1x accounting *list2*	选择已预先配置的 dot1x 记账方法列表 list2

5，在接口模式下使能 802.1X 认证

命令	作用
configure terminal	进入全局配置模式
interface *interface_id*	进入接口配置模式 *i*
dot1x port-control auto	使能 802.1X 认证

6，在接口模式下启用 VLAN 自动跳转功能

命令	作用
configure terminal	进入全局配置模式
interface *interface_id*	进入接口配置模式
dot1x dynamic-vlan enable	启用 VLAN 自动跳转功能

注意:

相应接入认证端未启用 VLAN 自动跳转功能时，接入认证设备将忽略封装在 RADIUS 报文中的下传 VLAN 属性

7，查看动态 VLAN 自动跳转信息

可以通过下列命令查看动态 VLAN 自动跳转相关信息

命令	作用
show dot1x user id *session_id*	查看会话号为 *session_id* 的用户相关信息，包括动态 VLAN 自动跳转信息。
show dot1x summary	查看接入认证端口所在真实 VLAN

有关的注意事项请参见“配置 802.1X 其他注意事项”章节。

23.2.25. 代理服务器屏蔽和拨号屏蔽

用户自行架设代理服务器以及用户认证后再自行拨号上网，这是网络安全最大的两个隐患。锐捷网络设备提供代理服务器屏蔽和拨号屏蔽功能。

实现该功能设备端不需任何设置，只需在 RADIUS 服务器端配置相应的属性。由于 Radius 没有标准的属性来表示最大数据率，我们只能通过厂商自定义属性来传递授权信息。我们定义的通用格式见授权一节的说明。

代理服务器屏蔽功能定义的 Vendor Type 为 0x20，拨号屏蔽功能定义的 Vendor Type 为 0x21。

Attribute-Specific 字段为四个字节的厂商自定义属性，定义了对使用代理服务器上网和拨号上网行为所采取的动作. 0x0000 表示正常连接，不进行检测屏蔽，0x0001 表示进行检测屏蔽。

若要屏蔽通过代理服务器上网，用户应填如下信息：

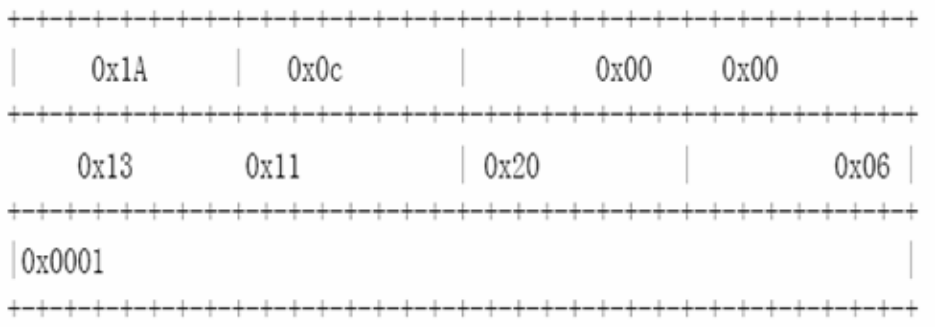


图 9

若要屏蔽通过拨号上网，用户应填如下信息：

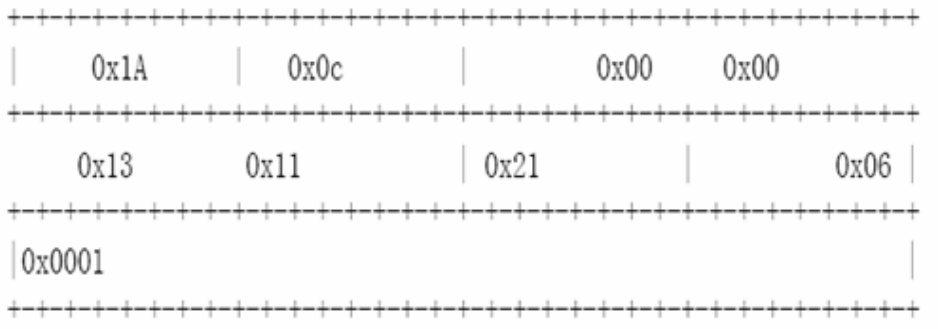


图 10

23.2.26. 配置客户端在线探测

为了保证计费的准确性，需要一种在线探测机制能够在短时间内获知用户是否在线。在标准实现中的重认证机制能够满足这种需求，但是标准实现中需要 RADIUS 服务器的参与，要实现准确的探测用户是否在线将会占用设备和 RADIUS 服务器的大量资源。为了满足在占用少量资源的基础上实现计费的准确性，我们采用了一种新的客户端在线探测机制。这种机制只需要在设备和客户端之间交互，并且对网络流量的占用极小，能够实现分钟级的计费精度(用户可以通过配置来确定计费的精度)。

注意:

实现客户端在线监测需要客户端软件支持这一功能。

以下两个定时器影响到在线探测的性能和精度：

- Hello Interval: 客户端定时发送通告的间隔。
- Alive Interval：客户端在线间隔。设备在此间隔期间没有收到客户端的通告，将主动断开同客户端连接，并通知计费服务器。该值必须大于 Hello Interval。

在特权模式下，我们可以按以下方式配置客户端在线探测功能:

命令	作用
configure terminal	进入全局配置模式
dot1x client-probe enable	打开客户端在线探测功能
dot1x probe-timer interval *interval*	配置 Hello Interval
dot1x probe-timer alive interval	配置设备的 Alive Interval
end	退出到特权模式

write	保存配置
show dot1x	显示配置

23.2.27. 配置 EAPOL 帧带 TAG 的选项开关

IEEE 802.1x 约定 EAPOL 报文不能加 VLAN TAG，但基于可能的应用需求，我们提供了相应的选项开关，在打开相应开关时，能根据 Trunk Port 的相应输出规则输出 TAG。

典型的应用环境就是在汇聚层打开 802.1x 认证，参见“典型应用的拓扑结构”。

在特权模式下，我们可以按以下方式配置 EAPOL 帧带 TAG 的选项开关。

命令	作用
configure terminal	进入全局配置模式
dot1x eapol-tag	打开 EAPOL 帧带 TAG 的功能。缺省该功能是关闭的
end	退出到特权模式
write	保存配置
show dot1x	显示配置

您可以用 **no dot1x eapol-tag** 命令来关闭该功能。

23.2.28. 配置基于端口的用户认证

802.1x 对用户的控制默认情况下是基于用户 MAC 进行控制的，只用通过认证的用户才能使用网络，而对于其他接在同一端口的用户无法使用网络，而基于端口的控制模式及表示当某一端口有一个用户认证通过时，此端口就变成已认证端口，所有接在此端口下的用户都能够正常的使用网络。

要配置端口的控制模式为基于端口的控制模式，从特权模式开始，按步骤进行以下设置。

命令	作用
configure terminal	进入全局配置模式
interface <*interface-id*>	进入接口模式
dot1x port-control auto	打开受控功能
dot1x port-control-mode {*mac-based*|*port-based*}	选择受控的模式

End	退出到特权模式
Write	保存配置
show dot1x port-control	显示端口 802.1X 配置

您可以用 **no dot1x port-control-mode** 命令来恢复默认受控方式。

下面的例子显示了如何配置端口的认证模式

```
Ruijie#configure terminal
Ruijie(config)# dot1x port-control-mode port-base
```

注意:

基于端口的认证模式下，每个端口只能接一个认证用户

对于基于端口的认证方式下，可以允许或禁止动态用户在多个认证端口之间迁移，默认情况是允许动态用户在不同端口之间迁移，如要禁止动态用户的迁移，从特权模式开始，按步骤进行以下设置。

命令	作用
configure terminal	进入全局配置模式
dot1x stationarity enable	禁止端口间的迁移
end	退到特权模式
Write	保存配置

23.2.29. 配置端口允许的最大用户数量

可以配置端口的最大用户数量来限制该端口实际可访问网络的用户数。端口在基于 MAC 认证模式时，该值表示该端口可认证的最大用户数量，当端口的实际认证用户数达到该值时，新的用户将无法通过认证；在基于端口认证模式时，该值表示该端口被授权后允许的最大动态用户数量，当端口的动态用户数达到该值后，该端口将不会允许新的动态用户访问网络。

要配置端口允许的最大用户数量，从特权模式开始，按步骤进行以下设置。

命令	作用
configure terminal	进入全局配置模式
interface <*interface-id*>	进入接口模式

dot1x port-control auto	打开受控功能
dot1x default-user-limit *<1-4000>*	设置端口允许的最大用户数
End	退出到特权模式
Write	保存配置
show dot1x port-control	显示端口 802.1X 配置

您可以用 **no dot1x default-user-limit** 命令来恢复默认端口限制用户数。

下面的例子显示了如何配置端口的限制用户数

```
Ruijie#configure terminal
Ruijie(config)# dot1x default-user-limit 20
```

23.3. 查看 802.1x 的配置及当前的统计值

本公司实现的 802.1X 可以查看丰富的状态机信息，为网管提供了强有力的管理依据，便于管理员对用户状态的时时监控，且方便解决故障。

- 查看 Radius 认证及记帐相关配置
- 查看当前的用户数
- 查看可认证地址列表
- 查看用户认证状态信息
- 查看 1X 客户端探测定时器设置

23.3.1. 查看 Radius 认证及记帐相关配置

用 **show radius server** 命令查看 Radius Server 的相关配置，用 **show aaa user** 查看用户相关信息

```
Ruijie# sh radius server
Server IP:       192.168.5.11
Accounting Port:  1813
Authen  Port:    1812
Server State:     Ready
```

23.3.2. 查看当前的用户数

本公司实现的 802.1X 可以查看两类当前的用户数，一是当前用户数，二是已认证用户数。当前用户数指的是当前认证用户总数（无论是否认证成功）；已认证用

户数，指的是已认证通过的用户的总数。

在特权模式下，查看当前用户数及已认证用户数，查看 1x 配置，包括当前用户数和已认证用户数使用 **show dot1x**。

以下例子是查看 802.1x 配置：

```
Ruijie# show dot1x
802.1X Status:       Disabled
Authentication Mode:  EAP-MD5
Authed User Number:   0
Re-authen Enabled:    Disabled
Re-authen Period:     3600 sec
Quiet Timer Period:   10 sec
Tx Timer Period:      3 sec
Supplicant Timeout:   3 sec
Server Timeout:       5 sec
Re-authen Max:        3 times
Maximum Request:      3 times
Filter Non-RG Supp:   Disabled
Client Oline Probe:   Disabled
Eapol Tag Enable:     Disabled
Authorization Mode:   Disabled
```

23.3.3. 查看可认证地址列表

本公司实现的 802.1x，对功能进行了扩展，可以设置在某些端口上只有哪些主机可以认证。查看可认证主机列表功能，可以让管理员查看目前已有的设置。

在特权模式下，按如下操作查看可认证主机列表

命令	作用
configure terminal	进入全局配置模式
dot1x auth-address-table address *mac-addr* **interface** *interface*	配置可认证主机列表
end	退出到特权模式
write	保存配置
show dot1x auth-address-table	查看可认证主机列表

使用 **no dot1x auth-address-table address** 命令删除指定的可认证主机列表。以下例子是查看可认证主机列表：

```
Ruijie# show dot1x auth-address-table
interface:g3/1
----------------------------------
mac addr: 00D0.F800.0001
```

23.3.4. 查看用户认证状态信息

管理员可以查看本设备的当前用户的认证状态，便于排解故障。

在特权模式下，按如下操作查看用户认证状态信息

命令	作用
show dot1x summary	查看用户认证状态信息

以下例子是查看用户认证状态信息：

```
Ruijie# show dot1x summary
ID   MAC          Interface  VLAN  Auth-State  Backend-State
Port-Status
---- ------------ --------- ----  ----------  ------------
1    00d0f8000001  Gi3/1         1    Authenticated   IDLE
Authed
```

23.3.5. 查看 1x 客户端探测定时器设置

在特权模式下，按如下操作查看 1x 定时器设置

命令	作用
show dot1x probe-timer	查看 1x 定时器设置

以下例子是查看 1x 定时器设置:

```
Ruijie# show dot1x probe-timer
Hello Interval: 20 Seconds
Hello Alive: 250 Seconds
```

23.3.6. 配置 802.1x 其它注意事项

1. 1X 和 ACL 同时应用

在非 IP 授权模式下，如果您打开某一个端口的 802.1x 认证功能，又将某一个 ACL 关联到某一个接口。则 ACL 在 MAC 地址的基础上生效。也就是说，只有源 MAC 为认证通过的用户 MAC 的报文才会经过 ACL 过滤，其它源 MAC 地址报文被丢弃，ACL 只能在该 MAC 地址的基础上进行限制。

比如，认证通过的 MAC 地址为 00d0.f800.0001，则所有源 MAC 为 00d0.f800.0001 的报文可以交换。如果该端口再关联 ACL，则 ACL 在这些能够交换的报文基础上将进一步过滤。如拒绝源 MAC 为该地址的 ICMP 报文。

在 IP 授权模式下，建议不要在受控口上设置 ACL，因为 ACL 优先级比认证用户高，认证通过的 IP+MAC 的绑定不会生效。某个端口认证通过两个用户：

用户 1： mac: 00d0.f800.0001 ip: 192.168.65.100

用户 2： mac: 00d0.f800.0002 ip: 192.168.65.101

然后在该端口上设置一个 ACL，如下：

ip access-list extended ip_acl:

deny icmp any any

原来的目的是为了允许认证用户通讯，且同时禁止发送 ICMP 报文。但 ACL 优先级比认证通过的 IP + MAC 高，该 ACL 的最后一条缺省 ACE 是 **deny any any**，所以认证通过的用户也无法通讯。

如果在 IP_acl 后面加一条 **permit any any**，则所有认证通过的用户任意修改 IP 后仍然可以通讯，但达不到 IP + MAC 一一绑定的目的。所以建议您不要使用 IP 授权 ＋ ACL 的模式

2. 由于 IP 授权模式下认证用户使用的硬件表项和其它运用（如 ACL、端口 IP 安全地址）共享过滤表项和过滤域模板，如果其它应用将硬件资源耗尽，则可能出现 IP 授权模式下用户认证不成功，或者成功但是无法通讯的问题。特别是过滤域模板，IP 授权模式下用户认证必须保证至少有一个模板可以使用。

3. 对认证端口上有用户进行认证或有已经认证成功用户情况下的限制说明

- 端口模式不能修改，例如使用命令 **switchport mode trunk**
- 端口在 ACCESS 模式下不能修改端口 Access VLAN
- 端口在 TRUNK 模式下不能修改端口 Allowed VLAN 及 Native VLAN

4. 在 VLAN 中有用户正在进行认证或有已经认证成功用户情况下的限制说明

- VLAN 不能删除
- VLAN 的类型不能修改，例如使用命令 private-vlan primary。

5. 对同一认证端口下多个用户认证情况的限制说明

- 第一个用户没有下发 VLAN，使用端口缺省 VLAN 作为第一个用户的下发 VLAN；
- 后续认证用户没有下发 VLAN，使用第一个用户下发 VLAN；
- 后续认证用户下发的 VLAN 必须同第一个用户一致，否则无法通过认证；
- 第 一个用户重认证后下发 VLAN 必须与该用户上次认证通过时下发 VLAN 相同，否则无法通过认证。

6. 由于 VLAN 跳转功能是 802.1X 认证通过后将整个端口切换到另外一个 VLAN 进行通信，因此该功能最适宜的部署场景是 802.1X 认证口下连单个用户或者 802.1X 受控口部署为端口模式。该功能会影响 WEB 认证部署,因此动态 VLAN 跳转不要和 WEB 认证在同一个端口上同时部署。

7. 开启 802.1X 认证的同时，如果也部署了 802.1X 的 IP 授权功能、或者部署了 GSN 方案、或者部署客户端自动获取功能、或者部署了安全通道功能，由于静态地址仅仅是免认证的，所以即便用户配置了静态地址，该地址也无法通信。可以

通过配置全局的 IP+MAC 绑定实现静态地址的通信。如果没有部署上述方案，仅配置静态地址和 802.1X 认证功能，则该静态地址可以在 802.1X 受控口上通信。

23.4. 配置自动获取客户端

在实际部署 802.1x 过程中 IT 实施人员往往因为客户端（锐捷的 Supplicant 软件，以下简称 SU）的部署工作量太大而感到头痛。而通过自动获取客户端的解决方案的推出，使得 IT 人员能够对客户端进行快速部署，省时省力省心，提高了工作效率。

自动获取 SU 客户端功能的原理是，当未认证用户通过浏览器访问网路资源时，会被自动重定向到下载服务器页面上，这样就可以下载客户端软件，轻松解决客户端部署难的问题。

我们将通过以下章节详细说明如何配置自动获取 SU 客户端：

- 设置全局客户端下载功能开关
- 设置 HTTP 重定向地址
- 设置重定向的 HTTP 端口
- 设置客户端下载服务器页面的主页地址
- 设置每个未认证用户的最大 HTTP 会话数
- 设置维持重定向连接的超时时间
- 设置免认证的网络资源范围

注意：

客户端自动获取方案使用限制：

- 受接入设备硬件容量影响，打开 tag-support 功能（S23 系列交换机 ARP CHECK 功能独有的命令）或 IPv6 ACL 功能后，客户端自动获取功能将无法启用；
- 开启客户端自动获取功能，将导致 802.1x 受控口下的 ACL 设置失效；
- 不能与全局的 IP 和 MAC 地址绑定功能共用，如果打开全局的 IP 和 MAC 地址绑定，则无法重定向，客户端自动获取功能失效；

23.4.1. 设置全局客户端下载功能开关

要成功应用自动获取客户端功能，必须打开全局的客户端下载功能的开关。缺省情况下，全局客户端下载功能是关闭的。若要开启客户端下载功能，请按如下的步骤：

命令	作用
configure terminal	进入全局配置模式
dot1x redirect	配置全局的客户端下载功能
end	退出到特权模式
write	保存配置

注意：

如果在开启客户端下载功能之前，已经开启了 802.1x 认证功能，则在开启客户端下载功能开关后，将导致所有的 802.1x 用户下线，需要重新认证才能上线。

使用 **no dot1x redirect** 命令将关闭全局客户端下载功能。以下例子是设置打开全局自动获取客户端客户端功能：

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# dot1x redirect
```

23.4.2. 设置 HTTP 重定向地址

要成功应用自动获取客户端功能，必须设置 HTTP 重定向的 IP 地址。当接入设备发现未认证用户试图通过 HTTP 访问网络资源时，接入设备将用户的访问请求重定向到客户端下载页面，通过下载页面，引导用户下载客户端，安装并进行认证。

一般情况下，客户端下载页面是下载服务器所提供的，因此 HTTP 重定向的地址就应该是下载服务器的地址。设置了这个 HTTP 重定向地址以后，这个地址将被设置为一个特殊的免认证的网络资源，未认证用户可以直接与这个地址进行 HTTP 通讯。

缺省情况下，没有设置 HTTP 重定向的 IP 地址。若要设置 HTTP 重定向的 IP 地址，请按如下的步骤：

命令	作用

configure terminal	进入全局配置模式
http redirect *ip-address*	设置 HTTP 重定向地址
show http redirect	查看 HTTP 重定向的配置
end	退出到特权模式
write	保存配置

使用 **no http redirect** 命令将清除 HTTP 重定向地址信息。以下例子是设置服务器的 IP 地址为 176.10.0.1：

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# http redirect 176.10.0.1
Ruijie(config)# show http redirect
```

23.4.3. 设置重定向的 HTTP 端口

当用户访问网络资源时（例如使用浏览器上网），此时用户会发出 HTTP 报文，接入设备通过拦截来自用户的 HTTP 报文，来判断用户是否在访问网络资源。当接入设备检测到未认证的用户在访问网络资源时，将阻止用户访问网络资源，并向用户弹出客户端下载页面。

缺省情况下，接入设备通过拦截用户发出的端口号为 80 的 HTTP 报文，来检测用户是否在访问网络资源。

要新增接入设备拦截用户发出的特定端口号的 HTTP 报文，请按照如下步骤：

命令	作用
configure terminal	进入全局配置模式
http redirect port *port-num*	设置对用户发出的特定目的端口号的 HTTP 请求进行重定向。最大允许配置 10 个不同的目的端口号，端口号 80 也含在该总数量范围内
show http redirect	查看 HTTP 重定向的配置
end	退出到特权模式
write	保存配置

使用 **no http redirect port** *port-num* 命令将删除对用户发出的特定目的端口号的 HTTP 请求进行重定向。以下例子是设置对用户发出的特定目的端口号为 8080 的 HTTP 请求进行重定向：

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

```
Ruijie(config)# show http redirect
```

23.4.4. 设置客户端下载服务器页面的主页地址

在启动自动获取客户端功能前，必须先配置客户端下载服务页面的主页地址。当未认证用户在进行网络访问时，将向用户弹出这个页面的信息，用户通过这个页面进行客户端的下载。

缺省时，没有设置客户端下载服务页面的主页地址。设置客户端下载服务页面的主页地址，请按照如下的步骤：

命令	作用
configure terminal	进入全局配置模式
http redirect homepage *url-string*	设置客户端下载服务页面的主页地址为 *url-string*，必须以“http://”或“https://”开头，不区分大小写；最大长度为 255 个字符
show http redirect	查看 HTTP 重定向的配置
end	退出到特权模式
write	保存配置

使用 **no http redirect homepage** 命令将清除客户端下载页面的主页地址。以下例子是设置认证页面的主页为 http://www.su-download.net/：

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# http redirect homepage
http://www.su-download.net/
Ruijie(config)# show http redirect
```

23.4.5. 设置每个未认证用户的最大 HTTP 会话数

未认证的用户在访问网络资源时，用户 PC 会发出 HTTP 会话连接请求，HTTP 报文会被接入设备拦截，并要求用户进行 Web 认证。为了防止未认证用户发起 HTTP 攻击，而导致接入设备的 TCP 连接耗尽，需要在接入设备上限制未认证用户的最大 HTTP 会话数。

由于用户在认证时，会占用一个 HTTP 会话，而用户的其他应用程序也可能占用着 HTTP 会话，因而不建议设置未认证用户的最大 HTTP 会话数为 1。缺省情况下，未认证用户的最大 HTTP 会话数为 3。

要更改未认证用户的最大 HTTP 会话数，请按照如下步骤：

命令	作用
configure terminal	进入全局配置模式
http redirect session-limit *session-num*	设置每个未认证的最大 HTTP 会话数为 *session-num*，取值范围 1-10
show http redirect	查看 HTTP 重定向的配置
end	退出到特权模式
write	保存配置

使用 **no http redirect session-limit** 命令将恢复未认证用户的最大 HTTP 会话数为 3。以下例子是设置未认证用户的最大 HTTP 会话数为 4：

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# http redirect session-limit 4
Ruijie(config)# show http redirect
```

23.4.6. 设置维持重定向连接超时时间

设置维持重定向连接的超时时间。因为未认证的用户通过 HTTP 访问网络资源时，其 TCP 连接请求将被拦截，实际上是与接入设备建立起 TCP 连接。在连接建立后，接入设备需要等待用户发出的 HTTP 的 GET/HEAD 报文，然后回复 HTTP 重定向报文后才能关闭连接。设置这个限制可以防止用户不发 GET/HEAD 报文，而又长时间占用 TCP 连接。缺省情况下，维持重定向连接的超时时间为 3 秒。

要更改维持重定向连接的超时时间，请按照如下步骤：

命令	作用
configure terminal	进入全局配置模式
http redirect timeout *seconds*	设置维持重定向连接的超时时间； *seconds*，取值范围 1-10
show http redirect	查看 HTTP 重定向的配置
end	退出到特权模式
write	保存配置

使用 **no http redirect timeout** 命令将恢复维持重定向连接超时时间为 3 秒。以下例子是设置维持重定向连接的超时时间为 4 秒：

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# http redirect timeout 4
```

```
Ruijie(config)# show http redirect
```

23.4.7. 设置免认证的网络资源范围

在端口上开启 802.1x 认证后，未认证用户需先使用客户端进行认证，才能访问网络资源。如果允许未认证用户，也可以访问一些免认证的网络资源，需要使用此命令设置免认证的网络资源。设置了免认证的网络资源，如果某网站属于免认证的网络资源，那么所有用户（包括未认证用户）都可以访问该网站。缺省情况下，没有设置免认证的网络资源，未认证用户不能访问网络资源。

要设置免认证的网络资源，请按照如下步骤：

命令	作用
configure terminal	进入全局配置模式
http redirect direct-site *ip-address* [*ip-mask*] [**arp**]	设置免认证的网络资源，最大允许配置 50 个。 如果接入设备启用了 ARP CHECK 功能，那么需要对免认证的网络资源范围进行 ARP 绑定，需要配置 **arp** 关键字
show http redirect	查看 HTTP 重定向的配置
end	退出到特权模式
write	保存配置

说明：

设置免认证的网络资源不能超过 50 个。此外，实际可用数量也会受其它安全功能占用表项的影响而减少。因此，如果需要设置的地址较多，请尽量使用 IP 地址+掩码的方式进行设置。

对于开启 ARP Check 情况，需要将二层交换机下联 PC 的网关设置为免认证的网络资源。

注意：

设置免认证的网络资源功能，只有在打开全局客户端下载功能后，在 802.1x 受控口上生效。

该功能不受 GSN、ACL 设置影响，即无法使用 GSN 阻断或使用 ACL 过滤该免认证的 IP 地址。

使用 **no http redirect direct-site** *ip-address*［i*p-mask*］［**arp**］命令将取消设置免认证的网络资源。以下例子是设置校园网内某免费网址 172.16.x.x 为免认证的网络资源：

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# http redirect direct-site 172.16.0.0 255.255.0.0
Ruijie(config)# show web-auth
```

23.4.8. 查看客户端自动获取的 HTTP 重定向的配置信息

在特权模式下使用如下命令查看客户端自动获取的 HTTP 重定向的配置信息：

命令	作用
show http redirect	查看客户端自动获取的 HTTP 重定向的配置信息

以下例子是查看查看客户端自动获取的 HTTP 重定向的配置信息：

```
Ruijie# show http redirect
http redirect settings
 server        : 172.16.0.1
 port          : 80 8080
 homepage      : http://www.su-download.net/
 session-limit : 3
 timeout       : 3

direct-site
  Address          Mask             ARP Binding
  ---------------- ---------------- -----------
  176.10.0.1       255.255.255.255   On
  176.10.5.0       255.255.255.128   Off
```

23.5. 自动获取客户端客户端典型配置举例

23.5.1. 组网需求

1) 网络中包括客户端下载服务器、DHCP 服务器、直通服务器（网站），DNS 服务器、核心交换机（例如 S86 系列交换机）、汇聚交换机（例如 S57 系列交换机等），若干台接入交换机（例如 S26 系列交换机），若干台用户 PC。
2) 接入交换机需要支持自动获取客户端功能。

23.5.2. 组网拓扑

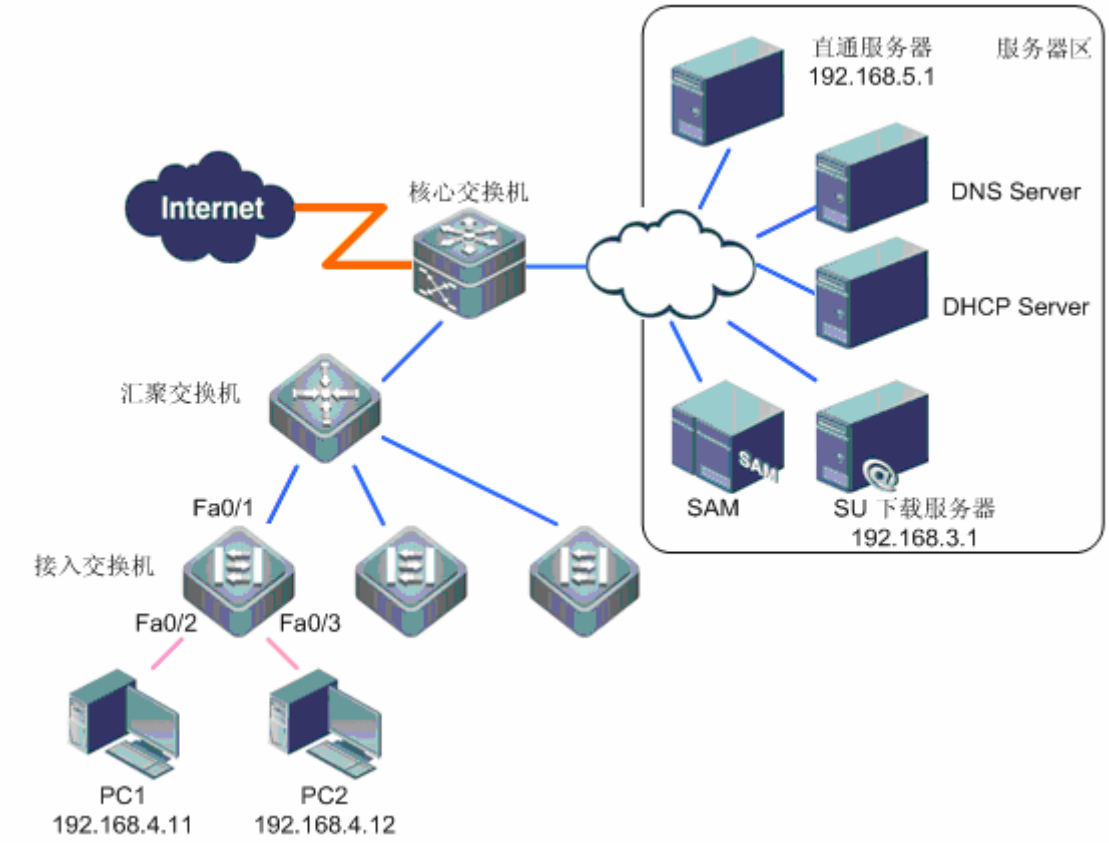


图 11

用户 PC 连接在接入交换机下，接入交换机上链端口连接汇聚交换机，汇聚交换机连接核心交换机，通过核心交换机可以访问 Internet；

服务器部署在服务器区内，通过内部网络与核心交换机相连。

PC1 从 DHCP 服务器获得 IP 地址为 192.168.4.11，PC2 从 DHCP 服务器获得 IP 地址为 192.168.4.12；他们的网关是 192.168.4.1

客户端下载服务器的域名为 www.su_download.com，通过内部 DNS 服务器可以进行解析，客户端下载页面的 URL 为：http://www.su_download.com/su/index.jsp。如果未部署内部 DNS 服务器，可以在 URL 中直接设置客户端下载服务器的 IP；

服务器区内存在公共服务器，无需认证均可访问；

23.5.3. 配置要点

客户端自动获取方案的注意事项：

- 打开了全局客户端下载功能后，802.1x 受控端口下即使是未认证的用户，其发出的 DHCP 和 DNS 报文是可以通过的。不会影响到用户获取 IP 地址，以及进行域名解析；

- 为了防止 TCP 攻击，限制用户在认证前的最大连接数以防止 TCP 攻击，缺省值是 3，最大能配置成 10。但用户 PC 可能发起多个 HTTP 连接，但不一定是浏览器发出的，有可能是其他软件，例如聊天、下载或视屏软件，甚至可能是木马病毒。这种情况下，可能会因其他软件占用了连接，导致浏览器无法建立连接，因此无法弹出客户端下载页面。这种限制的解决，需要在部署时注意，需要自动下载客户端的用户，若上网前开启的自动连接软件过多，要先关掉；

- 由于弹出客户端下载页面必须依靠客户 PC 能发起 HTTP 连接，而在进行连接之前，必须要能让客户 PC 获取到 DNS 解析的 IP 地址，以及网关的 ARP 报文。在这种情况下，接入设备放行未认证用户发给网关的 ARP 请求报文。因此，有可能出现一种 ARP 欺骗情况，即如果某个用户冒充同一个 VLAN 下的其它用户的 IP，给网关发送 ARP 报文，就会造成网关学习到错误的 ARP，对同一 VLAN 下的其它用户产生影响；

23.5.4. 配置步骤

打开全局客户端下载功能

```
Ruijie# config
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# dot1x redirect
```

在 S26 上设置认证服务器的 IP 地址

```
Ruijie(config)# http redirect 192.168.3.1
```

在 S26 上设置客户端下载的主页地址

```
Ruijie(config)# http redirect homepage
http://www.su_download.com/su/index.jsp
```

在 S26 上对 Fa0/2、Fa0/3 两个端口上开启 dot1x 认证功能

```
Ruijie(config)# interface range fa0/2-3
Ruijie(config-if-range)# dot1x port-control auto
Ruijie(config-if-range)# exit
```

在 S26 上设置免认证的网络资源范围，将公共服务器设置为直通的网站

```
Ruijie(config)# http redirect direct-site 192.168.5.1
```

如果打开了 ARP Check 功能，则需要加上 arp 选项：

```
Ruijie(config)# http redirect direct-site 192.168.5.1 arp
```

若开启 ARP 功能，则还必须将网关 IP 地址设置为免认证的网络资源范围，并开启 arp 选项，以保证在认证前，PC 能完成 DNS 及 ARP 请求。

在 S26 上将下联 PC 的网关 192.168.4.1 设置免认证的网络资源范围

```
Ruijie(config)# http redirect direct-site 192.168.4.1 arp
```

至此 PC1/PC2 如果未认证要访问 internet 就会先重定向到客户端下载服务器，通过客户端的下载及认证后，才能访问 internet。

显示验证

显示 HTTP 重定向的配置：

```
Ruijie# show http redirect
http redirect settings
 server        : 192.168.3.1
 port          : 80
 homepage      : http://www.su_download.com/su/index.jsp
 session-limit : 3
 timeout       : 3

direct-site
  Address          Mask             ARP Binding
  ---------------- ---------------- -----------
  192.168.4.1      255.255.255.255    On
  192.168.5.1      255.255.255.255    On
```

第24章 AAA 配置

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、授权和记帐（AAA）是进行访问控制的一种主要的安全机制。

24.1. 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。
- 记帐：记录用户使用网络资源的情况。当 AAA 记帐被启用时，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。每个记帐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帐、统计、跟踪。

说明：

部分产品的 AAA 仅提供认证功能。所有涉及产品规格的问题，可以通过向福建星网锐捷网络有限公司市场人员或技术支援人员咨询得到。

尽管 AAA 是最主要的访问控制方法，我司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

24.1.1. 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、授权以及记帐类型。通过创建方法列表来定义身份认证、记帐、授权类型，然后将这些方法列表应用于特定的服务或接口。

24.1.2. 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。我司产品使用方法列表中列出的第一个方法时，如果该方法无应答，则选择方法列表中的下一个方法。这个过程一直持续下去，直到与列出的某种安全方法成功地实现通信或用完方法列表。如果用完方法列表而还没有成功实现通信，则该安全功能宣告失败。

注意:

只有在前一种方法没有应答的情况下，我司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。

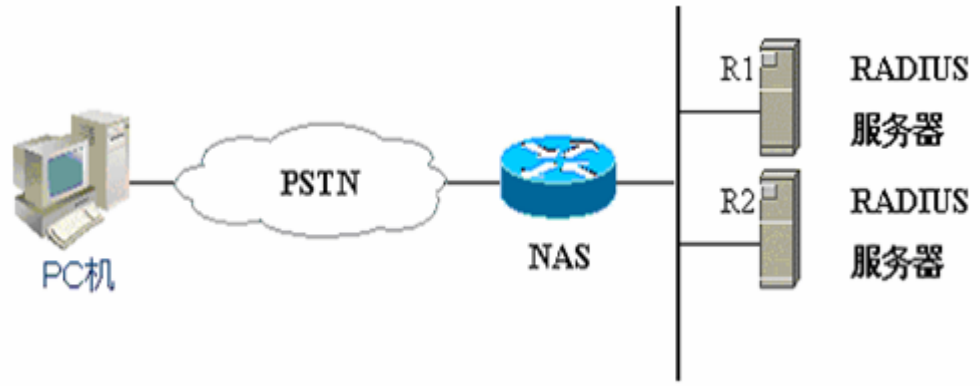


图 1 典型的 AAA 网络配置图

上图说明了一个典型的 AAA 网络配置，它包含两台安全服务器：R1 和 R2 是 RADIUS 服务器。

假设系统管理员已定义了一个方法列表，在这个列表中，R1 首先被用来获取身份信息，然后是 R2，最后是访问服务器上的本地用户名数据库。如果一个远程 PC 用户试图拨号进入网络，网络访问服务器首先向 R1 查询身份认证信息，假如用户通过了 R1 的身份认证，R1 将向网络访问服务器发出一个 ACCEPT 应答，这样用户即获准访问网络。如果 R1 返回的是 REJECT 应答，则拒绝用户访问网络，断

开连接。如果 R1 无应答，网络访问服务器就将它看作 TIMEOUT，并向 R2 查询身份认证信息。这个过程会一直在余下的指定方法中持续下去，直到用户通过身份认证、被拒绝或对话被中止。如果所有的方法返回 TIMEOUT，则认证失败，连接将被断开。

注意：

REJECT 应答不同于 TIMEOUT 应答。REJECT 意味着用户不符合可用身份认证数据库中包含的标准，从而未能通过身份认证，访问请求被拒绝。TIMEOUT 则意味着安全服务器对身份认证查询未作应答，当检测到一个 TIMEOUT 时，AAA 选择身份认证方法列表中定义的下一个身份认证方法将继续进行身份认证过程。

说明：

在本文中，与 AAA 安全服务器相关的认证、授权和记账配置，均以 RADIUS 为例，而与 TACACS+有关的内容请另外参考“配置 TACACS+”。

24.2. AAA 配置基本步骤

首先您必须决定要采用哪种安全解决方案，而且需要评估特定网络中的潜在安全风险，并选择适当的手段来阻止未经授权的访问。我们建议，在可能的情况下，尽量使用 AAA 确保网络安全。

24.2.1. 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：

1) 启用 AAA，使用全局配置层命令 **aaa new-model**。

2) 如果决定使用安全服务器，请配置安全协议的参数，如 RADIUS。

3) 定义身份认证方法列表，使用 **aaa authentication** 命令。

4) 如有需要，可将该方法列表应用于特定的接口或线路。

注意：

在应用特定方法列表时，如果没有明确指定使用命名的方法列表，则使用默认的身份认证方法列表进行身份认证。
因此，如果不准备使用默认的身份认证方法列表，则需要指定特定的方法列表。

对于本章中使用的命令的完整描述，请参见安全配置命令参考中的相关章节。

24.2.2. 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
aaa new-model	启用 AAA

24.2.3. 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
no aaa new-model	停用 AAA

24.2.4. 后续的配置过程

启用 AAA 以后，便可以配置与安全方案相关的其他部分，下表说明了可能要完成的配置任务以及相关内容所在的章节。

AAA 访问控制安全解决方案方法

配置任务	步骤	所在章节
配置 RADIUS 安全协议参数	2	配置 RADIUS
配置本地登录(Login)身份认证	3	配置认证
定义认证方法列表	4	配置认证
将方法列表应用于特定的接口或线路	5	配置认证
启用 RADIUS 授权	6	配置授权
启用 RADIUS 记账	7	配置记账

如果使用 AAA 实现身份认证，请参考“配置认证”中的相关部分。

24.3. 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。

24.3.1. 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。

注意:

只有在前一种方法没有应答的情况下，我司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。

24.3.2. 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
configure terminal	进入全局配置模式
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

configure terminal	进入全局配置模式
aaa new-model	打开 AAA 开关
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。
line vty *2*	进入线路 2 配置层
login authentication *test*	在 line 配置模式下，将名为“test”方法列表应用于线路。

当远程 PC 用户试图 Telnet 访问网络设备(NAS)，NAS 首先向 R1 查询身份认证信息，假如用户通过了 R1 的身份认证，R1 将向 NAS 发出一个 ACCEPT 应答，这样用户即获准访问网络。如果 R1 返回的是 REJECT 应答，则拒绝用户访问网络，断开连接。如果 R1 无应答，NAS 就将它看作 TIMEOUT，并向 R2 查询身份认证信息。这个过程会一直在余下的指定方法中持续下去，直到用户通过身份认证、被拒绝或对话被中止。如果所有的服务器(R1、R2)返回 TIMEOUT，则认证由 NAS 本地数据库完成。

注意:

REJECT 应答不同于 TIMEOUT 应答。REJECT 意味着用户不符合可用的身份认证数据库中包含的标准，从而未能通过身份认证，访问请求被拒绝。TIMEOUT 则意味着安全服务器对身份认证查询未作应答，当验证 TIMEOUT 时，AAA 选择认证方法列表中定义的下一个认证方法继续进行认证过程。

24.3.3. 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。

24.3.4. 配置 AAA 身份认证的通用步骤

要配置 AAA 身份认证，都必须执行以下任务：

- 使用 **aaa new-model** 全局配置命令启用 AAA。
- 如果要使用安全服务器，必须配置安全协议参数，如 RADIUS 和 TACACS+。具体的配置请参见“配置 RADIUS”和“配置 TACACS+”。
- 使用 **aaa authentication** 命令定义身份认证方法列表。
- 如果可能，将方法列表应用于某个特定的接口或线路。

注意：

我司产品 DOT1X 认证目前不支持 TACACS+。

24.3.5. 配置 AAA Login 认证

本节将具体介绍如何配置我司产品所支持的 AAA Login（登录）身份认证方法：

注意：

只有在全局配置模式下执行 **aaa new-model** 命令启用 AAA，AAA 安全特性才能进行配置使用（下同）。关于更详细的内容，请参见“AAA 概述”。

在很多情况下，用户需要通过 Telnet 访问网络访问服务器(NAS)，一旦建立了这种连接，就可以远程配置 NAS，为了防止网络未经授权的访问，要对用户进行身份认证。

AAA 安全服务使网络设备对各种基于线路的 Login（登录）身份认证变得容易。不论您要决定使用哪种 Login 认证方法，只要使用 **aaa authentication login** 命令定义一个或多个身份认证方法列表，并应用于您需要进行 Login 认证的特定线路就可以了。

要配置 AAA Login 认证，在全局配置模式下执行以下命令：

命令	作用
configure	terminal
aaa new-model	启用 AAA。
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。

line vty *line-num*	进入您需要应用 AAA 身份认证的线路。
login authentication {**default** | *list-name*}	将方法列表应用线路。

关键字 *list-name* 用来命名创建身份认证方法列表，可以是任何字符串；关键字 *method* 指的是认证实际算法。仅当前面的方法返回 ERROR（无应答），才使用后面的其他认证方法；如果前面的方法返回 FAIL(失败)，则不使用其他认证方法。为了使认证最后能成功返回，即使所有指定方法都没有应答，可以在命令行中将 **none** 指定为最后一个认证方法。

例如，在下例中，即使 RADIUS 服务器超时(TIMEOUT)，仍然能够通过身份认证：**aaa authentication login default group radius none**

注意:

由于关键字 **none** 使得拨号的任何用户在安全服务器没有应答情况下都能通过身份认证，所以仅将它作为备用的身份认证方法。我们建议：一般情况下，不要使用 **none** 身份认证，在特殊情况下，如所有可能的拨号用户都是可信任的，而且用户的工作不允许有由于系统故障造成的耽搁，可以在安全服务器无应答的情况下，将 **none** 作为最后一种可选的身份认证方法，建议在 **none** 认证方法前加上本地身份认证方法。

关键字	描述
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

上表列出了我司产品支持的 AAA Login 认证方法。

24.3.5.1. 使用本地数据库进行 Login 认证

要配置使用本地数据库进行 Login 认证时，首先需要配置本地数据库，我司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
configure terminal	进入全局配置模式
username *name* [**password** *password*]	建立本地用户，设置口令

end	退出到特权模式
show running-config	确认配置

定义本地 Login 认证方法列表并应用认证方法列表，可使用以下命令：

命令	作用
configure terminal	进入全局配置模式
aaa new-model	打开 AAA 开关
aaa authentication login {**default** | *list-name*} **local**	定义使用本地认证方法
end	退出到特权模式
show aaa method-list	确认配置的方法列表
configure terminal	进入全局配置模式
line vty *line-num*	进入线路配置模式
login authentication {**default** | *list-name*}	应用方法列表
end	退出到特权模式
show running-config	确认配置

24.3.5.2. 使用 RADIUS 进行 Login 认证

要配置用 RADIUS 服务器进行 Login 认证，首先要配置 RADIUS 服务器。配置 RADIUS 服务器，请在全局配置模式下，根据具体需求执行以下命令：

命令	作用
configure terminal	进入全局配置模式
aaa new-model	打开 AAA 开关
radius-server host *ip-address* [**auth-port** *port*] [**acct-port** *port*]	配置 RADIUS 服务器
end	退出到特权模式
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

configure terminal	进入全局配置模式
aaa new-model	打开 AAA 开关
aaa authentication login {**default** | *list-name*} **group radius**	定义使用 RADIUS 认证方法
end	退出到特权模式
show aaa method-list	确认配置的方法列表
configure terminal	进入全局配置模式
line vty *line-num*	进入线路配置模式
login authentication {**default** | *list-name*}	应用方法列表
end	退出到特权模式
show running-config	确认配置

24.3.6. 配置 AAA Enable 认证

本节将具体介绍如何配置我司产品所支持的 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
configure terminal	进入全局配置模式
aaa new-model	启用 AAA。
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。

注意：

如果进入 CLI 界面的时候经过了 Login 身份认证（**none** 方法除外），将记录当前使用的用户名。此时，进行 Enable 认证的时候，将不再提示输入用户名，直接使用与 Login 认证相同的用户名进行认证，注意输入的口令要与之匹配。

如果进入 CLI 界面的时候没有进行 Login 认证，或在 Login 认证的时候使用了 **none** 方法，将不会记录用户名信息。此时，如果进行 Enable 认证，将会要求重新输入用户名。这个用户名信息不会被记录，每次进行 Enable 认证都要重新输入。

一些认证方法，在认证时可以绑定安全级别。这样，在认证过程中，除了根据安全协议返回的成功或失败的应答外，还需要检查绑定的安全级别。如果服务协议能绑定安全级别，则需要在认证时校验绑定的级别。如果绑定的级别大于或等于要切换的目的级别，则 Enable 认证成功，并切换到目的级别；而如果绑定的级别小于要切换的目的级别，则 Enable 认证失败，提示失败信息，维持当前的级别不变。如果服务协议不能绑定安全级别，则不校验绑定的级别，就可以切换到目的级别。

注意：

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。

24.3.6.1. 使用本地数据库进行 Enable 认证

使用本地数据库进行 Enable 认证时，可以在设置本地用户时，为用户设置权限级别。如果没有设置，则默认的用户级别为 1 级。要配置使用本地数据库进行 Enable 身份认证时，首先需要配置本地数据库，并为用户设置权限级别，请在全局配置模式下，根据具体需求执行以下命令：

命令	作用
configure terminal	进入全局配置模式
username *name* [**password** *password*]	建立本地用户，设置口令
username *name* [**privilege** *level*]	为用户设置权限级别（可选）
end	退出到特权模式

show running-config	确认配置

定义本地 Enable 认证方法列表，可使用以下命令：

命令	作用
configure terminal	进入全局配置模式
aaa new-model	打开 AAA 开关
aaa authentication enable default local	定义使用本地认证方法
end	退出到特权模式
show aaa method-list	确认配置的方法列表
show running-config	确认配置

24.3.6.2. 使用 RADIUS 进行 Enable 认证

标准的 RADIUS 服务器可以通过 Service-Type 属性（标准属性号为 6）绑定权限，可以指定 1 级或 15 级权限；我司扩展的 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
configure terminal	进入全局配置模式
aaa new-model	打开 AAA 开关
aaa authentication enable default group radius	定义使用 RADIUS 认证方法
end	退出到特权模式
show aaa method-list	确认配置的方法列表
show running-config	确认配置

24.3.7. 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
configure terminal	进入全局配置模式
aaa new-model	启用 AAA。
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。
interface *interface-type interface-number*	进入需要应用 AAA 身份认证的异步或 ISDN 接口。
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。

24.3.8. 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
configure terminal	进入全局配置模式
aaa new-model	启用 AAA。
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。
dot1x authentication *list-name*	802.1x 应用认证方法列表。

IEEE802.1x 协议更具体的配置方式参见“802.1x 配置”中相关章节。

24.3.9. 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。

24.3.10. 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。

24.4. 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。

24.4.1. 授权类型

我司产品目前支持以下 AAA 授权类型：

- Exec 授权
- Command（命令）授权
- Network（网络）授权

其中 Exec 授权针对的是用户终端登录到 NAS 上的 CLI 界面时，授予用户终端的权限级别（分为 0~15 级）；命令授权针对的是用户终端登录到 NAS 上的 CLI 界面以后，针对具体命令的执行授权；而网络授权针对的是授予网络连接上的用户会话可使用的服务。

说明：

命令授权功能目前仅 TACACS+协议支持，具体内容请参考“配置 TACACS+”。

24.4.2. 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。我司产品 Network 授权仅支持 RADIUS 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。

24.4.3. 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
configure terminal	进入全局配置模式
aaa new-model	打开 AAA 开关
aaa authorization exec {**default** | *list-name*} *method1* [*method2*|…]	定义 AAA Exec 授权方法
aaa authorization network{**default** | *list-name*} *method1* [*method2*|…]	定义 AAA Network 授权方法

24.4.4. 配置 AAA Exec 授权

我司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
configure terminal	进入全局配置模式
aaa new-model	启用 AAA。
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。
line vty *line-num*	进入您需要应用 AAA Exec 授

	权的线路。
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**

关键字	描述
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

上表列出了我司产品支持的 AAA Exec 授权方法。

注意：

Exec 授权通常结合 Login 认证一起使用，并可以在同一个线路上同时使用 Login 认证和 Exec 授权。但是要注意，由于授权和认证可以采用不同的方法和不同的服务器，因此对于相同的用户，认证和授权可能有不同的结果。用户登录时，如果 Exec 授权失败，即使已经通过了 Login 认证，也不能进入到 CLI 界面。

24.4.4.1. 使用本地数据库进行 Exec 授权

要配置使用本地数据库进行 Exec 授权时，首先需要配置本地数据库。可以在设置本地用户时，为用户设置权限级别。如果没有设置，则默认的用户级别为 1 级。请在全局配置模式下，根据具体需求执行以下命令：

命令	作用
configure terminal	进入全局配置模式
username *name* [**password** *password*]	建立本地用户，设置口令

username *name* [**privilege** *level*]	为用户设置权限级别（可选）
end	退出到特权模式
show running-config	确认配置

定义本地 Exec 授权方法列表并应用授权方法列表，可使用以下命令：

命令	作用
configure terminal	进入全局配置模式
aaa new-model	打开 AAA 开关
aaa authorization exec {**default** | *list-name*} **local**	定义使用本地认证方法
end	退出到特权模式
show aaa method-list	确认配置的方法列表
configure terminal	进入全局配置模式
line vty *line-num*	进入线路配置模式
authorization exec {**default** | *list-name*}	应用方法列表
end	退出到特权模式
show running-config	确认配置

24.4.4.2. 使用 RADIUS 进行 Exec 授权

要配置用 RADIUS 服务器进行 Exec 授权，首先要配置 RADIUS 服务器，有关 RADIUS 服务器配置的信息，请参见“配置 RADIUS”。

配置好 RADIUS 服务器后，就可以配置基于 RADIUS 服务器的方法列表了，在全局配置模式下执行以下命令：

命令	作用
configure terminal	进入全局配置模式
aaa new-model	打开 AAA 开关
aaa authorization exec {**default** | *list-name*} **group radius**	定义使用 RADIUS 认证方法
end	退出到特权模式
show aaa method-list	确认配置的方法列表
configure terminal	进入全局配置模式
line vty *line-num*	进入线路配置模式

authorization exec {**default** | *list-name*}	应用方法列表
end	退出到特权模式
show running-config	确认配置

24.4.4.3. 配置 Exec 授权示例

下例演示如何进行 Exec 授权。我们设置 VTY 线路 0~4 上的用户登录时采用 Login 认证，并且进行 Exec 授权。其中 Login 认证采用本地认证，Exec 授权先采用 RADIUS、如果没有响应可以采用本地授权。远程 RADIUS 服务器地址为 192.168.217.64，共享密钥为 test；本地用户名为 ruijie，口令为 ruijie，绑定级别是 6 级。如下：

```
Ruijie# configure terminal
Ruijie(config)# aaa new-model
Ruijie(config)# radius-server host 192.168.217.64
Ruijie(config)# radius-server key test
Ruijie(config)# username ruijie password ruijie
Ruijie(config)# username ruijie privilege 6
Ruijie(config)# aaa authentication login mlist1 local
Ruijie(config)# aaa authorization exec mlist2 group radius local
Ruijie(config)# line vty 0 4
Ruijie(config-line)# login authentication mlist1
Ruijie(config-line)# authorization exec mlist2
Ruijie(config)# end
Ruijie# show running-config
aaa new-model
!
aaa authorization exec mlist2 group radius local
aaa authentication login mlist1 local
!
username ruijie password ruijie
username ruijie privilege 6
!
radius-server host 192.168.217.64
radius-server key 7 093b100133
!
line con 0
line vty 0 4
 authorization exec mlist2
 login authentication mlist1
!
end
```

24.4.5. 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 授权仅支持通过 RADIUS 协议进行，服务器下发的授权信息封装在 RADIUS 属性里，针对不同的网络连接应用，服务器下发的授权信息可能不相同。

注意:

目前该配置不支持 802.1X 的 AAA 授权，802.1X 通过另外的命令完成，具体参见“802.1X 配置”。

要配置 AAA Network 授权，在全局配置模式下执行以下命令：

命令	作用
configure terminal	进入全局配置模式
aaa new-model	启用 AAA。
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。

24.4.5.1. 使用 RADIUS 进行 Network 授权

要配置用 RADIUS 服务器进行 Network 授权，首先要配置 RADIUS 服务器，有关 RADIUS 服务器配置的信息，请参见“配置 RADIUS”。

配置好 RADIUS 服务器后，就可以配置基于 RADIUS 服务器的方法列表了，在全局配置模式下执行以下命令：

命令	作用
configure terminal	进入全局配置模式
aaa new-model	打开 AAA 开关

aaa authorization network {**default** | *list-name*} **group radius**	定义使用 RADIUS 授权方法。

24.4.5.2. 配置 Network 授权示例

下例演示如何进行网络授权。

```
Ruijie# configure terminal
Ruijie(config)# aaa new-model
Ruijie(config)# radius-server host 192.168.217.64
Ruijie(config)# radius-server key test
Ruijie(config)# aaa authorization network test group radius none
Ruijie(config)# end
Ruijie# show running-config
aaa new-model
!
aaa authorization network test group radius none
!
radius-server host 192.168.217.64
radius-server key 7 093b100133
!
```

24.5. 配置记帐

AAA 记帐功能够跟踪用户使用的服务和网络资源。启用记帐功能以后，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。

24.5.1. 记帐类型

我司产品目前支持以下记帐类型：

- Exec 记账
- Command（命令）记账
- Network（网络）记帐

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。

说明:

命令记账功能目前仅 TACACS+协议支持，具体内容请参考“配置 TACACS+”。

24.5.2. 记帐的准备工作

在配置 AAA 记帐以前，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。我司产品 Network 记账仅支持 RADIUS 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”。

24.5.3. 配置 AAA Exec 记帐

Exec 记帐对于已登录到 NAS 的用户终端，可以记录其进入和退出 CLI 界面的信息。在用户终端登录并进入到 NAS 的 CLI 界面时，会向安全服务器发送一个记账开始（Start）信息，在退出 CLI 界面时，会向服务器发送一个记账结束（Stop）信息。

注意:

只有登录到 NAS 的用户终端通过了 Login 认证，才会进行 Exec 记账。如果没有设置 Login 认证，或者认证时候采用了 none 方法，则不会进行 Exec 记账。针对同一个用户终端的登录，登入时如果没有进行过 Start 记账，登出时也就不会进行 Stop 记账。

要配置 AAA Exec 记账，在全局配置模式下执行以下命令：

命令	作用
configure terminal	进入全局配置模式
aaa new-model	启用 AAA。

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。
line vty *line-num*	进入您需要应用 AAA Exec 记账的线路。
accounting exec {**default** | *list-name*}	将方法列表应用线路。

关键字 *list-name* 用来命名创建记账方法列表，可以是任何字符串；关键字 *method* 指的是记账实际算法。仅当前面的方法返回 ERROR（无应答），才使用后面的其他记账方法；如果前面的方法返回 FAIL(失败)，则不使用其他记账方法。为了使记账最后能成功返回，即使所有指定方法都没有应答，可以在命令行中将 **none** 指定为最后一个记账方法。

说明:

使用关键字 **start-stop**，网络访问服务器在用户开始和结束访问网络服务时都给安全服务器发送记帐信息。

24.5.3.1. 使用 RADIUS 进行 Exec 记账

要配置用 RADIUS 服务器进行 Exec 记账，首先要配置 RADIUS 服务器，有关 RADIUS 服务器配置的信息，请参见“配置 RADIUS”。

配置好 RADIUS 服务器后，就可以配置基于 RADIUS 服务器的方法列表了，在全局配置模式下执行以下命令：

命令	作用
configure terminal	进入全局配置模式
aaa new-model	打开 AAA 开关
aaa accounting exec {**default** | *list-name*} **start-stop group radius**	定义使用 RADIUS 记账方法。
end	退出到特权模式
show aaa method-list	确认配置的方法列表
configure terminal	进入全局配置模式
line vty line-num	进入线路配置模式
accounting exec {**default** | *list-name*}	应用方法列表
end	退出到特权模式

show running-config	确认配置

24.5.3.2. 配置 Exec 记帐示例

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
```

24.5.4. 配置 AAA Network 记帐

Network（网络）记帐提供了关于用户会话的记账信息，包括报文的个数及字节数、IP 地址、用户名等。Network 记账目前只支持 RADIUS 协议。

说明:

RADIUS 记帐信息的格式随不同的 RADIUS 安全服务器而变化。记帐记录中的内容可能会由于我司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
configure terminal	进入全局配置模式
aaa new-model	启用 AAA。
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。

24.5.4.1. 使用 RADIUS 进行 Network 记账

要配置用 RADIUS 服务器进行 Network 记账，首先要配置 RADIUS 服务器，有关 RADIUS 服务器配置的信息，请参见“配置 RADIUS”。

配置好 RADIUS 服务器后，就可以配置基于 RADIUS 服务器的方法列表了，在全局配置模式下执行以下命令：

命令	作用
configure terminal	进入全局配置模式
aaa new-model	打开 AAA 开关
aaa accounting network {**default** | *list-name*} **start-stop group radius**	定义使用 RADIUS 记账方法。

24.5.4.2. 配置 Network 记帐示例

以下是使用 RADIUS 进行 Network 记帐的一个例子：

```
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
```

24.6. 监视 AAA 用户

要查看当前登录用户的信息，请在特权用户模式下执行命令：

命令	作用
show aaa user { *id* | **all** }	查看当前 AAA 用户信息

24.7. 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

configure terminal	进入全局配置模式
aaa new-model	打开 AAA 开关
aaa group server radius *gs_name*	配置 RADIUS 服务器组 进入服务器组配置模式
ip vrf forwarding *vrf_name*	为组选择 vrf

说明:

需要产品支持 vrf 功能

24.8. 配置 Login 的用户认证失败锁定

Login 登录交换机，为了防止 Login 用户破解密码，提供配置命令用于限制用户尝试密码的失败次数；超过尝试失败次数，用户被锁定多长时间不能登录。

要配置 Login 登录参量，请在全局配置模式下执行以下命令：

命令	作用
configure terminal	进入全局配置模式
aaa new-model	打开 AAA 开关
aaa local authentication attempts *num*	配置 login 登录，用户尝试失败次数
aaa local authentication lockout-time *num*	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）
end	退出到特权模式
show aaa user lockout {all | user-name *name-string*}	显示当前被锁定的用户列表
clear aaa local user lockout {all | user-name *name-string* }	清除被锁定的用户列表

说明:

默认情况下，Login 尝试失败次数为 3 次，被锁定的时间限制为 15 小时。

24.9. 配置基于域名的 AAA 服务

基于域名的 AAA 服务的配置相关内容，本节包含如下内容：

- 概述
- 基于域名的 AAA 服务配置任务
- 配置基于域名的 AAA 服务配置注意事项

注意：

目前基于域名的 AAA 服务，仅被应用于 IEEE802.1x 认证服务，IEEE802.1x 协议更具体的配置方式参见“802.1x 配置”中相关章节。

24.9.1. 概述

说明：

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。

在多域环境下，同一台 NAS（Network Access Switch）可为不同域中的用户提供 AAA 服务，各域中用户的属性（例如用户名及密码、服务类型、权限等）有可能各不相同，因此有必要通过设置域的方法把它们区分开，并为每个域单独配置包括 AAA 服务方法列表（例如使用的 RADIUS）在内的属性集。

设备基于域名的 AAA 服务基本原理如下：

- 解析用户携带的域名称
- 根据域名称查找用户所配置的域
- 根据设备上域配置信息查找相应的 AAA 服务的方法列表名
- 根据方法列表名在系统中查找对应的方法列表
- 使用该方法列表提供 AAA 服务

说明：

上述任何一个步骤失败，用户将无法使用申请的 AAA 服务

以下是典型的多个域环境拓扑图：

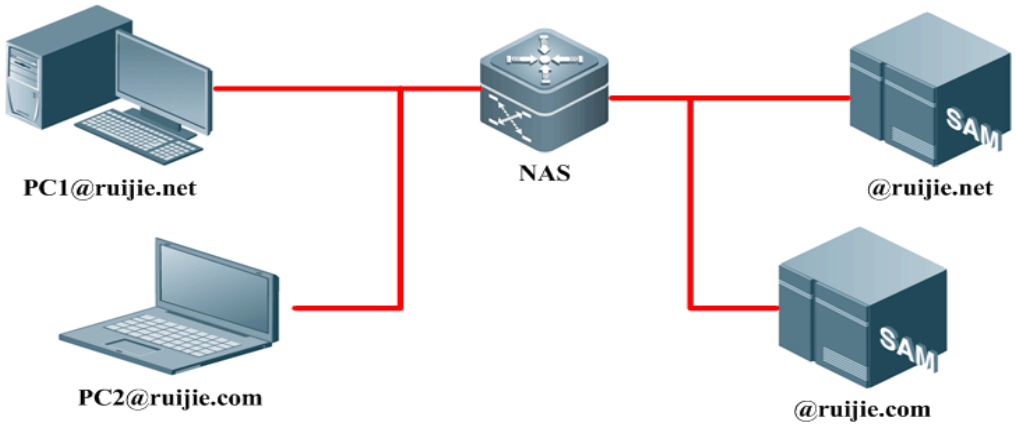


图 2 典型多个域网络图

24.9.2. 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

说明：

系统最多支持配置 32 个域。

24.9.2.1. 启用 AAA

命令	作用

configure terminal	进入全局配置模式
aaa new-model	启用 AAA 服务

具体命令说明请参见“启用 AAA 服务” 章节。

24.9.2.2. 定义 AAA 服务的方法列表

命令	作用
configure terminal	进入全局配置模式
aaa authentication dot1x {**default** | *list-name*} *method1* [*method2*...]	定义一个IEEE802.1x认证方法列表。
aaa accounting network {**default** | *list-name*} **start-stop** *method1* [*method2*...]	定义一个 Network 记账方法列表。
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。

24.9.2.3. 打开基于域名的 AAA 服务开关

命令	作用
configure terminal	进入全局配置模式
aaa domain enable	打开基于域名的 AAA 服务开关

24.9.2.4. 创建域

基于用户名查找匹配的域名时，遵循如下规则：

1、 支持使用单个'. ‘ 、'\' 、‘@ ‘字符区分用户名与域名。

2、 单个 ‘@’字符后跟随的字符串为“域名”。用户名中存在多个‘@’字符时，取最后 1 个‘@’字符后跟随的字符串为域名。如用户名为 a@b@c@d 时，取 a@b@c 为用户名，d 为域。

3、 单个 ‘ \’字符之前的字符串为“域名”。用户名中存在多个‘\’字符时，取第一个‘\’字符之前的字符串为域名。如用户名为 a\b\c\d 时，取 b\c\d 为用户名，a 为域名。

4、 单个 ‘.’ 字符后跟随的字符串为“域名”，用户名中存在多个‘.’字符时，根据预先的配置，取最后 1 个‘.’字符后跟随的字符串为域名。如用户名为 a.b.c.d 时，取 a.b.c 为用户名，d 为域名。

5、 若用户名中同时存在'. ‘ '\' ‘@ ‘三种字符，匹配域名时，将先进行‘@’字符规则判断，再进行‘\’字符规则判断，最后采用‘.’的判断规则。

命令	作用
configure terminal	进入全局配置模式
aaa domain *domain-name*	创建域名为 *domain-name* 的域，并进入域配置模式

说明：

基于域名的 AAA 服务支持最长 64 个字符的域名，不区分大小写。

24.9.2.5. 配置域属性集

在域配置模式下，为已存在的域，选择关联 AAA 服务的方法列表：

命令	作用
authentication dot1x {**default** | *list-name*}	在域配置模式下，选择认证方法列表
accounting network {**default** | *list-name*}	在域配置模式下，选择记账方法列表
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
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
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
access-limit *num*	在域配置模式下，配置该域能够容纳的最大用户数目，默认情况不限制用户的数目（只对 802.1x 用户生效）

说明：

1. 在域配置模式下，选择 AAA 服务方法列表时，这些方法列表是在进入域配置模式前已经定义；否则在域配置模式下，允许选择 AAA 方法列表名，但提示配置不存在；
2. 缺省域（default）：在基于域名的 AAA 服务开关打开情况下，如果用户没有携带域信息，则使用缺省域。如果用户携带的域在系统中没有配置，则判定为非法用户，不提供 AAA 服务；
3. 域配置模式下，没有选择方法列表的情况下，系统默认分配缺省方法列表；

24.9.2.6. 查看域配置

配置完成基于域名的 AAA 服务后，通过以下命令可以查看相应的配置：

命令	作用
show aaa domain [*domain-name*]	显示当前基于域名的 AAA 服务域信息

24.9.3. 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。

24.9.4. 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
```

第25章 RADIUS 配置

25.1. RADIUS 概述

RADIUS 是远程认证拨号用户服务(Remote Authentication Dial-In User Service)的简称，它是一种分布式的客户机/服务器系统，与AAA配合对试图连接的用户进行身份认证，防止未经授权的访问。在RGOS的实现中，RADIUS 客户端运行在设备或网络访问服务器（NAS）上，并向中央RADIUS服务器发出身份认证请求，中央服务器包含了所有的用户身份认证和网络服务信息。

由于RADIUS是一种完全开放的协议，很多系统如UNIX、WINDOWS 2000等均将RADIUS服务器作为一个组件安装，因此RADIUS是目前应用最广泛的安全服务器。

RADIUS的运行过程如下：

- 提示用户输入用户名和密码。
- 用户名和加密的密码通过网络发送到RADIUS服务器。
- RADIUS返回下述响应之一：
- ACCEPT：通过用户身份认证。
- REJECT：身份认证失败，提示重新输入用户名和密码。
- CHALLENGE：RADIUS 服务器发出询问请求，从用户那里收集更多认证信息。
- 在ACCEPT的响应中包含用户的授权信息。

下图是一个典型的RADIUS拓扑图：

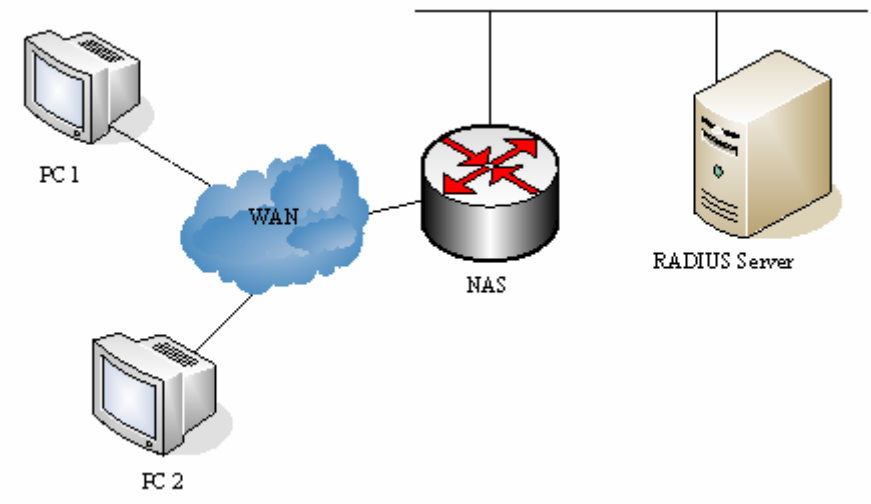


图 1 典型 RADIUS 网络配置

25.2. RADIUS 配置任务

要在网络设备上配置 RADIUS，必须先执行以下任务：

- 启用 AAA。关于如何启用 AAA 的信息，请参见“AAA 概述”。
- 使用 **aaa authentication** 命令定义 RADIUS 身份认证方法列表。关于使用 **aaa authentication** 命令定义身份认证列表的信息，请参见“配置认证”。
- 在特定线路上应用定义的认证列表，否则使用默认身份认证列表进行认证。关于更详细信息，请参见“配置认证”。

完成以上任务后，就可进行配置 RADIUS。配置 RADIUS 包括以下几个部分：

- 配置 RADIUS 协议参数
- 指定 RADIUS 认证

1，配置服务器

在网络设备上需要配置网络中能使用的 RADIUS 服务器，按照以下步骤

命令	作用
configure terminal	进入全局配置模式
radius-server host *ip-addr*	配置 IP 地址为 *ip-addr* 的远程 RADIUS 安全服务器。

2，修改服务器的端口

在特殊的应用环境下，RADIUS 服务器不使用的默认端口，按照以下步骤修改服务器的端口

命令	作用
configure terminal	进入全局配置模式
radius-server host *ip-addr* **auth-port** *port*	修改 IP 地址为 *ip-addr* 的 *RADIUS* 服务器认证端口为 *port*。
radius-server host *ip-addr* **acct-port** *port*	修改 IP 地址为 *ip-addr* 的 *RADIUS* 服务器记账端口为 *port*。

3，配置 RADIUS 协议参数

在网络设备上配置 RADIUS 之前，应确保 RADIUS 服务器的网络通讯良好。要配置 RADIUS 协议参数，请执行以下命令：

命令	作用
configure terminal	进入全局配置模式

radius-server retransmit *retries*	指定设备在确认 RADIUS 无效以前发送请求的次数（默认值为 3）。
radius-server timeout *seconds* **radius-server deadtime** *minutes*	指定设备重传请求以前等待的时间（默认值为 2 秒）。 指定设备发出请求没有回应而作为服务器死亡的需要等待时间（默认值为 5minutes）

4，配置 RADIUS 服务器共享密码

配置 RADIUS 服务器，相应的必须要配置共享密码。网络设备上的共享密码和 RADIUS 服务器上的共享密码必须一致，配置共享密码时可指示为 0 或 7，0 表示明文形式的共享密码，7 表示加密形式共享密码，不指定和指定为 0 的情况一致。

当系统配置了命令 **service password-encryption** 或者配置 RADIUS 共享密码指定为 7 时，通过 **show running** 查看 RADIUS 共享密码配置显示为加密形式，其他情况通过 **show running** 查看 RADIUS 共享密码配置显示为明文形式。

通过以下步骤为服务器配置共享密码。

命令	作用
configure terminal	进入全局配置模式
radius-server key [**0**|**7**] *text*	配置全局共享密码
radius-server host *ip_addr* **key** [**0**|**7**] *text*	为 IP 地址为 *ip_addr* 的服务器配置专用的共享密码。

说明：

在网络设备上必须为 RADIUS 服务器配置共享密码，可以只配置全局共享密码或服务器专用的共享密码，也可以两者同时配置。当服务器配置的专有共享密码和全局共享密码不同时，该服务器使用专用共享密码。

5，指定 RADIUS 身份认证

指定 RADIUS 服务器并定义了 RADIUS 身份认证共享密码后，需要为 RADIUS 定义身份认证方法列表。由于 RADIUS 身份认证是通过 AAA 来进行的，所以需要执行 **aaa authentication** 命令来定义身份认证方法列表，并指定身份认证方法为

RADIUS。关于更详细的信息，可以参考 AAA 配置。

6，指定 RADIUS 私有属性类型

通过该节可以自由配置私有属性的类型。默认配置如下：

我司产品私有属性识别默认配置：

ID	功能	TYPE
1	max down-rate	1
2	qos	2
3	user ip	3
4	vlan id	4
5	version to client	5
6	net ip	6
7	user name	7
8	password	8
9	file-diractory	9
10	file-count	10
11	file-name-0	11
12	file-name-1	12
13	file-name-2	13
14	file-name-3	14
15	file-name-4	15
16	max up-rate	16
17	version to server	17
18	flux-max-high32	18
19	flux-max-low32	19
20	proxy-avoid	20
21	dailup-avoid	21
22	ip privilige	22
23	login privilige	42
24	limit to user number	50

扩展厂商 ID 默认配置：

ID	功能	TYPE

1	max down-rate	76
2	qos	77
3	user ip	3
4	vlan id	4
5	version to client	5
6	net ip	6
7	user name	7
8	password	8
9	file-diractory	9
10	file-count	10
11	file-name-0	11
12	file-name-1	12
13	file-name-2	13
14	file-name-3	14
15	file-name-4	15
16	max up-rate	75
17	version to server	17
18	flux-max-high32	18
19	flux-max-low32	19
20	proxy-avoid	20
21	dailup-avoid	21
22	ip privilige	22
23	login privilige	42
24	limit to user number	50

说明：

两个功能不能配置为一个类型号

以下是网络设备配置私有类型的具体实例：

```
Ruijie# show radius vendor-specific
id    vendor-specific     type-value
----- ------------------- ----------
1     max down-rate       76
2     qos                 77
```

```
3    user ip           3
4    vlan id           4
5    version to client   5
6    net ip            6
7    user name          7
8    password           8
9    file-diractory      9
10   file-count         10
11   file-name-0         11
12   file-name-1         12
13   file-name-2         13
14   file-name-3         14
15   file-name-4         15
16   max up-rate         75
17   version to server    17
18   flux-max-high32     18
19   flux-max-low32      19
20   proxy-avoid         20
21   dailup-avoid        21
22   ip privilige        22
23   login privilige     42
24   limit to user number 50
```

```
Ruijie# configure
Ruijie(config)# radius attribute 24 vendor-type 67
Ruijie(config)# show radius vendor-specific
id    vendor-specific     type-value
----- -------------------- ----------
1    max down-rate       76
2    qos                77
3    user ip            3
4    vlan id            4
5    version to client   5
6    net ip             6
7    user name          7
8    password           8
9    file-diractory      9
10   file-count         10
11   file-name-0         11
12   file-name-1         12
13   file-name-2         13
14   file-name-3         14
15   file-name-4         15
16   max up-rate         75
17   version to server    17
18   flux-max-high32     18
```

```
19    flux-max-low32      19
20    proxy-avoid         20
21    dailup-avoid        21
22    ip privilige        22
23    login privilige     42
24    limit to user number 50
Ruijie(config)#
Ruijie(config)#
```

25.3. 监控 RADIUS

要监控 RADIUS 事件，请在特权用户模式执行以下命令：

命令	作用
debug radius event	打开 RADIUS 调试开关，查看 RADIUS 调试信息。

要监控 RADIUS 细节，请在特权用户模式执行以下命令：

命令	作用
debug radius detail	打开 RADIUS 调试开关，查看 RADIUS 调试信息。

25.4. RADIUS 配置示例

典型 RADIUS 网络配置图中，RADIUS 服务器对访问用户进行身份认证，并为访问用户启用记帐功能，记录用户使用网络服务情况。

说明：

RADIUS 服务器可以是 Windows 2000/2003 Server（IAS）、UNIX 系统所带组件，也可以是一些厂商通过的专用服务器软件。

以下是网络设备配置 RADIUS 的具体实例：

```
Ruijie# configure terminal
Ruijie(config)# aaa new-model
Ruijie(config)# radius-server host 192.168.12.219
auth-port 1645 acct-port 1646
Ruijie(config)# radius-server key aaa
Ruijie(config)# aaa authentication login test group radius
Ruijie(config)# end
Ruijie# show radius server
```

```
Server IP:       192.168.12.219
Accounting Port: 1646
Authen  Port:    1645
Server State:    Ready

Ruijie# configure terminal
Ruijie(config)# line vty 0
Ruijie(config-line)# login authentication test
Ruijie(config-line)# end
Ruijie# show running-config
!
aaa new-model
!
!
aaa authentication login test group radius
!
username ruijie password 0 starnet
!
radius-server host 192.168.12.219 auth-port 1645 acct-port 1646
!
line con 0
line vty 0
login authentication test
line vty 1 4
!
```

第26章 TACACS+配置

26.1. TACACS+概述

TACACS+（是在 TACACS（RFC 1492 Terminal Access Controller Access Control System））基础上进行了功能增强的安全协议。主要是通过 Client-Server 模式与 TACACS 服务器通信来实现多种用户的 AAA 功能，可用于终端用户的认证、授权和记账，在配置使用 TACACS+服务器前，需要先配置好 TACACS+服务器的相关内容。

TACACS+支持用户认证、授权和记账分析，即我们可以使用一台服务器进行认证，然后使用另外一台服务器进行授权，同时可以使用第三台服务器进行记账，每台服务器可以拥有自己的用户数据信息，可以独立进行用户的认证、授权和记账。

TACACS+的报文格式如下：

4	8	16	24	32 bit
Major	Minor	Packet type	Sequence no.	Flags
Session ID				
Length				

图 1

- Major Version — 主要 TACACS+ 版本号。
- Minor Version — 次要 TACACS+ 版本号。
- Packet Type — 可能值包括：

TAC_PLUS_AUTHEN： = 0x01 （认证）
TAC_PLUS_AUTHOR：= 0x02 （授权）
TAC_PLUS_ACCT：= 0x03 （记账）

- Sequence Number — 当前会话中的数据包序列号。会话中的第一个 TACACS+ 数据包序列号必须为 1，其后的每个数据包序列号逐次加 1。因此客户机只发送奇序列号数据包，而 TACACS+ Daemon 只发送偶序列号数据包。
- Flags — 该字段包括各种位图格式的标志（flag）。Flag 值表明数据包是否进行加密。
- Session ID — 该 TACACS+ 会话的 ID。
- Length — TACACS+ 数据包主体长度（不包括头部），报文全部以加密形式在网络上传输。

26.2. TACACS+应用

TACACS+的典型应用为终端用户的登录管理控制，在终端登录时（例如 Telnet 连接），网络设备（例如交换机或路由器）作为 TACACS+的客户端，将用户名和密码发给 TACACS+服务器进行验证，验证通过并得到授权之后可以登录到网络设备上进行操作。如图 2 所示：

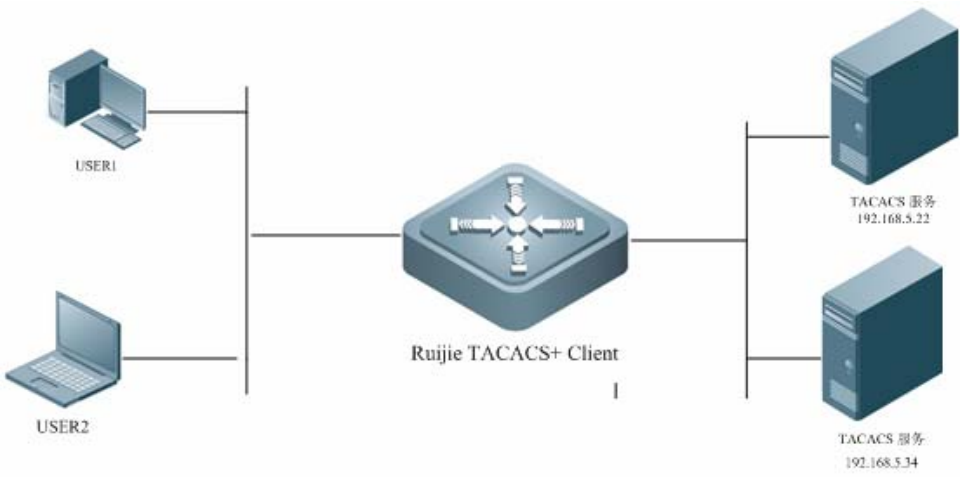


图 2

下边以终端登录的基本认证、授权和记账说明 TACACS+运行中的数据报文的交互：

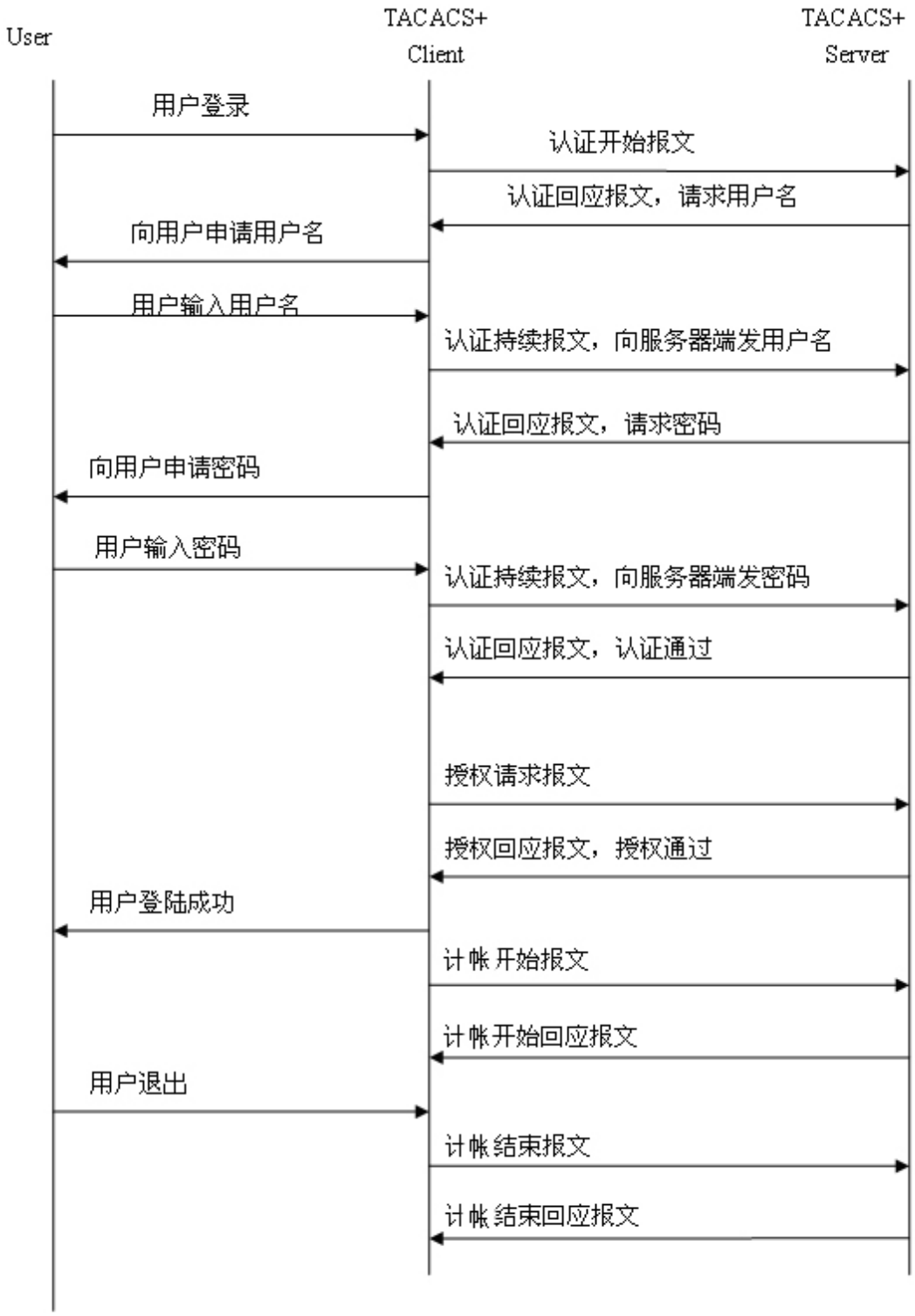


图 3

在整个过程中的基本消息交互流程可以分为三个部分：

1. 认证过程包含：

1） 用户请求登录网络设备。

2） TACACS+客户端收到请求之后，向 TACACS+服务器发送认证开始报文。

3） TACACS+服务器发送认证回应报文，请求用户名。

4） TACACS+客户端收到认证回应报文，向用户询问用户名。

5） 用户输入登录的用户名信息。

6） TACACS+客户端收到用户名后，向 TACACS+服务器发送认证持续报文，其中包括了用户名。

7） TACACS+服务器发送认证回应报文，请求登录密码。

8） TACACS+客户端收到认证回应报文，向用户询问登录密码。

9） 用户输入登录的密码信息。

10） TACACS+客户端收到登录密码后，向 TACACS+服务器发送认证持续报文，其中包括了登录密码。

11） TACACS+服务器发送认证回应报文，指示用户通过认证。

2. 认证通过后对用户进行授权：

1） TACACS+客户端向 TACACS+服务器发送授权请求报文。

2） TACACS+服务器发送授权回应报文，指示用户通过授权。

3） TACACS+客户端收到授权回应成功报文，向用户输出网络设备的配置界面。

3. 授权通过后，需要对登录的用户进行记账，记账：

1） TACACS+客户端向 TACACS+服务器发送记账开始报文。

2） TACACS+服务器发送记账回应报文，指示记账开始报文已经收到。

3） 用户退出。

4） TACACS+客户端向 TACACS+服务器发送记账结束报文。

5） TACACS+服务器发送记账回应报文，指示记账结束报文已经收到。

26.3. TACACS+配置任务

要在网络设备上配置 TACACS+，必须先执行以下任务：

- 使用 **aaa new-mode** 命令启用 AAA。在使用 TACACS+前必须先启用 AAA，关于如何启用 **aaa new-mode** 的信息，请参见“AAA 概述”。
- 使用 **tacacs-server host** 命令配置一个或多个 TACACS+服务器。
- 使用 **tacacs-server key** 命令指定服务器和网络设备共享的 key。
- 使用 **tacacs-server timeout** 命令指定等待服务器响应的超时时间。
- 如果需要认证，使用 **aaa authentication** 命令定义使用 TACACS+的身份认证方法列表。关于使用 **aaa authentication** 命令定义身份认证列表的信息，请参见“配置认证”。
- 如果需要授权，使用 **aaa authorization** 命令定义使用 TACACS+的授权方法

列表。关于使用 **aaa authorization** 命令定义授权方法列表的信息，请参见“配置授权”。

- 如果需要记帐，使用 **aaa accounting** 命令定义使用 TACACS+的记帐方法列表。关于使用 **aaa accounting** 命令定义记帐方法列表的信息，请参见“配置记帐”。
- 在特定线路上应用定义的方法列表，否则使用默认列表。

具体的配置 TACACS+的方法，参见以下章节：
指定TACACS+服务器主机
配置全局的TACACS+共享密钥
配置AAA服务器组
指定进行TACACS+认证
指定进行TACACS+授权
指定进行TACACS+记账
配置TACACS+协议参数

配置 TACACS+的举例，请参见以下章节：
使用TACACS+进行认证、授权、记账配置示例

26.3.1. 指定 TACACS+服务器主机

使用 **tacacs-server host** 命令，可以定义网络上 TACACS+服务器主机的 IP 地址和采用的密钥。要配置 TACACS+服务器主机，请执行以下命令：

命令	作用
configure terminal	进入全局配置模式。
tacacs-server host *ip-address* [**port** *integer*] [**timeout** *integer*] [**key** *string*]	配置远程 TACACS+服务器主机，通过不同的参数组合份配置该服务器的不同的参数： ● *ip-address*：配置服务器的地址。 ● **port** *integer* [可选]：确定服务器使用的端口，默认使用 49，可配置范围 1 到 65535。 ● **timeout** *integer* [可选]：用于配置本服务器的超时响应的时间，默认 5s，可配置范围 1 到 1000s。 ● **key** *string* [可选]：用于配置和对应 IP 的服务器的共享的密钥。

注意：

如果为配置的 TACACS+服务器单独指定了共享密钥，则针对该服务器，全局的TACACS+共享密钥将失效。

26.3.2. 配置全局的 TACACS+共享密钥

要配置全局的 TACACS+共享密钥，请执行以下命令：

命令	作用
configure terminal	进入全局配置模式。
tacacs-server key *string*	配置设备和 TACACS+服务器进行通讯的共享密钥，当对应的主机没有单独配置共享密钥时，则使用全局的配置。

注意：

配置 TACACS+，必须要配置共享密钥。并且网络设备上的共享密码和 TACACS+服务器上的共享密码必须一致。

26.3.3. 配置 AAA 服务器组

在网络设备上配置 AAA 服务器组，可以提供一个将现有服务器主机进行分组的方法，允许选择使用已经配置的服务器的一个子集，并将其应用在一个特定的服务中（例如用于 Login 认证）。

每个服务器组可以包含多个服务器，服务器主机按加入的先后排序，并组成各自的服务器主机列表。如果将多个服务器加入到服务器组，则先加入的排在前面，后加入的服务器作为前一个服务器的备用，当前一个服务器失效的时候，将尝试采用下一个备用的服务器。

要配置 AAA 服务器组，请执行以下命令：

命令	作用
configure terminal	进入全局配置模式。
tacacs-server host *ip-address* [**port** *integer*] [**timeout** *integer*] [**key** *string*]	配置远程 TACACS+服务器主机，参见前面的”指定 TACACS+服务器主机”章节。

aaa group server {**radius** | **tacacs+**} *group-name*	定义 AAA 服务器组，并为之指定一个名称。一个服务器组中的所有成员必须是相同类型的（RADIUS 或 TACACS+）。 执行该命令将进入 AAA 服务器组配置子模式。 注意：配置 TACACS+服务器组必须选择 **tacacs+**类型。
server *ip-address*	在服务器组中增加 TACACS+服务器主机，重复这个步骤可以增加多个服务器主机。 注意：要加入到服务器组的的每个服务器主机，必须事先通过 **tacacs-server host** 命令定义。
ip vrf forwarding *vrf-name*	（可选）配置 TACACS+服务器组使用的 vrf 名字(支持 VRF 的设备存在此命令)

26.3.4. 指定进行 TACACS+认证

在配置了 TACACS+服务器和共享密钥之后，必须为 TACACS+定义用于认证方法列表，才能进行 TACACS+认证。因为 TACACS+认证是通过 AAA 进行操作的，因此必须通过 **aaa authentication** 命令将 TACACS+定义为认证所使用的方法。TACACS+支持 Login 认证和 Enable 认证。

Login（登录）认证是针对登录到 NAS 设备的终端进行的身份认证。设置 Login 认证请执行以下命令：

命令	作用
configure terminal	进入全局配置模式。
aaa authentication login {**default** | *list-name*} **group** {**tacacs+** | *group-name*}	指定 Login 认证采用 TACACS+方法。
line [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*]	进入 line 模式，选择哪些终端线路需要采用 Login 认证。
login authentication {**default** | *list-name*}	将 Login 认证方法列表应用在终端线路上。

对于已登录到网络设备的终端用户，在进入命令行界面（CLI）的时候，会被授予一个初始权限级别（授权在下一个章节说明），如果用户的级别想从低切换到高时，为了防止未经授权的访问，需要对用户进行身份认证，称为 Enable 认证。设置 Enable 认证请执行以下命令：

命令	作用

configure terminal	进入全局配置模式。
aaa authentication enable default group {**tacacs+** | *group-name*}	指定 Enable 认证采用 TACACS+方法。

26.3.5. 指定进行 TACACS+授权

在配置了 TACACS+服务器和共享密钥之后，必须为 TACACS+定义用于授权方法列表，才能进行 TACACS+授权。因为 TACACS+授权是通过 AAA 进行操作的，因此必须通过 **aaa authorization** 命令将 TACACS+定义为授权所使用的方法。TACACS+支持 Exec 授权和 Command 授权。

对于已登录到网络设备的终端用户，在进入命令行界面（CLI）的时候，需要一个执行命令的权限级别。CLI 的权限级别从低到高分为 0~15 级，级别越高权限越大。设置 Exec 授权的目的是为不同的用户指派不同的权限，实现用户的分级管理，这个指派权限的过程称为 Exec 授权。要配置 Exec 授权，请执行以下命令：

命令	作用
configure terminal	进入全局配置模式。
aaa authorization exec {**default** | *list-name*} **group** {**tacacs+** | *group-name*}	指定 Exec 授权采用 TACACS+方法。
aaa authorization console	（可选）控制台线路默认不进行 Exec 授权的，如果要设置进行 Exec 授权的话，还需要打开这个开关。
line [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*]	进入 line 模式，选择哪些终端线路需要采用 Exec 授权。
authorization exec {**default** | *list-name*}	将 Exec 授权方法列表应用在终端线路上。

对于已经登录到网络设备的 CLI 界面的终端用户，将获得一个初始的级别（参见前面的 Exec 授权描述），可以访问和级别相符合的 CLI 命令集，但是并不意味着这个用户能真正执行这些命令，要执行命令之前还需要得到许可，这个过程称为 Command（命令）授权。要配置 Command 授权，请执行以下命令：

命令	作用
configure terminal	进入全局配置模式。
aaa authorization commands *level* {**default** | *list-name*} **group** {**tacacs+** | *group-name*}	指定 Exec 授权采用 TACACS+方法。 ● *level*：需要进行授权的命令级别。可配置的范围 0 到 15。

no aaa authorization config-commands	（可选）默认情况下，对所有模式下的命令都需要进行Command授权，如果执行这条命令，则全局配置模式和子配置模式下的命令都不进行授权。
line [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*]	进入 line 模式，选择哪些终端线路需要采用 Command 授权。
authorization commands *level* {**default** | *list-name*}	将 Command 授权方法列表应用在终端线路上。 ● *level*：需要进行授权的命令级别。可配置的范围 0 到 15。

26.3.6. 指定进行 TACACS+记账

在配置了 TACACS+服务器和共享密钥之后，必须为 TACACS+定义用于记账方法列表，才能进行 TACACS+记账。因为 TACACS+记账是通过 AAA 进行操作的，因此必须通过 **aaa accounting** 命令将 TACACS+定义为记账所使用的方法。TACACS+支持 Exec 记账和 Command 记账。

对于已登录到网络设备的终端用户，可以记录其进入和退出命令行界面（CLI）的信息。如果打开 Exec 记账功能，则在终端用户登录并进入到网络设备的 CLI 界面时，会向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。要配置 Exec 记账，请执行以下命令：

命令	作用
configure terminal	进入全局配置模式。
aaa accounting exec {**default** | *list-name*} **start-stop group** {**tacacs+** | *group-name*}	指定 Exec 记账采用 TACACS+方法。
line [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*]	进入 line 模式，选择哪些终端线路需要采用 Exec 记账。
accounting exec {**default** | *list-name*}	将 Exec 记账方法列表应用在终端线路上。

对于已登录到网络设备并进入到 CLI 界面的终端用户，如果打开 Command（命令）记账功能，可以记录其执行的命令的信息，并在执行命令成功的时候，将命令信息发送到服务器上去。要配置 Command 记账，请执行以下命令：

命令	作用
configure terminal	进入全局配置模式。

aaa accounting commands *level* {**default** | *list-name*} **start-stop group** {**tacacs+** | *group-name*}	指定 Exec 记账采用 TACACS+方法。 ● *level*：需要进行记账的命令级别。可配置的范围 0 到 15。
line [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*]	进入 line 模式，选择哪些终端线路需要采用 Exec 记账。
accounting commands *level* {**default** | *list-name*}	将 Exec 记账方法列表应用在终端线路上。 ● *level*：需要进行记账的命令级别。可配置的范围 0 到 15。

26.3.7. 配置 TACACS+协议参数

在网络设备上配置 TACACS+时，为确保 TACACS+服务器的网络通讯良好。还可配置 TACACS+协议参数，请执行以下命令：

命令	作用
configure terminal	进入全局配置模式
tacacs-server timeout *seconds*	指定设备重传请求以前等待的时间（默认值为 5 秒），当特定主机没有配置特定的超时时间时，则使用全局的配置时间。
Ip tacacs source-interface *interface*	指定发送 tacacs+请求到服务器使用的源 IP，默认为不指定

26.4. 使用 TACACS+ 进行认证、授权、记帐配置示例

典型 TACACS+网络配置图中，TACACS+服务器对访问用户进行身份认证、授权和记帐，下边分别通过 Login 认证、Enable 认证、Exec 授权和 Command 记帐，演示如何配置使用 TACACS+进行认证、授权和记帐。

26.4.1. Login 认证使用 TACACS+的配置示例：

1. 首先配置启用 aaa：

```
Ruijie# configure terminal
Ruijie(config)# aaa new-model
```

2. 然后配置 tacacs+ server 信息：

```
Ruijie(config)# tacacs-server host 192.168.12.219
```

```
Ruijie(config)# tacacs-server key aaa
```

3. 然后配置使用 tacacs+的认证方法：

```
Ruijie(config)# aaa authentication login test group tacacs+
```

4. 在接口上应用配置认证方法:

```
Ruijie(config)# line vty 0 4
Ruijie(config-line)# login authentication test
```

通过以上配置就实现了配置 login 的 tacacs+认证，配置显示如下。

```
Ruijie#show running-config
!
aaa new-model
!
aaa authentication login test group tacacs+
!
tacacs-server host 192.168.12.219
tacacs-server key aaa
!
line con 0
line vty 0 4
login authentication test
!
```

26.4.2. Enable 认证使用 TACACS+的配置示例：

1. 首先配置启用 aaa：

```
Ruijie# configure terminal
Ruijie(config)# aaa new-model
```

2. 然后配置 tacacs+ server 信息：

```
Ruijie(config)# tacacs-server host 192.168.12.219
Ruijie(config)# tacacs-server host 192.168.12.218
Ruijie(config)# tacacs-server host 192.168.12.217
Ruijie(config)# tacacs-server key aaa
```

3. 配置 tacacs+ server group 使用服务器列表中一部分服务器：

```
Ruijie(config)#aaa group server tacacs+ tacgroup1
Ruijie(config-gs-tacacs)#server 192.168.12.219
Ruijie(config-gs-tacacs)#server 192.168.12.218
```

4. 然后配置使用 tacgroup1 的认证方法：

```
Ruijie(config)# aaa authentication enable default group
tacgroup1
```

通过以上配置就实现了配置 enable 的部分 tacacs+服务器认证，配置显示如下。

```
Ruijie#show running-config
!
aaa new-model
!
!
aaa group server tacacs+ tacgroup1
server 192.168.12.219
server 192.168.12.218
!
aaa authentication enable default group tacgroup1
!
!
tacacs-server host 192.168.12.219
tacacs-server host 192.168.12.218
tacacs-server host 192.168.12.217
tacacs-server key aaa
!
line con 0
line vty 0 4
!
```

26.4.3. Exec 授权使用 TACACS+的配置示例：

1. 首先配置启用 aaa：

```
Ruijie# configure terminal
Ruijie(config)# aaa new-model
```

2. 然后配置 tacacs+ server 信息：

```
Ruijie(config)# tacacs-server host 192.168.12.219
Ruijie(config)# tacacs-server key aaa
```

3. 然后配置使用 tacacs+的授权方法：

```
Ruijie(config)# aaa authorization exec test group tacacs+
```

4. 在接口上应用配置授权:

```
Ruijie(config)# line vty 0 4
Ruijie(config-line)#authorization exec test
```

通过以上配置就实现了配置登录授权使用 tacacs+，配置显示如下。

```
Ruijie#show running-config
!
aaa new-model
```

```
!
!
aaa authorization exec test group tacacs+
!
tacacs-server host 192.168.12.219
tacacs-server key aaa
!
line con 0
line vty 0
authorization exec test
!
```

26.4.4. 15 级 Commans 记账使用 TACACS+的配置示例：

1. 首先配置启用 aaa：

```
Ruijie# configure terminal
Ruijie(config)# aaa new-model
```

2. 然后配置 tacacs+ server 信息：

```
Ruijie(config)# tacacs-server host 192.168.12.219
Ruijie(config)# tacacs-server key aaa
```

3. 然后配置使用 tacacs+的命令记账方法：

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

4. 在接口上应用配置授权:

```
Ruijie(config)# line vty 0 4
Ruijie(config-line)# accounting commands 15 default
```

通过以上配置就实现了配置 enable 的部分 tacacs+服务器认证，配置显示如下。

```
Ruijie#show running-config
!
aaa new-model
!
aaa accounting commands 15 default group tacacs+
!
!
tacacs-server host 192.168.12.219
tacacs-server key aaa
!
line con 0
line vty 0 4
!
```

第27章 SSH 终端服务

27.1. 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。

27.2. 锐捷 SSH 支持算法

支持算法	SSH1	SSH2
签名认证算法	RSA	RSA、DSA
密钥交换算法	基于 RSA 公钥加密的密钥交换算法。	KEX_DH_GEX_SHA1 KEX_DH_GRP1_SHA1 KEX_DH_GRP14_SHA1
加密算法	DES、3DES、Blowfish	DES 、 3DES 、 AES-128 、 AES-192、AES-256
用户认证算法	基于用户口令的认证方式	基于用户口令的认证方式
消息认证算法	不支持	MD5 、 SHA1 、 SHA1-96 、 MD5-96
压缩算法	NONE（无压缩）	NONE（无压缩）

27.3. 锐捷 SSH 支持

注意：

锐捷网络产品仅支持 SSH 服务器（兼容 SSHv1 与 SSHv2），不支持 SSH 客户端。

27.4. SSH 配置

27.4.1. 缺省的 SSH 配置

项目	缺省值
SSH 服务端状态	关闭
SSH 版本	兼容模式（支持版本 1 和 2）
SSH 用户认证超时时间	120s
SSH 用户重认证次数	3 次

27.4.2. 用户认证配置

1. 基于 SSH 连接安全性的考虑，禁止使用无认证方式登录。因此在用户登录认证时，所使用的登录认证方式必须设置密码；（Telnet 可以设置无认证登录）

2. 每次输入的用户名(Username)与密码(Password)长度必须大于零。如果当前认证方式不需要用户名时，用户名可以任意输入，但是输入长度必须大于零。

27.4.3. 打开 SSH Server

缺省情况下，SSH Server 处于关闭状态。打开 SSH Server，需要在全局配置模式下，执行 **enable service ssh-server** 命令，同时需要生成 SSH 密钥，使 SSH Server 的状态成为 ENABLE。

命令	说明
configure terminal	进入配置模式
enable service ssh-server	打开 SSH Server
crypto key generate {rsa|dsa}	生成密钥

注意：

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。

27.4.4. 关闭 SSH Server

关闭 SSH Server，需要在全局配置模式下，执行 **no enable service ssh-server** 命令，使 SSH Server 的状态成为 DISABLE。

命令	说明
configure terminal	进入配置模式
no enable service ssh-server	关闭 SSH Server

27.4.5. 配置 SSH server 支持版本

缺省情况下，SSH Server 兼容版本 1 和 2。使用以下命令配置 SSH 使用版本。

命令	说明
configure terminal	进入配置模式
ip ssh version {1 | 2}	配置 SSH 支持的版本
no ip ssh version	恢复 SSH 为缺省配置，支持 SSHv1 与 SSHv2；

27.4.6. 配置 SSH 用户认证超时时间

缺省情况下，SSH Server 的用户认证超时时间为 120 秒，。使用以下命令配置 SSH 的用户认证超时时间。

命令	说明
configure terminal	进入配置模式
ip ssh time-out *time*	配置 SSH 的超时时间（范围 1-120sec）
no ip ssh time-out	恢复 SSH 的缺省用户认证超时时间为 120 秒；

27.4.7. 配置 SSH 重认证次数

该配置命令用来设置 SSH 用户请求连接的认证重试次数，防止恶意猜测等非法行为。缺省情况下，SSH Server 的重认证次数为 3 次，即可以允许用户尝试三次输入用户名与密码进行认证尝试。使用以下命令配置 SSH 的重认证次数。

命令	说明
configure terminal	进入配置模式
ip ssh authentication-retries *retry times*	配置 SSH 的重认证次数（范围 0-5）
no ip ssh authentication-retries	恢复SSH的缺省重认证次数为 3 次；

注：上述命令具体配置请参见[SSH 命令参考手册]。

27.5. 使用 SSH 进行设备管理

您可以使用 SSH 对设备进行管理，前提是必须打开 SSH Server 功能，默认情况下是关闭该功能的。由于 Windows 自带的 Telnet 组件不支持 SSH，因此必须使用第三方客户端软件，当前兼容性较好的客户端包括：Putty，Linux，SecureCRT。下面以客户端软件 SecureCRT 为例介绍 SSH 客户端的配置，配置界面如下图：

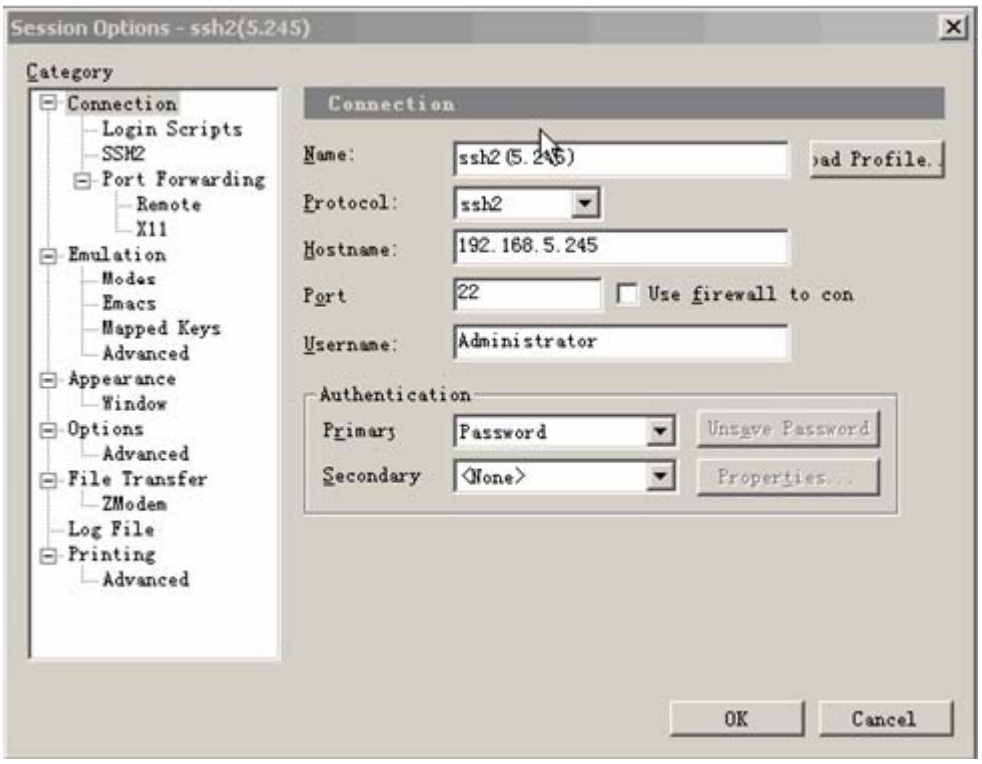


图 1

如图 1 使用协议 2 进行登陆，因此在 Protocol 选择 SSH2，Hostname 就是要登陆的主机的 IP 地址，这里为 192.168.5.245，端口为 22 即 SSH 监听的默认端口号，Username 为用户名，当设备只要求密码时，该用户名不会起作用，Authentication 为认证方式，我们只支持用户名密码的认证方式。使用的密码和 Telnet 密码是一致的。

然后点击 OK，进入出现以下的对话框：

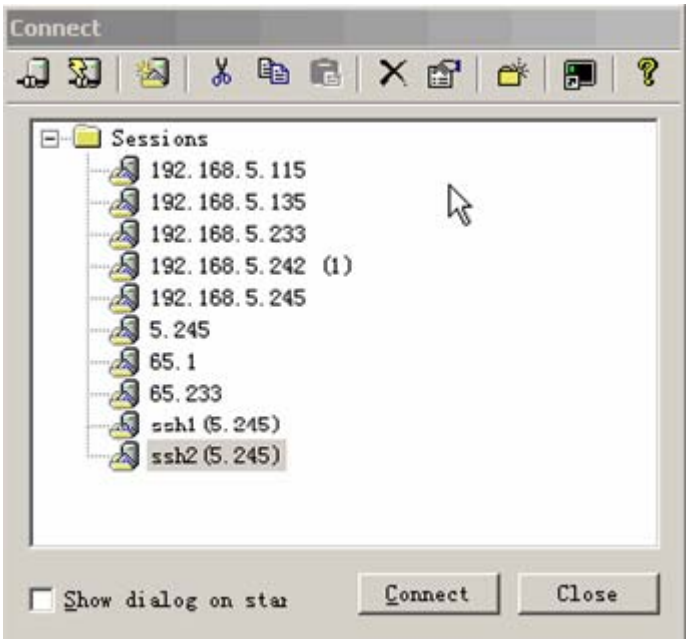


图 2

点击 Connect，登陆我们刚才配置的主机，如下图：

图 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 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：

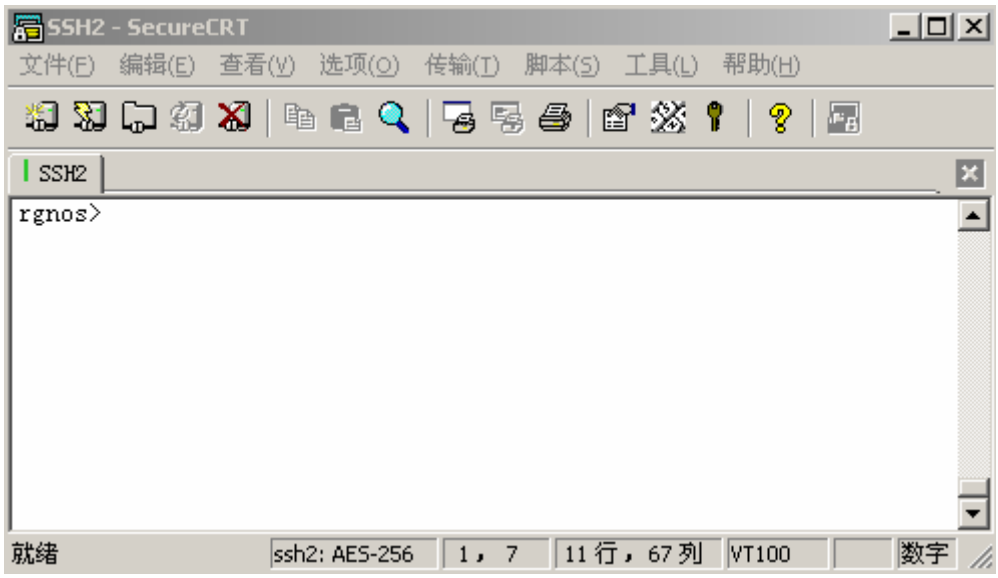


图 5

第28章 动态 ARP 检测配置

28.1. 了解 DAI

DAI 的全称是 Dynamic ARP Inspection，中文名为动态 ARP 检测。即对接收到的 ARP 报文进行合法性检查。不合法的 arp 报文会被丢弃。

28.1.1. 了解 ARP 欺骗攻击

由于 ARP 协议本身的缺陷，ARP 协议本身不对收到的 ARP 报文进行合法性检查。这就造成了攻击者利用协议的漏洞轻易的进行 ARP 欺骗攻击。这其中，最典型的就是中间人攻击。中间人攻击描述如下：

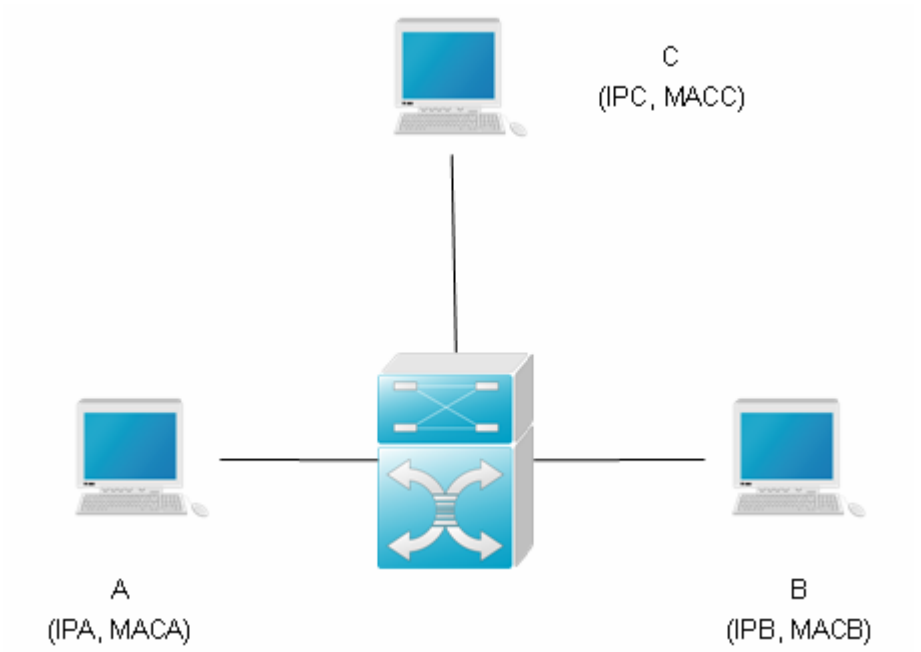


图 1

如图所示：设备 A,B,C 均连接在锐捷设备上，并且它们位于同一个子网，它们的 IP 和 MAC 分别表示为（IPA, MACA）(IPB, MACB) (IPC, MACC),当设备 A 需要和设备 B 进行网络层通信时，设备 A 将会在子网内广播一个 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/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。

28.1.2. 了解 DAI 和 ARP 欺骗攻击

DAI 确保了只有合法的 ARP 报文才会被设备转发。它主要执行以下几个步骤：

- 在打开 DAI 检查功能的 VLAN 所对应的非信任端口上拦截住所有 ARP 请求和应答报文
- 在做进一步相关处理之前，根据 DHCP 数据库的设置，对拦截住的 ARP 报文进行合法性检查。
- 释放没有通过检查的报文。
- 检查通过的报文继续做相应的处理，送给相应的目的地。

ARP 报文是否合法的依据是 DHCP snooping binding 数据库，具体请参考相应的配置指导《DHCP snooping 配置》。

28.1.3. 接口信任状态和网络安全

基于设备上每一个端口的信任状态，对 ARP 报文作出相应的检查，从受信任端口接收到的报文将跳过 DAI 检查，被认为是合法的 ARP 报文； 而从非信任端口接收到的 ARP 报文，将严格执行 DAI 检查。

在一个典型的网络配置中，应该将连接到网络设备的二层端口设置为受信任端口，连接到主机设备的二层端口设置为非信任端口。

注意:

将一个二层端口错误的配置成非信任端口可能会影响到网络正常通信。

具体配置命令请参考 ip arp inspection trust, show ip arp inspection interface。

28.1.4. 限制 ARP 报文的速率

由于设备执行 DAI 合法性检查，需要消耗一定的 CPU 资源，所以对 ARP 报文限速，即限制每秒钟接收的 ARP 报文的数量，可以有效避免针对 DAI 功能而产生的拒绝服务攻击。默认情况下，非信任端口每秒钟 ARP 报文的最大个数是 15。信任端口不受此限制。可以在二层接口配置模式下通过 ip arp inspection limit-rate 来

配置此速率限制。

具体配置命令请参考 ip arp inspection limit-rate。show ip arp inspection interface

28.2. 配置 DAI

DAI 是一个基于 **ARP** 协议的安全过滤技术，简而言之就是配置一系列的过滤策略使得经过设备的 ARP 报文的合法性得到比传统更加有效的检验。

要使用 DAI 相关功能，可选择性地执行以下各项任务：

- 启用指定 VLAN 的 DAI 功能（必须）
- 设置端口的信任状态（可选）
- 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）

28.2.1. 启用指定 VLAN 的 DAI 报文检查功能

缺省情况下，所有 VLAN 的 DAI 报文检查功能是关闭的。

如果没有启用了 VLAN vid 的 DAI 报文检查功能，vlan-id = vid 的 ARP 报文会跳过 DAI 相关的安全检查（不会跳过 ARP 报文限速）。

可以通过 **show ip arp inspection vlan** 查看所有 VLAN 是否启用了 DAI 报文检查功能

要配置 VLAN 的 DAI 报文检查功能，在接口配置模式中执行以下命令：

命令	作用
Ruijie(config)**# ip arp inspection vlan** *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 省略 *vlan-id* 时关掉所有 VLAN 的 DAI 报文检查功能

28.2.2. 设置端口的信任状态

此命令应用在二层接口配置模式，且此二层接口为一个 SVI 的成员口。

缺省情况下，所有二层端口都是不可信任的。

如果端口是可信任的，ARP 报文将跳过进一步的检查，否则，会使用 DHCP snooping 数据库的信息来检查当前 ARP 报文的合法性

要设置端口信任状态，在接口配置模式中执行以下命令：

命令	作用
Ruijie(config-if)**# ip arp inspection trust**	设置端口是可信任的
Ruijie(config-if)**# no ip arp inspection trust**	设置端口是不可信任的

28.2.3. 设置端口的 ARP 报文最大接收速率

在支持 NFPP 的设备中，由 NFPP 自动实现此功能，不存在此命令。

此命令应用在二层接口模式，且此二层接口为一个 SVI 的成员口。

缺省情况下，每一个非信任交换端口的默认接收 ARP 报文速率为每秒 15 个 ARP 报文。信任交换端口默认不做限制。

如果 1 秒钟内此端口收到的 ARP 报文超过限制值，后面收到的报文会被丢弃，不会做进一步处理。

可以通过 **show ip arp inspection interface** 命令查看各二层接口的速率限制。

要设置端口 ARP 报文最大接收速率，在接口配置模式中执行以下命令：

命令	作用
Ruijie(config-if)**# ip arp inspection limit-rate** { *<1-2048>* **| none**}	设置端口 ARP 报文最大接收速率，单位：报文/秒 **none**：表示不限制
Ruijie(config-if)**# no ip arp inspection limit-rate**	恢复缺省值

28.2.4. DHCP snooping database 相关配置

参考《DHCP Snooping 配置》。

如果没有配置 DHCP Snooping database，则所有 ARP 报文通过检查

28.3. 显示 DAI 配置

28.3.1. 显示 VLAN 是否启用 DAI 功能

要显示各 VLAN 的启用状态，在全局配置模式中执行以下命令：

命令	作用

Ruijie(config)# **show ip arp inspection vlan**	显示各 VLAN 的启用状态

28.3.2. 显示各二层接口 DAI 配置状态

要显示各二层接口 DAI 配置状态，在全局配置模式中执行以下命令：

命令	作用
Ruijie(config)# **show ip arp inspection interface**	显示各二层接口的 DAI 配置（包括信任状态，和速率限制）

28.4. 配置 ARP 报文的速率的注意事项

注意：

在 S23 系列产品上(包括单机和堆叠环境)，ARP 报文采用软件进行限速，单机环境在交换机 CPU 繁忙的情况下，限速的速率可能不准确，堆叠环境，在主机或从机 CPU 繁忙的情况下，限速的速率也可能不准确。具体表现形式为，单机 CPU 繁忙时，ARP 报文限速仅能限制到大约 150PPS~380PPS，报文流再大时，速率远大于之前限制范围时，也仅能限制到约 150PPS~380PPS，同时由于环境的不同，上述限制的数值可能会有些偏差；堆叠从机 CPU 繁忙时，从机的端口配置限速后，该端口 ARP 报文的发送速率会低至十几 PPS。

第29章 防网关 arp 欺骗配置

29.1. 概述

在二层交换机上，默认情况下 arp 报文是在本 vlan 内广播的，因此这就给针对网关的 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。

因此我们可以在二层交换机上配置防网关 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 就不能发送假冒网关的 arp 响应报文。

29.2. 配置防网关 arp 欺骗

29.2.1. 防网关 arp 欺骗的缺省配置

缺省没有设置任何网关地址。

29.2.2. 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*	在该端口下配置防网关 arp 欺骗，网关 ip 地址为指定 ip。

你可以在端口配置模式下通过命令 **no anti-arp-spoofing ip** *ip-address* 来将防网关 arp 配置清除。

注意：

在上链口上不能配置防网关 arp 欺骗。

S2300 系列产品默认情况下只对 untagged 报文流生效，如果需要匹配全部流，请参考下面的 **tag-support enable** 命令。

配置防网关 arp 欺骗或者 arp check 后，ipv6 acl 不能再使用，反之亦然。

29.2.3. 设置 S23 安全功能对 tag 报文的支持

缺省情况下，S23 系列产品的防网关 arp 欺骗/arp check 全局 ip+mac 绑定/端口安全下的 ip+mac 绑定/802.1x ip 授权等安全控制功能仅对 untag 报文生效，只有设置 tag-support enable 命令之后，这些安全控制功能才能对 tag/untag 报文同时生效。需要注意的是，当设置 tag-support enable 命令之后，以上安全功能的表项个数将减少一半，同时必须保存配置重启交换机，使功能生效。

命令	作用
Ruijie(config)#[no] **tag-support enable**	设置防网关 arp 欺骗/arp check 全局 ip+mac 绑定/端口安全下的 ip+mac 绑定/802.1x ip 授权模式的 tagged 报文流的匹配支持，该命令仅在 S23 系列产品支持，设置之后，上述安全功能的 tag/untag 报文都将生效，否则仅 untag 报文生效。

你可以在全局配置模式下通过命令 no tag-support enable 恢复缺省配置，使安全功能仅对 untag 报文生效。。

注意：

1. 该命令仅在 S2300 系列产品上使用。
2. 设置该命令后， 必须重启交换机使功能生效
3. 该命令会造成安全功能的应用冲突，说明如下：
   1) 防网关 arp 欺骗/arp check；
   2) 全局 ip+mac 绑定/端口安全下的 ip+mac 绑定/802。1x ip 授权模式；

以上两组功能在配置 tag-support 命令之前，必须保证没有同时配置，即当前配置只有功能 1)或者 2），不能 1）和 2）的功能同时设置，否则重启交换机将提示配置失败，配置的功能将出现异常。

29.3. 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
Ruijie **#show anti-arp-spoofing**	显示所有接口下的防网关 arp 欺骗信息

第30章 访问控制列表配置

30.1. 概述

作为我司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。我司产品目前支持以下访问列表：

- 标准 IP 访问控制列表
- 扩展 IP 访问控制列表
- MAC 访问控制列表
- MAC 扩展访问控制列表
- Expert 扩展访问控制列表
- IPV6 扩展访问控制列表

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。

30.1.1. 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。

30.1.2. 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。

图 1 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 1 所示。

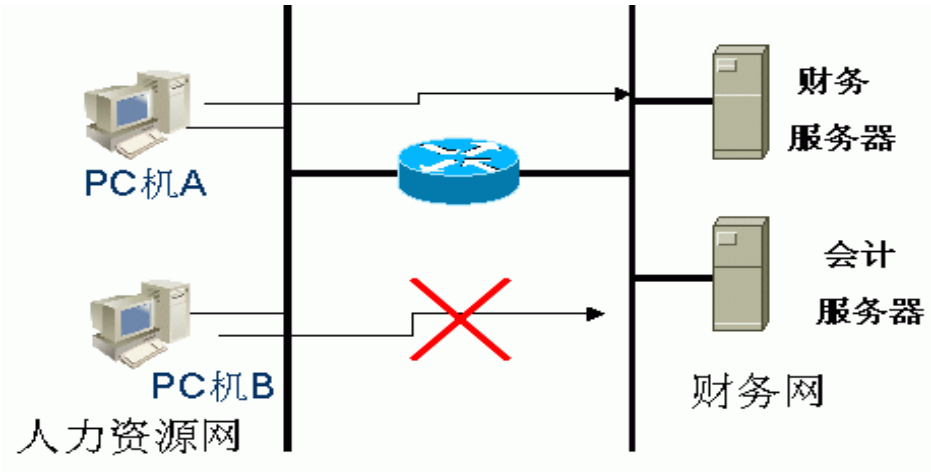


图 1　使用访问列表控制网络访问

30.1.3.　什么时候配置访问列表

您可以根据需要选择基本访问列表或动态访问列表。一般情况下，使用基本访问列表已经能够满足安全需要。但经验丰富的黑客可能会通过一些软件假冒源地址欺骗设备，得以访问网络。而动态访问列表在用户访问网络以前，要求通过身份认证，使黑客难以攻入网络，所以在一些敏感的区域可以使用动态访问列表保证网络安全。

说明：

通过假冒源地址欺骗设备即电子欺骗是所有访问列表固有的问题，使用动态列表也会遭遇电子欺骗问题：黑客可能在用户通过身份认证的有效访问期间，假冒用户的地址访问网络。解决这个问题的方法有两种，一种是尽量将用户访问的空闲时间设置小些，这样可以使黑客更难以攻入网络，另一种是使用 IPSEC 加密协议对网络数据进行加密，确保进入设备时，所有的数据都是加密的。

访问列表一般配置在以下位置的网络设备上：

- 内部网和外部网（如 INTERNET）之间的设备
- 网络两个部分交界的设备

- 接入控制端口的设备.

访问控制列表语句的执行必须严格按照表中语句的顺序，从第一条语句开始比较，一旦一个数据包的报头跟表中的某个条件判断语句相匹配，那么后面的语句就将被忽略，不再进行检查。

30.1.4. 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。

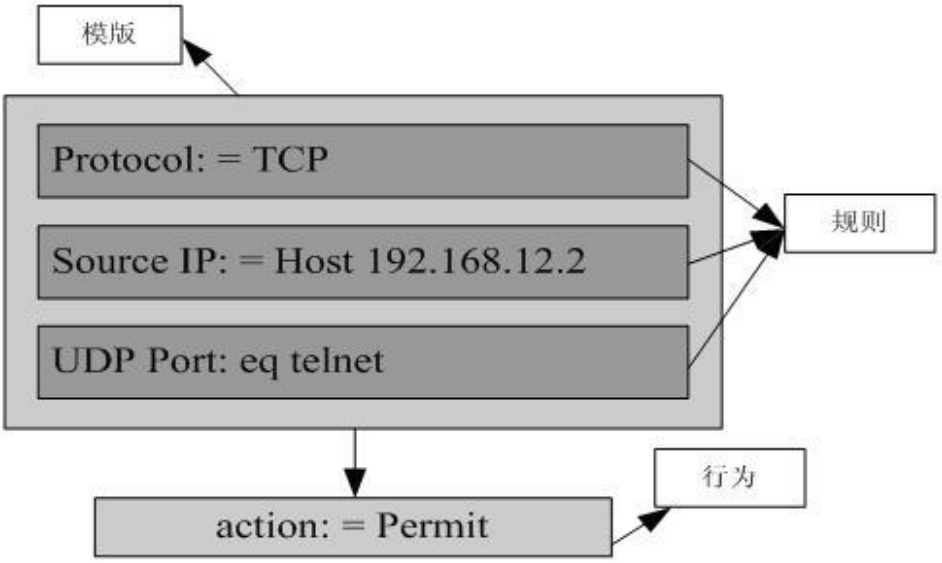


图 2　对 ACE：permit tcp host 192.168.12.2 any eq telnet 的分析

说明：

过滤域模板可以是三层字段(Layer 3 Field)和四层字段(Layer 4 Field)字段的集合，也可以是多个二层字段(Layer 2 Field)的集合，但标准与扩展的 ACL 的过滤域模板不能是二层和三层、二层和四层、二层和三层、四层字段的集合。要使用二层、三层、四层字段集合，可以应用 Expert 扩展访问控制列表（Expert ACLs）。

30.2. IP 访问列表配置

要在设备上配置访问列表，必须为协议的访问列表指定一个唯一的名称或编号，以便在协议内部能够唯一标识每个访问列表。下表列出了可以使用编号来指定访问列表的协议以及每种协议可以使用的访问列表编号范围。

协议	编号范围
标准 IP	1-99，1300 - 1999
扩展 IP	100-199，2000 - 2699

30.2.1. 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。

30.2.1.1. 隐含“拒绝所有数据流”规则语句

在每个访问列表的末尾隐含着一条“拒绝所有数据流”规则语句，因此如果分组与任何规则都不匹配，将被拒绝。

如下例：

```
access-list 1 permit host 192.168.4.12
```

此列表只允许源主机为 192.168.4.12 的报文通过，其它主机都将被拒绝。因为这条访问列表最后包含了一条规则语句：access-list 1 deny any。

又如：

```
Access-list 1 deny host 192.168.4.12
```

如果列表只包含以上这一条语句，则任何主机报文通过该端口时都将被拒绝。

注意：

在定义访问列表的时候，要考虑到路由更新的报文。由于访问列表末尾“拒绝所有数据流”，可能导致所有的路由更新报文被阻断。

30.2.1.2. 输入规则语句的顺序

加入的每条规则都被追加到访问列表的最后，语句被创建以后，就无法单独删除

它，而只能删除整个访问列表。所以访问列表语句的次序非常重要。设备在决定转发还是阻断分组时，设备按语句创建的次序将分组与语句进行比较，找到匹配的语句后，便不再检查其他规则语句。

假设创建了一条语句，它允许所有的数据流通过，则后面的语句将不被检查。

如下例：

```
access-list 101 deny ip any any
access-list 101 permit tcp 192.168.12.0 0.0.0.255 eq telnet any
```

由于第一条规则语句拒绝了所有的 IP 报文，所以 192.168.12.0/24 网络的主机 Telnet 报文将被拒绝，因为设备在检查到报文和第一条规则语句匹配，便不再检查后面的规则语句。

30.2.2. 配置 IP 访问列表

基本访问列表的配置包括以下两步：

1. 定义基本访问列表
2. 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	功能
Ruijie(config)# **access-list** *id* {**deny** | **permit**} {src *src-wildcard* | **host** *src* | **any** } [**time-range** *tm-rng-name*]	定义访问列表
Ruijie(config)# **interface** *interface*	选择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	功能
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** | **interface** *idx*} [**time-range** *tm-rng-name*]	为 ACL 添加表项,具体内容请参见命令参考
Ruijie(config-xxx-nacl)# **exit** Ruijie(config)# **interface** *interface*	退出访问控制列表模式，选择选择要应用访问列表的接口

Ruijie(config-if)# **ip access-group** *id* **in**	将访问列表应用特定接口

说明：

方式一只对数值 ACL 进行配置，方式二可以对命名和数值 ACL 进行配置，还可以指定表项的优先级(在支持 ACE 优先级的设备中)。

30.2.3. 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：

```
Ruijie# show access-lists [ id | name ]
```

此命令可以查看基本访问列表

30.2.4. IP 访问列表示例

- **配置要求**

有两台设备 Switch A 和 Switch B，如图 1-3：

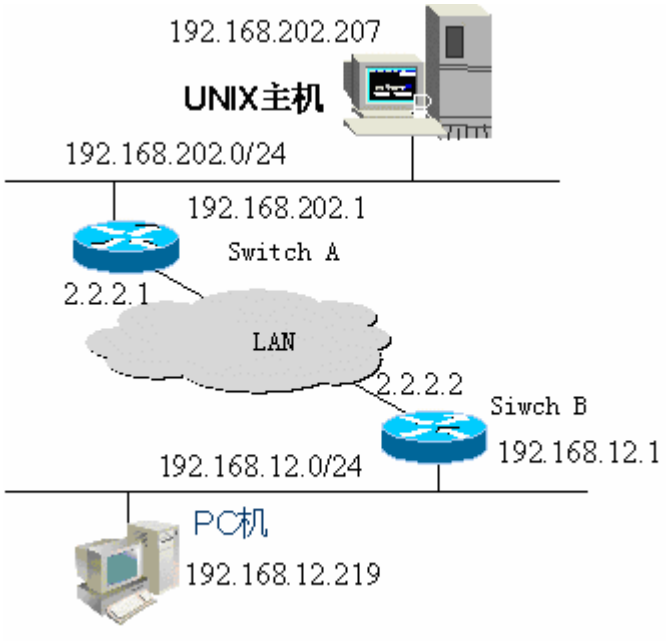


图 3 基本访问列表示例

要求通过在 Switch B 上配置访问列表，实现以下安全功能：

- 192.168.12.0/24 网段的主机只能在正常上班时间访问远程 UNIX 主机 TELNET 服务，拒绝 PING 服务。

- 在 Switch B 控制台上不能访问 192.168.202.0/24 网段主机的所有服务。

说明：

以上案例是银行系统应用的简化，即只允许分行或储蓄点局域网上的主机访问中心主机，不允许在设备上访问中心主机。

- **设备配置**

Switch B 的配置：

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# ip address 192.168.12.1 255.255.255.0
Ruijie(config-if)# exit
Ruijie(config)# interface GigabitEthernet 0/2
Ruijie(config-if)# ip address 2.2.2.2 255.255.255.0
Ruijie(config-if)# ip access-group 101 in
Ruijie(config-if)# ip access-group 101 out
```

按照要求，配置一个编号为 101 的扩展访问列表

```
Ruijie(config)# access-list 101 permit tcp 192.168.12.0 0.0.0.255 any eq telnet time-range check
Ruijie(config)# access-list 101 deny icmp 192.168.12.0 0.0.0.255 any
Ruijie(config)# access-list 101 deny ip 2.2.2.0 0.0.0.255 any
Ruijie(config)# access-list 101 deny ip any any
```

配置 Time-Range 时间区

```
Ruijie(config)# time-range check
Ruijie(config-time-range)# periodic weekdays 8:30 to 17:30
```

说明：

访问列表 101 最后一条规则语句 access-list 101 deny ip any any 可以不要，因为访问列表最后隐含一条拒绝所有的规则语句。

Switch A 的配置：

```
Ruijie(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
```

30.3. MAC 扩展访问列表的配置

要在设备上配置 MAC 访问列表，必须给协议的访问列表指定一个唯一的名称或编号，以便在协议内部能够唯一标识每个访问列表。下表列出可以使用编号来指定 MAC 访问列表编号范围。

协议	编号范围
MAC 扩展访问列表	700-799

30.3.1. 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。

30.3.2. 配置 MAC 扩展访问列表

MAC 访问列表的配置包括以下两步：

1. 定义 MAC 访问列表
2. 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	功能
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**	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	功能
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** Ruijie(config)# **interface** *interface*	退出访问控制列表模式，选择选择要应用访问列表的接口
Ruijie(config-if)# **mac access-group** {*id* | *name*} **in**	将访问列表应用特定接口

说明：

方式一只对数值 ACL 进行配置；方式二可以对命名和数值 ACL 进行配置，还可以指定表项的优先级(支持优先级 ACE 产品)

注意：

S23 系列交换机对 *ethernet-type* = xns-idp (*0x0600)类型的报文无法生效。*

30.3.3. 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：

```
Ruijie# show access-lists [ id | name]
```

可以查看基本访问列表

30.3.4. MAC 扩展访问列表示例

要求通过配置 MAC 访问列表，实现以下安全功能：

- 使用 IPX 协议的主机 0013.2049.8272 不能访问设备 giga 0/1 端口。
- 其他可以访问

配置以太口，在以太口上应用访问列表 101,对以太口上进出的所有报文进行检查

```
Ruijie> enable
Ruijie# configure terminal
Ruijie(config)# mac access-list extended mac-list
Ruijie(config-mac-nacl)# deny host 0013.2049.8272 any ipx
Ruijie(config-mac-nacl)# permit any any
Ruijie(config-mac-nacl)# exit
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# mac access-group mac-list in
Ruijie(config-if)# end
Ruijie# show access-lists
mac access-list extended mac-list
deny host 0013.2049.8272 any ipx
permit any any
Ruijie#
```

说明:

访问列表语句 permit any any 不能不要，因为访问列表最后隐含一条拒绝所有的规则语句。

30.4. IPv6 扩展访问列表的配置

30.4.1. 配置 IPv6 扩展访问列表

IPv6 访问列表的配置包括以下两步：

1. 定义 IPv6 访问列表
2. 应用列表于特定接口(应用特例)

要配置基本访问列表，有以下方式，在 ACL 配置模式下执行以下命令：

命令	功能
Ruijie(config)# **ipv6 access-list** *name*	进入配置访问列表模式
Ruijie (config-ipv6-nacl)# [*sn*] {**permit** | **deny** }*prot* {*src-ipv6-prefix/prefix-len* | **host** *src-ipv6-addr* | **any**} {*dst-ipv6-pfix/pfix-len* | **any** | **host** *dst-ipv6-addr*} [**dscp** *dscp*] [**flow-label** *flow-label*] [**time-range** *tm-rng-name*]	为 ACL 添加表项,命令的具体内容请参见命令参考
Ruijie(config-exp-nacl)# **exit** Ruijie(config)# **interface** *interface*	退出访问控制列表模式，选择选择要应用访问列表的接口

Ruijie(config-if)**# ipv6 traffic-filter** *name* {**in** | **out**}	将访问列表应用特定接口

30.4.2. 显示 IPv6 扩展访问列表的配置

要监控访问列表，请在特权用户模式执行以下命令：

```
Ruijie# show access-lists [name]
```

此命令可以查看基本访问列表

30.4.3. IPv6 扩展访问列表示例

要求通过配置访问列表，实现以下安全功能：

- 192.168.4.12 的主机能访问设备 gi 0/1 端口。
- 其他的不能访问

```
Ruijie> enable
Ruijie# config terminal
Ruijie(config)# ipv6 access-list v6-list
Ruijie(config-ipv6-nacl)# permit ipv6 ::192:68:4:12/24 any
Ruijie(config-ipv6-nacl)# deny ipv6 any any
Ruijie(config-ipv6-nacl)# exit
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# ipv6 traffic-filter v6-list in
Ruijie(config-if)# end
Ruijie# show access-lists
ipv6 access-list extended v6-list
petmit ipv6 ::192.168.4.12 any
deny any any
Ruijie#
```

30.5. 配置 TCP Flag 过滤控制

TCP Flag 过滤特性提供了一种灵活机制，当前 TCP Flag 过滤控制支持 Match-All 选项，接收到的报文匹配到有 TCP Flag 与 ACL 表项中定义的 TCP Flag 每一位均吻合，就由 ACL 规则来检验，使用者可以定义 TCP Flag 的任意组合，用来过滤某些具有特定 TCP Flag 的报文。

例如：

permit tcp any any match-all rst

允许 TCP Flag RST 置位，其他位为 0 的报文通过。

说明：

这种过滤特性可以在命名ACL，数值ACL配置协议号为TCP的情况下可选配置。MAC 扩展和 IP 标准没有此项功能。

请按照如下步骤配置 TCP Flag

命令	功能
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** [*port*]] *destination destination-wildcard* [**operator port** [*port*]] [**match-all** *flag-name*][**precedence** *precedence*]	为 ACL 添加表项,命令的具体内容请参见命令参考
Ruijie(config-exp-nacl)# **exit** Ruijie(config)# **interface** *interface*	退出访问控制列表模式，选择选择要应用访问列表的接口
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

1) enable 权限和密码

```
Ruijie> enable
Ruijie#
```

2) 进入全局配置模式

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

3) 进入 ACL 配置模式

```
Ruijie(config)# ip access-list extended test-tcp-flag
Ruijie(config-ext-nacl)#
```

4) 添加 ACL 表项

```
Ruijie(config-ext-nacl)# permit tcp any any match-all rst
```

5) 添加 deny 表项

```
Ruijie(config-ext-nacl)# deny tcp any any match-all fin
```

6) 重复添加删除表项，

7) end

```
Ruijie(config-ext-nacl)# end
```

8) 显示

```
Ruijie# show  access-list test-tcp-flag
ip access-lists extended test-tcp-flag
10 permit tcp any any match-all rst
20 deny tcp any any match-all fin
```

30.6. 按优先级配置 ACL 表项

为了体现 ACE 的优先级，对每个 ACL 列表提出标准，以规范该 ACL 列表下的 ACE 的编排方式，采用序号的起点-增量方式，具体描述如下：

- ACE 在链表中以序号自小至大方式排列；
- 以起点序号开始，如不指定序号均以前一 ACE 的序号为基础以增量递增。
- 指定序号时将该 ACE 以排序方式插入，增量保证了在两个相邻 ACE 之间能够插入新的 ACE。
- ACL 列表指定序号起点和序号增量。

提供 **ip access-list resequence** {*acl-id*| *acl-name*} *sn-start sn-inc* 命令，相关命令见命令参考。

每运行以上命令，便对 ACL list 下的 ace 重新排列，如名字为 tst_acl 的 ACL 下 ace 序号为：

初始时

```
ace1: 10
ace2: 20
ace3: 30
```

运行 **ip access-list resequence** *tst_acl 100 3*, ACE 的序号如下

```
Ruijie(config)# ip access-list resequence tst_acl 100 3
ace1: 100
ace2: 103
ace3: 106
```

不输入 sn-num 添加 ace4 时，序号如下

```
Ruijie(config-std-nacl)# permit 。。。
ace1: 100
ace2: 103
ace3: 106
ace4: 109
```

输入 seq-num = 105 添加 ace5 时，序号如下

```
Ruijie(config-std-nacl)# 105 permit 。。。
ace1: 100
ace2: 103
ace5: 105
```

```
ace3: 106
ace4: 109
```

序号的引用是为了实现 4 中的优先级添加 ace 的方式。

删除 ACE

```
Ruijie(config-std-nacl)# no 106
ace1: 100
ace2: 103
ace5: 105
ace4: 109
```

如上序号也可以方便 ACE 的删除。

30.7. 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	功能
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)，具体可参见 time range 的配置指南
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

说明：

Time Range 名字的长度为 1－32 个字符，不能包含空格

绝对的运行时间区间只能设置一个或不设置，基于 Time Range 的应用将仅在这

个时间区间内有效

您可以设置一个或多个周期性运行的时间段。如果您已经为这个 Time Range 设置了一个运行时间区间，则将在时间区间内周期性的生效

下面的例子以时间区 ACL 应用为例，说明如何在每周工作时间段内禁止 HTTP 的数据流：

```
Ruijie(config)# time-range no-http
Ruijie(config-time-range)# periodic weekdays 8:00 to 18:00
Ruijie(config)# end
Ruijie(config)# ip access-list extended limit-udp
Ruijie(config-ext-nacl)# deny tcp any any eq www time-range
no-http
Ruijie(config-ext-nacl)# exit
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# ip access-group no-http in
Ruijie(config)# end
```

下面为 Time Range 的显示范例:

```
Ruijie# show time-range
time-range entry: no-http(inactive)
periodic Weekdays 8:00 to 18:00
time-range entry: no-udp
periodic Tuesday 15:30 to 16:30
```

30.8. 配置举例

30.8.1. 配置 TCP 单向连接

通过配置 TCP Flag 过滤实现单向 ACL 的功能。

30.8.1.1. 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。

30.8.1.2. 拓扑图

图 4

如上图所示，通过三层交换机连接两个网络，网络 A 与交换机的 G3/1 口相连，网络 B 与交换机的 G3/2 口相连。

30.8.1.3. 分析

环境要求阻止网络 B 的主机发起到网络 A 的 TCP 通信请求，只要过滤从网络 B 发起经过交换机 G3/2 口转发的 TCP 连接请求报文即可。分析 TCP 连接过程可知，TCP 初始请求报文的 TCP 首部标志字段的 SYN 置位且 ACK 标志位为 0。因此，我们可以通过配置扩展访问控制列表的 Match-all 选项，在 G3/2 端口的入口方向，对 TCP 首部 SYN 标志位置 1 且 ACK 标志位为 0 的报文进行过滤，即可实现网络 A 单向访问网络 B 的应用。

30.8.1.4. 配置步骤

1) 定义访问控制列表

进入交换机的配置模式

```
Ruijie# configure terminal
```

在配置模式下创建扩展访问列表 ACL101

```
Ruijie(config)# ip access-list extended 101
```

拒绝TCP Flag的SYN=1，且其它（包含ACK标志位）标志位为0的报文通过

```
Ruijie(config-ext-nacl)# deny tcp any any match-all syn
```

允许其它IP报文通过

```
Ruijie(config-ext-nacl)# permit ip any any
```

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
```

第31章 QOS 配置

31.1. 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。

31.1.1. QoS 基础框架

不支持 QoS 功能的设备不具有提供传输品质服务的能力，它同等对待所有的交通数据流，并不保证某一特殊的数据流会受到特殊的转发待遇。当网络带宽充裕的时候，所有的数据流都得到了较好的处理，而当网络拥塞发生的时候，所有的数据流都有可能被丢弃。这种转发策略被称做提供最佳效果服务，因为这时设备是尽最大能力转发数据，设备本身的交换带宽得到了充分的利用。

本设备支持 QoS 功能，能够提供传输品质服务。针对某种类别的数据流，您可以为它赋予某个级别的传输优先级，来标识它的相对重要性，并使用设备所提供的各种优先级转发策略、拥塞避免等机制为这些数据流提供特殊的传输服务。配置了 QoS 的网络环境，增加了网络的性能可预知性，并能够有效地分配网络带宽，更加合理地利用网络资源。

本设备的 QoS 实现以 IETF（Internet Engineering Task Force） 的 DiffServ（Differentiated Servece Mode），差分服务模型） 体系为基础。DiffServ 体系规定网络中的每一个传输报文将被划分成不同的类别，分类信息被包含在了 IP 报文头中，DiffServ 体系使用了 IPv4 报文头中的 TOS（Type Of Service）或者 Ipv6 报文头中的 Traffic Class 字段的前 6 个比特来携带报文的分类信息。当然分类信息也可以被携带在链路层报文头上。一般地，附带在报文中的分类信息有：

- 携带在 802.1Q 帧头的 Tag Control Information 中的前 3 个比特，它包含了 8 个类别的优先级信息，通常称这三个比特为 User Priority bits。

- 携带在 IPv4 报文头中的 TOS 或者 IPv6 报文头中的 Traffic Class 字段的前 3 个比特，称作 IPprecedence value；或者携带在 IPv4 报文头中的 TOS 或者 IPv6 报文头中的 Traffic Class 字段的前 6 个比特，称作 Differentiated Services Code Point (DSCP) value。

在遵循 DiffServ 体系的网络中，各设备对包含相同分类信息的报文采取相同的传输服务策略，对包含不同分类信息的报文采取不同的传输服务策略。报文的分类信息可以由网络上的主机、设备或者其它网络设备赋予。可以基于不同的应用策略或者基于报文内容的不同为报文赋予类别信息。识别报文的内容以便为报文赋予类别信息的做法往往需要消耗网络设备的大量处理资源，为了减少骨干网络的处理开销，一般这种赋予类别信息的方式都使用在网络边界。设备根据报文所携带的类别信息，为各种交通流提供不同的传输优先级，或者为某种交通流预留带宽，或者适当地丢弃一些优先级较低的报文、或者采取其他一些操作等等。这些独立设备的这种行为在 DiffServ 体系中被称作每跳行为（Per-hop Behavior）。

如果网络上的所有设备提供了一致的每跳行为，那么对于 DiffServ 体系来说，这个网络就可以构成 End-to-end QoSsolution。

31.1.2. QOS 处理流程

31.1.2.1. Classifying

Classifying 即分类，其过程是根据信任策略或者根据分析每个报文的内容来确定将这些报文归类到以 CoS 值来表示的各个数据流中，因此分类动作的核心任务是确定输入报文的 CoS 值。分类发生在端口接收输入报文阶段，当某个端口关联了一个表示 QoS 策略的 Policy-map 后，分类就在该端口上生效，它对所有从该端口输入的报文起作用。

对于一般非 IP 报文，设备将根据以下准则来归类报文：

- 如果报文本身不包含 QoS 信息，即报文的第二层报文头中不包含 User Priority bits，那么可以根据报文输入端口的缺省 CoS 值来获得报文的 QoS 信息。端口的缺省 CoS 值和报文的 User Priority bits 一样，取值范围为 0～7。

- 如果报文本身包含 QoS 信息，报文的第二层报文头中包含 User Priority bits，那么可以直接从报文中获得 CoS 值。

说明：

以上两种归类准则只有当端口的 QoS 信任模式打开的时候才起作用。打开端口的 QoS 的信任模式意味着不通过分析报文的内容，而直接从报文中或报文的输入端口上获得报文 QoS 信息。

- 如果端口关联的 Policy-map 中使用了基于 Mac access-list extended 的 ACLs 归类，那么在该端口上，将通过提取报文的源 MAC 地址、目的 MAC 地址以及 Ethertype 域来匹配关联的 ACLs，以确定报文的 DSCP 值。要注意的是，如果端口关联了某个 Policy-map，但又没有为其设置相应的 DSCP 值，则设备将按照缺省行为为符合这种归类的报文分配优先级：即根据报文第二层报文头中包含的优

先级信息或端口的缺省优先级。

说明:

上面三种归类准则可能会同时作用于一个端口上。在这种情况下，上面三种归类准则按 3、2、1 的优先级起作用。即先根据 ACLs 归类，在归类失败的情况下，才有可能选择归类准则2、1，在这个时候，如果端口的QoS信任模式打开，则根据准则 2 和 1 直接从报文中或者从端口上获得 QoS 信息；如果端口的 QoS 信任模式关闭，那么那些归类失败的报文将被赋予 DSCP 的缺省值 0。

对于 IP 报文，可以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。

31.1.2.2. Policing

Policing 即策略，发生在数据流分类完成后，用于约束被分类的数据流所占用的传输带宽。Policing 动作检查被归类的数据流中的每一个报文，如果该报文超出了作用于该数据流的 Police 所允许的限制带宽，那么该报文将会被做特殊处理，它或者要被丢弃，或者要被赋予另外的 DSCP 值。

在 QoS 处理流程中，Policing 动作是可选的。如果没有 Policing 动作，那么被分类的数据流中的报文的 DSCP 值将不会作任何修改，报文也不会在送往 Marking 动作之前被丢弃。

31.1.2.3. Marking

Marking 即标识，经过 Classifying 和 Policing 动作处理之后，为了确保被分类报文对应 DSCP 的值能够传递给网络上的下一跳设备，需要通过 Marking 动作将为报文写入 QoS 信息，可以使用 QoS ACLs 改变报文的 QoS 信息，也可以使用 Trust 方式直接保留报文中 QoS 信息，例如，选择 Trust DSCP 从而保留 IP 报文头的 DSCP 信息。

31.1.2.4. Queueing

Queueing 即队列，负责将数据流中报文送往端口的某个输出队列中，送往端口的不同输出队列的报文将获得不同等级和性质的传输服务策略。

每一个端口上都拥有 8 个输出队列，通过设备上配置的 DSCP-to-CoS Map 和 Cos-to-Queue Map 两张映射表来将报文的 DSCP 值转化成输出队列号，以便确定报文应该被送往的输出队列。

31.1.2.5. Scheduling

Scheduling 即调度，为 QoS 流程的最后一个环节。当报文被送到端口的不同输出队列上之后，设备将采用 WRR 或者其它算法发送 8 个队列中的报文。

可以通过设置 WRR 算法的权重值来配置各个输出队列在输出报文的时候所占用的每循环发送报文个数,从而影响传输带宽。或通过设置 DRR 算法的权重值来配置各个输出队列在输出报文的时候所占用的每循环发送报文字节数,从而影响传输带宽。

31.2. 配置 QOS

31.2.1. 缺省 QOS 设置

用户在进行 QoS 配置之前，需要清楚和 QoS 有关的几点信息，如下：

- 一个接口最多关联 1 个 Policy-map
- 一个 Policy-map 可以拥有多个 Class-map
- 一个 Class-map 最多关联 1 个 ACL，该 ACL 的所有 ACE 必须具有相同过滤域模板
- 一个接口上关联的 ACE 的个数服从“配置安全 ACL”章节的限制

缺省情况下，QoS 功能是关闭的，即设备对所有的报文同等处理。但当您将一个 Policy Map 关联到某一个接口上，并设置了接口的信任模式时，该接口的 QoS

功能即被打开。要关闭该接口的 QoS 功能，您可以通过解除该接口的 Policy Map 设置，并将接口的信任模式设为 Off 即可。以下为 QOS 的缺省配置：

缺省 CoS 值	0
队列个数	8
队列轮转算法	WRR
QueueWeight	1:1:1:1:1:1:1:1
WRR Weight Range	1:15
DRR Weight Range	1:15
信任模式	No Trust

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

31.2.2. 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	说明
configure terminal	进入配置模式
interface *interface*	进入接口配置模式
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

no mls qos cos	默认的缺省 CoS 值

下面的例子将接口 Interface g0/4 缺省 CoS 值设置为 6

```
Ruijie# configure terminal
Ruijie(config)# interface g 0/4
Ruijie(config-if)# mls qos cos 6
Ruijie(config-if)# end
Ruijie# show mls qos interface g 0/4
Interface: GigabitEthernet 0/4
Attached input  policy-map:
Default COS: trust dscp
Default COS: 6
Ruijie#
```

31.2.3. 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	说明
configure terminal	进入配置模式
ip access-list extended {*id* | *name*} **…** **ip access-list standard** {*id* | *name*} **…** **mac access-list extended** {*id* | *name*} **…** **ipv6 access-list extended** *name* **…** **access-list** *id* [**…**]	创建 ACL 请参见 ACL 章节
[**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
[**no**] **match access-group** {*acl-num* | *acl-name* }	设置匹配 ACL，acl-name 为已经创建的 ACL 名字，acl-num 为已经创建的 ACL id，no 选项删除该匹配

例如，以下设置步骤创建了一个名为 Class1 的 Class-map，它关联一个 ACL:acl_1。这个 Class-map 将分类所有端口号为 80 的 TCP 报文

```
Ruijie(config)# ip access-list extended acl_1
Ruijie(config-ext-nacl)# permit tcp any any eq 80
Ruijie(config-ext-nacl)# exit
Ruijie(config)# class-map class1
```

```
Ruijie(config-cmap)# match access-group acl_1
Ruijie(config-cmap)# end
```

31.2.4. 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	说明
configure terminal	进入配置模式
[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
[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
[no]set ip dscp new-dscp	为该数据流中的 IP 报文设置新的 ip dscp 值；对于非 IP 报文，该设置不起作用； new-dscp 是要设置的新 DSCP 值，取值范围依产品不同而不同
police rate-bps burst-byte [exceed-action {drop | dscp dscp-value}] **no police**	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

说明：

若同一个 Policy Maps 被应用到多个接口上，则其中的 police 设置的速率带宽是多个接口共享的。要达到一个接口独占 Policy Maps 中的 police 设置的速率带宽，可通过配置一个被接口唯一关联的 Policy Maps（只需要 Policy Maps 的名称与其它的不一样，其关联的 Class 都可以和其它一样）。

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
```

31.2.5. 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	说明
configure terminal	进入配置模式
interface *interface*	进入接口配置模式
[**no**] **service-policy input policy-map-name**	将创建的 Policy Map 应用到接口上；policy-map-name 是已经创建的 policy map 的名字，input 为输入限速

31.2.6. 配置输出队列调度算法

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	说明
configure terminal	进入配置模式
mls qos scheduler wrr	**wrr** 为带帧数量权重轮转调度
no mls qos scheduler	恢复为缺省 **wrr** 调度

31.2.7. 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	说明
configure terminal	进入配置模式

wrr-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
no wrr-queue bandwidth	no 选项恢复权重的缺省值

下面的例子将 wrr 调度权重设置为 1:2:3:4

```
Ruijie# configure terminal
Ruijie(config)# wrr-queue bandwidth 1 2 3 4
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)#
```

31.2.8. 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	说明
configure terminal	进入配置模式

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。
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
```

31.2.9. 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	说明
configure terminal	进入配置模式

mls qos map cos-dscp *dscp1...dscp8* **no mls qos map cos-dscp**	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

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
```

31.2.10. 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	说明
configure terminal	进入配置模式
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；
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
```

31.2.11. 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	说明
configure terminal	进入配置模式
interface *interface*	进入接口配置模式
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 猝发流量限制值(Kbyte)
no rate-limit	取消端口限速

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/4
Ruijie(config-if)# rate-limit input 100 100
Ruijie(config-if)# end
Ruijie#
```

31.3. QOS 显示

31.3.1. 显示 class-map

您可以通过以下步骤显示 class-map 内容

命令	说明
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#
```

31.3.2. 显示 policy-map

您可以通过以下步骤显示 Policy-map 内容

命令	说明
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#
```

31.3.3. 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	说明
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 COS: trust dscp
Default COS: 6
Ruijie#show mls qos interface policers
Interface: GigabitEthernet 0/4
Attached input  policy-map: pp
Ruijie#
```

31.3.4. 显示 mls qos queueing

您可以通过以下步骤显示 qos 队列信息

命令	说明
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
```

31.3.5. 显示 mls qos scheduler

您可以通过以下步骤显示 QOS 调度方式

命令	说明
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#
```

31.3.6. 显示 mls qos maps

您可以通过以下步骤显示 **mls qos maps** 对应表

命令	说明
show mls qos maps [cos-dscp |dscp-cos]	显示 **dscp-cos maps dscp-cos 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
```

31.3.7. 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	说明
show mls qos rate-limit [**interface** *interface*]	显示[端口] 速率限制

```
Ruijie# show mls qos rate-limit
Interface: GigabitEthernet 0/4
rate limit input bps = 100 burst = 100
```

31.3.8. 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	说明
show policy-map interface *interface*	显示[端口] policymap 配置

```
Ruijie# show policy-map interface f0/1
FastEthernet 0/1  input (tc policy): pp
Class cc
set ip dscp 22
mark count 0
```

说明:

交换机设备目前不支持 mark count 的统计

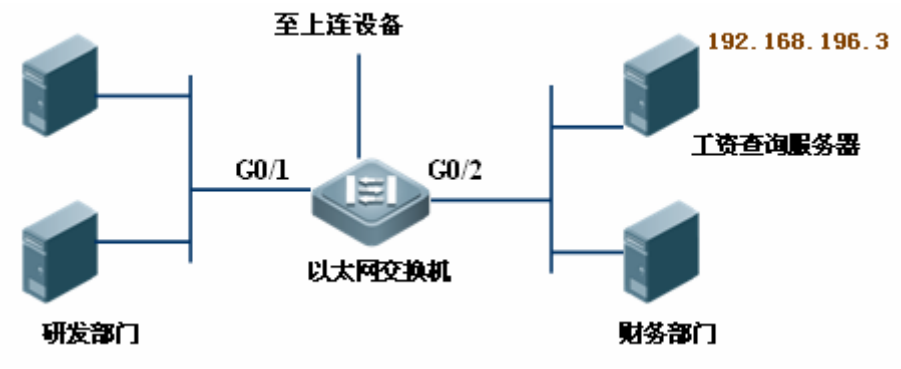
31.4. QOS 配置用例

31.4.1. 基于分类报文的流量限速

31.4.1.1. 应用需求

公司内网通过以太网交换机实现各部门之间的互连，其中财务部门由交换机的 G0/2 端口接入。现要求限制该部门工资查询服务器向外发送的最大流量不超过 512Kbps，并且对超出规格的流量做丢弃处理。

31.4.1.2. 拓扑图



31.4.1.3. 配置步骤

说明:

以下配置过程只列出了与 QOS ACL 相关的配置命令

#进入全局配置模式

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

#定义名为 salary_acl 的标准 ACL

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

#定义规则，允许工资服务器的流量

```
Ruijie(config-std-nacl)#permit host 192.168.217.223
```

#退回到全局配置模式

```
Ruijie(config-std-nacl)#exit
```

#创建名为 salaryclass 的 class map，进入 class-map 配置模式

```
Ruijie(config)#class-map salaryclass
```

#定义匹配的规则

```
Ruijie(config-cmap)#match access-group salary_acl
```

#退回到全局配置模式

```
Ruijie(config-cmap)#exit
```

#创建名为 salarypolicy 的策略，进入 policy-map 配置模式

```
Ruijie(config)#policy-map salarypolicy
```

#指定该策略执行的分类规则为 salaryclass

```
Ruijie(config-pmap)#class salaryclass
```

#限制工资查询服务器向外发送的最大流量不超过 512Kbps，猝发流量限制值为 32 Kbyte，并且对超出规格的流量做丢弃处理。

```
Ruijie(config-pmap-c)#police 512 32  exceed-action drop
```

#退回到 class-map 配置模式

```
Ruijie(config-pmap-c)#exit
```

#退回到全局配置模式

```
Ruijie(config-pmap)#exit
```

#进入 G0/2 的接口配置模式

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

#把 salarypolicy 策略应用在 G0/2 口的入口方向

```
Ruijie(config-if)#service-policy input salarypolicy
```

#退回到特权模式

```
Ruijie(config-if)#end
```

#在特权模式下用 show 命令查看相应的配置

```
Ruijie#show mls qos interface policers
Interface: GigabitEthernet 0/2
Attached input  policy-map: salarypolicy
Ruijie#show policy-map salarypolicy
 Policy Map salarypolicy
    Class salaryclass
```

```
     police 512 32 exceed-action drop

Ruijie#show class-map salaryclass
 Class Map salaryclass
   Match access-group salary_acl

Ruijie#show access-lists salary_acl
ip access-list standard salary_acl
 10 permit host 192.168.217.223
```

第32章 RLDP 配置

32.1. RLDP 概述

32.1.1. 理解 RLDP

RLDP 全称是 Rapid Link Detection Protocol，是我司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：

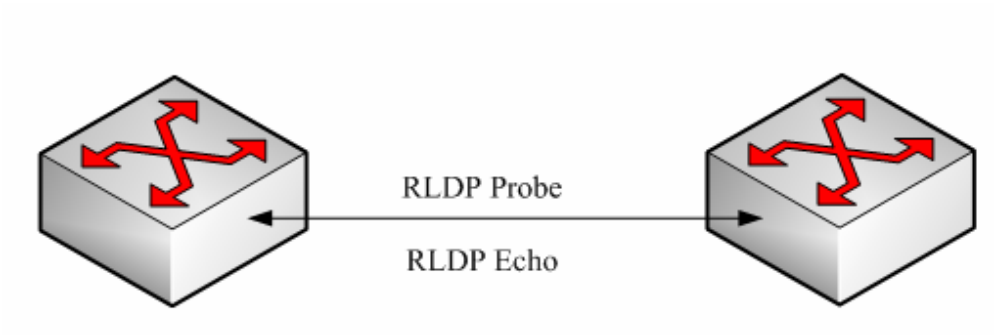


图 1

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。

说明：

要使用 RLDP 的单向检测和双向检测功能，必须保证链路两端的端口都打开了RLDP，并且不允许一个开启了RLDP的端口下连多个邻居端口，否则RLDP无法检测出每个邻居的链路健康状况。

32.1.2. 典型应用

环路检测：

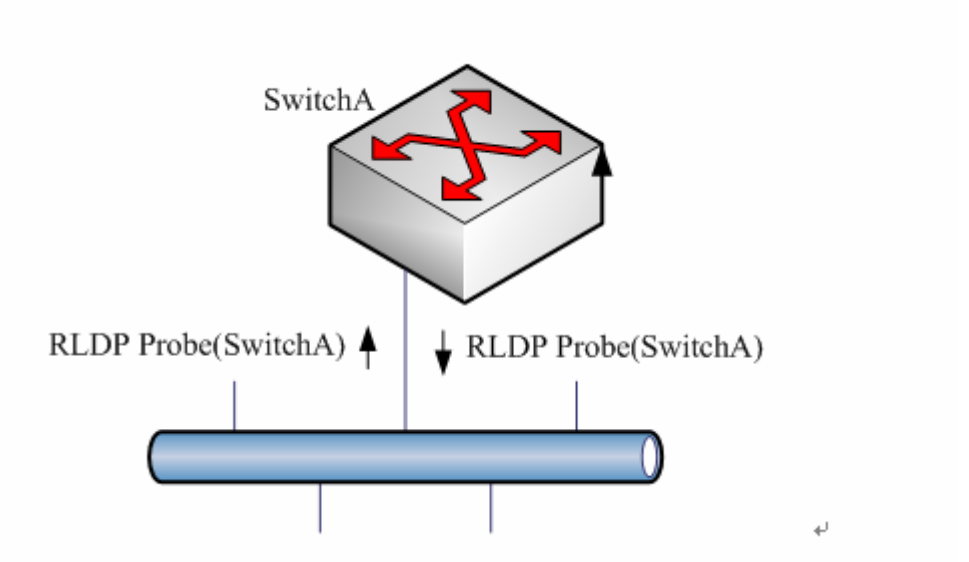


图 2 环路检测

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。

单向链路检测：

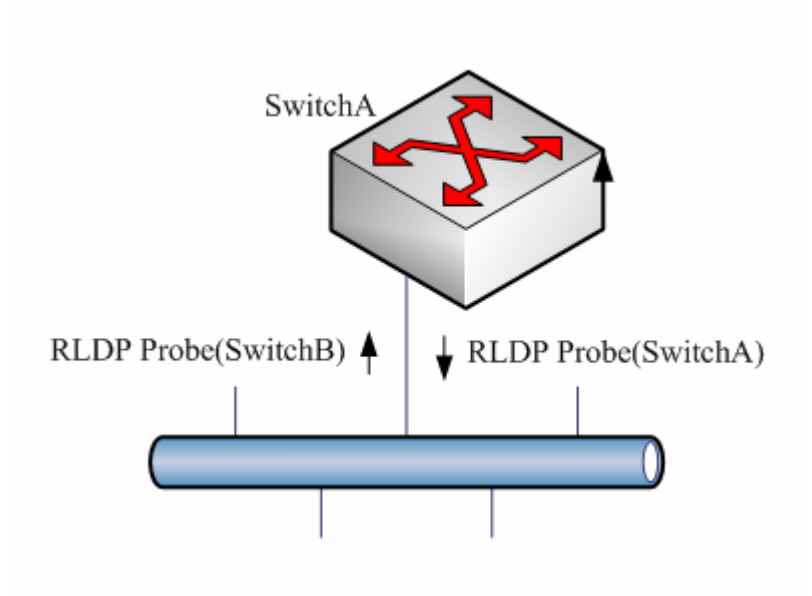


图 3 单向链路检测

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。

双向链路检测：

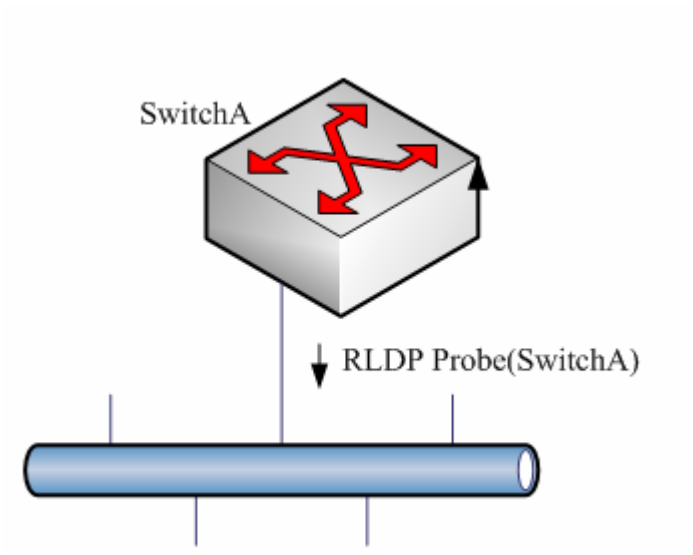


图 4 双向链路检测

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。

说明:

如果链路两端有某一方未开启 RLDP 也会被诊断为双向或单向链路故障，因此配置双向链路检测或单向链路检测时需要管理员保证链路两端都开启了 RLDP，以避免出现错误的诊断信息。

32.2. 配置 RLDP

我们将从以下几个章节描述如何配置 RLDP

- RLDP 的默认值
- 配置全局 RLDP
- 配置端口 RLDP
- 配置 RLDP 的探测间隔
- 配置 RLDP 的最大探测次数
- 恢复端口的 RLDP 状态

32.2.1. RLDP 的默认值

全局 RLDP 状态	DISABLE
端口 RLDP 状态	DISABLE
探测间隔	2S
最大探测次数	3 次

注意:

- RLDP 只能基于交换口(包括 AP)和路由口进行配置。
- RLDP 帧都是 untag。
- RLDP 故障处理类型中的 block 功能需要和 STP 互斥。也就是说如果用户配置了端口的故障处理类型为 blcok，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。

32.2.2. 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。

32.2.3. 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。

以下例子是在 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)# rldp port unidirection-detect shutdown-svi
Ruijie(config-if)# rldp port bidirection-detect warning
Ruijie(config-if)# rldp port loop-detect block
Ruijie(config-if)# end
```

```
Ruijie# show rldp interface gigabitEthernet 0/5
port state     : normal
local bridge   : 00d0.f822.33ac
neighbor bridge : 0000.0000.0000
neighbor port   :
unidirection detect information:
action : shutdown svi
state  :  normal
bidirection detect information :
action : warnning
state  :  normal
loop detect  information    :
action : block
state  :  normal
```

配置端口检测有几个注意点：

- 路由口不支持 shutdown-svi 的错误处理方法，因此该方法在路由口发生检测错误时将不被执行。
- 配置环路检测时要求端口下连的邻居设备不能开启 RLDP 检测，否则该端口将无法做出正确的检测。
- 如果在 aggregate port 上配置了 block 方法并且端口发生了链路检测错误，则在端口重新恢复检测前不要变更该 aggregate port 的成员口关系，否则成员口的转发状态将会和实际的设置效果不一致。
- 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。
- 受硬件芯片的限制，某些产品对于 block 的端口仍然会将报文送 cpu,这样在指定环路检测为 block 的处理方式，设备检测出环路并将端口 block 处理时，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。

32.2.4. 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。

32.2.5. 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。

说明：

最多探测次数只有在单向链路检测和双向链路检测下才会起作用，如果某个端口只开启了环路检测，该值将失效。

32.2.6. 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。

说明：

用户也可以在全局配置模式下使用 **errdisable recover** 命令来即时或定时重新启动被 rldp 设置成违例的端口（即采用 shutdown-port 检测方式而处于错误状态的端口）的 RLDP 检测。需要注意的是，当配置了 rldp 的端口间不是线路直连的时候，也就是说中间还有一些中继设备，此时如果使用 **errdisable revover interval** 来

定时恢复故障，需要将 rldp 的检测时间配置成大于 **errdisable recover interval** 的值，也就是 detect-interval* detect-max 的总时间要大于 **errdisable recover interval** 的值,以避免错误的判断。

32.3. 查看 RLDP 信息

锐捷提供的可查看的相关 RLDP 的信息如下：

- 查看所有端口的 RLDP 状态
- 查看指定端口的 RLDP 状态

32.3.1. 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  : 2
rldp max hello     : 3
rldp local bridge   : 00d0.f8a6.0134
------------------------------------------------
interface GigabitEthernet 0/1
port state:normal
neighbor bridge : 00d0.f800.41b0
neighbor port   : GigabitEthernet 0/2
unidirection detect information:
action : shutdown svi
state  : normal
interface GigabitEthernet 0/24
port state:error
neighbor bridge : 0000.0000.0000
neighbor port   :
bidirection detect information :
action : warnning
```

```
state  : error
```

从上述信息可以看到，端口 GigabitEthernet 0/1 配置了单向检测，并且当前未检测到错误，端口状态为正常(normal)。端口 GigabitEthernet 0/24 配置了双向检测，并且检测到了双向故障。

32.3.2. 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
Ruijie**# 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。

第33章 TPP 配置

33.1. TPP 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。

33.2. TPP 应用

拓扑防护主要是针对 MSTP 或 VRRP 以及其他分布式网络协议可能造成的网络拓扑振荡而产生的。MSTP 或 VRRP 等协议均使用定时报文通告机制来自动维护网络拓扑结构，自动适应网络中的拓扑变化。这也造成了网络拓扑易受攻击，当受到人为的网络攻击时，因 CPU 利用率过高或帧通路阻塞等原因，可能造成定时报文的短暂中断，从而造成网络拓扑发生错误的振荡，这给网络的正常通信造成极大危害。而拓扑防护功能正是为了最大限度的防止这种不必要的网络振荡，它与其他分布式协议（MSTP、VRRP 等）协同工作，从而使网络更加稳定、可靠。

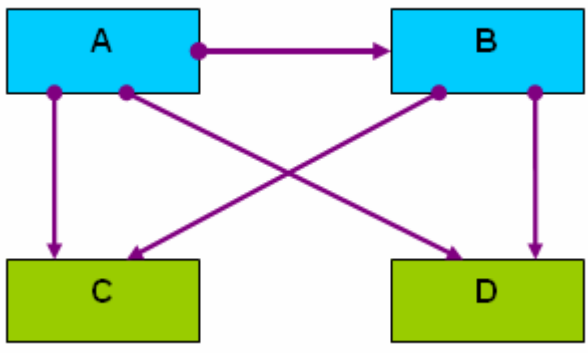


图 1

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。

33.3. TPP 配置

TPP 配置包括全局功能配置和端口功能配置。全局功能配置用于使能设备的拓扑防护功能，默认情况下，全局拓扑防护功能使能，这时它会检测本地和邻居设备的运行情况，对产生的异常情况进行处理。不过它不会向邻居设备通告本地的运行情况。端口功能配置用于使能端口的拓扑防护功能，端口的拓扑防护功能使能时，表示对端的邻居设备关心本地设备的运行情况，因此当本地设备发生异常时，将通告该端口的对端邻居设备。默认情况下，所有端口的拓扑防护功能关闭。

说明：

拓扑防护功能适用于点对点链路的网络，且相邻网络设备都必须使能拓扑防护功能。另外，部署 TPP 功能时，通常需要通过 cpu topology-limit 命令配置 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。

33.3.1. 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> **enable**	进入特权命令模式
Ruijie**# config terminal**	进入全局配置模式
Ruijie(config)**# topology guard**	使能全局拓扑防护
Ruijie(config)**# end**	退回特权命令模式

Ruijie**# copy running-config startup-config**	保存配置

使用 **no topology guard** 禁止设备的全局拓扑防护功能

33.3.2. 配置端口拓扑防护

配置命令如下：

命令	作用
Ruijie> **enable**	进入特权命令模式
Ruijie**# config terminal**	进入全局配置模式
Ruijie(config)# **interface gi** *0/1*	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
Ruijie(config-if)**# end**	退回特权命令模式

使用 **no tp-guard port enable** 禁止端口的拓扑防护，该命令只适用于二层交换口和路由口。不适用于 AP 成员口。

说明：

全局拓扑防护作为拓扑防护的全局开关，当全局拓扑防护使能时，设备会检测本设备的运行参数，同时监听各个邻居设备的运行参数，但当本地出现异常现象时，它不会向邻居设备发送异常通告报文进行通告。端口的拓扑防护功能使能时，当本地出现异常现象时，会向该端口对端的邻居设备发送异常通告报文进行异常通告。

33.4. TPP 典型配置举例

如下图为双核心组网拓扑图：

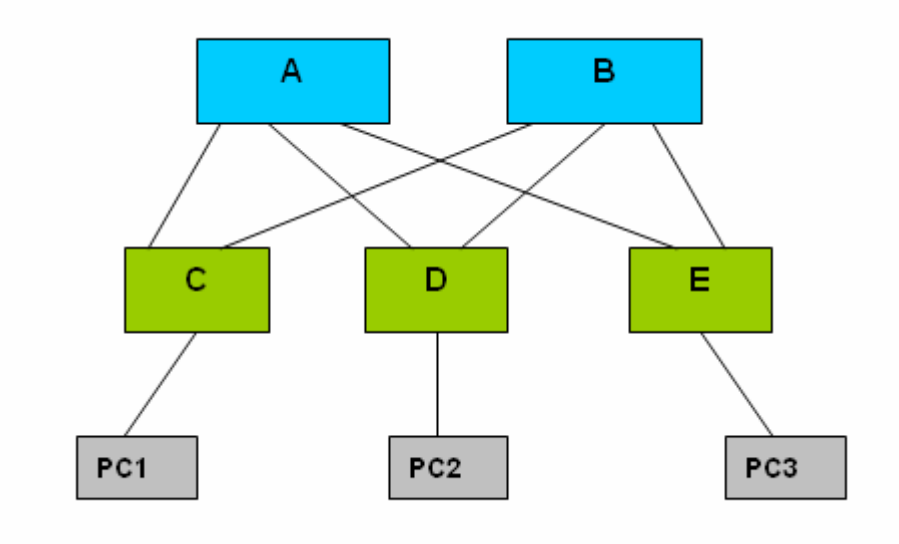


图 2

图中 A、B 为三层汇聚设备，C、D 和 E 为二层接入设备。

三层汇聚设备 A、B 和二层接入设备 C、D 和 E 均开启 MSTP，同时两台三层汇聚设备开启 VRRP 协议。拓扑防护功能使 MSTP 和 VRRP 运行更加稳定，避免网络拓扑发生不必要的振荡。

对于三层汇聚设备 A、B 使能全局拓扑防护功能，同时使能各个端口的拓扑防护功能。对于各台二层接入设备 C、D 和 E 使能全局拓扑防护功能。

33.5. 查看 TPP 信息

我们提供的可查看的 TPP 的相关信息如下：

查看设备的 TPP 配置及状态

33.5.1. 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。

```
Ruijie #show tpp
tpp state        : enable
tpp local bridge  : 00d0.f822.35ad
-----------------------------------
```

第34章 文件系统配置

34.1. 概述

所谓文件系统是指一个负责存取和管理辅助存储设备上文件信息的机构，交换机提供了串行 Flash 作为辅助存储器，用于存储和管理交换机的网络操作系统文件，以及一些交换机的配置文件。

文件数据在串行 Flash 上是以日志的格式保存的，每个文件都有一个文件头记录该文件的基本信息。当存储器被写满而无空间再去进行其他操作时，文件系统将自动整理碎片以及垃圾回收，以达到提供足够的空间进行文件操作，这个时间是相当快的，通常察觉不到，为了充分的利用有限的空间，文件系统还提供了数据压缩的功能以及数据节点索引信息。

34.2. 配置文件系统

我们将从以下几个小节描述如何配置文件系统：

- 切换目录
- 复制文件
- 显示目录内容
- 格式化系统
- 创建目录
- 移动文件
- 显示当前工作路径
- 删除文件
- 删除空目录

34.2.1. 文件系统配置指导

命令关键字对大小写不敏感，文件名对大小写敏感，最长文件名为 4096。

所有的文件名以及路径信息均不支持通配符操作。

注意:

强烈建议在拥有大flash存储空间的设备上，文件系统使用不超过128M的空间；否则，系统会明显的减慢启动速度，另外，在特权模式下首次执行查看文件命令**dir**的等待时间会显著增长。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。

34.2.2. 切换目录

从当前目录切入到指定目录。

在特权用户模式下，按如下步骤使用该命令：

命令	作用
Ruijie# **cd** *directroy*	进入指定的 directory 目录。
Ruijie# **cd** *../*	进入上一级目录
Ruijie# **cd** *./*	进入本级目录

以下例子是进入根目录下的 MNT 目录的 Document 目录：

```
Ruijie# cd mnt/document
```

之后再进行的操作将在 MNT/Document 目录下进行

34.2.3. 复制文件

复制文件到一个目录中或者一个文件中。

在特权用户模式下，按如下步骤配置 **copy** 命令可以实现文件到目录或文件到文件的拷贝：

命令	作用
Ruijie# **copy flash:** *filename* **flash:** *directoryname*	将文件复制到指定的目录中。
Ruijie# **copy flash:** *filename* **sour** *directoryname*	复制文件到指定的文件中。

以下是分别拷贝到一个目录和拷贝到一个文件的实例：

```
Ruijie# copy flash:config.tex flash:tmp/
Ruijie# copy flash:con_bak.txt flash:config.text
```

34.2.4. 显示目录内容

显示当前工作目录下或者指定目录下的信息：

命令	作用
Ruijie# **dir**	显示当前目录下的内容。

Ruijie# **dir** *directory*	显示指定目录的内容。

以下例子是显示当前目录内容和指定目录内容的举例：

```
Ruijie# dir
Ruijie# dir ../bak
```

34.2.5. 格式化系统

在特权用户模式下，按照下面的配置命令格式可以格式化文件系统要管理和操作的设备：

命令	作用
Ruijie# **makefs dev** *devname* **fs** *fs_name*	为名字为 *fs_name* 的文件系统格式化名字为 **dev** 设备。

以下例子是格式化 dev 目录下的第一个 MTD 设备，供 JFFS2 文件系统使用：

```
Ruijie# makefs dev/dev/mtd/mtdblock/1 fs jffs2
```

按照上面的配置将为 JFFS2 文件系统格式化 MTDBLOCK 目录下的一个设备，清空设备的数据供文件系统使用。

34.2.6. 创建目录

在特权用户模式下，按如下步骤在指定的位置创建需要的目录：

命令	作用
Ruijie# **mkdir** *directoryname*	创建目录

以下例子是在根目录下面创建一个 BAK 目录：

```
Ruijie# mkdir bak
```

34.2.7. 移动文件

在特权用户模式下，将指定的文件移动到指定的目录或者文件：

命令	作用
Ruijie# **rename flash:** *old_filename* **flash:** *new_filename*	将名字为 *old_filename* 文件命名成名字为 *new_filename* 的文件。

34.2.8. 显示当前工作路径

在特权用户模式下，按如下步骤设置可以显示当前的工作路径信息：

命令	作用
Ruijie# **pwd**	显示当前的工作路径信息

34.2.9. 删除文件

在特权用户模式下，按如下步骤设置来完成永久删除一个文件的功能：

命令	作用
Ruijie# **del** *filename*	删除指定的文件。

下面的例子是删除 MNT 目录下一个叫做 large.c 的临时文件：

```
Ruijie# del mnt/large.c
```

34.2.10. 删除空目录

在特权用户模式下，按如下步骤设置可以永久删除指定的空目录：

命令	作用
Red-Giant# **rmdir** *directoryname*	删除一个空目录。

以下的例子是删除一个空的目录 MNT：

```
Ruijie# rmdir mnt
```

第35章 系统日志配置

35.1. 概述

设备在运行过程中，有各种状态变化如链路状态 UP、DOWN 等，发生一些事件如收到异常报文、处理异常等。我司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。

35.1.1. 日志报文格式

我司产品的日志报文格式如下：

<priority> seq no: timestamp sysname

%ModuleName-severity-MNEMONIC: description

依次是：<优先级> 序号 时间戳 设备名 模块名-严重性-信息简写：信息内容

优先级值＝设备值＊8＋严重性

例子：

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

注意:

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。

35.2. 日志配置

35.2.1. 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

注意：

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

35.2.2. 设置日志信息显示设备

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

要设置接收日志的不同显示设备，请在全局配置模式或特权用户层下执行以下命令：

命令	作用
Ruijie(config)# **logging buffered** [*buffer-size* | *level*]	将日志记录到内存缓冲区
Ruijie# **termninal monitor**	允许日志信息显示在 VTY 窗口上
Ruijie(config)# **logging** *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

Logging Buffere：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** 。

Termninal Monitor：允许日志信息在当前 VTY(如 Telnet 窗口)上显示。
Logging Host：指定接收日志信息的 Syslog Server 地址，我司产品 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。

注意：

要将日志信息发送给 Syslog Server，必须打开日志信息的时间戳开关或序号开

关，否则日志信息将不会被发给 Syslog Server。

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

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

注意：

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。

35.2.3. 启用日志信息时间戳开关

要在日志信息上添加或取消时间戳，请在全局配置模式下执行以下命令：

命令	作用
Ruijie(config)# **service timestamps** *message-type* [**uptime** | **datetime**]	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。

注意：

如果当前设备不存在 RTC，配置设备时间无效。自动采用启机时间做为日志信息时间戳。

35.2.4. 启用日志信息系统名开关

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

命令	作用

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

35.2.5. 启用日志信息统计功能开关

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

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

35.2.6. 启用日志信息序列号开关

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

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

35.2.7. 设置日志信息显示级别

要限制在不同设备上显示的日志报文个数，可以通过设置不同设备上允许显示日志信息的严重性级别来实现。

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

我司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。

35.2.8. 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** *facility-type*	恢复日志信息的设备值为默认值。

下面是各种设备值的含义：

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

我司产品默认设备值为 23。

35.2.9. 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 报文的远端口。

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** *A.B.C.D*	设置日志报文的源 ip 地址

35.2.10. 设置发送用户 LOG 信息

默认情况下，用户登录与退出，以及执行配置命令，均不输出 LOG 信息。如果需要输出用户登录/退出的 LOG 信息，或者需要输出配置命令的 LOG 信息。请在全局配置模式下执行以下命令：

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

35.3. 日志监控

为了监控日志信息，请在特权用户模式下执行以下命令：

命令	作用
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

注意：

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

35.3.1. 日志配置举例

以下配置一个启用日志功能的一个典型例子：

```
Ruijie(config)# interface gigabitEthernet 0/1
```

```
Ruijie(config-if)# ip address 192.168.200.42 255.255.255.0
Ruijie(config-if)# exit
Ruijie(config)# service sequence-numbers                    //启用序列号
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
```

第36章 堆叠管理

36.1. 理解堆叠

36.1.1. 概述

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

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

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

36.1.2. 硬件结构

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

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

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

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

注意：

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

36.1.3. 堆叠的启动和停止

在启动阶段如果交换机的插槽内未插堆叠模块，则工作在单机模式下；如果交换

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

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

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

Device [2] loss has been detected, system will reset.
```

如果在 10 秒钟内堆叠电缆恢复连接，则堆叠环境可以恢复正常工作,系统将会发送相应的日志信息提示用户：

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

如果连接中断超过 10 秒，堆叠无法正常工作，堆叠系统会重新启动，重新建立堆叠。

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

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

注意:

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

36.2. 配置堆叠

36.2.1. 缺省配置

设备的堆叠属性缺省配置如下表所示：

属性	缺省值
堆叠口	堆叠模块
设备优先级	1
设备描述	SWITCH

36.2.2. 如何根据设备号确认堆叠成员设备

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

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

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

注意:

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

36.2.3. 配置设备优先级

在全局模式下,请使用如下命令配置:

命令	描述
Ruijie(config)# **device-priority** [*member*] *priority*	*member*:取值 1-MAX, 配置的成员设备. *priority*:取值 1-10, 指定设备的优先级 默认情况下配置的成员设备为 1

配置实例: 指定成员设备 2 的优先级为 8

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

注意:

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

36.2.4. 配置设备别名

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

命令	描述
Ruijie(config)# **device-description** [**member** *member*] *description*	*member*:取值 1-MAX，配置的成员设备. *description*:字符长度为 31，指设备的别名 默认情况下配置的成员设备为 1

配置实例: 指定成员设备 2 的别名为 red-giant

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

36.2.5. 参数保存

通过以下配置命令配置的堆叠信息将保存在所配置的成员设备中：

device-priority [*member*] *priority*
device-description [**member** *member*] *description*
stack on

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

36.3. 显示堆叠信息

在特权模式下，您可以使用如下命名显示堆叠信息

命令	描述
Ruijie# **show version devices**	显示系统设备信息
Ruijie# **show version slots**	显示插槽信息
Ruijie# **show version**	显示堆叠系统的版本信息
Ruijie# **show member** [*member*]	显示成员设备堆叠信息 *member*:取值 1-MAX,指定的成员设备

说明:

以下举例显示信息中可能含有其它产品系列的内容，具体显示信息（如产品型号、描述等）请以实际使用的设备信息为准。

实例: 显示堆叠系统的各种信息

```
Ruijie# show version devices

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


Ruijie# show version slots

   Device  Slot  Ports  Max Ports  Module
       ------  ----  -----  ---------  ----------------------------
   1       0     24     24
    M5750-24GT/12SFP_Static_Module
   1       1     1      1          M5700_STACK_IB4X
   1       2     0      1
   2       0     48     48
    M5750-48GT/4SFP_Static_Module
   2       1     1      1          M5700_STACK_IB4X
   2       2     1      1          M5700_STACK_IB4X
   3                      0                 24              24
    M5750-24GT/12SFP_Static_Module
   3       1     1      1          M5700_STACK_IB4X
   3       2     1      1          M5700_STACK_IB4X
   4                      0                 24              24
    M5750-24GT/12SFP_Static_Module
   4       1     1      1          M5700_STACK_IB4X
   4       2     1      1          M5700_STACK_IB4X
   5                      0                 24              24
    M5750-24GT/12SFP_Static_Module
   5       1     1      1          M5700_STACK_IB4X
   5       2     1      1          M5700_STACK_IB4X
   6                      0                 24              24
    M5750-24GT/12SFP_Static_Module
   6       1     1      1          M5700_STACK_IB4X
   6       2     0      1
   7                      0                 24              24
    M5750-24GT/12SFP_Static_Module
   7       1     1      1          M5700_STACK_IB4X
   7       2     1      1          M5700_STACK_IB4X
```

```
  8                    0               48              48
   M5750-48GT/4SFP_Static_Module
  8       1     1     1          M5700_STACK_IB4X
  8       2     1     1          M5700_STACK_IB4X
```

```
Ruijie# show version

System description             : Red-Giant 10G Routing
Switch(RG-S5750-24GT/12SFP) By Ruijie Network
System start time       : 2007-4-23 17:39:11
System hardware version : 1.0
System software version : RGOS 10.1.00(2), Release(12889)
System BOOT version     : 10.1.11330
System CTRL version     : 10.1.11330
System Serial Number    : 1234942570002
Device information:
 Device-1
  Hardware version : 1.0
  Software version : RGOS 10.1.00(2), Release(12889)
  BOOT version     : 10.1.11330
  CTRL version     : 10.1.11330
  Serial Number    : 1234942570002
 Device-2
  Hardware version : 1.0
  Software version : RGOS 10.1.00(2), Release(12889)
  BOOT version     : 10.1.11330
  CTRL version     : 10.1.11330
  Serial Number    : 1234942570001
 Device-3
  Hardware version : 1.0
  Software version : RGOS 10.1.00(2), Release(12889)
  BOOT version     : 10.1.11330
  CTRL version     : 10.1.11330
  Serial Number    : 1234942570003
 Device-4
  Hardware version : 1.0
  Software version : RGOS 10.1.00(2), Release(12889)
  BOOT version     : 10.1.11330
  CTRL version     : 10.1.11330
  Serial Number    : 1234942570004
 Device-5
  Hardware version : 1.0
  Software version : RGOS 10.1.00(2), Release(12889)
  BOOT version     : 10.1.11330
  CTRL version     : 10.1.11330
  Serial Number    : 1234942570005
```

```
 Device-6
  Hardware version : 1.0
  Software version : RGOS 10.1.00(2), Release(12889)
  BOOT version     : 10.1.11330
  CTRL version     : 10.1.11330
  Serial Number    : 1234942570006
 Device-7
  Hardware version : 1.0
  Software version : RGOS 10.1.00(2), Release(12889)
  BOOT version     : 10.1.11330
  CTRL version     : 10.1.11330
  Serial Number    : 1234942570007
 Device-8
  Hardware version : 1.0
  Software version : RGOS 10.1.00(2), Release(12889)
  BOOT version     : 10.1.11330
  CTRL version     : 10.1.11330
  Serial Number    : 1234942570008
```

```
Ruijie# show member

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

第37章 WEB 管理配置

37.1. 理解 WEB 管理

37.1.1. WEB 管理概述

WEB 管理通过使用浏览器如 IE 来管理网络设备，如交换机或路由器。

37.1.2. 工作原理

WEB 管理包括 WEB 服务器和 WEB 客户端两部分。WEB 服务器集成在设备上，用来接收和处理客户端发来的请求（读取 WEB 文件或执行命令请求），并把处理结果返回给客户端，WEB 客户端通常指网络浏览器，如 IE。

37.2. 缺省配置

下表用来描述 WEB 管理的缺省配置。

功能特性	缺省值
WEB 服务	关闭

说明：

如果要开启 WEB 服务，详细配置过程请看下面的“WEB 管理典型配置举例”小节。如果 WEB 配置 Enable 方法进行认证，则认证时不要输入用户名直接输入 Enable 密码进行认证。

37.3. 配置 WEB 管理

在浏览器地址栏中输入设备的管理 IP 地址，如：http://192.168.1.200,按回车后将进入如下面页：

图表 1 初始页面

选择好语言类型后点击“登录”按钮，这时会弹出认证对话框，请在此对话框中输入用户名、密码。

图表 2 登录认证对话框

认证成功后将进入 WEB 管理主页面，如下图：

图表 3 WEB 管理平台主页面

说明：

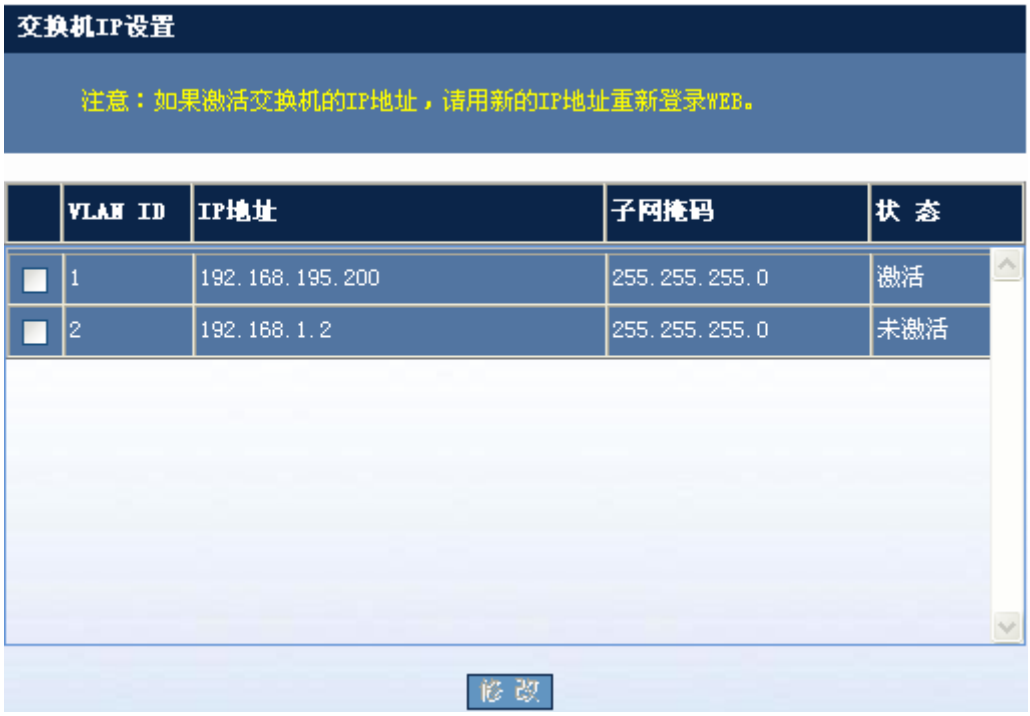
如果 WEB 管理使用 Enable 方法进行认证，则认证时，不要输入用户名直接输入 enable 密码。

37.3.1. 系统管理

37.3.1.1. 交换机 IP 设置

通过菜单“交换机 IP 设置”使用该功能。

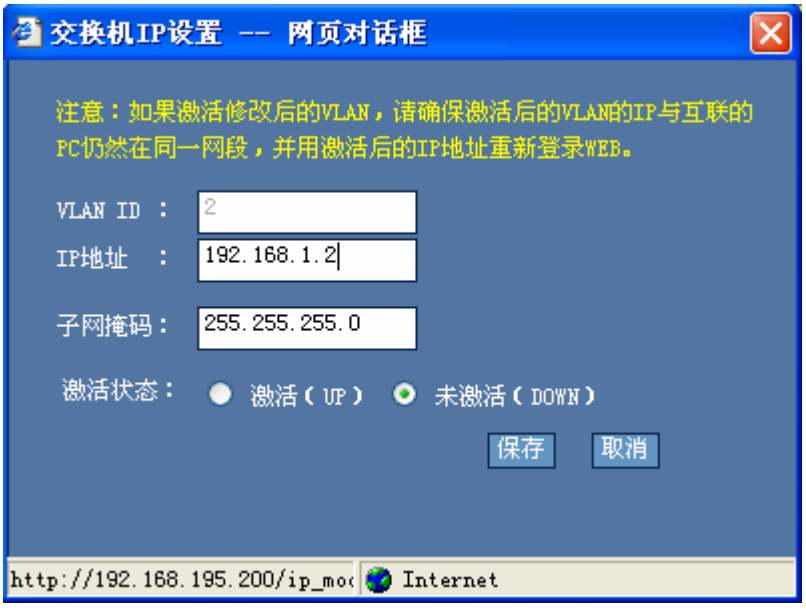
交换机 IP 设置页面：



图表 4 交换机 IP 设置

配置说明：

修改：如果要修改某个交换机 ip，请选中所对应的复选框，按“修改”按钮后，将弹出如下配置页面：



图表 5 交换机 IP 修改

用户可以对 IP 地址，子网掩码等参数进行修改，修改完后请按“保存”按钮使配置生效。

37.3.1.2. VLAN 管理

通过菜单项“VLAN 管理”使用该功能。

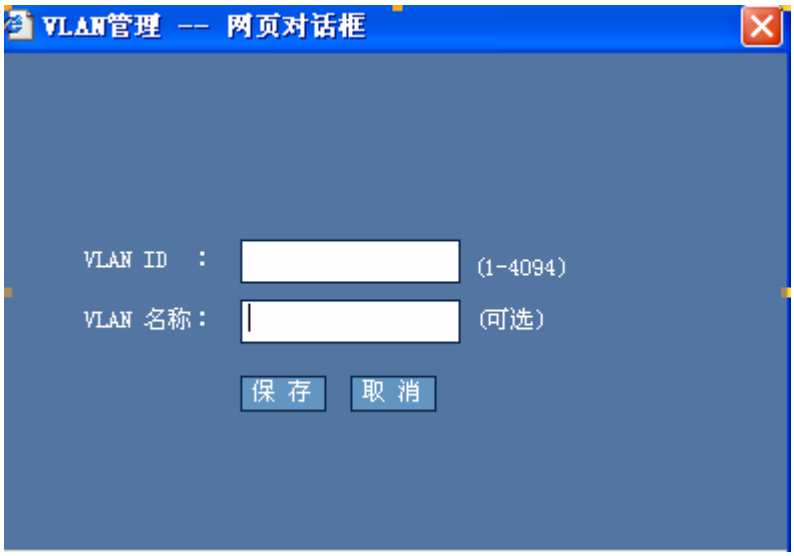
1）VLAN 管理页面

图表 6 VLAN 管理

配置说明：

进入该页面后，首先显示当前系统的 VLAN 信息。用户可以新建、删除、修改 VLAN，但默认 VLAN 不能被删除。

新建：点击“新建”按钮后，将弹出如下配置页面：

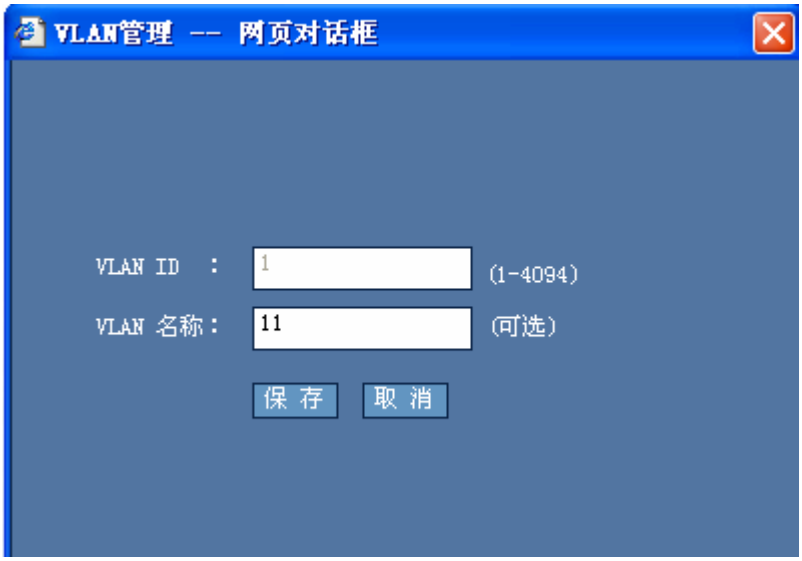


图表 7 新建 VLAN

请输入 VLAN ID 和 VLAN 名称（可选）后按“保存”按钮使配置生效。配置成功后，新建的 VLAN 将显示在 VLAN 管理页面上。

删除：如果要删除指定的 VLAN，请选中相应的复选框后按“删除”按钮使配置生效。

修改：如果要修改已配置的 VLAN，只要选中所对应的复选框后按“修改”按钮，这时将弹出如下配置页面：



图表 8 修改 VLAN

要修改的 VLAN 的信息将会显示在文本框中，这时对其修改后按“保存”按钮使配置生效。修改后的结果将显示在 VLAN 管理页面上。

2）指定 VLAN 页面

图表 9 指定 VLAN

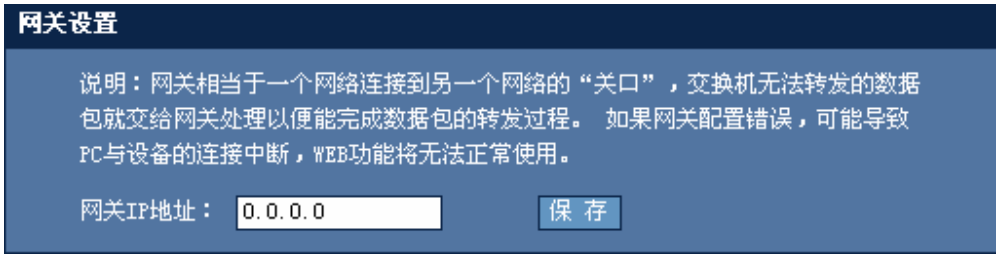
配置说明：

请指定所要设置的端口模式和 VLAN ID，当对所有端口都设置好后，请按“保存”按钮，使配置生效。

37.3.1.3. 网关设置

通过菜单项“网关设置”使用该功能。

网关设置页面：



图表 10 网关设置

配置说明：

如果交换机已配置了网关，则打开该页面后，将会在文本框中显示已配置的网关地址，如果要设置新的网关 IP 地址，只要在文本框中输入新的网关 IP 地址后，按“保存”按钮使配置生效。

37.3.1.4. 端口镜像

通过菜单项“端口镜像”使用该功能。

端口镜像设置页面：

图表 11 端口镜像设置

配置说明：

请先选择监控端口，然后再选中要被监控的端口前面的复选框按“保存”按钮使配置生效，监控端口与被监控端口不能是同一个口。按“删除端口监控”按钮，将删除端口监控配置。

37.3.1.5. 端口限速

通过菜单项“端口限速”使用该功能。

端口限速设置的主要页面：

图表 12 端口限速设置

配置说明：

请在要限速的端口相应文本框中输入限速值，一次可以对多个端口进行设置，设置好端口限速值后按“保存”按钮使配置生效。不限速的端口请保持相应的文本框为空。如果要取消所有端口的限速设置，请按“取消全部限速”按钮使配置生效。

37.3.1.6. 聚合端口

通过菜单项“聚合端口”使用该功能。

聚合端口设置页面：

图表 13 聚合端口设置

配置说明：

1）配置流量平衡算法

如果要配置流量平衡算法，请选择对应的算法选项后按“保存”按钮使配置生效。

2）配置聚合端口

如果要新建一个聚合端口，请按“新建”按钮，将弹出如下界面：

图表 14 新建聚合端口

此时，请选择成员端口并指定聚合端口号后按“保存”按钮使配置生效，如果某个成员端口已是其它聚合端口成员，则该成员端口前的复选框将不能被选中。

3）删除聚合端口

如果要删除聚合端口，请选中相应聚合端口前面的复选框后，按“删除”按钮使配置生效。

37.3.1.7. 端口设置

通过菜单项“端口设置”使用该功能。

端口设置页面：

图表 15 端口设置

配置说明：

请选择要配置的端口后对其进行设置，配置好参数后按“保存”按钮使配置生效。如果选择的参数设备不支持，对应的参数设置将不生效。

37.3.1.8. DHCP 中继

通过菜单项“DHCP 中继”使用该功能。

DHCP 中继设置页面：

图表 16 DHCP 中继

配置说明：

1)开启/关闭 DHCP 中继

要开/关闭 DHCP 中继功能，请选中相应的单选按钮后，按“保存”按钮使配置生效。

2)DHCP 服务器设置

请设置好 DHCP 服务器地址后，按“保存”按钮使配置生效。配置成功后配置结果将显示在下表中。如果要删除 DHCP 服务器，请选中对应的复选框后按“删除”按钮使配置生效。

37.3.1.9. DHCP Snooping

通过菜单项“DHCP Snooping”使用该功能。

DHCP Snooping 设置页面：

图表 17 DHCP Snooping 设置

配置说明：

1)DHCP Snooping 设置

要开启 DHCP Snooping 功能或 DHCP Snooping 源 MAC 检查功能，请选中相应的单选按钮后按“保存”使配置生效。

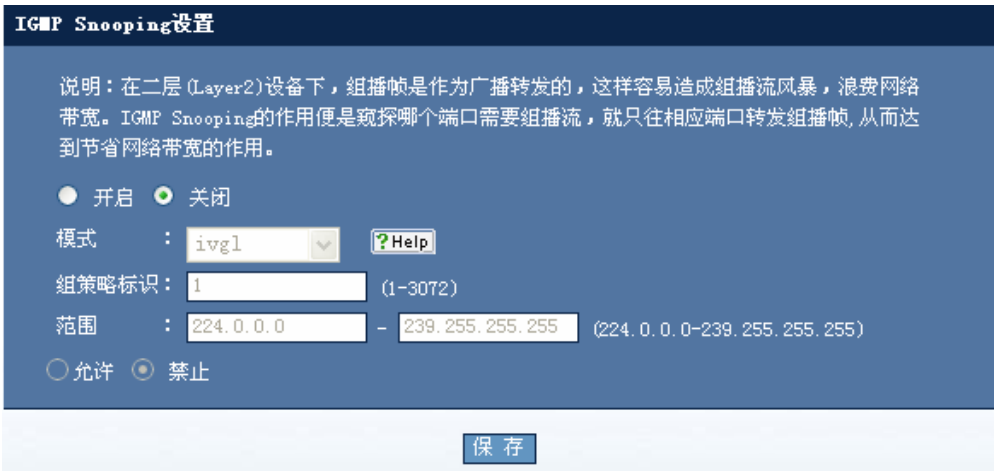
2)DHCP Snooping 信任端口设置

请选择要设置为信任端口的端口后按“保存”按钮使配置生效，配置成功后将在下表显示配置信息。如果要删除信任端口，请选中相应的复选框后按“删除”按钮使配置生效。

37.3.1.10. IGMP Snooping

通过菜单项“IGMP Snooping”使用该功能。

IGMP Snooping 设置页面：



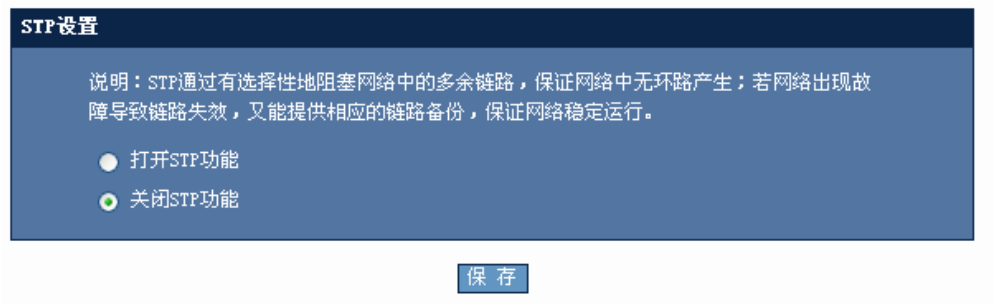
图表 18 IGMP Snooping 设置

配置说明：

如果要打开 IGMP Snooping 功能，请先选中“开启”单选按钮，这时模式下拉框变为可选状态，您可以从中选择 ivgl、svgl、ivgl-svgl 三中模式，如果选择了 svgl、ivgl-svgl 模式，才可以设置标识、IP 范围等参数。配置好参数后按“保存”按钮使配置生效。如果要关闭 IGMP Snooping 功能，请先选中“关闭”单选按钮按“保存”按钮使配置生效。

37.3.1.11. STP 设置

通过菜单项“STP 设置”使用该功能。以下是 STP 设置的主要页面：



图表 19 STP 设置

配置说明：

选中“打开 STP 功能”单选按钮或选中“关闭 STP 功能”单选按钮按“保存”按钮使配置生效。

37.3.1.12. SNMP 管理

通过菜单项“SNMP 管理”使用该功能。

SNMP 管理页面：

图表 20 SNMP 管理设置

配置说明：

如果开启 SNMP 管理功能，请选择“开启 SNMP”单选按钮，这时才可以设置团体名称、读写属性，设置好参数后，按“保存”按钮使配置生效。如果要关闭 SNMP 管理功能，请直接选择“关闭 SNMP”单选按钮后，按“保存”按钮使配置生效。如果要删除已配置的团体名称，请直接选中所要删除的表项所对应的复选框后按“删除”按钮使配置生效。

37.3.2. 安全

37.3.2.1. 防网关 ARP 欺骗

通过菜单项“防网关 ARP 欺骗”使用该功能。

防网关 ARP 欺骗页面：

图表 21 防网关 ARP 欺骗

配置说明：

请选中要配置的端口，在输入网关地址后按“保存”按钮使配置生效，一个端口可配置多个网关地址，如果要删除所配置的网关，请选中要删除的网关地址所对应的复选框，按“删除”按钮使配置生效。

37.3.2.2. 防 ARP 欺骗

通过菜单项“防 ARP 欺骗”使用该功能。

防 ARP 欺骗设置页面：

图表 22 防 ARP 欺骗设置

配置说明：

1)端口/MAC/IP 绑定

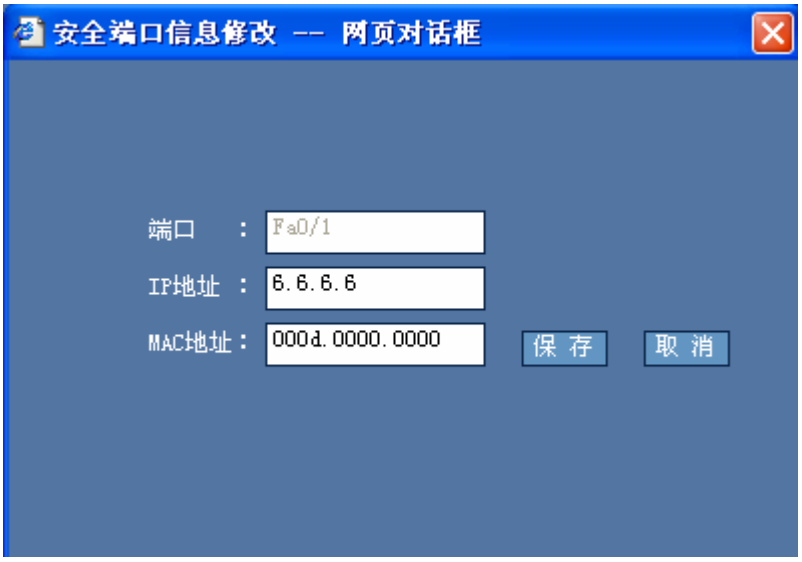
如果要配置端口/MAC/IP 绑定，请选中要配置的端口，并配置好 IP 和 MAC 后，按“保存”按钮使配置生效，如果选中的端口有学到 MAC 地址，则将会在端口自动学习到的地址文本框中显示出来，如上图所示，当选中 GigabitEthernet 0/15 口后，文本框中将列出该端口所学习到的 MAC 地址。

2）端口安全功能设置

选中所要配置的端口后，如果该端口开启了端口安全功能，则开启端口安全功能的单选按钮将会选中，反之则选中关闭端口安全功能单选按钮。如果开启了端口安全功能，则将会在下表中显示安全端口信息。

3)修改安全端口信息

如果要修改端口安全信息，请选中要修改的端口所对应的复选框后按“修改”按钮，将弹出安全端口修改设置界面，如下图：



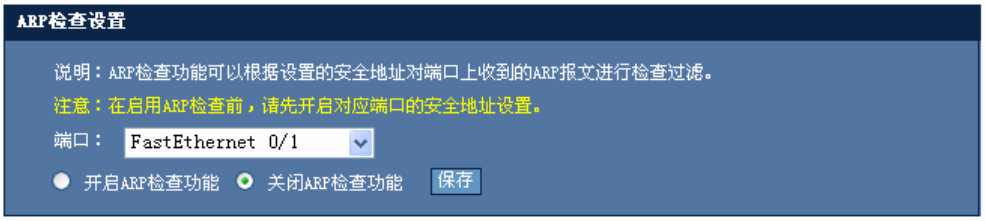
图表 23修改安全端口

修改好相关参数后按“保存”按钮使配置生效，如果端口类型为动态，则修改后端口类型将转换为静态。

37.3.2.3. APR 检查设置

通过菜单项“ARP 检查设置”使用该功能。

ARP 检查设置页面：



图表 24 ARP 检查设置

配置说明：

如果选中的端口已开启该功能，则“开启 ARP 检查功能”单选按钮将被选中，否则默认都选中“关闭 ARP 检查功能”单选按钮。

37.3.2.4. ACL

通过菜单项“ACL”使用该功能。

ACL 设置页面：

图表 25 ACL 设置

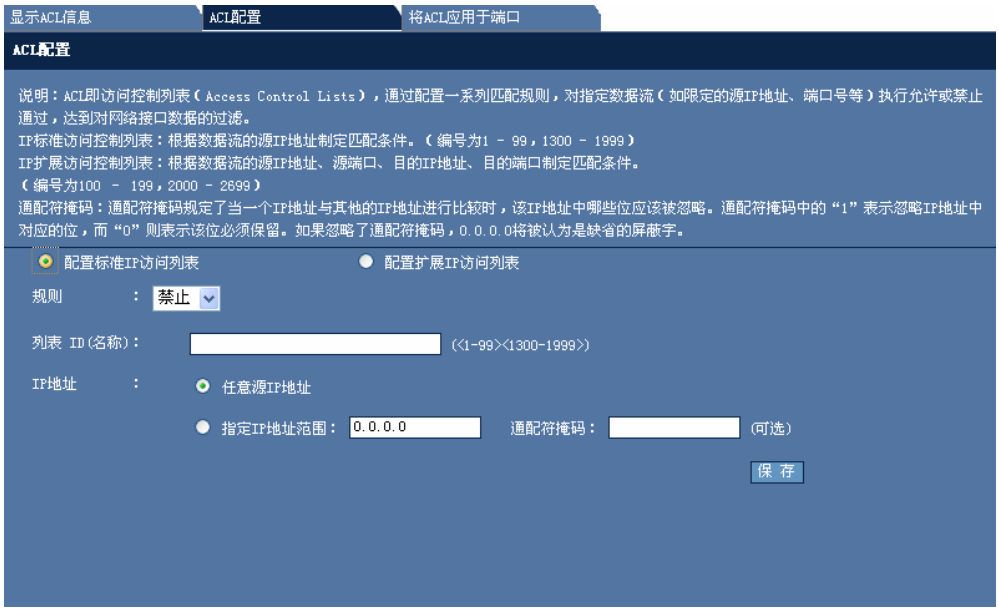
1）显示 ACL 信息

配置说明：

ACL 信息显示界面如图所示，如果要查看指定 ACL 的详细信息，请从 ACL 列表框中选中该条 ACL 后，便会在表格中显示出该 ACL 的所有 ACE。如果要删除某条 ACE，请选中对应的复选框后按“删除”按钮使配置生效。如果要删除整条 ACL，请按“全选”按钮后，选中所有 ACE，按“删除”按钮使配置生效。

2）ACL 配置

如果要配置标准 IP 访问列表，请点击“配置标准 IP 访问列表”单选按钮，下图为配置标准 IP 访问列表界面：



图表 26 配置标准 IP 访问列表

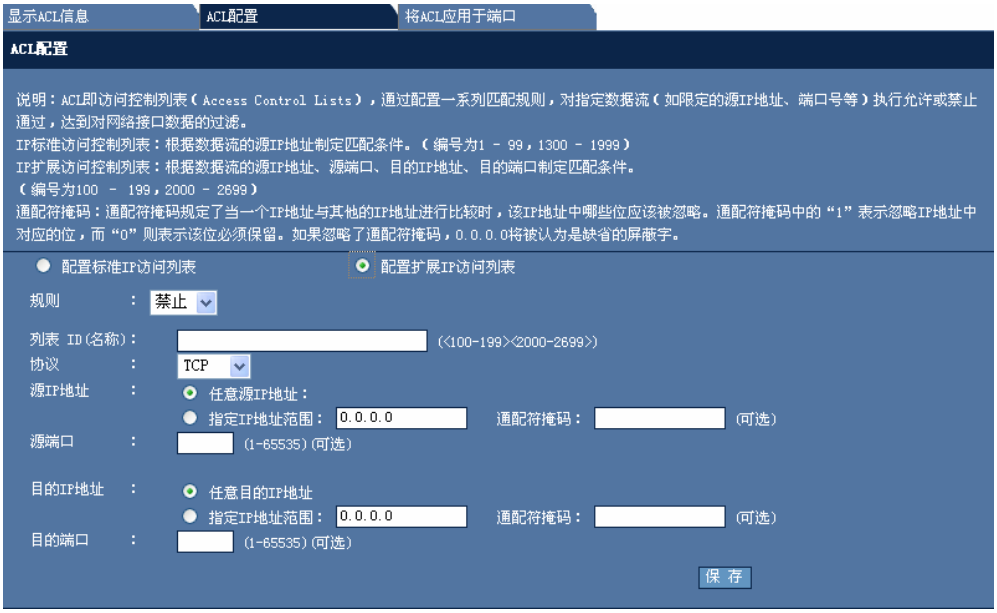
配置说明：

规则：请从下接列表中选择过滤规则，只有“禁止”和“允许”两种规则。

列表 ID（名称）：请输入标准访问列表号，也可以输入标准访问列表的名称。

IP 地址：如果选择指定 IP 地址范围,请输入正确的 IP 地址，通配符掩码文本框如果不需要，可以不填，配置好后按“保存”按钮使配置生效。

如果要配置扩展 IP 访问列表，请点击“配置扩展 IP 访问列表”单选按钮，下图为配置扩展 IP 访问列表：



图表 27 配置扩展 IP 访问列表

配置说明：

规则：请从下接列表中选择过滤规则，只有“禁止”和“允许”两种规则。

列表 ID（名称）：请输入扩展访问列表号，也可以输入扩展访问列表的名称。

协议：该选项支持 TCP、UDP、IP、ICMP

源 IP 地址：你可以选择任意源 IP 地址或指定 IP 地址范围，通配符为可选配置。

源端口：可选配置。

目的 IP 地址：你可以选择任意源 IP 地址或指定 IP 地址范围，通配符为可选配置

目的端口：可选配置。

配置好参数后，请按“保存”按钮使配置生效。

3）将 ACL 应用于端口

图表 28 将 ACL 应用于接口

配置说明：

端口：请选择要配置的端口

ACL 列表：请选择要应用于该端口的 ACL。

配置好参数后按“保存”按钮使配置生效。

如果要删除对应端口的配置，请选中要删除的表项后按“删除”按钮使配置生效。

注意：

如果要配置与 PC 所连的端口，请确认该 ACL 是否会影响 PC 与设备的交互。如果配置错误，将无法继续使用 WEB 来管理设备。

37.3.3. QOS

37.3.3.1. 分类设置

通过菜单项“分类设置”使用该功能。以下是分类设置的主要页面：

图表 29 分类设置

配置说明：

设置好类名和 ACL 后按“保存”按钮使配置生效。配置成功后，将在下表中显示出配置信息。如果要删除已配置的类，请选中该类所对应的复选框后按“删除”按钮使配置生效。

37.3.3.2. 策略设置

通过菜单项“策略设置”使用该功能。

策略设置页面：

图表 30 策略设置

配置说明：

策略名字：配置策略名字。

分类列表：列出已设置的分类名称，如果列表为空，则说明没有设置分类，请先到分类设置页面进行分类设置。

带宽：请输入指定范围内的带宽值。

突发流量：请输入指定范围内的值，请按页面上的提示输入。

带宽超限部分指定处理动作：如果指定DSCP优先级，请输入指定范围内的数字。

设置好参数后按“保存”按钮使配置生效。

如果要删除设置好的策略，请从策略列表中选中该策略后，将会在表格中显示该策略的详细信息，选中要删除的表项后按“删除”按钮使配置生效。如果要一同删除策略名，只要全选后按“删除”按钮使配置生效。

37.3.3.3. 流设置

通过菜单项“流设置”使用该功能。

流设置页面：

图表 31 流设置

配置说明：

端口：请选择要配置的端口。

策略列表：请选择要应用于该端口的策略，如果列表为空，请先设置策略。

限速方向：请选择限速方向。

设置好参数后按“保存”按钮使配置生效。如果要删除端口的配置，请选中要删除的表项所对应的复选框后按“删除”按钮使配置生效。

37.3.4. 系统状态

37.3.4.1. 系统信息

通过菜单项“系统信息”使用该功能。

系统信息页面：

系统信息	
设备型号：	S2924G
主机名 ：	Ruijie
软件版本：	RGOS 10.2(4), Release(55222),Web Version:10.2.55222
硬件版本：	1.0
MAC地址 ：	00d0f8f80fc4

图表 32系统信息

37.3.4.2. 当前配置

通过菜单项“当前配置”使用该功能。

当前配置页面：

当前配置

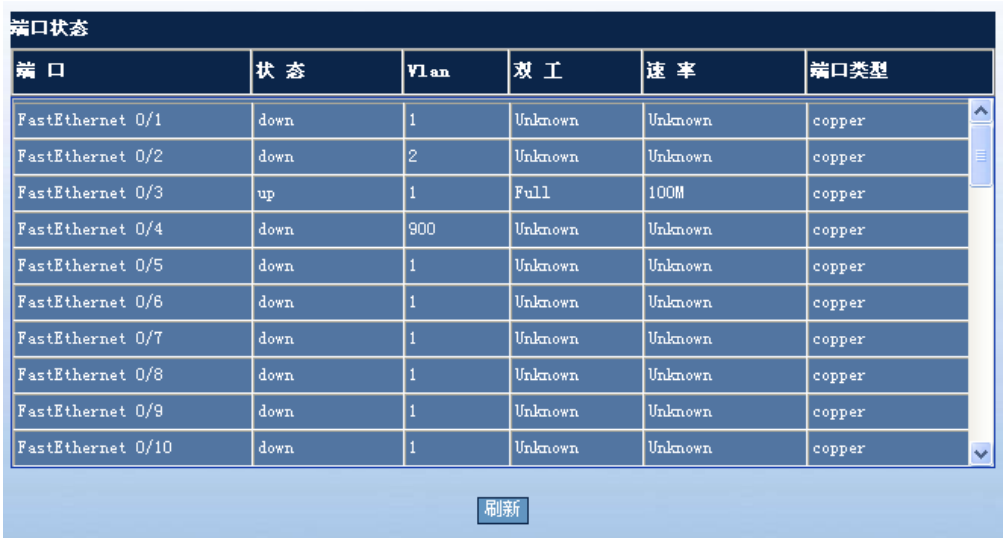
```
Building configuration...
Current configuration : 12931 bytes

!
version RGNOS 10.2.00(3), Release(30355)(Tue Mar 11 19:23:04     2008 -
23195A44470348C)
!
!
!
vlan 1
 name vlan1
!
vlan 2
!
vlan 3
!
vlan 4
!
vlan 5
!
vlan 6
!
vlan 7
!
```

图表 33 当前配置

37.3.4.3. 端口状态

通过菜单项“端口状态”使用该功能。

端口状态页面：

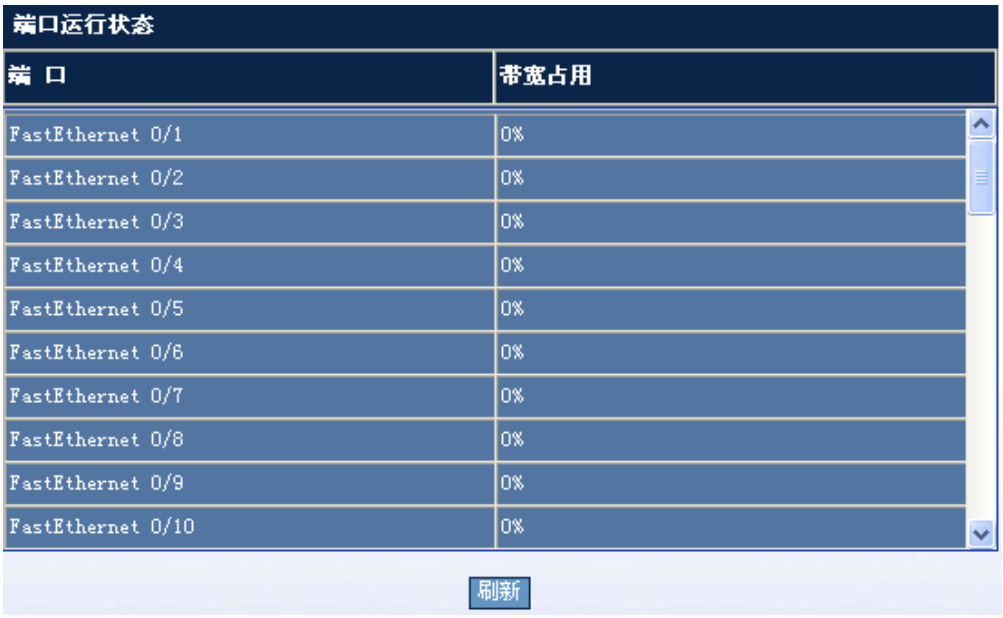


图表 34 端口状态

37.3.4.4. 端口运行状态

通过菜单项“端口运行状态”使用该功能。

端口运行状态页面：

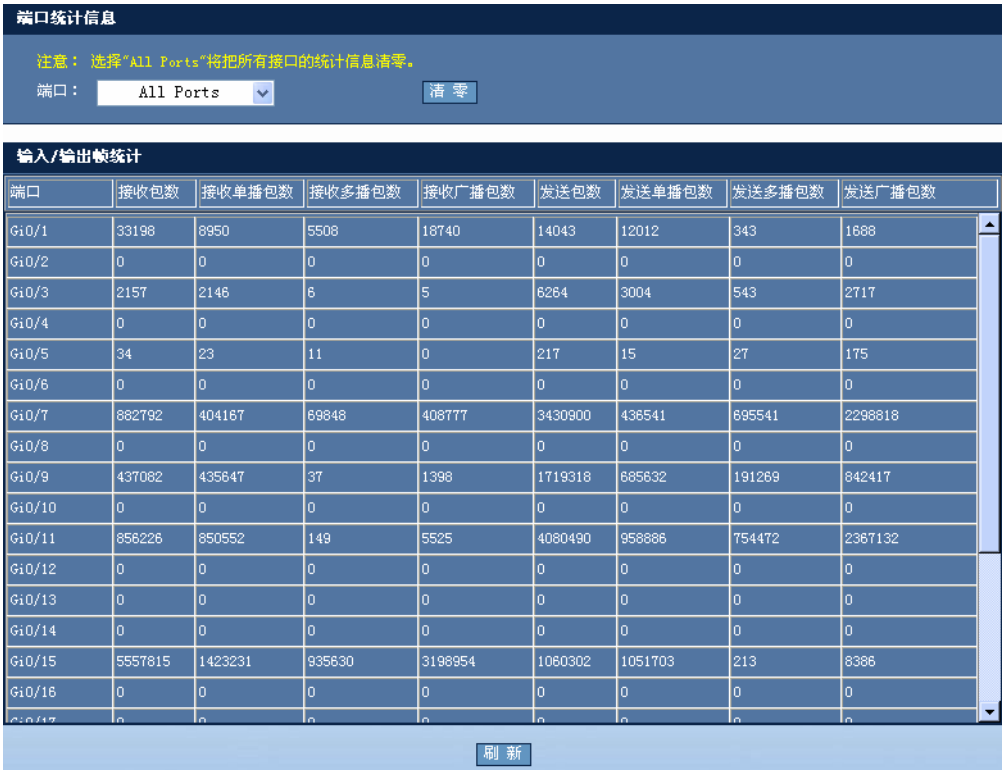


图表 35 端口运行状态

37.3.4.5. 端口统计信息

通过菜单项“端口统计信息”使用该功能。

端口统计信息页面：



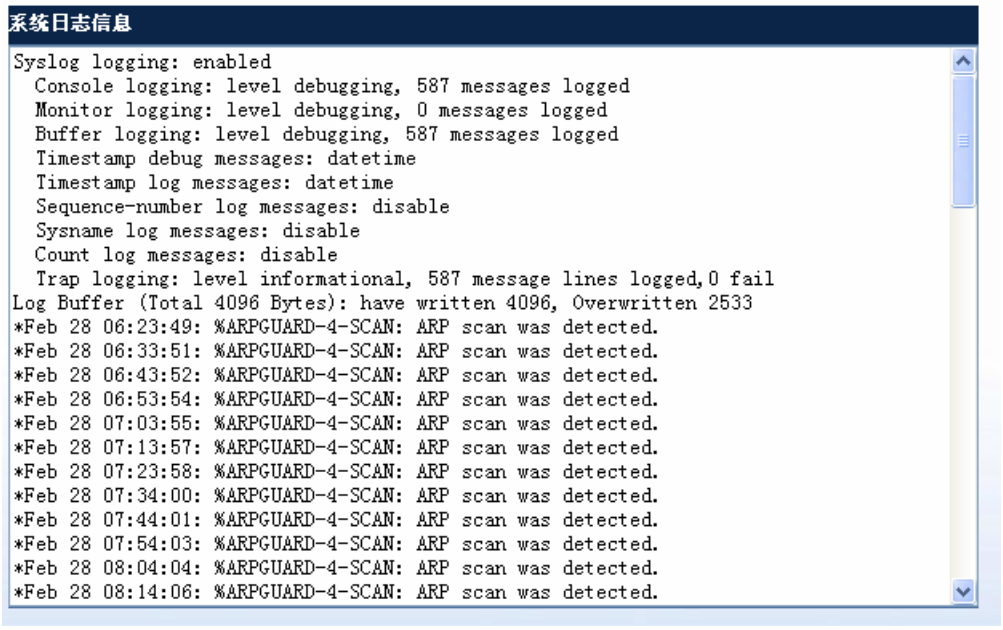
端口	接收包数	接收单播包数	接收多播包数	接收广播包数	发送包数	发送单播包数	发送多播包数	发送广播包数
Gi0/1	33198	8950	5508	18740	14043	12012	343	1688
Gi0/2	0	0	0	0	0	0	0	0
Gi0/3	2157	2146	6	5	6264	3004	543	2717
Gi0/4	0	0	0	0	0	0	0	0
Gi0/5	34	23	11	0	217	15	27	175
Gi0/6	0	0	0	0	0	0	0	0
Gi0/7	882792	404167	69848	408777	3430900	436541	695541	2298818
Gi0/8	0	0	0	0	0	0	0	0
Gi0/9	437082	435647	37	1398	1719318	685632	191269	842417
Gi0/10	0	0	0	0	0	0	0	0
Gi0/11	856226	850552	149	5525	4080490	958886	754472	2367132
Gi0/12	0	0	0	0	0	0	0	0
Gi0/13	0	0	0	0	0	0	0	0
Gi0/14	0	0	0	0	0	0	0	0
Gi0/15	5557815	1423231	935630	3198954	1060302	1051703	213	8386
Gi0/16	0	0	0	0	0	0	0	0

图表 36 端口统计信息

37.3.4.6. 日志信息显示

通过菜单项“日志信息显示”使用该功能。

系统日志信息页面：



图表 37 系统日志信息显示

37.3.5. 系统维护

37.3.5.1. Ping

通过菜单项“Ping”使用该功能。

Ping 页面：

图表 38 Ping

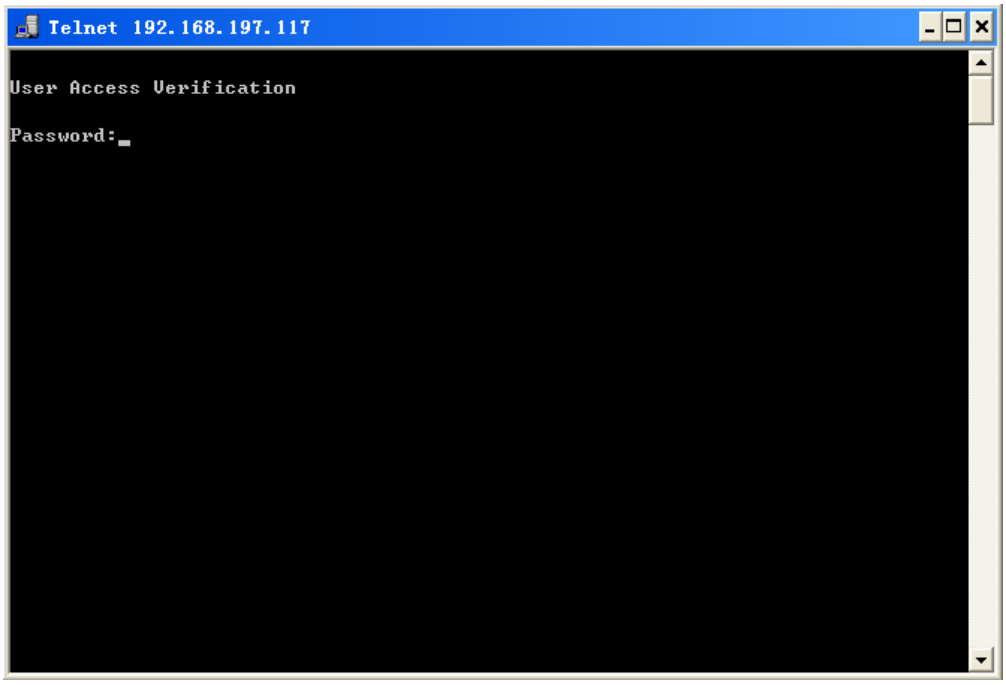
配置说明：

请在文本框中输入 IP 地址后，按“开始”按钮，如果 IP 地址不通，页面将等到 Ping 超时后才能响应。

37.3.5.2. Telnet

通过菜单项“Telnet”使用该功能。

Telnet 页面：



图表 39 Telnet

配置说明：

直接点击菜单项“Telnet”后，将直接启用 Telnet 功能。如果 PC 未开启 Telnet 服务，请先开启 PC 的 Telnet 服务。

37.3.5.3. 用户管理

通过菜单项“用户管理”使用该功能。

用户管理页面：

图表 40 用户管理

配置说明：

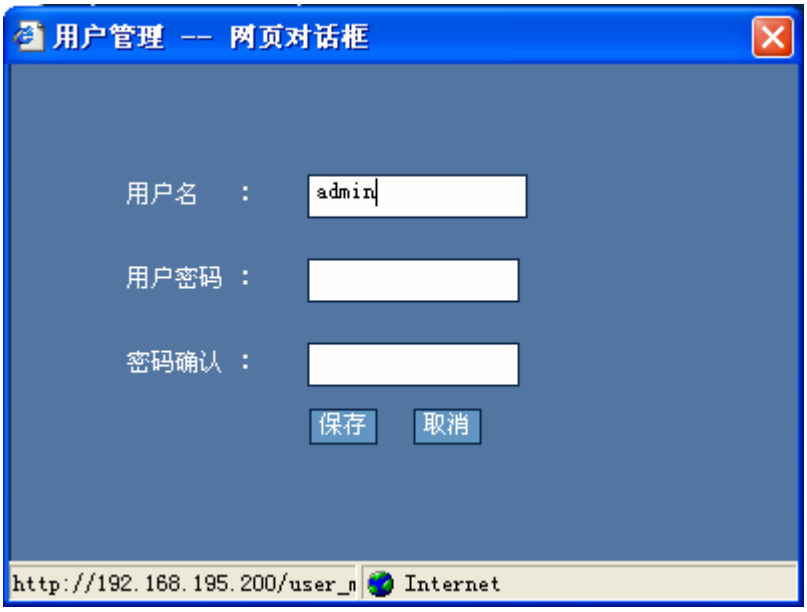
添加用户：如果要新加用户，请点击“添加用户”按钮，将弹出如下配置页面：

图表 41 添加用户

请输入用户名 和密码后按“保存”按钮使配置生效。配置成功后，新加的用户将显示在用户管理页面上。

删除：请选中要删除的用户所对应的复选框，按“删除”按钮。这时所选中的用户将被删除。

修改：请选中要修改的用户所对应的复选框，按“修改”按钮，将弹出如下配置页面：



图表 42 修改用户

请输入用户名和密码后按“保存”按钮使配置生效。配置成功后，修改后的用户将显示在用户管理页面上。

注意：

如果删除、修改的用户名是系统登录时使用的用户名，则将会弹出认证对话框，这时请用其它用户名或修改后的用户名重新认证。如果当前系统中只有一个用户名，则将不允许删除。

37.3.5.4. 密码设置

通过菜单项“密码设置”使用该功能。

密码设置页面：

图表 43 密码设置

配置说明：

1)修改 Enable 口令

如果要修改 Enable 口令，请输入新口令后按“保存”按钮，使配置生效。这时将弹出：

图表 44 登录验证对话框

请用新口令重新登录。

2)修改 Telnet 登录口令

如果要修改 Telnet 口令，请输入新口令后按“保存”按钮，使配置生效。

37.3.5.5. 导入/导出配置

通过菜单项“导入/导出配置”使用该功能。

导入/导出配置页面：

图表 45 导入/导出配置

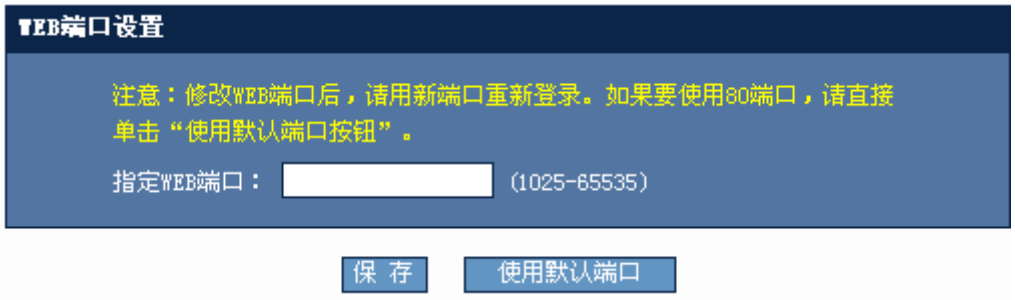
配置说明：

要导入、导出交换机上的 config.text 文件，请先输入 TFTP 服务器的 IP 和 TFTP 服务器上的文件名后按“保存”按钮使配置生效。

37.3.5.6. 设置 WEB 端口

通过菜单项“WEB 端口设置”使用该功能。

WEB 端口设置页面：



图表 46 WEB 端口设置

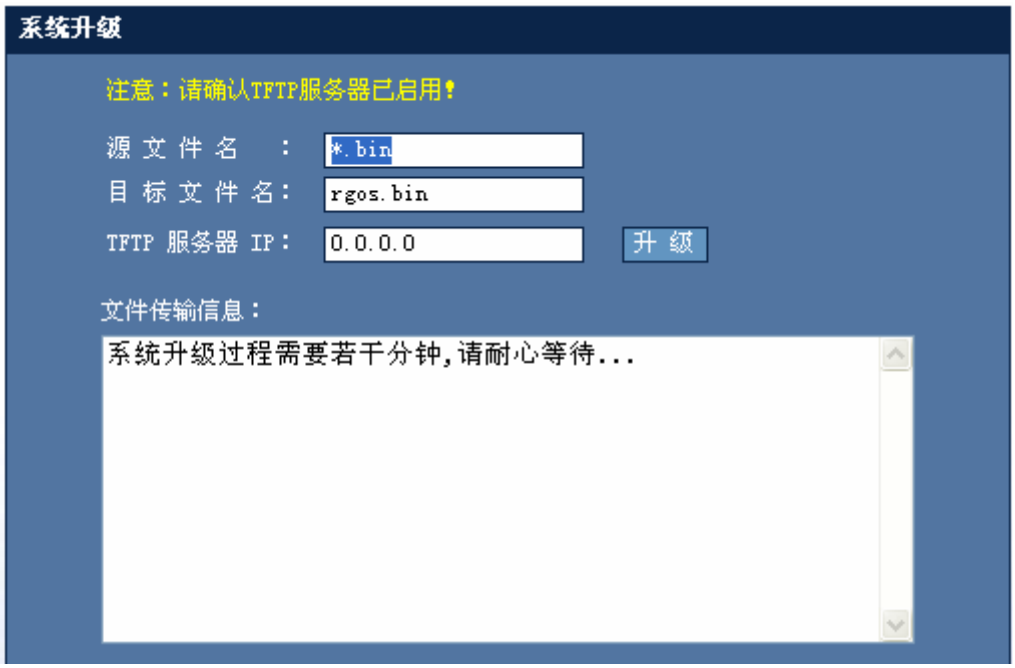
配置说明：

请输入合法范围内的端口后，按“保存”按钮使配置生效。端口设置完后请用新端口重新登录设备。如设新端口为 8080，设备IP地址为：192.168.1.1 则要用 http://192.168.1.1:8080 登录设备。如果要恢复为默认端口，请按“使用默认端口”按钮后，用 http://192.168.1.1重新登录。

37.3.5.7. 系统升级

通过菜单项“系统升统”使用该功能。

系统升统页面：



图表 47 系统升统

配置说明：

要升级系统，请确认已打开了 TFTP 服务器。源文件名为 TFTP 服务器上要升级的文件，目标文件名为升级到设备上后要命名的文件名，输入 TFTP 服务器的 IP 地址后按“升级”按钮使配置生效。

37.3.5.8. 退出系统

通过菜单项“退出系统”使用该功能。

配置说明：

当点击菜单项的“退出系统”后，将关闭浏览器窗口。

37.3.6. 查看配置

无

37.4. WEB 管理典型配置举例

37.4.1. 配置要点

WEB 管理在打开 WEB 服务后，默认就已配置 enable 方法进行认证。

37.4.2. 配置步骤

WEB 管理支持 Local 方法或 Enable 方法进行登录认证，只有认证通过了，用户才可以进入 WEB 管理页面，进行 WEB 配置。

1）用 Local 方法进行登录认证

详细配置如下：

a.进入 config 模式

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

b.打开 WEB 服务

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

c.配置 WEB 管理登录认证方法为 Local 方法

```
Ruijie(config)#ip http authentication local
```

d.配置本地用户名（必须为 15 级用户）和密码

```
Ruijie(config)#username admin password admin
Ruijie(config)#username admin privilege 15
```

e.配置设备管理 IP

```
Ruijie(config)#interface vlan 1
Ruijie(config-if-VLAN 1)#ip address 192.168.100.1
255.255.255.0
```

2）用 Enable 方法进行登录认证

详细配置如下：

a.进入 config 模式

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

b.打开 WEB 服务

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

c.配置 WEB 管理登录认证方法为 Enable 方法（该命令配置后不显示）

```
Ruijie(config)#ip http authentication enable
```

d.配置 Enable 密码

```
Ruijie(config)#enable password admin
```

e.配置设备管理 IP

```
Ruijie(config)#interface vlan 1
Ruijie(config-if-VLAN 1)#ip address 192.168.100.1
255.255.255.0
```

37.4.3. 显示验证

1）用 Local 方法进行登录认证

```
Ruijie(config)#show running-config
Building configuration...
Current configuration : 2014 bytes
!
version RGOS 10.2(4), Release(55435)(Wed May 13 11:50:07 CST
2009 -ngcf32)
vlan 1

username admin password admin      //WEB 管理认证用户名与密码
username admin privilege 15          //WEB 管理用户必须是 15
级用户
no service password-encryption
ip http authentication local          //WEB 管理用 local 方法
进行认证
!
enable service web-server          //开启 WEB 服务
!
…..
    ……
!
interface VLAN 1
 ip address 192.168.100.1 255.255.255.0   //设备管理 IP
 no shutdown
!
!
line con 0
line vty 0 4
 login
!
```

```
!
end
```

2）用 Enable 方法进行登录认证

```
Ruijie(config)#show running-config

Building configuration...
Current configuration : 2014 bytes

!
version RGOS 10.2(4), Release(55435)(Wed May 13 11:50:07 CST
2009 -ngcf32)
vlan 1

no service password-encryption
!
enable password admin            //WEB 管理 Enable 认证密码
enable service web-server          //开启 WEB 服务
!
…..
    ……
!
interface VLAN 1
 ip address 192.168.100.1 255.255.255.0   //设备管理 IP
 no shutdown
!
!
line con 0
line vty 0 4
 login
!
!
end
```