

配置手册

RG-NBS200&2000 系列交换机

NBS_RGOS11.4(1)B41

文档版本 : V1.0

版权声明

copyright © 2018 锐捷网络

保留对本文档及本声明的一切权利。

未得到锐捷网络的书面许可，任何单位和个人不得以任何方式或形式对本文档的部分内容或全部进行复制、摘录、备份、修改、传播、翻译成其他语言、将其全部或部分用于商业用途。



以上均为锐捷网络的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

免责声明

您所购买的产品、服务或特性等应受商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，锐捷网络对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。锐捷网络保留在没有任何通知或者提示的情况下对文档内容进行修改的权利。

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

前言

读者对象

本书适合下列人员阅读

- 网络工程师
- 技术推广人员
- 网络管理员

技术支持

- 锐捷睿易官方网站：<http://www.ruijiery.com/>
- 锐捷睿易在线客服：<http://webchat.ruijie.com.cn>
- 锐捷网络官方网站服务与支持版块：<http://www.ruijie.com.cn/service.aspx>
- 7x24 小时技术服务热线：400-100-0078
- 睿易网络技术论坛：<http://bbs.ruijiery.com/>
- 常见问题搜索：<http://www.ruijie.com.cn/service/known.aspx>
- 锐捷网络技术支持与反馈信箱：4001000078@ruijie.com.cn

本书约定

1. 命令行格式约定

命令行格式意义如下：

粗体：命令行关键字（命令中保持不变必须照输的部分）采用加粗字体表示。

斜体：命令行参数（命令中必须由实际值进行替代的部分）采用斜体表示

[]：表示用[]括起来的部分，在命令配置时是可选的。





{ x | y | ... }：表示从两个或多个选项中选取一个。

[x | y | ...]：表示从两个或多个选项中选取一个或者不选。

//：由双斜杠开始的行表示为注释行。

2. 各类标志

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

-
-  警告标志。表示用户必须严格遵守的规则。如果忽视此类信息，可能导致人身危险或设备损坏。
 -  注意标志。表示用户必须了解的重要信息。如果忽视此类信息，可能导致功能失效或性能降低。
 -  说明标志。用于提供补充、申明、提示等。如果忽视此类信息，不会导致严重后果。
 -  产品/版本支持情况标志。用于提供产品或版本支持情况的说明。
-

3. 说明

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



配置指南-系统配置

本分册介绍配置指南相关内容，包括以下章节：

1. 命令行界面
2. 基础管理
3. LINE
4. TIME RANGE
5. HTTP
6. 系统日志
7. CWMP
8. POE 管理
9. PKG-MGMT

1 命令行界面

1.1 概述

命令行界面(Command Line Interface , CLI)是用户与网络设备进行文本指令交互的窗口，用户可以在命令行界面输入命令，实现对网络设备的配置和管理。

协议规范

命令行界面无对应的协议规范。

1.2 典型应用

典型应用	场景描述
通过CLI配置管理网络设备	通过在命令行界面输入命令对网络设备进行配置管理。

1.2.1 通过CLI配置管理网络设备

应用场景

以下图为例，用户通过终端登录网络设备 A，在命令行界面输入命令实现对设备的配置管理。

图 1-1

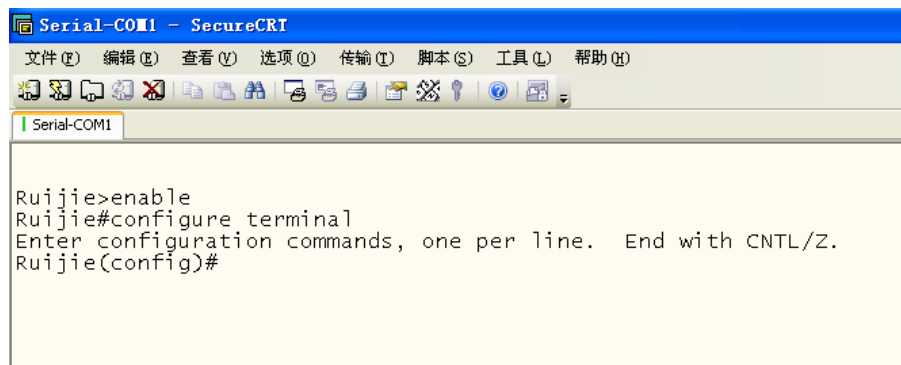


【注释】 A 为需要被管理的网络设备
PC 为用户端。

功能部署

下图列举了在 PC 上通过 Secure CRT 与网络设备 A 建立连接，并打开命令行界面配置命令。

图 1-2



```

Serial-COM1 - SecureCRT
文件(F) 编辑(E) 查看(V) 选项(O) 传输(T) 脚本(S) 工具(L) 帮助(H)
Serial-COM1

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

```

1.3 功能详解

功能特性

功能特性	作用
访问CLI	登录网络设备进行配置管理。
命令模式	命令行接口分为若干种命令模式，不同的命令模式可使用的命令不同。
系统帮助	用户在 CLI 配置过程中可获取系统的帮助信息。
简写命令	如果输入的字符足够识别唯一的命令关键字，可以不必完整输入。
命令的no和default选项	通过 no 或 default 命令，禁止某个功能特性、执行与命令本身相反的操作或恢复缺省配置。
错误命令的提示信息	当用户输入错误命令时，会弹出相应的错误提示信息。
历史命令	用户可以通过快捷键的方式查询、调用历史命令。
编辑特性	系统提供相关快捷键便于用户编辑命令。
show命令的查找和过滤	用户可以在 show 命令输出的信息中查找或过滤指定的内容。
命令别名	配置命令的别名，可以替代命令执行配置。

1.3.1 访问CLI

在使用 CLI 之前，用户需要通过一个终端或 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。在首次使用网络设备时，只能通过串口（Console）连接网络设备，称为带外（Out band）管理方式。在进行了相关配置后，还可以通过 Telnet 虚拟终端方式连接和管理网络设备。

1.3.2 命令模式

设备可供使用的命令非常多，为便于使用这些命令，将命令按功能进行分类。命令行接口分为若干个命令模式，所有命令都注册在某种（或几种）命令模式下。当使用某条命令时，需要先进入这个命令所在的模式。不同的命令模式之间既有联系又有区别。

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）。在此模式下，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。

要使用更多的命令，首先须进入特权模式（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。在全局配置模式下配置，可以进入接口配置模式等各种配置子模式。

各个命令模式概要如下（假定网络设备的名字为缺省的“Ruijie”）：

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)	访问网络设备时默认进入该模式。	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 <i>vlan_id</i> 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。
----------------------------	---	----------------------	--	------------------

1.3.3 系统帮助

用户在输入命令行的过程中，可以通过如下方式获取系统帮助。

1. 在任意模式的命令提示符下，输入问号（？）列出当前命令模式支持的命令及其描述信息。

例如：

```
Ruijie>?
Exec commands:
<1-99>      Session number to resume
disable     Turn off privileged commands
disconnect  Disconnect an existing network connection
enable      Turn on privileged commands
exit        Exit from the EXEC
help        Description of the interactive help system
lock        Lock the terminal
ping        Send echo messages
show        Show running system information
telnet      Open a telnet connection
traceroute  Trace route to destination
```

2. 在一条命令的关键字后空格并输入问号（？），可以列出该关键字关联的下一个关键字或变量。

例如：

```
Ruijie(config)#interface ?
Aggregateport  Aggregate port interface
Dialer         Dialer interface
GigabitEthernet Gigabit Ethernet interface
Loopback       Loopback interface
Multilink      Multilink-group interface
Null           Null interface
Tunnel         Tunnel interface
Virtual-ppp    Virtual PPP interface
Virtual-template Virtual Template interface
Vlan           Vlan interface
range          Interface range command
```

i 如果该关键字后带的是一个参数值，则列出该参数的取值范围及其描述信息，如下所示：

```
Ruijie(config)#interface vlan ?  
<1-4094> Vlan port number
```

3. 在输入不完整的命令关键字后输入问号（?），可以列出以该字符串开头的所有命令关键字。

例如：

```
Ruijie#d?  
debug delete diagnostic dir disable disconnect
```

4. 在输入不完整的命令关键字后，如果该关键字后缀唯一，可以键入<Tab>键生成完整关键字。

例如：

```
Ruijie# show conf<Tab>  
Ruijie# show configuration
```

5. 在任何命令模式下，还可以通过 **help** 命令获取帮助系统的摘要描述信息。

例如：

```
Ruijie(config)#help  
Help may be requested at any point in a command by entering  
a question mark '?'. If nothing matches, the help list will  
be empty and you must backup until entering a '?' shows the  
available options.  
Two styles of help are provided:  
1. Full help is available when you are ready to enter a  
command argument (e.g. 'show ?') and describes each possible  
argument.  
2. Partial help is provided when an abbreviated argument is entered  
and you want to know what arguments match the input  
(e.g. 'show pr?'.)
```

1.3.4 简写命令

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


例如进入 GigabitEthernet 0/1 接口配置模式的命令 “**interface gigabitEthernet 0/1**” 可以简写成：

```
Ruijie(config)#int g0/1  
Ruijie(config-if-GigabitEthernet 0/1)#
```

1.3.5 命令的no和default选项

大部分命令有 **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。

 各命令的 **no** 或 **default** 选项作用请参见相应的命令手册。

1.3.6 错误命令的提示信息

当用户输入错误命令时，会弹出相应的错误提示信息。

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。

1.3.7 历史命令

系统能够自动保存用户最近输入的历史命令，用户可以通过快捷键的方式查询、调用历史命令。

操作方法如下：

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

1.3.8 编辑特性

用户在进行命令行编辑时，可以使用如下按键或快捷键：

功能	按键、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	删除光标右边的一个字符。
输出时屏幕滚动一行或一页。	Return 键	在显示内容时用回车键将输出的内容向上滚动一行，显示下一行的内容，仅在输出内容未结束时使用。
	Space 键	在显示内容时用空格键将输出的内容向上滚动一页，显示下一页内容，仅在输出内容未结束时使用。


当编辑的光标接近右边界时，命令行会整体向左移动 20 个字符，命令行前部被隐藏的部分被符号 (\$) 代替，可以使用相关按键或快捷键将光标移到前面的字符或者回到命令行的首部。

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

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

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


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

 默认的终端行宽是 80 个字符。

1.3.9 show 命令的查找和过滤

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

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

 支持在任意模式下执行 **show** 命令。

 查找的信息内容需要区分大小写，以下相同。

要在 **show** 命令的输出信息中过滤指定的内容，可以使用以下命令：

命令	作用
show any-command 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。
show any-command include regular-expression	在 show 命令的输出内容中进行过滤，仅输出包含指定内容的行，其他信息将被过滤。

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

```
Ruijie#show running-config | include interface
interface GigabitEthernet 0/0
interface GigabitEthernet 0/1
interface GigabitEthernet 0/2
interface GigabitEthernet 0/3
interface GigabitEthernet 0/4
interface GigabitEthernet 0/5
interface GigabitEthernet 0/6
interface GigabitEthernet 0/7
interface Mgmt 0
```

1.3.10 命令别名

用户可以指定任意单词作为命令的别名，来简化命令行字符串的输入。


配置效果

1. 一个单词代替一条命令。

例如：将 “**ip route 0.0.0.0 0.0.0.0 192.1.1.1**” 配置别名 “mygateway”，执行该命令只要输入 “mygateway” 即可。

2. 一个单词代替一条命令的前半部分，再输入后半部分。

例如：将 “**ip address**” 配置别名 “ia”，执行 IP 地址配置可以先输入 “ia”，再输入指定的 IP 地址及掩码。

 这些默认的别名不能删除。

配置命令别名

相关命令如下：

【命令格式】 **alias mode command-alias original-command**

【参数说明】 **mode**：别名所代表的命令所处的命令模式。

command-alias：命令别名。

original-command：别名所代表的实际命令。

【命令模式】 全局模式

【使用指导】 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。

注意事项

- 别名替代的命令必须是命令行的第一个字符开始。
- 别名替代的命令必须是一个完整的输入形式。
- 命令别名在使用时必须完整输入，否则不能被识别。

配置举例

定义一个别名替代整条命令

【配置方法】 在全局配置模式下，配置命令别名“ir”代表默认路由设置“**ip route 0.0.0.0 0.0.0.0 192.168.1.1**”

```
Ruijie#configure terminal
Ruijie(config)#alias config ir ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

【检验方法】 ● 通过 **show alias** 查看别名是否设置成功。

```
Ruijie(config)#show alias
Exec mode alias:
  h                help
  p                ping
  s                show
  u                undebug
  un               undebug
Global configuration mode alias:
  ir                ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

● 使用设置好别名执行命令，通过 **show running-config** 查看是否配置成功。

```
Ruijie(config)#ir
Ruijie(config)#show running-config

Building configuration...
!
alias config ir ip route 0.0.0.0 0.0.0.0 192.168.1.1 //配置别名
...
ip route 0.0.0.0 0.0.0.0 192.168.1.1 //输入别名“ir”的配置结果
!
```

定义一个别名替代一个命令的前半部分

【配置方法】 在全局配置模式下，配置命令别名“ir”代表默认路由设置的“**ip route**”

```
Ruijie#configure terminal
Ruijie(config)#alias config ir ip route
```

【检验方法】 ● 通过 **show alias** 查看别名是否设置成功。

```
Ruijie(config)#show alias
Exec mode alias:
  h                help
```

```

p          ping
s          show
u          undebug
un         undebug
Global configuration mode alias:
ir         ip route

```

- 输入别名“ir”，再配置后半部分命令“0.0.0.0 0.0.0.0 192.168.1.1”。
- 通过 **show running-config** 查看是否配置成功。

```

Ruijie(config)#ir 0.0.0.0 0.0.0.0 192.168.1.1
Ruijie(config)#show running

Building configuration...
!
alias config ir ip route //配置别名
!
ip route 0.0.0.0 0.0.0.0 192.168.1.1 //输入别名“ir”及后半部分命令的配置结果
!

```

命令别名支持的系统帮助

- 命令别名支持帮助信息，在别名前面会显示一个星号(*)，格式如下：

```
*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。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，在帮助信息中将携带引号显示。

例如，在 EXEC 模式下配置别名“sv”代替命令 **show version**，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 *sv="show version" show start-chat
start-terminal-service

```

- 获取系统帮助时，命令别名可以获取与该命令相关的帮助信息。


例如，配置接口模式下的命令别名“ia”代表“ip address”，在接口模式下输入“ia?”，可获取等同“ip address?”的帮助信息，并且将别名替换成实际的命令：

```

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

```

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

 如果在命令之前输入了空格，将无法获取该别名表示的命令。

2 基础管理

2.1 概述

基础管理为首次接触网络设备管理的入门手册，介绍一些常用的网络设备管理、监控和维护的功能。

协议规范

无

2.2 典型应用

典型应用	场景描述
网络设备的管理	用户通过终端登录网络设备，在命令行界面输入命令实现对设备的配置管理。

2.2.1 网络设备的管理

应用场景

在本文档中，所涉及的管理都是通过命令行界面进行的，用户通过终端登录网络设备 A，在命令行界面输入命令实现对设备的配置管理。如下图所示：

图 2-1



2.3 功能详解

基本概念

▾ TFTP

TFTP (Trivial File Transfer Protocol,简单 文件传输协议) 是TCP/IP协议族中的一个用于客户机与 服务器之间进行简单文件传输的协议。

AAA

AAA (Authentication Authorization Accounting , 认证授权计帐)。

Authentication认证：验证用户的身份与可使用的 网络服务。

Authorization 授权：依据认证结果开放网络服务给用户。

Accounting计帐：记录用户对各种网络服务的用量，并提供给 计费系统。整个系统在 网络管理与安全问题中十分有效。

RADIUS

RADIUS (Remote Authentication Dial In User Service , 远程用户拨号认证系统) 是目前应用最广泛的 AAA协议。

Telnet

Telnet是位于OSI模型的第7层---应用层上的一种协议， 是一个通过创建 虚拟终端提供连接到远程 主机 终端仿真的TCP/IP协议。这一协议需要通过用户名和口令进行认证，是Internet远程登陆服务的标准协议。应用Telnet协议能够把 本地用户所使用的计算机变成远程 主机系统的一个 终端。

系统信息

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。

硬件信息

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，插槽上模块的描述（如果插槽没有插模块，则描述为空），插槽所插入模块包括物理端口数，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）。

功能特性

功能特性	作用
控制用户访问	通过使用口令保护和划分特权级别来控制网络上的终端访问网络设备。
控制登录认证	启用 AAA 的模式下，用户登录网络设备进行管理的时候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。
系统基本参数	系统的各项参数，例如时钟，标题，控制台速率等。
查看配置信息	查看系统配置信息主要包括查看系统正在运行的配置信息，以及查看存储在 NVRAM (非易失性随机存取存储器) 上设备的配置等。
使用Telnet	Telnet 属于 TCP/IP 协议族的应用层协议，它给出通过网络提供远程登录和虚拟终端通讯功能的规范。
重启	介绍系统重启。
批量执行文件中的命令	执行批处理文件能将事先写好的配置一次全部配置完毕

2.3.1 控制用户访问

通过使用口令保护和划分特权级别来控制网络上的终端访问网络设备。

工作原理

▾ 授权级别

网络设备的命令行界面针对用户划分 0-15 共 16 个授权级别，不同级别的用户可以执行的命令是不同的。数字小的级别权限较小，其中 0 级为最低级别，只能执行少数几条命令；15 级为最高级别，可以执行所有的命令。0-1 级一般称为普通用户级别，不允许对设备进行配置（默认不允许进入全局配置模式），2-15 级一般称为特权用户级别，可以对设备进行配置。

▾ 口令类别

口令分为 password 和 security 两种。password 为简单加密的口令，只能设置为 15 级口令。security 口令为安全加密口令，可以为 0~15 级设置口令。如果系统中同级别同时存在以上两种口令，则 password 口令不生效。如果设置非 15 级的 password 口令，则会给出警告提示，并自动转为 security 口令；如果设置 15 级的 password 口令和 security 口令完全相同，则会给出警告提示；口令必须以加密形式保存，password 口令使用简单加密，security 口令使用安全加密。

▾ 口令保护

在网络设备上为每个特权级别设置口令，当用户想升高权限级别时，需要输入目的级别对应的口令，口令校验通过以后才允许升高权限级别。用户降低级别则不需要通过口令校验。

缺省时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。

▾ 命令授权

每一条命令都有最低执行级别的要求，如果用户的权限级别达不到要求是无法执行该命令的。此时可以通过命令授权操作，将命令执行权限授予某个特权级别，将允许权限达到（大于或等于）该级别的用户执行该命令。

相关配置

▾ 设置 password 口令

- 使用 **enable password** 命令设置 password 口令。

▾ 设置 secret 口令

- 使用 **enable secret** 命令设置安全口令。
- 需要在切换用户级别时进行 secret 口令校验，可以配置此项。功能与 password 口令相同，但使用了更好的口令加密算法。为了安全起见，建议使用 secret 口令。

↘ 设置命令的级别

- 使用 **privilege** 命令设置命令的级别。
- 如果想让更多的授权级别使用某一条命令，则可以将该命令设置较低的用户级别；而如果想让命令的使用范围小一些，则可以将该命令设置较高的用户级别。

↘ 升高/降低用户级别

- 使用 **enable / disable** 命令升高/降低用户级别。
- 已经登录网络设备的用户，可以通过改变当前的用户级别，以访问不同级别的命令。

↘ 启用 line 线路口令保护

- 对远程登录（如 TELNET）进行口令验证，要配置 **line** 口令保护。
- 应先使用 **password[0 | 7] line** 命令配置 **line** 线路口令，然后执行 **login** 命令启动口令保护。
- 终端在缺省情况下不支持 **lock** 命令。

2.3.2 控制登录认证

在未启用 AAA 模式下，用户登录网络设备进行管理的时候，如果线路上设置了登陆认证（login），需要通过线路上所配置的口令进行校验，通过校验的用户才允许登录。如果线路上设置了本地认证（login local），则需要通过本地用户数据库来根据用户名和密码进行用户的管理权限的认证。

在启用 AAA 模式下，用户登录网络设备进行管理的时候，可以利用一些服务器根据用户名和密码进行用户的管理权限的认证，通过认证的用户才允许登录。

例如，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。通过这种方式，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。

工作原理

↘ 线路口令

配置线路（line）口令的目的，是为了在未启用 AAA 模式的情况下，用于终端登录时的口令校验。启用了 AAA 模式以后，线路上的口令校验将不生效。

↘ 本地认证

配置本地认证的目的，是为了在未启用 AAA 模式的情况下，通过本地用户数据库来根据用户名和密码进行用户的管理权限的认证。启用了 AAA 模式以后，线路上的本地认证设置将不生效。

↘ AAA 模式

AAA 是认证、授权和记账（Authentication, Authorization and Accounting）的简称，AAA 是一种体系结构框架，它提供包括认证、授权和记账在内三个互相独立的安全功能。启用了 AAA 模式以后，终端登录时候需要根据 AAA 所设置的登录认证方法列

表的要求，通过一些服务器（或本地用户数据库）来根据用户名和密码进行用户的管理权限的认证。AAA 功能详解参见 AAA 配置指南。

相关配置

配置本地用户

- 使用 **username** 命令配置用于本地身份认证和授权的账号信息，包括用户名、密码以及可选的授权信息。

线路登录进行本地认证

- 使用 **login local** 命令在 AAA 关闭时，LINE 线路登录认证时走本地用户认证。
- 应在每台设备上配置。

线路登录进行 AAA 认证

- AAA 打开的情况下，默认使用 **default** 认证方法。
- 使用 **login authentication** 命令在 LINE 线路上配置登录认证方法列表。
- AAA 设置为采用本地认证方法时需要配置。

设置连接超时时间

- 缺省的超时时间为 10 分钟。
- 使用 **exec-timeout** 命令设置连接超时时间。当前已接受的连接，在指定时间内，没有任何输入时，将中断此连接。
- 在需要延长或缩短这段等待时间时，应执行此配置项。

设置会话超时时间

- 缺省的超时时间为 0 min，代表永不超时。
- 使用 **session-timeout** 命令设置会话超时时间。
- 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。在需要延长或缩短这段等待时间时，应执行此配置项。

会话锁定

- 终端在缺省情况下不支持 **lock** 命令。
- 使用 **lockable** 命令允许用户锁住当前线路所连接的终端。
- 要使用会话锁定功能，需要在 line 配置模式下启用锁住 line 终端的功能，并在相应终端的 EXEC 模式下，通过使用 **lock** 命令锁住终端。

2.3.3 系统基本参数

系统时间

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。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。

配置系统名称和命令提示符

为了管理的方便，可以为一台网络设备配置系统名称(System Name)来标识它。默认系统名为“Ruijie”，如果系统名称超过 32 个字符，则截取其前 32 个字符。默认情况下，系统名称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。

标题

标题可以提供一些常规的登录提示信息。可以创建的标题 (banner) 类型有两种：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。

配置控制台速率

通过配置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。使用时可以根据实际需求，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。

设置连接超时

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。

相关配置

设置系统的日期和时钟

- 使用 **clock set** 命令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。

更新硬件时钟

- 如果硬件时钟和软件时钟不同步，使用 **clock update-calendar** 命令可以通过软件时钟的日期和时间复制给硬件时钟。

设置系统名称

- 使用 **hostname** 命令可以修改默认的系统名称。
- 缺省的主机名为 Ruijie。

设置命令提示符

- 通过 **prompt** 命令可以设置用户命令接口的提示符。

设置每日通知

- 缺省没有每日通知。
- 使用 **banner motd** 命令配置每日通知信息。
- 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）给用户。

配置登录标题

- 缺省没有登录标题。
- 使用 **banner login** 命令设置登录标题，用于提供一些常规的登录提示信息。

设置控制台的传输速率

- 使用 **speed** 命令配置终端设备的速率。
- 缺省的速率是 9600。

2.3.4 查看配置信息

查看系统配置信息主要包括查看系统正在运行的配置信息，以及查看存储在 NVRAM（非易失性随机存取存储器）上设备的配置等。

工作原理

系统正在运行的配置信息

系统正在运行的配置信息即 running-config 是系统上所有的组件模块当前运行的配置的总和，具有实时性的特点。在查看的时候，先需要向所有的运行组件请求搜集配置，并经过一定的编排组合后显示给用户。正因为实时性的特点，只有运行中的组件才可能提供此配置信息，如果组件未加载则不会显示其配置。这样，在系统启动、组件进程重启的过程中，组件处于不稳定状态下所收集的系统运行配置会有一些的差异。例如在某一时段收集的信息中缺乏某个组件的配置，过一段时间后再收集就有了。

系统的启动配置信息

存储在 NVRAM（非易失性随机存取存储器）上设备的配置即 startup-config 为设备启动时执行的配置，在系统重新启动后会导入 startup-config 成为新的运行配置。查看永久配置的过程就是读取设备 NVRAM 上的 startup-config 文件信息并显示。

相关配置

查看系统正在运行的配置信息

执行 **show running-config [interface interface]** 命令查看系统正在运行的配置信息或某个接口下的配置信息。

查看设备的启动配置信息

执行 **show startup-config** 命令查看设备的启动配置信息。

保存设备的启动配置信息

执行 **write** 命令或者 **copy running-config startup-config** 将设备的当前正在运行的配置信息，保存成为新的启动配置信息。

2.3.5 使用Telnet

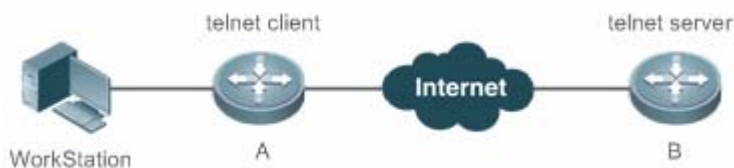
工作原理

Telnet 属于 TCP/IP 协议族的应用层协议，它给出通过网络提供远程登录和虚拟终端通讯功能的规范。

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

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

图 2-1



相关配置

使用 telnet client

- 使用 **telnet** 命令通过 telnet 登录到远程设备。
- 使用 **do telnet client**
- 使用 **do telnet** 命令通过 telnet 登录到远程设备。

恢复已建立的 Telnet Client 会话连接

- 执行 **<1-99>** 命令恢复已建立的 Telnet Client 会话连接。

断开挂起的 Telnet Client 连接

- 执行 **disconnect session-id** 命令断开指定的 Telnet Client 连接。


使用 Telnet Server


- 使用 **enable service telnet-server** 命令打开 Telnet Server 服务。
- 需要使用 Telnet 登录本地设备时，需要打开该服务。

2.3.6 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。

- 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。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。
- 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。

 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，否则有可能会造成设置失效，比如将系统时间调到重启时间之后。


相关配置


▾ 设置重启

- 使用 **reload** 命令设置重启策略。
- 使用该命令可以指定设备在指定的时刻启动，方便进行管理。

2.3.7 批量执行文件中的命令

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。

 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，则需要先在批处理文件中预先写入相应的应答信息，保证命令能够正常执行。

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



相关配置

▾ 批处理命令

- 使用 **execute** 命令批量执行文件中的命令。
- 使用该命令可以批量完成某个功能多条命令的配置，简化用户操作。

2.4 配置详解

配置口令与权限	 可选配置。设置口令与命令级别划分。	
	enable password	设置 password 口令
	enable secret	设置 secret 口令
	enable	升高用户级别
	login privilege log	在终端用户权限级别提升的情况下,输出相应的日志信息
	disable	降低用户级别
	privilege	设置命令的级别划分
	password	指定 line 线路口令
	login	启用 line 线路口令保护
配置登录与认证	 可选配置。配置不同登录方式及认证。	
	username	配置本地用户账号以及可选的授权信息
	login local	线路登录进行本地认证
	login access non-aaa	在 AAA 打开的情况下,配置该命令,在线路上可以选择采用非 AAA 服务来进行认证
	login authentication	线路登录进行 AAA 认证
	telnet	使用 Telnet Client
	do telenet	使用 DoTelnet Client
	enable service telnet-server	使用 Telnet Server
	exec-timeout	配置连接超时时间
	session-timeout	配置会话超时时间
	lockable	启用锁住 line 终端的功能
	lock	锁住当前 line 终端
设置系统基本参数	 可选配置。设置系统基本参数。	
	clock set	设置系统的日期和时钟
	clock update-calendar	更新硬件时钟
	hostname	设置系统名称
	prompt	设置命令提示符
	banner motd	设置每日通知
	bannerlogin	配置登录标题
打开或关闭指定的服务	 可选配置。打开与关闭指定的服务。	
	enable service	打开某项服务。

设置重启策略	 可选配置。设置系统重启时的策略。	
	<table border="1"> <tr> <td><code>reload</code></td> <td>重启设备。</td> </tr> </table>	<code>reload</code>
<code>reload</code>	重启设备。	
批量执行文件中的命令	 可选配置。批量执行文件的命令。	
	<table border="1"> <tr> <td><code>execute { [flash:] filename }</code></td> <td>批量执行指定文件中的命令。</td> </tr> </table>	<code>execute { [flash:] filename }</code>
<code>execute { [flash:] filename }</code>	批量执行指定文件中的命令。	

2.4.1 配置口令与权限

配置效果

- 设置用户的口令，可以控制对网络设备的访问。
- 对命令使用权限进行分级，对于特定级别的命令，只有达到或高于这个级别的用户才可以使用。
- 将命令的使用权授予较低的用户级别，让更多的授权级别使用该条命令。
- 该命令的使用权授予较高的用户级别，则该命令的使用范围会缩小。

注意事项

- 在设置口令中，如果使用带 **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。
- 缺省没有设置任何级别的 `password` 或 `secret` 口令，如果没有指定 `level`，则缺省的级别是 15 级。
- 如果设置非 15 级的 `password` 口令，系统将自动转换为 `secret` 口令，并给出提示信息。
- 如果同时设置了 `password` 口令和 `secret` 口令，则系统将选择使用 `secret` 口令。

配置方法

▾ 设置 password 口令

- 可选配置。需要在切换用户级别时进行 `password` 口令校验，可以配置此项。
- 使用 `enable password` 命令设置 `password` 口令。

▾ 设置 secret 口令

- 可选配置。需要在切换用户级别时进行 `secret` 口令校验，可以配置此项。
- 使用 `enable secret` 命令设置安全口令。
- 功能与 `password` 口令相同，但使用了更好的口令加密算法。为了安全起见，建议使用 `secret` 口令。

▾ 设置命令的级别

- 可选配置。

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

📄 升高/降低用户级别

- 已经登录网络设备的用户，可以通过改变当前的用户级别，以访问不同级别的命令。
- 使用 **enable / disable** 命令升高/降低用户级别。

📄 启用 line 线路口令保护

- 可选配置。对远程登录（如 TELNET）进行口令验证，要配置 **line** 口令保护。
- 应先使用 **password [0 | 7] line** 命令配置 **line** 线路口令，然后执行 **login** 命令启动口令保护。

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

检验方法

- 可以使用 **show privilege** 命令查看当前用户级别。
- 可以使用 **show running-config** 命令查看配置。

相关命令

📄 设置 password 口令

【命令格式】 **enable password [level level] { password | [0 | 7] encrypted-password }**

【参数说明】 *level*：用户的级别。

password：用户进入特权 EXEC 配置层的口令。

0：表示输入的口令字符串为明文字符串。

7：表示输入的口令字符串为密文字符串。

encrypted-password：口令文本。必须包含 1 到 26 个大小写字母和数字字符。


 口令前面可以有前导空格，但被忽略。中间及结尾的空格则作为口令的一部分。

【命令模式】 全局模式

【使用指导】 目前只能设置 15 级用户的口令，并且只能在未设置 security 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 security 口令。

如果设置的 15 级 password 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。

 如果指定了加密类型，然后输入一条明文口令，则不能重新进入特权 EXEC 模式。不能恢复用任意方法加密的已丢失口令。只能重新配置设备口令。

📄 设置 secret 口令

【命令格式】 **enable secret [level level] { secret | [0 | 5] encrypted-secret }**

【参数说明】 *level*：用户的级别。

secret：用户进入特权 EXEC 配置层的口令。

0 | 5 : 口令的加密类型, 0 无加密, 5 安全加密。

encrypted-password : 口令文本。

【命令模式】 全局配置模式

【使用指导】 配置不同权限级别的安全的口令。

📌 升高用户级别

【命令格式】 **enable** [*privilege-level*]

【参数说明】 *privilege-level* : 权限等级。

【命令模式】 特权用户模式

【使用指导】 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。

📌 降低用户级别


【命令格式】 **disable** [*privilege-level*]

【参数说明】 *privilege-level* : 权限等级

【命令模式】 特权用户模式

【使用指导】 从权限较高的级别切换到权限较低的级别需要输入相应级别的口令。

使用该命令从特权用户模式退到普通用户模式。如果加上权限等级, 则将当前权限等级降低到指定的权限等级。

 **disable** 命令后面所跟权限等级必须小于当前权限等级。

📌 设置命令的级别划分

【命令格式】 **privilege mode** [**all**] {**level level** | **reset**} *command-string*

【参数说明】 *mode* : 要授权的命令所属的 CLI 命令模式, 例如 :*config* 表示全局配置模式, *exec* 表示特权命令模式, *interface* 表示接口配置模式等等。

all : 将指定命令的所有子命令的权限, 变为相同的权限级别。

level level : 授权级别, 范围从 0 到 15。

reset : 将命令的执行权限恢复为默认级别。

command-string : 要授权的命令。

【命令模式】 全局模式

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

📌 指定 line 线路口令

【命令格式】 **password** [**0 | 7**] *line*

【参数说明】 **0** : 以明文方式配置口令。

7 : 以密文方式配置口令。

line : 配置的口令字符串。

【命令模式】 **line** 配置模式

【使用指导】 -

📌 启用 line 线路口令保护

【命令格式】 **login**

- 【参数说明】 -
- 【配置模式】 **line** 配置模式
- 【使用指导】 -

配置举例

配置命令授权

【网络环境】 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”）。

【配置方法】 ● 将 **reload** 命令及其子命令授予级别 1

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

【检验方法】 ● 进入 1 级，查看 **reload** 命令及子命令是否存在。

```
Ruijie# disable 1
Ruijie> reload ?
at                reload at
<cr>
```

常见错误

- 无

2.4.2 配置登录与认证

配置效果

- 建立线路登录身份认证。
- 通过网络设备上的 telnet 命令登录到远程设备上去。
- 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。
- 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。
- 使用锁住会话终端的功能，以防止访问。终端被锁定后，在终端下输入任何字符，系统都会提示输入解锁口令，口令认证成功，系统自动解锁。

注意事项

- 无

配置方法

▾ 配置本地用户

- 必选配置。
- 使用 **username** 命令配置用于本地身份认证和授权的账号信息，包括用户名、密码以及可选的授权信息
- 应在每台设备上配置本地身份认证的账号信息

▾ 线路登录进行本地认证

- 必选配置。
- 在 AAA 关闭时，LINE 线路登录认证时走本地用户认证。
- 应在每台设备上配置。

▾ 线路登录进行 AAA 认证

- 可选配置。AAA 设置为采用本地认证方法时需要配置。
- AAA 认证模式打开时，设置线路登录进行 AAA 认证。
- 应在每台设备上配置。

▾ 使用 telnet client

- 通过 telnet 登录到远程设备。
- 使用 do telnet client
- 通过 do telnet 登录到远程设备。

▾ 恢复已建立的 Telnet Client 会话连接

- 可选配置。Telnet Client 会话连接暂时退出后，如果需要恢复该连接，可以使用本命令恢复。

▾ 断开挂起的 Telnet Client 连接

- 可选配置。如果需要断开指定的 Telnet Client 连接，可以在 Telnet Client 设备上执行该配置项。

▾ 使用 Telnet Server

- 可选配置。需要使用 Telnet 登录本地设备时，需要打开该服务。
- 打开 Telnet Server 服务。

▾ 设置连接超时时间

- 可选配置。
- 当前已接受的连接，在指定时间内，没有任何输入时，将中断此连接。

- 在需要延长或缩短这段等待时间时，应执行此配置项。

📌 设置会话超时时间

- 可选配置。
- 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。
- 在需要延长或缩短这段等待时间时，应执行此配置项。

📌 会话锁定

- 可选配置。在已建立会话后需要临时离开设备时，在设备上执行会话锁定功能。
- 要使用会话锁定功能，需要在 line 配置模式下启用锁住 line 终端的功能，并在相应终端的 EXEC 模式下，通过使用 **lock** 命令锁住终端。

检验方法

- 使用 **show running-config** 命令可以查看配置。
- 在 AAA 关闭时，配置了本地用户以后，并在线路上设置采用本地认证。用户登录时将提示输入用户名和口令，认证通过后才允许进入命令行界面。
- 在 AAA 打开时，配置了本地用户后，并在 AAA 的登录认证方法中指定采用本地方法。用户登录时将提示输入用户名和口令，认证通过后才允许进入命令行界面。
- 已经登录进入命令行界面的用户，可以使用 **show user** 命令查看当前登录的用户信息。
- 在本地设备上开启 Telnet Server 后，用户可以使用 Telnet 客户端连接本地设备。
- 用户在被锁住的界面上输入回车后，会提示输入口令，只有口令与之前所设置的相符，才会解锁这个终端会话。
- 使用 **show sessions** 命令，可以查看已经建立的 Telnet Client 实例的每个实例信息。

相关命令

📌 配置本地用户

【命令格式】 **username** *name* [**login mode** { **console** | **ssh** | **telnet** }] [**online amount** *number*] [**permission** *oper-mode path*] [**privilege** *privilege-level*] [**reject remote-login**] [**web-auth**] [**nopassword** | **password**] [**0** | **7**] *text-string*]

【参数说明】 *name*：用户名。

login mode：配置账号的登录方式限制。

console：限制账号的登录方式为 console。

ssh：限制账号的登录方式为 ssh。

telnet：限制账号的的登录方式为 telnet。

online amount *number*：配置账号的同时在线数量。

permission *oper-mode path*：配置账号对指定文件的操作权限，*op-mode* 表示操作模式，*path* 表示作用的

文件或者目录的路径。

privilege *privilege-level* : 配置账号的权限级别, 取值范围 0 到 15。

reject remote-login : 限制使用该账号进行远程登录。

web-auth : 此账号只能用于 web 认证。

nopassword : 该账号不配置密码。

password [0 | 7] *text-string* : 配置账号的密码, 0 表示输入明文密码, 7 表示输入密文密码, 默认为输入明文密码。

【命令模式】 全局配置模式

【使用指导】 用于建立本地用户数据库, 供认证使用。

如果指定加密类型为 7, 则输入的合法密文长度必须为偶数。

通常无须指定加密类型为 7。一般情况下, 只有当复制并粘贴已经加密过的口令时, 才需要指定加密类型为 7。

↘ 线路登录进行本地认证

【命令格式】 **login local**

【参数说明】 -

【命令模式】 line 配置模式

【使用指导】 如果没有启用 AAA 安全服务, 则该命令用于配置 LINE 线路登录认证时走本地用户认证。这里的本地用户是指通过 **username** 命令配置的用户信息。

↘ 线路登录进行 AAA 认证

【命令格式】 **loginauthentication { default | *list-name* }**

【参数说明】 **default** : 默认的认证方法列表名。

list-name : 可选的方法列表名。

【配置模式】 line 配置模式

【使用指导】 AAA 认证模式打开时, 设置线路登录进行 AAA 认证。认证时使用 AAA 方法列表中的认证方法, 包括 Radius 认证、本地认证、无认证等。

↘ 使用 Telnet Client

【命令格式】 **telnet *host* [*port*] [/source { **ip** *A.B.C.D* | **interface** *interface-name* }]**

【参数说明】 *Host* : Telnet 服务器的 IPV4 地址或者主机名。

Port : Telnet 服务器的 TCP 端口号, 默认值为 23。

/source:指定 Telnet 客户端使用的源 IP 或者源接口。

ip *A.B.C.D* : 指定 Telnet 客户端使用的源 IPV4 地址。

interface *interface-name* : 指定 Telnet 客户端使用的源接口。

【命令模式】 特权用户模式

【使用指导】 通过 telnet 登录到远程设备, 可以是 IPV4 主机名、IPV4 地址。

↘ 使用 Do Telnet Client

【命令格式】 **do telnet *host* [*port*] [/source { **ip** *A.B.C.D* | **interface** *interface-name* }]**

【参数说明】 *Host* : Telnet 服务器的 IPV4 地址或者主机名。

Port : Telnet 服务器的 TCP 端口号, 默认值为 23。

/source:指定 Telnet 客户端使用的源 IP 或者源接口。

ip A.B.C.D :指定 Telnet 客户端使用的源 IPV4 地址。

interface interface-name :指定 Telnet 客户端使用的源接口。

【命令模式】 特权用户模式|配置模式|端口模式

【使用指导】 通过 do telnet 登录到远程设备，可以是 IPV4 主机名、IPV4 地址。

↘ 恢复已建立的 Telnet Client 会话连接

【命令格式】 <1-99>

【参数说明】 -

【命令模式】 普通用户模式

【使用指导】 该命令用于恢复使用已经建立的 Telnet Client 会话连接。当使用 **telnet** 命令发起 Telnet Client 会话连接时，可以使用热键 (ctrl+shift+6 x) 暂时退出该连接。如果需要恢复该连接，可以使用<1-99>命令进行恢复。同时，如果连接已建立，可以使用 **show sessions** 命令查看已建立的连接信息。

↘ 断开挂起的 Telnet Client 连接

【命令格式】 **disconnect session-id**

【参数说明】 *session-id* : 挂起的 Telnet Client 连接会话号。

【命令模式】 普通用户模式

【使用指导】 通过输入指定的 Telnet Client 连接会话号，断开指定的 Telnet Client 连接。

↘ 使用 Telnet Server

【命令格式】 **enable service telnet-server**

【参数说明】 -

【配置模式】 全局模式

【使用指导】 打开 Telnet Server 服务。

↘ 配置连接超时时间

【命令格式】 **exec-timeout minutes [seconds]**

【参数说明】 *minutes* : 指定的超时时间的分钟数。

seconds : 指定的超时时间的秒数。

【命令模式】 line 配置模式

【使用指导】 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。
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。

↘ 配置会话超时时间

【命令格式】 **session-timeout minutes[output]**

【参数说明】 *minutes* : 指定的超时时间的分钟数。

output : 是否将输出数据也作为输入，来判断是否超时。

【命令模式】 line 配置模式

【使用指导】 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。

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

▾ 启用锁住 line 终端的功能

- 【命令格式】 **lockable**
- 【参数说明】 -
- 【命令模式】 line 配置模式
- 【使用指导】 -

▾ 锁住当前 line 终端

- 【命令格式】 **lock**
- 【参数说明】 -
- 【配置模式】 line 配置模式
- 【使用指导】 -

配置举例

▾ 建立与远程网络设备的 Telnet 会话

- 【配置方法】
 - 建立与远程网络设备的 Telnet 会话，远程网络设备的 IP 地址是 192.168.65.119。
 - Telnet 支持在特权模式下配置，do telnet 支持在特配模式|配置模式|端口模式下配置

```
Ruijie# telnet 192.168.65.119
Trying 192.168.65.119 ... Open
User Access Verification
Password:
Ruijie(config)# do telnet 2AAA:BBBB::CCCC
Trying 2AAA:BBBB::CCCC ... Open
User Access Verification
Password:
Ruijie# telnet 2AAA:BBBB::CCCC
Trying 2AAA:BBBB::CCCC ... Open
User Access Verification
Password:
```

- 【检验方法】
 - 如果能正常与远程设备建立会话，则配置成功。

▾ 连接超时

- 【配置方法】
 - 设置超时时间为 20min

```
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
```

- 【检验方法】
 - 连接到本地设备的终端，在这段时间内容没有任何输入，将断开连接并退出。

设置超时时间为 20min

- 【配置方法】
- 设置超时时间为 20min

```
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
```

- 【检验方法】
- 连接到远程设备的终端，在这段时间内容没有任何输入，将断开连接并退出。

常见配置错误

- 无

2.4.3 设置系统基本参数

配置效果

- 设置系统的基本参数。


注意事项

- 无

配置方法

设置系统的日期和时钟

- 必选配置。
- 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。

 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。

更新硬件时钟

- 可选配置。
- 如果硬件时钟和软件时钟不同步，需要通过软件时钟的日期和时间复制给硬件时钟时，执行此配置项。

设置系统名称

- 可选配置。可以修改默认的系统名称。

↘ 设置命令提示符

- 可选配置。可以修改默认的命令提示符名称。

↘ 设置每日通知

- 可选配置。在希望告知使用者一些重要提示或警告信息时，可以选择在系统上设置每日通知。
- 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。

↘ 配置登录标题

- 可选配置。如果希望对使用者在登录或退出作一些重要信息的提示，可以选择配置此项。

↘ 设置控制台的传输速率

- 可选配置。可以修改默认的控制台速率。

检验方法

- 使用 **show clock** 命令来显示系统时间信息。
- 标题的信息将在你登录网络设备时显示。
- 使用 **show version** 命令查看系统、版本信息。

相关命令

↘ 设置系统的日期和时钟

【命令格式】 **clock set** *hh:mm:ss month day year*

【参数说明】 *hh:mm:ss*：当前时间，格式为小时（24 小时制）：分钟：秒。
day：日期（1-31），一个月中的日期。
month：月份（1-12），一年中的月份。
year：公元年（1993-2035），不能使用缩写。

【命令模式】 特权用户模式

【使用指导】 使用该命令设置系统时间，方便管理。

对于没有提供硬件时钟的网络设备，使用 **clock set** 设置网络设备上的时间仅对本次运行有效，当网络设备下电后，手工设置的时间将失效。

↘ 更新硬件时钟

【命令格式】 **clock update-calendar**

【参数说明】 -

【命令模式】 特权用户模式

【使用指导】 软件时钟就会覆盖硬件时钟的值。

↘ 设置系统名称

- 【命令格式】 **hostname name**
- 【参数说明】 *name*：系统名称，名称必须由可打印字符组成，长度不能超过 63 个字节。
- 【命令模式】 全局模式
- 【使用指导】 在全局配置模式下使用 **no hostname** 来将系统名称恢复缺省值。

设置命令提示符

- 【命令格式】 **prompt string**
- 【参数说明】 *string*：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。
- 【命令模式】 特权用户模式
- 【使用指导】 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。

设置每日通知

- 【命令格式】 **banner motd c message c**
- 【参数说明】 *c*：分界符，这个分界符可以是任何字符(比如'&'等字符)。
- 【命令模式】 全局配置模式
- 【使用指导】 输入分界符后，然后按回车键，即可以开始输入文本，需要在键入分界符并按回车键来结束文本的输入。需要注意的是，如果键入结束的分界符后仍然输入字符，则这些字符将被系统丢弃。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。

配置登录标题

- 【命令格式】 **banner login c message c**
- 【参数说明】 *c*：分界符，这个分界符可以是任何字符(比如'&'等字符)。
- 【命令模式】 全局配置模式
- 【使用指导】 输入分界符后，然后按回车键，即可以开始输入文本，需要在键入分界符并按回车键来结束文本的输入，需要注意的是，如果键入结束的分界符后仍然输入字符，则这些字符将被系统丢弃。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。
在全局配置模式下使用 **no banner login** 来删除登录标题。

设置控制台的传输速率

- 【命令格式】 **speed speed**
- 【参数说明】 *speed*：，单位是 bps。对于串行接口。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。
- 【命令模式】 line 配置模式
- 【使用指导】 用户可以根据需要来设置异步线路的波特率。命令 **speed** 将同时设置异步线路的接收速率以及发送速率。

配置举例

配置系统时间

- 【配置方法】 ● 把系统时间改成 2003-6-20，10:10:12

```
Ruijie# clock set 10:10:12 6 20 2003 //设置系统时间和日期
```

- 【检验方法】 ● 在特权模式下使用 **show clock** 命令来显示系统时间信息

```
Ruijie# show clock //确认修改系统时间生效
clock: 2003-6-20 10:10:54
```

配置每日通知

- 【配置方法】 ● 使用(#)作为分界符，每日通知的文本信息为“Notice: system will shutdown on July 6th.”

```
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)#
```

- 【检验方法】 ● 使用 **show running-config** 命令查看配置。
● 使用控制台、Telnet 或 SSH 连接本地设备，进入命令行界面之前时将显示每日通知信息。

```
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:
```

配置登录标题

- 【配置方法】 ● 使用(#)作为分界符，登录标题的文本为“Access for authorized users only. Please enter your password.”

```
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)#
```

- 【检验方法】 ● 使用 **show running-config** 命令查看配置。
● 使用控制台、Telnet 或 SSH 连接本地设备，进入命令行界面之前时将显示登录标题信息。

```
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:
```

如何将串口速率设置为 57600 bps

- 【配置方法】 ● 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
```

- 【检验方法】
- 使用 **show** 命令查看。

```
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
```

常见配置错误

- 无

2.4.4 打开或关闭指定的服务

配置效果

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

注意事项

-

配置方法

📌 打开 SNMP Server / SSH Server / Telnet Server

- 可选配置。在需要使用这些服务时执行此配置项。

检验方法

- 使用 **show running-config** 命令查看配置。
- 使用 **show services** 命令查看服务的开启状态。

相关命令

▾ 打开 SSH-Server/telnet-server/snmp-agent

【命令格式】 **enable service { ssh-server | telnet-server | snmp-agent }**

【参数说明】 **ssh-server** : 打开与关闭 SSH Server。
telnet-server : 打开与关闭 Telnet Server。
snmp-agent : 打开与关闭 Snmp Agent。

【命令模式】 全局模式

【使用指导】 该命令用于打开与关闭指定的服务。

配置举例

▾ 打开 SSH Server

【配置方法】 ● 打开 SSH Server

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

【检验方法】 ● 使用 **show running-config** 命令查看配置。
● 使用 **show ip ssh** 命令查看 SSH 服务配置和运行状况。

常见配置错误

无

2.4.5 设置重启策略

配置效果

设备在某些情况下需要重启，设置重启策略能使设备按照预设的方式进行重启。

注意事项

无

配置方法

直接重启

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。

定时重启

```
reload at hh:mm:ss month day year
```

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 `month day year` 是可选的,如果用户没有输入，则默认是系统时钟的年月日。

! 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,否则有可能会造成设置失效，比如将系统时间调到重启时间之后。

检验方法

-

相关命令

重启设备

【命令格式】 `reload [at { hh[:mm[:ss]] } [month [day [year]]]]`

【参数说明】 `at hh:mm:ss`：设置重启的时：分：秒，省略的部分使用系统当前的设置值。

`month`：月份（1-12）。

`day`：日期，从1到31。

`year`：公元年（1993-2035），不能使用缩写。

【命令模式】 特权用户模式

【使用指导】 使用该命令可以指定设备在指定的时刻启动，方便进行管理。

常见错误

- 无

2.4.6 批量执行文件中的命令

配置效果

批量执行指定文件中的命令。

注意事项

无

配置方法

通过 execute 命令实现

在 execute 命令的参数中指定需要批量执行的文件路径，执行 execute 命令即可。

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

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

检验方法

-

相关命令

- 【命令格式】 `execute { [flash:] filename }`
- 【参数说明】 `filename` 需要批处理的文件路径。
- 【命令模式】 特权用户模式
- 【使用指导】 使用该命令可以批量执行某个功能的相关命令，为用户提供方便。

常见错误

无

2.5 监视与维护

查看运行情况

作用	命令
show clock	显示当前系统时间。
show line { console line-num vty line-num line-num }	查看线路的配置信息。
show reload	查看系统的重新启动设置。
show running-config [interface interface]	查看当前设备系统正在运行的配置信息或某个接口下的配置信息。

show startup-config	查看存储在 NVRAM (非易失性随机存取存储器) 上设备的配置。
show version [devices module]	查看一些系统的信息。
show sessions	显示已经建立 Telnet Client 实例的每个实例信息。

3 LINE

3.1 概述

在网络设备上一般都具有多种类型的终端线路（line），并针对这些终端按类进行分组管理，对这些终端进行的配置称为线路（line）配置。在网络设备上，终端线路类型分为 CTY、VTY 等。

协议规范

- 无

3.2 典型应用

典型应用	场景描述
通过控制台访问设备	通过控制台进入网络设备的命令行界面。
通过VTY访问设备	通过 Telnet 或 SSH 进入网络设备的命令行界面。

3.2.1 通过控制台访问设备

应用场景



图 3-1

【注释】 A 为需要被管理的网络设备。
PC 为网络管理站。

功能部属

网络管理站使用串口线连接被管理的网络设备的控制台端口，用户在网络管理站上，通过控制台软件（超级终端或其他终端仿真软件）连接网络设备上的控制台并进入命令行界面，对网络设备进行配置和管理。

3.2.2 通过 VTY 访问设备

应用场景

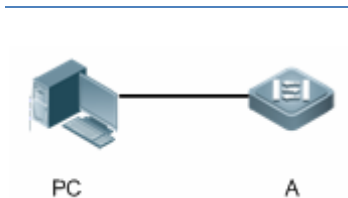


图 3-2

【注释】 A 为需要被管理的网络设备。
PC 为网络管理站。

功能部属

网络管理站和被管理的网络设备通过网络连接，用户在网络管理站上，通过 VTY 客户端软件（例如 Putty），使用 Telnet 或 SSH 连接网络设备上并进入命令行界面，对网络设备进行配置和管理。

3.3 功能详解

基本概念

CTY

CTY 线路类型指的是控制台端口（Console Port），大多数网络设备都会具有一个控制台端口，用户可以使用控制台终端，通过这个端口访问本地系统。

VTY

VTY 线路类型是虚拟终端线路，并没有与之对应的硬件，虚拟终端线路用于 Telnet 或 SSH 连接。

功能特性

功能特性	作用
基本功能	配置终端，显示、清除终端连接信息等。

3.3.1 基本功能

工作原理

无

相关配置

配置终端线路

在全局配置模式下，使用 **line** 命令可以进入指定的终端配置模式。

可以对终端的各项属性进行配置。

清除终端连接


当用户终端已经与设备连接时，对应的终端线路就处于占用状态，此时使用 **show user** 命令可以查看这些终端线路的连接状态。如果要使用户终端断开与网络设备的连接，可以使用 **clear line** 命令指定清除一个终端。被清除的终端线路上如果有关联的通讯协议（例如 Telnet、SSH 等）将会断开，已经进入的命令行界面也会退出。清除后的终端线路将恢复为非占用的状态，用户可以重新建立起连接。

设置 VTY 终端数目

使用 **line vty** 命令不仅可以进入 VTY 线路配置模式，还可以指定 VTY 终端的数目。

默认的 VTY 终端数目为 5 个，编号为 0~5。可以将终端数目最多扩展到 36 个，扩展的编号为 5~35。扩展的终端可以被删除，但默认的终端不可删除。

3.4 配置详解

配置项	配置建议 & 相关命令	
进入line模式	 必选配置。用于进入 line 模式。	
	line [console vty] first-line [last-line]	进入到指定的 LINE 模式
	line vty line-number	增加或减少当前可以使用的 VTY 连接数目

3.4.1 进入 line 模式

配置效果

进入 line 模式进行其他功能项的配置。

注意事项

无

配置方法

进入 LINE 模式

- 必选配置。
- 若无特殊情况，应在每台设备上进入 line 模式进行功能配置。

增加/减少 LINE VTY 数目

- 可选配置。
- 在需要增加或减少 LINE 线路时应使用此配置项。

检验方法

使用 `show line` 命令查看线路的配置信息。

相关命令

进入 LINE 模式

- 【命令格式】 `line [console | vty] first-line [last-line]`
- 【参数说明】 `console` : 控制台口。
`vty` : 虚终端线路，适用于 Telnet 或 SSH 连接。
`first-line` : 要进入的 first-line 编号。
`last-line` : 要进入的 last-line 编号。
- 【命令模式】 全局配置模式
- 【使用指导】 -

增加/减少 LINE VTY 数目

- 【命令格式】 `line vty line-number`
- 【参数说明】 `line-number` : VTY 连接数目，范围：0~35。
- 【命令模式】 全局配置模式
- 【使用指导】 使用 `no line vty line-number` 命令减少当前可以使用的 VTY 连接数目。

查看线路配置信息

- 【命令格式】 `show line { console line-num | vty line-num | line-num }`
- 【参数说明】 `console` : 控制台口。
`vty` : 虚终端线路，适用于 Telnet 或 SSH 连接。

line-num : 查看的 line 线路。

【命令模式】 特权配置模式

【使用指导】 -

配置举例

配置 VTY 终端扩展

【网络环境】

图 3-3



- 【配置方法】
- PC 使用控制台线连接网络设备 A，通过控制台终端进入命令行界面。
 - 执行 **show user** 查看终端线路连接状态。
 - 执行 **show line console 0** 查看控制台线路状态。
 - 进入全局配置模式，使用 **line vty** 命令将 VTY 终端数目扩展至 36 个。

A

```
Ruijie#show user
Line          User          Host(s)          Idle          Location
-----
* 0 con 0    ---          idle            00:00:00    ---

Ruijie#show line console 0

CON  Type  speed  Overruns
* 0   CON   9600   0
Line 0, Location: "", Type: "vt100"
Length: 24 lines, Width: 79 columns
Special Chars: Escape Disconnect Activation
                ^x      ^D      ^M
Timeouts:      Idle EXEC  Idle Session
                00:10:00  never
History is enabled, history size is 10.
Total input: 490 bytes
Total output: 59366 bytes
Data overflow: 0 bytes
stop rx interrupt: 0 times

Ruijie#show line vty ?
<0-5>  Line number
```

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#line vty 35
Ruijie(config-line)#
*Oct 31 18:56:43: %SYS-5-CONFIG_I: Configured from console by console
```

- 【检验方法】
- 输入 **show line** 命令，获取帮助时可以发现终端数量已经被扩展。
 - 执行 **show running-config** 命令查看配置。

A

```
Ruijie#show line vty ?
  <0-35> Line number

Ruijie#show running-config

Building configuration...
Current configuration : 761 bytes

version 11.0(1C2B1) (10/16/13 04:23:54 CST -ngcf78)
ip tcp not-send-rst
vlan 1
!
interface GigabitEthernet 0/0
!
interface GigabitEthernet 0/1
 ip address 192.168.23.164 255.255.255.0
!
interface GigabitEthernet 0/2
!
interface GigabitEthernet 0/3
!
interface GigabitEthernet 0/4
!
interface GigabitEthernet 0/5
!
interface GigabitEthernet 0/6
!
interface GigabitEthernet 0/7
!
interface Mgmt 0
!
line con 0
```

```
line vty 0 35
 login
 !
end
```

常见错误

无

3.4.2 配置 line 线路属性

配置效果

进入 line 模式后配置 line 线路属性。

注意事项

无

配置方法

▾ 设置线路的绝对超时时间

- 可选配置。
- 在需要 LINE 线路在规定时间内退出时可以使用 **absolute-timeout** 命令进行配置。

▾ 设置激活一个空的终端会话的字符

- 可选配置。
- 在登录并激活终端时，可以根据需要在 LINE 线路上使用 **activation-character** 命令进行配置。

▾ 开启命令自动执行功能

- 可选配置。
- 对于异步串口的终端用户可以在 LINE 线路上使用此配置项，设置命令自动执行的操作。

▾ 设置异步线路在流通讯模式下每个字符的数据位数量

- 可选配置。
- 可以在 LINE 线路上使用 **databits** 命令进行配置。

▾ 设置异步线路上命令行处理(EXEC)的字符编码方式

- 可选配置。
- 可以在 LINE 线路上使用 `exec-character-bits` 命令进行配置。

▾ 设置异步线路的流控模式

- 可选配置。
- 可以在 LINE 线路上使用 `flowcontrol` 命令进行配置。

▾ 设置异步线路的校验位

- 可选配置。
- 可以在 LINE 线路上使用 `parity` 命令进行配置。

▾ 设置异步线路的软流控的启动字符

- 可选配置。
- 可以在 LINE 线路上使用 `start-character` 命令进行配置。

▾ 设置异步线路的软流控的终止字符

- 可选配置。
- 可以在 LINE 线路上使用 `stop-character` 命令进行配置。

▾ 设置在异步线路上传输的每个字节中停止位的个数

- 可选配置。
- 可以在 LINE 线路上使用 `stopbits` 命令进行配置。

▾ 设置异步线路终端模拟的终端类型

- 可选配置。
- 可以在 LINE 线路上使用 `terminal-type` 命令进行配置。

检验方法

使用 `show line` 命令查看线路的配置信息。

相关命令

▾ 设置线路的绝对超时时间

【命令格式】 `absolute-timeout minutes`

【参数说明】 `minutes`：当前线路绝对超时的分钟数，取值范围为<0~60>。

【命令模式】 LINE 配置模式

【使用指导】 设置线路的绝对超时时间，只要时间一到，不管用户是否在操作终端，线路都会断开。线路断开前会提示终端

即将退出剩余时间：

```
Terminal will be login out after 20 second
```

✎ 设置用来激活一个空的终端会话的字符

【命令格式】 **activation-character** *ascii-value*

【参数说明】 *ascii-value*：激活终端会话的热键字符对应的 ASCII 值，取值范围为<0~127>。

【命令模式】 LINE 配置模式

【使用指导】 如果当前线路设置了自动选择(**autoselect**)功能，对应的激活终端会话的热键字符必须取系统缺省值才有效。

✎ 开启命令自动执行功能

【命令格式】 **autocommand** *autocommand-string*

【参数说明】 *autocommand-string*：将自动执行的命令行。

【命令模式】 LINE 配置模式

【使用指导】 **autocommand** 常见的应用是用户以哑终端方式，通过异步串口与路由器建立连接后，再通过 **autocommand** 指定的 Telnet 命令远程登录指定主机上或者通过 **autocommand** 命令获得指定的基于应用的终端服务功能。

✎ 设置异步线路在流通讯模式下每个字符的数据位数量

【命令格式】 **databits** *bit*

【参数说明】 *bit*：每个字符的数据位，取值范围为<5~8>。

【命令模式】 LINE 配置模式

【使用指导】 路由器的异步线路设备(如异步串口，AUX 口等等)在流通讯模式下产生带校验的 7 个数据位。如果校验产生，就指定数据位为 7。如果没有产生校验，就指定数据位为 8。数据位为 5 或者 6 的情况，只有在较老的设备上才会有应用，并且经常不使用。

✎ 设置异步线路上命令行处理(EXEC)的字符编码方式

【命令格式】 **exec-character-bits** { 7 | 8 }

【参数说明】 7：选择 7 位字符集合作为命令行处理的字符集合。

8：选择全 8 位字符集合作为命令行处理的字符集合。

【命令模式】 LINE 配置模式

【使用指导】 如果要在命令行中输入汉字或者显示汉字、图形或者其它国际字符，必须确保设置 **exec-character-bits 8**。

✎ 设置异步线路的流控模式

【命令格式】 **flowcontrol** { **hardware** | **none** | **software** }

【参数说明】 **hardware**：流控模式为硬流控。

none：流控模式为无流控。

software：流控模式为软流控。

【命令模式】 LINE 配置模式

【使用指导】 用户可以使用本命令来设置流控，从而可能控制从某一地发送数据的速度，使它与另一个接收点接收数据的速度相同。由于终端在数据发送的时候不能接收数据，所以设置流控可以防止数据的丢失。另外，在数据高速处理设备与低速处理设备之间(比如打印机与网络接口)也需要设置流控来确保数据不丢失。RGOS 提供两种方式实现流控：软件流控(**software flowcontrol**)，也称之为软流控，它使用控制键操作；硬件流控(**hardware**

flowcontrol)，也称之为硬流控，它使用硬件来进行。对于软流控，系统缺省的终止与启动字符分别是 Ctrl+S(XOFF，ASCII 值为 19)和 Ctrl+Q(XON，ASCII 值为 17)，系统也提供命令 **stop-character**、**start-character** 来设置它们。

设置异步线路的校验位

【命令格式】 **parity { even | none | odd }**

【参数说明】 **even**：偶校验。

none：无校验。**odd**：奇校验。

【命令模式】 LINE 配置模式

【使用指导】 使用某些设备(如异步串口、控制台口等)通讯的时候，常要求设置一个具体的校验位。

设置异步线路的软流控的启动字符

【命令格式】 **start-character ascii-value**

【参数说明】 *ascii-value*：异步线路的软流控的启动字符对应的 ASCII 值，取值范围为<0~255>。

【命令模式】 LINE 配置模式

【使用指导】 当异步线路上流控模式为软流控时，软流控启动字符标志着数据传输的开始。

设置异步线路的软流控的终止字符

【命令格式】 **stop-character ascii-value**

【参数说明】 *ascii-value*：异步线路的软流控的终止字符对应的 ASCII 值，取值范围为<0~255>。

【命令模式】 LINE 配置模式

【使用指导】 当异步线路上流控模式为软流控时，软流控终止字符标志着数据传输的结束。

设置在异步线路上传输的每个字节中停止位的个数

【命令格式】 **stopbits { 1 | 2 }**

【参数说明】 **1**：1 个停止位。

2：2 个停止位。

【命令模式】 LINE 配置模式

【使用指导】 异步线路与相连的异步设备(如传统哑终端、调制解调器 Modem 等)通讯常常需要设置通讯的停止位。

设置异步线路终端模拟的终端类型

【命令格式】 **terminal-type terminal-type-string**

【参数说明】 *terminal-type-string*：终端类型描述字符串，如 vt100，ansi 等等。

【命令模式】 LINE 配置模式

【使用指导】 用户也可以使用命令 **terminal-type vt100** 来恢复系统默认的线路终端模拟的终端类型。在进行 Telnet 连接等场合，用户可以根据需要使用本命令来设置线路终端模拟的终端类型。线路上进行 Telnet 连接的时候，就会使用该终端类型来进行终端类型协商(Telnet 选项协商号为 0x18)，详细内容可以参考 RFC 854。

配置举例

配置 line 线路的波特率、数据位、校验位及停止位

【网络环境】

图 3-4



【配置方法】

- PC 使用控制台线连接网络设备 A，通过控制台终端进入命令行界面。
- 进入全局配置模式，配置 line 线路的波特率、数据位、校验位、停止位。
- 执行 **show line console 0** 查看控制台线路状态。

A

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#line console 0
Ruijie(config-line)#speed 115200
Ruijie(config-line)#databits 8
Ruijie(config-line)#parity even
Ruijie(config-line)#stopbits 1
Ruijie#show line console 0

CON      Type      speed    Overruns
* 0      CON      115200  0
Line 0, Location: "", Type: "vt100"
Length: 24 lines, Width: 79 columns
Special Chars: Escape Disconnect Activation
                ^x      none
Timeouts:      Idle EXEC    Idle Session
                00:10:00  never
History is enabled, history size is 10.
Total input: 636 bytes
Total output: 30498 bytes
Data overflow: 0 bytes
stop rx interrupt: 0 times
```

【检验方法】

- 执行 **show running-config** 命令查看配置。

A

```
Ruijie#show line vty ?
<0-35> Line number

Ruijie#show running-config

Building configuration...
Current configuration : 761 bytes
```

```
version 11.0(1C2B1) (10/16/13 04:23:54 CST -ngcf78)
ip tcp not-send-rst
vlan 1
!
interface GigabitEthernet 0/0
!
interface GigabitEthernet 0/1
 ip address 192.168.23.164 255.255.255.0
!
interface GigabitEthernet 0/2
!
interface GigabitEthernet 0/3
!
interface GigabitEthernet 0/4
!
interface GigabitEthernet 0/5
!
interface GigabitEthernet 0/6
!
interface GigabitEthernet 0/7
!
interface Mgmt 0
!
line con 0
 parity even
 stopbits 1
 speed 115200
line vty 0 35
 login
!
end
```

常见错误

无

3.4.3 配置当前终端属性

配置效果

在当前终端特权模式下进行配置。

注意事项

无

配置方法

✎ 设置当前终端在流通讯模式下每个字符的数据位数量

- 可选配置。
- 可以在当前终端上使用 `terminal databits` 命令进行配置。

✎ 设置当前终端上命令行处理(EXEC)的字符编码方式

- 可选配置。
- 可以在当前终端上使用 `terminal exec-character-bits` 命令进行配置。

✎ 设置当前终端的流控模式

- 可选配置。
- 可以在当前终端上使用 `terminal flowcontrol` 命令进行配置。

✎ 设置当前终端上异步线路的校验位

- 可选配置。
- 可以在当前终端上使用 `terminal parity` 命令进行配置。

✎ 设置当前终端上的软流控的启动字符

- 可选配置。
- 可以在当前终端上使用 `terminal start-character` 命令进行配置。

✎ 设置当前终端上的软流控的终止字符

- 可选配置。
- 可以在当前终端上使用 `terminal stop-character` 命令进行配置。

✎ 设置当前终端上传输的每个字节中停止位的个数

- 可选配置。
- 可以在当前终端上使用 `terminal stopbits` 命令进行配置。

✎ 设置当前终端上终端模拟的终端类型

- 可选配置。

- 可以在当前终端上使用 **terminal terminal-type**命令进行配置。

检验方法

使用 **show line** 命令查看线路的配置信息。

相关命令

▾ 设置当前终端在流通讯模式下每个字符的数据位数量

- 【命令格式】 **terminal databits** *bit*
- 【参数说明】 *bit* : 每个字符的数据位, 取值范围为<5~8>。
- 【命令模式】 特权用户模式
- 【使用指导】 -

▾ 设置当前终端上命令行处理(EXEC)的字符编码方式

- 【命令格式】 **terminal exec-character-bits** { 7 | 8 }
- 【参数说明】 7 : 选择 7 位字符集作为命令行处理的字符集合。
8 : 选择全 8 位字符集作为命令行处理的字符集合。
- 【命令模式】 特权用户模式
- 【使用指导】 如果要在命令行中输入汉字或者显示汉字、图形或者其它国际字符, 必须确保设置 **terminal exec-character-bits 8**。

▾ 设置当前终端的流控模式

- 【命令格式】 **terminal flowcontrol** { hardware | none | software }
- 【参数说明】 **hardware** : 流控模式为硬流控。
none : 流控模式为无流控。
software : 流控模式为软流控。
- 【命令模式】 特权用户模式
- 【使用指导】 -

▾ 设置当前终端上异步线路的校验位

- 【命令格式】 **terminal parity** { even | none | odd }
- 【参数说明】 **even** : 偶校验。
none : 无校验。
odd : 奇校验。
- 【命令模式】 LINE 配置模式
- 【使用指导】 使用某些设备(如异步串口、控制台口等)通讯的时候, 常要求设置一个具体的校验位。

▾ 设置当前终端上的软流控的启动字符

- 【命令格式】 **terminal start-character** *ascii-value*

【参数说明】 *ascii-value* : 异步线路的软流控的启动字符对应的 ASCII 值, 取值范围为<0~255>。

【命令模式】 特权用户模式

【使用指导】 -

设置当前终端上的软流控的终止字符

【命令格式】 **terminal stop-character** *ascii-value*

【参数说明】 *ascii-value* : 异步线路的软流控的终止字符对应的 ASCII 值, 取值范围为<0~255>。

【命令模式】 特权用户模式

【使用指导】 -

设置当前终端上传输的每个字节中停止位的个数

【命令格式】 **terminal stopbits** { 1 | 2 }

【参数说明】 1 : 1 个停止位。

2 : 2 个停止位。

【命令模式】 特权用户模式

【使用指导】 -

设置当前终端上终端模拟的终端类型

【命令格式】 **terminal terminal-type** *terminal-type-string*

【参数说明】 *terminal-type-string* : 终端类型描述字符串, 如 vt100, ansi 等等。

【命令模式】 特权用户模式

【使用指导】 -

配置举例

配置当前终端的终端类型和波特率

【网络环境】

图 3-5



【配置方法】

- PC 使用控制台线连接网络设备 A, 通过控制台终端进入命令行界面。
- 进入特权用户模式, 配置当前终端的终端类型和波特率。

```
A Ruijie#terminal terminal-type ansi
Ruijie#terminal speed 115200
```

【检验方法】

- 执行 **show line console 0** 查看控制台线路状态。

```
A Ruijie#show line console 0

CON      Type      speed  Overruns
```


```
* 0    CON    115200  0
Line 0, Location: "", Type: "ansi"
Length: 24 lines, Width: 79 columns
Special Chars: Escape Disconnect Activation
             ^x    none
Timeouts:    Idle EXEC    Idle Session
             00:10:00    never
History is enabled, history size is 10.
Total input: 858 bytes
Total output: 57371 bytes
Data overflow: 0 bytes
stop rx interrupt: 0 times
```

常见错误

无

3.5 监视与维护

清除各类信息

 在设备运行过程中执行 **clear** 命令，可能因为重要信息丢失而导致业务中断。

作用	命令
清除线路的连接状态。	clear line { console <i>line-num</i> vty <i>line-num</i> <i>line-num</i> }

查看运行情况

作用	命令
查看线路的配置信息。	show line { console <i>line-num</i> vty <i>line-num</i> <i>line-num</i> }

4 TIME RANGE

4.1 概述

Time range 是一个时间控制服务，它提供给某些应用进行时间控制。例如，如果想要让 ACL 在一个星期的某些时间段内生效，可以配置一个 time range 并让 ACL 和这个 time range 相关联。

4.2 功能详解

基本概念

▾ 绝对时间区间

绝对时间区间是指可以为 time range 设置一个起始时间以及结束时间的区间。典型的绝对时间区间例如[2000 年 1 月 1 日 12 : 00 , 2001 年 1 月 1 日 12 : 00]。Time range 应用关联到这个 time range 之后，可以在该时间区间之内使某项功能起作用。

▾ 周期时间

周期时间是指可以为 time range 设置一个周期性的时间。典型的周期时间如“每周一 8 : 00 到每周五 17 : 00”。Time range 应用关联到这个 time range 之后，可以周期性地每周一到每周五使某项功能起作用。

功能特性

功能特性	作用
使用绝对时间区间	设置绝对时间区间允许 time range 应用在这个绝对时间区间之内使某项功能生效。
使用周期时间	设置周期时间允许 time range 应用在某个周期性的时间之内使某项功能生效。

4.2.1 使用绝对时间区间

工作原理

基于 time range 的应用在开启某项功能时，会判断当前的时间是否处于绝对时间区间之内，如果在其中，则可以让该功能在当前时间生效或者在当前时间不生效。

4.2.2 使用周期时间

工作原理

基于 time range 的应用在开启某项功能时，会判断当前的时间是否处于周期时间之内，如果在其中，则可以让该功能在当前时间生效或者在当前时间不生效。

4.3 配置详解

配置项	配置建议 & 相关命令	
配置time range	 必须配置。如果要使用 time range 功能，必须配置 time range。	
	time-range <i>time-range-name</i>	配置 time range。
	 可选配置。配置分类参数。	
	absolute { [start time date] [end time date] }	配置绝对时间区间。
	periodic <i>day-of-the-week</i> <i>time</i> to [<i>day-of-the-week</i>] <i>time</i>	配置周期时间。

4.3.1 配置time range

配置效果

- 配置 time range，配置其绝对时间区间或周期时间，以便让 time range 应用在对应的时间区间内使某项功能生效。

注意事项

无

配置方法

配置 time range

- 必须配置，在需要应用 time range 的设备上配置。

【命令格式】 **time-range** *time-range-name*

【参数说明】 *time-range-name*：要创建的 time range 的名字。

【缺省配置】 没有配置 time range

【命令模式】 全局模式

【使用指导】 有些应用（例如 ACL）可能基于时间运行，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，必须首先配置一个 Time-Range。创建完 time range 之后，可以在 time range 模式中配置相应的时间控制。

配置绝对时间区间

- 可选配置。

- 【命令格式】 **absolute** { *start time date* [*end time date*] }
- 【参数说明】 **start time date** : 区间的开始时间。
end time date : 区间的结束时间。
最大时间区间为 0 年 1 月 1 日 00 : 00 , 9999 年 12 月 31 日 23 : 59
- 【缺省配置】 没有配置绝对时间区间, 缺省时为最大时间区间。
- 【命令模式】 time-range 模式
- 【使用指导】 如果想要让某个功能在一个绝对时间区间内生效, 可以使用 **absolute** 命令配置一个开始和结束的时间区间。

配置周期时间

- 可选配置。

- 【命令格式】 **periodic** *day-of-the-week time to* [*day-of-the-week*] *time*
- 【参数说明】 *day-of-the-week* : 周期时间开始或者结束是在星期几
time : 周期时间开始或者结束是在几点几分
- 【缺省配置】 没有配置周期时间, 缺省时认为在周期时间内
- 【命令模式】 time-range 模式
- 【使用指导】 如果想要让某个功能在一个周期时间内生效, 可以使用 **periodic** 命令配置一个周期时间。没有配置周期时间, 默认认为在周期时间内生效。业务在修订某个周期时间前, 建议先解除关联 timerange, 等修订完之后再关联上。

检验方法

- 使用 **show time-range** [*time-range-name*]命令, 可以查看所配置的 time range 信息。

- 【命令格式】 **show time-range** [*time-range-name*]
- 【参数说明】 *time-range-name* : 可以指定显示某个 time range 的信息
- 【命令模式】 特权模式
- 【使用指导】 验证配置的 time range 是否正确。
- 【命令展示】 1 : 显示 time range 信息 :

```
Ruijie# show time-range
time-range entry: test (inactive)
absolute end 01:02 02 February 2012
```

4.4 监视与维护

查看运行情况

作用	命令
显示 time range。	show time-range [<i>time-range-name</i>]

5 HTTP服务

5.1 概述

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

协议规范

- RFC1945 : Hypertext Transfer Protocol -- HTTP/1.0
- RFC2616 : Hypertext Transfer Protocol -- HTTP/1.1

5.2 典型应用

典型应用	场景描述
HTTP应用服务	用户通过 Web 管理设备。

5.2.1 HTTP应用服务

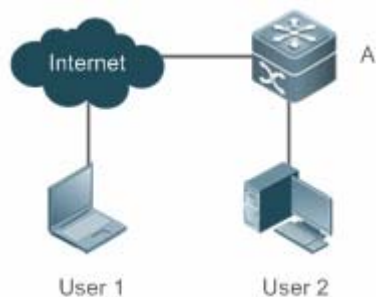
应用场景

设备开启 HTTP 服务后, 用户只需在 PC 机浏览器中输入 http://+设备的 IP 地址, 认证通过后就可以登陆到 Web 管理界面。在 Web 界面中, 用户可以进行设备状态信息监控、配置设备、上传和下载文件等操作。

以下图为例, 用户进行 Web 管理。

- 用户可以通过 Internet 进行远程访问设备, 也可以在本地局域网中通过登陆 Web 服务器对设备进行配置管理。
- 用户还可以再浏览器上设置使用 HTTP/1.0 还是 HTTP/1.1 协议来访问设备的 HTTP 服务。

图 5-1



【注释】 A 为锐捷设备。
用户 User1 通过 Internet 网络访问设备。

用户 User2 通过局域网访问设备。

功能部署

- 设备运行 HTTP 协议，用户在 PC 浏览器中通过 `http://设备的 ip 地址`，访问设备。

5.3 功能详解

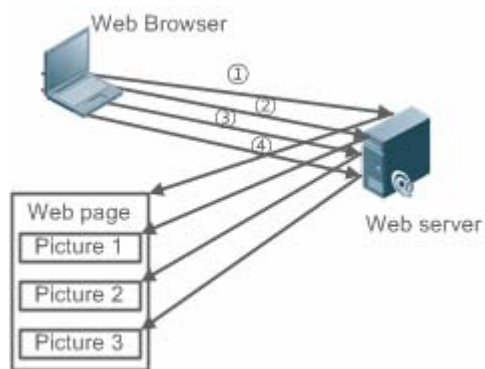
基本概念

HTTP 服务

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

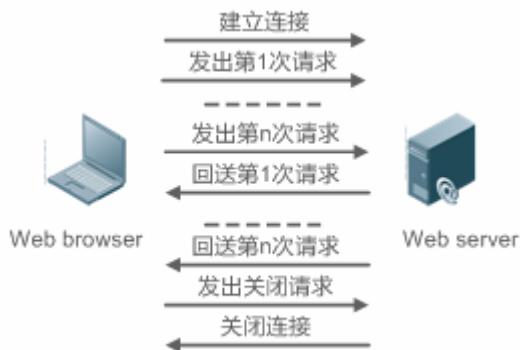
例如一个网页中可能需要很多图片，网页中包括的不是真正的图片内容，而是它们的 URL 连接地址，这样浏览器在访问过程中会发出多次请求，每次请求都要建立一个单独的连接，每次连接都是完全隔离的。建立和释放连接是一个相对费力的过程，从而严重影响了客户机和服务器的性能，如下图所示。

图 5-2



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

图 5-3



目前，锐捷设备支持 HTTP/1.0 和 HTTP/1.1 两种协议版本。

i 设备使用哪种协议版本由 Web 浏览器决定。

HTTP 升级服务

本地升级时，设备作为 HTTP 服务器，用户通过 Web 浏览器登陆到设备，将需要升级的文件上传到设备，实现设备上文件的升级。

功能特性

功能特性	作用
HTTP服务	用户通过 Web 界面登陆到设备中进行配置与管理。
HTTP本地升级服务	将需要升级的文件上传到设备，实现设备上文件的升级。

5.3.1 HTTP服务

HTTP 是为 Web 管理提供服务，用户通过 Web 界面登陆到设备中进行配置与管理。

工作原理

Web 管理包括 Web 客户端和 Web 服务器，同理 HTTP 服务也采用客户端/服务器模式。HTTP 客户端内嵌在 Web 管理客户端的 Web 浏览器中，能够发送 HTTP 报文和接收处理 HTTP 响应报文。而 Web 服务器(即 HTTP 服务器)则内嵌于设备中。客户端和服务器之间的信息交互过程如下：

- 在客户端与服务器之间建立 TCP 连接，HTTP 服务默认端口号是 80。
- 客户端向服务器发送请求消息。
- 服务器解析客户端发送的请求，请求内容包括获取 web 页面、执行 cli 命令，上传文件等。
- 服务器执行完请求内容后，将响应发送回给客户端。

相关配置

使能 HTTP 服务

缺省情况下，HTTP 服务功能关闭。

使用 **enable service web-server** 命令可以使能 HTTP 服务功能，包括 HTTP 服务。

必须使能 HTTP 服务功能，用户才能通过 Web 界面登陆到设备中进行配置与管理。

📌 配置 HTTP 认证信息

缺省情况下，系统默认创建两个账号，admin 账号和 guest 账号，这两个账号不可被删除，只可修改密码。其中 guest 账号默认对应 level 2 权限，在 web 端只拥有查看系统首页的权限。管理员账号为 admin 对应 level 0 权限，在 web 端管理员账号拥有所有的功能，并且可以编辑其他管理账号并授权该账号可访问的页面，新添加的账号对应 level 1 权限。

使用 **webmaster level** 命令可以配置认证的用户名和密码。

通过配置该命令，用户需要输入所配置的用户名和密码进行认证才能登陆 Web 页面。

📌 配置 HTTP 服务端口

缺省情况下，HTTP 服务端口为 80。

使用 **http port** 命令可以配置 HTTP 服务端口号，取值范围是 80 及 1025-65535。

通过配置 HTTP 服务端口号，可以减少非法用户对 HTTP 服务的攻击。

5.3.2 HTTP本地升级服务

设备作为 HTTP 服务器，用户通过 Web 浏览器登陆到设备，将需要升级的文件（包括组件包、web 包）上传到设备或者直接通过 tftp 上传文件到设备中。

工作原理

- 通过 Web 的“本地升级”功能上传组件包或 web 包
- 设备接收文件信息，接收成功后进行版本与合法性校验
- 文件校验成功后，如果是 web 包，直接升级；如果是组件包，用户在浏览器端通过是否重启设备来决定升级与否。

相关配置

📌 更新 Web 包

使用 **upgrade web download** 命令从 TFTP 服务器上下载 WEB 包。

通过配置该命令，从 TFTP 服务器上下载 WEB 包，合法性校验通过后，WEB 包直接进行升级，无需重启设备。

也可以使用 **upgrade web** 命令直接升级本地存在的 WEB 包。

📌 更新子系统组件

缺省情况下，不管是通过浏览器还是 TFTP 上传子系统组件，设备默认都是不升级的。

用户要升级子系统组件，都必须重启设备。

5.4 配置详解

配置项	配置建议 & 相关命令	
配置HTTP服务	 必须配置。用于启动 HTTP 服务。	
	enable service web-server	使能 HTTP 服务
	webmaster level	配置 HTTP 认证信息
	http port	配置 HTTP 服务端口
配置HTTP本地升级	 必须配置。用于实现 HTTP 本地升级。	
	upgrade web	升级设备存放的 WEB 包。
	upgrade web download	自动从服务器上下载 WEB 包，并自动升级

5.4.1 配置HTTP服务

配置效果

设备开启 HTTP 服务，用户通过认证后可以登陆到 Web 管理界面，进行设备状态信息监控、配置设备、上传和下载文件等操作。

配置方法

▾ 使能 HTTP 服务

- 必须配置。
- 若无特殊要求，应在每台锐捷设备上使能 HTTP 服务，否则 web 服务不可访问。

▾ 配置 HTTP 认证信息

- 默认情况下，已经配置用户名 admin、guest，对应的密码是 admin、guest。
- 若无特殊要求，用户可以使用默认的用户名登陆 web 页面，直接通过 web 浏览器来更新认证信息；如果一直使用默认账户，会存在安全隐患，因为 IP 一旦泄露，非授权人员就可以通过 web 获取到设备的配置信息等。

▾ 配置 HTTP 服务端口

- 如果要求改变 HTTP 服务端口，则必须配置 HTTP 服务端口。
- 若无特殊要求，可以使用默认的 HTTP 服务端口 80 进行访问。

检验方法

- 用户在浏览器上输入 `http://设备的ip:服务端口`，验证浏览器是否会跳转到认证页面。

相关命令

使能 HTTP 服务

【命令格式】 **enable service web-server [http | all]**

【参数说明】 **http | all** : 打开相应的服务。**http** 为打开 HTTP 服务。

【命令模式】 全局模式

【使用指导】 如果执行该命令时后面不跟任何关键字或者跟 **all** ,则表示同时打开 HTTP 服务 ;如果跟 **http** 关键字 ,则表示只打开 HTTP 服务。

使用 **no enable service web-server** 或者 **default enable service web-server** 用于关闭相应的 HTTP 服务。

配置 HTTP 认证信息

【命令格式】 **webmaster level privilege-level username name password { password | [0 | 7] encrypted-password }**

【参数说明】 *privilege-level* : 用户绑定权限等级。

name : 用户名。

password : 用户口令。

0 | 7 : 口令的加密类型 , 0 无加密 , 7 简单加密。缺省为 0。

encrypted-password : 口令文本。

【命令模式】 全局模式

【使用指导】 在使用 HTTP Server 的时候 , 需要进行登陆认证才能进入 Web 页面。使用该命令配置 Web 登陆认证的用户名和密码。

执行 **no webmaster level privilege-level** 删除指定权限等级的所有用户名与密码。

执行 **no webmaster level privilege-level username name** 删除指定用户名和密码。

i 用户名和密码有三个权限等级 ; 每个权限等级最多可以配置 10 个用户名和密码。

i 系统默认创建两个账号 , **admin** 账号和 **guest** 账号 , 这两个账号不可被删除 , 只可修改密码。其中 **guest** 账号默认对应 level 2 权限 , 在 web 端只拥有查看系统首页的权限。管理员账号为 **admin** 对应 level 0 权限 , 在 web 端管理员账号拥有所有的功能 , 并且可以编辑其他管理账号并授权该账号可访问的页面 , 新添加的账号对应 level 1 权限。

配置 HTTP 服务端口

【命令格式】 **http port port-number**

【参数说明】 *port-number* : 设置 HTTP 服务端口 , 取值范围为 80 及 1025-65535。

【命令模式】 全局模式

【使用指导】 使用该命令设置 HTTP 服务的端口。

配置举例

使用 Web 管理一台锐捷设备 , 通过 Web 浏览器登陆到锐捷中进行相关功能的配置

- 使用默认配置的 **admin** 认证信息进行登录。

- 为了提高安全性，要求 Web 浏览器即可以通过 HTTP 协议访问。
- 要求自己配置 HTTP 服务端口，减少非法用户对 HTTP 的攻击。

【网络环境】

图 5-4

**【配置方法】**

- 需要配置同时打开 HTTP 服务。
- 可以配置 HTTP 服务端口号为 8080.

A

```
A#configure terminal
A(config)# enable service web-server
A(config)# http port 8080
```

【检验方法】

查看 HTTP 配置信息。

A

```
A# show web-server status
http server status: enabled
http server port: 8080
```

常见错误

- 如果 HTTP 服务端口不是默认的 80 与 443，用户在浏览器中必须输入配置的具体服务端口，否则 web 端无法访问设备。

5.4.2 配置HTTP本地升级

配置效果

用户可以通过浏览器或者 upgrade web 命令升级。

注意事项

- 通过浏览器上传 Web 包，只要上传成功，并且版本校验通过，设备默认会直接升级为最新的 Web 包。
- 通过 **upgrade web download** 命令，自动从 tftp 服务器下载文件，并自动升级。
- 通过 **upgrade web** 命令，自动升级本地文件系统的 WEB 包。

配置方法

无

检验方法

- 用户直接通过浏览器访问，通过查看最新的 WEB 页面。

相关命令

从 TFTP 服务器下载 Web 文件包

- 【命令格式】 `upgrade web download tftp: path`
- 【参数说明】 `tftp`：表示通过普通数据口连接 tftp 服务器下载 WEB 包。
`path`：tftp 服务器上 WEB 包的路径。
- 【命令模式】 特权模式
- 【使用指导】 该命令是从 tftp server 端中下载 WEB 包，并自动升级。

从升级设备的 Web 文件包

- 【命令格式】 `upgrade web uri`
- 【参数说明】 `uri`：WEB 包存放的本地路径。
- 【命令模式】 特权模式
- 【使用指导】 该命令用于升级设备内存放的 WEB 包，并自动升级。

配置举例

用户通过官网获取到最新的 Web 包，希望设备运行最新的 Web 包

【网络环境】

图 5-5



- 与本地 PC 机相连，PC 机的 IP 地址是 10.10.10.13；给设备配置一个同网段的 IP 地址 10.10.10.131。
- 通过 web 登陆到设备中，并上传最新的 WEB 包到设备中。

A

```
A#configure terminal
A(config)# vlan 1
A(config-vlan)# exit
A(config)# interface vlan 1
A(config-VLAN 1)# ip address 10.10.10.131 255.255.255.0
A(config-VLAN 1)# exit
A(config)# enable service web-server
```

在 PC 机中，使用 WEB 页面的“本地升级”功能上传 WEB 包升级

- 【检验方法】 在 PC 机中，重新进行 Web 认证登陆，验证是否显示最新的 Web 页面。

通过 upgrade web download 方式升级 WEB 包

【网络环境】

图 5-6



【配置方法】

- 与本地 PC 机相连，PC 机的 IP 地址是 10.10.10.13；给设备配置一个同网段的 IP 地址 10.10.10.131。
- 打开 tftp 服务器。

A

```
A#configure terminal
A(config)# vlan 1
A(config-vlan)# exit
A(config)# interface vlan 1
A(config-VLAN 1)# ip address 10.10.10.131 255.255.255.0
A(config-VLAN 1)# end
A#upgrade web download tftp:// 10.10.10.13/web.upd
Press Ctrl+C to quit
!!!!!!!!!!
download 3896704 bytes
Begin to upgrade the web package...
Web package upgrade successfully.
```

【检验方法】 在 PC 机中，重新进行 Web 认证登陆，验证是否显示最新的 Web 页面。

通过 upgrade web 方式升级 WEB 包

【网络环境】

图 5-7



【配置方法】

- 与本地 PC 机相连，PC 机的 IP 地址是 10.10.10.13；给设备配置一个同网段的 IP 地址 10.10.10.131。
- 打开 tftp 服务器。

A

```
A#configure terminal
A(config)# vlan 1
A(config-vlan)# exit
A(config)# interface vlan 1
A(config-VLAN 1)# ip address 10.10.10.131 255.255.255.0
A(config-VLAN 1)# end
A#copy tftp://10.10.10.13/web.upd flash:/web.upd
Press Ctrl+C to quit
!!!!!!!!!!
Accessing tftp:// 10.10.10.13/web.upd finished, 3896704 bytes prepared
Flushing data to flash:/web.upd...
```



```
Flush data done
A #upgrade web flash:/web.upd
Web package upgrade successfully.
A #
```

【检验方法】 在 PC 机中，重新进行 Web 认证登陆，验证是否显示最新的 Web 页面。

常见配置错误

- 通过浏览器访问，发现没有更新到新的 WEB 包，可能是本地浏览器有缓存；将浏览器的缓存清空，在重新访问一次。

5.5 监视与维护

查看运行情况

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

6 系统日志

6.1 概述

设备在运行过程中，会发生各种状态变化如链路状态 UP、DOWN 等，也会遇到一些事件如收到异常报文、处理异常等。锐捷产品系统日志提供一种机制，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、监视终端等）上或被记录在相关媒介（内存缓冲区、日志文件）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。

i 下文仅介绍系统日志的相关内容。

协议规范

- RFC 3164 : The BSD syslog Protocol
- RFC 5424 : The Syslog Protocol

6.2 典型应用

典型应用	场景描述
系统日志输出到控制台	通过控制台监控系统日志信息。
系统日志发送到日志服务器	通过服务器监控系统日志信息。

6.2.1 系统日志输出到控制台

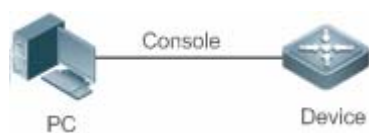
应用场景

可以将系统日志输出到控制台，方便管理员监控系统的运行状态，网络部署要求如下：

- 1、信息级别高于等于 informational（6 级）的日志信息允许输出到控制台。
- 2、只允许 ARP 模块和 IP 模块的日志信息输出到控制台。

组网环境如下所示：

图 6-1 系统日志输出到控制台组网图



功能部属

设备端的配置要点如下：

- 1、 设置允许输出到控制台的日志信息级别为 informational (6 级)。
- 2、 设置日志信息的过滤方向为：terminal (终端方向)。
- 3、 设置日志信息的过滤方式为：contains-only (“只包含” 过滤方式)。
- 4、 设置日志信息的过滤规则为：“单个匹配” 规则，模块名包含 ARP 或 IP。

6.2.2 系统日志发送到日志服务器

应用场景

可以将系统日志发送到日志服务器，方便管理员在服务器上统一监控设备的日志信息，假设网络中存在如下部署要求：

- 1、 系统日志信息发送到日志服务器上，日志服务器的 IP 地址为：10.1.1.1。
- 2、 信息级别高于等于 debugging (7 级) 的所有模块的日志信息允许发送到日志服务器上。
- 3、 系统日志信息发送到日志服务器的报文源接口为 Loopback 0。

组网环境如下所示：

图 6-2 系统日志发送到日志服务器组网图



功能部属

设备端的配置要点如下：

- 1、 设置日志服务器 IPv4 地址：10.1.1.1。
- 2、 设置允许发送到服务器的日志信息级别为 debugging (7 级)。
- 3、 设置发往服务器的日志信息的源接口为 Loopback 0。

6.3 功能详解

基本概念

系统日志的分类

系统日志可以分为如下两类：

- log 类，日志类信息
- debug 类，调试类信息

系统日志的级别

系统日志按严重性划分为 8 个等级，严重性由高到底依次为：emergencies、alerts、critical、errors、warnings、notifications、informational 和 debugging，并分别对应于 0~7 这 8 个数值，值越小代表级别越高。

根据日志级别输出信息时，将会输出日志级别高于或等于所设置级别的日志，比如，输出规则中指定允许级别为 informational 的信息输出，则级别为 emergencies ~ informational 的信息均会输出。

相关日志级别的说明如下表所示：

关键字	级别	描述
emergencies	0	系统不能正常运行的信息
alerts	1	需要立即采取措施改正的信息
critical	2	严重情况
errors	3	错误信息
warnings	4	警告信息
notifications	5	普通但是需要关注的信息
informational	6	说明性的信息
debugging	7	调试信息

系统日志的输出方向

系统日志的输出方向，可以分为 5 类，分别为：console、monitor、server、buffer、file，各个输出方向上的缺省输出级别和输出的日志分类各不相同，用户在使用过程中，可以对不同的输出方向配置不同的过滤规则。

相关日志输出方向的说明如下表所示：

输出方向的名称	缺省输出方向	缺省输出级别	描述
console	控制台	debugging (7 级)	可以输出 log、debug 信息
monitor	监视终端	debugging (7 级)	可以输出 log、debug 信息，便于远程维护
server	日志服务器	informational (6 级)	可以输出 log、debug 信息
buffer	日志缓冲区	debugging (7 级)	可以输出 log、debug 信息，是设备运行过程中的一块缓存，用于记录系统日志
file	日志文件	informational (6 级)	可以输出 log、debug 信息，定时将缓存中的日志信息写入到文件当中

RFC3164 日志格式

按照系统日志的输出方向不同，系统日志可能有不同格式。

- 当输出方向为非日志服务器（控制台、监视终端、日志缓冲区和日志文件）时，系统日志格式为：

```
seq no: *timestamp: sysname %module-level-mnemonic: content
```

对应的格式中文件说明如下：

序列号：*时间戳：系统名称 %模块名-级别-助记符：日志文本

例如，用户退出配置模式时，在控制台可以看到格式如下的日志：

```
001233: *May 22 09:44:36: Ruijie %SYS-5-CONFIG_I: Configured from console by console
```

- 当输出方向为日志服务器，系统日志格式为：

```
<priority>seq no: *timestamp: sysname %module-level-mnemonic: content
```

对应的格式中文件说明如下：

<优先级>序列号：*时间戳：系统名称 %模块名-级别-助记符：日志文本

例如，用户退出配置模式时，在日志服务器可以看到格式如下的日志：

```
<189>001233: *May 22 09:44:36: Ruijie %SYS-5-CONFIG_I: Configured from console by console
```

下面对每一个字段做详细说明：

6. priority (优先级)

本字段只有在向日志服务器输出日志时才有效。

优先级的计算按如下公式： $facility * 8 + level$ 。其中： $level$ 表示日志信息的级别； $facility$ 表示设备值，在设置日志信息的设备值时可以设置，默认值为 $local7 (23)$ ，参数取值范围如下表所示：

numerical code (标号)	facility keyword (设备值关键字)	facility description (设备值描述)
0	kern	kernel messages
1	user	user-level messages
2	mail	mail system
3	daemon	system daemons
4	auth1	security/authorization messages
5	syslog	messages generated internally by syslogd
6	lpr	line printer subsystem
7	news	network news subsystem
8	uucp	UUCP subsystem
9	clock1	clock daemon
10	auth2	security/authorization messages
11	ftp	FTP daemon
12	ntp	NTP subsystem
13	logaudit	log audit
14	logalert	log alert
15	clock2	clock daemon
16	local0	local use 0 (local0)
17	local1	local use 1 (local1)
18	local2	local use 2 (local2)
19	local3	local use 3 (local3)

20	local4	local use 4 (local4)
21	local5	local use 5 (local5)
22	local6	local use 6 (local6)
23	local7	local use 7 (local7)

7. seq no (序列号)

系统日志的序列号为 6 位整型数，并按系统日志产生的条目逐条递增，缺省情况下，该字段信息不会显示出来，可以通过命令开启或关闭该字段信息的输出。

8. timestamp (时间戳)

时间戳记录了系统日志产生的时间，方便用户查看和定位系统事件。锐捷设备的系统日志时间戳格式有两种，分别为 :datetime 格式和 uptime 格式。

- i** 如果当前设备不存在 RTC 时钟（一种用于记录系统绝对时间的硬件装置），缺省采用设备启动时间（uptime 格式）作为系统日志的时间戳。如果设备存在 RTC 时钟，则缺省采用设备绝对时间（datetime 格式）作为日志信息时间戳。

下面将对这两种时间戳格式进行详细说明：

- datetime 格式：

datetime 格式时间戳完整格式如下所示：

```
Mmm dd yyyy hh:mm:ss.msec
```

各个参数字段的说明如下表所示：

时间戳参数	参数名称	描述
Mmm	月份	Mmm 代表月份的英文缩写，1~12 月份依次为 :Jan、Feb、Mar、Apr、May、Jun、Jul、Aug、Sep、Oct、Nov、Dec
dd	天数	dd 代表当前月份对应的天数
yyyy	年份	yyyy 代表对应的年份，缺省情况下没有打开
hh	小时	hh 代表当前对应的小时数
mm	分钟	mm 代表当前对应的分钟数
ss	秒	ss 代表当前对应秒数
msec	毫秒	msec 代表当前对应的毫秒数

缺省情况下，系统输出的日志信息 datetime 格式时间戳不带年份和毫秒信息，用户可以通过命令开启或关闭系统日志的 datetime 格式时间戳是否携带年份和毫秒信息。

- uptime 格式：

uptime 格式时间戳完整格式如下所示：

```
dd:hh:mm:ss
```

整个时间戳字符串代表：系统自启机以来运行的天数：小时数：分钟数：秒数

9. sysname (系统名称)

该字段记录了生成该日志的设备名称，便于日志服务器标识该日志从哪个主机发送过来。缺省情况下，该字段信息不会显示出来，可以通过命令开启或关闭该字段信息的输出。

10. module (模块名)

该字段表示产生此日志的功能模块的名称，为一个 2~20 个字符的大写字符串（可包含大写字母、数字、下划线）。log 类的日志信息默认都要携带 module 字段，debug 类的日志信息有可能没有携带 module 字段。

11. level (日志级别)

系统日志的级别共分为 8 级，分别为 0~7 级。各模块生成的系统日志的级别在开发阶段已经确定，用户不能修改。

12. mnemonic (助记符)

该字段表示产生此日志的信息摘要，为一个 4~32 个字符的大写字符串（可包含大写字母、数字、下划线）。log 类的日志信息默认都要携带 mnemonic 字段，debug 类的日志信息有可能没有携带 mnemonic 字段。

13. content (日志文本)

该字段表示该系统日志的具体内容。

📄 RFC5424 日志格式

对于所有输出方向，系统的日志格式统一为：

```
<priority>version timestamp sysname MODULE LEVEL MNEMONIC [structured-data] description
```

对应的格式中文件说明如下：

```
<优先级>版本号 时间戳 系统名称 模块名 级别 助记符 结构化参数区 信息内容
```

例如，用户退出配置模式时，在控制台可以看到格式如下的日志：

```
<133>1 2013-07-24T12:19:33.130290Z ruijie SYS 5 CONFIG - Configured from console by console
```

下面对每一个字段做详细说明：

1. priority (优先级)

优先级的计算按如下公式： $facility * 8 + level$ 。其中： $level$ 表示日志信息的级别； $facility$ 表示设备值，在设置日志信息的设备值时可以设置，开启 RFC5424 日志开关时， $facility$ 默认值为 $local0 (16)$ 。

2. version (版本号)

RFC5424 中规定版本号固定为 1。

3. timestamp (时间戳)

时间戳记录了系统日志产生的时间，方便用户查看和定位系统事件。锐捷设备在开启 RFC5424 日志开关时，系统日志时间戳格式统一成如下形式：

```
YYYY-MM-DDTHH:MM:SS.SSECFRACZ
```

各个参数字段的说明如下表所示：

时间戳参数	参数名称	描述
YYYY	年份	YYYY 代表对应的年份
MM	月份	MM 代表当前年份对应的月份
DD	天数	DD 代表当前月份对应的天数
T	分隔符	日期必须以 T 结尾

HH	小时	HH 代表当前对应的小时数
MM	分钟	MM 代表当前对应的分钟数
SS	秒	SS 代表当前对应秒数
SECFRAC	毫秒	SECFRAC 代表当前对应的毫秒数 (1~6 位)
Z	结束符	时间必须以 Z 结尾

4. sysname (系统名称)

该字段记录了生成该日志的设备名称，便于日志服务器标识该日志从哪个主机发送过来。

5. MODULE (模块名)

该字段表示产生此日志的功能模块的名称，为一个 2~20 个字符的大写字母串 (可包含大写字母、数字、下划线)。log 类的日志信息默认都要携带 module 字段，debug 类的日志信息有可能没有携带 module 字段。

6. LEVEL (日志级别)

系统日志的级别共分为 8 级，分别为 0~7 级。各模块生成的系统日志的级别在开发阶段已经确定，用户不能修改。

7. MNEMONIC (助记符)

该字段表示产生此日志的信息摘要，为一个 4~32 个字符的大写字母串 (可包含大写字母、数字、下划线)。log 类的日志信息默认都要携带 mnemonic 字段，debug 类的日志信息有可能没有携带 mnemonic 字段。

8. structured-data (结构化参数区)

该字段是 RFC5424 新引入的字段，是一种利于机器解析的方式描述日志的参数信息。每条日志可以包含 0 个或多个参数信息，若没有参数信息，必须使用字符 '-' 占位，每一个参数信息的格式为：

```
[SD_ID@enterpriseID PARAM-NAME=PARAM-VALUE]
```

各个参数字段的说明如下表所示：

结构化参数区	参数名称	描述
SD_ID	参数信息名字	参数信息名字通过大写显示，且同一条日志当中不能存在相同的参数信息名字
@	分隔符	只有自定义的参数信息才需要添加 @enterpriseID，若为 RFC5424 标准所定义的参数信息，则不需要添加 @enterpriseID
enterpriseID	厂商 ID	厂商 ID 由 IANA 维护，锐捷设备的厂商 ID 号固定为 4881，可以通过 IANA 网站进行查询： http://www.iana.org/assignments/enterprise-numbers
PARAM-NAME	参数名	参数名字段全部通过大写显示，且同一条日志当中结构化参数区不能存在相同的参数名
PARAM-VALUE	参数值	参数值字段需要添加双引号，其中：IP 地址、MAC 地址类型的值格式化为大写显示，其它类型的值依据实际情况而定

9. description (日志文本)

该字段表示该系统日志的具体内容。

功能特性

功能特性	作用
系统日志功能开关	用于设置系统日志功能的打开与否。
系统日志格式设置	用于设置系统日志的显示格式。
系统日志信息设置	用于设置系统日志发往各个方向的参数信息。
系统日志过滤功能设置	用于设置系统日志过滤功能的参数信息。
系统日志上送功能设置	用于设置系统日志上送功能的参数信息
系统日志监控功能设置	用于设置系统日志监控功能的参数信息。

6.3.1 系统日志功能开关

用于设置系统日志功能的打开与否，主要包括：日志开关、日志信息统计功能开关。

相关配置

✎ 打开日志开关

缺省情况下，日志开关是打开的。

使用 **logging on** 命令在全局配置模式下打开日志开关，打开日志开关后，系统产生的日志信息才能往各个输出方向输出，并用于监视系统的运行状态。

✎ 启用日志信息统计功能开关

缺省情况下，日志信息统计功能是关闭的。

使用 **logging count** 命令在全局配置模式下开启日志信息统计功能，打开日志信息统计功能后，系统将记录各模块产生的日志信息的次数，以及最后产生此日志信息的时间等。

6.3.2 系统日志格式设置

用于设置系统日志的显示格式，主要包括：RFC5424 日志格式、日志时间戳格式、日志系统名称、日志序列号等。

相关配置

✎ 启用 RFC5424 日志格式开关

缺省情况下，RFC5424 日志格式是关闭的。

切换成 RFC5424 日志格式后，旧日志格式中的命令 **service sequence-numbers**、**service sysname**、**service timestamps**、**service private-syslog**、**service standard-syslog** 将会失效并隐藏掉。

在新旧日志格式切换前后，**show logging** 和 **show logging config** 命令的显示内容也会有所变化。

✎ 启用日志信息时间戳开关

缺省情况下，系统日志使用的格式为 `datetime` 格式，且 `datetime` 时间戳格式没有携带年份和毫秒信息。

使用 `service timestamps` 命令在全局配置模式下打开系统日志的 `datetime` 格式的时间戳的年份和毫秒信息，或者将系统日志的格式修订成 `uptime` 格式。

▾ 启用日志信息系统名称开关

缺省情况下，系统输出的日志信息没有携带 `sysname`（系统名称）。

使用 `service sysname` 命令在全局配置模式下开启系统日志的 `sysname`（系统名称）。

▾ 启用日志信息序列号开关

缺省情况下，系统输出的日志信息没有携带序列号。

使用 `service sequence-numbers` 命令在全局配置模式下开启日志信息的序列号。

▾ 启用标准日志格式显示开关

缺省情况下，设备上面的日志信息显示格式如下：

```
*timestamp: %module-level-mnemonic: content
```

依次为：

```
*时间戳: %模块名-级别-助记符: 日志文本。
```

使用 `service standard-syslog` 命令在全局配置模式下开启标准日志格式显示开关，开启标准日志格式显示开关后，设备输出的日志信息显示格式如下：

```
timestamp %module-level-mnemonic: content
```

与缺省情况相比，标准日志格式的时间戳中前面少了一个 `' * '`、后面少了一个 `':'`。

▾ 启用私有日志格式显示开关

缺省情况下，设备上面的日志信息显示格式如下：

```
*timestamp: %module-level-mnemonic: content
```

依次是：

```
*时间戳: %模块名-级别-助记符: 日志文本。
```

使用 `service private-syslog` 命令在全局配置模式下开启私有日志格式显示开关，开启私有日志格式显示开关后，设备输出的日志信息显示格式如下：

```
timestamp module-level-mnemonic: content
```

与缺省情况相比，私有日志格式的时间戳中前面少了一个 `' * '`、后面少了一个 `':'`，模块名前面少了一个 `' % '`。

6.3.3 系统日志信息设置

用于设置日志信息输出各个方向的参数信息，主要包括：日志信息输出控制台参数信息、日志信息输出监视终端参数信息、日志信息写入内存缓冲区参数信息、日志信息发往日志服务器参数信息、日志信息写入日志文件参数信息等。

相关配置

设置用户输入与日志信息输出同步

缺省情况下，用户输入与日志信息输出功能是关闭的。

使用 **logging synchronous** 命令在线路配置模式下设置用户输入与日志信息输出同步功能，防止用户正在输入字符时被打断。

设置日志信息速率控制功能

缺省情况下，日志信息不进行速率限制。

使用 **logging rate-limit { number | all number } console { number | all number } [except [severity]]**命令在全局配置模式下设置日志信息速率限制功能，限制每秒内允许输出的日志信息。

设置日志信息输出控制台的级别

缺省情况下，日志信息输出到控制台的级别为 debugging（7级）。

使用命令 **logging console [level]**命令在全局配置模式下设置允许在控制台上显示的日志信息级别。

设备允许日志信息输出到监视终端

缺省情况下，日志信息不允许输出到监视终端。

使用命令 **terminal monitor** 命令在特权模式下设置允许将日志信息输出到监视终端。

设置日志信息输出到监视终端的级别

缺省情况下，日志信息输出到监视终端的级别为 debugging（7级）。

使用命令 **logging monitor [level]**命令在全局配置模式下设置允许在监视终端上输出的日志信息级别。

设置日志信息写入到内存缓冲区的参数

缺省情况下，日志信息默认会写入到内存缓冲区，且默认级别为 debugging（7级）。

使用 **logging buffered [buffer-size] [level]**命令在全局配置模式下设置日志写入的内存缓冲区的参数（包括缓冲区大小、日志信息等级）。

设置日志信息发送往日志服务器

缺省情况下，日志信息不会发往日志服务器。

使用 **logging server { ip-address } [udp-port port]**命令在全局配置模式下设置日志发往指定的日志服务器。

设置日志信息发往日志服务器的级别

缺省情况下，日志信息发往日志服务器的级别为 informational（6级）。

使用命令 **logging trap [level]**命令在全局配置模式下设置允许发往日志服务器的日志信息级别。

设置日志信息发往日志服务器的设备值

在没有开启 RFC5424 日志格式的情况下，日志信息发往服务器的系统设备值默认为 local7 (23)；在开启 RFC5424 日志格式的情况下，日志信息发往服务器的系统设备值默认为 local0 (16)。

使用 **logging facility** *facility-type* 命令在全局配置模式下设置发往日志服务器的日志信息的系统设备值。

✎ 设置发往日志服务器的日志报文源地址

缺省情况下，发往 Syslog Server 的日志报文源地址为发送报文接口的 IP 地址。

使用 **logging source** [**interface**] *interface-type interface-number* 命令设置日志报文的源接口。倘若设备上未配置该源接口、或该源接口上未配置 IP 地址，则日志报文源地址也仍为发送报文接口的 IP 地址。

使用 **logging source** { **ip** *ip-address* } 命令设置日志报文的源 IP 地址。倘若设备上未配置该 IP 地址，则日志报文源 IP 地址仍为发送报文接口的 IP 地址。

✎ 设置日志信息写入到日志文件参数

缺省情况下，日志信息不会写入日志文件中，开启日志信息写文件功能后，默认的级别为 informational (6 级)。

使用 **logging file flash:filename** [*max-file-size*] [*level*] 命令在全局配置模式下设置日志信息写入的日志文件参数 (包括文件存储的设备类型、文件名称、文件大小、日志信息等级)。

✎ 设置日志文件的个数

缺省情况下，日志文件的个数为 16。

使用 **logging file numbers** *numbers* 命令在全局配置模式下设置日志文件的个数。

✎ 设置日志信息写入到日志文件的时间间隔

缺省情况下，日志信息写入日志文件的时间间隔为 3600 秒 (1 小时)。

使用 **logging flash interval** *seconds* 命令在全局配置模式下设置日志信息写入日志文件的时间间隔。

✎ 设置日志信息写入到日志文件的保存时间

缺省情况下，系统对日志文件的保存时间是没有限制的。

使用 **logging life-time level** *level days* 命令在全局配置模式下设置日志信息的保存时间，方便管理员针对不同级别的日志信息指定不同的保存天数。

✎ 设置将缓冲区当中的日志信息立即写入到日志文件中

缺省情况下，设备产生的日志信息会先缓存在系统日志缓冲区中，只有当缓冲区满或定时器到期后，才会将缓冲区中的日志信息写入到日志文件中。

使用 **logging flash flush** 命令在全局配置模式下将系统缓冲区中的日志信息立即写入到日志文件中，方便用户进行日志信息收集。

6.3.4 系统日志过滤功能设置

缺省情况下，系统打出来的日志信息都可以输出到各个方向，当某些情况下，用户可能不关心某些日志信息或者只关心某些日志信息，则可以使用日志过滤功能，对该日志信息进行过滤。

工作原理

▾ 过滤方向

日志过滤方向主要分为以下四类：

- **buffer**：代表过滤掉去向日志缓冲区的日志信息（即 **show logging** 显示出来的日志信息）；
- **file**：代表过滤掉去向日志文件的日志信息；
- **server**：代表过滤掉去向日志服务器的日志信息；
- **terminal**：代表过滤掉去向控制台和监视终端（包括 Telnet/SSH 等）的日志信息；

以上四类过滤方向为或（|）关系，即可以联合使用（对往多个方向的日志信息进行过滤），也可以单独使用（只对往某一方向的日志信息进行过滤）。

▾ 过滤方式

日志过滤方式主要分为以下两种：

- **contains-only**：代表“只包含”，意思是：只输出包含在过滤规则里面的关键字的日志信息，其它没有包含在过滤规则里面的关键字的日志信息不会输出。某些情况下，用户可能只关心某些日志信息是否产生，则可以在设备上面应用“只包含”这一日志过滤类型，让包含了此规则的日志信息才输出到终端界面，方便用于观察某些事件是否有发生。
- **filter-only**：代表“只过滤”，意思是：将过滤掉包含在过滤规则里面的关键字的日志信息，不会输出这些过滤掉的日志信息。某些情况下，当遇到某一个模块打出来的日志信息太多，可能会引起终端界面出现刷屏，且用户又不关心此类日志信息的时候，可以在设备上面应用“只过滤”这一日志过滤类型，并配置对应的过滤规则，将刷屏的日志信息过滤掉。

以上两种过滤方式为互斥关系，即同一时刻只能配置一种过滤方式。

▾ 过滤规则

日志过滤规则主要分为以下两种：

- **exact-match**：代表精确匹配，若选择精确匹配，则后面的三个过滤选项（日志模块名、日志等级、日志助记符）都需要选上。某些情况下，用户可能只想过滤掉某一特定的日志信息，则可以使用“精确匹配”规则。
- **single-match**：代表单个匹配，若选择单个匹配，则后面的三个过滤选项（日志模块名、日志等级、日志助记符）只需要选择其中的一个。某些情况下，用户可能想过滤掉某一类型的日志信息，则可以使用“单个匹配”规则。

当用户配置的日志信息过滤规则中，若“单个匹配”规则和“精确匹配”规则中同时配置了一样的模块名、助记符或信息等级，则单个匹配规避的优先级高于精确匹配。

相关配置

设置日志信息的过滤方向

缺省情况下，日志信息的过滤方向为 all，即过滤去往所有方向的日志信息。

使用 `logging filter direction { all | buffer | file | server | terminal }` 命令在全局配置模式下设置日志信息的过滤方向，指定过滤去往哪几个方向的日志信息。

设置日志信息的过滤方式

缺省情况下，日志信息的过滤方式为“只过滤”。

使用 `logging filter type { contains-only | filter-only }` 命令在全局配置模式下设置日志信息的过滤方式。

设置日志信息的过滤规则

缺省情况下，设备上面没有配置日志信息的过滤规则，不对日志信息进行过滤。

使用 `logging filter rule exact-match module module-name mnemonic mnemonic-name level level` 命令在全局配置模式下设置日志信息的“精确匹配”过滤规则。

使用 `logging filter rule single-match { level level | mnemonic mnemonic-name | module module-name }` 命令在全局配置模式下设置日志信息的“单个匹配”过滤规则。

6.3.5 系统日志监控功能设置

打开日志监控功能后，系统将对外界连接到设备的行为进行监控，并记录对应的 LOG 信息。

工作原理

在设备上面开启记录用户登录或退出 LOG 信息后，系统将对外界连接到设备的行为进行记录，记录的信息包括：登录的用户名、登录的源地址等。

在设备上面开启记录用户操作的 LOG 信息，系统将对修改设备配置的行为进行记录，记录的信息包括：操作的用户名、操作的源地址、操作的内容。

相关配置

设置用户登录或退出 LOG 信息

缺省情况下，用户登录或退出设备的时候，设备是不会记录相关的 Log 信息。

使用 `logging userinfo` 命令在全局配置模式下设置用户登录/退出的 Log 信息。设置此功能后，当外界通过 Telnet、SSH、HTTP 等方式连接到设备时，设备将打出对应的 Log 信息，方便管理员监控设备的连接情况。




设置用户操作的 LOG 信息

缺省情况下，用户修订设备配置的时候，设备是不会记录相关的操作 Log 信息。

使用 **logging userinfo command-log** 命令在全局配置模式下设置用户操作的 Log 信息。设置此功能后,当有用户修改设备配置时,系统就会打出相应的 Log 信息提醒设备管理员。

6.4 配置详解

配置项	配置建议&相关命令	
配置系统日志的显示格式	 可选配置,用于设置系统日志的显示格式	
	service timestamps [<i>message-type</i> [<i>uptime</i> <i>datetime</i> [<i>msec</i>] [<i>year</i>]]]	设置系统日志的时间戳格式
	service sysname	设置系统日志格式中添加系统名称
	service sequence-numbers	设置系统日志格式中添加系列号
	service standard-syslog	设备系统日志格式为标准日志格式
	service private-syslog	设备系统日志格式为私有日志格式
	service log-format rfc5424	设备系统日志格式为 RFC5424 日志格式
配置系统日志输出到控制台	 可选配置,用于设置系统日志输出到控制台的参数信息	
	logging on	打开日志开关
	logging count	打开日志信息统计功能
	logging console [<i>level</i>]	设置日志信息允许输出到控制台的级别
	logging rate-limit { <i>number</i> <i>all number</i> <i>console</i> { <i>number</i> <i>all number</i> } } [except [<i>severity</i>]]	设置日志信息速率限制功能
配置系统日志输出到监视终端	 可选配置,用于设置系统日志输出到监视终端的参数信息	
	terminal monitor	允许在当前监视终端上显示日志信息
	logging monitor [<i>level</i>]	设置日志信息允许输出到监视终端的级别
配置系统日志写入到内存缓冲区	 可选择配置,用于设置系统日志写入内存缓冲区的参数信息	
	logging buffered [<i>buffer-size</i>] [<i>level</i>]	设置日志写入的内存缓冲区的参数(包括缓冲区大小、日志信息等级)
配置系统日志发送往日志服务器	 可选配置,用于设置系统日志发送到日志服务器的参数信息	
	logging server { <i>ip-address</i> } [udp-port <i>port</i>]	设置日志发往指定的日志服务器
	logging trap [<i>level</i>]	设置允许发往日志服务器的日志级别
	logging facility <i>facility-type</i>	设置发往服务器的日志信息的系统设备值
	logging source [<i>interface</i>] <i>interface-type</i> <i>interface-number</i>	设置发往服务器的日志信息的源接口
logging source { <i>ip ip-address</i> }	设置发往服务器的日志信息的源地址	
配置系统日志写入到日志文	 可选配置,用于设置系统日志写入文件的参数信息	

件	logging file flash:filename [<i>max-file-size</i>] [<i>level</i>]	设置日志信息写入的文件参数（包括文件存储的类型、文件名称、文件大小、日志信息等级）
	logging file numbers numbers	设置日志信息写入文件的个数，缺省值为 16
	logging flash interval seconds	设置日志信息写入文件的频率，缺省值为 3600
	logging life-time level level days	设置日志信息写入文件的保存时间
配置系统日志过滤功能	 可选配置，用于设置系统日志的过滤功能参数信息	
	logging filter direction { all buffer file server terminal }	设置日志信息的过滤方向
	logging filter type { contains-only filter-only }	设置日志信息的过滤方式
	logging filter rule exact-match module module-name mnemonic mnemonic-name level level	设置日志信息的“精确匹配”过滤规则
	logging filter rule single-match { level level mnemonic mnemonic-name module module-name }	设置日志信息的“单个匹配”过滤规则
配置系统日志监控功能	 可选配置，用于设置系统日志的监控功能参数信息	
	logging userinfo	开启记录用户登录/退出的日志信息
	logging userinfo command-log	开启记录用户操作的日志信息
配置用户输入与日志信息同步输出功能	 可选配置，用于设置用户输入与日志信息同步输出功能	
	logging synchronous	设置用户输入与日志信息输出同步功能

6.4.1 配置系统日志的显示格式

配置效果

- 调整系统日志的显示格式。

注意事项

📄 RFC3164 日志格式

- 如果当前设备不存在 RTC 时钟（一种用于记录系统绝对时间的硬件装置），系统缺省采用设备启动时间（**uptime** 格式）作为日志信息时间戳，此时配置设备时间无效，如果设备存在 RTC 时钟，则缺省采用设备时间（**datetime** 格式）作为日志信息时间戳。
- 日志序列号是一个长整型数值，每产生一条日志，序列号就递增，但是由于日志序列号只显示 6 位整数，故当序列号从 1 开始每增加到 1000000 或序列号到达 2^{32} 时候就会发生一次翻转，即序列号又从 000000 开始显示。

✎ RFC5424 日志格式

- 开启 RFC5424 日志格式后，日志时间戳统一成一种格式，不再区分 **uptime** 格式和 **datetime** 格式。
- RFC5424 日志格式中时间戳格式包括有时区和没有时区两种，当前只支持没有时区的显示格式。

配置方法

✎ 设置系统日志的时间戳格式

- 可选配置，缺省情况下系统日志的时间戳采用 **datetime** 格式。
- 若无特殊要求，在需要设置系统日志时间戳格式的设备上面配置。

✎ 设置系统日志格式中添加系统名称

- 可选配置，缺省情况下系统日志的格式中没有添加系统名称。
- 若无特殊要求，在需要为日志格式中添加系统名称的设备上面配置。

✎ 设置系统日志格式中添加序列号

- 可选配置，缺省情况下系统日志的格式中没有添加序列号。
- 若无特殊要求，在需要为日志格式添加序列号的设备上面配置。

✎ 设置系统日志格式为标准日志格式

- 可选配置，缺省情况下系统日志的格式中为默认格式。
- 若无特殊要求，在需要使用标准日志格式的设备上面配置。

✎ 设置系统日志格式为私有日志格式

- 可选配置，缺省情况下系统日志的格式中为默认格式。
- 若无特殊要求，在需要使用私有日志格式的设备上面配置。

✎ 设置系统日志格式为 RFC5424 日志格式

- 可选配置，缺省情况下系统关闭 RFC5424 日志格式。
- 若无特殊要求，在需要使用 RFC5424 日志格式的设备上面配置。

检验方法

- 通过触发系统产生一条日志信息，用于查看设置后的系统日志的显示格式。

相关命令

✎ 设置系统日志的时间戳格式

【命令格式】 **service timestamps** [*message-type* [**uptime** | **datetime** [**msec**] [**year**]]]

【参数说明】 *message-type* : 日志类型, 有两种 log 和 debug

uptime : 设备启动时间, 格式: *天*小时*分*秒, 例: 07:00:10:41

datetime : 当前设备日期, 格式: 月 日期 时:分:秒, 例: Jul 27 16:53:07

msec : 当前设备日期支持毫秒显示

year : 当前设备日期支持年份显示

【命令模式】 全局配置模式

【使用指导】 系统日志的时间戳格式有两种: 设备启动时间(**uptime**)格式或者设备日期(**datetime**)格式, 用户可以根据需要选择不同类型的时间戳格式。

📌 设置系统日志格式中添加系统名称

【命令格式】 **service sysname**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 可以在日志信息中系统名称, 加上系统名称以后, 系统日志发送到服务器后, 在服务器上, 可以清楚地知道日志信息来自哪个设备。

📌 设置系统日志格式中添加序列号

【命令格式】 **service sequence-numbers**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 可以在日志信息中加上序列号, 序列号从 1 开始。加上序号以后, 就可以非常清楚地知道日志信息有没有丢失, 以及日志产生的先后顺序。

📌 设置系统日志格式为标准日志格式

【命令格式】 **service standard-syslog**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 默认情况下, 设备上面的日志信息显示格式如下 (默认格式):

```
*timestamp: %module-level-mnemonic: content
```

依次是:

```
*时间戳: %模块名-级别-助记符: 日志文本。
```

若打开标准日志格式显示功能, 设备上面的日志信息显示格式如下:

```
timestamp %module-level-mnemonic: content
```

与缺省情况相比, 标准日志格式的时间戳中前面少了一个 '*'、后面少了一个 ':'

📌 设置系统日志格式为私有日志格式

【命令格式】 **service private-syslog**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 默认情况下, 设备上面的日志信息显示格式如下 (默认格式):

```
*timestamp: %module-level-mnemonic: content
```

依次是：

```
*时间戳: %模块名-级别-助记符: 日志文本。
```

若打开标准日志格式显示功能，设备上面的日志信息显示格式如下：

```
timestamp module-level-mnemonic: content
```

与缺省情况相比，私有日志格式的时间戳中前面少了一个'*'、后面少了一个':'，模块名前面少了一个'%'

设置系统日志格式为 RFC5424 日志格式

【命令格式】 **service log-format rfc5424**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】

切换到 RFC5424 日志格式后，旧日志格式中的命令 **service sequence-numbers**、**service sysname**、**service timestamps**、**service private-syslog**、**service standard-syslog** 将会失效并隐藏掉。

在新旧日志格式切换之后，**show logging** 和 **show logging config** 的命令的显示内容将会有所变化。

配置举例

配置 RFC3164 日志显示格式

【网络环境】 假设网络环境中，有以下日志时间戳格式设置要求：

- 1、切换日志格式为 RFC3164 格式；
- 2、日志时间戳格式调整为 **datetime** 格式，并且开启毫秒信息和年份信息的显示；
- 3、日志时间戳格式中要求添加系统名称；
- 4、日志时间戳格式中要求添加系列号。

【配置方法】 ● 在设备上面配置系统日志的显示格式

```
Ruijie# configure terminal
Ruijie(config)# no service log-format rfc5424
Ruijie(config)# service timestamps log datetime year msec
Ruijie(config)# service timestamps debug datetime year msec
Ruijie(config)# service sysname
Ruijie(config)# service sequence-numbers
```

【检验方法】 用户设置了日志时间戳格式后，在系统新产生日志信息的时候，将会依据所设置的时间戳格式进行日志信息的构造和输出。

- 通过 **show logging config** 命令可以查看用户配置的相关参数信息。
- 通过进入/退出全局配置模式触发产生一条新的日志信息，可以观察新产生的日志信息的时间戳格式。

```
Ruijie(config)#exit
001302: *Jun 14 2013 19:01:40.293: Ruijie %SYS-5-CONFIG_I: Configured from console by admin on console
Ruijie#show logging config
```

```
Syslog logging: enabled
  Console logging: level informational, 1306 messages logged
  Monitor logging: level informational, 0 messages logged
  Buffer logging: level informational, 1306 messages logged
  File logging: level informational, 121 messages logged
  File name:syslog_test.txt, size 128 Kbytes, have written 5 files
  Standard format:false
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
  Sequence-number log messages: enable
  Sysname log messages: enable
  Count log messages: enable
  Trap logging: level informational, 121 message lines logged,0 fail
```

配置 RFC5424 日志显示格式

【网络环境】 假设网络环境中，需要切换 RFC5424 日志格式要求：

1、切换日志格式为 RFC5424 格式。

【配置方法】 ● 在设备上面配置系统日志的显示格式

```
Ruijie# configure terminal
Ruijie(config)# service log-format rfc5424
```

【检验方法】 用户把日志格式切换为 RFC5424 格式，设备日志就会按照 RFC5424 格式输出。

- 通过 **show logging config** 命令可以查看用户配置的相关参数信息。
- 通过进入/退出全局配置模式触发产生一条新的日志信息，可以观察新产生的日志信息的格式。

```
Ruijie(config)#exit
<133>1 2013-07-24T12:19:33.130290Z ruijie SYS 5 CONFIG - Configured from console by console
Ruijie#show logging config
Syslog logging: enabled
  Console logging: level debugging, 4740 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 4745 messages logged
  Statistic log messages: disable
  Statistic log messages to terminal: disable
  Delay-send file name:syslog_ftp_server, Current write index:3, Current send index:3, Cycle:10
seconds
  Count log messages: enable
  Trap logging: level informational, 2641 message lines logged,4155 fail
```

```
logging to 192.168.23.89
logging to 2000::1
Delay-send logging: 2641 message lines logged
logging to 192.168.23.89 by tftp
```

6.4.2 配置系统日志输出到控制台

配置效果

- 可以将系统产生的日志信息输出到控制台，方便管理员监控系统的运行状态。

注意事项

- 如果系统产生的日志信息太多，则可以通过限制日志信息的速率来减少输出到控制台日志信息。

配置方法

▾ 打开日志开关

- 可选配置，缺省情况下系统日志开关已经打开。

▾ 打开日志信息统计功能

- 可选配置，缺省情况下系统日志信息统计功能是关闭的。
- 若无特殊要求，在需要打开日志信息统计功能的设备上配置。

▾ 设置日志信息允许输出控制台的级别

- 可选配置，缺省级别为 debugging（7级）。
- 若无特殊要求，在需要设置日志信息允许输出控制台级别的设备上配置。

▾ 设置日志信息速率限制功能

- 可选配置，缺省情况下不进行速率限制。
- 若无特殊要求，在需要设置日志信息速率限制功能的设备上配置。

检验方法

- 通过 `show logging config` 命令可以查看设置的允许输出控制台的日志级别参数。

相关命令

打开日志开关

- 【命令格式】 **logging on**
- 【参数说明】 -
- 【命令模式】 全局配置模式
- 【使用指导】 缺省情况下，系统日志开关是打开的，一般情况下，不要关闭日志开关，如果觉得打印的信息太多，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。

打开日志信息统计功能

- 【命令格式】 **logging count**
- 【参数说明】 -
- 【命令模式】 全局配置模式
- 【使用指导】 缺省情况下，系统日志信息统计功能是关闭的。启用了日志报文统计功能后，从命令打开时将系统中输出的日志信息进行分类统计，主要记录日志信息的产生次数，以及最后产生的时间等。

设置日志信息允许输出到控制台的级别

- 【命令格式】 **logging console [level]**
- 【参数说明】 *level* : 日志信息的级别
- 【命令模式】 全局配置模式
- 【使用指导】 控制台默认允许显示的日志信息级别为 debugging (7 级)。可以通过特权命令 **show logging config** 来查看允许在控制台上显示的日志信息级别。

设置日志信息速率限制功能

- 【命令格式】 **logging rate-limit { number | all number | console { number | all number } } [except [severity]]**
- 【参数说明】
 - number* : 每秒钟内允许处理的日志信息，范围为 1~10000。
 - all** : 设置对所有的日志信息进行速率控制，包括 0~7 级所有日志信息。
 - console** : 设置每秒钟内允许在控制台上显示的日志信息数。
 - except severity** : 小于等于此严重性级别的日志信息，不进行速率控制；默认级别为 error(3)，对小于等于 error 级别的日志信息不进行速率控制。
- 【命令模式】 全局配置模式
- 【使用指导】 默认情况下，不对日志信息进行速率限制。

配置举例

配置系统日志输出到控制台

- 【网络环境】 假设网络环境中，有以下日志输出控制台格式要求：
 - 1、打开日志信息统计功能；
 - 2、设置允许输出到控制台的日志信息级别为 informational (6 级)；
 - 3、设置日志信息输出到控制台的速率为每秒 50 条；
- 【配置方法】
 - 在设备上面配置系统日志输出到控制台

```
Ruijie# configure terminal
Ruijie(config)# logging count
Ruijie(config)# logging console informational
Ruijie(config)# logging rate-limit console 50
```

- 【检验方法】
- 通过 **show logging config** 命令可以查看用户配置的相关参数信息。

```
Ruijie(config)#show logging config
Syslog logging: enabled
  Console logging: level informational, 1303 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 1303 messages logged
  File logging: level informational, 118 messages logged
  File name:syslog_test.txt, size 128 Kbytes, have written 5 files
  Standard format:false
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
  Sequence-number log messages: enable
  Sysname log messages: enable
  Count log messages: enable
  Trap logging: level informational, 118 message lines logged,0 fail
```

6.4.3 配置系统日志输出到监视终端

配置效果

- 可以将系统产生的日志信息输出到远程监视终端，方便管理员监控系统的运行状态。

注意事项

- 如果系统产生的日志信息太多，则可以通过限制日志信息的速率来减少输出到监视终端的日志信息。
- 默认情况下，用户远程连接到设备后，当前监视终端上不允许输出日志信息。需要手动输入 **terminal monitor** 命令开启当前终端的日志信息输出功能。

配置方法

▾ 允许在当前监视终端上显示日志信息

- 必选配置，缺省情况下不允许在监视终端上显示日志信息。
- 若无特殊要求，应在每个连接到设备的监视终端配置。

设置日志信息允许输出到监视终端的级别

- 可选配置，缺省级别为 debugging（7 级）。
- 若无特殊要求，在需要设置日志信息允许输出到监视终端级别的设备上配置。

检验方法

- 通过 **show logging config** 命令可以查看设置的允许输出到监视终端的日志级别参数。

相关命令

允许在当前监视终端上显示日志信息

【命令格式】 **terminal monitor**

【参数说明】 -

【命令模式】 特权模式

【使用指导】 默认情况下，用户远程连接到设备后，当前监视终端上不允许输出日志信息。需要手动输入 **terminal monitor** 命令开启当前终端的日志信息输出功能。

设置日志信息允许输出到监视终端的级别

【命令格式】 **logging monitor [level]**

【参数说明】 *level*：日志信息的级别

【命令模式】 全局配置模式

【使用指导】 监视终端默认允许显示的日志信息级别为 debugging（7 级）。
可以通过特权命令 **show logging config** 来查看允许在监视终端上显示的日志信息级别。

配置举例

配置系统日志输出到监视终端

【网络环境】 假设网络环境中，有以下日志信息输出到监视终端设置要求：
1、设置允许在监视终端上显示日志信息；
2、设置允许输出到控制台的日志信息级别为 informational（6 级）。

【配置方法】 ● 在设备上配置系统日志输出到监视终端

```
Ruijie# configure terminal
Ruijie(config)# logging monitor informational
Ruijie(config)# line vty 0 4
Ruijie(config-line)# monitor
```

【检验方法】 ● 通过 **show logging config** 命令可以查看用户配置的相关参数信息。

```
Ruijie#show logging config
```


【网络环境】 假设网络环境中，有以下日志信息输出到监视终端设置要求：

- 1、设置允许在监视终端上显示日志信息；
- 2、设置允许输出到控制台的日志信息级别为 informational（6级）。

【配置方法】 ● 在设备上面配置系统日志输出到监视终端

```
Ruijie# configure terminal
Ruijie(config)# logging monitor informational
Ruijie(config)# line vty 0 4
Ruijie(config-line)# monitor
```

【检验方法】 ● 通过 **show logging config** 命令可以查看用户配置的相关参数信息。

```
Syslog logging: enabled
  Console logging: level informational, 1304 messages logged
  Monitor logging: level informational, 0 messages logged
  Buffer logging: level debugging, 1304 messages logged
  File logging: level informational, 119 messages logged
  File name:syslog_test.txt, size 128 Kbytes, have written 5 files
  Standard format:false
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
  Sequence-number log messages: enable
  Sysname log messages: enable
  Count log messages: enable
  Trap logging: level informational, 119 message lines logged,0 fail
```

常见错误

- 若要取消当前终端的日志信息输出功能，需要使用的命令是：**terminal no monitor**，而不是 **no terminal monitor**。

6.4.4 配置系统日志写入到内存缓冲区

配置效果

- 可以将系统产生的日志信息写入到内存缓冲区，方便管理员通过 **show logging** 命令查看近期系统产生的日志信息。

注意事项

- 系统日志写入内存缓冲区后，当缓冲区满时，将循环覆盖重写。

配置方法

设置日志写入的内存缓冲区的参数

- 可选配置，缺省情况下系统会将日志信息写入到内存缓冲区，且默认级别为 debugging（7级）。
- 若无特殊要求，在需要设置日志写入内存缓冲区级别的设备上面配置。

检验方法

- 通过 **show logging config** 命令可以查看设置的允许写入内存缓冲区的日志级别参数。
- 通过 **show logging** 命令可以查看系统写入内存缓冲区的日志信息。

相关命令

设置日志写入的内存缓冲区的参数

【命令格式】 **logging buffered** [*buffer-size*] [*level*]

【参数说明】 *buffer-size* : 内存缓冲的大小

level : 允许写入到内存缓冲区的信息级别

【命令模式】 全局配置模式

【使用指导】 默认写入内存缓冲区的日志信息级别为 debugging（7级）。

可以通过特权命令 **show logging** 来查看允许写入内存缓冲区的日志信息级别和缓冲的大小等参数信息。

配置举例

配置系统日志写入到内存缓冲区的参数

【网络环境】 假设网络环境中，有以下日志信息写入到内存缓冲区设置要求：

- 1、设置日志内存缓冲区的大小为 128K（131072 字节）；
- 2、设置允许写入到内存缓冲区的日志信息级别为 informational（6级）。

【配置方法】 ● 在设备上面配置系统日志写入到内存缓冲区参数信息

```
Ruijie# configure terminal
Ruijie(config)# logging buffered 131072 informational
```

【检验方法】 ● 通过 **show logging** 命令可以查看用户配置的相关参数信息及系统最近产生的日志信息。

```
Ruijie#show logging
Syslog logging: enabled
  Console logging: level informational, 1306 messages logged
  Monitor logging: level informational, 0 messages logged
  Buffer logging: level informational, 1306 messages logged
  File logging: level informational, 121 messages logged
  File name:syslog_test.txt, size 128 Kbytes, have written 5 files
  Standard format:false
```

【网络环境】 假设网络环境中，有以下日志信息写入到内存缓冲区设置要求：

- 1、设置日志内存缓冲区的大小为 128K (131072 字节)；
- 2、设置允许写入到内存缓冲区的日志信息级别为 informational (6 级)。

【配置方法】 ● 在设备上面配置系统日志写入到内存缓冲区参数信息

```
Ruijie# configure terminal
Ruijie(config)# logging buffered 131072 informational
```

【检验方法】 ● 通过 **show logging** 命令可以查看用户配置的相关参数信息及系统最近产生的日志信息。

```
Timestamp debug messages: datetime
Timestamp log messages: datetime
Sequence-number log messages: enable
Sysname log messages: enable
Count log messages: enable
Trap logging: level informational, 121 message lines logged, 0 fail
Log Buffer (Total 131072 Bytes): have written 4200
001301: *Jun 14 2013 19:01:09.488: Ruijie %SYS-5-CONFIG_I: Configured from console by admin on console
001302: *Jun 14 2013 19:01:40.293: Ruijie %SYS-5-CONFIG_I: Configured from console by admin on console
// 这里省略其它日志信息，客户 show logging 时以实际为准。
```

6.4.5 配置系统日志发送往日志服务器

配置效果

- 可以将系统产生的日志信息发送往日志服务器，方便管理员在服务器上统一监控设备的日志信息。

注意事项

- 要将日志信息发送给日志服务器，必须打开日志信息的时间戳开关或序列号开关，否则日志信息将不会发给日志服务器。

配置方法

📄 设置日志发往指定的日志服务器

- 必选配置，缺省情况下系统产生的日志信息不会发送日志服务器。
- 若无特殊要求，应在每台设备上面配置。

📄 设置日志信息允许发往日志服务器的级别

- 可选配置，缺省情况下系统发往日志服务器的日志级别为 informational (6 级)。
- 若无特殊要求，在需要设置日志信息允许发往日志服务器级别的设备上面配置。

设置发往服务器的日志信息的系统设备值

- 可选配置，在没有开启 RFC5424 日志格式的情况下，日志信息发往服务器的系统设备值默认为 local7 (23)；在开启 RFC5424 日志格式的情况下，日志信息发往服务器的系统设备值默认为 local0 (16)。
- 若无特殊要求，在需要设置发往服务器的日志信息的系统设备值的设备上面配置。

设置发往服务器的日志信息的源接口

- 可选配置，缺省情况下发往日志服务器的日志报文源地址为发送报文接口的 IP 地址。
- 若无特殊要求，在需要设备发往服务器的日志信息的源接口的设备上面配置。

设置发往服务器的日志信息的源地址

- 可选配置，缺省情况下发往日志服务器的日志报文源地址为发送报文接口的 IP 地址。
- 若无特殊要求，在需要设置发往服务器的日志信息的源地址的设备上面配置。

检验方法

- 通过 **show logging config** 命令可以查看设置的日志服务器参数信息。

相关命令

设置日志发往指定的日志服务器

【命令格式】 **logging server** { *ip-address* } [**udp-prot** *port*]

或 **logging** { *ip-address* } [**udp-prot** *port*]

【参数说明】 *ip-address* : 接收日志信息的主机 IP 地址

udp-port *port* : 指定日志主机的端口号 (默认端口号为 514)

【命令模式】 全局配置模式

【使用指导】 该命令用于指定接收日志信息的日志服务器地址，可以同时指定多个日志服务器，日志信息将被同时分给配置的所有的日志服务器。

 锐捷产品允许配置最多 5 个日志服务器。

设置日志信息允许发往日志服务器的级别

【命令格式】 **logging trap** [*level*]

【参数说明】 *level* : 日志信息的级别

【命令模式】 全局配置模式

【使用指导】 默认发送往日志服务器的日志信息级别为 informational (6 级)。

可以通过特权命令 **show logging config** 来查看允许发送往日志服务器的级别。

设置发往服务器的日志信息的系统设备值

- 【命令格式】 **logging facility** *facility-type*
- 【参数说明】 *facility-type* : 日志信息设备值
- 【命令模式】 全局配置模式
- 【使用指导】 在没有开启 RFC5424 日志格式的情况下, 日志信息发往服务器的系统设备值默认为 local7 (23); 在开启 RFC5424 日志格式的情况下, 日志信息发往服务器的系统设备值默认为 local0 (16)。

设置发往服务器的日志信息的源接口

- 【命令格式】 **logging source** [**interface**] *interface-type interface-number*
- 【参数说明】 *interface-type* : 接口类型
interface-number : 接口编号
- 【命令模式】 全局配置模式
- 【使用指导】 默认情况下, 发送给服务器的日志报文源 IP 地址是报文发送接口的 IP 地址。
为了便于跟踪管理, 可以使用该命令将所有日志报文的源 IP 地址固定为某个接口的 IP 地址, 这样管理员就通过唯一地址识别从哪台设备发送出来的日志报文, 倘若设备上未配置该源接口或源接口上未配置 IP 地址, 则日志报文源 IP 地址仍为报文发送接口的 IP 地址。

设置发往服务器的日志信息的源地址

- 【命令格式】 **logging source** { **ip** *ip-address* }
- 【参数说明】 **ip** *ip-address* : 指定向 IPV4 日志主机发送日志报文的源 IPV4 地址
- 【命令模式】 全局配置模式
- 【使用指导】 默认情况下, 发送给 Syslog Server 的日志报文源 IP 地址是报文发送接口的 IP 地址。
为了便于跟踪管理, 可以使用该命令将所有日志报文的源 IP 地址固定为某个 IP 地址, 这样管理员就通过唯一地址识别从哪台设备发送出来的日志报文, 倘若设备上未配置该 IP 地址, 则日志报文源 IP 地址仍为报文发送接口的 IP 地址。

配置举例

配置系统日志发送往日志服务器

- 【网络环境】 假设网络环境中, 有以下日志信息发送往日志服务器设置要求:
 - 1、设置日志服务器 IPv4 地址: 10.1.1.100;
 - 2、设置允许发送到日志服务器的日志信息级别为 debugging (7 级);
 - 3、设置发往日志服务器的日志信息的源接口为 Loopback 0。

- 【配置方法】
 - 在设备上配置系统日志发送往日志服务器

```
Ruijie# configure terminal
Ruijie(config)# logging server 10.1.1.100
Ruijie(config)# logging trap debugging
Ruijie(config)# logging source interface Loopback 0
```

- 【检验方法】
- 通过 **show logging config** 命令可以查看用户配置的相关参数信息。

```
Ruijie#show logging config
Syslog logging: enabled
  Console logging: level informational, 1307 messages logged
  Monitor logging: level informational, 0 messages logged
  Buffer logging: level informational, 1307 messages logged
  File logging: level informational, 122 messages logged
  File name:syslog_test.txt, size 128 Kbytes, have written 5 files
  Standard format:false
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
  Sequence-number log messages: enable
  Sysname log messages: enable
  Count log messages: enable
  Trap logging: level debugging, 122 message lines logged,0 fail
  logging to 10.1.1.100
```

6.4.6 配置系统日志写入到日志文件

配置效果

- 可以将系统产生的日志信息按指定的频率写入到日志文件，便于管理员在设备本地随时查看历史日志信息。

注意事项

- 系统产生的日志信息是先缓冲到内存缓冲区当中，然后当缓冲区的时候或定时（默认为间隔 1 小时）写入到日志文件的，并不是产生日志信息的时候就立即写入到日志文件当中。

配置方法

✚ 设置日志信息写入的日志文件参数

- 必选配置，缺省情况下系统产生的日志信息不会写入日志文件中。
- 若无特殊要求，应在每台设备上面配置。

✚ 设置日志信息写入文件的个数

- 可选配置，缺省情况下系统日志写入到文件的个数为 16。
- 若无特殊要求，在需要设置日志文件个数的设备上面配置。

✚ 设置日志信息写入文件的时间间隔

- 可选配置，缺省情况下系统日志写入到文件的时间间隔为每小时写一次。
- 若无特殊要求，在需要设置日志信息写入文件的时间间隔的设备上面配置。

设置日志信息写入文件的保存时间

- 可选配置，缺省情况下系统对日志文件的保存时间是没有限制的。
- 若无特殊要求，在需要设备日志信息写入文件的保存时间的设备上面配置。

设置将缓冲区当中的日志信息立即写入到日志文件中

- 可选配置，缺省情况下设备产生的日志信息会先缓存在系统日志缓冲区中，只有当缓冲区满或定时器到期后，才会将缓冲区中的日志信息写入到日志文件中。
- 若无特殊要求，应在用户收集日志文件的时候进行配置，且该命令配置一次作用一次，配置后立即将存在缓冲区中的日志信息写入到日志文件中。

检验方法

- 通过 `show logging config` 命令可以查看设置的日志服务器参数信息

相关命令

设置日志信息写入的日志文件参数

【命令格式】 `logging file { flash:filename | } [max-file-size] [level]`

【参数说明】 `flash`：日志文件选择保存在扩展 FLASH 当中。

`filename`：日志文件名，不需要携带文件类型后缀，固定为 txt 类型。

`max-file-size`：日志文件的最大值。从 128K 到 6M bytes，缺省大小为 128K。

`level`：允许写入到日志文件的信息级别。

【命令模式】 全局配置模式

【使用指导】 该命令将在指定的文件存储设备上根据指定的文件名创建文件用于储存日志，文件大小会随日志增加而增加，但其上限以配置的 `max-file-size` 为准，若没有指定 `max-file-size`，则日志文件的大小默认为 128K。

配置该命令后，系统将日志信息保存到文件中，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 类型，配置文件后缀名将被拒绝。

配置了日志写文件功能后，日志信息将间隔 1 小时，写入到文件当中，而日志文件的名称（假设此次已经配置：`logging file flash:syslog`）依次为 `syslog.txt`、`syslog_1.txt`、`syslog_2.txt`..... `syslog_14.txt`、`syslog_15.txt` 总共 16 个日志文件。这 16 个日志文件循环重写 比如 写完 `syslog.txt` 后 写 `syslog_1.txt` 直至 `syslog_15.txt`，然后再返回来写 `syslog.txt`，这样子循环重写。

设置日志文件个数

【命令格式】 `logging file numbers numbers`

【参数说明】 `numbers`：日志文件的个数，范围：2~32，单位：个

【命令模式】 全局配置模式

【使用指导】 通过此命令设置日志信息写入文件的个数。

修改日志文件的个数，系统不会删除已经产生的日志文件，因此，如果为了节约扩展 FLASH 的空间，用户需要手动删除系统已经产生的日志文件（删除之前可以先通过 tftp 将日志文件传输到外界服务器）。例如：系统开启日志写文件功能后，默认会写 16 个日志文件，并且假设设备已经产生了 16 个日志文件，此时想修改日志文件的个数为 2 个，系统产生的新日志信息将在索引值为 0 和 1 的两个日志文件中进行不断的循环覆盖重写，但是之前已经产生的索引值为 2 到 16 的日志文件还是会保留，系统不会删除，用户可以根据需要手动删除日志文件。

设置日志信息写入文件的时间间隔


- 【命令格式】 **logging flash interval seconds**
- 【参数说明】 *seconds*：日志信息写入到 FLASH 文件的时间间隔，范围：1~51840，单位：秒
- 【命令模式】 全局配置模式
- 【使用指导】 通过此命令设置日志信息保存到文件中的时间间隔，且从命令配置后开始计时。

设置日志信息写入文件的保存时间

- 【命令格式】 **logging life-time level level days**
- 【参数说明】 *level*：日志信息的级别。
days：日志信息保存时间。单位：天。保存时间不小于 7 天。
- 【命令模式】 全局配置模式
- 【使用指导】 用户开启了基于时间的日志保存功能，系统针对同一级别、同一天内产生的日志信息，写入到同一个日志文件中，日志文件的名称形如“yyyy-mm-dd_filename_level.txt”，其中：yyyy-mm-dd 为日志信息产生的当天绝对时间；filename 为 **logging file flash** 命令配置的日志文件名称，level 为对应的日志信息级别。
用户对某个等级的日志信息进行保存时间限制后，当对应级别的日志信息超过日志保存时间限制后，将进行删除。为了网管的方便，目前系统要求日志信息最少可以保存 7 天，最长可以保存 365 天。
为了兼容以前的配置命令，用户在没有开启基于时间的日志保存功能时，日志仍然基于文件大小进行日志信息的保存。

设置将缓冲区当中的日志信息立即写入到日志文件中

- 【命令格式】 **logging flash flush**
- 【参数说明】 -
- 【命令模式】 全局配置模式
- 【使用指导】 在系统开启日志信息写日志文件功能后，设备产生的日志信息会先缓存在系统日志缓冲区中，只有当缓冲区满或定时器到期后，才会将缓冲区中的日志信息写入到日志文件中，可以通过该命令设置将系统缓冲区中的日志信息立即写入到日志文件中。

 用户配置 **logging flash flush** 命令时，配置一次作用一次，配置后立即将存在缓冲区中的日志信息写入到日志文件中

配置举例

配置系统日志写入到日志文件

【网络环境】 假设网络环境中，有以下日志信息写入到日志文件设置要求：

- 1、设置日志文件名称为 syslog；
- 2、设置允许输出到控制台的日志信息级别为 debugging（7级）；
- 3、设备日志信息写入到文件的时间间隔为 10 分钟（600 秒）。

【配置方法】 ● 在设备上面配置系统日志写入到日志文件

```
Ruijie# configure terminal
Ruijie(config)# logging file flash:syslog debugging
Ruijie(config)# logging flash interval 600
```

【检验方法】 ● 通过 **show logging config** 命令可以查看用户配置的相关参数信息。

```
Ruijie(config)#show logging config
Syslog logging: enabled
  Console logging: level informational, 1307 messages logged
  Monitor logging: level informational, 0 messages logged
  Buffer logging: level informational, 1307 messages logged
  File logging: level debugging, 122 messages logged
  File name:syslog.txt, size 128 Kbytes, have written 1 files
  Standard format:false
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
  Sequence-number log messages: enable
  Sysname log messages: enable
  Count log messages: enable
  Trap logging: level debugging, 122 message lines logged,0 fail
    logging to 10.1.1.100
```

6.4.7 配置系统日志过滤功能

配置效果

- 在某些情况下，管理员可能不想让某些日志信息显示出来，则可以通过此功能过滤系统产生的日志信息。
- 默认情况下，各个模块打出来的日志信息都可以显示到控制台或其它终端上面。设置日志信息过滤原则可以让某些日志信息打出到某些终端中，或者只想让某些日志信息打出到某些终端中。

注意事项

- 日志信息的两种过滤类型，分为：“只包含”和“只过滤”，某一时刻只能配置其中的一种类型。

- 当用户配置的日志信息过滤规则中，若单个匹配规则和精确匹配规则中同时配置了一样的模块名、助记符或信息等级，则单个匹配规则的优先级高于精确匹配。

配置方法

设置日志信息的过滤方向

- 可选配置，缺省情况下过滤方向为 all（即过滤所有方向的日志信息）。
- 若无特殊要求，在需要设置日志信息的过滤方向的设备上配置。

设置日志信息的过滤方式

- 可选配置，缺省情况下日志过滤方式为“只过滤”。
- 若无特殊要求，在需要设置日志信息的过滤方式的设备上配置。

设置日志信息的过滤规则

- 必选配置，缺省情况下，系统没有设置任何过滤规则，不对日志信息进行过滤。
- 若无特殊要求，在需要设置日志信息的过滤规则的设备上配置。

检验方法

- 通过 **show running** 命令可以查看设置的日志过滤功能参数信息

相关命令

设置日志信息的过滤方向

【命令格式】 **logging filter direction { all | buffer | file | server | terminal }**

【参数说明】 **all**：代表过滤往所有方向的日志信息。

buffer：代表过滤往日志缓冲区的日志信息（即 show logging 显示出来的日志信息）；

file：代表只过滤往日志文件的日志信息；

server：代表只过滤往日志服务器的日志信息；

terminal：代表过滤往控制台和 VTY 终端（包括 Telnet/SSH 等）的日志信息。

【命令模式】 全局配置模式

【使用指导】 默认为 all，即过滤所有方向的日志信息。

default logging filter direction 命令恢复日志信息的过滤方向为 all。

设置日志信息的过滤方式

【命令格式】 **logging filter type { contains-only | filter-only }**

【参数说明】 **contains-only** 代表“只包含”，意思是：只输出包含了过滤规则里面的关键字的日志信息，其它没有包含过滤规则里面的关键字的日志信息不会输出；

filter-only 代表“只过滤”，意思是：将过滤掉包含了过滤规则里面的关键字的日志信息，不会输出这些过滤

掉的日志信息。

【命令模式】 全局配置模式

【使用指导】 日志过滤方式分为“只包含”和“只过滤”两种方式。默认为 filter-only，即“只过滤”。

设置日志信息的过滤规则

【命令格式】 **logging filter rule { exact-match module module-name mnemonic mnemonic-name level level | single-match { level level | mnemonic mnemonic-name | module module-name } }**

【参数说明】 **exact-match**：代表精确匹配，若选择精确匹配，则后面的三个过滤选项都需要选上。

single-match：代表单个匹配，若选择单个匹配，则后面的三个过滤选项只需要选择其中的一个。

module module-name：模块名，即填写要过滤的模块名称。

mnemonic mnemonic-name：助记符名称，即填写要过滤的日志信息助记符名称。

level level：日志信息级别，即填写要过滤的日志信息等级。

【命令模式】 全局配置模式

【使用指导】 日志过滤规则分为“精确匹配”和“单个匹配”两种过滤规则。

no logging filter rule exact-match [module module-name mnemonic mnemonic-name level level]命令删除日志信息的“精确匹配”过滤规则。支持一次性删除所有的“精确匹配”过滤规则，也可以逐条进行删除。

no logging filter rule single-match [level level | mnemonic mnemonic-name | module module-name]命令删除日志信息的“单个匹配”过滤规则。支持一次性删除所有的“单个匹配”过滤规则，也可以逐条进行删除。

配置举例

配置系统日志过滤功能

【网络环境】 假设网络环境中，有以下日志信息过滤功能设置要求：

- 1、设置日志信息的过滤方向为 **terminal**、**server** 两个方向；
- 2、设置日志信息的过滤方式为“只过滤”；
- 3、设备日志信息的过滤规则为“单个匹配”，并且模块名包含 **SYS** 的日志信息过滤掉。

【配置方法】 ● 在设备上面配置系统日志的过滤功能

```
Ruijie# configure terminal
Ruijie(config)# logging filter direction server
Ruijie(config)# logging filter direction terminal
Ruijie(config)# logging filter type filter-only
Ruijie(config)# logging filter rule single-match module SYS
```

【检验方法】 ● 通过 **show running-config | include logging** 命令可以查看用户配置的相关参数信息。

● 通过进入/退出全局配置模式，观察系统是否会输出日志信息。

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

【网络环境】 假设网络环境中，有以下日志信息过滤功能设置要求：

- 1、设置日志信息的过滤方向为 **terminal**、**server** 两个方向；
- 2、设置日志信息的过滤方式为“只过滤”；
- 3、设备日志信息的过滤规则为“单个匹配”，并且模块名包含 SYS 的日志信息过滤掉。

【配置方法】 ● 在设备上面配置系统日志的过滤功能

```
Ruijie# configure terminal
Ruijie(config)# logging filter direction server
Ruijie(config)# logging filter direction terminal
Ruijie(config)# logging filter type filter-only
Ruijie(config)# logging filter rule single-match module SYS
```

【检验方法】 ● 通过 **show running-config | include logging** 命令可以查看用户配置的相关参数信息。
● 通过进入/退出全局配置模式，观察系统是否会输出日志信息。

```
Ruijie#show running-config | include logging
logging filter direction server
logging filter direction terminal
logging filter rule single-match module SYS
```

6.4.8 配置系统日志监控功能

配置效果

- 记录用户登录/退出的日志信息。开启记录用户登录/退出的日志信息后，当外界通过 Telnet/SSH 连接到设备时，设备将打出对应的 Log 信息，方便管理员监控设备的连接情况。
- 记录用户修订设备配置的日志信息。开启记录用户操作的日志信息后，当用户修订设备配置的时候，设备将打出对应的 Log 信息，方便管理员监控设备的配置修订情况。

注意事项

- 若设备上面同时配置 **logging userinfo** 和 **logging userinfo command-log**，则进行 **show running-config** 查看时，只会显示 **logging userinfo command-log**。

配置方法

▾ 开启记录用户登录/退出日志信息

- 可选配置，缺省情况下用户输入与日志信息输出同步功能是关闭的。
- 若无特殊要求，应在设备各个线路上面配置。

▾ 开启记录用户操作的日志信息

- 可选配置，缺省情况下用户输入与日志信息输出同步功能是关闭的。
- 若无特殊要求，应在设备各个线路上面配置。

检验方法

- 通过 **show running** 命令可以查看设置的用户输入同步输出功能参数信息

相关命令

▾ 开启记录用户登录/退出日志信息

【命令格式】 **logging userinfo**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 默认情况下，用户登录/退出设备的时候，设备是不会记录相关的 Log 信息。

▾ 开启记录用户操作的日志信息

【命令格式】 **logging userinfo command-log**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 设置执行配置命令时，记录用户操作的 Log 信息。默认情况下，用户修订设备配置的时候，设备是不会记录相关的操作 Log 信息。

配置举例

▾ 配置系统日志监控功能

【网络环境】 假设在网络环境当中，有以下日志信息监控功能设置要求：

- 1、开启记录用户登录/退出日志信息；
- 2、开启记录用户操作的日志信息。

【配置方法】 ● 在设备上面配置日志监控功能

```
Ruijie# configure terminal
Ruijie(config)# logging userinfo
Ruijie(config)# logging userinfo command-log
```

【检验方法】 ● 通过 **show running-config | include logging** 命令可以查看用户配置的相关参数信息。
● 通过在设备全局配置模式里面配置一条命令，触发系统产生用户操作的日志信息。

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

【网络环境】 假设在网络环境当中，有以下日志信息监控功能设置要求：

- 1、开启记录用户登录/退出日志信息；
- 2、开启记录用户操作的日志信息。

【配置方法】 ● 在设备上面配置日志监控功能

```
Ruijie# configure terminal
Ruijie(config)# logging userinfo
Ruijie(config)# logging userinfo command-log
```

【检验方法】 ● 通过 **show running-config | include logging** 命令可以查看用户配置的相关参数信息。
● 通过在设备全局配置模式里面配置一条命令，触发系统产生用户操作的日志信息。

```
Ruijie(config)#interface gigabitEthernet 0/0
*Jun 16 15:03:43: %CLI-5-EXEC_CMD: Configured from console by admin command: interface
GigabitEthernet 0/0
Ruijie#show running-config | include logging
logging userinfo command-log
```

6.4.9 配置用户输入与日志信息同步输出功能

配置效果

- 默认情况下，用户输入与日志信息输出不同步。配置输入同步功能后，即使在用户输入的过程中打印日志，在打印结束后仍然会将用户之前的输入显示出来，从而保证输入的完整性和连贯性。

注意事项

- 该配置命令需要在线路配置模式下面进行配置，并且在每个需要开启此功能的线路上面均要进行配置。

配置方法

▾ 设置用户输入与日志信息输出同步功能

- 可选配置，缺省情况下用户输入与日志信息输出同步功能是关闭的。
- 若无特殊要求，应在设备各个需要开启此功能的线路上面配置。

检验方法

- 通过 **show running** 命令可以查看设置的用户输入同步输出功能参数信息

相关命令

设置用户输入与日志信息输出同步功能

【命令格式】 **logging synchronous**

【参数说明】 -

【命令模式】 线路配置模式

【使用指导】 此命令打开用户输入与日志信息输出同步功能，可以防止用户正在输入的字符时被打断。

配置举例

配置用户输入与日志信息输出同步功能

【网络环境】 假设在网络环境当中，有以下用户输入同步输出功能设置要求：

- 1、设置用户输入与日志信息同步输出功能。

【配置方法】

- 在设备上面配置用户

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

【检验方法】

- 通过 **show running-config | begin line** 命令可以查看用户配置的相关参数信息。


```
Ruijie#show running-config | begin line
line con 0
 logging synchronous
 login local
```

如下所示，当用户敲入“vlan”后接口 0/1 发生状态改变，打印日志，打印结束后日志模块会自动把用户已经输入的“vlan”打印出来，使得用户可以继续输入：

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

6.5 监视与维护

清除各类信息

 在设备运行过程中执行 **clear** 命令，可能因为重要信息丢失而导致业务中断。

作用	命令
清除内存缓冲区中的日志信息	clear logging

查看运行情况

作用	命令
查看内存缓冲区中的日志报文，以及日志相关统计信息，日志信息按时间戳从旧到新的顺序显示	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，日志信息按时间戳从新到旧顺序显示	show logging reverse
查看系统日志配置的参数、统计信息	show logging config
查看系统中各模块日志信息统计情况	show logging count

7 CWMP

7.1 概述

CWMP 协议(CPE WAN Management Protocol 即 CPE 广域网管理协议)提供了设备统一管理的通用框架、消息规范、管理方法和数据模型,解决了用户侧设备数量繁多,部署分散,不易统一管理和维护的问题,提高了问题响应效率,节约了运维成本。

CWMP 协议主要提供下面一些功能:

- 自动配置和动态服务提供,用户侧设备启动初次接入网络时自动从管理服务器处获取配置,用户侧设备在运行过程中,管理服务器可以动态的改变其配置和状态;
- 主程序 / 配置文件管理,提供主程序和配置文件的升级及配置文件的上传;
- 软件模块功能的管理,通过各软件模块实现的数据模型对各软件模块进行管理;
- 状态行为监控,用户侧设备运行时状态及配置变化通告给管理服务器,通过这些实时变化的通告实现对用户侧设备的监控;
- 故障诊断,管理服务器通过用户侧设备提供的信息诊断或解决连接性问题及其他服务性问题,同时可以执行一些预定义的诊断行为。

 下文仅介绍 CWMP 的相关内容。

协议规范

TR069 的协议规范详见官方论坛:<http://www.broadband-forum.org/technical/trlist.php>。以下是主要的几份规范:

- 《TR-069_Amendment-4.pdf》, CWMP 协议标准。
- 《TR-098_Amendment-2.pdf》, CWMP 协议网关产品数据模型规范。
- 《TR-106_Amendment-6.pdf》, CWMP 协议 CPE 数据模型标准。
- 《TR-181_Issue-2_Amendment-5.pdf》, CPE 数据模型 2 规范。
- 《tr-098-1-4-full.xml》, CWMP 协议网关产品数据模型定义。
- 《tr-181-2-4-full.xml》, CWMP 协议 CPE 数据模型 2 定义。

7.2 典型应用

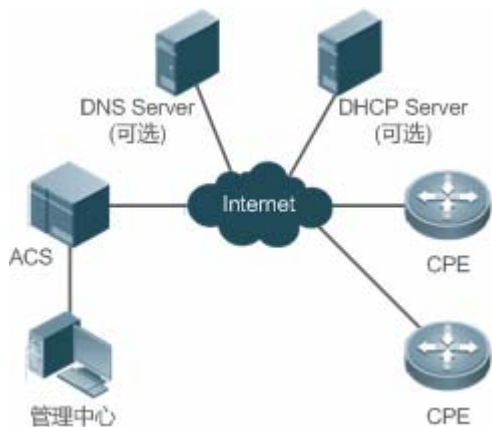
典型应用	场景描述
CWMP网络应用场景	通过配置 CPE 设备与 ACS 服务器建立连接,以实现 CPE 设备主程序升级,配置文件上传,恢复等功能。

7.2.1 CWMP 网络应用场景

应用场景

CWMP 的网络结构中主要包括 CPE、ACS、管理中心、DHCP 服务器和 DNS 服务器。大量的 CPE 接受 ACS 的管理，管理中心通过控制 ACS 服务器，实现对 CPE 设备的管理控制，一般控制中心为 WEB 浏览器，通过 WEB 浏览器控制 ACS 服务器

图 7-1



- 【注释】
- DHCP 服务器用于动态获取 ACS 的 URL，如果使用静态配置 ACS 的 URL，DHCP 服务器在该网络中为可选元素
 - DNS 服务器用于解析 ACS 或 CPE 的域名，如果 ACS 和 CPE 的 URL 中直接使用 IP 地址而不是域名，DNS 服务器在该网络中为可选元素

功能部属

- CPE 和 ACS 设备要运行 HTTP 协议

7.3 功能详解

基本概念

常用术语

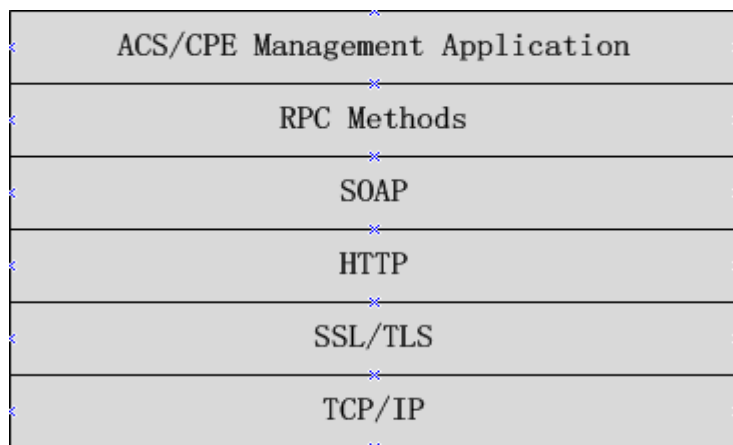
- CPE : Customer Premises Equipment (顾客预置设备)。
- ACS : Auto-Configuration Server (自动配置服务器)。

- RPC : Remote Procedure Call (远程过程调用)。
- DM : Data Model , 数据模型。

协议结构

CWMP 的协议结构如下图所示：

图 7-2 CWMP 的协议结构



如图所示，协议规范将 CWMP 协议的工作分为 6 个层次，各层次的功能及作用说明如下：

- ACS/CPE Management Application

运用程序管理层，该层并非 CWMP 协议本身的范畴，它是指 CPE/ACS 的各功能模块为了支持 CWMP 的管理进行的开发，如同 SNMP 一样，各功能模块的 MIB 管理本身即不属于 SNMP 的协议范畴。

- RPC Methods

RPC 方法管理层，该层提供了 ACS 与 CPE 之间交互的各种 RPC 方法，实现各种 RPC 方法的操作。

- SOAP

简单对象访问协议层，该层提供了 CWMP 协议的 XML 形式封装与解封装，CWMP 消息格式必须符合 SOAP 的封装语法。

- HTTP

所有的 CWMP 消息最终通过 HTTP 协议进行传输，ACS 和 CPE 同时支持 HTTP 客户端和服务器端功能，服务器端用于监控对端的反响连接。

- SSL/TLS

该层提供 CWMP 协议的安全性保证，包括数据完整性，机密性及认证的保护。

- TCP/IP

TCP/IP 协议栈。

RPC 方法管理

ACS 对 CPE 的管理监控主要是通过 RPC 方法进行的，主要包括如下的一些方法：

- GET 系列方法

该系列方法主要用于 ACS 远程获取 CPE 支持的 RPC 方法、CPE 支持的数据模型参数名、数据模型参数的值和数据模型参数的属性。

- SET 系列方法

该系列方法主要用于 ACS 远程设置 CPE 支持的数据模型参数的值和数据模型参数的属性。

- INFORM 方法

INFORM 方法用于 CPE 向 ACS 通告自己的设备标识、参数信息及所发生的事件。INFORM 方法为 ACS 与 CPE 建立会话时交互的第一个方法。

- DownLoad 方法

DownLoad 方法实现 ACS 远程控制 CPE 下载文件的管理，包括 CPE 主程序升级的控制、配置文件升级的控制和 WEB 包升级的控制。

- UpLoad 方法

UpLoad 方法实现 ACS 远程控制 CPE 上传文件的管理，包括 CPE 配置文件上传的控制、日志文件上传的控制。

- Reboot 方法

Reboot 方法用于 ACS 远程控制 CPE 的重启行为。

📄 会话管理

CWMP 协议工作的基础是 CWMP 协议会话，CWMP 的交互就是 CWMP 的会话交互，CWMP 协议在 ACS 与 CPE 之间的所有交互都以其会话为基础，通过会话传输、管理、维护其操作，实现 ACS 与 CPE 之间的有效交互，实现 ACS 对 CPE 的管理和监控。ACS 与 CPE 的一次会话过程即为两者建立 TCP 连接，Inform 协商开始到当前所有交互完成 TCP 连接断开为止，这个过程称之为一次会话过程。根据会话发起方角色的不同将其分为 CPE 主动发起的会话和 ACS 请求的会话两种，下面就这两种运用场景进行说明。

📄 数据模型管理

CWMP 数据模型是 CWMP 工作的依据，CWMP 对所有功能模块的管理都是对 CWMP 数据模型的操作，各功能模块注册并实现自己支持数据模型，如果 SNMP 中各功能模块实现的 MIB 一样。

CWMP 数据模型以字符串的形式表示，为了区分数据模型的层次关系，以“.”分隔符区分上下级数据模型节点之间的关系，如 InternetGatewayDevice.LANDevice 的数据模型表示中，InternetGatewayDevice 为 LANDevice 的父数据模型节点，而 LANDevice 为 InternetGatewayDevice 子数据模型节点。

数据模型节点分为两类，一类为对象节点（object），一类为参数节点（parameter），也叫叶子节点。对象节点是指那些其下还有子节点的节点。而参数节点即没有子节点的叶子节点。对象节点分单实例对象节点和多实例对象节点，单实例对象节点指只存在单个实例对象的节点，多实例对象节点指存在多个实例对象的节点。数据模型节点分为可读节点和可读可写节点，可读节点只能读取其参数的值，不能进行修改，可读可写节点除了可读该节点参数值外还能对其进行修改。

数据模型节点存在两种属性，一种为是否通告的属性，即该数据模型对应参数值发生变化（非 CWMP 协议引起的变化）时是否将其通告给 ACS 服务器；一种是模型节点参数可被其他管理方式（非 ACS）写操作的标识，即其他管理方式如 Telnet 等是否可对该参数值进行修改。ACS 可以通过 RPC 方法修改数据模型的属性。

CWMP 协议对数据模型的管理通过对应的 RPC 方法进行。

📄 事件管理

在 CPE 设备上,当一些 ACS 感兴趣或关心的事件发生时,CPE 需要将这些事件通告给 ACS,ACS 通过监控这些事件来监控 CPE 的工作状态,CWMP 的事件如同 SNMP 中的 TRAP 和产品日志功能中的日志信息。ACS 可以通过 RPC 方法控制和调整自己关心的事件,过滤掉不关心的事件类型。CWMP 中的事件总体分为两类,单量事件类型和增量事件类型,单量事件类型的事件是指同一个事件第二次发生时,该事件不再有量的变化而是丢弃老的,保留新的,增量事件类型是指同一事件后续多次发生时,老的不能丢弃,新产生的事件作为一个完整的事件保留,量上加 1。

CPE 产生的所有事件通过 INFORM 方法向 ACS 通告。

功能特性

功能特性	作用
主程序升级	ACS 通过 DownLoad 方法控制 CPE 的主程序升级
配置文件升级	ACS 通过 DownLoad 方法控制 CPE 的配置文件升级
配置文件上传	ACS 通过 UpLoad 方法控制 CPE 的配置文件上传
CPE备份恢复	当设备出现脱管状态时,远程设备恢复到脱管前的状态

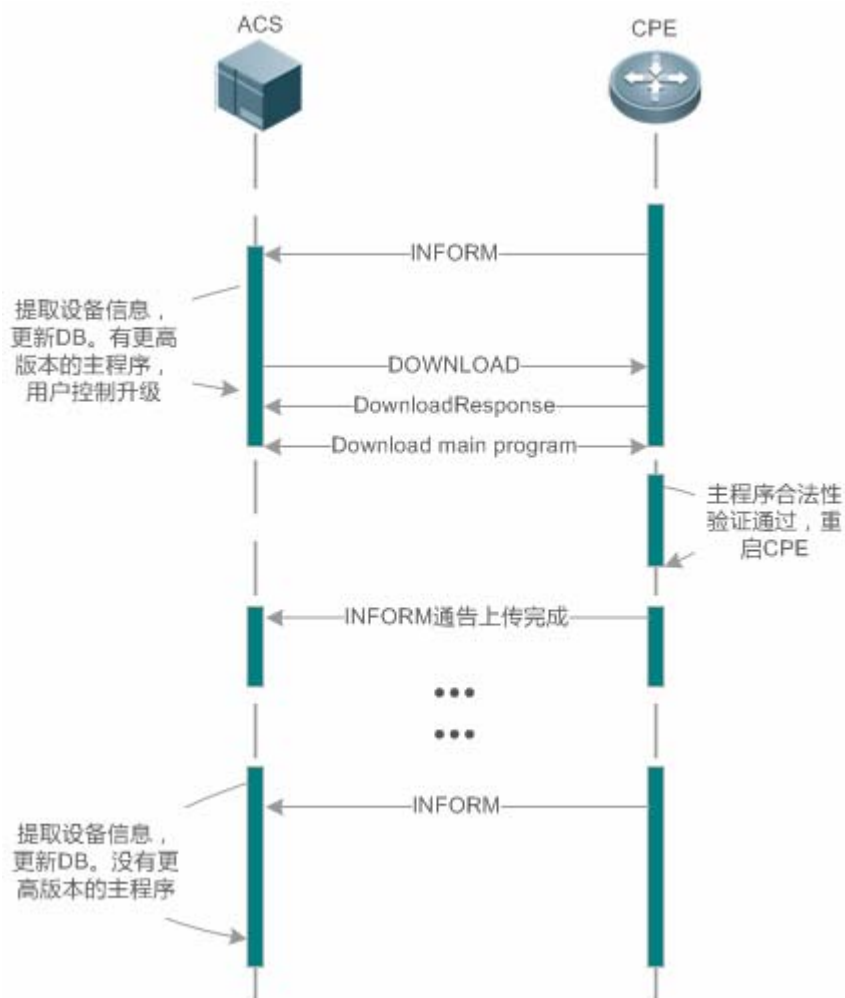
7.3.1 主程序升级

主程序升级,是指对各网元设备的主程序进行更新,通过主程序的升级来达到对设备版本的升级或更新换代

工作原理

主程序升级时序图

图 7-3



用户指定 CPE 升级配置文件，ACS 向 CPE 下发升级配置文件的 DownLoadand 方法。CPE 从 DownLoad 方法中指定的文件服务器下载配置文件，升级自身的配置文件，更新完配置文件后重启 CPE 设备，完成配置文件的升级。CPE 重启后向 ACS 通告主程序管理升级完成。

 ACS 可以同时作为文件服务器，文件服务器也可以作为单独的服务器部署。

相关配置

使能 cwmp 功能

- 缺省情况下，CWMP 功能开启。
- 全局配置模式下使用 **cwmp** 命令可以开启 cwmp 功能。

配置 ACS URL

- 缺省情况下，无默认 ACS URL。

- 在 CWMP 配置模式下，使用 **acs url** 命令可以配置 ACS URL 地址。

↘ 配置 ACS 用户名

- 缺省情况下，无默认 ACS 用户名。
- 在 CWMP 配置模式下，使用 **acs username** 命令可以配置 ACS 用户名。

↘ 配置 ACS 用户密码

- 缺省情况下，无默认 ACS 用户密码。
- 在 CWMP 配置模式下，使用 **acs password** 命令可配置 ACS 用户密码

↘ 配置 CPE 的 URL

- 缺省情况下，无默认 CPE URL。
- 在 CWMP 配置模式下，使用 **cpe url** 命令可以配置 CPE URL。

↘ 配置 CPE 的用户名

- 缺省情况下，无默认 CPE 用户名。
- 在 CWMP 配置模式下，使用 **cpe username** 命令可以配置 CPE 的用户名。

↘ 配置 CPE 的用户密码

- 缺省情况下，无默认 CPE 用户密码。
- 在 CWMP 配置模式下，使用 **cpe password** 命令可配置 ACS 用户密码

↘ 使能 CPE 周期性 INFORM 功能

- 缺省情况下，CPE 的 INFORM 通告时间间隔为 600s。
- 在 CWMP 配置模式下，使用 **timer cpe-timeout** 命令可以配置 CPE 周期性 INFORM 功能。

↘ 配置 CPE 无数据超时时间

- 缺省情况下，CPE 的无数据超时间为 30s。
- 在 CWMP 配置模式下，使用 **timer cpe-timeout** 命令可以配置 CPE 会话无数据超时时间。

↘ 配置 CPE 文件下载功能

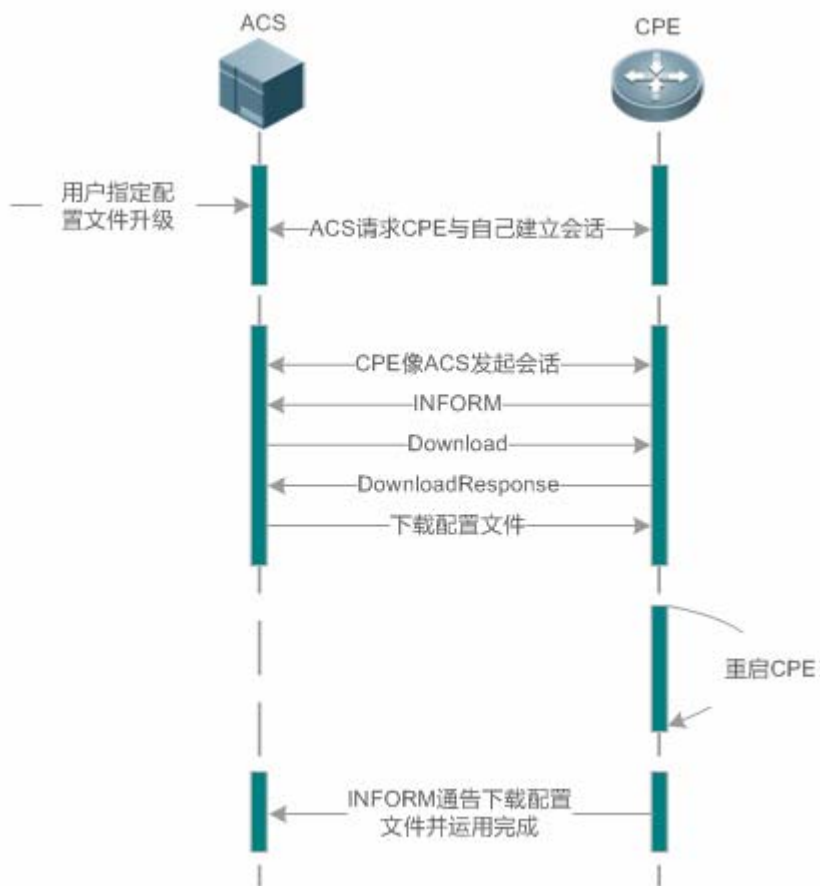
- 缺省情况下，CPE 文件下载功能为默认允许接收。
- 在 CWMP 配置模式下，使用 **no disable download** 命令开启 CPE 接受 ACS 下发的主程序和配置文件下载。

7.3.2 配置文件升级

配置文件升级，是指将整个设备的当前的配置文件替换为指定的配置，设备复位后，系统将运行全新的配置

工作原理

图 7-4



用户指定 CPE 升级配置文件，ACS 向 CPE 下发升级配置文件的 DownLoad 方法。CPE 从 DownLoad 方法中指定的文件服务器下载配置文件，升级自身的配置文件，更新完配置文件后重启 CPE 设备，完成配置文件的升级。CPE 重启后向 ACS 通告配置文件升级完成。

 ACS 可以同时作为文件服务器，文件服务器也可以作为单独的服务器部署。

相关配置

使能 cwmp 功能

同主程序升级中的使能 cwmp 功能配置

配置 ACS URL

同主程序升级中的配置 ACS URL 功能配置

↳ **配置 ACS 用户名**

同主程序升级中的配置 ACS 用户名功能配置

↳ **配置 ACS 用户密码**

同主程序升级中的配置 ACS 用户密码功能配置

↳ **配置 CPE 的 URL**

同主程序升级中的配置 cpe url 功能配置

↳ **配置 CPE 的用户名**

同主程序升级中的配置 cpe 用户名功能配置

↳ **配置 CPE 的用户密码**

同主程序升级中的配置 cpe 用户密码功能配置

↳ **使能 CPE 周期性 INFORM 功能**

同主程序升级中的配置 cpe 周期性 inform 功能配置

↳ **配置 CPE 无数据超时时间**

同主程序升级中的配置 cpe 无数据超时功能配置

↳ **配置 CPE 文件下载功能**

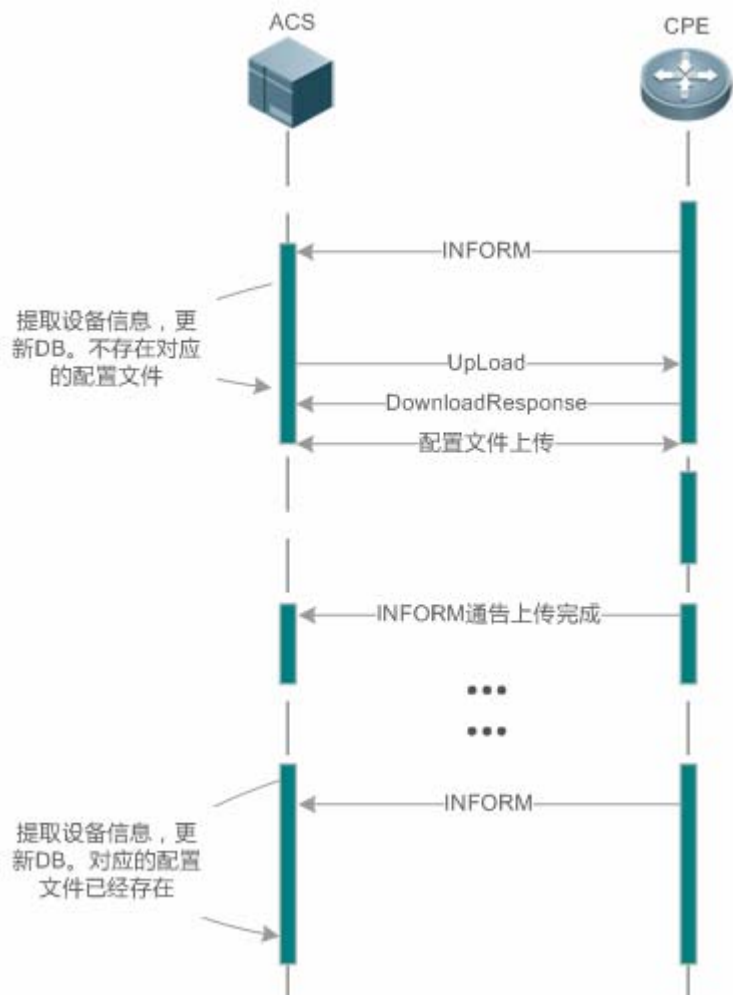
同主程序升级中的配置 cpe 文件下载功能配置

7.3.3 配置文件上传

配置文件上传，ACS 控制 CPE 的配置文件是通过 UpLoad 方法上传其配置文件

工作原理

图 7-5



CPE 初次上线 ACS，ACS 需要学习 CPE 的配置文件，学习过程如下：

- ACS 初次收到 CPE 的 INFORM 消息，根据 INFORM 消息中的设备信息，找到或建立对应的 CPE DB 信息；
- ACS DB 中还不存在当前 CPE 的配置文件，ACS 向该 CPE 下发上传配置文件的 Upload 方法；
- CPE 将当前的配置文件上传给 ACS 服务器；
- CPE 通告 ACS 配置文件上传完成。

相关配置

使能 cwmp 功能

同主程序升级中的使能 cwmp 功能配置

配置 ACS URL

同主程序升级中的配置 ACS URL 功能配置

配置 ACS 用户名

同主程序升级中的配置 ACS 用户名功能配置

📌 配置 ACS 用户密码

同主程序升级中的配置 ACS 用户密码功能配置

📌 配置 CPE 的 URL

同主程序升级中的配置 cpe url 功能配置

📌 配置 CPE 的用户名

同主程序升级中的配置 cpe 用户名功能配置

📌 配置 CPE 的用户密码

同主程序升级中的配置 cpe 用户密码功能配置

📌 使能 CPE 周期性 INFORM 功能

同主程序升级中的配置 cpe 周期性 inform 功能配置

📌 配置 CPE 无数据超时时间

同主程序升级中的配置 cpe 无数据超时功能配置

📌 配置 CPE 文件上传功能

- 缺省情况下，CPE 文件下载功能为默认允许接收。
- 在 CWMP 配置模式下，使用 **no disable upload** 命令开启 CPE 接受 ACS 下发的配置文件和日志文件上传。

7.3.4 CPE 备份恢复

CPE 备份恢复，是指管理端由于一些异常的操作导致远程设备脱管，当这种情况发生时，需要远程设备恢复到脱管前的状态，恢复对远程设备的管理，重新对远程设备执行正确的管理与操作。

工作原理

在设备上配置 CPE 主程序/配置在异常情况下的恢复功能，指当 CPE 进行主程序/配置升级后无法连接 ACS，出现脱管现象时，能及时的恢复到脱管前的主程序和配置，恢复 ACS 对 CPE 的管理，这种情况的出现一般是下发了错误的主程序或配置所导致。




CPE 在每次接收主程序升级以及配置下发时，先备份当前的配置与主程序，并提供机制用于判断是否出现上述场景描述的问题，若出现，则将系统恢复到之前的可管理状态。

相关配置

📌 配置 CPE 备份恢复功能

- 缺省情况下，CPE 备份恢复功能为开启，默认恢复时间为 60s。
- 在 CWMP 配置模式下，使用 **cpe back-up** 命令开启 CPE 备份恢复功能。
- 恢复时间设置越大，CPE 启动恢复延迟时间越久。

7.4 配置详解

配置项	配置建议 & 相关命令	
建立CWMP基本连接	 必须配置。配置 CPE 连接 ACS 时用于认证的用户名和密码及配置 ACS 连接 CPE 时用于认证的用户名和密码	
	cwmp	使能 CWMP 并进入 CWMP 配置模式
	acs username	配置 CPE 连接 ACS 时用于认证的用户名
	acs password	配置 CPE 连接 ACS 时用于认证的密码
	cpe username	配置 ACS 连接 CPE 时用于认证的用户名
	cpe password	配置 ACS 连接 CPE 时用于认证的密码
	 可选配置。配置 CPE 及 ACS 设备的 URL	
acs url	配置 CPE 连接 ACS 的 URL。	
cpe url	配置 ACS 连接 CPE 的 URL	
配置CWMP相关属性	 可选配置。配置 CPE 设备的基本功能(如 CPE 主程序/配置备份恢复功能，不向 ACS 上传配置文件和日志文件的管理等)	
	cpe inform	配置 CPE 周期性 INFORM 通告功能
	cpe back-up	配置 CPE 主程序/配置备份恢复功能
	disable download	配置不接收 ACS 下发下载主程序和配置文件的管理
	disable upload	配置不向 ACS 上传配置文件和日志文件的管理
	timer cpe- timeout	配置 ACS 无响应 CPE 超时时间

7.4.1 建立 CWMP 基本连接

配置效果

- 实现 ACS 设备与 CPE 设备会话连接的建立

注意事项

- 无

配置方法

▾ 使能 CWMP 并进入 CWMP 配置模式

- 默认开启 CWMP 功能。
- 必须配置。
- CPE 设备上配置。

▾ 配置 CPE 连接 ACS 时用于认证的用户名

- 必须配置。
- ACS 设备上配置。
- 只能配置一个 ACS 用户名，多次配置 ACS 的用户名时，最新的配置生效。

▾ 配置 CPE 连接 ACS 时用于认证的密码

- 必须配置。
- ACS 设备上配置
- ACS 用户密码可以为明文和密文形式，只能配置一个 ACS 用户密码，多次配置 ACS 的用户密码时，最新的配置生效。

▾ 配置 ACS 连接 CPE 时用于认证的用户名

- 必须配置。
- CPE 设备上配置
- 只能配置一个 CPE 用户名，多次配置 CPE 的用户名时，最新的配置生效。

▾ 配置 ACS 连接 CPE 时用于认证的密码

- 必须配置。
- CPE 设备上配置
- ACS 用户密码可以为明文和密文形式，只能配置一个 ACS 用户密码，多次配置 ACS 的用户密码时，最新的配置生效。

▾ 配置 CPE 连接 ACS 的 URL

- 默认 NULL，可选配置。
- CPE 设备上配置。
- 只能配置一个 ACS URL，多次配置 ACS 的 URL 时，最新的配置生效，ACS 的 URL 必须是 HTTP 的形式。

▾ 配置 ACS 连接 CPE 的 URL

- 默认 NULL，可选配置。
- CPE 设备上配置。

- 只能配置一个 CPE URL，多次配置 CPE 的 URL 时，最新的配置生效。CPE 的 URL 必须是 HTTP 的形式，不支持域名的形式配置 CPE 的 URL。

检验方法

- 通过 `show cwmp status` 命令查看

相关命令

配置 CWMP 开启功能

- 【命令格式】 `cwmp`
- 【参数说明】 -
- 【命令模式】 全局模式
- 【使用指导】 -

配置 CPE 连接 ACS 时用于认证的用户名

- 【命令格式】 `acs username username`
- 【参数说明】 `username username`：配置 CPE 连接 ACS 用于认证的用户名。
- 【命令模式】 cwmp 配置模式
- 【使用指导】 -

配置 CPE 连接 ACS 时用于认证的密码

- 【命令格式】 `ip pim sparse-mode`
- 【参数说明】 `Password`: CPE 连接 ACS 用于认证的密码。
`encryption-type`: 可配置为 0 或 7，为 0 表示无加密，为 7 表示简单加密
`encrypted-password`: 密码文本
- 【命令模式】 cwmp 配置模式
- 【使用指导】 -

配置 ACS 连接 CPE 时用于认证的用户名

- 【命令格式】 `acs username username`
- 【参数说明】 `Username`: 配置 ACS 连接 CPE 用于认证的用户名
- 【命令模式】 cwmp 配置模式
- 【使用指导】 -

配置 ACS 连接 CPE 时用于认证的密码

- 【命令格式】 `cpe password {password | encryption-type encrypted-password}`
- 【参数说明】 `Password`: CPE 连接 ACS 用于认证的密码。
`encryption-type`: 可配置为 0 或 7，为 0 表示无加密，为 7 表示简单加密

encrypted-password: 密码文本

【命令模式】 cwmp 配置模式

【使用指导】 配置 ACS 连接 CPE 用于认证的密码，通常无须输入加密类型。一般情况下，只有当复制并粘贴已经加密过后该命令的密码时，才需要输入加密类型。有效密码的格式要求如下：

- 必须包含 1 到 26 个大小写字母和数字字符。
- 密码前面可以有前导空格，但被忽略。中间及结尾的空格则作为密码的一部分。

配置 CPE 连接 ACS 的 URL

【命令格式】 **acs url url**

【参数说明】 *url* : ACS 的 URL。

【命令模式】 CWMP 配置模式

【使用指导】 配置 CPE 连接 ACS 的 URL，在没有手动配置 ACS URL 的情况下，如果使用了 DHCP 获取到了动态的 ACS URL，将使用动态获取到的 ACS URL 向 ACS 发起连接。对 ACS 的 URL 格式要求如下：

- ACS 的 URL 必须是 `http://ip [: port]/ path` 的格式。
- ACS URL 的最大长度为 256 个字符。

配置 ACS 连接 CPE 的 URL

【命令格式】 **cpe url url**

【参数说明】 *url* : cpe 的 URL。

【命令模式】 cwmp 配置模式

【使用指导】 配置 ACS 连接 CPE 的 URL，在没有手动配置的情况下，CPE 将根据 ACS 的 URL 自动选取 CPE 的 URL，CPE 的 URL 格式要求如下：

- CPE 的 URL 必须是 `http://ip [: port]/` 的格式。
- CPE URL 的最大长度为 256 个字符。

配置举例

i 以下配置举例，仅介绍 CWMP 相关的配置。

在 CPE 设备上配置用户名和密码

【网络环境】

图 7-6



【配置方法】

- 使能 CWMP
- 在 CPE 设备上配置 CPE 连接 ACS 时用于认证的用户名和密码
- 在 CPE 设备上配置 ACS 连接 CPE 时用于认证的用户名和密码

CPE

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

```
Ruijie(config-cwmp)# acs username USERB
Ruijie(config-cwmp)# acs password PASSWORDB
Ruijie(config-cwmp)# cpe username USERB
Ruijie(config-cwmp)# cpe password PASSWORDB
```

【检验方法】 ● 通过在 CPE 设备上 **show** 命令查看命令是否配置成功

CPE

```
Ruijie # show cwmp configuration

CWMP Status           : enable
ACS URL                : http://10.10.10.1:7547/acs
ACS username          : USERA
ACS password           : *****
CPE URL                : http://10.10.10.2:7547/
CPE username          : USERB
CPE password           : *****
```

📌 配置 ACS 和 CPE 的 URL 连接

【网络环境】 同图 7-6

【配置方法】 ● 配置 ACS 设备的 URL 地址
● 配置 CPE 设备的 URL 地址

CPE

```
Ruijie# configure terminal
Ruijie(config)# cwmp
Ruijie(config-cwmp)# acs url http://10.10.10.1:7547/acs
Ruijie(config-cwmp)# cpe url http://10.10.10.1:7547/
```

【检验方法】 通过在 CPE 设备上 **show** 命令查看命令是否配置成功

CPE

```
Ruijie #show cwmp configuration

CWMP Status           : enable
ACS URL                : http://10.10.10.1:7547/acs
ACS username          : USERA
ACS password           : *****
CPE URL                : http://10.10.10.2:7547/
```

常见错误

- 如果用户输入密码类型为密文，密码长度超过 254 或者长度不为偶数错误
- 如果用户输入密码类型为明文，密码长度超过 126 错误
- 如果用户输入密码类型为明文，并且包括非法字符错误
- 如果 ACS URL 地址为 NULL，则提示错误

- 如果 CPE URL 地址为 NULL，则提示错误

7.4.2 配置 CWMP 相关属性

配置效果

- 用于实现 CPE 设备常用功能的配置(如主程序/配置备份恢复，是否接受 ACS 下发主程序及配置文件，是否向 ACS 上传配置文件和日志文件管理等)

配置方法

配置 CPE 周期性通告功能

- 可选配置，单位为秒，取值范围 30~3600，缺省值 600s。
- 当 CPE 设备需要重新设定周期性通告时间的时候配置该功能。
- CPE 设备上配置。

配置不接受 ACS 下发下载主程序和配置文件的管理

- 可选配置，默认接受 ACS 下发下载主程序和配置文件的管理。
- 当 CPE 设备不希望接受 ACS 下发下载主程序和配置文件管理的时候，配置该功能。
- CPE 设备上配置。

配置不向 ACS 上传配置文件和日志文件的管理

- 可选配置，默认为向 ACS 上传配置和日志文件管理。
- 当 CPE 设备不需要向 ACS 上传配置文件和日志文件的管理，配置该功能。
- CPE 设备上配置，当 CPE 设备不向 ACS 上传配置文件和日志文件的管理时配置该功能。

配置 CPE 主程序/配置备份恢复功能

- 可选配置，默认开启 CPE 主程序/配置备份恢复功能，单位为秒，取值范围 30-10000，默认备份恢复时间为 60s。
- 当 CPE 设备需要修改 CPE 主程序/配置备份恢复功能的时间时，配置该功能。
- CPE 设备上配置。

配置 ACS 无响应 CPE 超时时间

- 可选配置，单位为秒，取值范围 10~600，默认值为 30s。
- 当 CPE 设备需要修改 ACS 无响应 CPE 超时时间时，配置该功能。
- CPE 设备上配置。

检验方法

- 通过 `show cwmp configuration` 命令查看

相关命令

配置 CPE 周期性通告功能

【命令格式】 `cpe inform [interval seconds] [start-time time]`

【参数说明】 *Seconds*：配置 CPE 周期性 INFORM 通告时间间隔。单位为秒，取值范围 30 ~ 3600，缺省值 600。

Time：开始周期性 INFORM 的日期时间，格式为 yyyy-mm-ddThh:mm:ss

【命令模式】 cwmp 配置模式

【使用指导】 配置 CPE 周期性 INFORM 通告功能。

- 在没有配置 INFORM 开始时间的情况下，周期性 INFORM 从开启该功能开启，每经过一个 INFORM 周期通告一次。
- 在配置了 INFORM 开始日期时间的情况下，周期性 INFORM 的开始时间为该指定时间。如配置 INFORM 周期为 60 秒，开始时间为明天中午 12 点，则周期性 INFORM 通告从明天中午 12 点才开始，且每经过 60 秒 INFORM 通告一次。

配置不接收 ACS 下发下载主程序和配置文件的管理通告功能

【命令格式】 `disable download`

【参数说明】 -

【命令模式】 cwmp 配置模式

【使用指导】 配置不接收 ACS 下发的主程序和配置文件。

- 这个命令对配置脚本文件不起作用，配置 `disable` 的情况下，配置脚本可以执行。

配置 CPE 不向 ACS 上传配置文件和日志文件的管理

【命令格式】 `disable upload`

【参数说明】

【命令模式】 cwmp 配置模式

【使用指导】

配置 CPE 主程序/配置备份恢复功能

【命令格式】 `cpe back-up [delay-time seconds]`

【参数说明】 *Seconds*: CPE 主程序/配置备份恢复的延迟时间

【命令模式】 cwmp 配置模式

【使用指导】

配置 ACS 无响应 CPE 超时时间

【命令格式】 `timer cpe- timeout seconds`

【参数说明】 *Seconds*: 超时时间，单位为秒，取值范围 10 ~ 600。

【命令模式】 cwmp 配置模式

【使用指导】

配置举例

配置 CPE 周期 INFORM 通告时间间隔

【网络环境】 同图 7-6

- 【配置方法】
- 开启 CWMP 功能并进入 CWMP 配置模式
 - 配置 CPE 周期 INFORM 通告时间间隔为 60 秒

```
CPE
Ruijie#config
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#cpe inform interval 60
```

【检验方法】 通过在 CPE 设备上 **show** 命令查看命令是否配置成功

```
CPE
Ruijie #show cwmp configuration
CWMP Status           : enable
.....
CPE inform interval   : 60s
```

配置拒绝 ACS 下发下载主程序和配置文件的管理。

【网络环境】 同图 7-6

- 【配置方法】
- 开启 CWMP 功能并进入 CWMP 配置模式
 - 配置拒绝 ACS 下发下载主程序和配置文件的管理

```
CPE
Ruijie#config
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#disable download
```

【检验方法】 通过在 CPE 设备上 **show** 命令查看命令是否配置成功

```
CPE
Ruijie #show cwmp configuration
CWMP Status           : enable
.....
CPE download status   : disable
```

配置关闭 CPE 接受 ACS 下发的配置文件和日志文件上传。

【网络环境】 同图 7-6

- 【配置方法】
- 开启 CWMP 功能并进入 CWMP 配置模式
 - 配置关闭 CPE 接受 ACS 下发的配置文件和日志文件上传

```
CPE
Ruijie#config
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)# disable upload
```

【检验方法】 通过在 CPE 设备上 **show** 命令查看命令是否配置成功

```
CPE
Ruijie #show cwmp configuration
CWMP Status                : enable
.....
CPE upload status          : disable
```

▾ 配置备份恢复的延迟时间

【网络环境】 同图 7-6

- 【配置方法】
- 开启 CWMP 功能并进入 CWMP 配置模式
 - 配置备份恢复的延迟时间为 30s

```
CPE
Ruijie#config
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)# cpe back-up Seconds 30
```

【检验方法】

- 通过在 CPE 设备上 **show** 命令查看命令是否配置成功

```
CPE
Ruijie #show cwmp configuration
CWMP Status                : enable
.....
CPE back up delay time     : 30s
```

▾ 配置 CPE 无数据超时时间

【网络环境】 同图 7-6

- 【配置方法】
- 开启 CWMP 功能并进入 CWMP 配置模式
 - 配置备份恢复的延迟时间为 30s

```
CPE
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# cwmp
Ruijie(config-cwmp)# timer cpe-timeout 100
```

【检验方法】

- 通过在 CPE 设备上 **show** 命令查看命令是否配置成功

```
CPE Ruijie#show cwmp configuration
CWMP Status           : enable
.....
CPE wait timeout      : 100s
```

常见配置错误

无

7.5 监视与维护

查看运行情况

作用	命令
显示 CWMP 功能的当前配置	show cwmp configuration
显示 CWMP 的当前运行状态	show cwmp status

8 PoE

8.1 概述

Power over Ethernet，简称 **PoE**，是一个可以在以太网中透过双绞线来传输电力与数据到装置上的技术。通过这项技术包括网络电话、WIFI AP、网络摄影机、集线器、电脑等装置都能直接从双绞线上得到电力。

PoE 交换机供电的最长距离按照标准为 100m。支持 PoE 的交换机可对每个端口以及整个设备的供电情况进行统计，通过查询命令进行显示。

协议规范

目前 PoE 有标准 IEEE 802.3af、IEEE 802.3at，这两个标准的主要特性及区别如下表所示：

参数	802.3af	802.3at
PD 可用功率	12.95W	25.50W
PSE 提供的最大功率	15.4W	30W
PSE 电压范围	44.0-57.0V	50.0-57.0V
PD 电压范围	37.0-57.0V	42.5-57.0V
最大网线阻抗	20 Ω	12.5 Ω
电源管理方式	在线路初始化的时候划分电源级别	在线路初始化的时候划分为 4 个级别或者以 0.1W 为单

		位做动态调整
支持的线缆	3 类或 5 类双绞线	5 类双绞线

8.2 典型应用

典型应用	场景描述
PoE供电场景	PoE 交换机为场景中受电设备供电，数据交换功能

8.2.1 PoE 供电场景

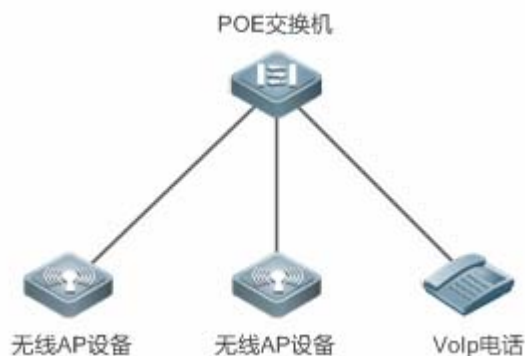
应用场景

在使用 PoE 交换机搭建的 PoE 系统中，PoE 交换机扮演 PoE 电源和 PSE 的组合。在提供正常的网络数据交换服务基础上，提供供电功能。系统中的主要用户受电设备，包括 WLAN 的 AP 设备，VoIP 电话等。

PoE 交换机提供电源管理功能，包括端口供电使能，供电优先级管理，端口过温保护，设备及端口供电状态查询等。

对于支持 PoE+ 的 PoE 交换机，支持与受电设备间建立 LLDP 联动，动态管理端口供电功率。

图 8-1



功能部属

- 在缺省情况下，PoE 交换机端口开启供电使能，检测到设备接入后，启动供电。
- 在 PoE 系统总供电功率不足的情况下，用户可手动配置端口供电优先级，确保制定端口优先上电。
- LLDP 联动功能默认关闭，若需要需手动开启。

8.3 功能详解

基本概念

▾ PoE 电源

PoE 电源为整个 PoE 系统供电，分为外置电源和内置电源两种类型。在我司的产品中，盒式 PoE 交换机一般有内部电源，部分产品也支持外部电源，外部电源称为 RPS。

▾ PSE

PSE (Power Sourcing Equipment , 供电设备)。PSE 在 PoE 端口的线路上寻找、检测 PD，对 PD 分级，并向其供电。当检测到 PD 拔出后，PSE 停止供电。

▾ PD

PD 是接受 PSE 供电的设备。分为标准 PD 和非标准 PD，标准 PD 是指符合 IEEE 802.3af 和 802.3at 标准的 PD 设备。常见的非标 PD 有特征电阻非标 PD、Cisco 预标准 PD、只支持信号线供电的 PD、只支持空闲线供电的 PD 等，我司产品采用信号线供电方式，因此不支持只支持空闲线供电的 PD。

PD 设备在接受 PoE 电源供电的同时，允许连接其他电源供电，进行电源冗余备份。

功能特性

功能特性	作用
PoE系统供电管理	管理系统供电策略，如供电模式等，同时支持对 PoE 系统供电的监控管理，如系统告警水线、trap 发送使能控制等。
PoE端口供电管理	管理 PoE 端口供电策略，如端口使能，供电优先级等。
PoE系统辅助功能	辅助系统供电管理功能，如系统的功率告警水线，端口的 PD 描述符配置等。
LLDP分级功能	PD 可以通过和 PSE 的 LLDP 报文交互，动态调整功率分配

8.3.1 PoE 系统供电管理

工作原理

PoE 系统供电管理支持：

用户可以切换供电模式(为设备连接的 PD 分配功率的方式)，PoE 交换机支持的供电管理模式有自动模式 (Auto mode)、节能模式 (Energy-saving mode) 和静态模式 (Static mode)。

自动模式下，根据检测出的端口 PD 分级类型来分配功率。设备对 0~4 类的 PD 设备是按以下关系来分配功率的：Class0 为 15.4W，Class1 为 4W，Class2 为 7W，Class3 为 15.4W，Class4 为 30W。在该模式下，如有一台分配为 Class3 的设

备,即使消耗的功率只有 11W, PoE 供电设备也会按照 15.4W 的功率为端口分配功率。自动模式为 PoE 交换机默认的供电管理模式。

节能模式下,设备按照 PD 设备实际的消耗来动态的调整功率分配。设置为该模式后, PoE 供电设备可以为更多的 PD 设备供电,但是也可能由于部分 PD 功率的波动影响到其他 PD 设备的供电情况。节能模式为 PoE 交换机的可选模式,如果交换机不支持该模式,在配置时会输出相应的提示信息。

当使用节能模式的时候, PoE 交换机按照 PD 设备的实际消耗功率来计算系统的消耗功率。如果存在 PD 设备在这种模式下消耗功率波动很大,就会导致 PoE 交换机负载过重损坏 PoE 设备。PoE 交换机提供了设置 PoE 系统保留功率的命令来保护 PoE 交换机一直有功率“富裕”,当前消耗的功率不会超过 PoE 交换机本身的极限。

静态模式下,按照用户的配置来分配功率,每个端口必须分配功率才能供电。如果电源的功率不足以分配全部端口,那么部分端口从小依次分配到电源功率分配完为止。静态模式为 PoE 交换机的可选模式,如果交换机不支持该模式,在配置时会输出相应的提示信息。

提供了热启动不间断供电功能,在系统重新启动的时候,已经处于供电状态的 PD 设备在 PoE 交换机热启动的过程中不会掉电。热启动完成后,系统回到配置文件中保存的状态。

相关配置

配置供电管理模式

缺省模式下,供电管理模式为 auto。

使用 `poe mode { auto | energy-saving }` 命令可以配置供电管理模式。由于不同的供电管理模式提供了不同的 PD 分配功率的方式,模式切换可能影响供电 PD 数。

。

配置系统的保留功率

缺省情况下,系统保留功率为 0。

使用 `poe reserve-power int` 命令配置系统的保留功率。在系统切换到节能模式时,保留功率配置生效。

热启动不间断供电功能

缺省情况下,系统关闭热启动不间断供电功能

使用 `poe uninterruptible-power` 命令设置热启动不间断供电功能,保存配置后生效。若系统热启动,启动过程中, PoE 系统为 PD 提供稳定供电。

8.3.2 PoE 端口供电管理

工作原理

PoE 端口供电管理支持：

用户可以使能或者关闭端口的 PoE 功能。

用户可以配置 PoE 交换机的端口供电优先级。优先级从高到低依次为：Critical、High 和 Low。在自动模式和节能模式下，高优先级的端口优先得到供电。在 PoE 交换机整机功率不足的时候，低优先级的端口先掉电。端口的默认优先级全部为低。

相同优先级的端口优先级按照端口号顺序排列，端口号小的优先级高，比如端口 1 的优先级就比端口 2 和 3 高。

相同优先级端口，新插入的端口，不抢占已经处于供电状态的端口；不同优先级的端口，高优先级端口可以抢占低优先级的端口。

用户可以配置交换机按照时间段管理某个端口的上下电。时间段设置通过全局配置模式下的 **time-range** 完成。

用户可以通过配置端口的最大功率，来限制端口的最大输出功率值。在自动模式和节能模式下，设置最大功率可以限制端口的最大输出功率，当端口的功率持续超过设置的最大功率 10 秒后，端口的供电停止，端口上的设备下电，log 提示端口功率过载，端口的 LED 灯显示为黄色。10 秒后，端口会再次被上电，如果端口的功率依然持续超过最大功率 10 秒以上，端口会再次被下电并不断循环这个过程。

PoE 目前普遍应用行业内标准 IEEE 802.3af 和 802.3at，在实际应用中 PD 设备形形色色，难免有不符合标准的 PoE 设备。锐捷交换机提供了 PoE 兼容命令，可以兼容部分非标准的 PoE 设备。

相关配置

▾ 端口供电使能控制

缺省情况下，端口打开 PoE 供电功能。

使用 **no poe enable** 命令可以关闭端口的 PoE 功能。

▾ 配置端口供电优先级

缺省情况下，端口供电优先级为 Low。

使用 **poe priority { low | high | critical }** 命令配置端口供电优先级。在功率不足情况下，高优先级可抢占低优先级，可能出现部分低优先级端口因功率不足而下电的情况。

▾ 配置端口的最大供电功率

缺省情况下，端口无最大功率限制。

使用 **poe max-power int** 命令配置端口的最大供电功率。在静态模式下，端口最大供电功率配置不生效。如配置端口最大供电功率为 15.4W，端口连接 PD 设备消耗功率大于配置最大功率的 1.1 倍，端口出现过流现象。

▾ 配置端口的定时断电功能

缺省情况下，端口无定时断电功能。

使用 **poe power-off time-range range-name** 命令配置端口的定时断电功能。在 time-range 时钟周期内，PoE 不为连接的 PD 供电。

▾ 配置非标准 PD 设备兼容功能

缺省情况下，端口不兼容非标准 PD 设备。

使用 **poe legacy** 命令配置使能非标准 PD 设备兼容功能。

8.3.3 PoE 供电辅助功能

工作原理

PoE 标准 MIB , RFC3621 中提供了 `pethMainPseUsageThreshold` 项来设置系统的功率告警水位。

PoE 交换机也提供了 CLI 设置项来设置这个值。设置这个 CLI , 功能和配置 `pethMainPseUsageThreshold` MIB 项相同 , 设置系统的功率告警水位。如果在 MIB 上同时开启了 `pethNotificationControlEnable` 开关 , MIB 就可以收到告警功率的通告。

在实际应用中需要控制系统在功率变化和端口上下电时是否进行发送 trap 通告。PoE 标准 MIB RFC3621 中提供了 `pethNotificationControlEnable` 项来设置是否进行发送上述 trap 通告。

在实际应用中常常需要记录指定 PoE 端口上接入的 PD 名字 ,RFC3621 中提供了 `pethPsePortType` 项来设置端口的 PD 描述。

PoE 交换机也提供了 CLI 设置项来设置这个值。

相关配置

配置系统的功率告警水位

缺省情况下 , 系统功率告警水位为 99。

使用 **poe warning-power int** 命令配置系统的功率告警水位。

配置系统的 trap 发送开关

缺省情况下 , 系统关闭 trap 发送开关。

使用 **poe notification-control enable** 命令配置系统的 trap 发送开关。

配置端口的 PD 描述符

缺省情况下 , 端口无 PD 描述符信息。

使用 **poe pd-description pd-name** 命令配置端口的 PD 描述符。

8.3.4 LLDP 分级功能

工作原理

按照 IEEE 802.3at 标准 ,支持 802.3at 的 PD 设备必须既支持硬件二次分级 (标准中称为 2-Event Physical Layer classification) 也支持 LLDP 分级 (标准中称为 : Data Link Layer classification) ——PD 可以通过和 PSE 的 LLDP 报文交互 , 标识自身是 Class 4 设备的 Type 类型。PSE 供电设备只需要支持其中一种。锐捷交换机支持 LLDP 分级功能。

Class 4 Type2 的 PD 设备插入 PoE 交换机以后，首先进行检测和分级，然后 PD 设备得到供电。PoE 交换机默认识别设备为 Type 1 设备，并提供最大 13W 的功率。在进行 LLDP 分级以后，PD 设备可以被识别为 Type2 设备，如果 PoE 交换机功率足够，那么 PD 可以得到最大 25.5W 的功率。如果 PoE 交换机已经无法分配更多的功率，那么 PD 设备会不断的发送 LLDP 功率请求报文，请求功率分配。

每个级别的 PD 能够请求的最大功率为：

分级	类型	最大功率(W)	供电管理分配功率(W)
Class 0	Type 1	13	15.4
Class 1	Type 1	3.9	4
Class 2	Type 1	6.5	7
Class 3	Type 1	13	15.4
Class 4	Type 1	13	15.4
Class 4	Type 2	25.5	30

因为 PSE 提供的功率需要扣掉线缆损耗，所以供电管理分配的功率比 PD 请求的最大功率略大。

该功能默认开启且只在供电管理模式为自动模式时生效。

相关配置


配置 LLDP 分级功能

缺省情况下，系统关闭 LLDP 分级功能。

使用 `poe class-ldp enable` 命令配置使能 LLDP 分级功能。

8.4 配置详解

配置项	配置建议 & 相关命令	
配置PoE系统供电	 必须配置，管理系统的 PoE 供电	
	<code>poe mode</code>	配置供电管理模式
	<code>poe reserve-power</code>	配置系统的保留功率
	<code>poe uninterruptible-power</code>	热启动不间断供电功能
配置PoE端口供电	 必须配置，管理具体端口的 PoE 供电	
	<code>poe enable</code>	端口供电使能控制
	<code>poe priority</code>	配置端口的供电优先级
	<code>poe max-power</code>	配置端口的最大功率
	<code>poe power-off time-range name</code>	配置端口的定时断电功能
	<code>poe legacy</code>	非标准 PD 设备兼容功能
配置PoE供电辅助功能	 可选配置，方便用户对 PoE 系统的管理	
	<code>poe warning-power</code>	配置系统的功率告警水线

	po notification-control enable	配置系统的 trap 发送开关
	po pd-description	配置端口的 PD 描述符
使能LLDP分级功能	 可选配置，管理 PoE 设备与 PD 间的 LLDP 分级功能	
	po class-ldp enable	使用 LLDP 分级功能

8.4.1 配置 PoE 系统供电

配置效果

- 配置 mode，改变 PD 设备功率分配方式。auto 模式下根据 PD 等级分配，energy-saving 模式下根据实际消耗功率分配。
- 配置 reserve-power，在节能模式下，该部分功率不对外供出使用。
- 配置 uninterruptible-power，热重起过程中，保持 PoE 供电功能。

注意事项

配置方法

配置供电管理模式

- 必须配置，默认为 auto 模式。
- 供电管理模式切换，所有 PoE 端口下电，端口按照新的供电管理模式重新上电
- 若希望 PoE 交换机可以给更多的端口供电，可采用 energy-saving 模式，端口分配功率根据实际消耗功率计算。
- 支持全局配置以及单端口独立配置。

配置系统的保留功率

- 必须配置，仅在 energy-saving 模式下生效。
- 设置系统保留功率命令，只有在当前 PoE 交换机的供电管理模式为节能模式的时候才发生作用。
- 在节能模式设置保留功率，可能会导致已上电的端口下电。
- 支持全局配置。

热启动不间断供电功能

- 可选配置，默认关闭。
- 在实际应用中如果需要重启交换机，比如升级 PoE 交换机管理软件后重新启动 PoE 交换机，可是这个时候 PoE 交换机上有许多 PD 设备正在正常供电中，如果直接重启，会造成正在工作的 PD 设备下电然后再上电，PD 设备会有一段时间中断工作。

- 开启或关闭该功能后必须保存配置才能保证在下一次的复位中生效。如果用户忘记了保存配置，或者在保存配置后又改动了 PoE 配置，系统将会提示用户保存配置。
- 支持全局配置。

检验方法

通过查看 PoE 系统的供电状态，检查配置是否正确，配置是否对供电生效。

相关命令

配置供电管理模式

- 【命令格式】 **poe mode { auto | energy-saving }**
- 【参数说明】 { auto | energy-saving }：自动模式、节能模式
- 【命令模式】 全局模式下
- 【使用指导】 -

配置系统的保留功率

- 【命令格式】 **poe reserve-power int**
- 【参数说明】 *int*：保留功率的百分比 <0~50>
- 【命令模式】 全局模式下
- 【使用指导】 -

热启动不间断供电功能

- 【命令格式】 **poe uninterruptible-power**
- 【参数说明】 -
- 【命令模式】 全局模式下
- 【使用指导】 -

配置举例

配置系统供电管理策略

- 【网络环境】
 - 接入的 PD 设备，消耗功率都比较低，但是接入数量大，满端口接入。
 - 要求热启动不间断。
- 【配置方法】
 - 切换模式为 energy-saving 模式。
 - 配置系统保留功率 20%。
 - 配置支持热启动不间断供电功能。

```
Ruijie# configure terminal
Ruijie(config)# poe mode energy-saving
Ruijie(config)# poe reserve-power 20
Ruijie(config)# poe uninterruptible-power
```

```
Ruijie(config)# exit
```

```
Ruijie# write
```

【检验方法】 通过 **show poe powersupply** 可以查看到配置信息以及供电信息。

```
Ruijie#show poe powersupply
Device member           : 1
Power management        : energy-saving
PSE total power         : 1000W
PSE total power consumption : 369.6W
PSE total remain power  : 630.4W
PSE total powered port  : 0
PSE disconnect mode     : dc
PSE reserve power       : 20%
PSE warning power       : 99%
PSE class lldp          : disable
    PSE member           : 1
    PSE Power Enabled    : enable
    PSE max power        : 369.6W
    PSE priority         : low
    PSE alloc power      : 369.6W
    PSE available power  : 295.7W
    PSE total power consumption : 0 W
    PSE total remain power : 295.7W
    PSE peak power       : 0 W
    PSE average power    : 0 W
    PSE powered port     : 0
```

常见错误

8.4.2 配置 PoE 端口供电

配置效果

- 配置 time-range，在 time-range 时间内，端口下电。
- 配置端口 priority，在功率不足情况下，高优先级端口可抢占低优先级端口功率，同优先级不抢占。
- 配置 legacy，兼容支持非标准 PD 设备。

- 配置端口 max-power，若端口消耗功率大于 max-power 的 1.1 倍，端口下电，进入 10 秒的惩罚时间，后重新启动上电流程。
- 配置端口 alloc-power，在 static 模式下，根据 alloc-power 分配端口功率。

注意事项

配置方法

▾ 端口供电使能控制

- 必须配置，默认打开。
- 在打开或关闭一个端口的 PoE 功能时，需配置端口供电使能控制。
- 缺省情况下，接入汇聚交换机端口的 PoE 功能为开启状态，核心交换机的 PoE 功能为关闭状态。
- 如果使用 **interface range** 命令批量配置端口的 PoE 功能，由于 range 命令是一个接一个端口配置的，一个端口 PoE 功能的开启或关闭，会影响到设备全局的供电管理。所以可能在配置的过程中会出现端口上电又下电的现象，这属于正常现象。
- 支持单端口独立配置

▾ 配置端口的定时断电功能

- 可选配置。
- 在端口使能供电的情况下，配置 time-range，按照 range-name 设定的时间段管理某个端口的上下电。
- PoE 端口的定时供电功能时间精度为 1 分钟 30 秒。
- PoE 端口的定时断电功能，“range-name”，即时间范围的名字最长为 32 个字符。
- 支持单端口独立配置。

▾ 配置端口的供电优先级

- 必须配置，默认端口 low 优先级。
- 在功率不足的场景中，若考虑为部分端口优先稳定供电，可通过配置端口优先级实现。
- 该命令在供电管理模式为静态模式的时候是没有意义的，因为在静态模式下端口的功率按照用户配置强制分配，交换机不能做自动选择，所以该命令在静态模式下不生效。如果在切换到静态模式前端口已经配置了端口的优先级，那么该命令会被显示出来，可是不生效。
- 支持全局配置以及单端口独立配置。

▾ 非标准 PD 设备兼容功能

- 可选配置，默认不支持。
- 若接入的 PD 设备不符合 PoE 标准，可开启支持非标准 PD 设备兼容功能，为其供电。

- 在没有接入 PD 设备的端口上使用这个命令，可能导致对端设备被错误的上电烧毁，请确保端口在接入 PD 设备的时候使用该命令。
- 不符合标准的 PoE 设备，Class 分级统一显示为 0。
- 如果不设置这个命令，插入非标准的 PD 设备，非标准的 PD 设备不会被上电，系统不会有任何提示信息。
- 支持单端口独立配置。

配置端口的最大功率

- 可选配置，默认端口无最大功率限制。
- 该命令只在自动模式和节能模式下生效。
- 将 max-power 设置为 0，端口下电，并不再上电。
- 只支持 802.3af 的 PoE 交换机，max-power 的配置范围为<0-15.4>。
- 配置端口最大功率，其最大消耗功率不超过配置功率的 1.1 倍，降低因单端口消耗功率过高对功率管理的影响。
- 支持单端口独立配置。

检验方法

通过查看 PoE 端口的 PoE 信息，检查配置是否正确，配置是否对供电生效。

相关命令

端口供电使能控制

- 【命令格式】 **poe enable**
- 【参数说明】 -
- 【命令模式】 接口模式下
- 【使用指导】 -

配置端口的定时断电功能

- 【命令格式】 **poe power-off time-range name**
- 【参数说明】 *name*: time-range 描述符
- 【命令模式】 接口模式下
- 【使用指导】 -

配置端口供电优先级

- 【命令格式】 **poe priority { low | high | critical }**
- 【参数说明】 { low | high | critical } : 优先级，有 Low 、 High、 Critical 可以选择
- 【命令模式】 接口模式下
- 【使用指导】 -

配置非标准 PD 设备兼容功能

- 【命令格式】 **poeg legacy**
- 【参数说明】 -
- 【命令模式】 接口模式下
- 【使用指导】 -

配置端口的最大功率

- 【命令格式】 **poeg max-power int**
- 【参数说明】 *int*：最大功率，单位为 W，范围为<0-30>，在只支持 802.3af 的系统上范围为<0-15.4>
- 【命令模式】 接口模式下
- 【使用指导】 -

配置举例

配置端口供电管理策略

- 【网络环境】
- 端口 g0/1 要求稳定供电，尽量不受网络环境影响。
 - 端口在每日 8:00 到 12:00 时间段下电，其他时间上电。
 - 端口最大供电功率不超过 17W。
- 【配置方法】
- 配置 g0/1 口优先级为 critical。
 - 配置 time-range，并关联 PoE 的端口 time-range 配置。
 - 配置 g0/1 端口最大功率为 15.4W。

```
Ruijie# configure terminal
Ruijie(config)# time-range poe-time
Ruijie(config-time-range)# periodic daily 8:00 to 12:00
Ruijie(config-time-range)# exit
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# poe power-off time-range poe-time
Ruijie(config-if)# poe priority critical
Ruijie(config-if)# poe max-power 15.4
```

- 【检验方法】 通过 **show poeg interface gigabitEthernet 0/1** 可以查看到配置信息以及供电信息。

```
Ruijie#show poeg interface gigabitEthernet 0/1
Interface           : gi0/1
Power enabled       : enable
Power status        : on
Max power           : 15.4W
Allocate power      : N/A
Current power       : 14.8 W
Average power       : 14.8 W
Peak power          : 14.8 W
LLDP requested power : 0 W
LLDP allocated power : 0 W
Voltage             : 53.5 V
```

```
Current          : 278 mA
PD class         : 4
Trouble cause    : None
Priority         : critical
Legacy          : off
Power-off time-range : poe-time
Power management : auto
```

常见错误

-

8.4.3 配置 PoE 供电辅助功能

配置效果

- 配置 warning-power，当系统使用功率超出告警水线时，告警提示。
- 配置 notification-control，控制系统在功率变化和端口上下电时是否进行发送 trap 通告。
- 配置 pd-description，帮助识别具体端口 PD 设备。

注意事项

-

配置方法

▾ 配置系统的功率告警水线

- 必须配置，默认为 99，与 RFC3621 MIB 中规定的一致。
- 配置系统的功率告警水线，在系统使用功率超出水线时，会有告警信息提示。
- 如果通过 MIB pethMainPseUsageThreshold 配置系统的功率告警水线，那么这个 CLI 也会被配置。
- 支持全局配置。

▾ 配置系统的 trap 发送开关

- 必须配置，默认关闭。
- 打开 trap 发送开关，打开和关闭系统告警功率通告和端口上下电通告等会发送 trap 信息。
- 此 CLI 命令只能控制 RFC3621 中定义的 trap 发送，对于非 RFC3621 中定义的 trap 发送控制不生效。

- 打开RFC3621中定义的trap发送功能时,当告警功率从小于或者等于系统功率的状态变为大于系统功率的时候通告一次,如果后续告警功率一直大于系统功率,则不再发送 trap;当告警功率从大于或者等于系统功率的状态变为小于系统功率的时候通告一次,如果后续告警功率一直小于系统功率,则不再发送 trap。
- 支持全局配置以及单端口独立配置。

配置端口的 PD 描述符

- 可选配置,默认端口无 PD 描述符。
- 配置端口的 PD 描述符,方便于管理者识别端口上的 PD 设备。
- 如果通过 MIB pethPsePortType 配置端口描述符,那么这个 CLI 也会被配置。
- 支持单端口独立配置。

检验方法

通过检测系统使用功率在告警功率水线上波动时是否有告警信息输出,检测告警功率配置是否生效。

PoE 设备连接 SNMP 服务器,操作端口上下电,查看服务器是否接收到相应的 trap 信息,检测 trap 配置是否生效。

通过查看端口的 PoE 信息,可确认端口的 PD 描述符配置是否正确。

相关命令

配置系统的功率告警水线

- 【命令格式】 **poe warnig-power int**
- 【参数说明】 *int*: 告警功率百分比,范围为<0-99>
- 【命令模式】 全局模式下
- 【使用指导】 -

配置系统的 trap 发送开关

- 【命令格式】 **poe notification-control enable**
- 【参数说明】 -
- 【命令模式】 全局模式下
- 【使用指导】 -

配置端口的 PD 描述符

- 【命令格式】 **poe pd-description pd-name**
- 【参数说明】 *pd-name*: PD 描述符名字,参数为字符串,最长支持 32 个字符
- 【命令模式】 接口模式下
- 【使用指导】 -

配置举例

配置系统供电管理策略

- 【网络环境】
- 系统功率超过 80%时，需要有告警信息提示。
 - 在端口上、下电时，需要发送 trap 通告信息。
 - 可识别端口连接的 PD 设备。

- 【配置方法】
- 配置系统告警功率水线为 80%。
 - 配置使能系统 trap 发送开关。
 - 配置端口 g0/1 的 PD 描述符为 ap220。

```
Ruijie# configure terminal
Ruijie(config)# poe poe warnig-power 80
Ruijie(config)# poe notification-control enable
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# poe pd-description ap220
```

- 【检验方法】 通过 **show running-config** 可以查看到配置信息以及供电信息。

常见错误

8.4.4 使能 LLDP 分级功能

配置效果

- 配置 class-lldp，支持 PoE 交换机与 PD 设备间通过 LLDP 协议，协商供电等级以及供电功率。

注意事项

配置方法

使用 LLDP 分级功能

- 可选配置，默认关闭。
- 系统切换在 auto 模式；全局配置使能 LLDP 分级功能；同时确认端口上无 max-power 配置。
- 如果端口配置了 Max-power 命令限制最大功率，那么这个端口上的 LLDP 功率调整功能失效。
- PoE 交换机不允许 PD 设备通过 LLDP 报文请求调整自身的优先级，端口的优先级由 PoE 交换机配置统一管理。
- 支持端口独立配置。

检验方法

通过查看端口的 PoE 信息中的“PD class”信息，查看端口是否处于与 PD 设备的 LLDP 联动过程中。

相关命令

▾ 使用 LLDP 分级功能

- 【命令格式】 **poe class-lldp enable**
- 【参数说明】 -
- 【命令模式】 全局模式下
- 【使用指导】 -

配置举例

▾ 配置端口供电管理策略

【网络环境】 PD 等级为 4 的设备建立与 PSE 之间的联动功能。

【配置方法】 配置使能 LLDP 分级功能。

```
Ruijie# configure terminal
Ruijie(config)# poe class-lldp enable
```

【检验方法】 通过 **show poe interface gigabitEthernet 0/1** 可以查看到配置信息以及供电信息。

```
Ruijie#show poe interface gigabitEthernet 0/1
Interface           : gi0/1
Power enabled       : enable
Power status        : on
Max power           : 15.4W
Allocate power      : N/A
Current power       : 14.8 W
Average power       : 14.8 W
Peak power          : 14.8 W
LLDP requested power : 0 W
LLDP allocated power : 0 W
Voltage             : 53.5 V
Current             : 278 mA
PD class            : 4(Type1)
Trouble cause       : None
Priority             : critical
Legacy              : off
Power-off time-range : poe-time
Power management    : auto
```

常见错误

8.5 监视与维护

清除各类信息

查看运行情况

作用	命令
查看指定端口的 PoE 配置和状态信息	show poe interface
查看所有端口的 PoE 状态或配置	show poe interfaces
查看当前 PoE 系统的供电状态	show poe powersupply

查看调试信息

9 PKG_MGMT

9.1 概述

Package Management 是 RGOS 系统的包管理及升级模块，负责对设备内各个组件安装、升降级、查询、维护，其中升级是主要功能。通过对设备的软件进行升级，用户可以在系统上安装更加稳定的或含有更多的特性的软件版本，RGOS 系统采用模块化的构成方式，系统既可以进行整体升级和子系统的升级，也可以进行各个功能包的独立升级。

- ✔ 本文描述的组件升级涵盖了设备的组件升级，且本文只针对 11.0 以后的各项目平台，不涉及 11.0 以前项目升级到 11.0 以后项目。

协议规范

无

9.2 典型应用

典型应用	场景描述
升降级子系统组件	升降级设备的 boot, kernel, rootfs 等子系统组件。
升降级单个功能组件包	升降级设备单个功能组件包。

9.2.1 升降级子系统组件

应用场景

升级子系统组件包，完成升级后设备内原先的系统软件全部被更新，整体软件功能得到增强。通常盒式设备子系统组件包称为 main 包。

该升级方式的主要特点是：升级完成后设备内所有软件都将更新，所有已知软件 bug 都将得到完整解决，但升级过程较长。

功能部署

盒式设备升级前可以将 main 包放在 TFTP 服务器程序的根目录下，通过网络下载设备内，再执行本地升级命令完成升级。

9.2.2 升降级单个功能组件包

应用场景

设备软件由若干功能组件组成，每个功能组件都是一个独立的功能模块。升级独立的功能组件包，在完成升级后仅该安装包对应功能模块的缺陷得到了修订、或者功能组件得到了增强，其它功能组件保持不变。

该升级场景的特点是：功能组件包通常较小，升级速度较快，升级完成后仅对应的功能模块得到改善，其它功能模块保持不变。

功能部署

升级功能组件包前，可以将其存放在 TFTP 服务器的根目录，通过网络下载安装到本地完成升级。

9.3 功能详解

基本概念

▾ 子系统

子系统以映像的方式存储于设备，RGOS 的子系统包括：


- boot：设备上电启动首先加载 boot 运行，它负责设备的基础初始化，加载并运行系统映像。
- kernel：它是系统的 OS 核心部分，负责屏蔽系统的硬件构成、给应用程序提供抽象的运行环境。
- rootfs：它是系统中应用程序的集合。

▾ main 安装包

盒式设备子系统升降级时往往使用 main 安装包，该包是 boot，kernel 和 rootfs 子系统的合并包。该包可以用来完成系统整体升降级。

▾ RGOS 的功能组件包

RGOS 的功能组件包则是指实现某个功能的集合，在设备出厂时，所有已支持的功能均已包含在 rootfs 子系统中，通过升级单个功能组件包可以只更新系统内特定功能或特性。

 本文中的“安装包”均指包含子系统或功能模块的安装文件。

功能特性

功能特性	作用
子系统组件升降级及管理	升降级子系统。查询当前设备可用的子系统组件，并激活选定的子系统组件。
功能组件升降级	升降级功能组件。查询设备中存在的功能组件包及其版本和安装信息。

9.3.1 子系统组件升降级及管理

子系统的升降级就是将安装包内的子系统组件替换设备内的子系统组件，达到软件功能更新的目的。因为存在子系统冗余设计，所以升降级时往往并不是直接覆盖设备内当前正在使用的子系统，而是在设备内新增子系统然后再激活新增子系统。

工作原理

↘ 升降级

各子系统在设备内存在的形式各有不同，因此对子系统的升降级方式也各有差别：

- boot：该子系统一般以映像形式存在于 norflash 设备内，所以该子系统的升降级就是将映像写入 norflash 设备。
- kernel：该子系统以文件形式存在于特定分区，所以该子系统的升降级就是文件的写入。
- rootfs：该子系统一般以映像形式存在于 nandflash 设备内，所以该子系统的升降级就是将映像写入 nandflash 设备。

↘ 管理

查询当前有哪些子系统组件可用，之后依据实际需求，有选择性的加载子系统组件。

各子系统组件都包含冗余设计，在升降级过程中：

- boot：始终存在主、从两个 boot，升级只涉及主 boot，从 boot 始终冗余。
- kernel：至少存在一个冗余备份，若空间足够可存在多个冗余。
- rootfs：始终存在一个冗余备份。

对于 boot 组件因为较为特殊，并不将该组件纳入子系统管理的范畴。在升级 kernel 或 rootfs 子系统组件时升降级模块总是在配置文件记录当前使用的子系统组件和冗余的子系统组件以及各种版本管理信息。

相关配置

↘ 升级

- 将升级文件存放在设备本地后，使用 **upgrade** 命令升级。

9.3.2 功能组件升降级及管理

工作原理

功能组件升级的原理实际上就是组件文件的替换过程，即包内的组件文件替换设备中的组件文件。

功能组件的管理是利用数据库记录功能组件的信息。安装组件，显示组件信息，卸载组件实际上就是数据库添加，查询，删除的结果。

相关配置

↘ 升级

- 将升级文件存放在设备本地后，使用 **upgrade** 命令升级。

9.4 配置详解

配置项	配置建议 & 相关命令	
安装包升降级	 基本功能，用于子系统组件包，功能组件包的安装，升降级。	
	<code>upgrade url [force]</code>	<i>url</i> 为安装包存放的本地路径。该命令用于升级设备内存放的安装包。
	<code>upgrade download tftp://path [force]</code>	<i>path</i> 为 tftp 服务器上安装包的路径，该命令自动从服务器上下载安装包，并自动升级

9.4.1 安装包升降级

配置效果

可用安装包包括板卡设备对应的 main 安装包，各功能组件包。

- 升级设备对应的 main 安装包，完成升级后该板卡设备内原先的系统软件全部被更新，整体软件功能得到增强。
- 升级独立的功能组件包，在完成升级后仅该安装包对应功能模块的 bug 得到了修订，功能组件得到了增强，其它功能组件保持不变。

 通常发布 main 包来升级盒式设备。

注意事项

-

配置方法

📌 升级板卡设备对应的 main 安装包

- 可选配置。设备内原先的系统软件全部需要被更新时，选择此配置项。
- 升级前需要将安装包下载到设备本地，使用 `upgrade` 命令升级。

 通常发布 main 包来升级盒式设备

📌 升级各功能组件包

- 可选配置。如果仅需要对某功能模块的缺陷进行修复，或增强该功能模块的性能的话，选择此配置项。
- 升级前需要将安装包下载到设备本地，使用 `upgrade` 命令升级。

检验方法

- 完成升级功能组件后可执行 `show component` 命令查看是否升级成功。

相关命令

升级安装包

【命令格式】 **upgrade url [force]**

【参数说明】 *url* : *url* 为安装包存放的本地路径。该命令用于升级设备内存放的安装包。

force : 表示强制升级

【命令模式】 特权模式

【使用指导】

i 该命令支持各子系统组件安装包, 功能组件安装包。使用该命令前, 先使用 **copy** 命令将功能包拷入设备文件系统内。

当使用该命令、不指定范围参数时, 升级功能将按照自动同步配置, 对匹配到的系统部件进行升级。

【命令格式】 **upgrade download tftp:/path [force]**

【参数说明】 *path* : *path* 为 tftp 服务器上安装包的路径, 该命令自动从服务器上下载安装包, 并自动升级。

force : 表示强制升级。

【命令模式】 特权模式

【使用指导】 该命令支持各子系统组件安装包, 功能组件安装包。使用该命令自动完成安装文件拷贝操作并升级。

显示已安装的功能组件

【命令格式】 **show component [component_name]**

【参数说明】 [*component_name*] 组件名称。

当不存在此参数值时: 命令用于显示设备中所有已安装的组件及各组件的基本信息。

当存在此参数值时: 命令用于显示对应组件的详细信息, 并校验组件内容是否完整, 检测该组件能否正常工作。

【命令模式】 特权模式

【使用指导】 -

配置举例

盒式设备子系统安装包升级举例

【网络环境】 升级前必须将安装包拷入设备内, 升级模块提供以下几种解决方案。

- 用户首先使用 **copy tftp**, **copy xmodem** 等文件系统命令将服务器上的安装包拷入设备文件系统, 再使用 **upgrade url** 升级本地文件系统内的安装包;
- 直接使用 **upgrade download tftp://path** 命令升级 tftp 服务器端存放的安装包文件;

【配置方法】

- 执行升级命令
- 完成子系统升级后设备重启生效

```
Ruijie# upgrade download tftp://192.168.201.98/eg1000m_main_1.0.0.0f328e91.bin
Accessing tftp://192.168.201.98/eg1000m_main_1.0.0.0f328e91.bin..
```

```

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!
Transmission finished, file length 21525888 bytes.
Upgrade processing is 10%
Upgrade processing is 60%
Upgrade processing is 90%

Upgrade info [OK]
    Kernel version[2.6.32.91f9d21->2.6.32.9f8b56f]
    Rootfs version[1.0.0.2ad02537->1.0.0.1bcc12e8]
Upgrade processing is 100%
Reload system to take effect!
Reload system?(Y/N)y
Restarting system.

```

- 【检验方法】
- 查看当前设备运行的版本信息，若版本信息发生变换说明升级成功

```

Ruijie#show version detail
System description      : EG1000m
System start time      : 2013-10-19 02:25:28
System uptime          : 0:00:00:50
System hardware version : 1.00
System software version : eg1000m_RGOS11.0(1C2) Release(20131022)
System boot version    : 1.0.0.e7a1451
System core version    : 2.6.32.9f8b56f
System main version    : 1.0.0.1bcc12e8
System boot build      : unknown
System core build      : 2013/10/22 04:54:03
System main build      : 2013/10/22 05:33:38

```

▾ 盒式设备功能包升级举例

【网络环境】 升级前必须将安装包拷入设备内，升级模块提供以下几种解决方案。

- 用户首先使用 **copy tftp**，**copy xmodem** 等文件系统命令将服务器上的安装包拷入设备文件系统，再使用 **upgrade url** 升级本地文件系统内的安装包；
- 直接使用 **upgrade download tftp://path** 命令升级 tftp 服务器端存放的安装包文件；
-

【配置方法】

- 执行升级命令
- 依照升级后的提示确定是否需要设备重启

- 【检验方法】
- 查看当前设备功能组件版本信息，若版本信息发生变换说明升级成功

```
Ruijie# show component
Package :sysmonit
  Version:1.0.1.23cd34aa      Build time: Wed Dec  7 00:58:56 2011
  Size:12877    Install time :Wed Mar 5 14:23:12 2012
  Description:this is a system monit package
  Required packages: None

-----

package:bridge
  Version: 2.3.1.1252ea      Build time: Wed Dec  7 00:54:56 2011
  Size:26945    Install time : Wed Mar 19:23:15 2012
  Description:this is a bridge package
  Required packages: None
```

常见错误

若升级过程中出现错误，升级模块会加以提示例如：

```
Upgrade info [ERR]
  Reason:creat config file err(217)
```

常见错误提示有以下几种：

- 安装包无效：可能的原因是该安装包已经被损坏或者根本不是一个安装包。该错误的处理方式要求用户重新获取安装包，再执行升级操作。
- 设备不支持安装包：可能的原因是误用了其它设备的安装包。该错误的处理方式要求用户重新获取并核对安装包后在执行升级操作。

9.5 监视与维护

清除各类信息

-

查看运行情况

作用	命令
显示当前设备已安装所有组件及各组件信息。	show component [<i>cprmonent_name</i>]



配置指南-以太网交换

本分册介绍配置指南相关内容，包括以下章节：

1. 接口
2. MAC 地址
3. Aggregate Port
4. VLAN
5. MSTP
6. LLDP

1 接口

1.1 概述

接口是网络设备上能够实现数据交换功能的重要部件。我司网络设备上支持两种类型的接口：物理接口和逻辑接口。物理接口意味着该接口在设备上有对应的、实际存在的硬件接口，如：百兆以太网接口、千兆以太网接口等。逻辑接口意味着该接口在路由器上没有对应的、实际存在的硬件接口，逻辑接口可以与物理接口关联，也可以独立于物理接口存在，如：Loopback 接口和 Tunnel 接口等等。实际上对于网络协议而言，无论是物理接口还是逻辑接口，都是一样对待的。

i 下文仅介绍接口的相关内容。

协议规范

- 无。

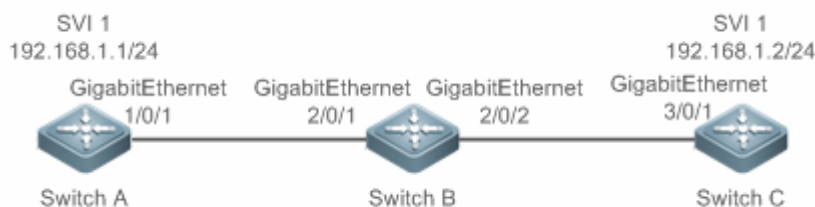
1.2 典型应用

典型应用	场景描述
以太网物理接口实现二层数据交换	通过二层以太网物理接口实现网络设备的二层数据通信。
以太网物理接口实现三层数据路由	通过三层以太网物理接口实现网络设备的三层数据通信。

1.2.1 以太网物理接口二层数据交换

应用场景

图 1-1



上图中，三台交换机设备 Switch A、Switch B 和 Switch C 组成了一个简单的二层数据交换网络。

【注释】

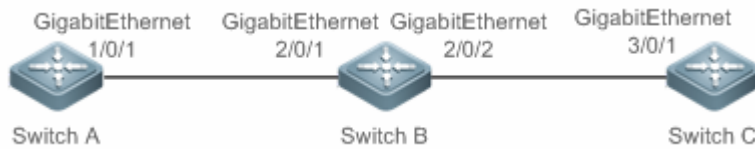
功能部属

- Switch A 和 Switch B 分别通过千兆以太网物理接口 GigabitEthernet 1/0/1 和 GigabitEthernet 2/0/1 进行相连。
- Switch B 和 Switch C 分别通过千兆以太网物理接口 GigabitEthernet 2/0/2 和 GigabitEthernet 3/0/1 进行相连。
- 将接口 GigabitEthernet 1/0/1、GigabitEthernet 2/0/1、GigabitEthernet 2/0/2 和 GigabitEthernet 3/0/1 配置为 Trunk 口。
- 分别在 Switch A 和 Switch C 上创建一个交换虚拟接口(Switch Virtual Interface, SVI) SVI 1，并给 SVI 1 接口配置相同网段的 IP 地址，其中，Switch A 的 SVI 1 接口的 IP 地址配置为 192.168.1.1/24，Switch C 的 SVI 1 接口的 IP 地址配置为 192.168.1.2/24。
- 在 Switch A 和 Switch C 上分别执行 ping 192.168.1.2 和 ping 192.168.1.1 操作，可以实现设备 B 上的二层数据交换功能。

1.2.2 以太网物理接口三层路由通信

应用场景

图 1-2



上图中，三台交换机设备 Switch A、Switch B 和 Switch C 组成了一个简单的三层数据通信网络。

【注释】

功能部属

- Switch A 和 Switch B 分别通过千兆以太网物理接口 GigabitEthernet 1/0/1 和 GigabitEthernet 2/0/1 进行相连。
- Switch B 和 Switch C 分别通过千兆以太网物理接口 GigabitEthernet 2/0/2 和 GigabitEthernet 3/0/1 进行相连。
- 将接口 GigabitEthernet 1/0/1、GigabitEthernet 2/0/1、GigabitEthernet 2/0/2 和 GigabitEthernet 3/0/1 配置为三层路由接口。
- 分别给 GigabitEthernet 1/0/1 和 GigabitEthernet 2/0/1 配置相同网段的 IP 地址，其中，GigabitEthernet 1/0/1 的 IP 地址配置为 192.168.1.1/24，GigabitEthernet 2/0/1 的 IP 地址配置为 192.168.1.2/24。
- 分别给 GigabitEthernet 2/0/2 和 GigabitEthernet 3/0/1 配置相同网段的 IP 地址，其中，GigabitEthernet 2/0/2 的 IP 地址配置为 192.168.2.1/24，GigabitEthernet 3/0/1 的 IP 地址配置为 192.168.2.2/24。
- 在 Switch C 上配置一条静态路由表项使其能够三层直通 192.168.1.0/24 网段。
- 在 Switch A 和 Switch C 上分别执行 ping 192.168.2.2 和 ping 192.168.1.1 操作，可以实现设备 B 上的三层路由通信功能。

1.3 功能详解

基本概念

接口类型分类

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)
 - FC 接口(某些数据中心产品支持)
1. 常见的二层接口可分为以下几种类型：
 - [交换端口 \(Switch Port \)](#)
 - [二层聚合端口 \(L2 Aggregate Port \)](#)
 2. 常见的三层接口可分为以下几种类型
 - 路由端口 (Routed Port)
 - 三层聚合端口 (L3 Aggregate Port)
 - SVI 口

- Loopback 接口

3. FC 接口类型

- FC 接口
- FC 聚合口

↘ 交换端口

交换端口由设备上的单个物理端口构成，只有二层交换功能。交换端口被用于管理物理接口和与之相关的第二层协议。

↘ 二层聚合端口

聚合端口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聚合端口（以下简称聚合端口）。

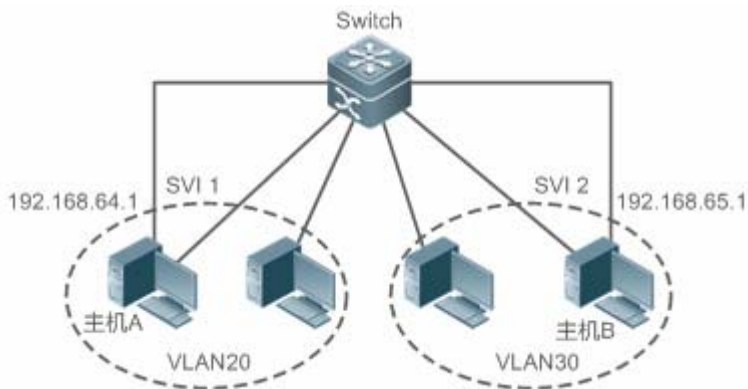
对于二层交换来说聚合端口就好像一个高带宽的交换端口，它可以把多个端口的带宽叠加起来使用，扩展了链路带宽。此外，通过二层聚合端口发送的帧还将在二层聚合端口的成员端口上进行流量平衡，如果聚合端口中的一条成员链路失效，二层聚合端口会自动将这个链路上的流量转移到其他有效的成员链路上，提高了连接的可靠性。

↘ SVI 口

SVI 接口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。用户也可以创建 SVI 接口为一个网关接口，就相当于是对应各个 VLAN 的虚拟接口，可用于三层设备中跨 VLAN 之间的路由。创建一个交换虚拟接口很简单，用户可通过 `interface vlan` 接口配置命令来创建 SVI 接口，然后给交换虚拟接口分配 IP 地址来建立 VLAN 之间的路由。

如图所示，VLAN 20 的主机可直接互相通讯，无需通过三层设备的路由，若 VLAN 20 内的主机 A 想和 VLAN 30 内的主机 B 通讯必须通过 VLAN 20 对应的 SVI 1 和 VLAN30 对应的 SVI 2 才能实现。

图 1-3



↘ 路由端口

在三层设备上，可以把单个物理端口设置为路由端口，作为三层交换的网关接口。一个路由端口与一个特定的 VLAN 没有关系，而是作为一个访问端口。路由端口不具备二层交换的功能。用户可通过 `no switchport` 命令将一个交换端口转变为路由端口，然后给路由端口分配 IP 地址来建立路由。注意的是，当使用 `no switchport` 接口配置命令时，将删除该端口的所有二层特性。

i 当一个端口是二层聚合端口的成员端口或者是未认证成功的 DOT1X 认证口时，是不能用 `switchport` 或者 `no switchport` 命令进行层次切换的。

↘ 三层聚合端口

三层聚合端口同二层聚合端口一样，也是由多个物理成员端口汇聚构成的一个逻辑上的聚合端口组。汇聚的端口必须为同类型的三层接口。对于三层交换来说，聚合端口作为三层交换的网关接口，它相当于把同一聚合组内的多条物理链路视为一条逻辑链路，是链路带宽扩展的一个重要途径。此外，通过三层聚合端口发送的帧同样能在三层聚合端口的成员端口上进行流

量平衡,当聚合端口中的一条成员链路失效后,三层聚合端口会自动将这个链路上的流量转移到其它有效的成员链路上,提高了连接的可靠性。

三层聚合端口不具备二层交换的功能。用户可通过 **no switchport** 命令将一个无成员的二层聚合端口转变为三层聚合端口,接着将多个路由端口加入此三层聚合端口,然后给三层聚合端口分配 IP 地址来建立路由。

Loopback 口

Loopback 接口是完全软件模拟的本地三层逻辑接口,它永远都处于 UP 状态。发往 Loopback 接口的数据包将会在设备本地处理,包括路由信息。Loopback 接口的 IP 地址可以用来作为 OSPF 路由协议的设备标识、实施发向 Telnet 或者作为远程 Telnet 访问的网络接口等等。配置一个 Loopback 接口类似于配置一个以太网接口,可以把它看作一个虚拟的以太网接口。

FC 口

FC 接口(Fibre Channel interface, FC 接口)是物理光纤通道接口,用于支撑 FC 存储网络通讯。通过配置 FC 接口的不同工作模式(E、F、NP),允许和原有的 FC SAN 网络或者新建 FC SAN 网络建立丰富的连接,从而实现融合网络的组网。

FC 聚合口

FC 聚合口也称 FC AP,同二层聚合口以及三层聚合口类似。FC 聚合口就是把多个工作于 E 模式的 FC 物理端口捆绑在一起形成一个虚拟逻辑端口。理论上,FC 聚合口带宽是其所有成员接口的各带宽总和。因此,使用 FC 聚合功能用于满足更高的带宽需求。

功能特性

功能特性	作用
接口配置命令的使用	进入接口配置模式,在接口配置模式下用户可配置接口的相关属性。对于逻辑口,用户进入接口模式时,如果该接口不存在,将会首先创建出该接口。
接口的描述和管理状态	用户可以为一个接口起一个专门的名字来标识这个接口,有助于用户记住一个接口的功能; 用户可以设置接口的管理状态。
接口的MTU	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。
配置接口带宽	用户可以基于接口配置接口的带宽。
配置接口的 Load-interval	用户可以指定每隔多少时间计算报文输入输出的负载情况。
配置接口载波时延	用户可以调整接口的载波时延来调整接口状态从 Down 状态到 Up 状态或者从 Up 状态到 Down 状态的时间延时。
接口的LinkTrap策略	在设备中可以基于接口配置是否发送该接口的 LinkTrap 信息。
接口索引永久化功能	接口索引永久化功能,即设备重启后接口索引不变。
配置路由口	在三层设备上,用户可以把物理端口设置为路由端口,作为三层交换的网关接口。
配置三层AP口	在三层设备上,可以把 AP 端口设置为三层 AP 端口,作为三层交换的网关接口。
选择接口介质类型	光电复用端口,用户可以根据需要选择使用光口还是电口。
接口的速率,双工、流控和自协商因子模式	用户可以调整接口的速率,双工模式、流控模式和自协商因子模式。
模块自动检测	在配置接口速率为自动协商模式的情况下,能够根据插入的模块类型自动调节接口的速率。
保护口	用户可以通过将某些端口设置为保护口来实现端口之间不能互相通信。同时还可以通过配置操作来设置保护口之间不能进行路由。

端口违例恢复	当端口因发生违例而被关闭之后，用户可以在全局模式下使用端口违例恢复命令来将所有违例接口从错误状态中恢复过来，重新复位使能该接口。
接口节能管理	用户配置接口节能使能，能够使接口工作在低功耗模式下。
端口震荡保护	用户配置端口震荡保护功能，当端口发生震荡时，系统自动 shutdown 端口，用于保护端口

1.3.1 接口配置命令的使用

用户可在全局配置模式下使用 **interface** 命令进入接口配置模式。在接口配置模式下用户可配置接口的相关属性。

工作原理

在全局配置模式下输入 **interface** 命令，进入接口配置模式。对于逻辑口，用户进入接口模式时，如果该接口不存在，将会首先创建出该接口。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（接口的编号）。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。

对于逻辑口，可以在全局配置模式下通过执行 **no interface** 命令删除指定的逻辑接口。

▾ 接口编号规则

对于物理端口，在单机模式下编号由两部分组成：插槽号和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；在 VSU 模式或者堆叠模式下编号由三部分组成：设备号，插槽号和端口在插槽上的编号，例如设备号为 1，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 1/2/3。

设备号是从 1 到支持的成员设备的最大数量。

插槽的编号规则：静态插槽的编号固定为 0，动态插槽（可插拔模块或线卡）的编号是从 1 - 插槽的个数。动态插槽的编号规则是：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，称为光电复用端口，无论使用那种介质，都使用相同的端口编号。

对于聚合端口，其编号的范围为 1 - 设备支持的聚合端口个数。

对于交换虚拟接口，其编号就是这个交换虚拟接口对应的 VLAN 的 VID。

▾ 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。

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：

常见的有效的接口范围格式：

- **FastEthernet** device/slot/{第一个 port} - {最后一个 port}；
- **GigabitEthernet** device/slot/{第一个 port} - {最后一个 port}；

- **TenGigabitEthernet** device/slot/{第一个 port} - {最后一个 port} ;
- **FortyGigabitEthernet** device/slot/{第一个 port} - {最后一个 port} ;
- **AggregatePort** Aggregate-port 号– Aggregate-port 号 , 范围是 1 ~ 设备支持的最大聚合端口数量 ;
- **vlan** vlan-ID-vlan-ID, VLAN ID 范围 1 ~ 4094 ;
- **Loopback** loopback-ID-loopback-ID, 范围是 1 ~ 2147483647 ;

在一个 **interface range** 中的接口必须是相同类型的, 即或者全是 FastEthernet、GigabitEthernet、AggregatePort , 或者全是 SVI 接口等。

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。

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。

1.3.2 接口的描述和管理状态

用户可以为一个接口起一个专门的名字来标识这个接口, 有助于用户记住一个接口的功能。

用户可以进入接口模式对接口进行关闭和打开管理。

工作原理

接口的描述

用户可以根据要表达的含义来设置接口的具体名称, 比如, 用户想将 GigabitEthernet 1/1 分配给用户 A 专门使用, 用户就可以将这个接口的描述设置为 “Port for User A” 。

接口的管理状态

在某些情况下, 用户可能需要禁用某个接口。用户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。用户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。

1.3.3 接口的 MTU

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。

工作原理

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。MTU 是指帧中有效数据段的长度, 不包括以太网封装的开销。

端口收到或者转发的帧, 如果长度超过设置的 MTU 将被丢弃。

MTU 允许设置的范围为 64~9216 字节, 粒度为 4 字节, 缺省一般为 1500 字节。

i 此配置命令只对物理端口和 AP 口有效。

1.3.4 配置接口带宽

工作原理

主要用于一些路由协议(如 OSPF 路由协议)计算路由量度和 RSVP 计算保留带宽。修改接口带宽不会影响物理接口的数据传输速率。

i 接口的带宽命令不能实际影响某个接口的带宽，它只是个路由参数，不会影响物理链路的接口的真正带宽。

1.3.5 配置接口的 Load-interval

工作原理

接口的 load-interval 可以指定每隔多少时间计算报文输入输出的负载情况，一般是每隔 10 秒钟计算一次每秒中输入输出的报文数和比特数。

1.3.6 配置接口载波时延

工作原理

接口的载波时延 Carry-delay 是指接口链路的载波检测信号 DCD 从 Down 状态到 Up 状态或者从 Up 状态到 Down 状态的时间延时，如果 DCD 在延时之内发生变化，那么系统将忽略这种状态的变化而不至于上层的数据链路层重新协商。如果参数设置的比较大，那么几乎每次瞬间的 DCD 变化将无法被检测到；相反，如果参数设置成 0，那么每次微小的 DCD 信号的跳变都将被系统检测到，这样系统也就将增加不稳定性。

i 如果 DCD 载波中断时间比较长，那么将该参数设长些，可以尽快加速拓扑收敛和路由汇聚，以便网络拓扑或者路由表可以较快的收敛。如果相反，DCD 载波中断时间小于网络拓扑或者路由汇聚所花的时间，那么应该将该参数设置相对的大些，以免造成没有必要的网络拓扑振荡或者路由振荡。

1.3.7 接口的 LinkTrap 策略

在设备中，用户可以基于接口配置选择是否发送该接口的 LinkTrap 状态变化信息。

工作原理

当接口的 LinkTrap 发送功能打开时，如果该接口的 Link 状态变化，SNMP 将发出 LinkTrap 信息，反之则不发。

1.3.8 接口索引永久化功能

和接口的名字一样，接口索引也可以用于标识一个接口，接口索引是一个接口的“身份 ID”，每个接口创建时，系统会自动为每个接口分配不重复的接口索引值，而当设备重启后，一个接口的索引值可能会和重启前的一致。接口索引永久化功能，即设备重启后接口索引不变。

工作原理

当配置了该功能，设备重启后相同接口的接口索引值保持不变。

1.3.9 配置路由口

工作原理

在三层设备上，可以把物理端口设置为路由端口，作为三层交换的网关接口。路由端口不具备二层交换的功能。用户可通过 `no switchport` 命令将一个交换端口转变为路由端口，然后给路由端口分配 IP 地址来建立路由。注意的是，当使用 `no switchport` 接口配置命令时，将删除该端口的所有二层特性。

1.3.10 配置三层 AP 口

工作原理

在三层设备上，类似三层路由口一样，用户可通过 **no switchport** 命令将一个二层 AP 端口转变为三层 AP 端口，然后给该 AP 端口分配 IP 地址来建立路由。注意的是，当使用 **no switchport** 接口配置命令时，将删除该 AP 端口的所有二层特性。

- ❗ 当 AP 口中含有成员口时，不允许将二层 AP 口配置为三层 AP 口，反之，也不允许将带有成员口的三层 AP 口转变为二层 AP 口。

1.3.11 选择接口介质类型

对于光电复用端口，用户可以根据需要选择使用光口还是电口。

工作原理

用户可以选择使用光口还是电口。但是这两种介质不能同时生效。一旦用户选定介质类型，接口的连接状态、速率、双工和流控等属性都是指该介质类型的属性，如果用户改变介质类型，新选介质类型的这些属性将使用默认值，用户可以根据需要重新设定这些属性。

📌 光电复用端口支持接口介质自动选择

- 如果用户配置接口介质自动选择，在接口只有一种介质连接上时，设备使用当前连接的介质；
- 在接口的两种介质都连接上时，设备将使用用户配置的优先介质。介质自动选择优先介质默认为电口，用户可以通过配置 **medium-type auto-select prefer fiber** 来设置优先介质为光口。在自动选择模式下，接口的速率、双工、流控等属性将使用默认值。

- ❗ 配置为介质自动选择的端口，对方端口必须设置为自动协商，否则会出现介质切换错误。
- ❗ 此配置命令只对物理端口有效，聚合端口和 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。
- ❗ 配置为聚合端口成员口的端口，其介质类型必须一致，否则无法加入到聚合端口中。聚合端口成员口的端口类型不能改变。配置为介质自动选择的接口不能加入聚合端口。

1.3.12 接口的速率、双工、流控和自协商因子模式

对于以太网物理接口和 AP 口，用户可以配置管理接口的速率、双工、流控和自协商因子模式。

工作原理

📌 接口的速率

通常情况下，以太网物理接口速率是通过和对端设备自协商决定的。协商得到的速率可以是接口速率能力范围内的任意一个速率。用户也可以通过配置接口能力范围内的任意一个具体速率值让以太网物理接口工作在该指定速率值上。

对于 AP 口，当用户设置 AP 口的速率时，实际上是生效到该 AP 口的所有成员口上(这些成员口都是以太网物理接口)的。

📌 接口的双工

以太网物理接口和 AP 口的双工模式时存在三种情况：

- 可以将接口设置为全双工属性实现接口在发送数据包的同时可以接收数据包；
- 可以将接口设置为半双工属性控制接口同一时刻只能发送数据包或接收数据包时；
- 当设置接口的双工属性为自协商模式时，接口的双工状态由本接口和对端接口自动协商而定。

对于 AP 口，当用户设置 AP 口的双工模式时，实际上是生效到该 AP 口的所有成员口上(这些成员口都是以太网物理接口)的。

▾ 接口的流控

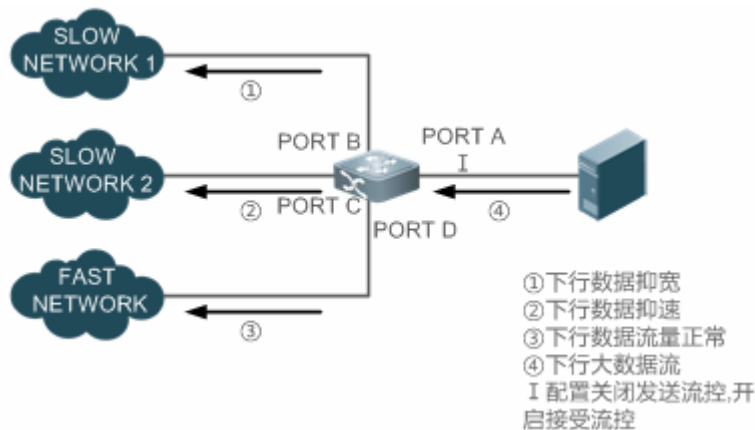
接口的流控模式分为非对称流控模式和对称流控模式：

- 对称流控模式，即在一般情况下，接口开启流控模式后，接口上将会处理接收到的流控帧，并在接口出现拥塞时发送流控帧，接收和发送流控帧的处理是一致的，这就是对称流控模式。
- 非对称流控模式，即在一些情况下，设备希望某个接口能够处理接收到的流控帧保证报文不会因为拥塞而丢弃，又不想发出流控帧而导致整个网络速率下降，这个时候，就要通过配置非对称流控，将接收流控帧和发送流控帧的处理步调分开。

对于 AP 口，当用户设置 AP 口的流控模式时，实际上是生效到该 AP 口的所有成员口上(这些成员口都是以太网物理接口)的。

如**错误！未找到引用源。**所示，设备的端口 A 为上联口，端口 B-D 为下联端口，其中端口 B 和 C 对应的是一个慢速网络，假如端口 A 上开启了接收流控和发送流控功能，由于端口 B 和 C 对应的是一个慢速网络，在发送端口 B 的数据流过大，导致端口 B 和 C 拥塞，进而导致端口 A 上的入口拥塞，端口 A 上就会发送流控帧，当上联设备响应流控帧时，就会降低往端口 A 的数据流，间接导致端口 D 上的网速下降。这个时候，可以配置端口 A 的发送流控功能关闭，来保障整个网络带宽利用率。

图 1-4



▾ 接口的自协商因子模式

接口的自协商因子模式有 on 和 off 两种。接口的自协商状态和接口的自协商因子模式并不完全等同，接口的自协商状态通常由接口的速率、双工、流控和自协商因子模式共同决定。

对于 AP 口，当用户设置 AP 口的自协商因子模式时，实际上是生效到该 AP 口的所有成员口上(这些成员口都是以太网物理接口)的。

- ① 一般情况下，只要接口的速率、双工和流控中的一种属性为 auto 模式，或者接口的自协商模式为 on 模式，那么接口的自协商工作状态就是 on 的，即接口的自协商功能是打开的；反之，当接口的速率、双工和流控中的属性全部为非 auto 模式，并且接口的自协商模式为 off 模式时，那么接口的自协商工作状态就是 off 的，即接口的自协商功能是关闭的。
- ② 对于百兆光口，接口的自协商功能永远都是关闭的，即百兆光口的自协商工作状态永远都是 off 的；对于千兆电口，接口的自协商功能永远都是开启的，即千兆电口的自协商工作状态永远都是 on 的。

1.3.13 模块自动检测

在配置接口速率为自动协商模式的情况下，能够根据插入的模块类型自动调节接口的速率。

工作原理

目前支持的模块有 SFP 和 SFP+两种模块，其中 SFP 为千兆模块，SFP+为万兆模块，若插入的是 SFP 模块，则接口工作在千兆模式，若插入的是 SFP+模块，则接口工作在万兆模式。

i 模块的自动检测功能只在速率配置为自动协商时才能生效。

1.3.14 保护口

有些应用环境下，要求交换机上的部分端口间不能互相通讯，可以通过将某些端口设置为保护口(Protected Port)来达到目的。同时还可以通过配置操作来设置保护口之间不能进行路由。

工作原理

保护口

当端口设为保护口之后，保护口之间互相无法通讯，保护口与非保护口之间可以正常通讯。

保护口有两种模式，一种是阻断保护口之间的二层交换，但允许保护口之间进行路由，第二种是同时阻断保护口之间的二层交换和阻断路由；在两种模式都支持的情况下，第一种模式将作为缺省配置模式。

当两个保护口设为一个镜像会话端口对时，该镜像会话的源端口发送或接收的帧依然能够镜像到该镜像会话的目的端口上。目前只支持在以太网物理接口和 AP 口上设置保护口。当一个 AP 口被设置为保护口时，该 AP 所有成员口都被设置为保护口。

1.3.15 端口违例恢复

某些协议具备设置端口违例（关闭端口）的功能，用以保证网络的安全性和稳定性。比如端口安全协议，当用户配置开启端口安全，并配置端口上最大安全地址数量，当端口下学习到的地址数超过最大安全地址数时，将产生端口违例事件。另外生成树协议、DOT1X 协议、REUP 协议等也都具备类似的功能，违例的端口会自动关闭该接口，以保证安全性。

工作原理

当端口因发生违例而被关闭之后，可以在全局模式下使用端口违例恢复命令来将所有违例接口从错误状态中恢复过来，重新复位使能该接口。可以选择手动恢复，也可以选择定时自动恢复。

1.3.16 端口节能管理配置

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

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

工作原理

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

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

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

i 仅工作在 100M 和 1000M 速率模式的电口支持 EEE 功能。

EEE 功能仅在端口开启自协商能力时生效。

1.3.17 端口震荡保护

当发生接口震荡时，会产生大量硬件中断，从而消耗大量 CPU 资源，另一方面频繁的接口震荡容易损害接口，用户可以配置接口震荡保护功能来保护接口。

工作原理

接口链路震荡保护功能由用户自行决定是否开启，默认情况下为开启保护功能。当接口发生震荡时，接口每 2s 或 10 秒都会检测一次震荡，如果检测到接口 2s 内震荡 6 次，则打印提示信息，连续打印 10 次提示信息(也就是 20s 内连续检测到接口震荡)，则关闭接口；对于 10s 检测一次震荡，如果检测到接口 10s 发生 10 次震荡，则打印提示信息，不关闭接口。

1.3.18 接口 Syslog

用户可以通过配置打开或关闭 Syslog 开关来决定是否查看接口状态发生改变或异常的信息。

工作原理

接口 Syslog 开关由用户自行决定是否开启，默认情况下为开启。当接口发生异常情况，比如接口状态发生改变，接口收到错误帧或接口发生震荡时，系统将打印提示信息告之用户。

1.4 配置详解

配置项	配置建议 & 相关命令	
接口配置管理	 可选配置。主要用于进行接口的创建、删除、接口描述管理等管理配置。	
	interface	创建一个接口，并进入指定接口配置模式，或者直接进入该接口的接口配置模式。
	interface range	输入一定范围的接口，当这些接口未被创建时，同时进行接口创建，并进入接口批量配置模式。
	define interface-range	将批量操作的接口定义成宏定义形式。
	snmp-server if-index persist	开启接口索引永久化功能，即设备重启后接口索引不变。
	description	在接口配置模式下，使用该命令设置接口的描述，最多 80 字符。
	snmp trap link-status	基于接口配置是否发送该接口的 LinkTrap 信息。
	shutdown	在接口配置模式下，使用该命令关闭接口。
	physical-port dither protect	在全局配置模式下，配置接口震荡保护功能
	logging [link-updown error-frame link-dither]	在全局配置模式下，配置接口开启打印接口状态信息
配置接口属性	 可选配置。主要用于进行接口的属性等管理配置。	
	bandwidth	在接口配置模式下，使用该命令设置接口的带宽参数。
	carrier-delay	在接口配置模式下，使用该命令设置接口载波时延。

	load-interval	在接口配置模式下,使用该命令设置接口的负载计算的间隔时间
	duplex	设置接口的双工模式。
	flowcontrol	打开或关闭接口的流量控制。
	medium-type	选择接口的介质类型。
	mtu	设置接口的 MTU。
	negotiation mode	设置接口的自协商因子模式。
	speed	设置接口的速率。
	switchport	在接口配置模式下使用不带任何参数的 switchport 命令 将一个接口设置为二层接口模式,使用 no switchport 命令将一个接口设置为三层接口模式。
	switchport protected	设置接口为保护口模式。
	errdisable recovery	在全局配置模式下,使用改命令来恢复违例端口
	eee enable	在接口配置模式下,使能端口节能状态

1.4.1 接口配置管理

配置效果

- 能够创建出指定的单个逻辑口,并进入接口的配置模式,或者对于已经存在的物理接口或者逻辑接口,可以进入接口的配置模式。
- 能够批量创建出指定的逻辑口,并进入接口批量操作的配置模式,或者对于已经存在的物理接口或者逻辑接口,可以进入接口批量操作的配置模式。
- 能够实现相同接口在设备重启前后接口索引保持不变。
- 设置接口的描述符,对该接口直观、形象化的理解。
- 能够启用或者关闭接口的 LinkTrap 功能。
- 配置接口管理状态,关闭或者打开接口。

注意事项

- 对于逻辑接口,可以使用该命令的 **no** 命令形式删除接口或者将指定范围接口的批量删除,但不可以使用该命令的 **no** 命令形式删除指定的物理接口或批量删除指定范围的物理接口。
- 可以使用该命令的 **default** 命令形式将指定物理接口或者逻辑接口或者指定范围的接口在接口模式下的相关配置恢复到缺省配置。

配置方法

配置单个指定的接口

- 可选配置。
- 可以用于需要创建某个不存在的逻辑接口或者进入已经存在的物理接口和逻辑接口的接口配置模式以进行接口相关的配置时,需要配置该命令。

【命令格式】 **interface** *interface-type* *interface-number*

【参数说明】 *interface-type interface-number*: 即接口的类型和接口编号,可以是以太网物理接口、AP 口、SVI 口、Loopback 口等。

【缺省配置】 无

【命令模式】 全局配置模式

- 【使用指导】
- 对于逻辑接口，如果该接口未被创建，则首先创建出该接口并进入接口的配置模式。
 - 对于物理接口或者已经创建的逻辑接口，直接进入该接口的配置模式。
 - 使用 **no** 命令形式删除指定的逻辑接口。
 - 使用 **default** 命令形式将该接口的接口模式下配置恢复到缺省配置。

配置一定范围的接口

- 可选配置。
- 可以用于需要批量创建不存在的逻辑接口或者进入已经存在的物理接口和逻辑接口的接口批量配置模式以进行接口相关的配置时，需要配置该命令。

【命令格式】 **interface range** { *port-range* | **macro** *macro_name* }

【参数说明】 *port-range*：即批量操作的接口类型和接口编号范围，可以是以太网物理接口、AP 口、SVI 口、Loopback 口等。

macro_name：即一定范围接口类型的宏定义名。

【缺省配置】 无

【命令模式】 全局配置模式

- 【使用指导】
- 对于逻辑接口，如果接口未被创建，则首先创建出接口然后再进入接口的批量配置模式。
 - 对于物理接口或者已经创建的逻辑接口，直接进入接口的批量配置模式。
 - 使用 **default** 命令形式批量将接口模式下配置恢复到缺省配置。
 - 使用宏定义的时候，需要在全局配置模式下，先将一定范围的接口类型通过 **define interface-range** 命令进行宏定义成 *macro_name*，然后再通过 **interface range macro macro_name** 进行接口的批量配置管理。

配置接口的索引永久化

- 可选配置。
- 可以用于需要保持接口索引在系统重启前后一致时使用。

【命令格式】 **snmp-server if-index persist**

【参数说明】 -

【缺省配置】 该功能关闭。

【命令模式】 全局配置模式

- 【使用指导】 执行该命令后，保存配置时将会把当前所有接口的索引保存起来，重启后接口使用重启前分配的接口索引。可以使用该命令的 **no** 命令或者 **default** 命令形式关闭该功能。

配置接口的描述符

- 可选配置。
- 可以用于为接口设置描述信息时使用。

【命令格式】 **description** *string*

【参数说明】 *string*：最长 80 个字符

【缺省配置】 缺省无接口描述符

【命令模式】 接口配置模式

- 【使用指导】 该命令配置接口的描述符。可以使用该命令的 **no** 命令或者 **default** 命令形式取消配置接口的描述符。-

配置接口的 LinkTrap

- 可选配置。
- 可以用于通过 SNMP 获取接口状态变化的 Trap 信息。

- 【命令格式】 **snmp trap link-status**
- 【参数说明】 -
- 【缺省配置】 缺省情况下，该功能打开
- 【命令模式】 接口配置模式
- 【使用指导】 该命令配置是否发送该接口的 LinkTrap，当功能打开时，如果接口的 Link 状态变化，SNMP 将发出 LinkTrap，反之则不发。可以使用该命令的 **no** 命令或者 **default** 命令形式关闭该功能。

▾ 配置接口的管理状态

- 可选配置。
 - 用于关闭或者打开接口。
 - 接口关闭后将无法收发报文。
- 【命令格式】 **shutdown**
- 【参数说明】 -
- 【缺省配置】 接口的管理状态是 UP
- 【命令模式】 接口配置模式
- 【使用指导】 对接口执行 **shutdown** 操作时，即关闭该接口，执行 **no shutdown** 操作将重新打开该接口。注意有些情况下，不允许将端口执行 **no shutdown** 操作，比如该端口处于端口违例状态，那么该端口将无法执行 **no shutdown** 操作。可以使用该命令的 **no** 命令或者 **default** 命令形式重新打开该接口。

▾ 配置接口震荡保护功能

- 可选配置。
 - 用于保护发生震荡的接口。
- 【命令格式】 **physical-port dither protect**
- 【参数说明】
- 【缺省配置】 默认开启接口震荡保护功能
- 【命令模式】 全局配置模式
- 【使用指导】

▾ 配置打印接口 Syslog 信息功能

- 可选配置。
 - 用于开启或关闭打印接口状态信息功能。
- 【命令格式】 **[no] logging [link-updown | error-frame | link-dither]**
- 【参数说明】
- 【缺省配置】 开启打印接口 Syslog 信息
- 【命令模式】 全局配置模式
- 【使用指导】

检验方法

▾ 配置单个指定的接口

- 执行 **interface** 操作，如果能够正常进入接口模式，即说明配置是成功的。
- 对于逻辑接口，如果是执行 **no interface** 操作，也可以通过 **show running** 命令或者 **show interfaces** 命令查看对应的接口是否存在，如果不存在，则该逻辑接口是被正常删除的。

- 执行 **default interface** 操作，通过 **show running** 命令查看对应的接口下的配置是否都恢复到了缺省配置，如果是，则说明该操作是成功的。

配置一定范围的接口

- 执行 **interface range** 操作，如果能够正常进入接口批量配置模式，即说明配置是成功的。
- 执行 **default interface range** 操作，通过 **show running** 命令查看对应的接口下的配置是否都恢复到了缺省配置，如果是，则说明该操作是成功的。

配置接口索引永久化

- 配置完该命令后，执行 **write** 保存配置操作，重启设备后，通过 **show interface** 命令查看接口的接口索引值，如果对于同一个接口的索引值在设备重启后保持一致，那么说明接口的索引永久化功能是正常的。

配置接口的 LinkTrap

- 选择一个物理端口，进行网线插拔，同时打开 SNMP 服务器，如果在网线插拔的时候，SNMP 服务器能够正常收到该接口的 Link 状态变化的 Trap 信息，则说明该功能是正常的。
- 执行 **no** 命令形式操作，如果验证到在一个物理端口，进行网线插拔，同时打开 SNMP 服务器，如果在网线插拔的时候，SNMP 服务器无法收到该接口的 Link 状态变化的 Trap 信息，则说明已经正常关闭了接口的 LinkTrap 功能。

配置接口的管理状态

- 选择一个物理端口，插上网线，让端口 Up 起来，对该端口执行 **shutdown** 关闭接口的操作，用户在控制台上能够看到端口状态变成管理 Down 的 Syslog 信息，同时该端口上的指示灯灭掉，则关闭端口的功能是正常的，并且通过 **show interfaces** 命令可以看到接口状态显示为 administratively down。在此基础上，执行 **no shutdown** 重新打开该接口，用户在控制台上能够看到端口 Up 的 Syslog 信息，同时该端口上的指示灯重新亮起来，则打开端口的功能是正常的。

配置接口震荡保护功能

- 在全局配置模式下配置命令，如 **physical-port dither protect**。选择一个物理端口，频繁插拔网线模拟端口发生震荡的情况，在控制台上可以看到系统打印端口发生震荡的信息，经过连续打印若干次之后，系统会提示端口不稳定将 shutdown 接口。

配置打印接口 Syslog 信息功能

- 在全局配置模式下配置命令，如 **logging link-updown** 查看接口状态信息。选择一个物理端口，插拔网线，接口将发生两次状态改变，用户可以在控制台上看到接口 link 状态从 up 变为 down 的信息，又从 down 变为 up 的信息；配置 **no logging link-updown** 后，再次插拔网线，控制台上看不到信息，说明该功能是正常的。

配置举例

配置接口基本属性

【网络环境】 192.168.1.1/24 192.168.1.2/24

图 1-5



- 【配置方法】
- 将 2 台设备通过交换端口进行连接。
 - 分别给 2 台设备配置一个 SVI 口，并配置相同网段的 IP 地址。

- 在 2 台设备上分别配置接口索引永久化。
- 在 2 台设备上分别启用 LinkTrap 功能。
- 在两台设备上配置接口管理状态。

```

A
A# configure terminal
A(config)# snmp-server if-index persist
A(config)# interface vlan 1
A(config-if-VLAN 1)# ip address 192.168.1.1 255.255.255.0
A(config-if-VLAN 1)# exit
A(config)# interface gigabitethernet 0/1
A(config-if-GigabitEthernet 0/1)# snmp trap link-status
A(config-if-GigabitEthernet 0/1)# shutdown
A(config-if-GigabitEthernet 0/1)# end
A# write

B
B# configure terminal
B(config)# snmp-server if-index persist
B(config)# interface vlan 1
B(config-if-VLAN 1)# ip address 192.168.1.2 255.255.255.0
B(config-if-VLAN 1)# exit
B(config)# interface gigabitethernet 0/1
B(config-if-GigabitEthernet 0/1)# snmp trap link-status
B(config-if-GigabitEthernet 0/1)# shutdown
B(config-if-GigabitEthernet 0/1)# end
B# write

```

【检验方法】 在 A、B 设备上分别进行如下检验：

- 检查设备上的 GigabitEthernet 0/1 和 SVI 1 在接口 GigabitEthernet 0/1 在 **shutdown** 操作后的接口状态是否正确
- 检查接口 GigabitEthernet 0/1 **shutdown** 操作后，是否有发出该接口 Link Down 的 Trap 信息
- 重启设备后，接口 GigabitEthernet 0/1 的接口索引值是否和重启前的一致

```

A
A# show interfaces gigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is administratively down , line protocol is DOWN
Hardware is GigabitEthernet, address is 00d0.f865.de9b (bia 00d0.f865.de9b)
Interface address is: no ip address
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Bridge, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  Rxload is 1/255, Txload is 1/255
  Queue   Transmitted packets   Transmitted bytes   Dropped packets   Dropped
bytes
    0           0           0           0
0
    1           0           0           0
0
    2           0           0           0
0
    3           0           0           0
0
    4           0           0           0
0
    5           0           0           0
0
    6           0           0           0
0

```

```

    7                4                440                0
0
Switchport attributes:
  interface's description:""
  lastchange time:0 Day:20 Hour:15 Minute:22 Second
  Priority is 0
  admin medium-type is Copper, oper medium-type is Copper    admin duplex mode is AUTO, oper
duplex is Unknown
  admin speed is AUTO, oper speed is Unknown
  flow control admin status is OFF, flow control oper status is Unknown
  admin negotiation mode is OFF, oper negotiation state is ON
  Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF
Port-type: access
  Vlan id: 1
  10 seconds input rate 0 bits/sec, 0 packets/sec
  10 seconds output rate 0 bits/sec, 0 packets/sec
  4 packets input, 408 bytes, 0 no buffer, 0 dropped
  Received 0 broadcasts, 0 runts, 0 giants
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
  4 packets output, 408 bytes, 0 underruns , 0 dropped
  0 output errors, 0 collisions, 0 interface resets
A# show interfaces vlan 1
Index(dec):4097 (hex):1001
VLAN 1 is UP , line protocol is DOWN
Hardware is VLAN, address is 00d0.f822.33af (bia 00d0.f822.33af)
Interface address is: 192.168.1.1/24
ARP type: ARPA, ARP Timeout: 3600 seconds
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Ethernet-II, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  Rxload is 0/255, Txload is 0/255

```

B

```

B# show interfaces gigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is administratively down , line protocol is DOWN
Hardware is GigabitEthernet
Interface address is: no ip address, address is 00d0.f865.de9b (bia 00d0.f865.de9b)
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Bridge, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  Rxload is 1/255, Txload is 1/255

```

Queue	Transmitted packets	Transmitted bytes	Dropped packets	Dropped bytes
0	0	0	0	0
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	4	440	0	0

```
0
Switchport attributes:
  interface's description:""
  lastchange time:0 Day:20 Hour:15 Minute:22 Second
  Priority is 0
  admin medium-type is Copper, oper medium-type is Copper
  admin duplex mode is AUTO, oper duplex is Unknown
  admin speed is AUTO, oper speed is Unknown
  flow control admin status is OFF, flow control oper status is Unknown
  admin negotiation mode is OFF, oper negotiation state is ON
  Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF
Port-type: access
  Vlan id: 1
  10 seconds input rate 0 bits/sec, 0 packets/sec
  10 seconds output rate 0 bits/sec, 0 packets/sec
  4 packets input, 408 bytes, 0 no buffer, 0 dropped
  Received 0 broadcasts, 0 runts, 0 giants
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
  4 packets output, 408 bytes, 0 underruns , 0 dropped
  0 output errors, 0 collisions, 0 interface resets
B# show interfaces vlan 1
Index(dec):4097 (hex):1001
VLAN 1 is UP , line protocol is DOWN
Hardware is VLAN, address is 00d0.f822.33af (bia 00d0.f822.33af)
Interface address is: 192.168.1.2/24
ARP type: ARPA, ARP Timeout: 3600 seconds
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Ethernet-II, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  Rxload is 0/255, Txload is 0/255
```

常见错误

- 无。

1.4.2 配置接口属性

配置效果

- 将设备通过交换端口或者路由端口进行连接和数据通信。
- 在设备上分别调整各种接口属性。

注意事项

- 无。

配置方法

▾ 配置路由端口

- 可选配置。
- 可以用于需要将接口转换为三层路由口时使用。
- 配置成三层路由口后将使该接口上运行的二层协议失效。
- 支持二层交换口上配置。

【命令格式】 **no switchport**

- 【参数说明】 -
- 【缺省配置】 交换机上的以太网物理端口缺省为二层交换
- 【命令模式】 接口配置模式
- 【使用指导】 在三层交换机设备上，使用该命令可以将一个二层交换口配置成三层路由口。使用 **switchport** 命令可以将一个三层路由口转换成二层交换口。

配置三层 AP 口

- 可选配置。
 - 可以在接口配置模式下，执行 **no switchport** 命令将一个二层 AP 口配置成三层 AP 口。使用 **switchport** 命令时，可以将一个三层 AP 口配置成二层 AP 口。
 - 配置成三层路由口后将使该接口上运行的二层协议失效。
 - 支持二层聚合口上配置。
- 【命令格式】 **no switchport**
- 【参数说明】 -
- 【缺省配置】 缺省情况下，交换机上的 AP 端口缺省为二层 AP 口
- 【命令模式】 接口配置模式
- 【使用指导】 在三层交换机设备上，进入二层 AP 口的接口模式后，使用该命令可以将一个二层 AP 口配置成三层 AP 口。进入三层 AP 口的接口模式后，使用 **switchport** 命令可以将一个三层 AP 口转换成二层 AP 口。

配置接口介质类型

- 可选配置。
 - 对于光电复用口，接口的缺省介质为电口。
 - 配置的端口介质类型变化时，可能会引起端口状态震荡。
 - 支持以太网物理端口上及聚合口上配置。
- 【命令格式】 **medium-type { auto-select [prefer [fiber | copper]] | fiber | copper }**
- 【参数说明】 **auto-select**：自动选择介质类型
prefer [fiber | copper]：自动选择的时候优先选择某种介质类型
fiber：强制选择光口
copper：强制选择电口
- 【缺省配置】 缺省情况下，端口上选择的介质类型为电口
- 【命令模式】 接口配置模式
- 【使用指导】 如果同一端口可以选择光口和电口两种介质类型，用户只能使用其中之一。一旦确定介质类型之后，在配置端口的属性，例如状态、双工、流量控制和速率等，都是指端口当前选择类型的属性。改变端口类型后，新类型对应的端口的属性为其默认属性，用户可以根据需要重新配置。
- 如果用户配置端口介质自动选择，在端口只有一种介质连接上时，设备使用当前连接的介质；在端口的两种介质都连接上时，设备将使用用户配置的优先介质。介质自动选择优先介质默认为电口，用户可以通过配置 **medium-type auto-select prefer fiber** 来设置优先介质为光口。在自动选择模式下，端口的速率、双工、流控等属性将使用默认值。

配置接口速率

- 可选配置。
 - 配置的端口速率模式变化时，可能会引起端口震荡。
 - 支持以太网物理端口上及聚合口上配置。
- 【命令格式】 **speed [10 | 100 | 1000 | auto]**
- 【参数说明】 **10**：表示接口的速率为 10Mbps。
100：表示接口的速率为 100Mbps。

1000：表示接口的速率为 1000Mbps。

auto：表示接口的速率为自适应的。

【缺省配置】 缺省情况下，接口的速率是自协商模式，即接口的速率配置缺省为 auto 模式

【命令模式】 接口模式

【使用指导】 如果接口是聚合端口的成员，则该接口的速率由聚合端口的速率决定。接口退出聚合端口时使用自己的速率设置。使用 **show interfaces** 命令查看设置。接口类型不同，允许设置的速率类型也会有所不同，如 SFP 类型的接口就不允许把速率设为 10M。

配置接口双工模式

- 可选配置。
- 配置的端口双工模式变化时，可能会引起端口震荡。
- 支持以太网物理端口上及聚合口上配置。

【命令格式】 **duplex { auto | full | half }**

【参数说明】 **auto**：表示全双工和半双工自适应。

full：表示全双工。

half：表示半双工。

【缺省配置】 缺省情况下，接口的双工是自协商模式，即接口的双工配置缺省为 auto 模式

【命令模式】 接口模式

【使用指导】 接口的双工属性与接口的类型有关。可以使用 **show interfaces** 命令查看接口双工的设置。

配置接口流控模式

- 可选配置。
- 一般情况下，接口的流控模式缺省为 off 模式。部分产品的缺省模式为 on 模式。
- 接口开启流控模式后，在接口上出现拥塞时，将接收或者发送流控帧调整网络数据流量。
- 配置的端口流控模式变化时，可能会引起端口震荡。
- 支持以太网物理端口上及聚合口上配置。

【命令格式】 **flowcontrol { auto | off | on }**

【参数说明】 **auto**：自协商流量控制。

off：关闭流量控制。

on：打开流量控制。

【缺省配置】 缺省情况下，接口的流控一般是 off 模式，即接口的流控功能缺省是关闭的

【命令模式】 接口配置模式

【使用指导】 -

配置接口自协商因子模式

- 可选配置。
- 配置的端口自协商因子变化时，可能会引起端口震荡。
- 支持以太网物理端口上及聚合口上配置。

【命令格式】 **negotiation mode { on | off }**

【参数说明】 **on**：自协商因子模式为 on 模式。

off：自协商因子模式为 off 模式。

【缺省配置】 缺省情况下，接口的自协商因子是 off 模式

【命令模式】 接口配置模式

【使用指导】 -

配置接口 MTU

- 可选配置。
- 可以通过设置端口的 MTU 来控制端口允许收发的最大帧长。
- 支持以太网物理端口及 SVI 口设置。

【命令格式】 **mtu num**

【参数说明】 *num* : 64 - 9216

【缺省配置】 缺省情况下, 接口的 MTU 值一般为 1500 字节

【命令模式】 接口模式

【使用指导】 设置接口所支持的 MTU, 即链路层数据部分的最大长度。目前只支持设置物理端口和包含成员口的 AP 口的 MTU。

配置接口带宽

- 可选配置。
- 一般情况下, 接口的带宽值和接口支持的速率值相同。

【命令格式】 **bandwidth kilobits**

【参数说明】 *kilobits* : 以每秒 K 比特为单位, 范围为 1 到 2147483647。

【缺省配置】 缺省情况下, 接口带宽值一般和接口类型相匹配, 比如对于千兆以太网物理端口, 该接口的缺省带宽值为 1000000, 万兆以太网物理端口则为 10000000

【命令模式】 接口配置模式

【使用指导】 -

配置接口载波时延

- 可选配置。
- 配置的载波时延时间较长时, 接口物理状态变化时会较晚引起协议状态的变化, 若配置为 0 秒时, 接口物理状态变化则立刻引起协议状态变化。

【命令格式】 **carrier-delay {[milliseconds] num | up [milliseconds] num }**

【参数说明】 *num* : 默认以秒为单位, 范围 0~60 秒。

milliseconds : 配置以毫秒为单位的载波延迟, 范围 0~60000 毫秒。

Up : 设置载波检测信号 DCD 从 Down 状态到 Up 状态的时间延时。

【缺省配置】 缺省情况下, 接口的 Carry-delay 值为 2 秒

【命令模式】 接口配置模式

【使用指导】 -以毫秒为单位设置载波延迟必须是 100 毫秒的整数倍

配置接口 Load-interval

- 可选配置。
- 配置的报文采样时间影响接口报文平均速率的计算, 配置的时间较短时, 报文平均速率能较快反映报文实时流量的变化。

【命令格式】 **load-interval seconds**

【参数说明】 *seconds* : 以秒为单位, 范围 5-600 秒。

【缺省配置】 缺省情况下, 接口的 load-interval 值为 10 秒

【命令模式】 接口配置模式

【使用指导】 -

设置保护口

- 可选配置。

- 配置为保护口的端口之间无法进行二层报文转发。
- 支持以太网物理端口上及聚合口上配置。

【命令格式】 **switchport protected**

【参数说明】 -

【缺省配置】 缺省情况下，接口不是一个保护口

【命令模式】 接口配置模式

【使用指导】 -

▾ 端口违例恢复

- 可选配置。
- 端口违例发生后，端口被关闭，缺省情况下不会恢复。配置了端口违例恢复后，违例的端口会被恢复，端口会被打开。

【命令格式】 **errdisable recovery [interval time]**

【参数说明】 *time*：自动恢复定时时间，取值范围为 30-86400，单位是秒。

【缺省配置】 缺省情况下，没有该功能

【命令模式】 全局配置模式

【使用指导】 缺省情况下，端口违例不会恢复，这个时候可以使用此命令手动恢复或者配置自动恢复。

▾ 配置端口节能

- 可选配置。
- 配置该命令后，开启端口节能模式。

【命令格式】 **eee enable**

【参数说明】

【命令模式】 接口配置模式

【使用指导】 缺省情况下，端口节能模式为关闭状态，使用此命令使能端口节能模式，使用该命令的 **no** 命令或者 **default** 命令形式取消配置接口 EEE 功能。

检验方法

- 可以通过 **show interfaces** 命令查看接口的属性配置是否正常。

【命令格式】 **show interfaces [interface-type interface-number] [description | switchport | trunk]**

【参数说明】 *interface-type interface-number*：接口类型和接口编号

description：接口的描述符信息，包括 link 状态

switchport：二层接口信息，只对二层接口有效

trunk：Trunk 端口信息，对物理端口和聚合端口有效

【命令模式】 特权模式

【使用指导】 如果不加参数，则显示接口的基本信息

【命令展示】

```
SwitchA#show interfaces GigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is DOWN , line protocol is DOWN
  Hardware is Broadcom 5464 GigabitEthernet, address is 00d0.f865.de9b (bia 00d0.f865.de9b)
  Interface address is: no ip address
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Ethernet-II, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  Ethernet attributes:
    Last link state change time: 2012-12-22 14:00:48
    Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds
    Priority is 0
    Medium-type is Copper
```

```

Admin duplex mode is AUTO, oper duplex is Unknown
Admin speed is AUTO, oper speed is Unknown
Flow receive control admin status is OFF,flow send control admin status is OFF
Flow receive control oper status is Unknown,flow send control oper status is Unknown
Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF
Bridge attributes:
Port-type: trunk
Native vlan:1
Allowed vlan lists:1-4094 //Trunk 口的许可 VLAN 列表
Active vlan lists:1, 3-4 //实际生效的 vlan ( 即该设备上仅创建了 VLAN1、3 和 4 )
Queueing strategy: FIFO
Output queue 0/0, 0 drops;
Input queue 0/75, 0 drops
Rxload is 1/255,Txload is 1/255
5 minutes input rate 0 bits/sec, 0 packets/sec
5 minutes output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer, 0 dropped
Received 0 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
0 packets output, 0 bytes, 0 underruns , 0 dropped
0 output errors, 0 collisions, 0 interface resets

```

- 可以通过 **show eee interfaces status** 命令查看接口 EEE 状态。

【命令格式】 **show eee interfaces [interface-type interface-number] status**

【参数说明】 *interface-type interface-number* : 接口类型和接口编号

status : 接口 EEE 状态

【命令模式】 特权模式

【使用指导】 指定接口时不加参数 **status** , 显示单个接口的 EEE 信息 , 否则显示所有接口的 EEE 信息。

【命令展示】 1 : 显示接口 GigabitEthernet 0/1 的 EEE 状态信息。

```

Ruijie#show eee interface gigabitEthernet 0/1
Interface           : Gi0/1
EEE Support         : Yes
Admin Status       : Enable
Oper Status        : Disable
Remote Status      : Disable
Trouble Cause      : Remote Disable

```

Interface	接口信息
EEE Support	是否支持 EEE 功能
Admin Status	设置状态
Oper Status	实际生效状态
Trouble Cause	端口 EEE 状态不正常的原因

2 : 显示所有接口 EEE 状态信息。

```

Ruijie#show eee interface status
Interface EEE      Admin   Oper    Remote  Trouble
          Support  Status Status  Status  Cause
-----
Gi0/1    Yes      Enable  Disable Disable  Remote Disable
Gi0/2    Yes      Enable  Disable Unknown  None
Gi0/3    Yes      Enable  Enable  Enable  None
Gi0/4    Yes      Enable  Enable  Enable  None
Gi0/5    Yes      Enable  Enable  Enable  None
Gi0/6    Yes      Enable  Enable  Enable  None
Gi0/7    Yes      Enable  Enable  Enable  None
Gi0/8    Yes      Enable  Enable  Enable  None
Gi0/9    Yes      Enable  Enable  Enable  None

```

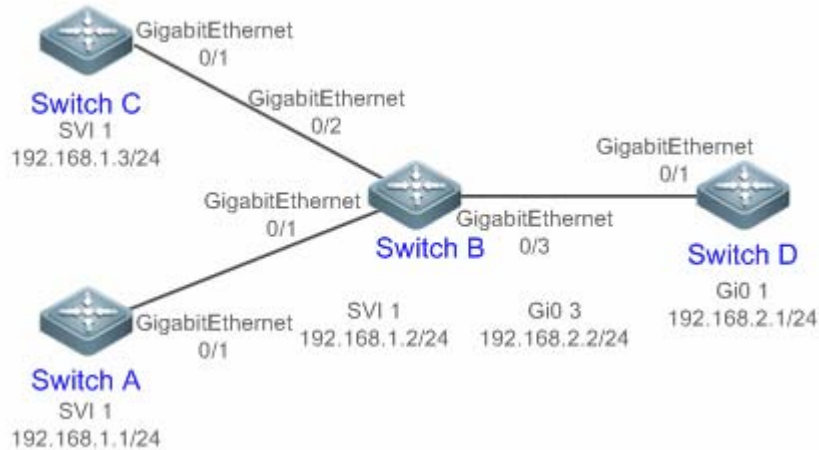
Gi0/10	Yes	Enable	Enable	Enable	None
--------	-----	--------	--------	--------	------

配置举例

配置接口属性

【网络环境】

图 1-6



【配置方法】

- 在 Switch A 上配置 GigabitEthernet 0/1 为 Access 模式交换端口，缺省 VLAN ID 为 1，配置 SVI 1，并为 SVI1 配置 IP 以及到 Switch D 的路由。
- 在 Switch B 上配置 GigabitEthernet 0/1 和 GigabitEthernet 0/2 为 Trunk 模式交换端口，Native VLAN ID 为 1，并配置 SVI 1，并为 SVI 1 配置 IP，配置 GigabitEthernet 0/3 为路由口并为该端口配置另一个网段的 IP。
- 在 Switch C 上配置 GigabitEthernet 0/1 为 Access 模式交换端口，缺省 VLAN ID 为 1，配置 SVI 1，并为 SVI 1 配置 IP。
- 在 Switch D 上配置 GigabitEthernet 0/1 为路由端口，并为该端口配置 IP 以及到 Switch A 的路由。

A

```
A# configure terminal
A(config)# interface GigabitEthernet 0/1
A(config-if-GigabitEthernet 0/1)# switchport mode access
A(config-if-GigabitEthernet 0/1)# switchport access vlan 1
A(config-if-GigabitEthernet 0/1)# exit
A(config)# interface vlan 1
A(config-if-VLAN 1)# ip address 192.168.1.1 255.255.255.0
A(config-if-VLAN 1)# exit
A(config)# ip route 192.168.2.0 255.255.255.0 VLAN 1 192.168.1.2
```

B

```
B# configure terminal
B(config)# interface GigabitEthernet 0/1
B(config-if-GigabitEthernet 0/1)# switchport mode trunk
B(config-if-GigabitEthernet 0/1)# exit
B(config)# interface GigabitEthernet 0/2
B(config-if-GigabitEthernet 0/2)# switchport mode trunk
B(config-if-GigabitEthernet 0/2)# exit
B(config)# interface vlan 1
B(config-if-VLAN 1)# ip address 192.168.1.2 255.255.255.0
B(config-if-VLAN 1)# exit
B(config)# interface GigabitEthernet 0/3
B(config-if-GigabitEthernet 0/3)# no switchport
B(config-if-GigabitEthernet 0/3)# ip address 192.168.2.2 255.255.255.0
B(config-if-GigabitEthernet 0/3)# exit
```

C

```
C# configure terminal
C(config)# interface GigabitEthernet 0/1
C(config-if-GigabitEthernet 0/1)# port-group 1
C(config-if-GigabitEthernet 0/1)# exit
```

```

C(config)# interface aggregateport 1
C(config-if-AggregatePort 1)# switchport mode access
C(config-if-AggregatePort 1)# switchport access vlan 1
C(config-if-AggregatePort 1)# exit
C(config)# interface vlan 1
C(config-if-VLAN 1)# ip address 192.168.1.3 255.255.255.0
C(config-if-VLAN 1)# exit

D# configure terminal
D(config)# interface GigabitEthernet 0/1
D(config-if-GigabitEthernet 0/1)# no switchport
D(config-if-GigabitEthernet 0/1)# ip address 192.168.2.1 255.255.255.0
D(config-if-GigabitEthernet 0/1)# exit
A(config)# ip route 192.168.1.0 255.255.255.0 GigabitEthernet 0/1 192.168.2.2

```

【检验方法】 在 A、B、C、D 四台设备上分别进行如下检验：

- A Ping 其它 3 台设备的接口 IP，两两之间可以相互访问。
- B 和 D 互 Ping 能通。
- 检查接口状态是否正确。

```

A# show interfaces gigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is UP , line protocol is UP
Hardware is GigabitEthernet, address is 00d0.f865.de90 (bia 00d0.f865.de90)
Interface address is: no ip address
MTU 1500 bytes, BW 100000 Kbit
Encapsulation protocol is Ethernet-II, loopback not set
Keepalive interval is 10 sec , set
Carrier delay is 2 sec
Ethernet attributes:

Last link state change time: 2012-12-22 14:00:48
Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds
Priority is 0
Admin medium-type is Copper, oper medium-type is Copper
Admin duplex mode is AUTO, oper duplex is Full
Admin speed is AUTO, oper speed is 100M
Flow control admin status is OFF, flow control oper status is OFF
Admin negotiation mode is OFF, oper negotiation state is ON
Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF
Bridge attributes:
Port-type: access
Vlan id: 1
Rxload is 1/255, Txload is 1/255
10 seconds input rate 0 bits/sec, 0 packets/sec
10 seconds output rate 67 bits/sec, 0 packets/sec
362 packets input, 87760 bytes, 0 no buffer, 0 dropped
Received 0 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
363 packets output, 82260 bytes, 0 underruns , 0 dropped
0 output errors, 0 collisions, 0 interface resets

B# show interfaces gigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is UP , line protocol is UP
Hardware is GigabitEthernet, address is 00d0.f865.de91 (bia 00d0.f865.de91)
Interface address is: no ip address
MTU 1500 bytes, BW 100000 Kbit
Encapsulation protocol is Ethernet-II, loopback not set
Keepalive interval is 10 sec , set
Carrier delay is 2 sec

```

```

Ethernet attributes:

  Last link state change time: 2012-12-22 14:00:48
  Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds
  Priority is 0
  Admin medium-type is Copper, oper medium-type is Copper
  Admin duplex mode is AUTO, oper duplex is Full
  Admin speed is AUTO, oper speed is 100M
  Flow control admin status is OFF, flow control oper status is OFF
  Admin negotiation mode is OFF, oper negotiation state is ON
  Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF

Bridge attributes:

  Port-type: trunk
  Native vlan: 1
  Allowed vlan lists: 1-4094
  Active vlan lists: 1
  Rxload is 1/255, Txload is 1/255
  10 seconds input rate 0 bits/sec, 0 packets/sec
  10 seconds output rate 67 bits/sec, 0 packets/sec
  362 packets input, 87760 bytes, 0 no buffer, 0 dropped
  Received 0 broadcasts, 0 runts, 0 giants
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
  363 packets output, 82260 bytes, 0 underruns , 0 dropped
  0 output errors, 0 collisions, 0 interface resets

```

C

```

C# show interfaces gigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is UP , line protocol is UP
Hardware is GigabitEthernet, address is 00d0.f865.de92 (bia 00d0.f865.de92)
Interface address is: no ip address
  MTU 1500 bytes, BW 100000 Kbit
  Encapsulation protocol is Ethernet-II, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  Ethernet attributes:

    Last link state change time: 2012-12-22 14:00:48
    Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds
    Priority is 0
    Admin medium-type is Copper, oper medium-type is Copper
    Admin duplex mode is AUTO, oper duplex is Full
    Admin speed is AUTO, oper speed is 100M
    Flow control admin status is OFF, flow control oper status is OFF
    Admin negotiation mode is OFF, oper negotiation state is ON
    Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF
  Rxload is 1/255, Txload is 1/255
  10 seconds input rate 0 bits/sec, 0 packets/sec
  10 seconds output rate 67 bits/sec, 0 packets/sec
  362 packets input, 87760 bytes, 0 no buffer, 0 dropped
  Received 0 broadcasts, 0 runts, 0 giants
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
  363 packets output, 82260 bytes, 0 underruns , 0 dropped
  0 output errors, 0 collisions, 0 interface resets

```

D

```

D# show interfaces gigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is UP , line protocol is UP
Hardware is GigabitEthernet, address is 00d0.f865.de93 (bia 00d0.f865.de93)
Interface address is: 192.168.2.1/24
  MTU 1500 bytes, BW 100000 Kbit

```



```

Encapsulation protocol is Ethernet-II, loopback not set
Keepalive interval is 10 sec , set
Carrier delay is 2 sec
Ethernet attributes:

  Last link state change time: 2012-12-22 14:00:48

  Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds

  Priority is 0
  Admin medium-type is Copper, oper medium-type is Copper
  Admin duplex mode is AUTO, oper duplex is Full
  Admin speed is AUTO, oper speed is 100M
  Flow control admin status is OFF, flow control oper status is OFF
  Admin negotiation mode is OFF, oper negotiation state is ON
  Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF
  Rxload is 1/255, Txload is 1/255
  10 seconds input rate 0 bits/sec, 0 packets/sec
  10 seconds output rate 67 bits/sec, 0 packets/sec
  362 packets input, 87760 bytes, 0 no buffer, 0 dropped
  Received 0 broadcasts, 0 runts, 0 giants
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
  363 packets output, 82260 bytes, 0 underruns , 0 dropped
  0 output errors, 0 collisions, 0 interface resets


```

常见错误

- 无。

1.5 监视与维护

清除各类信息

 在设备运行过程中执行 **clear** 命令，可能因为重要信息丢失而导致业务中断。

作用	命令
清除接口的统计值。	clear counters [<i>interface-type interface-number</i>]
接口硬件复位。	clear interface <i>interface-type interface-number</i>

查看运行情况

显示接口配置和状态

作用	命令
显示指定接口的全部状态和配置信息。	show interfaces [<i>interface-type interface-number</i>]
显示接口的状态。	show interfaces [<i>interface-type interface-number</i>] status
显示接口违例状态。	show interfaces [<i>interface-type interface-number</i>] status err-disable
查看端口链路状态变化时间和次数。	show interfaces [<i>interface-type interface-number</i>] link-state-change statistics
显示可交换接口（非路由接口）的 administrative 和 operational 状态信息。	show interfaces [<i>interface-type interface-number</i>] switchport
显示指定接口的描述配置和接口状态。	show interfaces [<i>interface-type interface-number</i>] description
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。	show interfaces [<i>interface-type interface-number</i>] counters

显示上一个采样时间间隔内增加的报文统计值。	show interfaces [<i>interface-type interface-number</i>] counters increment
显示错误报文统计值。	show interfaces [<i>interface-type interface-number</i>] counters error
显示接口报文收发速率	show interfaces [<i>interface-type interface-number</i>] counters rate
显示接口简要统计值	show interfaces [<i>interface-type interface-number</i>] counters summary
线缆检测状态显示。在线缆处于短路或断路等异常状态时，线缆检测有助于正确判断线缆的工作状况。	show interfaces [<i>interface-type interface-number</i>] line-detect
显示接口带宽利用率	show interfaces [<i>interface-type interface-number</i>] usage
显示接口 EEE 状态。	show eee interfaces [<i>interface-type interface-number</i>] status

查看调试信息



输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

无。

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。在线缆处于短路或断路等异常状态时，线缆检测有助于正确判断线缆的工作状况。



只有电介质的物理口才支持线缆检测，光介质物理口、聚合端口不支持线缆检测。



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。

作用	命令
在接口模式下执行线缆检测。在线缆处于短路或断路等异常状态时，线缆检测有助于正确判断线缆的工作状况。	line-detect

2 MAC 地址

2.1 概述

MAC 地址表记录了与该设备相连的设备的 MAC 地址、接口号以及所属的 VLAN ID。

设备在转发报文时通过报文的目的 MAC 地址以及报文所属的 VLAN ID 的信息在 MAC 地址表中查找相应的转发输出口。

根据 [mac 地址](#) 查找到转发出口后就可以采取单播、组播或广播的方式转发报文。

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

协议规范

- IEEE 802.3 : Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications
- IEEE 802.1Q : Virtual Bridged Local Area Networks

2.2 典型应用

典型应用	场景描述
动态地址学习	通过动态地址学习，实现报文单播转发
MAC地址变化通知	通过 MAC 地址添加删除通知，监控网络设备下用户变化。

2.2.1 动态地址学习

应用场景

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

设备的 MAC 地址表为空的情况下，UserA 要与 UserB 进行通讯，UserA 首先发送报文到交换机的端口 GigabitEthernet 0/2，此时设备将 UserA 的 MAC 地址学习到 MAC 地址表中。

由于地址表中没有 UserB 的源 MAC 地址，因此设备以广播的方式将报文发送到除了 UserA 以外的所有端口，包括 User B 与 User C 的端口，此时 UserC 能够收到 UserA 所发出的不属于它的报文。

图 2-1 动态地址学习步骤一

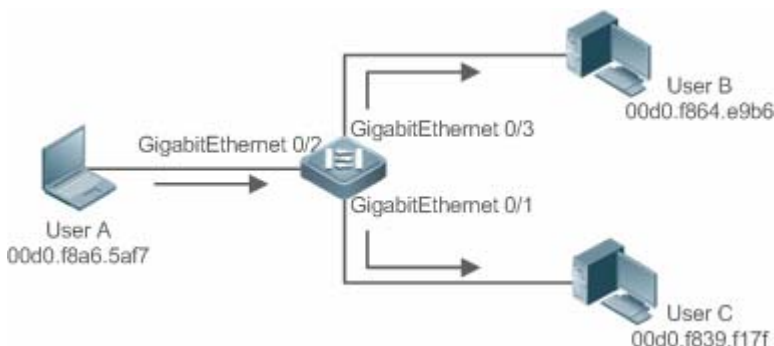


图 2-2 以太网交换 MAC 地址表一

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

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

图 2-3 动态地址学习步骤二

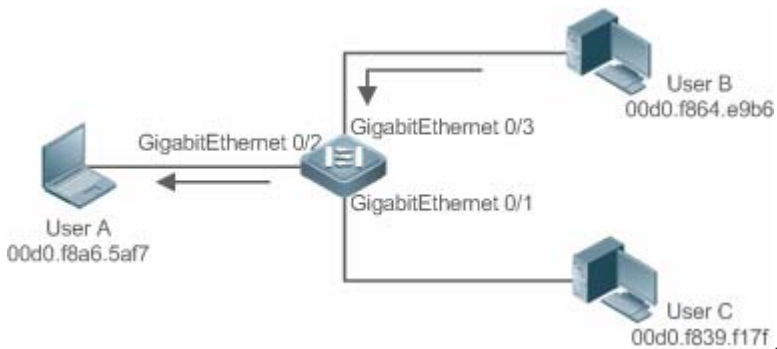


图 2-4 设备 MAC 地址表二

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

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

功能部属

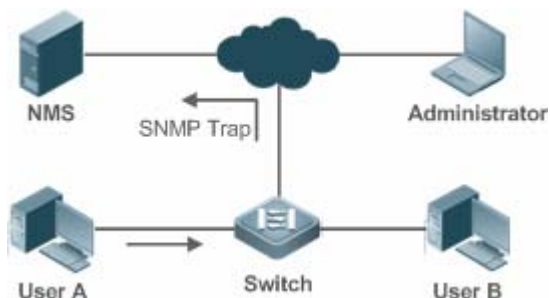
- 二层交换设备通过动态地址学习，实现报文本播转发，减少广播报文，减轻网络不必要的负荷。

2.2.2 MAC 地址变化通知

设备的 MAC 地址通知功能通过与网络管理工作站（NMS）的协作为网络管理提供了监控网络设备下用户变化的机制。

应用场景

图 2-5 MAC 地址通知



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

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

当使用设备下接的用户较多时，可能会出现短时间内会有大量的 MAC 地址变化产生，导致网络流量增加。为了减轻网络负担，可以设置发送 MAC 地址通知的时间间隔。在达到配置的时间间隔之后，系统将这个时间内的所有通知信息进行打包封装，此时在每条地址通知信息中，包含了若干个 MAC 地址变化的信息，从而可以有效地减少网络流量。

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

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

功能部属

- 二层交换设备开启 MAC 地址变化通知，实现监控网络设备下的用户变化。

2.3 功能详解

基本概念

▾ 动态地址

通过设备的自动地址学习过程产生的 MAC 地址表项被称为动态地址。

▾ 地址老化

设备的 MAC 地址表是有容量限制的，设备采用地址表老化机制进行不活跃的地址表项淘汰。

设备在学习到一个新的地址的同时启动该地址的老化记时，在达到老化记时前，如果设备没有再一次收到以该地址为源 MAC 地址的报文，则该地址在达到老化时间后会从 MAC 地址表中删除。

▾ 单播转发

设备能够在 MAC 地址表中查到与报文的源 MAC 地址和 VLAN ID 相对应的表项并且表项中的输出端口是唯一的，报文直接从表项对应的端口输出。

▾ 广播转发

设备收到目的地址为 ffff.ffff.ffff 的报文或者在 MAC 地址表中查找不到对应的表项时，报文被送到所属的 VLAN 中除报文输入端口外的其他所有端口输出。

功能特性

功能特性	作用
VLAN 的动态地址个数限制	用户可规划各个 VLAN 内可学习的动态地址数
接口的动态地址个数限制	用户可规划各个接口下可学习的动态地址数

2.3.1 接口的动态地址个数限制

工作原理

配置了接口的动态地址个数限制功能的接口只能够学到用户所指定个数的 MAC 地址，对超出用户配置上限部份的地址将不再学习，以这些地址为目的地址的报文将以广播方式转发。

i 如果配置接口的动态地址学习个数限制的上限小于当前接口下已学习到的动态地址数，此时设备不再学习该接口下的地址，直到接口下的地址数通过地址老化删除到小于上限后，设备才会重新学习。

2.4 配置详解

配置项	配置建议&相关命令	
配置动态地址	⚠️ 可选配置。用于实现动态地址学习。	
	mac-address-learning	配置全局或接口 MAC 地址学习能力
	mac-address-table aging-time	配置动态地址老化时间
配置静态地址	⚠️ 可选配置。用于绑定设备下接的网络设备的 MAC 地址与端口关系。	
	mac-address-table static	配置静态地址
配置过滤地址	⚠️ 可选配置。用于过滤报文。	
	mac-address-table filtering	配置过滤地址
配置MAC地址变化通知	⚠️ 可选配置。用于监控网络设备下的用户变化。	
	mac-address-table notification	配置全局 MAC 地址变化通知功能
	snmp trap mac-notification	配置接口 MAC 地址变化通知功能

2.4.1 配置动态地址

配置效果

实现动态地址学习，报文正常单播转发。

配置方法

配置全局 MAC 地址学习能力

- 可选配置。
- 如果需要关闭全局 MAC 地址学习能力，则应该执行此配置项。
- 交换机设备上配置。

【命令格式】 **mac-address-learning { enable | disable }**

【参数说明】 **enable**：开启全局 MAC 地址学习能力
disable：关闭全局 MAC 地址学习能力

【缺省配置】 全局地址学习能力开启

【命令模式】 全局模式

【使用指导】 -

i 全局 MAC 地址学习能力缺省开启。当全局 MAC 地址学习能力关闭时，全局无法进行 MAC 地址学习；当全局 MAC 地址学习能力开启时，按端口的 MAC 地址学习能力生效。

配置接口 MAC 地址学习能力

- 可选配置。。
- 如果需要关闭接口 MAC 地址学习能力，则应该执行此配置项。
- 交换机设备上配置。

【命令格式】 **mac-address-learning**

【参数说明】 -

【缺省配置】 地址学习能力开启

【命令模式】 接口模式

【使用指导】 接口必须是二层接口，包括交换口、AP 口。

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

配置动态地址老化时间

- 可选配置。
- 如果需要修改动态地址老化时间，则应该执行此配置项。
- 交换机设备上配置。

【命令格式】 **mac-address-table aging-time value**

【参数说明】 *value*：老化时间。取值范围{ 0 | 10 - 1000000 }，缺省值 300 秒。

【缺省配置】 缺省值是 300 秒

【命令模式】 全局模式

【使用指导】 当设置该值为 0 时，地址老化功能将被关闭，学习到的地址将不会被老化。

- i** 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。

检验方法

- 检查设备是否能正常学习动态地址。
- 通过 **show mac-address-table dynamic** 命令查看动态地址信息。
- 通过 **show mac-address-table aging-time** 命令查看动态地址老化时间。

【命令格式】 **show mac-address-table dynamic [address mac-address] [interface interface-id] [vlan vlan-id]**

【参数说明】 **address mac-address**：查看设备上特定动态 MAC 地址信息。

interface interface-id：指定的物理接口或是 Aggregate Port。

vlan vlan-id：查看特定的 VLAN 中的动态地址。

【命令模式】 特权模式，全局模式，接口模式

【使用指导】 -

【命令展示】

```
Ruijie# show mac-address-table dynamic
Vlan      MAC Address      Type      Interface
-----
1         0000.0000.0001  DYNAMIC  GigabitEthernet 1/1
1         0001.960c.a740   DYNAMIC  GigabitEthernet 1/1
1         0007.95c7.dff9   DYNAMIC  GigabitEthernet 1/1
1         0007.95cf.eee0   DYNAMIC  GigabitEthernet 1/1
1         0007.95cf.f41f   DYNAMIC  GigabitEthernet 1/1
1         0009.b715.d400   DYNAMIC  GigabitEthernet 1/1
1         0050.bade.63c4   DYNAMIC  GigabitEthernet 1/1
```

字段解释：

字段	说明
Vlan	MAC 地址所在的 VLAN
MAC Address	MAC 地址
Type	MAC 地址类型
Interface	MAC 地址所在的接口

【命令格式】 **show mac-address-table aging-time**

【参数说明】 -

【命令模式】 特权模式，全局模式，接口模式

【使用指导】 -

```

【命令展示】 Ruijie# show mac-address-table aging-time
Aging time   : 300

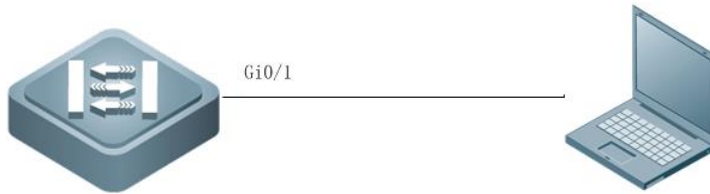
```

配置举例

配置动态地址

【网络环境】

图 2-6



【配置方法】

- 打开接口 MAC 地址学习能力
- 配置动态地址老化时间为 180 秒
- 删除接口 GigabitEthernet 0/1 下 VLAN 1 中的所有动态地址

```

Ruijie# configure terminal
Ruijie(config-if-GigabitEthernet 0/1)# mac-address-learning
Ruijie(config-if-GigabitEthernet 0/1)# exit
Ruijie(config)# mac aging-time 180
Ruijie# clear mac-address-table dynamic interface GigabitEthernet 0/1 vlan 1

```

【检验方法】

- 查看接口 MAC 地址学习能力
- 查询动态地址老化时间
- 查看接口 GigabitEthernet 0/1 下 VLAN 1 中的所有动态地址

```

Ruijie# show mac-address-learning
GigabitEthernet 0/1   learning ability: enable
Ruijie# show mac aging-time
Aging time   : 180 seconds
Ruijie# show mac-address-table dynamic interface GigabitEthernet 0/1 vlan 1
Vlan          MAC Address          Type          Interface
-----
1             00d0.f800.1001      STATIC       GigabitEthernet 1/1

```

常见错误

配置接口地址学习能力时，接口没有先配置成二层接口，包括交换口、AP 口。

2.4.2 配置静态地址

配置效果

- 配置静态地址，绑定设备下接的网络设备的 MAC 地址与端口关系。

配置方法

配置静态地址

- 可选配置。。
- 如果需要绑定设备下接的网络设备的 MAC 地址与端口关系，则应该执行此配置项。
- 交换机设备上配置。

【命令格式】 **mac-address-table static** mac-address vlan *vlan-id* **interface** interface-id

【参数说明】 **address** mac-address：指定要删除的 MAC 地址
vlan vlan-id：指定要删除的 MAC 地址所在的 VLAN。

interface*interface-id* : 指定的物理接口或是 Aggregate Port。

【缺省配置】 缺省没有设置任何静态地址

【命令模式】 全局模式

【使用指导】 当设备在 *vlan-id* 指定的 VLAN 上接收到以 *mac-address* 为目的地址的报文时，这个报文将被转发到 *interface-id* 所指定的接口上。

检验方法

- 通过命令 **show mac-address-table static** 显示静态地址信息是否正确。

【命令格式】 **show mac-address-table static [address***mac-address* **] [interface***interface-id* **] [vlan***vlan-id* **]**

【参数说明】 **address***mac-address* : 查看设备上特定静态 MAC 地址信息。

interface*interface-id* : 指定的物理接口或是 Aggregate Port。

vlan*vlan-id* : 查看特定的 VLAN 中的静态地址。

【命令模式】 特权模式，全局模式，接口模式

【使用指导】 -

【命令展示】

```
Ruijie#show mac-address-table static
Vlan    MAC Address    Type    Interface
-----
1       00d0.f800.1001  STATIC  GigabitEthernet 1/1
1       00d0.f800.1002  STATIC  GigabitEthernet 1/1
1       00d0.f800.1003  STATIC  GigabitEthernet 1/1
```

配置举例

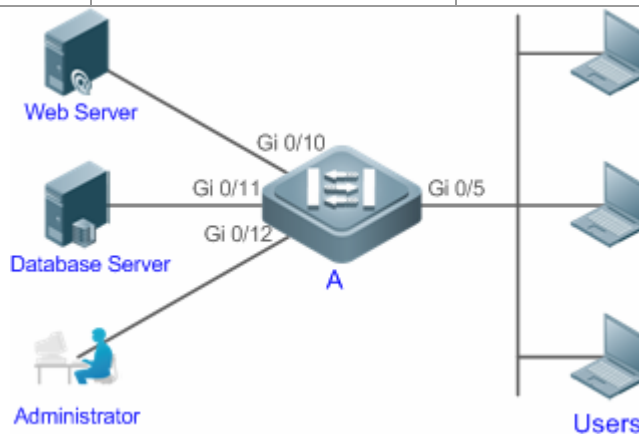
配置静态地址

本例的 MAC 地址同 VLAN、接口对应关系如下表所示：

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

【网络环境】

图 2-7



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

A

```
A# configure terminal
A(config)# mac-address-table static 00d0.f800.3232.0001 vlan 2 interface gigabitEthernet 0/10
A(config)# mac-address-table static 00d0.f800.3232.0002 vlan 2 interface gigabitEthernet 0/11
A(config)# mac-address-table static 00d0.f800.3232.1000 vlan 2 interface gigabitEthernet 0/12
```

【检验方法】 在交换机上查看配置的静态 MAC 地址

A

```
A# show mac-address-table static
Vlan      MAC Address      Type      Interface
-----
2         00d0.f800.3232.0001  STATIC   GigabitEthernet 0/10
2         00d0.f800.3232.0002  STATIC   GigabitEthernet 0/11
2         00d0.f800.3232.1000  STATIC   GigabitEthernet 0/12
```

常见错误

- 配置静态地址时，指定接口没有先配置成二层接口，包括交换口、AP 口。

2.4.3 配置过滤地址

配置效果

- 配置过滤地址，当在对应 VLAN 中接收到源 MAC 或目的 MAC 为过滤地址的报文时，将丢弃此报文。

配置方法

配置过滤地址

- 可选配置。。
- 如果需要过滤报文，则应该执行此配置项。
- 交换机设备上配置。

【命令格式】 **mac-address-table filtering** *mac-address* **vlan** *vlan-id*

【参数说明】 **address***mac-address*：指定要删除的 MAC 地址
vlan*vlan-id*：指定要删除的 MAC 地址所在的 VLAN。

【缺省配置】 缺省没有设置任何过滤地址

【命令模式】 全局模式

【使用指导】 当设备在 *vlan-id* 指定的 VLAN 上接收到以 *mac-address* 指定的地址为源地址或目的地址的报文将被丢弃。

检验方法

- 通过命令 **show mac-address-table filter** 显示过滤地址信息。

【命令格式】 **show mac-address-table filter** [**address***mac-address*] [**vlan***vlan-id*]

【参数说明】 **address***mac-address*：查看设备上特定过滤 MAC 地址信息。
vlan*vlan-id*：查看特定的 VLAN 中的过滤地址。

【命令模式】 特权模式，全局模式，接口模式

【使用指导】 -

【命令展示】

```
Ruijie#show mac-address-table filtering
Vlan      MAC Address      Type      Interface
-----
1         0000.2222.2222   FILTER
```

配置举例

配置过滤地址

- 【配置方法】
- 指定过滤地址对应的目的 MAC 地址 (*Mac-address*)
 - 指定过滤地址所属的 VLAN (*vlan-id*)

```
Ruijie# configure terminal
```

```
Ruijie(config)# mac-address-table static 00d0.f800.3232.0001 vlan 1
```

【检验方法】 在交换机上查看配置的过滤 MAC 地址

```
Ruijie# show mac-address-table filter
Vlan      MAC Address      Type      Interface
-----
1         00d0.f800.3232.0001  FILTER
```

常见错误

无。

2.4.4 配置 MAC 地址变化通知

配置效果

- 配置 MAC 地址变化通知，监控网络设备下的用户变化。

配置方法

配置接收 MAC 地址通知的 NMS

- 可选配置。
- 如果需要接收 MAC 地址通知，则应该执行此配置项。
- 交换机设备上配置。

【命令格式】 **snmp-server host** *host-addr* **traps** [**version** { 1 | 2c | 3 [**auth** | **noauth** | **priv**] }] *community-string*

【参数说明】 **host** *host-addr* : 指明接收者的 IP。

version { 1 | 2c | 3 [**auth** | **noauth** | **priv**] } : 指明发送哪种版本的 snmp trap 报文，对 v3 版本还可以指定是否认证以及安全等级参数。

community-string : 认证名

【缺省配置】 缺省不需要配置

【命令模式】 全局模式

【使用指导】 -

配置使能发送 Trap 功能

- 可选配置。
- 如果需要发送 Trap，则应该执行此配置项。
- 交换机设备上配置。

【命令格式】 **snmp-server enable traps**

【参数说明】 -

【缺省配置】 缺省不需要配置

【命令模式】 全局模式

【使用指导】 -

配置全局 MAC 地址通知开关

- 可选配置。
- 全局开关被关闭，所有接口的 MAC 地址通知功能也均被关闭。
- 交换机设备上配置。

- 【命令格式】 **mac-address-table notification**
- 【参数说明】 -
- 【缺省配置】 缺省全局 MAC 地址变化通知开关关闭
- 【命令模式】 全局模式
- 【使用指导】 -

配置接口 MAC 地址通知开关

- 可选配置
- 如果需要接收接口 MAC 地址变化通知，则应该执行此配置项。
- 交换机设备上配置。

- 【命令格式】 **snmp trap mac-notification { added | removed }**
- 【参数说明】 **added**：当地址增加时通知。
removed：当地址被删除时通知。
- 【缺省配置】 缺省接口 MAC 地址变化通知开关关闭
- 【命令模式】 接口模式
- 【使用指导】 -

配置 MAC 地址通知的时间间隔与历史记录容量

- 可选配置。
- 如果需要修改 MAC 地址通知的时间间隔或历史记录容量，则应该执行此配置项。
- 交换机设备上配置。

- 【命令格式】 **mac-address-table notification { interval value | history-size value }**
- 【参数说明】 **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。
- 【缺省配置】 时间间隔缺省为 1 秒，表项默认通告的最大通告个数为 50。
- 【命令模式】 全局模式
- 【使用指导】 -

检验方法

- 通过命令 **show mac-address-table notification** 检查 NMS 是否能正常接收 MAC 地址变化通知。

- 【命令格式】 **show mac-address-table notification [interface[interface-id]] history]**
- 【参数说明】 **interface**：显示全部接口上的 MAC 通知功能设置。
interface-id：查看接口的 MAC 地址变化通知的使能状况。
history：查看 MAC 地址变化通知信息的历史记录表。
- 【命令模式】 特权模式，全局模式，接口模式
- 【使用指导】 -
- 【使用指导】 1、查看 MAC 地址通告功能的全局配置信息

```
Ruijie#show mac-address-table notification
MAC Notification Feature : Enabled
Interval(Sec): 300
Maximum History Size : 50
Current History Size : 0
```

字段解释：

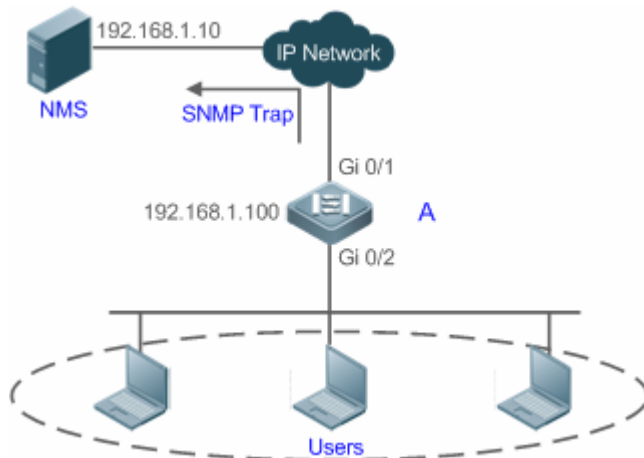
字段	说明
Interval(Sec)	通告 MAC 地址的时间间隔

Maximum History Size	MAC 地址通告历史记录表的最大表项个数
Current History Size	当前记录条目数

配置举例

【网络环境】

图 2-8



图为某企业内部网络示意图。下联用户通过 Gi0/2 口连接到交换机。

为了便于管理员对下联用户使用网络情况信息的掌控，希望通过配置达到以下目的：

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

【配置方法】

- 打开交换机全局 MAC 地址通知开关，在 Gi0/2 接口上配置 MAC 地址通知功能。
- 配置 NMS 主机地址，使能交换机主动发送 SNMP Trap 通知。交换机到 NMS（网络管理工作站）的路由可达。
- 设置交换机发送 MAC 地址通知的时间间隔为 300 秒（默认时间间隔为 1 秒）。

A

```
Ruijie# configure terminal
Ruijie(config)# mac-address-table notification
Ruijie(config)# interface gigabitEthernet 0/2
Ruijie(config-if-GigabitEthernet 0/2)# snmp trap mac-notification added
Ruijie(config-if-GigabitEthernet 0/2)# snmp trap mac-notification removed
Ruijie(config-if-GigabitEthernet 0/2)# exit
Ruijie(config)# snmp-server host 192.168.1.10 traps version 2c comefrom2
Ruijie(config)# snmp-server enable traps
Ruijie(config)# mac-address-table notification interval 300
```

【检验方法】

- 查看 MAC 地址通知功能的全局配置信息。
- 查看接口的 MAC 地址变化通知的使能状况。
- 查看接口 MAC 地址表，并使用使用 **clear mac-address-table dynamic** 命令模拟动态地址的老化。
- 查看 MAC 地址通知功能的全局配置信息。
- 查看 MAC 地址变化通知信息的历史记录表。

A

```
Ruijie# show mac-address-table notification
MAC Notification Feature : Enabled
Interval(Sec): 300
Maximum History Size : 50
Current History Size : 0
Ruijie# show mac-address-table notification interface GigabitEthernet 0/2
```

```

Interface                MAC Added Trap    MAC Removed Trap
-----
GigabitEthernet 0/2     Enabled           Enabled
Ruijie# show mac-address-table interface GigabitEthernet 0/2
Vlan          MAC Address      Type      Interface
-----
1             00d0.3232.0001   DYNAMIC   GigabitEthernet 0/2
Ruijie# show mac-address-table notification
MAC Notification Feature : Enabled
Interval(Sec): 300
Maximum History Size : 50
Current History Size : 1
Ruijie# show mac-address-table notification history
History Index : 0
Entry Timestamp: 221683
MAC Changed Message :
Operation:DEL Vlan:1 MAC Addr: 00d0.3232.0003 GigabitEthernet 0/2


```

常见错误

无。

2.5 监视与维护

清除各类信息

 在设备运行过程中执行 **clear** 命令，可能因为重要信息丢失而导致业务中断。

作用	命令
清除动态地址表项。	clear mac-address-table dynamic [address <i>mac-address</i>] [interface <i>interface-id</i>] [vlan <i>vlan-id</i>]

查看运行情况

作用	命令
查看 MAC 地址表。	show mac-address-table { dynamic static filter } [address <i>mac-address</i>] [interface <i>interface-id</i>] [vlan <i>vlan-id</i>]
查看动态地址老化时间	show mac-address-table aging-time
查看地址变化通知配置及历史记录表	show mac-address-table notification [interface <i>interface-id</i>] [history]

查看调试信息

 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
打开 MAC 运行情况的调试开关。	debug bridge mac

3 Aggregate Port

3.1 概述

Aggregate Port (简称 AP) 是将多个物理链接捆绑在一起形成一个逻辑链接, 可以用于扩展链路带宽, 提供更高的连接可靠性。

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

比如两台设备之间, 单个端口相连最多为 1000M (假定两台设备的端口都为 1000M), 当该链路上承载的业务流量超过 1000M 时, 超过的部分就会被丢弃, 而端口聚合将可以解决这一问题。例如, 使用若干根网线连接这两台设备, 再将这若干个端口进行聚合绑定, 这样这些端口就逻辑捆绑形成了 $1000M * n$ 的最大流量。

又比如, 如果两台设备是通过单个网线相连接, 当这两个端口之间出现链路断开时, 这条链路上承载的业务就会断掉, 而如果将若干个互连的端口进行聚合绑定, 只要有一条链路没有出现链路断开, 那么在那些端口上承载的业务就不会断掉。

i 下文仅介绍 AP 的相关内容。

协议规范

- IEEE 802.3ad

3.2 典型应用

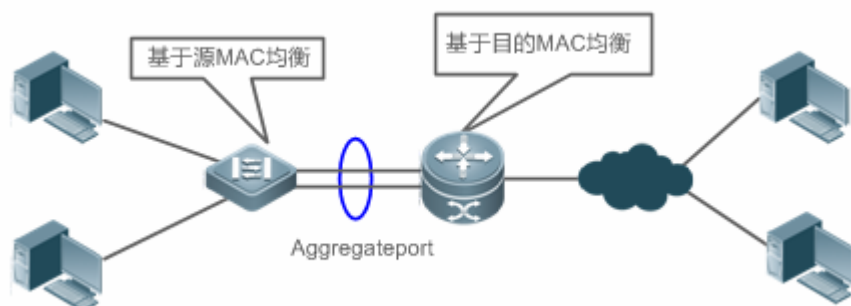
典型应用	场景描述
AP链路聚合及流量平衡	汇聚和核心设备之间通常存在大量报文流, 需要更大的端口带宽来支撑, 这时候就可以把设备上多条物理链路聚合成一条逻辑链路, 增大链路带宽, 并通过配置适当的流量平衡算法, 使聚合口上的报文尽可能平衡到每一条物理链路, 以提高带宽利用率。

3.2.1 AP链路聚合及流量平衡

应用场景

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

图 3-1 AP 链路聚合及流量平衡示意图



【注释】

功能部属

- 把交换机与路由器之间的直连端口配置成一个静态 AP 或 LACP
- 在交换机上设置基于源 MAC 的流量平衡算法
- 在路由器上设置基于目的 MAC 的流量平衡算法

3.3 功能详解

基本概念

▾ 静态 AP

静态 AP 模式是一种利用手工配置模式直接将物理端口加入到 AP 聚合组中，在物理端口的链路状态和协议状态准备好的情况下，就能进行数据报文转发的一种聚合模式。

静态 AP 模式下的 AP 接口，称为静态 AP 口，对应的成员口称为静态 AP 成员口。

▾ LACP

LACP 是一个关于动态链路聚合的协议，它通过协议报文 LACPDU(Link Aggregation Control Protocol Data Unit，链路聚合控制协议数据单元)和相连的设备交互信息。

LACP 模式下的 AP 接口，称为 LACP AP 口，对应的成员口称为 LACP AP 成员口。

▾ AP 成员端口模式

AP 成员端口有 3 种聚合模式：主动(Active)模式、被动模式(Passive)和静态模式。

其中主动模式的端口会主动发起 LACP 报文协商；被动模式的端口则只会对收到的 LACP 报文做应答；静态模式不会发出 LACP 报文进行协商，这种模式只会在静态 AP 模式下生效。各个聚合模式的相邻端口聚合模式要求如下：

端口模式	相邻端口聚合模式要求
主动模式	主动模式或者被动模式
被动模式	主动模式
静态模式	静态模式

▾ AP 成员端口状态

静态 AP 成员端口的状态主要有以下两种：



- 当成员端口的链路处于 Down 状态，端口不能转发任何数据报文，显示为“Down”状态；
- 当成员端口链路处于 Up 状态，且链路协议准备好后，端口可以参与转发数据报文，显示为“Up”状态。

LACP 成员端口可能处于以下三种状态：

- 当端口的链路处于 Down 状态，端口不能转发任何数据报文，显示为“down”状态；
- 端口链路处于 Up 状态，并经过 LACP 协商后，端口被置于聚合状态(端口被作为一个聚合组的一个成员，参与聚合组的数据报文转发)，显示为“bndl”状态；
- 当端口链路处于 UP 状态，但是由于对端没有启用 LACP，或者因为端口属性和主端口不一致等一些因素导致经过报文协商端口被置于挂起状态（处于挂起状态的端口不参与数据报文转发），显示为“susp”状态。

i 只有全双工的端口才能进行 LACP 聚合。

i 成员端口的速率、流控、介质类型以及成员端口的二、三层属性必须一致才能进行 LACP 聚合绑定。

-  LACP 成员端口聚合后修改端口的上述属性将导致同聚合组内的其他端口也无法进行 LACP 聚合绑定。
-  已经启用禁止成员口加入或者退出 AP 功能的端口不能将端口加入静态 AP 或者 LACP AP, 或者从静态 AP 或者 LACP AP 中退出。

AP 容量模式

由于系统中总的成员口数量有限制，系统总支持成员口数 = 系统支持的最大 AP 口数量 * 单个 AP 口支持最大成员口数。因此当希望系统中最大 AP 口数量大一点，那么单个 AP 口下的最大成员口数就会小一点，反过来单个 AP 最大成员口数大一点，全局最大 AP 数量就小一点。某些特定的场景有这种需求，这就引出了 AP 容量模式的概念，在某些产品设备上支持 AP 容量模式可配置，比如系统支持 16384 个成员口，那么容量模式可以选择 1024*16、512*32 等等（最大 AP 数*单个 AP 下最大成员口数）。

LACP 的系统 ID

每台设备仅能配置一个 LACP 聚合系统。聚合系统有一个系统 ID 来标示这个系统的优劣，同时存在一个系统优先级，这是一个可配置的数值。系统 ID 由 LACP 的系统优先级和设备 MAC 地址组成。系统优先级越小，系统 ID 的优先级越高；在系统优先级相同的情况下，比较设备的 MAC 地址，设备 MAC 地址越小，系统 ID 的优先级越高。系统 ID 优先级较高的系统决定端口状态，低优先级系统的端口状态随高优先级系统的端口状态变化而变化。

LACP 的端口 ID


每个端口有独立的 LACP 端口优先级，这是一个可配置的数值。端口 ID 由 LACP 的端口优先级和端口号组成。端口优先级数值越小，端口 ID 的优先级越高；在端口优先级相同的情况下，端口号越小，端口 ID 的优先级越高。

LACP 的主端口


当有动态成员处于 Up 状态时，LACP 会根据端口的速率，双工速率等关系，并综合聚合组内端口 ID 优先级、聚合组内已经 Up 的成员口的绑定状态等信息，选择其中的一个成员口端口作为主端口。只有和主端口属性相同的端口才能处于聚合状态，参与聚合组的数据转发。当端口的属性变化时，LACP 会重新选择主端口；当新的主端口不处于聚合状态时，LACP 会把同一个聚合组内的成员解聚合，重新聚合。

AP 优选口

通常用在 AP 口同服务器双系统对接的场景下。通过指定 AP 的某个成员为优选口，使得特定报文（管理 vlan 的报文）经优选口转发至服务器，而不会被流量均衡到其他成员口，保障了同服务器间的正常通信。

-  请将连接服务器管理网卡的端口设置为 AP 优选口。

在某些 Linux 服务器上存在双系统，比如 HP 服务器存在主系统和远程管理系统，主系统也就是 Linux 系统，远程管理系统，即 ILO(Integrated Light-Out)，提供硬件级的远程管理功能。ILO 即使在主系统重启的过程中，依然能对服务器进行远程管理。主系统双网卡绑定成聚合口，用于主系统业务处理；管理系统使用其中一张网卡做远程管理，也就是两个系统复用了一张网卡，但业务由不同 VLAN 隔离开，管理系统所用的 VLAN 我们称为管理 VLAN。这样对于交换机设备来说，和服务器双网卡对接的也会是一个聚合口，这个聚合口上管理 VLAN 的报文就需要往同服务器网卡相连的那个成员口发出，这样才能保证与服务服务器上远程管理系统正常通信。为此，可以通过配置 AP 优选口来指定管理 VLAN 报文的转发。

-  若服务器双网卡使用 LACP 绑定，当主系统重启时，LACP 协议还未运行，设备上 LACP 协议处于协商失败的状态，聚合口会处于 Down 状态，这时 AP 优选口会自动降为静态成员口，直接绑定到聚合口，以便聚合口能够服务器远程管理系统保持通信，直到 Linux 系统重启完成，LACP 协议正常运行之后，设备上 AP 优选口重新启用 LACP 协议进行协商。

功能特性

功能特性	作用
链路聚合	将物理链路通过静态或动态的方式聚合，以达到扩展带宽、链路备份的作用。
流量平衡	通过不同的流量均衡模式，可以灵活地对聚合组内流量进行负载均衡。

3.3.1 链路聚合

工作原理

AP 链路聚合方式分为两种，一种是通过手工配置，即静态 AP；另一种是通过 LACP 协议动态聚合。

- 静态 AP

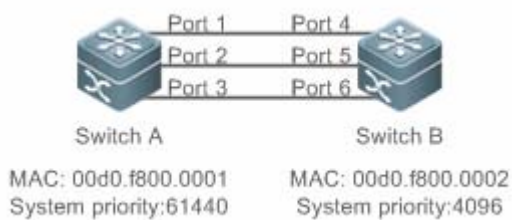
静态 AP 实现简单，用户只要将指定的物理端口通过配置命令加入到同一个聚合组 AP 中，就可以实现多条物理链路的聚合。成员端口一旦加入聚合组后，即可参与 AP 聚合组的数据收发功能，并参与聚合组的流量均衡。

- 动态 AP(LACP)

如果端口启用 LACP 协议，端口会发送 LACPDU 来通告自己的系统优先级、系统 MAC、端口的优先级、端口号和操作 key 等。相连设备收到对端的 LACP 报文后，根据报文中的系统 ID 比较两端的系统优先级。在系统 ID 优先级较高的一端，将按照端口 ID 优先级从高到低的顺序，设置聚合组内端口处于聚合状态，并发出更新后的 LACP 报文，对端设备收到报文后，也会把相应的端口设置成聚合状态，从而使双方在端口退出或者加入聚合组上达到一致。只有双方的端口都完成动态聚合绑定操作后，该物理链路才能进行数据报文的转发。

LACP 成员口链路绑定之后，还会进行周期性的 LACP 报文交互，在一段时间没有收到 LACP 报文时，就认为收包超时，成员口链路解除绑定，端口重新处于不可转发状态。这里的超时时间有两种模式：长超时模式和短超时模式。在长超时模式下，端口间隔 30 秒发送一个报文，若 90 秒没有收到对端报文，就处于收包超时；在短超时模式下，端口间隔 1 秒发送一个报文，若 3 秒钟没有收到对端报文，就处于收包超时。

图 3-2LACP 协商



如上图所示，交换机 A 和交换机 B 通过 3 个端口连接在一起。设置交换机 A 的系统优先级为 61440，设置交换机 B 的系统优先级为 4096。在交换机 A 和 B 的 3 个直连端口上打开 LACP 链路聚合，设置 3 个端口的聚合模式为主动模式，设置 3 个端口的端口优先级为默认优先级 32768。

在收到对端的 LACP 报文后，交换机 B 发现自己的系统 ID 优先级比较高(交换机 B 的系统优先级比交换机 A 高)，于是按照端口 ID 优先级的顺序(端口优先级相同的情况下，按照端口号从小到大的顺序)设置端口 4、5、6 处于聚合状态。交换机 A 收到交换机 B 更新后的 LACP 报文后，发现对端的系统 ID 优先级比较高，并且把端口设置成聚合状态了，也把端口 1、2、3 设置成聚合状态了。

3.3.2 流量平衡

工作原理

AP 可以根据报文的源 MAC 地址、目的 MAC 地址、源 IP 地址、目的 IP 地址、L4 层源端口、L4 层目的端口号等报文特征信息，进行一种或几种组合模式算法对报文流进行区分，将属于同一报文流从同一条成员链路通过，不同的报文流则平均分配到各个成员链路中。例如，采用源 MAC 地址流量平衡模式，会根据报文的源 MAC 地址将报文分配到 AP 的各个成员链路上。不同源 MAC 的报文，根据源 MAC 地址在各成员链路间平衡分配；相同源 MAC 的报文，固定从同一个成员链路转发。


目前可支持的 AP 流量平衡模式如下：

- 源 MAC 或目的 MAC 地址
- 源 MAC+目的 MAC 地址
- 源 IP 地址或目的 IP 地址
- 源 IP 地址+目的 IP 地址
- L4 层源端口或 L4 层目的端口
- L4 层源端口+L4 层目的端口
- 源 IP+L4 层源端口
- 源 IP+L4 层目的端口
- 目的 IP+L4 层源端口
- 目的 IP+L4 层目的端口
- 源 IP+L4 层源端口+L4 层目的端口
- 目的 IP+L4 层源端口+L4 层目的端口
- 源 IP+目的 IP+L4 层源端口
- 源 IP+目的 IP+L4 层目的端口
- 源 IP+目的 IP+L4 层源端口+L4 层目的端口
- 输入报文的面板端口
- 聚合链路成员口轮询均衡
- 增强模式

- i** 根据报文的 IP 地址或端口号进行流量平衡的模式仅适用于三层报文，如果在此流量平衡模式下收到二层报文，则自动根据设备的默认方式进行流量平衡。
- i** 各种流量平衡模式都是利用流量算法（哈希算法）、根据该模式采用的输入参数（源 MAC、目的 MAC、源 MAC+目的 MAC、源 IP、目的 IP、源 IP+目的 IP、源 ip+目的 ip 和 L4 端口号等）计算特定报文应选择的成员链路，来实现流量均衡。这种算法能够保证输入参数不同的报文被大致均衡地分配给各成员链路，但并不意味着，输入参数不同的报文就一定选择不同的成员链路。比如，对 IP 模式而言，两个具有不同源 IP+目的 IP 地址的报文，通过计算可能分配到同一个 AP 的成员链路。
- i** 不同产品，流量均衡支持度可能存在差异。

3.4 配置详解

配置项	配置建议&相关命令	
配置静态AP	! 必须配置。用于手工设置链路聚合。	
	interface aggregateport	创建一个以太网 AP 口。
	port-group	配置以太网静态 AP 成员口。
配置AP的容量模式	! 可选配置。用于指定当前系统的 AP 容量模式。	
	aggregateport capacity mode	设置全局 AP 容量模式。
配置LACP	! 必须配置。用于动态设置链路聚合。	
	lACP system-priority	配置 LACP 系统的优先级。
	lACP port-priority	配置端口的优先级。
配置AP的LinkTrap功能	! 可选配置。用于打开接口的 LinkTrap 通告功能。	
	lACP short-timeout	配置端口为短超时模式

	aggregateport member linktrap	打开发送 AP 成员口 LinkTrap 通告功能。
配置流量平衡模式	 可选配置。用于指定当前聚合链路的流量均衡模式。	
	aggregateport load-balance	设置 AP 的全局或单个 AP 口流量平衡算法。

3.4.1 配置静态AP

配置效果

- 通过手工添加 AP 口成员，将多个物理端口绑定，以实现链路聚合。
- 聚合后的逻辑链路带宽是成员链路带宽的总和。
- 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。

注意事项

- 只有物理端口才允许加入 AP 口。
- 不同介质类型或者不同端口类型的接口不允许加入同一个 AP 口。
- 二层端口只能加入二层 AP，三层端口只能加入三层 AP；包含成员口的 AP 口不允许改变二层/三层属性。
- 一个端口加入 AP，端口的属性将被 AP 的属性所取代。
- 一个端口从 AP 中删除，则端口的属性将恢复为加入 AP 前的属性。

! 当一个端口加入 AP 后，该端口的属性取代为 AP 口的属性，所以一般情况下不允许在 AP 成员口上进行配置，或者将配置单独生效到 AP 成员口上。但一些少数的命令或者功能，如 shutdown 和 no shutdown 配置命令等，这些仍然可以支持在 AP 成员口上配置，且配置能生效。所以用户在使用 AP 成员口的时候，需要根据具体的功能要求来确定是否支持单独在 AP 成员口上生效，并进行正确配置。

配置方法

创建以太网 AP 口

- 必须配置。
- 在支持 AP 功能的设备上配置。以太网口使用聚合功能时需要创建对应的以太网 AP 口。

【命令格式】 `interface aggregateport ap-number`

【参数说明】 `ap-number`：AP 接口编号

【缺省配置】 缺省情况下，AP 口未被创建。

【命令模式】 全局配置模式

【使用指导】 在全局配置模式下，用户可以通过 `interfaces aggregateport` 配置命令创建一个以太网 AP 口。用户可以在全局配置模式下，通过 `no interfaces aggregateport ap-number` 删除指定的以太网 AP 口。

- i** 用户可以通过在指定以太网端口的接口模式下，执行 `port-group` 命令将物理端口加入一个静态 AP；如果该 AP 不存在，则同时自动创建这个 AP 口。
- i** 用户也可以通过在指定物理端口的接口模式下，执行 `port-group mode` 命令将物理端口加入一个 LACP AP；如果该 AP 不存在，则同时自动创建这个 AP 口。
- i** 配置 AP 功能时，需要在链路两端的设备上都配置，且需要配置相同的 AP 类型(静态 AP 或者 LACP)。
- i** ，因此二者的聚合总量需符合交换机本身的限制。

配置以太网静态 AP 成员口

- 必须配置。
- 在支持 AP 功能的设备上配置。使用静态聚合功能时需要配置对应的静态 AP 成员口。

【命令格式】 `port-group ap-number`

- 【参数说明】 **port-group** *ap-number*: AP 接口编号
- 【缺省配置】 以太网端口不属于任何静态 AP 的成员口
- 【命令模式】 以太网接口配置模式
- 【使用指导】 在接口模式下，用户可以通过 **port-group** 配置命令向 AP 口中添加成员口。在接口配置模式下使用 **no port-group** 命令将此成员口退出 AP。

- ❗ 为保证链路聚合功能正常，在链路两端的设备上需要对称配置静态 AP 成员口。
- ❗ 将普通端口加入某个 AP 口后，当该端口再次从 AP 口退出时，普通端口上的原先相关的配置可能会恢复为缺省的配置。不同功能对 AP 口的成员的原有配置的处理方式有所不同，因此建议在端口从 AP 口退出后，应查看并确认端口的配置。
- ❗ AP 成员端口从 AP 口退出变成普通端口后，该端口会被 **shutdown** 以防止出现环路等问题，用户需要在确认拓扑无异常之后再接口模式下执行 **no shutdown** 命令重新使能该接口。
- ❗ 为保证链路聚合功能正常，在链路两端的设备上需要对称配置 FC 静态 AP 成员口。

📌 二层 AP 与三层 AP 的转化

- 为可选配置。
- 如果需要启用 AP 口的三层路由等功能，比如需要在 AP 口上配置 IP 地址，或者配置静态路由表项等，需要先将二层 AP 口转化为三层 AP 口，再在三层 AP 口上启用路由等功能。
- 该功能可在三层交换机或者无线 AC 等支持二、三层功能和 AP 功能的设备上配置。

- 【命令格式】 **no switchport**
- 【参数说明】 -
- 【缺省配置】 在支持二、三层功能和接口二、三层转换功能的设备上，AP 口缺省为二层口。
- 【命令模式】 AP 接口配置模式
- 【使用指导】 L3 AP 是三层设备才支持的功能，所有二层设备均不支持。

- ❗ 对于三层设备，如果该设备不支持二层功能，AP 口被创建时，则是一个三层 AP 口，否则 AP 口被创建时是一个二层 AP 口。

📌 创建以太网 AP 子接口

- 可选配置。
- 如果设备支持配置子接口的功能，则也同时支持在 AP 口上通过 **interface aggregateport sub-ap-number** 创建相应的子接口。
- 该功能可在三层交换机等支持三层功能和 AP 功能的设备上配置。

- 【命令格式】 **interface aggregateport sub-ap-number**
- 【参数说明】 *sub-ap-number*: AP 子接口编号
- 【缺省配置】 缺省 AP 口没有任何子接口。
- 【命令模式】 AP 接口配置模式
- 【使用指导】 在支持二、三层功能和接口二、三层转换功能的设备上，AP 口主接口需要先转换为三层口，才允许该 AP 口主接口创建子接口。

检验方法

- 通过 **show running** 命令查看相应的配置。
 - 通过 **show aggregateport summary** 命令查看 AP 口配置情况。
- 【命令格式】 **show aggregateport aggregate-port-number [load-balance | summary]**
- 【参数说明】 *aggregate-port-number*: AP 接口号
- load-balance**: 显示 AP 的流量平衡算法

summary : 显示 AP 中的每条链路的摘要信息

【命令模式】 各模式均可执行

【使用指导】 如果没有指定 AP 接口号，则所有 AP 的信息将被显示出来

【命令展示】

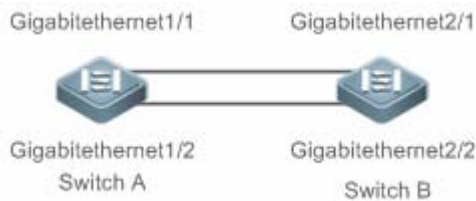
```
Ruijie# show aggregateport 1 summary
AggregatePort MaxPorts SwitchPort Mode      Load balance      Ports
-----
Ag18          Enabled ACCESSdst-macGi0/2
```

配置举例

配置以太网静态 AP

【网络环境】

图 3-3



【配置方法】

- 将 SwitchA 上的端口 GigabitEthernet 1/1 和 GigabitEthernet 1/2 加入到静态 AP 3 中。
- 将 SwitchB 上的端口 GigabitEthernet 2/1 和 GigabitEthernet 2/2 加入到静态 AP 3 中。

SwitchA

```
SwitchA#configure terminal
SwitchA(config)#interface range GigabitEthernet 1/1-2
SwitchA(config-if-range)# port-group 3
```

SwitchB

```
SwitchB#configure terminal
SwitchB(config)#interface range GigabitEthernet 2/1-2
SwitchB(config-if-range)# port-group 3
```

【检验方法】

- 通过 **show aggregateport summary** 查看 AP 口和成员口的对应关系是否正确。

SwitchA

```
SwitchA#show aggregateport summary
AggregatePort MaxPorts SwitchPort Mode      Ports
```

```
Ag3          8      Enabled  ACCESS Gi1/1, Gi1/2
```

SwitchB

```
SwitchB#show aggregateport summary
AggregatePort MaxPorts SwitchPort Mode      Ports
```

```
Ag3          8      Enabled  ACCESS Gi2/1, Gi2/2
```

常见错误

-

3.4.2 配置LACP

配置效果

- 相连设备根据 LACP 自协商，动态聚合链路。
- 聚合后的逻辑链路带宽是成员链路带宽的总和。
- 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。
- 长超时模式时，链路故障后 90 秒才能感知到；配置短超时模式时，3 秒钟就能感知到。

注意事项

- 将普通端口加入某个 LACP AP 口后, 当该端口再次从 LACP AP 口退出时, 普通端口上的原先相关的配置可能会恢复为缺省的配置。不同功能对 LACP AP 口的成员的原有配置的处理方式有所不同, 因此建议在端口从 LACP AP 口退出后, 应查看并确认端口的配置。
- 改变 LACP 的系统优先级可能引起 LACP 的成员端口出现解聚合再聚合现象。
- 改变 LACP 成员口的端口优先级可能引起该 LACP 成员口对应的聚合组所有端口出现解聚合再聚合现象。

配置方法

配置 LACP 成员口

- 必须配置。
- 将指定的物理端口配置为 LACP 成员口。在支持 LACP 功能的设备上配置。使用 LACP 功能时需要配置对应的 LACP 成员口。

【命令格式】 **port-group** *key-number* *mode* { **active** | **passive** }

【参数说明】 *Key-number* : 为聚合组的管理 key, *Key-number* 取值范围根据不同产品支持的聚合组数量不同而变, 这个 *Key-number* 值就是对应的 LACP AP 口的端口号。

active: 表示端口以主动模式加入动态聚合组

passive: 模式表示端口以被动模式加入聚合组

【缺省配置】 物理端口不属于任何 LACP 的成员口

【命令模式】 物理接口配置模式

【使用指导】 在接口模式下, 用户可以通过下面的配置命令向 LACP AP 口中添加成员口。

i 为保证 LACP 功能正常, 在链路两端的设备上需要对称配置 LACP 成员口。

配置 LACP 的系统优先级

- 为可选配置。
- 在需要调整该设备系统 ID 优先级时进行配置, 配置值越小, 系统 ID 优先级越高, 系统 ID 优先级高的设备优先选择聚合端口。
- 可在支持 LACP 功能的设备上配置该功能。

【命令格式】 **lacp system-priority** *system-priority*

【参数说明】 *system-priority* : LACP 系统的优先级, 可选范围为 0-65535, 默认优先级为 32768。

【缺省配置】 LACP 的系统优先级为 32768

【命令模式】 全局配置模式

【使用指导】 在全局模式下, 用户可以通过下面的配置命令配置 LACP 的系统优先级。一台设备的所有的动态链路组只能有一个 LACP 系统优先级, 修改这个值会影响到交换机上的所有聚合组。在接口配置模式下使用 **no lacp system-priority** 命令将 LACP 的系统优先级恢复到缺省值。

配置 LACP 成员口的端口优先级

- 可选配置。
- 在需要调整端口 ID 优先级时进行配置, 配置值越小, 端口 ID 优先级越高, 端口 ID 优先级高的端口会被优选为主端口。
- 可在支持 LACP 功能的设备上配置该功能。

【命令格式】 **lacp port-priority** *port-priority*

【参数说明】 *port-priority* : 端口的优先级, 可选范围为 0-65535, 默认优先级为 32768。

【缺省配置】 LACP 成员口的端口优先级为 32768

【命令模式】 物理接口配置模式

【使用指导】 在全局模式下，用户可以通过下面的配置命令配置 LACP 的系统优先级。在接口配置模式下使用 **no lacp port-priority** 命令将 LACP 的系统优先级恢复到缺省值。

配置 LACP 成员口的超时模式

- 可选配置。
- 在需要更实时感知链路故障的场景下，需要配置成短超时模式。配置短超时模式时，端口 3 秒收包超时，长超时模式，端口 90 秒收包超时。
- 可在支持 LACP 功能的设备上配置该功能，比如交换机产品等。

【命令格式】 **lacp short-timeout**

【参数说明】 -

【缺省配置】 LACP 成员口的端口超时模式为长超时

【命令模式】 接口配置模式

【使用指导】 仅在物理口上支持。

在接口配置模式下使用 **no lacp short-timeout** 命令将 LACP 超时模式恢复为缺省值。

检验方法

- 通过 **show running** 命令查看相应的配置。
- 通过 **show lacp summary** 命令查看 LACP 链路状态。

【命令格式】 **show lacp summary** [*key-number*]

【参数说明】 *key-name* : 指定的 LACP AP 接口号

【命令模式】 各模式均可执行

【使用指导】 如果没有指定 *key-number*，则所有 LACP AP 的链路聚合状态信息将被显示出来。

【命令展示】

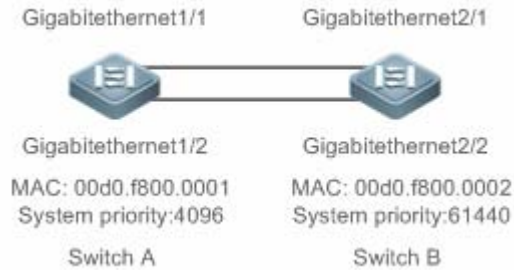
```
Ruijie(config)#show lacp summary 3
System Id:32768, 00d0.f8fb.0002
Flags: S - Device is requesting Slow LACPDUs
       F - Device is requesting Fast LACPDUs.
       A - Device is in active mode.           P - Device is in passive mode.
Aggregate port 3:
Local information:
LACP port      Oper   Port   Port
Port   Flags   State   Priority   Key   NumberState
-----
Gi0/1SAbnd140960x30x10x3d
Gi0/2SAbnd140960x30x20x3d
Gi0/3SAbnd140960x30x30x3d
Partner information:
Port      Flags      LACP port   Dev ID   Oper   Port   Port
          State   Priority     ID      Key    Number State
-----
Gi0/1    SA         61440      00d0.f800.0001  0x3    0x1    0x3d
Gi0/2    SA         61440      00d0.f800.0001  0x3    0x2    0x3d
Gi0/3    SA         61440      00d0.f800.0001  0x3    0x3    0x3d
```

配置举例

配置 LACP

【网络环境】

图 3-4



【配置方法】

- 在 SwitchA 上设置 LACP 系统优先级为 4096。
- 在 SwitchA 上的端口 GigabitEthernet1/1 和 GigabitEthernet1/2 上启用动态链路聚合协议,将其加入到 LACP 3 中。
- 在 SwitchB 上设置 LACP 系统优先级为 61440。
- 在 SwitchB 上的端口 GigabitEthernet2/1 和 GigabitEthernet2/2 启用动态链路聚合协议,将其加入到 LACP 3 中。

SwitchA

```
SwitchA# configure terminal
SwitchA(config)# lacp system-priority 4096
SwitchA(config)#interface range GigabitEthernet 1/1-2
SwitchA(config-if-range)# port-group 3 mode active
SwitchA(config-if-range)# end
```

SwitchB

```
SwitchB# configure terminal
SwitchB(config)# lacp system-priority 61440
SwitchB(config)#interface range GigabitEthernet 2/1-2
SwitchB(config-if-range)# port-group 3 mode active
SwitchB(config-if-range)# end
```

【检验方法】

- 通过 **show lacp summary 3** 查看 LACP 和成员口的对应关系是否正确。

SwitchA

```
SwitchA#show LACP summary 3
System Id:32768, 00d0.f8fb.0001
Flags: S - Device is requesting Slow LACPDUs
       F - Device is requesting Fast LACPDUs.
       A - Device is in active mode.           P - Device is in passive mode.
Aggregate port 3:
Local information:
LACP port      Oper   Port   Port
Port   Flags   State  Priority   Key   Number State
-----
Gil/1   SA     bndl   32768     0x3   0x10x3d
Gil/2   SA     bndl   32768     0x3   0x20x3d
Partner information:
LACP port      Oper   Port   Port
Port   Flags   Priority  Dev ID   Oper   Port   Port
              Key   NumberState
-----
Gil/1   SA     32768   00d0.f800.0002  0x3   0x1   0x3d
Gil/2   SA     32768   00d0.f800.0002  0x3   0x2   0x3d
```

SwitchB

```
SwitchB#show LACP summary 3
System Id:32768, 00d0.f8fb.0002
Flags: S - Device is requesting Slow LACPDUs
       F - Device is requesting Fast LACPDUs.
       A - Device is in active mode.           P - Device is in passive mode.
Aggregate port 3:
Local information:
LACP port      Oper   Port   Port
Port   Flags   State  Priority   Key   Number State
-----
```

Gi2/1	SA	bndl	32768	0x3	0x10x3d	
Gi2/2	SA	bndl	32768	0x3	0x20x3d	
Partner information:						
		LACP port		Oper	Port	Port
Port	Flags	Priority	Dev ID	Key	Number	State
-----	-----	-----	-----	-----	-----	-----
Gi2/1	SA	32768	00d0.f800.0001	0x3	0x1	0x3d
Gi2/2	SA	32768	00d0.f800.0001	0x3	0x2	0x3d

常见错误

-

3.4.3 配置AP的LinkTrap功能

配置效果

当聚合链路发生变化时，系统会发出相应的 LinkTrap 通告。

注意事项

-

配置方法

配置 AP 口的 LinkTrap

- 在接口模式下配置。为可选配置。AP 口的 LinkTrap 通告功能默认开启，在此情况下，AP 口的链路状态或者协议状态发生变化时，设备会发出 LinkTrap 通告；当不需要该 AP 口的 LinkTrap 通告时，配置关闭该功能。
- 可在所有支持 AP 功能的设备上配置该功能。

【命令格式】 **snmp trap link-status**

【参数说明】 -

【缺省配置】 LinkTrap 通告默认开启

【命令模式】 AP 接口配置模式

【使用指导】 在接口模式下，用户可以对指定的 AP 口设置是否发送 LinkTrap 通告功能。当该功能打开，AP 口发生 Link 状态变化时将发出 LinkTrap 通告，反之则不发。缺省情况下，该功能是打开的。用户可以在指定 AP 口的接口模式下，通过配置 **no snmp trap link-status** 命令关闭指定 AP 口的 LinkTrap 通告功能。
AP 成员口不支持在端口模式下打开 LinkTrap 通告功能。需要通过下面的配置，即在全局模式下配置 **aggregateport member linktrap** 命令来打开 AP 成员口的 LinkTrap 通告功能。

配置 AP 成员口的 LinkTrap

- 为可选配置。成员口 LinkTrap 默认关闭，当需要使能成员口的 LinkTrap 通告功能时，配置开启。
- 可在所有支持 AP 功能的设备上配置该功能。

【命令格式】 **aggregateport member linktrap**

【参数说明】 -

【缺省配置】 缺省情况下，AP 成员口的 LinkTrap 通告功能是关闭的。

【命令模式】 全局配置模式

【使用指导】 用户可以在全局配置模式下，通过配置 **aggregateport member linktrap** 命令打开所有 AP 成员口的 LinkTrap 通告功能。默认情况下，AP 成员口不发送 LinkTrap 通告。用户可以在全局配置模式下，通过配置 **no aggregateport member linktrap** 命令关闭所有 AP 成员口的 LinkTrap 通告功能。

检验方法

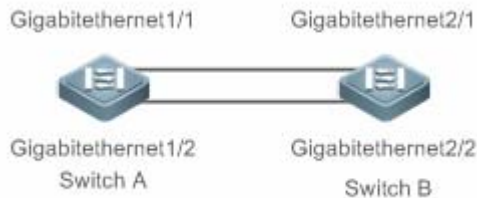
- 通过 **show running** 命令查看相应的配置。
- 打开 LinkTrap 通告的情况下，通过 MIB 软件可以监控到 AP 口或成员口的 LinkTrap 通告。

配置举例

配置 AP 的 LinkTrap 功能

【网络环境】

图 3-5



【配置方法】

- 将 SwitchA 上的端口 GigabitEthernet 1/1 和 GigabitEthernet 1/2 加入到静态 AP 3 中。
- 将 SwitchB 上的端口 GigabitEthernet 2/1 和 GigabitEthernet 2/2 加入到静态 AP 3 中。
- 在 SwitchA 上配置关闭 AP 3 的 LinkTrap 功能，同时打开成员口的 LinkTrap 功能。
- 在 SwitchB 上配置关闭 AP 3 的 LinkTrap 功能，同时打开成员口的 LinkTrap 功能。

SwitchA

```

SwitchA# configure terminal
SwitchA(config)#interface range GigabitEthernet 1/1-2
SwitchA(config-if-range)# port-group 3
SwitchA(config-if-range)# exit
SwitchA(config)#aggregateport member linktrap
SwitchA(config)#interface Aggregateport3
SwitchA(config-if-AggregatePort 3)#nosnmp trap link-status
  
```

SwitchB

```

SwitchB# configure terminal
SwitchB(config)#interface range GigabitEthernet 2/1-2
SwitchB(config-if-range)# port-group 3
SwitchB(config-if-range)# exit
SwitchB(config)#aggregateport member linktrap
SwitchB(config)#interface Aggregateport3
SwitchB(config-if-AggregatePort 3)#nosnmp trap link-status
  
```

【检验方法】

- 通过 **show running** 查看 AP 的流量均衡算法配置是否正确。

SwitchA

```

SwitchA#show run | include AggregatePort 3
Building configuration...
Current configuration: 54 bytes
interface AggregatePort 3
no snmp trap link-status
SwitchA#show run | include AggregatePort
aggregateport member linktrap
  
```

SwitchB

```

SwitchB#show run | include AggregatePort 3
Building configuration...
Current configuration: 54 bytes
interface AggregatePort 3
no snmp trap link-status
SwitchB#show run | include AggregatePort
aggregateport member linktrap
  
```

常见错误

3.4.4 配置流量平衡模式

配置效果

系统会根据指定的流量平衡算法，对输入报文进行流量分配。同一报文流将固定通过同一条链路输出，不同报文流将平均分配到各个链路。在增强模式下，设备先判断发送报文的类型，然后根据指定报文的字段进行流量均衡。

注意事项

配置方法

设置 AP 的全局流量平衡算法

- 为可选配置，当需要改变 AP 的流量平衡算法以实现更好的流量均衡时，需要配置该功能。
- 可在所有支持 AP 功能的设备上配置该功能。

【命令格式】 **aggregateport load-balance**{**dst-mac** | **src-mac** | **src-dst-mac** | **dst-ip** | **src-ip** | **src-dst-ip** | **src-l4port** | **dst-l4port** | **src-dst-l4port** }

【参数说明】 **dst-mac**：根据输入报文的目的 MAC 地址进行流量分配。

src-mac：根据输入报文的源 MAC 地址进行流量分配。

src-dst-ip：根据源 IP 与目的 IP 进行流量分配。

dst-ip：根据输入报文的目的 IP 地址进行流量分配。

src-ip：根据输入报文的源 IP 地址进行流量分配。

src-dst-mac：根据源 MAC 与目的 MAC 进行流量分配。

src-l4port：根据 L4 层源端口号进行流量分配。

dst-l4port：根据 L4 层目的端口号进行流量分配。

src-dst-l4port：根据 L4 层源端口号与 L4 层目的端口号进行流量分配。

【缺省配置】 AP 的流量均衡模式为基于源和目的 MAC(如交换机产品系列)或者基于源和目的 IP(如网关产品系列)的流量均衡方式。

【命令模式】 全局配置模式

【使用指导】 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。

在某些支持基于指定 AP 口配置流量平衡算法的产品上，上述的流量平衡算法配置命令也可以进入 AP 口的接口模式下进行配置，配置生效后，该 AP 口上就会以新配置的流量平衡算法进行工作。同样的，在这些产品下面，用户可以在 AP 口的接口模式下使用 **no aggregateport load-balance** 命令使该 AP 口下配置的流量平衡算法失效，进而生效为当前设备上生效的 AP 全局流量平衡算法。

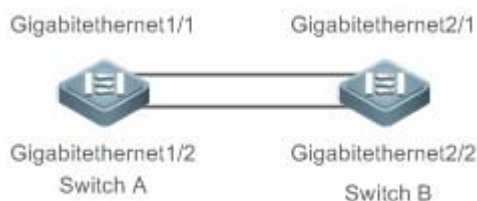
i 在支持基于 AP 口配置流量均衡的产品上，**aggregateport load-balance** 还支持在 AP 口接口模式下进行配置。

配置举例

配置流量平衡模式

【网络环境】

图 3-6



- 【配置方法】
- 将 SwitchA 上的端口 GigabitEthernet 1/1 和 GigabitEthernet 1/2 加入到静态 AP 3 中。
 - 将 SwitchB 上的端口 GigabitEthernet 2/1 和 GigabitEthernet 2/2 加入到静态 AP 3 中。
 - 在 SwitchA 上配置全局的 AP 流量均衡模式为基于源 MAC 地址的流量均衡方式。
 - 在 SwitchB 上配置全局的 AP 流量均衡模式为基于目的 MAC 地址的流量均衡方式。

SwitchA

```
SwitchA# configure terminal
SwitchA(config)#interface range GigabitEthernet 1/1-2
SwitchA(config-if-range)# port-group 3
SwitchA(config-if-range)# exit
SwitchA(config)# aggregateport load-balance src-mac
```

SwitchB

```
SwitchB# configure terminal
SwitchB(config)#interface range GigabitEthernet 2/1-2
SwitchB(config-if-range)# port-group 3
SwitchB(config-if-range)# exit
SwitchB(config)# aggregateport load-balance dst-mac
```

- 【检验方法】
- 通过 **show aggregateport load-balance** 查看 AP 的流量均衡算法配置是否正确。

SwitchA

```
SwitchA#show aggregatePort load-balance
Load-balance : Source MAC
```

SwitchB

```
SwitchB#show aggregatePort load-balance
Load-balance : Destination MAC
```

常见错误

-

3.4.5 配置AP的容量模式

配置效果

- 改变当前系统支持的最大可配置 AP 口数和单个 AP 口下最大可配置成员口数。

注意事项

- 默认配置下，系统有一个默认的 AP 容量模式，可以通过 **show aggregateport capacity** 命令查看当前容量模式。
- 配置容量模式时，当系统中已经存在的最大 AP 号或者某个 AP 下成员口数量超过了要配置的容量值，则容量模式配置会失败。

配置方法

配置 AP 容量模式

- 为可选配置，当需要改变当前系统 AP 的容量值时配置，以适应网络部署中 AP 的个数或者每个 AP 口允许聚合的成员口个数的变化需求。
- 可在核心交换机等支持改变 AP 容量功能的设备上配置该功能。

【命令格式】 **aggregateport capacity mode** *capacity-mode*

【参数说明】 *capacity-mode*：模式选项

【缺省配置】缺省情况下，AP 的容量模式随着不同的产品系列而不同，比如有 256*16(其中，256 代表设备支持的最大 AP 口个数，16 代表每个 AP 口支持的最大成员口个数)等容量模式。

【命令模式】全局配置模式

【使用指导】在支持容量模式配置的产品中，系统会提供几种可配置的容量模式供用户选择，在全局配置模式下，用户可以通过 **aggregateport capacity mode** *capacity-mode* 配置命令来选择需要的容量模式。用户可以在全局配置模式下，通过 **no aggregateport capacity mode** 将容量模式恢复为默认值。

检验方法

- 通过 **show running** 命令查看相应的配置。
- 通过 **show aggregateport capacity** 命令查看当前 AP 容量模式以及 AP 口容量使用情况。

【命令格式】 **show aggregateport capacity**

【参数说明】 -

【命令模式】 各模式均可执行

【使用指导】 -

```
Ruijie# show aggregateport capacity
AggregatePort Capacity Information:
Configuration Capacity Mode: 128*16.
Effective Capacity Mode      : 256*8.
Available Capacity          : 128*8.
Total Number: 128, Used: 1, Available: 127.
```

配置举例

配置 AP 的容量模式

【网络环境】

图 3-1



【配置方法】

- 将 SwitchA 上的端口 GigabitEthernet 1/1 和 GigabitEthernet 1/2 加入到静态 AP 3 中。
- 将 SwitchB 上的端口 GigabitEthernet 2/1 和 GigabitEthernet 2/2 加入到静态 AP 3 中。
- 将 SwitchA 上的 AP 容量模式配置为 128*128 模式。
- 将 SwitchB 上的 AP 容量模式配置为 256*64 模式。

SwitchA

```
SwitchA# configure terminal
SwitchA(config)# interface range GigabitEthernet 1/1-2
SwitchA(config-if-range)# port-group 3
SwitchA(config-if-range)# exit
SwitchA(config)# aggregateport capacity mode 128*128
```

SwitchB

```
SwitchB# configure terminal
SwitchB(config)# interface range GigabitEthernet 2/1-2
SwitchB(config-if-range)# port-group 3
SwitchB(config-if-range)# exit
SwitchB(config)# aggregateport capacity mode 256*64
```

【检验方法】

SwitchA

```
SwitchA# show aggregatePort capacity
AggregatePort Capacity Information:
Configuration Capacity Mode: 128*128.
Effective Capacity Mode      : 128*128.
Available Capacity Mode      : 128*128.
Total Number : 128, Used: 1, Available: 127.
```

SwitchB

```
SwitchB# show aggregatePort capacity
AggregatePort Capacity Information:
Configuration Capacity Mode: 256*64.
Effective Capacity Mode      : 256*64.
```

Available Capacity Mode : 256*64.
 Total Number : 256, Used: 1, Available: 255.

常见错误


3.5 监视与维护

清除各类信息

查看运行情况

作用	命令
查看 LACP 的链路聚合状态,可指定显示特定聚合组的信息,参数 <i>key-numebr</i> 表示 LACP 聚合组的 ID。	show lacp summary [<i>key-numebr</i>]
显示 AP 口摘要信息或流量平衡算法。	show aggregateport [<i>ap-number</i>] { load-balance summary }

查看调试信息

 输出调试信息,会占用系统资源。使用完毕后,请立即关闭调试开关。

作用	命令
打开 AP 的调试开关。	debug lsm ap
打开 LACP 的调试开关。	debug lacp { packet event database ha realtime stm timer all }

4 VLAN

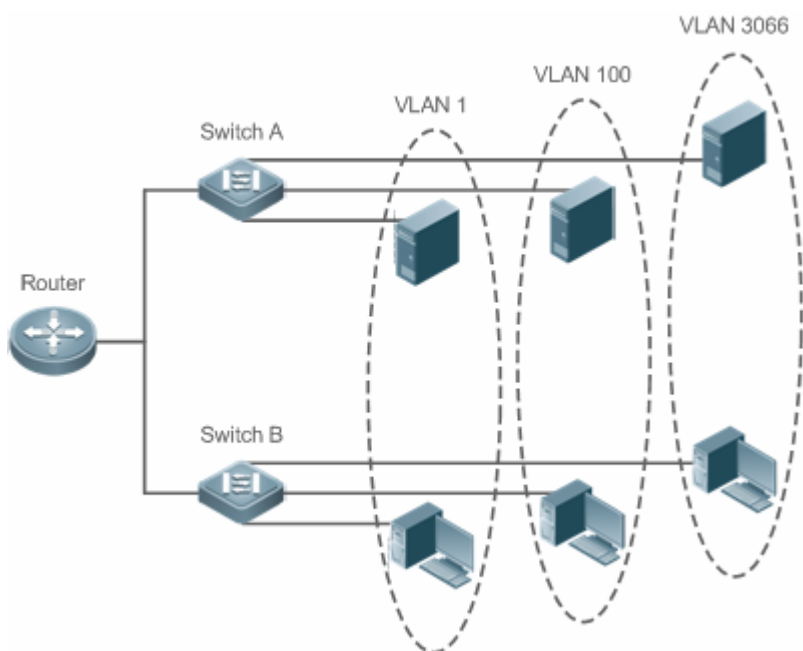
4.1 概述

VLAN 是虚拟局域网 (Virtual Local Area Network) 的简称，它是在一个物理网络上划分出来的逻辑网络。这个网络对应于 ISO 模型的第二层网络。

VLAN 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。

可以把一个端口定义为一个 VLAN 的成员，所有连接到这个特定端口的终端都是虚拟网络的一部分，并且整个网络可以支持多个 VLAN。当在 VLAN 中增加、删除和修改用户的时候，不必从物理上调整网络配置。VLAN 之间的通讯必须通过三层设备，见下图。

图 4-1



协议规范

- IEEE 802.1Q

4.2 典型应用

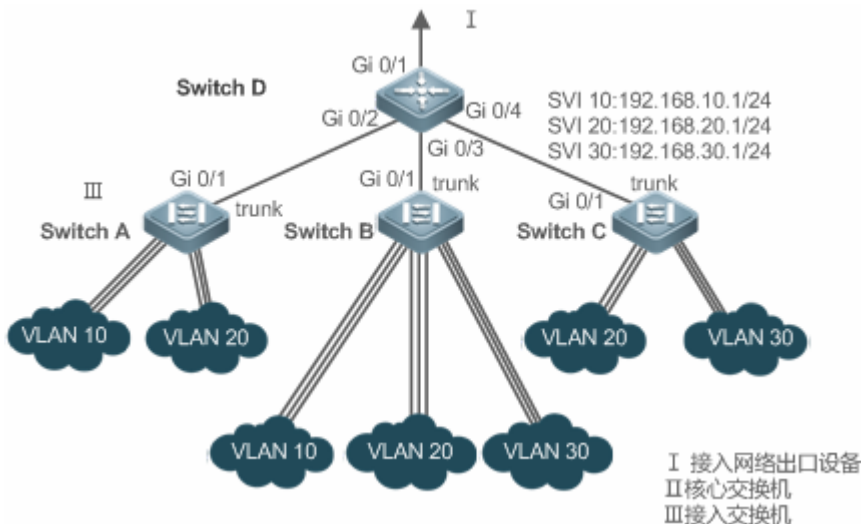
典型应用	场景描述
VLAN间二层隔离、三层互连	用户内网被划分为多个 VLAN，实现相互间的 2 层隔离，VLAN 间通过 3 层核心交换机的 IP 转发能力实现子网互连。

4.2.1 VLAN间二层隔离、三层互连

应用场景

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。

图 4-2



【注释】 Switch A、Switch B、Switch C 为接入交换机。

在核心交换机配置 3 个 VLAN，配置下连接接入交换机的端口为 trunk 口，并指定许可 vlan 列表，实现 2 层隔离；在核心交换机配置 3 个 SVI 口，分别作为 3 个 VLAN 对应 IP 子网的网关接口，配置对应的 IP 地址；分别在 3 台接入交换机创建 VLAN，为各 VLAN 分配 Access 口，指定上连核心交换机的 trunk 口。

功能部属

- 在 Intranet 中通过划分多个 VLAN，实现 VLAN 间的二层隔离。
- 三层交换设备中配置 SVI 接口，实现 VLAN 之间的三层通信。

4.3 功能详解

基本概念

↘ VLAN

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。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。

- ① 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。
- ① 许可配置的 VLAN ID 范围为 1-4094。
- ① 当硬件资源不足的情况下，系统将返回创建 VLAN 失败信息。

↘ 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：

端口类型	作用
Access 端口	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 端口 (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。
Uplink 端口	一个 Uplink 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，并且以 tag 方式转发 native-vlan 的帧。

Hybrid 端口	一个 Hybrid 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 ,并且允许以 untag 方式转发多个 VLAN 的帧 ,也可以通过设置许可 VLAN 列表 (Allowed-VLANs)来加以限制。
-----------	---

功能特性

功能特性	作用
VLAN	划分的 VLAN 间二层隔离

4.3.1 VLAN

VLAN 是虚拟局域网的简称，每个 VLAN 具备 VLAN 的独立广播域，不同的 VLAN 之间是二层隔离的。

工作原理

每个 VLAN 具备 VLAN 的独立广播域，不同的 VLAN 之间是二层隔离的。

VLAN 的二层隔离：如果 VLAN 没有配置 SVI，各个 VLAN 之间是二层隔离的，即 VLAN 间的用户之间不能通信；

VLAN 的三层互连：三层交换设备中如果 VLAN 配置 SVI，各个 VLAN 间能三层互连通信；

4.4 配置详解

配置项	配置建议&相关命令
配置基本VLAN	 必选配置。用于创建 VLAN，加入 ACCESS 模式接口。
	vlan 输入一个 VLAN ID。
	 可选配置。配置 ACCESS 口，用于传输单个 VLAN 的信息。
	switchportmodeaccess 定义该接口的类型为二层 Access 口
	switchportaccess vlan 将这个接口分配给一个 vlan
	add interface 向当前 VLAN 中添加一个或一组 Access 口
	 可选配置，用于 VLAN 重命名。 name 为 VLAN 取一个名字。
配置TRUNK	 必选配置。配置接口模式为 TRUNK 口。
	switchportmodetrunk 定义该接口的类型为二层 Trunk 口
	 可选配置。配置 TRUNK 口，用于传输多个 VLAN。
	switchporttrunkallowedvlan 配置这个 Trunk 口的许可 VLAN 列表。 switchporttrunk native vlan 为这个口指定一个 Native VLAN
配置UPLINK	 必选配置。配置接口模式为 UPLINK 口。
	switchportmodeuplink 配置为端口为 Uplink 口
	 可选配置，用于恢复接口模式。 noswitchportmode 删除端口模式
配置HYBRID	 必选配置。配置接口模式为 HYBRID 口。
	switchportmodehybrid 配置为端口为 Hybrid 口
	 可选配置。用于转发多个 VLAN 的帧，并且允许以 UNTAG 方式转发多个 VLAN 的帧。 noswitchportmode 删除端口模式
	switchport hybrid allowed vlan 设置端口的输出规则
	switchporthybridnativevlan 设置 Hybrid 口的默认 VLAN

4.4.1 配置基本VLAN

配置效果

- 一个 VLAN 是以 VLAN ID 来标识的。在设备中，您可以添加、删除、修改 VLAN2-4094，而 VLAN 1 是由设备自动创建，并且不可被删除。可以在接口配置模式下配置一个端口的 VLAN 成员类型或加入、移出一个 VLAN。

注意事项

- 无

配置方法

创建、修改一个 vlan

- 必须配置。
- 当硬件资源不足的情况下，系统将返回创建 VLAN 失败信息。
- 使用 `vlan vlan-id` 命令添加一个新的 VLAN 或者进入 VLAN 模式。
- 交换机设备上配置。

【命令格式】 `vlan vlan-id`

【参数说明】 `vlan-id`: VLAN vid，范围为 1-4094

【缺省配置】 VLAN 1 由设备自动创建，并且不可被删除

【命令模式】 全局配置模式

【使用指导】 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。使用 `novlan vlan-id` 命令可以删除 vlan，其中不允许删除的 VLAN 有：默认 VLAN1、配置 SVI 的 VLAN、SUBVLAN 等。

vlan 重命名

- 可选配置。
- 用户不能将 VLAN 重命名为其他 VLAN 的缺省名字。
- 交换机设备上配置。

【命令格式】 `name vlan-name`

【参数说明】 `vlan-name`：要重新命名的 VLAN 名字

【缺省配置】 缺省情况下，VLAN 的名称为该 VLAN 的 VLAN ID。比如，VLAN 0004 就是 VLAN 4 的缺省名字。

【命令模式】 VLAN 配置模式

【使用指导】 如果想把 VLAN 的名字改回缺省名字，只需输入 `no name` 命令即可

将当前 ACCESS 口加入到指定 VLAN

- 可选配置。
- 通过 `switchportmodeaccess` 命令指定二层接口（switch port）的模式为 access 口。
- 通过 `switchportaccessvlan vlan-id` 命令将一个 access port 加入指定 VLAN，可传输该 VLAN 流量。
- 交换机设备上配置。

【命令格式】 `switchportmodeaccess`

【参数说明】 -

【缺省配置】 switch port 缺省模式为 access

【命令模式】 接口配置模式

【使用指导】 -

【命令格式】 `switchportaccessvlan vlan-id`

【参数说明】 `vlan-id`: VLAN vid：

【缺省配置】 Access 口缺省仅加入 VLAN 1

【命令模式】 接口配置模式

【使用指导】 如果把一个接口分配给一个不存在的 VLAN，那么这个 VLAN 将自动被创建。

向当前 VLAN 添加 ACCESS 口

- 可选配置。
- 该命令只对 Access 口有效，VLAN 添加 Access 口后，接口可传输该 VLAN 数据。
- 交换机设备上配置。

【命令格式】 **addinterface**{ *interface-id* | *range**interface-range*}

【参数说明】 *interface-id* : 单个接口

interface-range : 多个接口

【缺省配置】 缺省情况下，所有二层以太网口都属于 VLAN1

【命令模式】 VLAN 配置模式

【使用指导】 在 VLAN 配置模式下，将指定的 Access 口加入该 VLAN。该命令的配置效果同在接口模式下指定该接口所属 VLAN 的命令（即 **switchportaccess vlan** *vlan-id*）效果一致。

i 对于两种形式的接口加入 VLAN 命令，配置生效的原则是后配置的命令覆盖前面配置的命令

检验方法

- 往 ACCESS 口发送 untag 报文，报文在该 VLAN 内广播。
- 使用命令 **showvlan** 和 **showinterfaceswitchport** 查看配置显示是否生效。

【命令格式】 **show vlan** [*id* *vlan-id*]

【参数说明】 *vlan-id* : VLAN ID 号

【命令模式】 所有模式

【使用指导】 -

【命令展示】

```
Ruijie(config-vlan)#show vlan id 20
VLAN Name                Status    Ports
-----
20 VLAN0020              STATIC    Gi0/1
```

配置举例

基本 VLAN 与 access 口配置

以下配置举例，仅介绍 VLAN 相关的配置。

- 【配置方法】
- 创建一个新 VLAN，并且重命名
 - 将一个 ACCESS 口加入加入 VLAN，两种方式。

```
Ruijie# configure terminal
Ruijie(config)# vlan 888
Ruijie(config-vlan)# name test888
Ruijie# configure terminal
Ruijie(config)# interface GigabitEthernet 0/3
Ruijie(config-if-GigabitEthernet 0/3)# switchport mode access
Ruijie(config-if-GigabitEthernet 0/3)# switchport access vlan 20
```

或者用如下方式：把 Access 口(GigabitEthernet 0/3)添加到 VLAN20：

```
Ruijie# configure terminal
SwitchA(config)#vlan 20
SwitchA(config-vlan)#add interface GigabitEthernet0/3
```

【检验方法】 **show** 显示是否正确

```
Ruijie(config-vlan)#show vlan
VLAN Name                Status    Ports
-----
1 VLAN0001              STATIC
20 VLAN0020            STATIC    Gi0/3
888 test888            STATIC
Ruijie(config-vlan)#
```

```
Ruijie#show interfaceGigabitEthernet0/3 switchport
Interface                               Switchport Mode      Access Native Protected VLAN lists
-----
GigabitEthernet 0/3                    enabled             ACCESS      20      1      Disabled ALL
```

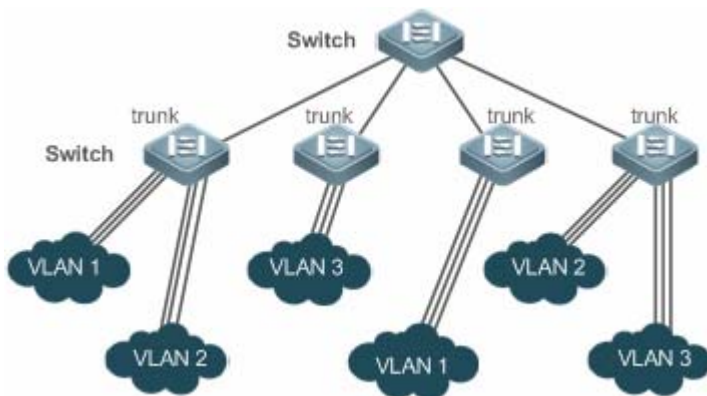
4.4.2 配置TRUNK

配置效果

一个 Trunk 是将一个或多个以太网交换接口和其他的网络设备（如路由器或交换机）进行连接的点对点链路，一条 Trunk 链路可以传输属于多个 VLAN 的流量。

锐捷设备的 Trunk 采用 802.1Q 标准封装。下图显示了一个采用 Trunk 连接的网络。

图 4-3



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）。

必须为 Trunk 口指定一个 Native VLAN。所谓 Native VLAN，就是指在这个接口上收发的 UNTAG 报文，都被认为是属于这个 VLAN 的。显然，这个接口的缺省 VLAN ID（即 IEEE 802.1Q 中的 PVID）就是 Native VLAN 的 VLAN ID。同时，在 Trunk 上发送属于 Native VLAN 的帧，则必然采用 UNTAG 的方式。每个 Trunk 口的缺省 Native VLAN 是 VLAN 1。

在配置 Trunk 链路时，请确认连接链路两端的 Trunk 口使用相同的 Native VLAN。

配置方法

配置一个 TRUNK 口

- 必须配置。
- 将接口配置成 trunk 可传输多个 VLAN 的流量。
- 交换机设备上配置。

【命令格式】 **switchportmodetrunk**

【参数说明】 -

【缺省配置】 缺省模式是 ACCESS 模式，可配置成 TRUNK 模式

【命令模式】 接口配置模式

【使用指导】 如果想把一个 Trunk 口的所有 Trunk 相关属性都复位成缺省值，请使用 **no switchport mode** 配置命令。

定义 Trunk 口的许可 VLAN 列表

- 可选配置。
- 一个 Trunk 口缺省可以传输本设备支持的所有 VLAN（1 - 4094）的流量。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。
- 交换机设备上配置。

【命令格式】 **switchporttrunkallowedvlan {all | [add |remove | except| only]} vlan-list**

- 【参数说明】 参数 `vlan-list` 可以是一个 VLAN，也可以是一系列 VLAN，VLAN ID 按顺序排列，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；
`only` 表示将列出的 VLAN 列表加入许可 VLAN 列表，其他 VLAN 从许可列表中删除；
- 【缺省配置】 trunk 口和 uplink 口属于所有 VLAN
- 【命令模式】 接口配置模式
- 【使用指导】 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

配置 Native VLAN

- 可选配置。
- 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。
- 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。
- 交换机设备上配置。

【命令格式】 `switchporttrunknativevlan vlan-id`

【参数说明】 `vlan-id`: VLAN vid

【缺省配置】 trunk/uplink 的默认 VLAN 为 VLAN 1

【命令模式】 接口配置模式

【使用指导】 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。

i 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。

检验方法

- 往 TRUNK 口发送 tag 报文，报文在指定 VLAN 内广播。
- 使用命令 `showvlan` 和 `showinterfaceswitchport` 查看配置显示是否生效。

【命令格式】 `show vlan [id vlan-id]`

【参数说明】 `vlan-id`: VLAN ID 号

【命令模式】 所有模式

【使用指导】 -

【命令展示】

```
Ruijie(config-vlan)#show vlan id 20
VLAN Name                Status    Ports
-----
20 VLAN0020              STATIC    Gi0/1
```

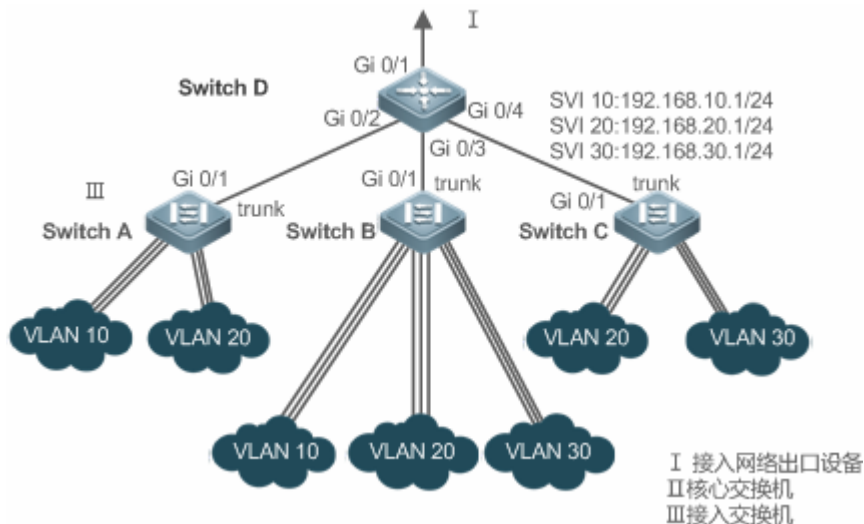
配置举例

! 以下配置举例，仅介绍 TRUNK 相关的配置。

配置基本 VLAN，实现二层隔离、三层互连

【网络环境】

图 4-4



【配置方法】 组网需求

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

配置要点

本例以核心交换机和 1 台接入交换机为例说明配置过程。要点如下：

- 在核心交换机配置 3 个 VLAN，配置下连接接入交换机的端口为 trunk 口，并指定许可 vlan 列表，实现 2 层隔离；
- 在核心交换机配置 3 个 SVI 口，分别作为 3 个 VLAN 对应 IP 子网的网关接口，配置对应的 IP 地址；
- 分别在 3 台接入交换机创建 VLAN，为各 VLAN 分配 Access 口，指定上连核心交换机的 trunk 口。本例以接入交换机 Switch A 为例说明配置步骤。

D

```
D#configure terminal
D(config)#vlan10
D(config-vlan)#vlan20
D(config-vlan)#vlan30
D(config-vlan)#exit
D(config)#interfacerange GigabitEthernet 0/2-4
D(config-if-range)#switchportmode trunk
D(config-if-range)#exit
D(config)#interface GigabitEthernet 0/2
D(config-if-GigabitEthernet 0/2)#switchport trunk allowed vlan remove 1-4094
D(config-if-GigabitEthernet 0/2)#switchport trunk allowed vlan add 10,20
D(config-if-GigabitEthernet 0/2)#interface GigabitEthernet 0/3
D(config-if-GigabitEthernet 0/2)#switchport trunk allowed vlan remove 1-4094
D(config-if-GigabitEthernet 0/2)#switchport trunk allowed vlan add 10,20,30
D(config-if-GigabitEthernet 0/2)#interface GigabitEthernet0/4
D(config-if-GigabitEthernet 0/2)#switchport trunk allowed vlan remove 1-4094
D(config-if-GigabitEthernet 0/2)#switchport trunk allowed vlan add 20,30
D#configure terminal
D(config)#interface vlan 10
D(config-if-VLAN 10)#ip address 192.168.10.1 255.255.255.0
D(config-if-VLAN 10)#interface vlan 20
D(config-if-VLAN 20)#ip address 192.168.20.1 255.255.255.0
D(config-if-VLAN 20)#interface vlan 30
D(config-if-VLAN 30)#ip address 192.168.30.1 255.255.255.0
D(config-if-VLAN 30)#exit
```

A

```
A#configure terminal
A(config)#vlan10
A(config-vlan)#vlan20
```

```
A(config-vlan)#exit
A(config)#interfacerange GigabitEthernet 0/2-12
A(config-if-range)#switchport mode access
A(config-if-range)#switchport access vlan 10
A(config-if-range)#interfacerange GigabitEthernet 0/13-24
A(config-if-range)#switchport mode access
A(config-if-range)#switchport access vlan 20
A(config-if-range)#exit
A(config)#interface GigabitEthernet 0/1
A(config-if-GigabitEthernet 0/1)#switchportmode trunk
```

【检验方法】 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
- 查看端口 Gi 0/2、Gi 0/3、Gi 0/4 的 vlan 状态

D

```
D#show vlan
VLANName 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
D#show interface GigabitEthernet 0/2 switchport
Interface          Switchport Mode      Access Native Protected VLAN lists
-----
GigabitEthernet 0/2    enabled TRUNK 1      1      Disabled 10, 20
D#show interface GigabitEthernet0/3 switchport
Interface          Switchport Mode      Access Native Protected VLAN lists
-----
GigabitEthernet 0/3    enabled TRUNK 1      1      Disabled 10, 20, 30
D#show interface GigabitEthernet0/4switchport
Interface          Switchport Mode      Access Native Protected VLAN lists
-----
GigabitEthernet 0/4    enabled TRUNK 1      1      Disabled 20, 30
```

常见错误

- 无

4.4.3 配置UPLINK

配置效果

- UPLINK 端口一般用于 QinQ (出自标准 IEEE 802.1ad) 环境中，它和 TRUNK 端口的功能很相似，不同之处在于 UPLINK 端口只发送 TAG 帧，而 TRUNK 端口缺省 VLAN 的帧以 UNTAG 形式发送。

配置方法

📌 配置一个 UPLINK 口

- 必须配置。
- 将接口配置成 uplink 口，可传输多个 vlan 的流量，但只能发送 TAG 帧。
- 交换机设备上配置。

【命令格式】 **switchportmodeuplink**

【参数说明】 -

- 【缺省配置】 缺省模式是 ACCESS 模式，可配置成 ACCESS 模式 UPLINK 模式
- 【命令模式】 接口配置模式
- 【使用指导】 如果想把一个 UPLINK 口的所有 UPLINK 相关属性都复位成缺省值，请使用 **no switchport mode** 配置命令。

▾ 定义 UPLINK 口的许可 VLAN 列表

- 可选配置。
- 可以通过设置 UPLINK 口的许可 VLAN 列表来限制某些 VLAN 的流量不能通过这个 UPLINK 口。
- 交换机设备上配置。

- 【命令格式】 **switchporttrunkallowedvlan {all | [add |remove | except| only]} vlan-list**
- 【参数说明】 参数 vlan-list 可以是一个 VLAN，也可以是一系列 VLAN，VLAN ID 按顺序排列，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；
only 表示将列出的 VLAN 列表加入许可 VLAN 列表，其他 VLAN 从许可列表中删除；
- 【命令模式】 接口配置模式
- 【使用指导】 如果想把 UPLINK 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

▾ 配置 Native VLAN

- 可选配置。
- 如果一个帧带有 Native VLAN 的 VLAN ID，在通过这个 UPLINK 口转发时，不会被剥去 TAG。这与 TRUNK 相反。
- 交换机设备上配置。

- 【命令格式】 **switchporttrunknativevlan vlan-id**
- 【参数说明】 *vlan-id*: VLAN vid
- 【命令模式】 接口配置模式
- 【使用指导】 如果想把 UPLINK 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。

检验方法

- 往 UPLINK 口发送 tag 报文，报文在指定 VLAN 内广播。
- 使用命令 **showvlan** 和 **showinterfaceswitchport** 查看配置显示是否生效。

【命令格式】 **show vlan [id vlan-id]**

【参数说明】 *vlan-id*: VLAN ID 号

【命令模式】 所有模式


【使用指导】 -

【命令展示】

```
Ruijie(config-vlan)#show vlan id 20
VLAN Name                Status    Ports
-----
20 VLAN0020              STATIC    Gi0/1
```

配置举例

▾ 配置一个 uplink 口

 以下配置举例，仅介绍 UPLINK 相关的配置。

【配置方法】 下面是一个把端口 Gi0/1 变成 UPLINK 的例子：

```
Ruijie#configure terminal
```

```
Ruijie(config)#interface gi 0/1
Ruijie(config-if-GigabitEthernet 0/1)#switchport mode uplink
Ruijie(config-if-GigabitEthernet 0/1)#end
```

【检验方法】 show 显示是否正确

```
Ruijie# show interfaces GigabitEthernet 0/1switchport
Interface                               Switchport Mode      Access Native Protected VLAN lists
-----
GigabitEthernet 0/1                    enabled  UPLINK      1      1      disabled ALL
```

4.4.4 配置HYBRID

配置效果

- HYBRID 端口一般用于 SHARE VLAN 的环境中。HYBRID 端口在缺省情况下与 TRUNK 端口相同，不同是它可以设置除了缺省 VLAN 外的其它 VLAN 的帧以 UNTAG 形式发送

配置方法

配置一个 HYBRID 口

- 必须配置。
- 将接口配置成 hybrid 口，可传输多个 VLAN 的流量。
- 交换机设备上配置。

【命令格式】 **switchportmode hybrid**

【参数说明】 -

【缺省配置】 缺省模式是 ACCESS 模式，可配置成 HYBRID 模式

【命令模式】 接口配置模式

【使用指导】 如果想把一个 HYBRID 口的所有 HYBRID 相关属性都复位成缺省值，请使用 **no switchport mode** 配置命令。

定义 HYBRID 口的许可 VLAN 列表

- 可选配置。
- 一个 HYBRID 口缺省可以传输本设备支持的所有 VLAN(1 - 4094)的流量。也可以通过设置 HYBRID 口的许可 VLAN 列表来限制某些 VLAN 的流量不能通过这个 HYBRID 口。
- 交换机设备上配置。

【命令格式】 **switchport hybrid allowed vlan[[add] only]tagged[[add]untagged|remove] vlan_list**

【参数说明】 *vlan-id*: VLAN vid

【缺省配置】 默认 hybrid 口属于所有 VLAN，端口以 Tag 形式加入所有除了默认 VLAN 以外的其它 VLAN，默认 VLAN 以 UNTag 形式加入

【命令模式】 接口配置模式

【使用指导】 -

配置 Native VLAN

- 可选配置。
- 如果一个帧带有 Native VLAN 的 VLAN ID，在通过这个 HYBRID 口转发时，会自动被剥去 TAG。
- 交换机设备上配置。

【命令格式】 **switchporthybridnativevlan vlan_id**

【参数说明】 *vlan-id*: VLAN vid

【缺省配置】 缺省的 Native VLAN 是 VLAN 1

【命令模式】 接口配置模式

【使用指导】 如果想把 HYBRID 的 Native VLAN 列表改回缺省的 VLAN 1，请使用 **no switchport hybrid native vlan** 接口

配置命令。

检验方法

- 往 HYBRID 口发送 tag 报文，报文在指定 VLAN 内广播。
- 使用命令 **showvlan** 和 **showinterfaceswitchport** 查看配置显示是否生效。

【命令格式】 **show vlan [id vlan-id]**

【参数说明】 *vlan-id* : AP VLAN ID 号

【命令模式】 所有模式


【使用指导】 -

【命令展示】

```
Ruijie(config-vlan)#show vlan id 20
VLAN Name                Status    Ports
-----
20 VLAN0020              STATIC   Gi0/1
```

配置举例

配置一个 hybrid 口

 以下配置举例，仅介绍 HYBRID 相关的配置。

【配置方法】 下面是一个端口 Gi0/1 关于 HYBRID 配置的例子：

```
Ruijie#configure terminal
Ruijie(config)#interface gigabitEthernet0/1
Ruijie(config-if-GigabitEthernet 0/1)#switchport mode hybrid
Ruijie(config-if-GigabitEthernet 0/1)#switchport hybrid native vlan 3
Ruijie(config-if-GigabitEthernet 0/1)#switchport hybrid allowed vlan untagged 20-30
Ruijie(config-if-GigabitEthernet 0/1)#end
```

【检验方法】 **show run** 显示是否正确

```
Ruijie(config-if-GigabitEthernet 0/1)#show run interfacegigabitEthernet 0/1

Building configuration...
Current configuration : 166 bytes

interface GigabitEthernet 0/1
 switchport
 switchport mode hybrid
 switchport hybrid native vlan 3
 switchport hybrid allowed vlan add untagged 20-30
```

4.5 监视与维护


清除各类信息

无

查看运行情况

作用	命令
查看 VLAN 配置	show vlan
查看交换口配置	showinterfaceswitchport

查看调试信息

 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
打开 VLAN 的调试开关。	debug bridge vlan

5 MSTP

5.1 概述

生成树协议是一种二层管理协议，它通过选择性地阻塞网络中的冗余链路来消除二层环路，同时还具备链路备份的功能。

与众多协议的发展过程一样，生成树协议也是随着网络的发展而不断更新的，从最初的 STP (Spanning Tree Protocol , 生成树协议) 到 RSTP(Rapid Spanning Tree Protocol , 快速生成树协议) 再到最新的 MSTP(Multiple SpanningTree Protocol , 多生成树协议)。

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

- 发现并启动局域网的一个最佳树型拓扑结构。
- 发现故障并随之进行恢复，自动更新网络拓扑结构，使在任何时候都选择了可能的最佳树型结构。

局域网的拓扑结构是根据管理员设置的一组网桥配置参数自动进行计算的。使用这些参数能够生成最好的一棵拓扑树。只有配置得当，才能得到最佳的方案。

RSTP 协议完全向下兼容 802.1D STP 协议，除了和传统的 STP 协议一样具有避免回路、提供冗余链路的功能外，最主要的特点就是“快”。如果一个局域网内的网桥都支持 RSTP 协议且管理员配置得当，一旦网络拓扑改变而要重新生成拓扑树只需要不超过 1 秒的时间（传统的 STP 需要大约 50 秒）。

STP 和 RSTP 存在的不足：

- STP 不能快速迁移，即使是在点对点链路或边缘端口，也必须等待两倍的 Forward Delay 的时间延迟，端口才能迁移到转发状态。
- RSTP 可以快速收敛，但和 STP 一样还存在如下缺陷：由于局域网内所有 VLAN 都共享一棵生成树，因此所有 VLAN 的报文都沿这棵生成树进行转发，不能按 VLAN 阻塞冗余链路，也无法在 VLAN 间实现数据流量的负载均衡。

MSTP(Multiple Spanning Tree Protocol , 多生成树协议)，由 IEEE 制定的 802.1s 标准定义，它可以弥补 STP、RSTP 的缺陷，既可以快速收敛，也能使不同 VLAN 的流量沿各自的路径转发，从而为冗余链路提供了更好的负载分担机制。简单地说，STP/RSTP 是基于端口的，MSTP 是基于实例的。所谓实例就是多个 VLAN 的一个集合，通过多个 VLAN 捆绑到一个实例的方法可以节省通信开销和资源占用率。

本设备既支持 STP 协议，也支持 RSTP 协议与 MSTP 协议，遵循 IEEE 802.1D、IEEE 802.1w 及 IEEE 802.1s 标准。

i 下文仅介绍 MSTP 的相关内容。

协议规范

- IEEE 802.1D : Media Access Control (MAC) Bridges
- IEEE 802.1w : Part 3: Media Access Control (MAC) Bridges—Amendment 2: Rapid Reconfiguration
- IEEE 802.1s : Virtual Bridged Local Area Networks—Amendment 3: Multiple Spanning Trees

5.2 功能详解

基本概念

▾ BPDU (Bridge Protocol Data Units)

要生成一个稳定的树型拓扑网络需要依靠以下元素：

- 每个网桥拥有的唯一的桥 ID (Bridge ID)，由桥优先级和 Mac 地址组合而成。
- 网桥到根桥的路径花费 (Root Path Cost)，以下简称根路径花费。
- 每个端口 ID (Port ID)，由端口优先级和端口号组合而成。

网桥之间通过交换 BPDU (Bridge Protocol Data Units，网桥协议数据单元) 帧来获得建立最佳树形拓扑结构所需要的信息。这些帧以组播地址 01-80-C2-00-00-00 (十六进制) 为目的地址。

每个 BPDU 由以下这些要素组成：

- Root Bridge ID (本网桥所认为的根桥 ID)。
- Root Path Cost (本网桥的根路径花费)。
- Bridge ID (本网桥的桥 ID)。
- Message Age (报文已存活的时间)
- Port ID (发送该报文端口的 ID)。

Forward-Delay Time、Hello Time、Max-Age Time 三个协议规定的时间参数。

其他一些诸如表示发现网络拓扑变化、本端口状态的标志位。

当网桥的一个端口收到高优先级的 BPDU (更小的 Bridge ID，更小的 Root Path Cost 等)，就在该端口保存这些信息，同时向所有端口更新并传播这些信息。如果收到比自己低优先级的 BPDU，网桥就丢弃该信息。

这样的机制就使高优先级的信息在整个网络中传播开，BPDU 的交流就有了下面的结果：

- 网络中选择了一个网桥为根桥 (Root Bridge)。
- 除根桥外的每个网桥都有一个根口 (Root Port)，即提供最短路径到 Root Bridge 的端口。
- 每个网桥都计算出了到根桥 (Root Bridge) 的最短路径。
- 每个 LAN 都有了指派网桥 (Designated Bridge)，位于该 LAN 与根桥之间的最短路径中。指派网桥和 LAN 相连的端口称为指派端口 (Designated Port)。
- 根口 (Root port) 和指派端口 (Designated Port) 进入 Forwarding 状态。

▾ Bridge ID

按 IEEE 802.1W 标准规定，每个网桥都要有单一的网桥标识 (Bridge ID)，生成树算法中就是以它为标准来选出根桥 (Root Bridge) 的。Bridge ID 由 8 个字节组成，后 6 个字节为该网桥的 mac 地址，前 2 个字节如下表所示，前 4 bit 表示优先级 (Priority)，后 8 bit 表示 System ID，为以后扩展协议而用，在 RSTP 中该值为 0，因此给网桥配置优先级就要是 4096 的倍数。

	Bit 位	值
Priority value	16	32768
	15	16384
	14	8192
	13	4096
System ID	12	2048
	11	1024
	10	512
	9	256
	8	128
	7	64

6	32
5	16
4	8
3	4
2	2
1	1

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。

Port Roles and PortStates

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

- Root port：提供最短路径到根桥 (Root Bridge) 的端口。
- Designated port：每个 LAN 的通过该口连接到根桥。
- Alternate port：根口的替换口，一旦根口失效，该口就立该变为根口。
- Backup port：Designated Port 的备份口，当一个网桥有两个端口都连在一个 LAN 上，那么高优先级的端口为 Designated Port，低优先级的端口为 Backup Port。
- Disable port：当前不处于活动状态的口，即 Operation State 为 Down 的端口都被分配了这个角色。

以下为各个端口角色的示意图 1、2、3：

R = RootPort D = Designated Port A = AlternatePort B = BackupPort

在没有特别说明情况下，端口优先级从左到右递减。

图 5-1

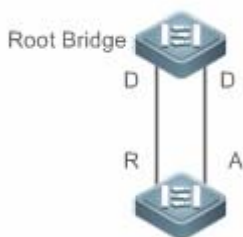


图 5-2

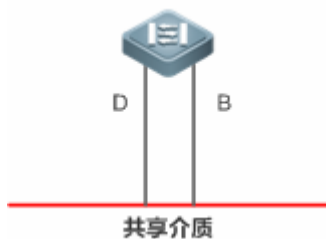
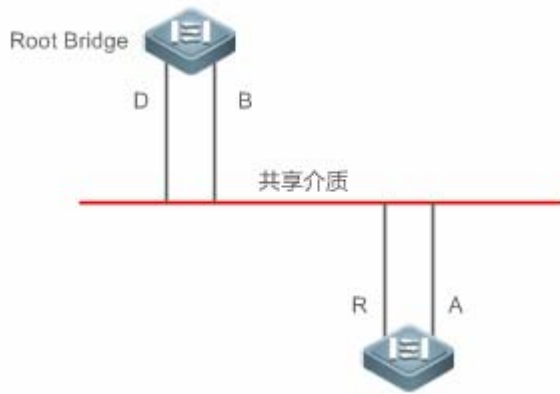


图 5-3



每个端口有三个状态 (Port State) 来表示是否转发数据包, 从而控制着整个生成树拓扑结构。

- Discarding : 既不对收到的帧进行转发, 也不进行源 Mac 地址学习。
- Learning : 不对收到的帧进行转发, 但进行源 Mac 地址学习, 这是个过渡状态。
- Forwarding : 既对收到的帧进行转发, 也进行源 Mac 地址的学习。

对一个已经稳定的网络拓扑, 只有 Root Port 和 Designated Port 才会进入 Forwarding 状态, 其它端口都只能处于 Discarding 状态。

📌 Hop Count

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

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

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

功能特性

功能特性	作用
STP协议	STP (Spanning Tree Protocol, 生成树协议), 由 IEEE 制定的 802.1D 标准定义, 用于在局域网中消除数据链路层物理环路的协议。
RSTP协议	RSTP (Rapid Spanning Tree Protocol, 快速生成树协议), 由 IEEE 制定的 802.1w 标准定义, 它在 STP 基础上进行了改进, 实现了网络拓扑的快速收敛。
MSTP协议	MSTP (Multiple Spanning Tree Protocol, 多生成树协议), 由 IEEE 制定的 802.1s 标准定义, 它可以弥补 STP、RSTP 和 PVST 的缺陷, 既可以快速收敛, 也能使不同 VLAN 的流量沿各自的路径转发, 从而为冗余链路提供了更好的负载分担机制。
MSTP的可选特性	包括以下功能: Port Fast 特性、BPDU Guard、BPDU Filter、Tc-protection、TC Guard、TC 过滤、BPDU 源 MAC 检查、BPDU 非法长度过滤、边缘口的自动识别、ROOT Guard 功能及 LOOP Guard 功能。

5.2.1 STP

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。

工作原理

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

- 发现并启动局域网的一个最佳树型拓扑结构。
- 发现故障并随之进行恢复，自动更新网络拓扑结构，使在任何时候都选择了可能的最佳树型结构。

局域网的拓扑结构是根据管理员设置的一组网桥配置参数自动进行计算的。使用这些参数能够生成最好的一棵拓扑树。只有配置得当，才能得到最佳的方案。

相关配置

▾ 打开 spanning-tree 功能

缺省情况下，spanning-tree 功能是关闭的。

使用 **spanning-tree [forward-time seconds | hello-time seconds | max-ageseconds]**命令可以打开 STP，所带参数可在打开 STP 的同时，设置全局的基本设置。

forward-time 取值范围是<4-30>，hello-time 取值范围是<1-10>，max-age 取值范围是<6-40>。



在设备运行过程中执行 **clear** 命令，可能因为重要信息丢失而导致业务中断。forward-time、hello-time、max-age 三个值的范围是相关的，修改了其中一个会影响到其他两个的值范围。这三个值之间有一个制约关系： $2 * (\text{Hello Time} + 1.0 \text{ second}) \leq \text{Max-Age Time} \leq 2 * (\text{Forward-Delay} - 1.0 \text{ second})$ ，不符合这个条件的值也会设置不成功。

5.2.2 RSTP

RSTP 协议完全向下兼容 802.1D STP 协议，除了和传统的 STP 协议一样具有避免回路、提供冗余链路的功能外，最主要的特点就是“快”。如果一个局域网内的网桥都支持 RSTP 协议且管理员配置得当，一旦网络拓扑改变而要重新生成拓扑树只需要不超过 1 秒的时间（传统的 STP 需要大约 50 秒）。

工作原理

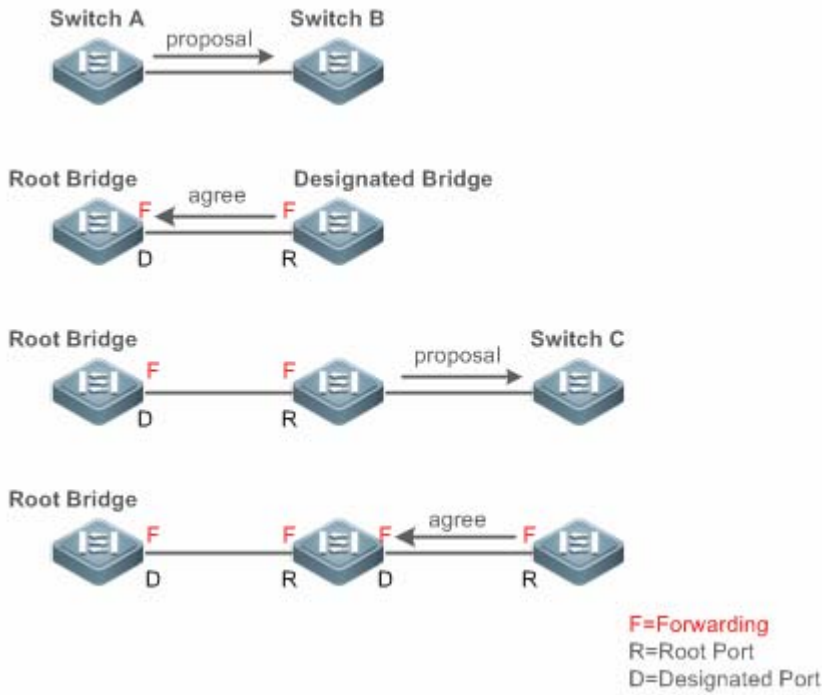
▾ RSTP 的快速收敛

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

STP 协议是选好端口角色（Port Role）后等待 30 秒（为 2 倍的 Forward-Delay Time，Forward-Delay Time 可配置，默认为 15 秒）再 Forwarding 的，而且每当拓扑发生变化后，每个网桥重新选出的 Root Port 和 Designated Port 都要经过 30 秒再 Forwarding，因此要等整个网络拓扑稳定为一个树型结构就大约需要 50 秒。

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

图 5-4



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

以下列出了“非点对点连接”的范例图。

非点对点连接范例：

图 5-5

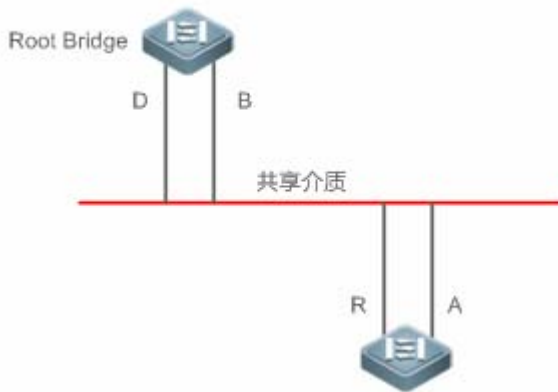
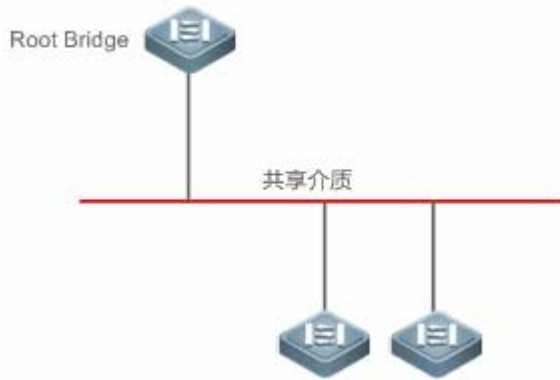
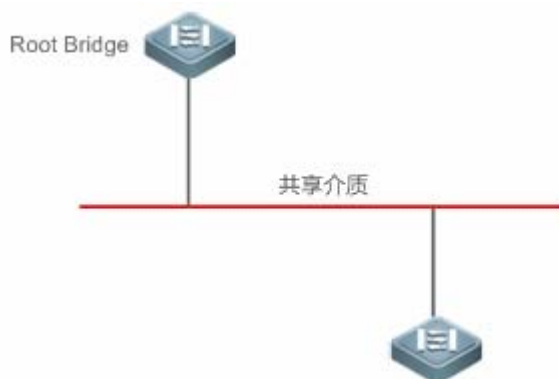


图 5-6



下图为“点对点”连接，请用户注意区分

图 5-7



▾ RSTP 与 STP 的兼容

RSTP 协议可以与 STP 协议完全兼容，RSTP 协议会根据收到的 BPDU 版本号来自动判断与之相连的网桥是支持 STP 协议还是支持 RSTP 协议，如果是与 STP 网桥互连就只能按 STP 的 Forwarding 方法，过 30 秒再 Forwarding，无法发挥 RSTP 的最大功效。

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

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

图 5-8

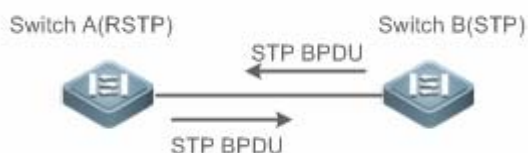
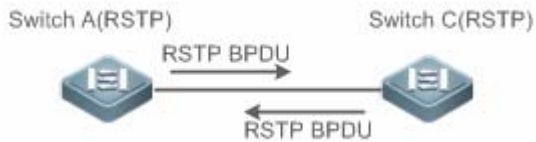


图 5-9



相关配置

配置 Protocol Migration 处理

使用 `clear spanning-tree detected-protocols [interface interface-id]` 命令可以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。

5.2.3 MSTP 协议

MSTP (Multiple Spanning Tree Protocol), 多生成树协议, 它可以弥补 STP、RSTP 的缺陷, 既可以快速收敛, 也能使不同 VLAN 的流量沿各自的路径转发, 从而为冗余链路提供了更好的负载分担机制。

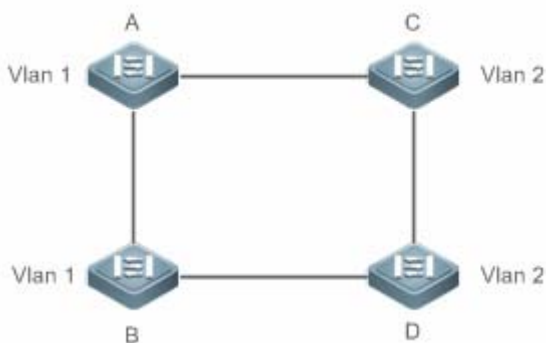
工作原理

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

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

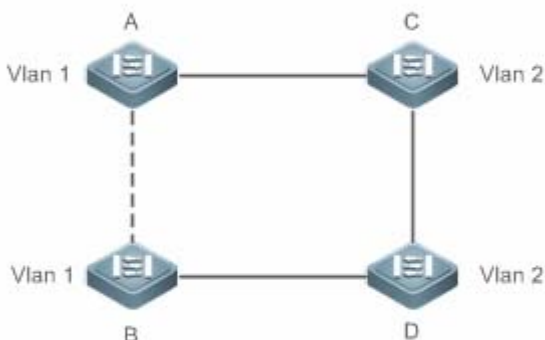
如下图所示, 设备 A、B 在 Vlan1 内, 设备 C、D 在 Vlan2 内, 然后连成环路。

图 5-10



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。

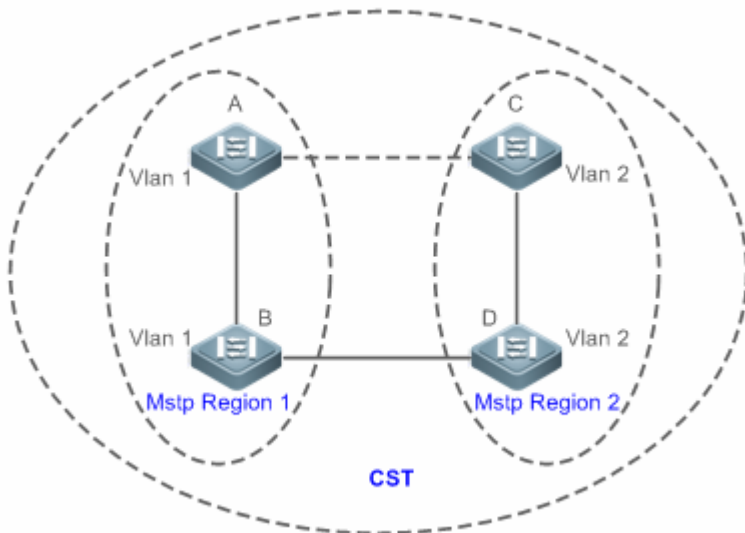
图 5-11



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

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

图 5-12



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。

📌 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，所以系统最多可以支持 65 个 Instance。用户还可以按需要分配 1-4094 个 Vlan 属于不同的 Instance（0 - 64），未分配的 Vlan 缺省就属于 Instance 0。这样，每个 MSTI（MST Instance）就是一个“Vlan 组”，根据 BPDU 里的 MSTI 信息进行 MSTI 内部的生成树算法，不受 CIST 和其他 MSTI 的影响。

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

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

i 建议在关闭 MSTP 模式后配置 Instance—vlan 的对应表，配置好后再打开 MSTP，以保证网络拓扑的稳定和收敛。

📌 IST（MSTP region 内的生成树）

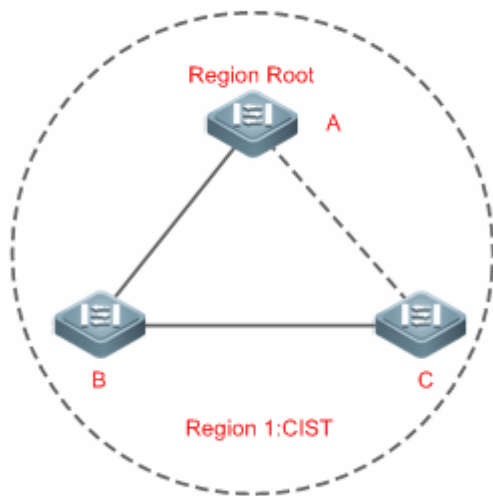
划分好 MSTP Region 后,每个 Region 里就按各个 Instance 所设置的 Bridge Priority、Port Priority 等参数选出各个 Instance 独立的 Root Bridge,以及每台设备上各个端口的 Port Role,然后就 Port Role 指定该端口在该 Instance 内是 FORWARDING 还是 DISCARDING 的。

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、不含环路的网络拓扑。

如下图所示,在 Region 1 内,设备 A、B、C 组成环路。

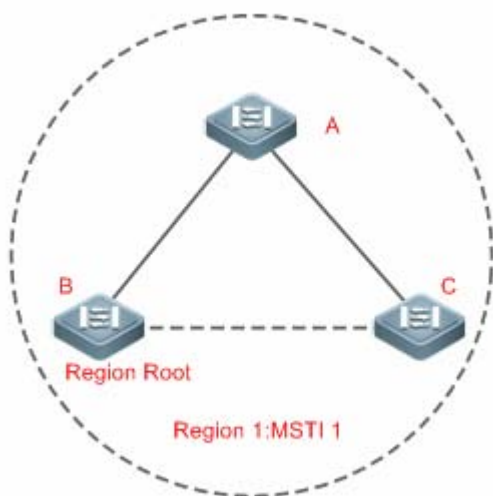
在 CIST (Instance 0) 中,如图 17,因 A 的优先级最高,被选为 Region Root,再根据其他参数,把 A 和 C 间的链路给 DISCARDING。因此,对 Instance 0 的“Vlan 组”来说,只有 A 到 B、B 到 C 的链路可用,打断了这个“Vlan 组”的环路。

图 5-13



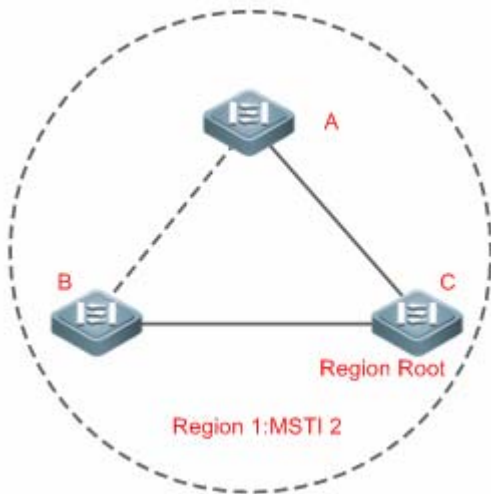
而对 MSTI 1 (Instance 1) 来说,如图 18, B 的优先级最高,被选为 Region Root,再根据其他参数,把 B 和 C 间的链路给 DISCARDING。因此,对 Instance 1 的“Vlan 组”来说,只有 A 到 B、A 到 C 的链路可用,打断了这个“Vlan 组”的环路。

图 5-14



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 5-15

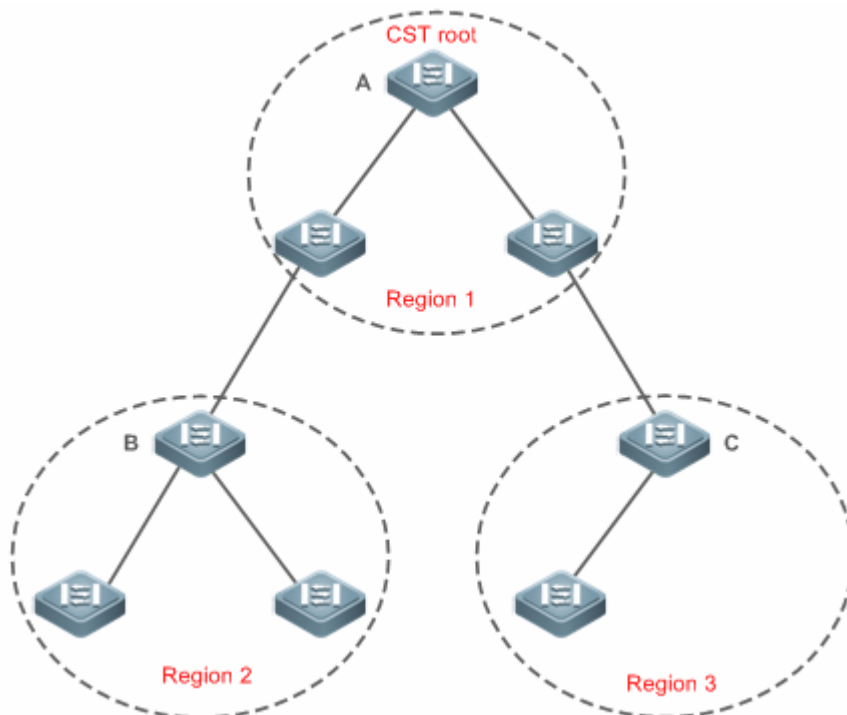


用户在这里要注意的是 MSTP 协议本身不关心一个端口属于哪个 Vlan ,所以用户应该根据实际的 Vlan 配置情况来为相关端口配置对应的 Path Cost 和 Priority ,以防 MSTP 协议打断了不该打断的环路。

📌 CST (MSTP region 间的生成树)

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

图 5-16



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

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

↘ 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”章节内容。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。

相关配置

↘ 配置 STP 的模式

缺省情况下, STP 模式是 MSTP。

使用 `spanning-tree mode [stp | rstp | mstp]` 命令可以修改 STP 模式。

5.2.4 MSTP 的可选特性

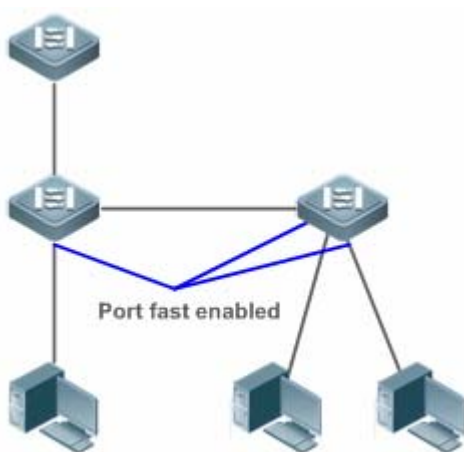
MSTP 的可选特性, 主要包括 Port Fast 端口设置、BPDU Guard 设置、BPDU Filter 设置、TC Guard 和 Guard 模式设置等。主要用来在 MSTP 的组网应用中, 能够根据网络的拓扑结构和应用特点, 针对性地进行 MSTP 的配置部署, 增加 MSTP 协议运行的稳定性、健壮性和抗攻击性, 满足 MSTP 协议在不同用户场景的应用需求。

工作原理

↘ 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 5-17



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。

↘ BPDU Guard

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

可以在全局模式中用 `spanning-tree portfast bpduguard default` 命令打开全局的 BPDU Guard enabled 状态, 在这种状态下, 如果某个 Interface 打开了 Port Fast, 或该接口自动识别为边缘口, 而该 Interface 收到了 BPDU, 该端口就会进入

Error-disabled 状态,以示配置错误;同时整个端口被关闭,表示网络中可能被非法用户增加了一台网络设备,使网络拓扑发生改变。

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

📌 BPDU Filter

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

可以在全局模式中用 spanning-tree portfast bpdufilter default 命令打开全局的 BPDU Filter enabled 状态,在这种状态下,Port Fast enabled 的 Interface 将既不收 BPDU,也不发 BPDU,这样,直连 Port Fast enabled 端口的主机就收不到 BPDU。而如果 Port Fast enabled 的 Interface 因收到 BPDU 而使 Port Fast Operational 状态 disabled,BPDU Filter 也就自动失效。

也可以在 Interface 配置模式下用 spanning-tree bpdufilter enable 命令设置了单个 Interface 的 BPDU Filter enable (与该端口是否打开 Port Fast 无关)。在这个情况下该 Interface 既不收 BPDU,也不发 BPDU,并且是直接 Forwarding 的。

📌 Tc-protection

TC-BPDU 报文是指携带 TC 标志的 BPDU 报文,交换机收到这类报文表示网络拓扑发生了变化,会进行 MAC 地址表的删除操作,对三层交换机,还会引发快转模块的重新打通操作,并改变 ARP 表项的端口状态。为避免交换机受到伪造 TC-BPDU 报文的恶意攻击时频繁进行以上操作,负荷过重,影响网络稳定,可以使用 TC-protection 功能进行保护。

Tc-protection 只能全局的打开和关闭,缺省情况下为关闭此功能。

在打开相应功能时,收到 TC-BPDU 报文后的一定时间内(一般为 4 秒),只进行一次删除操作,同时监控该时间段内是否收到 TC-BPDU 报文。如果在该时间段内收到了 TC-BPDU 报文,则设备在该时间超时后再进行一次删除操作。这样可以避免频繁的删除 MAC 地址表项和 ARP 表项。

📌 TC Guard

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

- ⚠️ 错误的使用 tc-guard 功能会使网络之间的通讯中断。
- ⚠️ 建议在确认网络当中有非法的 tc 报文攻击的情况下再打开此功能。
- ⚠️ 打开全局的 tc-guard,则所有端口都不会对外扩散 tc 报文。适用于桌面接入设备上开启。
- ⚠️ 打开接口的 tc-guard,则对于该接口产生的拓扑变化以及收到的 tc 报文,将不向其它端口扩散。适合在上链口,尤其是汇聚接核心的端口开启该功能。

📌 TC 过滤

配置 TC Guard 功能,端口将不扩散 TC 报文到本设备上其它参与生成树计算的端口,这里的不扩散包括了两种情况:一种是端口收到的 TC 报文不扩散,一种是端口自己产生的 TC 报文不扩散。端口自己产生的 TC 报文是指当端口转发状态发生变化时(例如从 block 到 forwarding 的转变),端口会产生 TC 报文,表示拓扑可能发生了变化。

这样,可能引发的问题时,由于 TC Guard 阻止了 TC 报文的扩散,导致当发生拓扑变化的时候,设备没有清除相应端口的 MAC 地址,转发数据出错。

因此,引入了 TC 过滤的概念。TC 过滤是指对于端口收到的 TC 报文不处理,而正常的拓扑变化的情况,能够处理。这样,解决了未配置 Portfast 的端口频繁地 UP/DOWN 引起的清地址和核心路由中断的问题,又能保证发生拓扑变化时,核心路由表项能够得到及时地更新。

- ⚠️ TC 过滤功能缺省关闭。

▾ 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。

▾ 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。

▾ 边缘口的自动识别

指派口在一定的时间内(为 3 秒),如果收不到下游端口发送的 BPDU,则认为该端口相连的是一台网络设备,从而设置该端口为边缘端口,直接进入 Forwarding 状态。自动标识为边缘口的端口因收到 BPDU 而自动识别为非边缘口。

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

该功能是缺省打开的。

- ⚠ 边缘口的自动标识功能与手工的 Port Fast 冲突时,以手工配置的为准。
- ⚠ 该功能作用于指派口与下游端口进行快速协商转发的过程中,所以 STP 协议不支持该功能。同时如果指派口已经处于转发状态,对该端口进行 Autoedge 的配置不会生效,只有在重新快速协商的过程中才生效,如拔插网线。
- ⚠ 端口如果先打开了 BPDU Filter,则该端口直接 Forwarding,不会自动识别为边缘口。
- ⚠ 该功能只适用与指派口。

▾ ROOT Guard 功能

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

接口打开 Root Guard 功能时,强制其在所有实例上的端口角色为指定端口,一旦该端口收到优先级更高的配置信息时,Root Guard 功能会将该接口置为 root-inconsistent (blocked)状态,在足够长的时间内没有收到更优的配置信息时,端口会恢复成原来的正常状态。

当端口因 Root Guard 而处于 blocked 状态时,可以通过手动恢复为正常状态,即关闭端口的 ROOT Guard 功能或关闭接口的保护功能(在接口模式下配置 spanning-tree guard none)。


- ⚠ 错误的使用 ROOT Guard 特性会导致网络链路的断开。
- ⚠ 在非指派口上打开 ROOT Guard 功能会强制其为指派口,同时端口会进入 BKN 状态,该状态表示端口因 Root 不一致而进入 blocked 状态。
- ⚠ 如果端口在 MST0 因收到更优的配置消息而进入 BKN 状态,会强制端口在其它所有的实例中处于 BKN 状态。
- ⚠ 端口的 ROOT Guard 和 LOOP Guard 同一时刻只能有一个生效。

▾ LOOP Guard 功能

由于单向链路的故障,根口或备份口由于收不到 BPDU 会变成指派口进入转发状态,从而导致了网络中环路产生,LOOP Guard 功能防止了这种情况的发生。


对于配置了环路保护的端口,如果收不到 BPDU,会进行端口角色的迁移,但端口状态将一直被设成 discarding 状态。直到重新收到 BPDU 而进行生成树的重计算。


- ⚠ 可以基于全局或接口打开 LOOP Guard 特性。
- ⚠ 端口的 ROOT Guard 和 LOOP Guard 同一时刻只能有一个生效。

 MSTP 进程重启前，端口进入环路保护的 block 状态，而 MSTP 进程重启后，如果端口仍然接收不到 BPDU，则端口将转变成指派口并进入 forward 状态。因此，建议在重启 MSTP 进程前，检查端口进入环路保护的 block 状态的原因并及时解决，避免进程重启后生成树拓扑仍然出现异常。

📌 BPDU 透传

在 IEEE 802.1Q 标准中，BPDU 的目的 MAC 地址 01-80-C2-00-00-00 是作为保留地址使用的，即遵循 IEEE 802.1Q 标准的设备，对于接收到的 BPDU 帧是不转发的。然而，在实际的网络部署中，可能需要设备能够支持透传 BPDU 帧。例如，设备未开启 STP 协议时，需要透传 BPDU 帧，使得与之互连的设备之间的生成树计算正常。

 BPDU 透传默认关闭。

 BPDU 透传功能只在 STP 协议关闭时才起作用。当 STP 协议打开时，设备不透传 BPDU 帧。

相关配置

📌 配置接口的 Portfast 开关

缺省情况下，接口上的 Port Fast 开关是关闭的。

在全局配置模式下，使用 **spanning-tree portfast default** 命令可以打开所有接口的 Portfast 开关；使用 **no spanning-tree portfast default** 命令关闭所有接口的 portfast 开关。

在接口配置模式下使用 **spanning-tree portfast** 命令可以打开某个接口的 Portfast 开关；使用 **spanning-tree portfastdisabled** 命令关闭某个接口的 portfast 开关。

📌 配置接口的 BPDU guard 开关

缺省情况下，接口上的 BPDU guard 开关是关闭的。

在全局配置模式下，使用 **spanning-tree portfast bpduguard default** 命令可以打开所有接口的 BPDU guard 开关；使用 **no spanning-tree portfast bpduguard default** 命令关闭所有接口的 BPDU guard 开关。

在接口配置模式下使用 **spanning-tree bpduguardenabled** 命令可以打开某个接口的 BPDU guard 开关；使用 **spanning-tree bpduguarddisabled** 命令关闭某个接口的 BPDU guard 开关。

📌 配置接口的 BPDU Filter 开关

缺省情况下，接口上的 BPDU Filter 开关是关闭的。

在全局配置模式下，使用 **spanning-tree portfast bpdufilter default** 命令可以打开所有接口的 BPDU Filter 开关；使用 **no spanning-tree portfast bpdufilter default** 命令关闭所有接口的 BPDU Filter 开关。

在接口配置模式下使用 **spanning-tree bpdufilter enabled** 命令可以打开某个接口的 BPDU Filter 开关，使用 **spanning-tree bpdufilter disabled** 命令关闭某个接口的 BPDU Filter 开关。

📌 配置 Tc-protection 开关

缺省情况下，Tc-protection 开关是关闭的。

在全局配置模式下，使用 **spanning-tree tc-protection** 命令可以打开所有接口的 Tc-protection 开关，使用 **no spanning-tree tc-protection** 命令关闭所有接口的 Tc-protection 开关。

Tc-protection 只能全局的打开和关闭。

📌 配置接口的 TC Guard 开关

缺省情况下，接口上的 tc guard 开关是关闭的。

在全局配置模式下，使用 **spanning-tree tc-protection tc-guard** 命令可以打开所有接口的 tc guard 开关；使用 **no spanning-tree tc-protection tc-guard** 命令关闭所有接口的 tc guard 开关。

在接口配置模式下使用 **spanning-tree tc-guard** 命令可以打开某个接口的 tc guard 开关,使用 **no spanning-tree tc-guard** 命令关闭某个接口的 tc guard 开关。

配置接口的 TC 过滤开关

缺省情况下,接口上的 TC 过滤功能是关闭的。

在接口配置模式下使用 **spanning-tree ignore tc** 命令打开某个接口的 TC 过滤功能;使用 **no spanning-tree ignore tc** 命令关闭某个接口的 TC 过滤功能。

配置接口的 BPDU 源 MAC 检查

缺省情况下,接口上的 BPDU 源 MAC 检查功能是关闭的。

在接口配置模式下使用 **bpdu src-mac-check H.H.H** 命令打开某个接口的 BPDU 源 MAC 检查功能;使用 **no bpdu src-mac-check** 命令关闭某个接口的 BPDU 源 MAC 检查功能。

配置接口的边缘口自动识别功能

缺省情况下,接口上的边缘口自动识别功能是关闭的。

在接口配置模式下使用 **spanning-tree autoedge** 命令打开某个接口的边缘口自动识别功能;使用 **spanning-tree autoedgedisabled** 命令关闭某个接口的边缘口自动识别功能。

配置接口的 Root Guard 功能

缺省情况下,接口上的 Root Guard 功能是关闭的。

在接口配置模式下使用 **spanning-tree guard root** 命令打开某个接口的 Root Guard 功能;使用 **no spanning-tree guard root** 命令关闭某个接口的 Root Guard 功能。

配置接口的 Loop Guard 功能

缺省情况下,接口上的 Loop Guard 功能是关闭的。

在全局配置模式下,使用 **spanning-tree loopguard default** 命令打开所有接口的 Loop Guard 功能,使用 **no spanning-tree loopguard default** 命令关闭所有接口的 Loop Guard 功能。

在接口配置模式下使用 **spanning-tree guard loop** 命令打开某个接口的 Loop Guard 功能;使用 **no spanning-tree guard loop** 命令关闭某个接口的 Loop Guard 功能。



配置 BPDU 透传功能

缺省情况下,BPDU 透传功能是关闭的。

在全局配置模式下,使用 **bridge-frame forwarding protocol bpdu** 命令打开 BPDU 透传功能;使用 **no bridge-frame forwarding protocol bpdu** 命令关闭 BPDU 透传。

BPDU 透传功能只在 STP 协议关闭时才起作用。当 STP 协议打开时,设备不透传 BPDU 帧。

5.3 配置详解

配置项	配置建议&相关命令	
打开生成树协议	 必须配置。用于打开生成树协议。	
	spanning-tree	打开生成树协议,并配置基本属性
	spanning-tree mode	配置生成树模式
配置生成树的兼容性	 可选配置。用于兼容友商设备。	

	spanning-tree compatible enable	打开接口的兼容模式
	clear spanning-tree detected-protocols	对 BPDU 进行强制版本检查
配置MSTP Region	⚠️ 可选配置。用于配置 MSTP Region。	
	spanning-tree mst configuration	进入 MSTP Region 配置模式
配置RSTP快速收敛	⚠️ 可选配置。用于配置端口的连接类型是不是“点对点连接”。	
	spanning-tree link-type	配置 link type
配置优先级	⚠️ 可选配置。用于配置设备优先级或者端口优先级。	
	spanning-tree priority	配置设备优先级
	spanning-tree port-priority	配置端口优先级
配置接口的路径花费	⚠️ 可选配置。用于配置端口的路径花费或路径花费缺省计算方法。	
	spanning-tree cost	配置端口的路径花费
	spanning-tree pathcost method	配置路径花费的缺省计算方法
配置BPDU帧的最大跳数	⚠️ 可选配置。用于配置 BPDU 帧的最大跳数。	
	spanning-tree max-hops	配置 BPDU 帧的最大跳数。
配置接口port fast的相关特性	⚠️ 可选配置。用于配置 port fast 特性。	
	spanning-tree portfast	打开 port fast 特性
	spanning-tree portfast bpduguard default	打开所有接口的 BPDU Guard
	spanning-tree bpduguard enabled	打开某个接口的 BPDU Guard
	spanning-tree portfast bpdufilter default	打开所有接口的 BPDU Filter
	spanning-tree bpdufilter enabled	打开某个接口的 BPDU Filter
配置TC相关的特性	⚠️ 可选配置。用于配置 TC 特性。	
	spanning-tree tc-protection	打开 tc protection
	spanning-tree tc-protection tc-guard	打开所有接口的 tc guard
	spanning-tree tc-guard	打开某个接口的 tc guard
	spanning-tree ignore tc	打开某个接口的 tc 过滤
配置BPDU源MAC检查	⚠️ 可选配置。用于配置 BPDU 源 MAC 检查功能。	
	bpdu src-mac-check	打开某个接口的 BPDU 源 MAC 检查
配置边缘口的自动识别	⚠️ 可选配置。用于配置边缘口的自动识别功能。	
	spanning-tree autoedge	打开某个接口的边缘口自动识别，缺省是打开的。
配置接口保护相关的特性	⚠️ 可选配置。用于配置接口保护相关的功能。	
	spanning-tree guard root	打开某个接口的 root guard
	spanning-tree loopguard default	打开所有接口的 loop guard
	spanning-tree guard loop	打开某个接口的 loop guard
	spanning-tree guard none	关闭某个接口的 guard 特性
配置BPDU透传功能	⚠️ 可选配置。用于配置 BPDU 透传功能。	
	bridge-frame forwarding protocol bpdu	打开 BPDU 透传功能

5.3.1 打开生成树协议

配置效果

- 打开全局 Spanning Tree 协议，同时设置全局的基本设置
- 配置 Spanning Tree 模式

注意事项

- 缺省情况下，Spanning Tree 协议是关闭的；当打开 Spanning Tree 协议时，设备即开始运行生成树协议，本设备缺省运行的是 MSTP 协议。
- Spanning Tree 协议的缺省模式是 MSTP 模式。
- Spanning Tree 协议与数据中心的 TRILL 协议功能互斥。

配置方法

打开 Spanning Tree 协议

- 必须配置。
- 若无特殊要求，应在每台设备上启动 Spanning Tree 协议。

配置 Spanning Tree 模式

- 可选配置
- 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。

检验方法

- 显示验证

相关命令

打开 Spanning Tree 协议

【命令格式】 **spanning-tree** [**forward-time** *seconds* | **hello-time***seconds* | **max-age***seconds*] **tx-hold-count** *numbers*

【参数说明】 **forward-time***seconds*：端口状态改变的时间间隔，取值范围为 4-30 秒，缺省值为 15 秒。

hello-time*seconds*：设备定时发送 BPDU 报文的时间间隔，取值范围为 1-10 秒，缺省值为 2 秒。

max-age*second*：BPDU 报文消息生存的最长时间，取值范围为 6-40 秒，缺省值为 20 秒。

tx-hold-count *numbers*：配置每秒最多发送 BPDU 个数，取值范围为 1-10 个，缺省值为 3 个。

【命令模式】 全局配置模式

【使用指导】 **forward-time**、**hello-time**、**max-age** 三个值的范围是相关的，修改了其中一个会影响到其他两个的值范围。这三个值之间有一个制约关系：

$2 * (\text{Hello Time} + 1.0 \text{ second}) \leq \text{Max-Age Time} \leq 2 * (\text{Forward-Delay} - 1.0 \text{ second})$

您配置的这三个参数必须满足这个条件，否则有可能导致拓扑不稳定，也会设置不成功。

配置 Spanning Tree 模式

【命令格式】 **spanning-tree mode** [**stp** | **rstp** | **mstp**]

【参数说明】 **stp**：Spanning tree protocol(IEEE 802.1d)

rstp：Rapid spanning tree protocol(IEEE 802.1w)

mstp : Multiple spanning tree protocol(IEEE 802.1s)

【命令模式】 全局配置模式

【使用指导】 有些友商产品不完全按标准实现，可能会导致一些兼容性的问题。在管理员发现其他厂家的设备与本设备不兼容时，使用此命令可以切换到低版本的 Spanning Tree 模式，以兼容之。

配置举例

配置 Spanning Tree 协议和定时器参数

【网络环境】

图 5-18



【配置方法】

- 设备开启生成树协议，同时配置生成树协议模式为 STP 协议。
- 配置根桥 DEV A 的定时器参数为：Hello Time=4s，Max Age=25s，Forward Delay=18s。

DEV A

第一步，开启生成树协议，同时配置生成树协议模式为 STP 协议。

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#spanning-tree
Ruijie(config)#spanning-treemode stp
```

第二步，配置根桥 DEV A 的定时器参数

```
Ruijie(config)#spanning-treehello-time 4
Ruijie(config)#spanning-treemax-age 25
Ruijie(config)#spanning-treeforward-time 18
```

DEV B

第一步，开启生成树协议，同时配置生成树协议模式为 STP 协议。

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#spanning-tree
Ruijie(config)#spanning-treemode stp
```

【检验方法】

- 通过 **show spanning-tree summary** 查看生成树拓扑和协议配置参数。

DEV A

```
Ruijie#show spanning-tree summary

Spanning tree enabled protocol stp
  Root ID    Priority    0
             Address    00d0.f822.3344
             this bridge is root
             Hello Time 4 sec Forward Delay 18 sec Max Age 25 sec

  Bridge ID  Priority    0
             Address    00d0.f822.3344
             Hello Time 4 sec Forward Delay 18 sec Max Age 25 sec

Interface    Role Sts Cost      Prio    OperEdge Type
-----
Gi0/2        Desg FWD 20000    128     False   P2p
Gi0/1        Desg FWD 20000    128     False   P2p
```

DEV B

```
Ruijie#show spanning-tree summary

Spanning tree enabled protocol stp
  Root ID    Priority    0
             Address    00d0.f822.3344
             this bridge is root
             Hello Time 4 sec Forward Delay 18 sec Max Age 25 sec

  Bridge ID  Priority    32768
             Address    001a.a917.78cc
             Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec

Interface      Role Sts Cost      Prio  OperEdge Type
-----
Gi0/2          Altn BLK 20000    128   False  P2p Bound(STP)
Gi0/1          Root FWD 20000    128   False  P2p Bound(STP)
```

常见错误

- 配置生成树协议定时器相关参数，只有在设备选举为生成树的根桥时才起作用。即非根桥的定时器参数是以根桥的定时器参数为准。

5.3.2 配置生成树的兼容性

配置效果

- 配置接口的兼容性模式，可以实现与其它产商之间的互连。
- 配置Protocol Migration进行强制版本检查会影响 RSTP与STP的兼容。

注意事项

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

配置方法

配置接口的兼容性模式

- 可选配置

配置 Protocol Migration

- 可选配置
- 管理员发现对端设备可支持 RSTP 协议时，可将本设备设置为强制版本检查，强制两对接设备运行 RSTP 协议。

检验方法

- 显示验证。

相关命令

配置接口的兼容性模式

【命令格式】 **spanning-tree compatible enable**

【参数说明】 -

【命令模式】 接口模式

- 【使用指导】 打开接口的兼容模式，可以使当前端口的接口属性信息有选择性的携带 MSTI 的信息进行发送，以实现与其它产商之间的互连。

配置 Protocol Migration

- 【命令格式】 **clear spanning-tree detected-protocols [interface interface-id]**
- 【参数说明】 **interface interface-id** : 对应的接口
- 【命令模式】 特权模式
- 【使用指导】 此命令用来强制接口发送 RSTP BPDU 帧，对 BPDU 帧执行强制检查。

配置举例

配置 Spanning Tree 协议兼容模式

【网络环境】

图 5-19



- 【配置方法】
- 设备 A, B 配置实例 1, 2。实例 1 关联 VLAN 10，实例 2 关联 VLAN 20。
 - 端口 gi 0/1 属于 VLAN 10，gi 0/2 属于 VLAN 20，配置端口的生成树兼容模式。

DEV A

第一步，创建实例 1, 2。实例 1 关联 VLAN 10，实例 2 关联 VLAN 20。

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#spanning-tree mst configuration
Ruijie(config-mst)#instance 1 vlan 10
Ruijie(config-mst)#instance 2 vlan 20
```

第二步，配置端口所属的 VLAN，同时开启端口的生成树兼容模式。

```
Ruijie(config)#int gi 0/1
Ruijie(config-if-GigabitEthernet 0/1)#switchport access vlan 10
Ruijie(config-if-GigabitEthernet 0/1)#spanning-tree compatible enable
Ruijie(config-if-GigabitEthernet 0/1)#int gi 0/2
Ruijie(config-if-GigabitEthernet 0/2)#switchport access vlan 20
Ruijie(config-if-GigabitEthernet 0/2)#spanning-tree compatible enable
```

DEV B

同 DEV A。

- 【检验方法】
- 通过 **show spanning-tree summary** 查看生成树拓扑计算是否正确。

DEV A

```
Ruijie#show spanning-tree summary

Spanning tree enabled protocol mstp
MST 0 vlans map : 1-9, 11-19, 21-4094
  Root ID    Priority    32768
             Address     001a. a917. 78cc
             this bridge is root
             Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec

  Bridge ID  Priority    32768
```


DEV B

```

Address      001a.a917.78cc
Hello Time   2 sec Forward Delay 15 sec Max Age 20 sec

Interface      Role Sts Cost      Prio    OperEdge Type
-----
Gi0/2          Desg FWD 20000    128     False   P2p
Gi0/1          Desg FWD 20000    128     False   P2p

MST 1 vlans map : 10
  Region Root Priority  32768
                Address  001a.a917.78cc
                this bridge is region root

  Bridge ID Priority  32768
            Address  001a.a917.78cc

Interface      Role Sts Cost      Prio    OperEdge Type
-----
Gi0/1          Desg FWD 20000    128     False   P2p

MST 2 vlans map : 20
  Region Root Priority  32768
                Address  001a.a917.78cc
                this bridge is region root

  Bridge ID Priority  32768
            Address  001a.a917.78cc

Interface      Role Sts Cost      Prio    OperEdge Type
-----
Gi0/2          Desg FWD 20000    128     False   P2p
Ruijie#show spanning-tree summary

Spanning tree enabled protocol mstp
MST 0 vlans map : 1-9, 11-19, 21-4094
  Root ID      Priority  32768
                Address  001a.a917.78cc
                this bridge is root
                Hello Time  2 sec Forward Delay 15 sec Max Age 20 sec

  Bridge ID Priority  32768
            Address  00d0.f822.3344
            Hello Time  4 sec Forward Delay 18 sec Max Age 25 sec

Interface      Role Sts Cost      Prio    OperEdge Type
-----
Gi0/2          Altn BLK 20000    128     False   P2p
Gi0/1          Root FWD 20000    128     False   P2p

MST 1 vlans map : 10
  Region Root Priority  32768
                Address  001a.a917.78cc
                this bridge is region root

  Bridge ID Priority  32768
            Address  00d0.f822.3344

Interface      Role Sts Cost      Prio    OperEdge Type
-----

```

```

Gi0/1          Root FWD 20000    128    False   P2p

MST 2 vlans map : 20
  Region Root Priority   32768
                Address   001a. a917. 78cc
                this bridge is region root

  Bridge ID Priority     32768
                Address   00d0. f822. 3344

Interface      Role Sts Cost      Prio    OperEdge Type
-----
Gi0/2          Root FWD 20000    128    False   P2p

```

常见错误

- 配置端口的兼容模式，需要关注端口的 VLAN 裁剪信息。建议链路两端的端口 VLAN 列表配置一致。

5.3.3 配置MSTP Region

配置效果

- 配置 MSTP Region 可以改变哪些设备处于同一个 MSTP Region 内，从而影响网络拓扑。

注意事项

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

配置方法

配置 MSTP Region

- 可选配置
- 要让多台设备处于同一个 MSTP Region 时配置。
- 通过 **instance instance-id vlan vlan-range** 命令配置 MST Instance 与 Vlan 的对应关系。
- 通过 **name name** 命令配置 MST 名称。
- 通过 **revision version** 命令配置 MST 版本号。

检验方法

- 显示验证。

相关命令

进入 MSTP Region 配置模式

- 【命令格式】 **spanning-tree mst configuration**
- 【参数说明】 -
- 【命令模式】 全局配置模式
- 【使用指导】 进入 MST 配置模式后，

配置 MST Instance 与 Vlan 的对应关系

【命令格式】 **Instance** *instance-id* **vlan** *vlan-range*

【参数说明】 *instance-id* : MST Instance ID, 范围为 0 - 64。

vlan-range : VLAN ID, 范围为 1 - 4094。

【命令模式】 MST 配置模式

【使用指导】 把 vlan 组添加到一个 MST instance 中使用此命令。

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。

配置 MST 名称

【命令格式】 **name** *name*

【参数说明】 *name* : MST 配置名称，该字符串最多可以有 32 个字节。

【命令模式】 MST 配置模式

【使用指导】 -

配置 MST 版本号

【命令格式】 **revision** *version*

【参数说明】 *version* : 指定 MST revision number, 范围为 0 - 65535。缺省值为 0

【命令模式】 MST 配置模式

【使用指导】 -

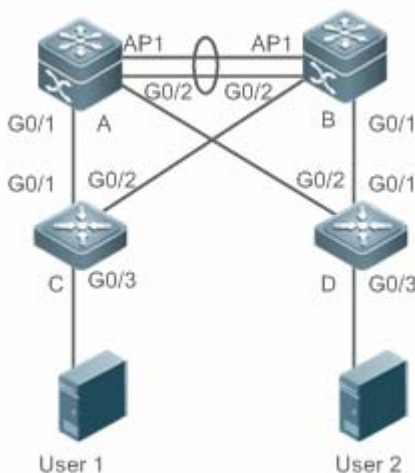
配置举例

i 以下配置举例，仅介绍与 MSTP 和 VRRP 相关的配置。

在 MSTP+VRRP 拓扑中，配置 MSTP 协议，实现 VLAN 的负载均衡

【网络环境】

图 5-20



【配置方法】

- 在交换机 A, B, C, D 上，打开 MSTP 协议，创建实例 1, 2。
- 配置交换机 A 为 MSTP 的实例 0 和 1 的根桥，交换机 B 为实例 2 的根桥。
- 配置交换机 A 为 VLAN 1, 10 的 VRRP 的 Master 设备，交换机 B 为 VLAN 20 的 VRRP 的 Master 设备。

A

第一步，配置 VLAN 10, 20，同时设备互联端口配置成 Trunk 口

```
A(config)#vlan 10
A(config-vlan)#vlan 20
A(config-vlan)#exit
A(config)#int range gi 0/1-2
A(config-if-range)#switchport mode trunk
A(config-if-range)#int ag 1
A(config-if-AggregatePort 1)# switchport mode trunk
```

第二步，打开 MSTP，同时创建实例 1, 2

```
A(config)#spanning-tree
A(config)# spanning-tree mst configuration
A(config-mst)#instance 1 vlan 10
A(config-mst)#instance 2 vlan 20
A(config-mst)#exit
```

第三步，配置设备 A 为实例 0 和 1 的根桥

```
A(config)#spanning-tree mst 0 priority 4096
A(config)#spanning-tree mst 1 priority 4096
A(config)#spanning-tree mst 2 priority 8192
```

第四步，配置 VRRP 的优先级，使设备 A 为 VLAN 10 的 VRRP Master 设备，同时配置 VRRP 虚网关 IP 地址

```
A(config)#interface vlan 10
A(config-if-VLAN 10)ip address 192.168.10.2 255.255.255.0
A(config-if-VLAN 10) vrrp 1 priority 120
A(config-if-VLAN 10) vrrp 1 ip 192.168.10.1
```

第五步，VRRP 的默认优先级为 100，使设备 A 为 VLAN 20 的 VRRP Backup 设备

```
A(config)#interface vlan 20
A(config-if-VLAN 20)ip address 192.168.20.2 255.255.255.0
A(config-if-VLAN 20)vrrp 1 ip 192.168.20.1
```

B

第一步，配置 VLAN 10, 20，同时设备互联端口配置成 Trunk 口

```
B(config)#vlan 10
B(config-vlan)#vlan 20
B(config-vlan)#exit
B(config)#int range gi 0/1-2
B(config-if-range)#switchport mode trunk
B(config-if-range)#int ag 1
B(config-if-AggregatePort 1)#switchport mode trunk
```

第二步，打开 MSTP，同时创建实例 1, 2

```
B(config)#spanning-tree
B(config)#spanning-tree mst configuration
B(config-mst)#instance 1 vlan 10
B(config-mst)#instance 2 vlan 20
B(config-mst)#exit
```

第三步，配置设备 A 为实例 2 的根桥

```
B(config)#spanning-tree mst 0 priority 8192
B(config)#spanning-tree mst 1 priority 8192
B(config)#spanning-tree mst 2 priority 4096
```

第四步，配置 VRRP 虚网关 IP 地址

```
B(config)#interface vlan 10
B(config-if-VLAN 10)ip address 192.168.10.3 255.255.255.0
B(config-if-VLAN 10)vrrp 1 ip 192.168.10.1
```

第五步，配置 VRRP 的优先级为 120，使设备 B 为 VLAN 20 的 VRRP Master 设备

```
B(config)#interface vlan 20
B(config-if-VLAN 20)vrrp 1 priority 120
B(config-if-VLAN 20)ip address 192.168.20.3 255.255.255.0
B(config-if-VLAN 20)vrrp 1 ip 192.168.20.1
```

C

第一步，配置 VLAN 10, 20，同时设备互联端口配置成 Trunk 口

```
C(config)#vlan 10
C(config-vlan)#vlan 20
C(config-vlan)#exit
C(config)#int range gi 0/1-2
C(config-if-range)#switchport mode trunk
```

第二步，打开 MSTP，同时创建实例 1, 2

```
C(config)#spanning-tree
C(config)#spanning-tree mst configuration
C(config-mst)#instance 1 vlan 10
C(config-mst)#instance 2 vlan 20
C(config-mst)#exit
```

第三步，配置设备 C 直接用户的端口为 Portfast 口，同时启用 BPDU Guard。

```
C(config)#int gi 0/3
C(config-if-GigabitEthernet 0/3)#spanning-tree portfast
C(config-if-GigabitEthernet 0/3)#spanning-tree bpduguard enable
```

D

同设备 C。

【检验方法】

- 通过 show spanning-tree summary 查看生成树拓扑计算的正确性。
- 通过 show vrrp brief 查看 VRRP 主备是否建立成功。

A

```
Ruijie#show spanning-tree summary

Spanning tree enabled protocol mstp
MST 0 vlans map : 1-9, 11-19, 21-4094
  Root ID    Priority    4096
            Address    00d0.f822.3344
            this bridge is root
            Hello Time 4 sec Forward Delay 18 sec Max Age 25 sec

  Bridge ID  Priority    4096
            Address    00d0.f822.3344
            Hello Time 4 sec Forward Delay 18 sec Max Age 25 sec

Interface    Role Sts Cost      Prio    OperEdge Type
-----
Ag1          Desg FWD 19000     128     False   P2p
Gi0/1        Desg FWD 200000    128     False   P2p
Gi0/2        Desg FWD 200000    128     False   P2p

MST 1 vlans map : 10
  Region Root Priority    4096
            Address    00d0.f822.3344
            this bridge is region root

  Bridge ID  Priority    4096
            Address    00d0.f822.3344

Interface    Role Sts Cost      Prio    OperEdge Type
-----
Ag1          Desg FWD 19000     128     False   P2p
```

```

Gi0/1          Desg FWD 200000    128    False  P2p
Gi0/2          Desg FWD 200000    128    False  P2p

```

```

MST 2 vlans map : 20
  Region Root Priority  4096
                Address  001a.a917.78cc
                this bridge is region root

```

```

  Bridge ID Priority  8192
            Address  00d0.f822.3344

```

```

Interface      Role Sts Cost      Prio    OperEdge Type
-----

```

```

Ag1            Root FWD 19000    128    False  P2p
Gi0/1          Desg FWD 200000  128    False  P2p
Gi0/2          Desg FWD 200000  128    False  P2p

```

B

```
Ruijie#show spanning-tree summary
```

```

Spanning tree enabled protocol mstp
MST 0 vlans map : 1-9, 11-19, 21-4094
  Root ID  Priority  4096
            Address  00d0.f822.3344
            this bridge is root
            Hello Time  4 sec  Forward Delay 18 sec  Max Age 25 sec

```

```

  Bridge ID Priority  8192
            Address  001a.a917.78cc
            Hello Time  2 sec  Forward Delay 15 sec  Max Age 20 sec

```

```

Interface      Role Sts Cost      Prio    OperEdge Type
-----

```

```

Ag1            Root FWD 19000    128    False  P2p
Gi0/1          Desg FWD 200000  128    False  P2p
Gi0/2          Desg FWD 200000  128    False  P2p

```

```

MST 1 vlans map : 10
  Region Root Priority  4096
                Address  00d0.f822.3344
                this bridge is region root

```

```

  Bridge ID Priority  8192
            Address  001a.a917.78cc

```

```

Interface      Role Sts Cost      Prio    OperEdge Type
-----

```

```

Ag1            Root FWD 19000    128    False  P2p
Gi0/1          Desg FWD 200000  128    False  P2p
Gi0/2          Desg FWD 200000  128    False  P2p

```

```

MST 2 vlans map : 20
  Region Root Priority  4096
                Address  001a.a917.78cc
                this bridge is region root

```

```

  Bridge ID Priority  4096
            Address  001a.a917.78cc

```

```

Interface      Role Sts Cost      Prio    OperEdge Type
-----

```

C

```

Ag1          Desg FWD 19000    128    False  P2p
Gi0/1        Desg FWD 200000   128    False  P2p
Gi0/2        Desg FWD 200000   128    False  P2p
Ruijie#show spanning-tree summary

Spanning tree enabled protocol mstp
MST 0 vlans map : 1-9, 11-19, 21-4094
  Root ID    Priority    4096
             Address    00d0.f822.3344
             this bridge is root
             Hello Time  4 sec  Forward Delay 18 sec  Max Age 25 sec

  Bridge ID  Priority    32768
             Address    001a.a979.00ea
             Hello Time  2 sec  Forward Delay 15 sec  Max Age 20 sec

Interface      Role Sts Cost      Prio    Type  OperEdge
-----
Fa0/2          Altn BLK 200000   128     P2p   False
Fa0/1          Root FWD 200000   128     P2p   False

MST 1 vlans map : 10
  Region Root Priority    4096
             Address    00d0.f822.3344
             this bridge is region root

  Bridge ID  Priority    32768
             Address    001a.a979.00ea

Interface      Role Sts Cost      Prio    Type  OperEdge
-----
Fa0/2          Altn BLK 200000   128     P2p   False
Fa0/1          Root FWD 200000   128     P2p   False

MST 2 vlans map : 20
  Region Root Priority    4096
             Address    001a.a917.78cc
             this bridge is region root

  Bridge ID  Priority    32768
             Address    001a.a979.00ea

Interface      Role Sts Cost      Prio    Type  OperEdge
-----
Fa0/2          Root FWD 200000   128     P2p   False
Fa0/1          Altn BLK 200000   128     P2p   False
略

```

D

常见错误

- MSTP 拓扑中，MST 域的配置建议配置一致。
- 配置实例和 VLAN 的映射关系时，VLAN 没有创建。
- 在 MSTP+VRRP 拓扑中，设备如果运行 STP 或 RSTP 协议，则该设备是按照不同 MST 域的算法进行生成树计算。

5.3.4 配置RSTP快速收敛

配置效果

- 配置 link-type 关系到 RSTP 是否能快速的收敛。

注意事项

- 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”。

配置方法

配置 link-type

- 可选配置

检验方法

- 显示验证。
- 使用 `show spanning-tree[mstinstance-id] interfaceinterface-id` 命令查看生成树接口的配置信息。

相关命令

配置 link-type

【命令格式】 `spanning-treelink-type [point-to-point | shared]`

【参数说明】 `point-to-point`：强制设置该接口的连接类型为 point-to-point

`shared`：强制设置该接口的连接类型为 shared

【命令模式】 接口配置模式

【使用指导】 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。当用户不设置该值时，设备会根据端口的“双工”状态来自动设置的。

配置举例

配置 RSTP 快速收敛

【配置方法】 配置端口的连接类型为点对点网络。

```
Ruijie(config)#int gi 0/1
Ruijie(config-if-GigabitEthernet 0/1)#spanning-tree link-type point-to-point
```

【检验方法】

- 通过 `show spanning-tree summary` 查看端口连接类型。

```
Ruijie#show spanning-tree summary

Spanning tree enabled protocol mstp
MST 0 vlans map : ALL
  Root ID    Priority    32768
             Address    001a.a917.78cc
             this bridge is root
             Hello Time  2 sec   Forward Delay 15 sec   Max Age 20 sec

  Bridge ID  Priority    32768
             Address    00d0.f822.3344
             Hello Time  2 sec   Forward Delay 15 sec   Max Age 20 sec

Interface      Role Sts Cost      Prio    OperEdge Type
-----
Gi0/1          Root FWD 20000    128     False   P2p
```


常见错误

- 端口的连接类型和速率、双工有关。如果是半双工，则连接类型为 shared。

5.3.5 配置优先级

配置效果

- 设置设备优先级 (Switch Priority) 关系着到底哪个设备为整个网络的根，同时也关系到整个网络的拓扑结构。
- 设置端口的优先级 (Port Priority) 关系着到底哪个端口进入 Forwarding 状态。

注意事项

- 建议管理员把核心设备的优先级设得高些 (数值小)，这样有利于整个网络的稳定。可以给不同的 Instance 分配不同的设备优先级，各个 Instance 可根据这些值运行独立的生成树协议。对于不同 Region 间的设备，它们只关心 CIST (Instance 0) 的优先级。如 Bridge ID 所讲，优先级的设置值有 16 个，都为 4096 的倍数，分别是 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440。缺省值为 32768。
- 当有两个端口都连在一个共享介质上，设备会选择高优先级 (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。
- 端口优先级和设备优先级一样，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。

配置方法

配置设备优先级

- 可选配置
- 在管理员需要改变网络的根或者拓扑结构时需要配置设备优先级。

配置端口优先级

- 可选配置
- 在管理员需要改变哪个端口优先进入 Forwarding 状态时配置。

检验方法

- 显示验证
- 使用 `show spanning-tree[mst instance-id] interface interface-id` 命令查看生成树接口的配置信息。

相关命令

配置设备优先级

【命令格式】 `spanning-tree[mst instance-id]priority priority`

【参数说明】 `mst instance-id` : Instance 号，范围为 0 - 64

`priority priority` : 设备优先级，可选用 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344 和 61440。共 16 个整数，均为 4096 的倍数。

【命令模式】 全局配置模式

【使用指导】 设置设备的优先级关系到哪个设备为整个网络的根，同时也关系到整个网络的拓扑结构。

配置端口优先级

【命令格式】 `spanning-tree [mstinstance-id] port-priority priority`

【参数说明】 **mstinstance-id** : Instance 号, 范围为 0 - 64。

port-priority priority : 端口优先级, 可选用 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240, 共 16 个整数, 均为 16 的倍数。

【命令模式】 接口配置模式

【使用指导】 在 Region 内形成环路时, 优先选择高优先级的端口处于发送状态。优先级相同时, 以选用接口号较小的端口。

使用此命令, 这将影响到 Region 内形成环路中的哪个端口会处于发送状态。

配置举例

配置端口优先级

【网络环境】

图 5-21



【配置方法】

- 配置网桥优先级, 使 DEV A 为生成树根桥。
- 配置 DEV A 的端口 gi 0/2 的端口优先级为 16, 使 DEV B 的端口 gi 0/2 选举为根端口。

DEV A

第一步, 打开生成树协议, 配置网桥优先级。

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

第二步, 配置端口 Gi 0/2 的端口优先级。

```
Ruijie(config)# int gi 0/2
Ruijie(config-if-GigabitEthernet 0/2)#spanning-tree mst 0 port-priority 16
```

DEV B

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

【检验方法】

- 通过 `show spanning-tree summary` 查看生成树拓扑计算结果。

DEV A

```
Ruijie# Ruijie#show spanning-tree summary

Spanning tree enabled protocol mstp
MST 0 vlans map : ALL
  Root ID    Priority    0
            Address    00d0.f822.3344
            this bridge is root
            Hello Time  2 sec  Forward Delay 15 sec  Max Age 20 sec

  Bridge ID  Priority    0
            Address    00d0.f822.3344
            Hello Time  2 sec  Forward Delay 15 sec  Max Age 20 sec

Interface    Role Sts Cost      Prio    OperEdge Type
-----
Gi0/2        Desg FWD 20000    16      False   P2p
Gi0/1        Desg FWD 20000    128     False   P2p
```

DEV B

```

Ruijie#show spanning-tree summary

Spanning tree enabled protocol mstp
MST 0 vlans map : ALL
  Root ID    Priority    0
            Address    00d0. f822. 3344
            this bridge is root
            Hello Time  2 sec  Forward Delay 15 sec  Max Age 20 sec

  Bridge ID  Priority    32768
            Address    001a. a917. 78cc
            Hello Time  2 sec  Forward Delay 15 sec  Max Age 20 sec

Interface          Role Sts Cost          Prio    OperEdge Type
-----
Gi0/2              Root FWD 20000         128     False    P2p
Gi0/1              Altn BLK 20000         128     False    P2p

```

常见错误

- 端口优先级只有在指派端口修改才起作用。

5.3.6 配置接口的路径花费

配置效果

- 端口的路径花费（Path Cost）会影响端口的转发状态，及影响整个网络的拓扑结构。
- 当某端口 Path Cost 为缺省值时，配置路径花费的计算方法会影响端口的路径花费计算结果。

注意事项

- 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。
- 当该端口 Path Cost 为缺省值时，设备会自动根据端口速率计算出该端口的 Path Cost。但 IEEE 802.1d-1998 和 IEEE 802.1t 对相同的链路速率规定了不同 Path Cost 值，802.1d-1998 的取值范围是短整型（short）（1—65535），802.1t 的取值范围是长整型（long）（1—200,000,000）。其中对于 AP 的 Cost 值有两个方案：我司的私有方案固定为物理口的 Cost 值*95%；标准推荐的方案为 20,000,000,000/(AP 的实际链路带宽)，其中 AP 的实际链路带宽为成员口的带宽*UP 成员口个数。请管理员一定要统一好整个网络内 Path Cost 的标准。缺省模式为私有长整型模式。
- 下表列出两种方法对不同链路速率自动设置的 Path Cost。

端口速率	Interface	IEEE 802.1d (short)	IEEE 802.1t (long)	IEEE 802.1t (long standard)
10M	普通端口	100	2000000	2000000
	Aggregate Link	95	1900000	2000000 ÷ linkupcnt
100M	普通端口	19	200000	200000
	Aggregate Link	18	190000	200000 ÷ linkupcnt
1000M	普通端口	4	20000	20000
	Aggregate Link	3	19000	20000 ÷ linkupcnt
10000M	普通端口	2	2000	2000
	Aggregate Link	1	1900	20000 ÷ linkupcnt

- 默认采用我司的私有长整型模式。修改成标准推荐方案的 path cost 方案后，AP 的 cost 会随着 UP 成员口数量的变化而变化，而端口 cost 值变化会导致网络拓扑发生变化。
- AP 为静态 AP 时，表格中的 linkupcnt 为 UP 成员口个数；AP 为 LACP AP 时，表格中的 linkupcnt 为参与 AP 数据转发的成员口个数；当 AP 内没有任何成员口 linkup 时，linkupcnt 为 1。具体 AP 和 LACP 的配置，请参见 AP 章节的说明。

配置方法

配置端口的路径花费

- 可选配置
- 在管理员需要数据报文优先走哪个端口或哪条路径时配置。

配置 Path Cost 的缺省计算方法

- 可选配置
- 在管理员需要修改路径花费计算方式时配置。

检验方法

- 显示验证。
- 使用 `show spanning-tree[mstinstance-id] interfaceinterface-id` 命令查看生成树接口的配置信息。

相关命令

配置端口的路径花费

- 【命令格式】 `spanning-tree [mstinstance-id]cost cost`
- 【参数说明】 `mstinstance-id`：Instance 号，范围为 0 - 64
`cost cost`：路径花费值，范围为 1 - 200,000,000
- 【命令模式】 接口配置模式
- 【使用指导】 `cost` 值越大表明路径花费越高。

配置 Path Cost 的缺省计算方法

- 【命令格式】 `spanning-tree pathcost method {long [standard] | short}`
- 【参数说明】 `long`：采用 802.1t 标准设定 path-cost 的值。
`standard`：standard 表示按照标准推荐的公式计算 cost 值。
`short`：采用 802.1d 标准设定 path-cost 的值。
- 【命令模式】 全局配置模式
- 【使用指导】 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。

配置举例

配置端口的路径花费

【网络环境】

图 5-22



【配置方法】

- 配置网桥优先级，使 DEV A 为生成树根桥。
- 配置 DEV B 的端口 gi 0/2 的端口路径花费为 1，使端口 gi 0/2 选举为根端口。

DEV A

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

DEV B

```
Ruijie(config)#spanning-tree
Ruijie(config)# int gi 0/2
Ruijie(config-if-GigabitEthernet 0/2)# spanning-tree cost 1
```

【检验方法】

- 通过 **show spanning-tree summary** 查看生成树拓扑计算结果。

DEV A

```
Ruijie# Ruijie#show spanning-tree summary

Spanning tree enabled protocol mstp
MST 0 vlans map : ALL
  Root ID   Priority   0
           Address   00d0.f822.3344
           this bridge is root
           Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec

  Bridge ID Priority   0
           Address   00d0.f822.3344
           Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec

Interface      Role Sts Cost      Prio   OperEdge Type
-----
Gi0/2          Desg FWD 20000    128    False   P2p
Gi0/1          Desg FWD 20000    128    False   P2p
```

DEV B

```
Ruijie#show spanning-tree summary

Spanning tree enabled protocol mstp
MST 0 vlans map : ALL
  Root ID   Priority   0
           Address   00d0.f822.3344
           this bridge is root
           Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec

  Bridge ID Priority   32768
           Address   001a.a917.78cc
           Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec

Interface      Role Sts Cost      Prio   OperEdge Type
-----
Gi0/2          Root FWD 1         128    False   P2p
Gi0/1          Altn BLK 20000    128    False   P2p
```

常见错误

- 修改端口路径花费，只有在接收端口配置才起作用。

5.3.7 配置BPDU帧的最大跳数

配置效果

- 配置 BPDU 帧的最大跳数 (Maximum-Hop Count) ，会影响 BPDU 的生命期，从而影响网络拓扑。

注意事项

- BPDU 帧最大跳数的缺省值是 20，一般不需要进行修改。

配置方法

▾ 配置 Maximum-Hop Count

- 可选配置。如果网络拓扑规模较大，使得 BPDU 帧的传递超过了默认的 20 跳，则建议更改 max-hops 配置。

检验方法

- 显示验证。

相关命令

▾ 设置 BPDU 帧的最大跳数

【命令格式】 **spanning-tree max-hops hop-count**

【参数说明】 *hop-count* : BPDU 在被丢弃之前可以经过设备的次数，范围为 1 - 40

【命令模式】 全局配置模式

【使用指导】 在 Region 内，Root Bridge 发送的 BPDU 包含一个 Hop Count 项，从 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。此命令指定了 BPDU 在一个 Region 内经过多少台设备后被丢弃。改变 max-hops 将影响到所有 Instance。

配置举例

▾ 设置 BPDU 帧的最大跳数

- 【配置方法】
- 配置 BPDU 帧的最大跳数为 25。

```
Ruijie(config)#spanning-tree max-hops 25
```

- 【检验方法】
- 通过 show spanning-tree 命令查看配置。

```
Ruijie# show spanning-tree
StpVersion : MSTP
SysStpStatus : ENABLED
MaxAge : 20
HelloTime : 2
ForwardDelay : 15
BridgeMaxAge : 20
BridgeHelloTime : 2
BridgeForwardDelay : 15
MaxHops: 25
TxHoldCount : 3
PathCostMethod : Long
BPDUGuard : Disabled
BPDUFilter : Disabled
LoopGuardDef : Disabled
```

```
##### mst 0 vlans map : ALL
BridgeAddr : 00d0.f822.3344
Priority: 0
TimeSinceTopologyChange : 2d:0h:46m:4s
TopologyChanges : 25
DesignatedRoot : 0.001a.a917.78cc
RootCost : 0
RootPort : GigabitEthernet 0/1
CistRegionRoot : 0.001a.a917.78cc
CistPathCost : 20000
```

常见错误

无

5.3.8 配置接口port fast的相关特性

配置效果

- 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。
- 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。
- 打开 BPDU Filter 后，相应端口会既不发，也不收 BPDU。

注意事项

- 打开某接口的 portfast，全局的 BPDU guard 配置才生效。
- 打开全局的 BPDU Filter enabled 状态下，Port Fast enabled 的 Interface 将既不收 BPDU，也不发 BPDU，这样，直连 Port Fast enabled 端口的主机就收不到 BPDU。而如果 Port Fast enabled 的 Interface 因收到 BPDU 而使 Port Fast Operational 状态 disabled，BPDU Filter 也就自动失效。
- 打开某接口的 portfast，全局的 BPDU filter 配置才生效。

配置方法

配置 port fast

- 可选配置
- 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。

打开 BPDU Guard

- 可选配置
- 如果设备的端口直连着网络终端，为了防止受到 BPDU 攻击导致生成树拓扑发生异常，可以在这些端口上配置 BPDU Guard 功能。开启 BPDU Guard 的端口收到 BPDU，端口会进入 Error-disabled 状态。
- 如果设备的端口直连着网络终端，为了防止端口下连出现环路，也可以配置 BPDU Guard 功能防止环路。该应用依赖下连设备（比如 HUB）能够转发 BPDU 帧。

打开 BPDU Filter

- 可选配置
- 为了防止异常的 BPDU 报文对生成树拓扑的影响，可以在端口配置 BPDU Filter 功能过滤掉这些异常的 BPDU。

检验方法

- 显示验证。
- 使用 **show spanning-tree[mstinstance-id] interfaceinterface-id** 命令查看生成树接口的配置信息。

相关命令

配置接口的 Port Fast

- 【命令格式】 **spanning-tree portfast**
- 【参数说明】 -
- 【命令模式】 接口配置模式
- 【使用指导】 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。

配置所有接口的 BPDU Guard

- 【命令格式】 **spanning-tree portfast bpduguard default**
- 【参数说明】 -
- 【命令模式】 全局配置模式
- 【使用指导】 打开 BPDU guard，如果在该端口上收到 BPDU，则会进入 error-disabled 状态。使用 show spanning-tree 命令查看设置。

配置某个接口的 BPDU Guard

- 【命令格式】 **spanning-tree bpduguardenabled**
- 【参数说明】 -
- 【命令模式】 接口配置模式
- 【使用指导】 打开单个接口的 BPDU Guard 的情况下，如果该接口收到了 BPDU，就进入 Error-disabled 状态。

配置所有接口的 BPDU Filter

- 【命令格式】 **spanning-tree portfast bpdufilter default**
- 【参数说明】 -
- 【命令模式】 全局配置模式
- 【使用指导】 打开 BPDU Filter 后，相应端口会既不发也不收 BPDU。

配置某个接口的 BPDU Filter

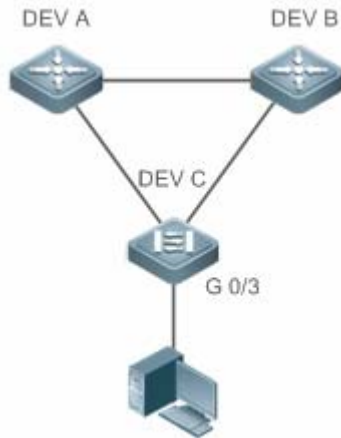
- 【命令格式】 **spanning-tree bpdufilter enabled**
- 【参数说明】 -
- 【命令模式】 接口配置模式
- 【使用指导】 打开 BPDU Filter 后，相应端口会既不发 BPDU，也不收 BPDU。

配置举例

配置端口的 Port Fast 特性

【网络环境】

图 5-23



【配置方法】

- 配置 DEV C 的端口 gi 0/3 为 Port Fast 端口，同时开启 BPDU Guard 功能。

DEV C

```

Ruijie(config)# int gi 0/3
Ruijie(config-if-GigabitEthernet 0/3)# spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, switches, bridges to this interface when portfast is
enabled, can cause temporary loops.
Ruijie(config-if-GigabitEthernet 0/3)#spanning-tree bpduguard enable
  
```

【检验方法】

- 通过 **show spanning-tree interface** 命令查看端口的配置信息。

DEV C

```

Ruijie#show spanning-tree int gi 0/3

PortAdminPortFast : Enabled
PortOperPortFast : Enabled
PortAdminAutoEdge : Enabled
PortOperAutoEdge : Enabled
PortAdminLinkType : auto
PortOperLinkType : point-to-point
PortBPDUGuard : Enabled
PortBPDUFilter : Disabled
PortGuardmode : None

##### MST 0 vlans mapped :ALL
PortState : forwarding
PortPriority : 128
PortDesignatedRoot : 0.00d0.f822.3344
PortDesignatedCost : 0
PortDesignatedBridge :0.00d0.f822.3344
PortDesignatedPortPriority : 128
PortDesignatedPort : 4
PortForwardTransitions : 1
PortAdminPathCost : 20000
PortOperPathCost : 20000
Inconsistent states : normal
PortRole : designatedPort
  
```

常见错误

无

5.3.9 配置TC相关的特性

配置效果

- 打开 TC Protection 功能时，收到 TC-BPDU 报文后的一定时间内（一般为 4 秒），只进行一次删除操作。这样可以避免频繁的删除 MAC 地址表项和 ARP 表项。
- 打开 TC Guard 后，当一个端口收到 TC 报文的时候，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。
- TC 过滤是指对于端口收到的 TC 报文不处理，而正常的拓扑变化的情况，能够处理。

注意事项

- 建议在确认网络当中有非法的 tc 报文攻击的情况下再打开 TC Guard 功能。

配置方法

打开 TC Protection 功能

- 可选配置
- 缺省是关闭的。

打开 TC Guard 功能

- 可选配置
- 缺省是关闭的。
- 需要过滤掉端口收到的 TC 报文或端口因拓扑变化自己产生的 TC 报文时，可以配置端口的 TC Guard 功能。

打开 TC 过滤功能

- 可选配置
- 缺省是关闭的。
- 只需要过滤掉端口收到的 TC 报文时，可以配置端口的 TC 过滤功能。

检验方法

- 显示验证。

相关命令

打开 tc protection

- 【命令格式】 **spanning-tree tc-protection**
- 【参数说明】 -
- 【命令模式】 全局配置模式
- 【使用指导】 -

配置所有接口的 tc guard

- 【命令格式】 **spanning-tree tc-protection tc-guard**
- 【参数说明】 -
- 【命令模式】 全局配置模式
- 【使用指导】 启用 tc-guard 功能，能防止 tc 报文的扩散。

配置某个接口的 tcguard

- 【命令格式】 **spanning-tree tc-guard**
- 【参数说明】 -
- 【命令模式】 接口配置模式
- 【使用指导】 启用 tc-guard 功能，能防止 tc 报文的扩散。

配置某个接口的 tc 过滤

- 【命令格式】 **spanning-tree ignore tc**
- 【参数说明】 -
- 【命令模式】 接口配置模式
- 【使用指导】 启用 tc 过滤功能，则端口收到的 TC 报文将不处理。

配置举例

配置端口的 TC Guard 功能

- 【配置方法】 配置端口的 TC Guard 功能

```
Ruijie(config)#int gi 0/1
Ruijie(config-if-GigabitEthernet 0/1)#spanning-tree tc-guard
```

- 【检验方法】
 - 通过 **show run interface** 命令查看端口的 TC Guard 配置。

```
Ruijie#show run int gi 0/1

Building configuration...
Current configuration : 134 bytes

interface GigabitEthernet 0/1
 switchport mode trunk
 spanning-tree tc-guard
```

常见错误

- 错误地配置 TC Guard 或 TC 过滤功能，可能会导致网络设备报文转发出错。比如在拓扑发生变化的情况下，没有及时清除 MAC 地址导致报文转发出错。

5.3.10 配置BPDU源MAC检查

配置效果

- 打开 BPDU 源 MAC 检查开关，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。

注意事项

- 当确定了某端口点对点链路对端相连的交换机时，可以配置 BPDU 源 MAC 检查来达到只接收对端交换机发送的 BPDU 帧。

配置方法

打开 BPDU 源 MAC 检查

- 可选配置
- 缺省是关闭的。
- 为了防止恶意的 BPDU 攻击，可以配置 BPDU 源 MAC 检查功能。

检验方法

- 显示验证。

相关命令

▾ 打开某个接口的 bpdu 源 mac 检查

【命令格式】 **bpdu src-mac-check H.H.H**

【参数说明】 *H.H.H*：表示只接收源 mac 地址为该地址的 bpdu 帧。

【命令模式】 接口模式

【使用指导】 使用 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。

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，且一个端口只允许配置一个过滤 MAC 地址。

配置举例

▾ 配置端口的 BPDU 源 MAC 检查功能

【配置方法】 配置端口的 BPDU 源 MAC 检查

```
Ruijie(config)#int gi 0/1
Ruijie(config-if-GigabitEthernet 0/1)#bpdu src-mac-check 00d0.f800.1234
```

【检验方法】 ● 通过 **show run interface** 命令查看端口的 Spanning Tree 配置。

```
Ruijie#show run int gi 0/1

Building configuration...
Current configuration : 170 bytes

interface GigabitEthernet 0/1
 switchport mode trunk
 bpdu src-mac-check 00d0.f800.1234
 spanning-tree link-type point-to-point
```

常见错误

- 配置 BPDU 源 MAC 检查，是只接收以配置的 MAC 为源 MAC 的 BPDU 帧，而丢弃其它所有 BPDU 帧。

5.3.11 配置边缘口的自动识别

配置效果

- 打开边缘口自动识别功能时，如果在一定的时间范围内(为 3 秒)，指派口没有收到 BPDU，则自动识别为边缘口。但因为收到 BPDU 而使 Port Fast Operational State 为 disabled。

注意事项

- 一般情况下不需要关闭边缘口自动识别功能。

配置方法

▾ 打开边缘口的自动识别

- 可选配置

- 缺省是打开的。

检验方法

- 显示验证。

相关命令

▾ 打开边缘口的自动识别

【命令格式】 **spanning-tree autoedge**

【参数说明】 -

【命令模式】 接口模式

【使用指导】 指派口在一定的时间内(为 3 秒), 如果收不到下游端口发送的 BPDU, 则认为该端口相连的是一台网络设备, 从而设置该端口为边缘端口, 直接进入 Forwarding 状态。自动标识为边缘口的端口因收到 BPDU 而自动识别为非边缘口。

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

配置举例

▾ 关闭端口的 Auto Edge 功能

【配置方法】 关闭端口的 Auto Edge 功能

```
Ruijie(config)#int gi 0/1
Ruijie(config-if-GigabitEthernet 0/1)#spanning-tree autoedge disabled
```

【检验方法】 ● 通过 **show spanning-tree interface** 命令查看端口的 Spanning Tree 配置。

```
Ruijie#show spanning-tree interface gi 0/1

PortAdminPortFast : Disabled
PortOperPortFast : Disabled
PortAdminAutoEdge : Disabled
PortOperAutoEdge : Disabled
PortAdminLinkType : point-to-point
PortOperLinkType : point-to-point
PortBPDUGuard : Disabled
PortBPDUFilter : Disabled
PortGuardmode : None

##### MST 0 vlans mapped :ALL
PortState : forwarding
PortPriority : 128
PortDesignatedRoot : 0.00d0.f822.3344
PortDesignatedCost : 0
PortDesignatedBridge :0.00d0.f822.3344
PortDesignatedPortPriority : 128
PortDesignatedPort : 2
PortForwardTransitions : 6
PortAdminPathCost : 20000
PortOperPathCost : 20000
Inconsistent states : normal
PortRole : designatedPort
```

常见错误

- 边缘端口的自动识别功能, 默认指派口 3 秒内未接收到 BPDU 就将端口识别成边缘端口并立即 Forward。如果网络环境存在丢包或收发报文延迟现象, 建议将端口的自动识别功能关闭。

5.3.12 配置接口保护相关的特性

配置效果

- 接口打开 Root Guard 功能时,强制其在所有实例上的端口角色为指定端口,一旦该端口收到优先级更高的配置信息时,Root Guard 功能会将该接口置为 root-inconsistent (blocked)状态,在足够长的时间内没有收到更优的配置信息时,端口会恢复成原来的正常状态。
- 由于单向链路的故障,根口或备份口由于收不到 BPDU 会变成指派口进入转发状态,从而导致了网络中环路的生产,LOOP Guard 功能防止了这种情况的发生。

注意事项

- 端口的 ROOT Guard 和 LOOP Guard 同一时刻只能有一个生效。

配置方法

▾ 打开 ROOT Guard 特性

- 可选配置。
- 为了防止因维护人员的错误配置或网络中的恶意攻击,根桥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,可以在设备的指派端口上配置 ROOT Guard 功能。

▾ 打开 LOOP Guard 特性

- 可选配置。
- 为了防止接收端口(根端口、Master 端口或 Alternate 端口)因接收不到指派网桥发送的 BPDU 而使网络拓扑发生变化,从而引起可能的环路,可以在上述接收端口上配置 LOOP Guard 功能,提高设备的稳定性。

▾ 关闭 Guard 特性

- 可选配置。
- 缺省是关闭的。

检验方法

- 显示验证。

相关命令

▾ 打开某个接口的 root guard 特性

- 【命令格式】 **spanning-tree guard root**
- 【参数说明】 -
- 【命令模式】 接口配置模式
- 【使用指导】 启用 root guard 功能,能防止因错误配置或非法报文的攻击导致当前根桥地位的变化。

▾ 打开所有接口的 loop guard 特性

- 【命令格式】 **spanning-tree loopguard default**
- 【参数说明】 -
- 【命令模式】 全局配置模式
- 【使用指导】 启用 loop guard 功能,能防止根端口或备份口因收不到 bpdu 而产生的可能的环路。

▾ 打开某个接口的 loop guard 特性

- 【命令格式】 **spanning-tree guard loop**
- 【参数说明】 -
- 【命令模式】 接口配置模式
- 【使用指导】 启用 loop guard 功能，能防止根端口或备份口因收不到 bpdu 而产生的可能的环路。

关闭某个接口的 guard 特性

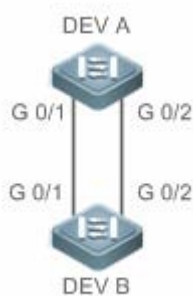
- 【命令格式】 **spanning-tree guard none**
- 【参数说明】 -
- 【命令模式】 接口配置模式
- 【使用指导】 缺省是关闭 guard 功能。

配置举例

配置端口的 Loop Guard 特性

【网络环境】

图 5-24



- 【配置方法】
- 配置 DEV A 为生成树根桥，DEV B 为非根桥。
 - 配置 DEV B 的端口 gi 0/1 和 gi 0/2 的 LOOP Guard 特性。

DEV A

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

DEV B

```
Ruijie(config)#spanning-tree
Ruijie(config)#int range gi 0/1-2
Ruijie(config-if-range)#spanning-tree guard loop
```

- 【检验方法】
- 通过 **show spanning-tree interface** 命令查看端口的 Spanning Tree 配置。

DEV A 略

DEV B

```
Ruijie#show spanning-tree int gi 0/1

PortAdminPortFast : Disabled
PortOperPortFast : Disabled
PortAdminAutoEdge : Enabled
PortOperAutoEdge : Disabled
PortAdminLinkType : auto
PortOperLinkType : point-to-point
PortBPDUGuard : Disabled
PortBPDUFilter : Disabled
PortGuardmode : Guard loop

##### MST 0 vlans mapped :ALL
PortState : forwarding
PortPriority : 128
```

```
PortDesignatedRoot : 0.001a.a917.78cc
PortDesignatedCost : 0
PortDesignatedBridge :0.001a.a917.78cc
PortDesignatedPortPriority : 128
PortDesignatedPort : 17
PortForwardTransitions : 1
PortAdminPathCost : 20000
PortOperPathCost : 20000
Inconsistent states : normal
PortRole : rootPort

Ruijie#show spanning-tree int gi 0/2

PortAdminPortFast : Disabled
PortOperPortFast : Disabled
PortAdminAutoEdge : Enabled
PortOperAutoEdge : Disabled
PortAdminLinkType : auto
PortOperLinkType : point-to-point
PortBPDUGuard : Disabled
PortBPDUFilter : Disabled
PortGuardmode : Guard loop

##### MST 0 vlans mapped :ALL
PortState : discarding
PortPriority : 128
PortDesignatedRoot : 0.001a.a917.78cc
PortDesignatedCost : 0
PortDesignatedBridge :0.001a.a917.78cc
PortDesignatedPortPriority : 128
PortDesignatedPort : 18
PortForwardTransitions : 1
PortAdminPathCost : 20000
PortOperPathCost : 20000
Inconsistent states : normal
PortRole : alternatePort
```

常见错误

- 将 ROOT Guard 功能配置在根端口、Master 端口或 Alternate 端口，可能会错误地将端口 BLOCK。

5.3.13 配置BPDU透传功能

配置效果

- 设备未开启 STP 协议时，需要透传 BPDU 帧，使得与之互连的设备之间的生成树计算正常。

注意事项

- BPDU 透传功能只在 STP 协议关闭时才起作用。当 STP 协议打开时，设备不透传 BPDU 帧。

配置方法

配置 BPDU 透传功能

- 可选配置
- 设备未开启 STP 协议时，如里需要透传 BPDU 帧，则需要配置 BPDU 透传功能。

检验方法

- 显示验证。

相关命令

配置 BPDU 透传功能

【命令格式】 **bridge-frame forwarding protocol bpdu**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 在 IEEE 802.1Q 标准中, BPDU 的目的 MAC 地址 01-80-C2-00-00-00 是作为保留地址使用的, 即遵循 IEEE 802.1Q 标准的设备, 对于接收到的 BPDU 帧是不转发的。然而, 在实际的网络布署中, 可能需要设备能够支持透传 BPDU 帧。例如, 设备未开启 STP 协议时, 需要透传 BPDU 帧, 使得与之互连的设备之间的生成树计算正常。

BPDU 透传功能只在 STP 协议关闭时才起作用。当 STP 协议打开时, 设备不透传 BPDU 帧。

配置举例

配置 BPDU 透传功能

【网络环境】

图 5-25



DEV A, C 上开启生成树协议, DEV B 未开启生成树协议。

【配置方法】

- DEV B 上配置 BPDU 透传功能, 使得 DEV A, C 之间的 STP 协议能够正确计算。

DEV B

```
Ruijie(config)#bridge-frame forwarding protocol bpdu
```

【检验方法】

- 通过 show run 查看 BPDU 透传功能是否开启。

DEV B

```
Ruijie#show run

Building configuration...
Current configuration : 694 bytes
bridge-frame forwarding protocol bpdu
```

常见错误

无

5.4 监视与维护

清除各类信息

! 在设备运行过程中执行 **clear** 命令, 可能因为重要信息丢失而导致业务中断。

作用	命令
清除端口的收发包统计信息	clear spanning-tree counters [interface <i>interface-id</i>]
清除 STP 的拓扑改变信息	clear spanning-tree mst <i>instance-id</i> topchange record

查看运行情况

作用	命令
----	----

显示 MSTP 的各项参数信息及生成树的拓扑信息	show spanning-tree
显示 MSTP 的收发包统计信息	show spanning-tree counters [interface <i>interface-id</i>]
显示 MSTP 的各 instance 的信息及其端口转发状态信息	show spanning-tree summary
显示因根保护或环路保护而 block 的端口	show spanning-tree inconsistent-ports
显示 MST 域的配置信息	show spanning-tree mst-configuration
显示该 instance 的 MSTP 信息	show spanning-tree mst <i>instance-id</i>
显示指定 interface 的对应 instance 的 MSTP 信息	show spanning-tree mst <i>instance-id</i> interface <i>interface-id</i>
显示指定实例中的接口的拓扑改变信息	show spanning-tree mst <i>instance-id</i> topochange record
显示指定 interface 的所有 instance 的 MSTP 信息	show spanning-tree interface <i>interface-id</i>
显示 forward-time	show spanning-tree forward-time
显示 Hello time	show spanning-tree hello-time
显示 max-hops	show spanning-tree max-hops
显示 tx-hold-count	show spanning-tree tx-hold-count
显示 pathcost method	show spanning-tree pathcost-method

查看调试信息



输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
打开生成树所有的调试开关	debug mstp all
打开生成树 GR 的调试开关	debug mstp gr
打开接收 BPDU 报文的调试开关	debug mstp rx
打开发送 BPDU 报文的调试开关	debug mstp tx
打开生成树事件调试开关	debug mstp event
打开生成树 Loop Guard 特性调试开关	debug mstp loopguard
打开生成树 Root Guard 特性调试开关	debug mstp rootguard
打开 Bridge Detect 状态机调试开关	debug mstp bridgedetect
打开 Port Information 状态机调试开关	debug mstp portinfo
打开 Port Protocol Migration 状态机调试开关	debug mstp protomigrat
打开生成树拓扑变化的调试开关	debug mstptopochange
打开生成树接收状态机调试开关	debug mstp receive
打开 Port Role Transitions 状态机调试开关	debug mstp roletran
打开 Port State Transition 状态机调试开关	debug mstp statetran
打开生成树发送状态机调试开关	debug mstp transmit

6 LLDP

6.1 概述

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

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

一台支持 LLDP 协议的锐捷交换机产品 , 当对端设备是支持 LLDP 协议的锐捷交换机产品 , 或支持 LLDP-MED 协议的终端设备的时候 , 该产品可以发现邻居信息。

- 支持 LLDP 协议的锐捷交换机产品。
- 支持 LLDP-MED 协议的终端设备。

协议规范

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

6.2 典型应用

典型应用	场景描述
利用LLDP查看拓扑连接情况	网络拓扑中有若干交换机设备、MED 设备、NMS 设备。
利用LLDP进行错误检测	网络拓扑中有直连的两台交换机设备 , 错误配置信息将显示。

6.2.1 利用LLDP查看拓扑连接情况

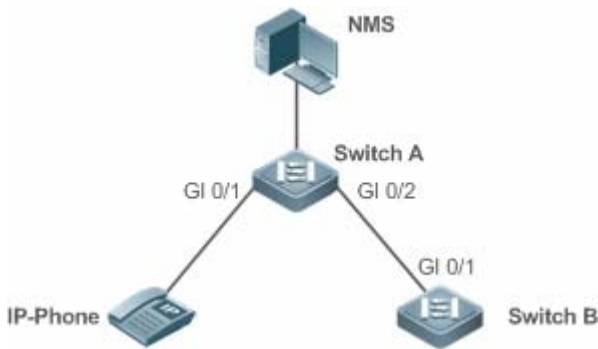
应用场景

网络拓扑中有若干交换机设备、MED 设备、NMS 设备。

以下图为例 , LLDP 功能默认打开 , 不需要再进行配置。

- Switch A 和 Switch B 可以互相发现对方是自己的邻居设备。
- Switch A 在端口 Gi 0/1 上可以发现邻居 MED 设备 IP-Phone。
- NMS (Network Management System , 网络管理系统) 能够访问 Switch A 的邻居设备信息。

图 6-1



- 【注释】 锐捷交换机产品 Switch A 和 Switch B、IP-Phone 都支持 LLDP 和 LLDP-MED。
交换机端口上 LLDP 的工作模式为 TxRx。
LLDP 报文的发送时间参数采用缺省值，即发送时间间隔为 30 秒、传输 LLDP 报文的延迟时间为 2 秒。

功能部属

- 在交换机中运行 LLDP 协议，实现邻居发现。
- 在交换机中运行 SNMP 协议，实现网络管理系统获取和设置交换机中的 LLDP 相关信息。

6.2.2 利用LLDP进行错误检测

应用场景

网络拓扑中有直连的两台交换机设备，错误配置信息将显示。

以下图为例，LLDP 功能默认打开，LLDP 错误检测功能缺省打开，不需要再进行配置。

- 管理员在对 Switch A 进行 VLAN 配置、端口速率双工配置、聚合端口配置和端口 MTU 配置时，如果配置的信息与相连接的邻居设备 Switch B 的配置不匹配，将提示相应的错误信息。反之亦然。

图 6-2



- 【注释】 两台锐捷交换机产品 Switch A 和 Switch B 都支持 LLDP 协议。
交换机端口上 LLDP 的工作模式为 TxRx。
LLDP 报文的发送时间参数采用缺省值，即发送时间间隔为 30 秒、传输 LLDP 报文的延迟时间为 2 秒。

功能部属

- 在交换机中运行 LLDP 协议，实现邻居发现，并检测两端的交换机直接接口的配置信息是否错误。

6.3 功能详解

基本概念

LLDPDU

LLDPDU 是指封装在 LLDP 报文中的协议数据单元，它由一系列的 TLV 封装而成。这些 TLV 集合包括了三个固定的 TLV 加上一系列可选的 TLVs 和一个 End Of TLV 组成。LLDPDU 的具体格式如图所示：

图 6-3 LLDPDU 格式

Chassis ID TLV	Port ID TLV	Time To Live TLV	Optional TLV	...	Optional TLV	End Of LLDPDU TLV
M	M	M				M

其中：

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

LLDP 报文封装格式

LLDP 报文支持两种封装格式：Ethernet II 和 SNAP（Subnetwork Access Protocols，子网访问协议）。

其中 Ethernet II 格式封装的 LLDP 报文如图所示：

图 6-4 Ethernet II 格式封装的 LLDP 报文

Destination Address	Source Address	Ethertype	LLDPDU	FCS
---------------------	----------------	-----------	--------	-----

其中：

- Destination Address：目的 MAC 地址，为 LLDP 的组播地址 01-80-C2-00-00-0E。
- Source Address：源 MAC 地址，为设备的端口 MAC 地址。
- Ethertype：以太网类型，为 0x88CC。
- LLDPDU：LLDP 协议数据单元。
- FCS：帧校验序列。

SNAP 格式封装的 LLDP 报文如图所示：

图 6-5 SNAP 格式封装的 LLDP 报文

Destination Address	Source Address	SNAP-encoded Ethertype	LLDPDU	FCS
---------------------	----------------	------------------------	--------	-----

其中：

- Destination Address：目的 MAC 地址，为 LLDP 的组播地址 01-80-C2-00-00-0E。
- Source Address：源 MAC 地址，为设备的端口 MAC 地址。
- SNAP-encoded Ethertype：SNAP 封装的以太网类型，为 AA-AA-03-00-00-00-88-CC。
- LLDPDU：LLDP 协议数据单元。
- FCS：帧校验序列。

TLV

LLDPDU 中封装的 TLV 可以分成二个大类：

- 基本管理 TLV
- 组织定义 TLV

基本管理 TLV 是一组用于网络管理的基础 TLV 集合。组织定义 TLV 是由标准组织和其它机构定义的 TLV，比如 IEEE 802.1 组织、IEEE 802.3 组织分别定义了各自的 TLV 集合。

1. 基本管理 TLV

基本管理 TLV 集合包含了两种类型的 TLV：固定 TLV 和可选 TLV。固定 TLV 是指该 TLV 信息必须包含在 LLDPDU 中发布，可选 TLV 是指根据需要确定 TLV 是否包含在 LLDPDU 中发布。

基本管理 TLV 的内容见表：

TLV 类型	TLV 说明	在 LLDPDU 中用法
End Of LLDPDU TLV	LLDPDU 的结束标志，占用 2 个字节	固定
Chassis ID TLV	用于标识设备，通常用 MAC 地址表示	固定
Port ID TLV	用于标识发送 LLDPDU 的端口	固定
Time To Live TLV	本地信息在邻居设备上的存活时间，当收到 TTL 为 0 的 TLV 时，此时需要删除掉对应的邻居信息。	固定
Port Description TLV	发送 LLDPDU 的端口描述符	可选
System Name TLV	描述设备的名称	可选
System Description TLV	设备描述信息，包括硬件/软件版本、操作系统等信息	可选
System Capabilities TLV	描述设备的主要功能，例如桥接、路由、中继等功能	可选
Management Address TLV	管理地址，同时包含了接口号和 OID (Object Identifier，对象标识)。	可选

✔ 锐捷交换机系列产品 LLDP 协议支持基本管理 TLV 的发布。

2. 组织定义 TLV

不同的组织（例如 IEEE 802.1、IEEE 802.3、IETF 或者设备供应商）定义特定的 TLV 信息去通告设备的特定信息。TLV 格式中通过 OUI（Organizationally Unique Identifier，组织唯一标识符）字段来区分不同的组织。

- 组织定义 TLV 属于可选的 TLV 集合，根据用户的实际需要在 LLDPDU 中发布。目前比较常见的组织定义 TLV 有以下三种：IEEE 802.1 组织定义的 TLV

IEEE 802.1 组织定义的 TLV 见表：

TLV 类型	TLV 说明
Port VLAN ID TLV	端口的 VLAN 标识符
Port And Protocol VLAN ID TLV	端口的协议 VLAN 标识符
VLAN Name TLV	端口的 VLAN 名称
Protocol Identity TLV	端口支持的协议类型

✔ 锐捷交换机系列产品 LLDP 协议，不支持发送 Protocol Identity TLV，但支持接收该类型的 TLV。

- IEEE 802.3 组织定义的 TLV

IEEE 802.3 组织定义的 TLV 见表：

TLV 类型	TLV 说明
MAC/PHY Configuration//Status TLV	端口的速率双工状态、是否支持并使能自动协商功能
Power Via MDI TLV	端口的供电能力
Link Aggregation TLV	端口的链路聚合能力及当前的聚合状态
Maximum Frame Size TLV	端口所能传输的最大的帧的大小

✔ 锐捷交换机系列产品 LLDP 协议支持 IEEE 802.3 组织定义的 TLV 的发布。

- LLDP-MED TLV

LLDP-MED 以 IEEE 802.1AB LLDP 协议为基础，它扩展了 LLDP，使用户能够更方便地部署 VoIP（Voice Over IP，基于 IP 的语音传输）网络及进行故障检测。它提供了网络配置策略、设备发现、以太网供电管理和目录管理等应用，满足了节约成本、有效地管理和易于部署方面的需求，简化了语音设备地部署。

LLDP-MED 定义的 TLV 见表：

TLV 类型	TLV 说明
LLDP-MED Capabilities TLV	设备是否支持 LLDP-MED、LLDPDU 中封装的 LLDP-MED TLV 类型以及当前设备的类型（网络连接设备或终端）
Network Policy TLV	通告端口的 VLAN 的配置、支持的应用类型（如语音或视频）、二层的优先级信息等
Location Identification TLV	定位标识终端设备。在网络拓扑收集等应用中能够精确地定位出终端设备
Extended Power-via-MDI TLV	提供了更高级的供电管理
Inventory – Hardware Revision TLV	MED 设备的硬件版本
Inventory – Firmware Revision TLV	MED 设备的固件版本
Inventory – Software Revision TLV	MED 设备的软件版本
Inventory – Serial Number TLV	MED 设备的序列号
Inventory – Manufacturer Name TLV	MED 设备的制造商的名称
Inventory – Model Name TLV	MED 设备的模块名称
Inventory – Asset ID TLV	MED 设备的资产标识符，用于目录管理和资产跟踪

✔ 锐捷交换机系列产品 LLDP 协议支持 LLDP-MED 定义的 TLV 的发布。

功能特性

功能特性	作用
LLDP工作模式	配置 LLDP 报文收发的模式。
LLDP报文的传输机制	直连支持 LLDP 协议的交换机设备可发送 LLDP 报文给对方。
LLDP报文的接收机制	直连支持 LLDP 协议的交换机设备可接收对方发送的 LLDP 报文。

6.3.1 LLDP工作模式

配置 LLDP 工作模式，能够使交换机收发 LLDP 报文的方式发生变化。

工作原理

LLDP 提供了三种工作模式：

- TxRx：既发送也接收 LLDPDU。
- Rx Only：只接收不发送 LLDPDU。
- Tx Only：只发送不接收 LLDPDU。

当端口的 LLDP 工作模式发生变化时，端口将对协议状态机进行初始化操作，通过配置端口初始化的延迟时间，可以避免由于工作模式频繁改变而导致端口不断地进行初始化操作。

相关配置

配置 LLDP 工作模式

缺省情况下，接口上的工作模式为 TxRx。

使用 `lldp mode` 命令可以改变接口上的工作模式。

必须在接口上配置工作模式为 TxRx 才能使 LLDP 协议报文收发功能正常。若接口工作模式配置为 Rx Only，那么设备只能接收 LLDP 报文，但无法发送 LLDP 报文；若接口工作模式配置为 Tx Only，那么设备只能发送 LLDP 报文，但无法接收 LLDP 报文；若接口工作模式关闭，将不再收发 LLDP 报文。

6.3.2 LLDP报文的传输机制

LLDP 报文的传输能让对端设备发现其邻居设备的存在，当取消 LLDP 传输模式或端口被管理 Shutdown 的时候，能够通告给对端设备其邻居信息不再有效。

工作原理

LLDP 工作在 TxRx 或 Tx Only 模式时，会周期性的发送 LLDP 报文。当本地设备的信息发生变化时，会立即发送 LLDP 报文。为了避免本地信息的频繁变化引起的频繁发送 LLDP 报文，在发送完一个 LLDP 报文后需要延迟一定的时间后再发往下一个 LLDP 报文。该延迟时间可以手工配置。

LLDP 提供了两种报文类型：

- 标准 LLDP 报文：包含了本地设备的管理和配置信息。
- Shutdown 通告报文：当取消了 LLDP 的传输模式或者端口被管理 Shutdown 时，将触发 LLDP Shutdown 通告报文的发送。Shutdown 通告报文由 Chassis ID TLV、Port ID TLV、Time To Live TLV 和 End OF LLDP TLV 组成。其中 Time To Live TLV 中 TTL 等于 0。当设备收到 LLDP Shutdown 通告报文时，将认为邻居信息已经不再有效并立即删除邻居信息。

当 LLDP 工作模式由关闭或 Rx 转变为 TxRx 或 Tx 或者发现新邻居时(即收到新的 LLDP 报文且本地尚未保存该邻居信息)，为了让邻居设备尽快学习到本设备的信息，将启动快速发送机制。快速发送机制调整 LLDP 报文的发送周期为 1 秒，并连续发送一定数量的 LLDP 报文。

相关配置

配置 LLDP 工作模式

缺省情况下，接口上的工作模式为 TxRx。

使用 `lldp mode txrx` 和 `lldp mode tx` 命令可以使 LLDP 报文传输功能打开，使用 `lldp mode rx` 和 `no lldp mode` 命令可以使 LLDP 报文传输功能关闭。

必须在接口上配置工作模式为 TxRx 或 Tx Only 才能使 LLDP 的报文传输功能正常。若接口工作模式配置为 Rx Only，那么设备只能接收 LLDP 报文，但无法发送 LLDP 报文。

配置 LLDP 报文的发送延迟时间

缺省情况下，LLDP 报文的发送延迟时间为 2 秒。

使用 `lldp timer tx-delay` 命令可以修改 LLDP 报文的发送延迟时间。

延迟时间配置过小，本地信息的频繁变化引起的频繁发送 LLDP 报文；配置值太大，本地信息的变化可能不能使发送 LLDP 报文。

配置 LLDP 报文的发送时间间隔

缺省情况下，LLDP 报文的发送时间间隔为 30 秒。

使用 `lldp timer tx-interval` 命令可以修改 LLDP 报文的发送时间间隔。

配置值太小，则会使 LLDP 发送频率过高；配置值太大，则可能会使对端设备不能及时发现本地设备。

配置允许发布的 TLV 类型

缺省情况下，接口上允许发布除 Location Identification TLV 之外的所有类型的 TLV。

使用 `lldp tlv-enable` 命令可以改变允许发布的 TLV 类型。

增加或减少发送的 LLDP 报文中 LLDPDU 的对应 TLV 字段。

配置 LLDP 快速发送报文的个数

缺省情况下，LLDP 快速发送报文的个数为 3 个。

使用 `lldp fast-count` 命令可以改变 LLDP 快速发送报文的个数。

改变快速发送机制下快速发送报文的个数。

6.3.3 LLDP报文的接收机制

LLDP 报文的接收能够发现邻居设备的存在以及何时应该老化邻居信息。

工作原理

LLDP 工作在 TxRx 或 RxOnly 模式时，能够接收 LLDP 报文。当设备收到 LLDP 报文时，会进行有效性检查。通过报文校验后，判断是新的邻居信息还是已经存在的邻居信息更新，并将邻居信息保存在本地设备。同时根据报文中 TTL TLV 的值设置邻居信息在本地设备的存活时间。如果收到 TTL TLV 的值为 0，表示需要立即老化掉该邻居信息。

相关配置

配置 LLDP 工作模式

缺省情况下，接口上的工作模式为 TxRx。


使用 `lldp mode txrx` 和 `lldp mode rx` 命令可以使 LLDP 报文接收功能打开，使用 `lldp mode tx` 和 `no lldp mode` 命令可以使 LLDP 报文接收功能关闭。

必须在接口上配置工作模式为 TxRx 或 Rx Only 才能使 LLDP 的报文接收功能正常。若接口工作模式配置为 Tx Only 或关闭，那么设备只能发送 LLDP 报文，但无法接收 LLDP 报文。

6.4 配置详解

配置项	配置建议 & 相关命令	
配置LLDP功能	⚠️ 可选配置。用于打开或关闭全局和接口的 LLDP 功能。	
	<code>lldp enable</code>	打开 LLDP 功能
	<code>no lldp enable</code>	关闭 LLDP 功能
配置LLDP工作模式	⚠️ 可选配置。用于配置 LLDP 报文收发模式。	
	<code>lldp mode {rx tx txrx }</code>	配置 LLDP 工作模式
	<code>no lldp mode</code>	关闭 LLDP 工作模式
配置允许发布的TLV类型	⚠️ 可选配置。用于配置允许发布的 TLV 类型。	
	<code>lldp tlv-enable</code>	配置允许发布的 TLV 类型
	<code>no lldp tlv-enable</code>	取消发布指定的 TLV 类型
配置LLDP报文中发布管理地址	⚠️ 可选配置。用于配置 LLDP 报文中发布。	
	<code>lldp management-address-tlv [ip-address]</code>	配置 LLDP 报文中发布管理地址
	<code>no lldp management-address-tlv</code>	取消管理地址的发布
配置快速发送LLDP报文的个数	⚠️ 可选配置。用于配置快速发送 LLDP 报文的个数。	
	<code>lldp fast-count value</code>	配置快速发送 LLDP 报文的个数
	<code>no lldp fast-count</code>	恢复缺省快速发送 LLDP 报文个数

配置TTL乘数和LLDP报文发送时间间隔	⚠️ 可选配置。用于配置 TTL 乘数和 LLDP 报文发送时间间隔。	
	<code>lldp hold-multiplier value</code>	配置 TTL 乘数
	<code>no lldp hold-multiplier</code>	恢复缺省 TTL 乘数
	<code>lldp timer tx-interval seconds</code>	配置 LLDP 报文发送时间间隔
	<code>no lldp timer tx-interval</code>	恢复缺省 LLDP 报文发送时间间隔
配置LLDP报文的发送延迟时间	⚠️ 可选配置。用于配置 LLDP 报文的发送延迟时间。	
	<code>lldp timer tx-delay seconds</code>	配置 LLDP 报文的发送延迟时间
	<code>no lldp timer tx-delay</code>	恢复缺省 LLDP 报文的发送延迟时间
配置端口初始化的延迟时间	⚠️ 可选配置。用于配置端口初始化的延迟时间。	
	<code>lldp timer reinit-delay seconds</code>	配置端口初始化的延迟时间
	<code>no lldp timer reinit-delay</code>	恢复缺省端口初始化的延迟时间
配置LLDP Trap功能	⚠️ 可选配置。用于配置 LLDP Trap 功能。	
	<code>lldp notification remote-change enable</code>	打开 LLDP Trap 功能
	<code>no lldp notification remote-change enable</code>	关闭 LLDP Trap 功能
	<code>lldp timer notification-interval</code>	配置发送 LLDP Trap 信息的时间间隔
	<code>no lldp timer notification-interval</code>	恢复缺省发送 LLDP Trap 信息的时间间隔
配置LLDP错误检测功能	⚠️ 可选配置。用于配置 LLDP 错误检测功能。	
	<code>lldp error-detect</code>	打开 LLDP 错误检测功能
	<code>no lldp error-detect</code>	关闭 LLDP 错误检测功能
配置LLDP报文封装格式	⚠️ 可选配置。用于配置 LLDP 报文封装格式。	
	<code>lldp encapsulation snap</code>	配置 LLDP 报文的封装格式为 SNAP
	<code>no lldp encapsulation snap</code>	配置 LLDP 报文的封装格式为 Ethernet II
配置LLDP Network Policy策略	⚠️ 可选配置。用于配置 LLDP Network Policy 策略。	
	<code>lldp network-policy profile profile-num</code>	配置 LLDP Network Profile 策略
	<code>no lldp network-policy profile profile-num</code>	删除 LLDP Network Profile 策略
配置设备的普通地址信息	⚠️ 可选配置。用于配置设备的普通地址信息。	
	{ country state county city division neighborhood street-group leading-street-dir trailing-street-suffix street-suffix number street-number-suffix landmark additional-location-information name postal-code building unit floor room type-of-place postal-community-name post-office-box additional-code } ca-word	配置设备的普通地址信息

	<pre>no { country state county city division neighborhood street-group leading-street-dir trailing-street-suffix street-suffix number street-number-suffix landmark additional-location-information name postal-code building unit floor room type-of-place postal-community-name post-office-box additional-code } ca-word</pre>	删除设备的普通地址信息
配置设备的紧急电话号码信息	 可选配置。用于配置设备的紧急电话号码信息。	
	<pre>lldp location elin identifier id elin-location tel-number</pre>	配置设备的紧急电话号码信息
	<pre>no lldp location elin identifier id</pre>	删除设备的紧急电话号码信息

6.4.1 配置LLDP功能

配置效果

- 打开或关闭 LLDP 的功能。

注意事项

- 如果要求接口上 LLDP 功能生效，则要同时开启全局和该接口上的 LLDP 功能。

配置方法

- 可选配置。
- 可对全局或接口下配置 LLDP 功能。

检验方法

显示 LLDP 的状态信息。

- 检查全局 LLDP 功能是否开启。
- 检查接口下 LLDP 功能是否开启。

相关命令

打开 LLDP 功能

- 【命令格式】 **lldp enable**
- 【参数说明】 -
- 【命令模式】 全局模式、接口模式
- 【使用指导】 需要全局打开 LLDP 开关，接口的 LLDP 功能才生效。

关闭 LLDP 功能

- 【命令格式】 **no lldp enable**
- 【参数说明】 -
- 【命令模式】 全局模式、接口模式
- 【使用指导】 -

配置举例

关闭 LLDP 功能

【配置方法】 关闭全局 LLDP 功能。

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

【检验方法】 显示 LLDP 全局状态信息。

```
Ruijie(config)#show lldp status
```

```
Global status of LLDP: Disable
```

常见错误

- 接口已开启 LLDP 功能，但是全局没有开启 LLDP 功能，此时接口下的 LLDP 功能还是不能生效。
- 端口学习到的邻居个数限制在 5 个，即端口最多只能学习到 5 个邻居。
- 如果邻居设备不支持 LLDP，但是邻居设备下连的设备支持 LLDP，由于邻居设备可能会转发 LLDP 的报文，这样，端口可能会学习到非直连的设备的信息。

6.4.2 配置 LLDP 工作模式

配置效果

- 配置接口的 LLDP 的工作模式为 TxRx，则该接口可发送和接收报文。
- 配置接口的 LLDP 的工作模式为 Tx，则该接口只能发送报文，不能接收报文。
- 配置接口的 LLDP 的工作模式为 Rx，则该接口只能接收报文，不能发送报文。
- 关闭接口的 LLDP 工作模式，则该接口不能接收和发送报文。

注意事项

- LLDP 运行在实际的物理接口上（对于 AP 口，则实际是运行在 AP 成员口上）。堆叠口，VSL 口不支持 LLDP。

配置方法

- 可选配置。
- 用户可根据实际需要在工作模式修改为 Tx 或 Rx 模式。

检验方法

显示接口下 LLDP 的状态信息。

- 检查接口下 LLDP 的工作模式是否和配置的一致。

相关命令

配置 LLDP 工作模式

【命令格式】 `lldp mode { rx | tx | txrx }`

【参数说明】 rx：表示只接收不发送 LLDPDU

tx：表示只发送不接收 LLDPDU

txrx：表示即发送又接收 LLDPDU

【命令模式】 接口模式

【使用指导】 接口 LLDP 功能生效的前提是全局使能了 LLDP 且接口 LLDP 的工作模式处于 tx、rx 或 txrx。

关闭 LLDP 工作模式

- 【命令格式】 **no lldp mode**
- 【参数说明】 -
- 【命令模式】 接口模式
- 【使用指导】 关闭接口的 LLDP 工作模式，此时接口不再发送和接收 LLDP 报文。

配置举例

配置 LLDP 工作模式

- 【配置方法】 接口下配置 LLDP 的工作模式为 Tx 模式。

```
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#lldp mode tx
```

- 【检验方法】 显示 LLDP 在接口下的状态信息。

```
Ruijie(config-if-GigabitEthernet 0/1)#show lldp status interface gigabitethernet 0/1
Port [GigabitEthernet 0/1]
Port status of LLDP          : Enable
Port state                   : UP
Port encapsulation           : Ethernet II
Operational mode             : TxOnly
Notification enable          : NO
Error detect enable          : YES
Number of neighbors          : 0
Number of MED neighbors      : 0
```

常见配置错误

-

6.4.3 配置允许发布的TLV类型

配置效果

- 用户可以通过配置运行发布的 TLV 类型，使发送 LLDP 报文中 LLDPDU 的内容改变。

注意事项

- 配置基本管理 TLV、IEEE 802.1 组织定义 TLV、IEEE 802.3 组织定义 TLV 时，如果指定 **all** 参数，将发布该类型的所有可选 TLV。
- 配置 LLDP-MED TLV 时，如果指定 **all** 参数，将发布除 Location Identification TLV 之外的所有类型的 LLDP-MED TLV。
- 配置允许发布 LLDP-MED Capability TLV 时，需要先配置允许发布 LLDP 802.3 MAC/PHY TLV，取消发布 LLDP 802.3 MAC/PHY TLV 时，需要先取消发布 LLDP-MED Capability TLV
- 配置 LLDP-MED TLV 时，必须配置允许发布 LLDP-MED Capability TLV，才可以配置允许发布 LLDP-MED 其它类型的 TLV。取消发布 LLDP-MED TLV，必须先取消发布 LLDP-MED 其它类型的 TLV，才允许取消发布 LLDP-MED Capability TLV。当设备下联 IP 电话，若 IP 电话支持 LLDP-MED，则可以通过配置 network policy TLV 下发策略给 IP 电话
- 如果设备缺省支持 DCBX 功能，缺省情况下端口上不允许发布 IEEE 802.3 TLV 及 LLDP-MED TLV

配置方法

- 可选配置。
- 用户可根据实际需要在某接口下配置允许发布的 TLV 类型。

检验方法

显示端口上可发布的 TLV 配置信息。

- 检查接口下允许发布的 TLV 是否和配置的一致。

相关命令

配置 LLDP 允许发布的 TLV

【命令格式】 `lldp tlv-enable { basic-tlv { all | port-description | system-capability | system-description | system-name } | dot1-tlv { all | port-vlan-id | protocol-vlan-id [vlan-id] | vlan-name [vlan-id] } | dot3-tlv { all | link-aggregation | mac-physic | max-frame-size | power } | med-tlv { all | capability | inventory | location { civic-location | elin } identifier id | network-policy profile [profile-num] | power-over-ethernet }`

【参数说明】 **basic-tlv**：基本管理 TLV

port-description：表示 Port Description TLV

system-capability：表示 System Capabilities TLV

system-description：表示 System Description TLV

system-name：表示 System Name TLV

dot1-tlv：802.1 组织定义的 TLV

port-vlan-id：表示 Port VLAN ID TLV

protocol-vlan-id：表示 Port And Protocol VLAN ID TLV

vlan-id：表示端口协议 VLAN ID，配置范围为：1-4094

vlan-name：表示 VLAN Name TLV

vlan-id：表示指定 VLAN 名称对应的 VLAN ID，配置范围为：1-4094

dot3-tlv：802.3 组织定义的 TLV

link-aggregation：表示 Link Aggregation TLV

mac-physic：表示 MAC/PHY Configuration/Status TLV

max-frame-size：表示 Maximum Frame Size TLV

power：表示 Power Via MDI TLV

med-tlv：LLDP MED TLV

capability：表示 LLDP-MED Capabilities TLV

inventory：表示目录管理 TLV，包括硬件版本、固件版本、软件版本、序列号、制造产商名称、模块名称和资产标识符等

location：表示 Location Identification TLV

civic-location：表示封装网络连接设备的普通地址信息

elin：表示封装紧急电话号码信息

id：表示配置的策略 ID，配置范围为：1-1024

network-policy：表示 Network Policy TLV

profile-num：Network Policy 策略 ID，配置范围为：1-1024

power-over-ethernet：表示 Extended Power-via-MDI TLV

【命令模式】 接口模式

【使用指导】



取消发布指定的 TLV 类型

【命令格式】 `no lldp tlv-enable {basic-tlv { all | port-description | system-capability | system-description | system-name } | dot1-tlv { all | port-vlan-id | protocol-vlan-id | vlan-name } | dot3-tlv { all | link-aggregation | mac-physic | max-frame-size | power } | med-tlv { all | capability | inventory | location { civic-location | elin } identifier id | network-policy profile [profile-num] | power-over-ethernet }`

- 【参数说明】
- basic-tlv** : 基本管理 TLV
 - port-description** : 表示 Port Description TLV
 - system-capability** : 表示 System Capabilities TLV
 - system-description** : 表示 System Description TLV
 - system-name** : 表示 System Name TLV
 - dot1-tlv** : 802.1 组织定义的 TLV
 - port-vlan-id** : 表示 Port VLAN ID TLV
 - protocol-vlan-id** : 表示 Port And Protocol VLAN ID TLV
 - vlan-name** : 表示 VLAN Name TLV
 - dot3-tlv** : 802.3 组织定义的 TLV
 - link-aggregation** : 表示 Link Aggregation TLV
 - mac-physic** : 表示 MAC/PHY Configuration/Status TLV
 - max-frame-size** : 表示 Maximum Frame Size TLV
 - power** : 表示 Power Via MDI TLV
 - med-tlv** : LLDP MED TLV
 - capability** : 表示 LLDP-MED Capabilities TLV
 - inventory** : 表示目录管理 TLV , 包括硬件版本、固件版本、软件版本、序列号、制造产商名称、模块名称和资产标识符等
 - location** : 表示 Location Identification TLV
 - civic-location** : 表示封装网络连接设备的普通地址信息
 - elin** : 表示封装紧急电话号码信息
 - id** : 表示配置的策略 ID , 配置范围为 : 1-1024
 - network-policy** : 表示 Network Policy TLV
 - profile-num** : Network Policy 策略 ID , 配置范围为 : 1-1024
 - power-over-ethernet** : 表示 Extended Power-via-MDI TLV
- 【命令模式】 接口模式
- 【使用指导】 

配置举例

配置 LLDP 允许发布的 TLV

【配置方法】 配置取消发布 IEEE 802.1 组织定义的 Port And Protocol VLAN ID TLV

```
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#no lldp tlv-enable dot1-tlv protocol-vlan-id
```

【检验方法】 显示 LLDP 在接口下的 TLV 配置信息。

```
Ruijie(config-if-GigabitEthernet 0/1)#show lldp tlv-config interface gigabitethernet 0/1
LLDP tlv-config of port [GigabitEthernet 0/1]
```

NAME	STATUS	DEFAULT
Basic optional TLV:		
Port Description TLV	YES	YES
System Name TLV	YES	YES
System Description TLV	YES	YES
System Capabilities TLV	YES	YES
Management Address TLV	YES	YES
IEEE 802.1 extend TLV:		
Port VLAN ID TLV	YES	YES

Port And Protocol VLAN ID TLV	NO	YES
VLAN Name TLV	YES	YES
IEEE 802.3 extend TLV:		
MAC-Physic TLV	YES	YES
Power via MDI TLV	YES	YES
Link Aggregation TLV	YES	YES
Maximum Frame Size TLV	YES	YES
LLDP-MED extend TLV:		
Capabilities TLV	YES	YES
Network Policy TLV	YES	YES
Location Identification TLV	NO	NO
Extended Power via MDI TLV	YES	YES
Inventory TLV	YES	YES

常见配置错误

-

6.4.4 配置LLDP报文中发布管理地址

配置效果

- 配置接口下 LLDP 报文中的发布管理地址，可使管理地址 TLV 发生改变。
- 取消管理地址发布将使 LLDP 报文中的管理地址按缺省情况下选取。

注意事项

- LLDP 运行在实际的物理接口上（对于 AP 口，则实际是运行在 AP 成员口上）。堆叠口，VSL 口不支持 LLDP。

配置方法

- 可选配置。
- 在接口下配置 LLDP 报文发布的管理地址。

检验方法

显示本地设备接口下的 LLDP 信息。

- 检查本地设备接口下的 LLDP 信息是否和配置的相同。

相关命令

配置 LLDP 报文中发布的管理地址

【命令格式】 **lldp management-address-tlv** [*ip-address*]

【参数说明】 *ip-address* : LLDP 报文中发布的管理地址

【命令模式】 接口模式

【使用指导】 缺省情况下，LLDP 报文发布管理地址。发布的管理地址为端口允许通过的最小 VLAN 的 IPv4 地址，如果该 VLAN 未配置 IPv4 地址，则继续查找下一个允许通过的最小 VLAN，直到找到 IPv4 地址为止。

取消管理地址的发布

【命令格式】 **no lldp management-address-tlv**

【参数说明】 -

【命令模式】 接口模式

【使用指导】 缺省情况下，LLDP 报文发布管理地址。发布的管理地址为端口允许通过的最小 VLAN 的 IPv4 地址，如果该 VLAN 未配置 IPv4 地址，则继续查找下一个允许通过的最小 VLAN，直到找到 IPv4 地址为止。

配置举例

配置 LLDP 报文中发布的管理地址

【配置方法】 在接口下配置 LLDP 报文发布的管理地址为 192.168.1.1

```
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#lldp management-address-tlv 192.168.1.1
```

【检验方法】 查看对应接口下相应的配置信息

```
Ruijie(config-if-GigabitEthernet 0/1)#show lldp local-information interface GigabitEthernet 0/1
Lldp local-information of port [GigabitEthernet 0/1]
  Port ID type           : Interface name
  Port id                : GigabitEthernet 0/1
  Port description       : GigabitEthernet 0/1

  Management address subtype : ipv4
  Management address       : 192.168.1.1
  Interface numbering subtype : ifIndex
  Interface number        : 1
  Object identifier       :

  802.1 organizationally information
  Port VLAN ID           : 1
  Port and protocol VLAN ID (PPVID) : 1
  PPVID Supported        : YES
  PPVID Enabled          : NO
  VLAN name of VLAN 1   : VLAN0001
  Protocol Identity      :

  802.3 organizationally information
  Auto-negotiation supported : YES
  Auto-negotiation enabled  : YES
  PMD auto-negotiation advertised : 1000BASE-T full duplex mode, 100BASE-TX full duplex mode,
100BASE-TX half duplex mode, 10BASE-T full duplex mode, 10BASE-T half duplex mode
  Operational MAU type      : speed(100)/duplex(Full)
  PoE support               : NO
  Link aggregation supported : YES
  Link aggregation enabled  : NO
  Aggregation port ID      : 0
  Maximum frame Size       : 1500

  LLDP-MED organizationally information
  Power-via-MDI device type : PD
  Power-via-MDI power source : Local
  Power-via-MDI power priority :
  Power-via-MDI power value  :
  Model name                 : Model name
```

常见配置错误

-

6.4.5 配置快速发送LLDP报文的个数

配置效果

- 改变快速发送机制下 LLDP 报文发送的个数。

注意事项

- -

配置方法

- 可选配置。
- 在全局配置模式下配置快速发送 LLDP 报文个数。

检验方法

显示全局 LLDP 的状态信息。

- 检查 LLDP 快速发送个数是否和配置的相同。

相关命令

配置快速发送 LLDP 报文的个数

- 【命令格式】 **lldp fast-count value**
- 【参数说明】 value : LLDP 快速发送报文的个数，缺省为 3 个，可配置的范围为 1-10
- 【命令模式】 全局模式
- 【使用指导】 -

恢复缺省快速发送 LLDP 报文个数

- 【命令格式】 **no lldp fast-count**
- 【参数说明】 -
- 【命令模式】 全局模式
- 【使用指导】 -

配置举例

配置快速发送 LLDP 报文的个数

- 【配置方法】 全局配置模式下配置快速发送 LLDP 报文的个数为 5 个

```
Ruijie(config)#lldp fast-count 5
```

- 【检验方法】 显示全局 LLDP 的状态信息。

```
Ruijie(config)#show lldp status
Global status of LLDP           : Enable
Neighbor information last changed time :
Transmit interval                : 30s
Hold multiplier                  : 4
Reinit delay                     : 2s
Transmit delay                   : 2s
Notification interval           : 5s
Fast start counts                : 5
```

常见配置错误

-

6.4.6 配置TTL乘数和LLDP报文发送时间间隔

配置效果

- 改变 TTL 乘数的值。
- 改变 LLDP 报文发送时间间隔。

注意事项

-

配置方法

- 可选配置。
- 全局配置模式下进行配置。

检验方法

显示接口下 LLDP 的状态信息。

- 检查接口下 LLDP 的工作模式是否和配置的相同。

相关命令

配置 TTL 乘数

【命令格式】 **lldp hold-multiplier value**

【参数说明】 value : TTL 乘数, 缺省为 4, 配置范围为 2-10

【命令模式】 全局模式

【使用指导】 LLDP 报文中 Time To Live TLV 的值=TTL 乘数×报文发送时间间隔+1。因此, 通过调整 TTL 乘数可以控制本设备信息在邻居设备的存活时间。

恢复缺省 TTL 乘数

【命令格式】 **no lldp hold-multiplier**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 LLDP 报文中 Time To Live TLV 的值=TTL 乘数×报文发送时间间隔+1。因此, 通过调整 TTL 乘数可以控制本设备信息在邻居设备的存活时间。

配置 LLDP 报文发送时间间隔

【命令格式】 **lldp timer tx-interval seconds**

【参数说明】 seconds : LLDP 报文的发送时间间隔, 可配置范围为 5-32768

【命令模式】 全局模式

【使用指导】 -

恢复缺省 LLDP 报文发送时间间隔

【命令格式】 **no lldp timer tx-interval**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 -

配置举例

配置 LLDP 工作模式

【配置方法】 配置 TTL 乘数为 3，LLDP 报文的发送间隔为 20 秒，此时，本地设备信息在邻居设备的存活时间为 61 秒

```
Ruijie(config)#lldp hold-multiplier 3
Ruijie(config)#lldp timer tx-interval 20
```

【检验方法】 显示全局 LLDP 状态信息。

```
Ruijie(config)#lldp hold-multiplier 3
Ruijie(config)#lldp timer tx-interval 20
Ruijie(config)#show lldp status
Global status of LLDP           : Enable
Neighbor information last changed time :
Transmit interval                : 20s
Hold multiplier                  : 3
Reinit delay                     : 2s
Transmit delay                   : 2s
Notification interval           : 5s
Fast start counts                : 3
```

常见配置错误

-

6.4.7 配置 LLDP 报文的发送延迟时间

配置效果

- 改变 LLDP 报文的发送延迟时间。

注意事项

-

配置方法

- 可选配置。
- 用户可根据实际需要在全局配置模式下进行配置。

检验方法

显示全局 LLDP 的状态信息。

- 检查 LLDP 报文的发送延迟时间是否和配置的不同。

相关命令

配置 LLDP 报文的发送延迟时间

【命令格式】 **lldp timer tx-delay seconds**

【参数说明】 seconds：LLDP 报文的发送延迟时间，可配置范围为 1-8192

【命令模式】 全局模式

【使用指导】 当本地信息发生变化时，会立即向邻居设备发送 LLDP 报文。为了避免本地信息频繁变化引起的频繁地发送 LLDP 报文，可以配置 LLDP 报文的发送延迟时间来限制 LLDP 报文的频繁发送。

恢复缺省的 LLDP 报文的发送延迟时间

【命令格式】 **no lldp timer tx-delay**

【参数说明】 -

- 【命令模式】 全局模式
- 【使用指导】 当本地信息发生变化时，会立即向邻居设备发送 LLDP 报文。为了避免本地信息频繁变化引起的频繁地发送 LLDP 报文，可以配置 LLDP 报文的发送延迟时间来限制 LLDP 报文的频繁发送。

配置举例

配置 LLDP 报文的发送延迟时间

- 【配置方法】 配置发送 LLDP 报文的延迟时间为 3 秒

```
Ruijie(config)#lldp timer tx-delay 3
```

- 【检验方法】 查看全局 LLDP 状态信息

```
Ruijie(config)#show lldp status
Global status of LLDP           : Enable
Neighbor information last changed time :
Transmit interval               : 30s
Hold multiplier                 : 4
Reinit delay                   : 2s
Transmit delay                  : 3s
Notification interval          : 5s
Fast start counts               : 3
```

常见配置错误

-

6.4.8 配置端口初始化的延迟时间

配置效果

- 改变端口初始化的延迟时间。

注意事项

● -

配置方法

- 可选配置。
- 用户可根据实际需要对接口状态机初始化的延迟时间进行配置。

检验方法

显示全局 LLDP 的状态信息。

- 检查全局 LLDP 的端口初始化的延迟时间是否和配置的不同。

相关命令

配置端口初始化的延迟时间

- 【命令格式】 **lldp timer reinit-delay** *seconds*

- 【参数说明】 *seconds*：端口初始化的延迟时间，配置范围为 1-10 秒

- 【命令模式】 全局模式

- 【使用指导】 为了避免端口的工作模式的频繁变化引起的频繁地初始化状态机，可以配置端口初始化的延迟时间。

恢复缺省端口初始化的延迟时间

- 【命令格式】 **no lldp timer reinit-delay**
- 【参数说明】 -
- 【命令模式】 全局模式
- 【使用指导】 为了避免端口的工作模式的频繁变化引起的频繁地初始化状态机，可以配置端口初始化的延迟时间。

配置举例

配置端口初始化的延迟时间

- 【配置方法】 配置端口初始化的延迟时间为 3 秒，并显示 LLDP 的状态信息。

```
Ruijie(config)#lldp timer reinit-delay 3
```

- 【检验方法】 显示全局 LLDP 的状态信息。

```
Ruijie(config)#show lldp status
Global status of LLDP           : Enable
Neighbor information last changed time :
Transmit interval               : 30s
Hold multiplier                 : 4
Reinit delay                    : 3s
Transmit delay                  : 2s
Notification interval          : 5s
Fast start counts               : 3
```

常见配置错误

-

6.4.9 配置LLDP Trap功能

配置效果

- 改变发送 LLDP Trap 信息的时间间隔。

注意事项

-

配置方法

打开 LLDP Trap 功能

- 可选配置。
- 接口配置模式下进行配置。

配置发送 LLDP Trap 信息的时间间隔

- 可选配置。
- 全局配置模式下进行配置。

检验方法

显示 LLDP 的状态信息。

- 检查 LLDP Trap 功能是否打开。
- 检查发送 LLDP Trap 信息的时间间隔和配置的不同。

相关命令

打开 LLDP Trap 功能

- 【命令格式】 **lldp notification remote-change enable**
- 【参数说明】 -
- 【命令模式】 接口模式
- 【使用指导】 通过配置 Trap 功能，可以将本地设备的 LLDP 信息（例如发现新邻居、检测到与邻居的通信链路故障等信息）发送给网管服务器，管理员可以根据此信息监控网络的运行状况。

关闭 LLDP Trap 功能

- 【命令格式】 **no lldp notification remote-change enable**
- 【参数说明】 -
- 【命令模式】 接口模式
- 【使用指导】 通过配置 Trap 功能，可以将本地设备的 LLDP 信息（例如发现新邻居、检测到与邻居的通信链路故障等信息）发送给网管服务器，管理员可以根据此信息监控网络的运行状况。

配置发送 LLDP Trap 信息的时间间隔

- 【命令格式】 **lldp timer notification-interval seconds**
- 【参数说明】 *seconds*：配置发送 LLDP Trap 信息的时间间隔，缺省的时间间隔是 5 秒，可配置的范围是 5-3600
- 【命令模式】 全局模式
- 【使用指导】 为了防止 LLDP Trap 信息的频繁发送，可以配置发送 LLDP Trap 的时间间隔。在这段时间间隔内，检测到 LLDP 信息变化，将发送 Trap 给网管服务器。

恢复缺省的发送 LLDP Trap 信息的时间间隔

- 【命令格式】 **no lldp timer notification-interval**
- 【参数说明】 -
- 【命令模式】 全局模式
- 【使用指导】 为了防止 LLDP Trap 信息的频繁发送，可以配置发送 LLDP Trap 的时间间隔。在这段时间间隔内，检测到 LLDP 信息变化，将发送 Trap 给网管服务器。

配置举例

打开 LLDP Trap 功能及配置发送 LLDP Trap 信息的时间间隔

- 【配置方法】 使能 LLDP Trap 功能，并配置 LLDP Trap 信息的发送时间间隔为 10 秒。

```
Ruijie(config)#lldp timer notification-interval 10
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#lldp notification remote-change enable
```

- 【检验方法】 显示 LLDP 的状态信息。

```
Ruijie(config-if-GigabitEthernet 0/1)#show lldp status
Global status of LLDP           : Enable
Neighbor information last changed time :
Transmit interval               : 30s
Hold multiplier                  : 4
Reinit delay                    : 2s
Transmit delay                   : 2s
Notification interval           : 10s
Fast start counts                : 3

-----
Port [GigabitEthernet 0/1]
-----
Port status of LLDP             : Enable
```

Port state	: UP
Port encapsulation	: Ethernet II
Operational mode	: RxAndTx
Notification enable	: YES
Error detect enable	: YES
Number of neighbors	: 0
Number of MED neighbors	: 0

常见配置错误

-

6.4.10 配置LLDP错误检测功能

配置效果

- LLDP 错误检测功能打开，当 LLDP 检测到错误时，将打印 LOG 信息提示管理员。
- 配置 LLDP 错误检测功能，错误检测包括链路两端的 VLAN 配置检测、端口状态检测、端口聚合配置检测、MTU 配置检测及环路检测

注意事项

-

配置方法

- 可选配置。
- 用户可根据实际需要在接口模式下进行配置，打开或关闭 LLDP 错误检测功能。

检验方法

显示接口下 LLDP 的状态信息。

- 检查接口下 LLDP 错误检测功能是打开还是关闭，与实际配置是否一致。

相关命令

▾ 打开 LLDP 错误检测功能

【命令格式】 **lldp error-detect**

【参数说明】 -

【命令模式】 接口模式

【使用指导】 LLDP 错误检测功能是依靠链路两端的设备交互 LLDP 报文中的特定的 TLV 信息进行的，为了保证检测功能的正确运行，需要设备发布正确的 TLV 信息。

▾ 关闭 LLDP 错误检测功能

【命令格式】 **no lldp error-detect**

【参数说明】 -

【命令模式】 接口模式

【使用指导】 LLDP 错误检测功能是依靠链路两端的设备交互 LLDP 报文中的特定的 TLV 信息进行的，为了保证检测功能的正确运行，需要设备发布正确的 TLV 信息。

配置举例

▾ 打开 LLDP 错误检测功能

【配置方法】 打开 LLDP 在接口 GI 0/1 下的错误检测功能。

```
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#lldp error-detect
```

【检验方法】 显示 LLDP 在接口下的状态信息。

```
Ruijie(config-if-GigabitEthernet 0/1)#show lldp status interface gigabitethernet 0/1
Port [GigabitEthernet 0/1]
Port status of LLDP          : Enable
Port state                   : UP
Port encapsulation          : Ethernet II
Operational mode             : RxAndTx
Notification enable         : NO
Error detect enable         : YES
Number of neighbors         : 0
Number of MED neighbors     : 0
```

常见配置错误

-

6.4.11 配置LLDP报文封装格式

配置效果

- 改变 LLDP 报文的封装格式。

注意事项

-

配置方法

- 可选配置。
- 用户可根据实际需要在接口下改变 LLDP 报文的封装格式。

检验方法

显示接口下 LLDP 的状态信息。

- 检查接口下 LLDP 报文封装格式是否和配置的不同。


相关命令

▾ 配置 LLDP 报文的封装格式为 SNAP

【命令格式】 **lldp encapsulation snap**

【参数说明】 -

【命令模式】 接口模式


【使用指导】  为了保证本地设备和邻居设备的正常通信，需要将 LLDP 报文配置成相同的封装格式。

▾ 恢复缺省的 LLDP 报文的封装格式，即为 Ethernet II

【命令格式】 **no lldp encapsulation snap**

【参数说明】 -

【命令模式】 接口模式

【使用指导】  为了保证本地设备和邻居设备的正常通信，需要将 LLDP 报文配置成相同的封装格式。

配置举例

配置 LLDP 报文的封装格式为 SNAP

【配置方法】 配置 LLDP 报文的封装格式为 SNAP。

```
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#lldp encapsulation snap
```

【检验方法】 显示 LLDP 在接口下的状态信息。

```
Ruijie(config-if-GigabitEthernet 0/1)#show lldp status interface gigabitethernet 0/1
Port [GigabitEthernet 0/1]
Port status of LLDP          : Enable
Port state                   : UP
Port encapsulation          : Snap
Operational mode             : RxAndTx
Notification enable         : NO
Error detect enable         : YES
Number of neighbors         : 0
Number of MED neighbors     : 0
```

常见配置错误

-

6.4.12 配置LLDP Network Policy策略

配置效果

- 改变 LLDP Network Policy 策略。
- 当设备下联 IP 电话，若 IP 电话支持 LLDP-MED，则可以通过配置 Network Policy TLV 下发策略给 IP 电话，由 IP 电话修改语音流 Tag 和 QOS。在设备上，除配置上述策外，还需要配置步骤为：1.使能 Voice VLAN 功能，把连接 IP 电话的端口静态加入 Voice VLAN；2.把连接 IP 电话的端口配置为 QOS 信任口（推荐使用信任 DSCP 模式）；3.如果在此端口上同时开启了 1X 认证，则还需要配置一条安全通道，允许 Voice VLAN 内的报文通过。若 IP 电话不支持 LLDP-MED，则必须使能 Voice VLAN 功能，并将话机 MAC 地址手动配置到 Voice VLAN OUI 列表中。
- QOS 信任模式的配置方法请参见《IP QOS》章节；Voice VLAN 的配置方法请参见《Voice VLAN》章节；安全通道的配置方法请参见《ACL》章节。

注意事项

-

配置方法

- 可选配置。
- 用户可根据实际需要配置 LLDP Network Policy 策略。

检验方法

显示本地设备的 LLDP network-policy 配置策略信息。

- 检查 LLDP Network Policy 策略是否和配置的相同。

相关命令

配置 LLDP Network Profile 策略

【命令格式】 **lldp network-policy profile** *profile-num*

【参数说明】 *profile-num* : LLDP network-policy 策略的标识, 范围为: 1-1024

【命令模式】 全局模式

【使用指导】 使用此命令进入 LLDP network-policy 配置模式, 使用此命令时需要指定策略 ID。

进入 LLDP network-policy 配置模式后, 可使用{ voice | voice-signaling } vlan 命令配置具体的 network-policy 策略。

删除 LLDP Network Profile 策略

【命令格式】 **no lldp network-policy profile** *profile-num*

【参数说明】 *profile-num* : LLDP network-policy 策略的标识, 范围为: 1-1024

【命令模式】 接口模式

【使用指导】 使用此命令进入 LLDP network-policy 配置模式, 使用此命令时需要指定策略 ID。

进入 LLDP network-policy 配置模式后, 可使用{ voice | voice-signaling } vlan 命令配置具体的 network-policy 策略。

配置举例

配置 LLDP Network Profile 策略

【配置方法】 配置接口 1 发布的 LLDP 报文中 Network Policy TLV 策略为 1 : voice 应用类型 vlan id 是 3 , cos 是 4 , dscp 是 6。

```
Ruijie#config
Ruijie(config)#lldp network-policy profile 1
Ruijie(config-lldp-network-policy)# voice vlan 3 cos 4
Ruijie(config-lldp-network-policy)# voice vlan 3 dscp 6
Ruijie(config-lldp-network-policy)#exit
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# lldp tlv-enable med-tlv network-policy profile 1
```

【检验方法】 显示本地设备的 LLDP network-policy 配置策略信息。

```
network-policy information:
-----
network policy profile :1
voice vlan 3 cos 4
voice vlan 3 dscp 6
```

常见配置错误

-

6.4.13 配置设备的普通地址信息

配置效果

- 设备的地址信息发生变化。

注意事项

-

配置方法

- 可选配置。
- 用户可根据实际需要配置设备的普通地址信息。

检验方法

显示本地设备的 LLDP 普通地址信息。

- 检查 LLDP 普通地址信息是否和配置的相同。

相关命令

▾ 配置设备的普通地址信息

【命令格式】 配置 LLDP 普通地址信息。用户可以使用 no 选项删除地址信息。
{ **country** | **state** | **county** | **city** | **division** | **neighborhood** | **street-group** | **leading-street-dir** | **trailing-street-suffix** | **street-suffix** | **number** | **street-number-suffix** | **landmark** | **additional-location-information** | **name** | **postal-code** | **building** | **unit** | **floor** | **room** | **type-of-place** | **postal-community-name** | **post-office-box** | **additional-code** } *ca-word*

【参数说明】 **country** : 国家代码, 2 个字符。china : CH
state : 地址信息 CA 类型为 1
county : CA 类型为 2
city : CA 类型为 3
division : CA 类型为 4
neighborhood : CA 类型为 5
street-group : CA 类型为 6
leading-street-dir : CA 类型为 16
trailing-street-suffix : CA 类型为 17
street-suffix : CA 类型为 18
number : CA 类型为 19
street-number-suffix : CA 类型为 20
landmark : CA 类型为 21
additional-location-information : CA 类型为 22
name : CA 类型为 23
postal-code : CA 类型为 24
building : CA 类型为 25
unit : CA 类型为 26
floor : CA 类型为 27
room : CA 类型为 28
type-of-place : CA 类型为 29
postal-community-name : CA 类型为 30
post-office-box : CA 类型为 31
additional-code : CA 类型为 32
ca-word : 地址信息

【命令模式】 LLDP Civic Address 配置模式

【使用指导】 进入 LLDP Civic Address 配置模式后, 配置 LLDP 普通地址信息。

▾ 删除设备的普通地址信息

【命令格式】 no { **country** | **state** | **county** | **city** | **division** | **neighborhood** | **street-group** | **leading-street-dir** | **trailing-street-suffix** | **street-suffix** | **number** | **street-number-suffix** | **landmark** | **additional-location-information** | **name** | **postal-code** | **building** | **unit** | **floor** | **room** | **type-of-place** | **postal-community-name** | **post-office-box** | **additional-code** }

【参数说明】 -

【命令模式】 LLDP Civic Address 配置模式

【使用指导】 进入 LLDP Civic Address 配置模式后，配置 LLDP 普通地址信息。

配置设备类型信息

【命令格式】 **device-type** *device-type*

【参数说明】 *device-type*：设备类型，缺省为 1，取值范围为 0-2

0 表示设备类型为 DHCP Server

1 表示设备类型为 Switch

2 表示设备类型为 LLDP MED 终端

【命令模式】 LLDP Civic Address 配置模式

【使用指导】 进入 LLDP Civic Address 配置模式后，配置 LLDP 普通地址中设备类型信息。

恢复设备类型信息

【命令格式】 **no device-type**

【参数说明】 -

【命令模式】 LLDP Civic Address 配置模式

【使用指导】 进入 LLDP Civic Address 配置模式后，恢复 LLDP 普通地址中设备类型信息为缺省值。

配置举例

配置设备的普通地址信息

【配置方法】 配置设备接口 1 的地址为：交换机设备，地址是国家：CH，城市：Fuzhou，邮编：350000。

```
Ruijie#config
Ruijie(config)#lldp location civic-location identifier 1
Ruijie(config-lldp-civic)# country CH
Ruijie(config-lldp-civic)# city Fuzhou
Ruijie(config-lldp-civic)# postal-code 350000
```

【检验方法】 显示设备接口 1 的 LLDP 普通地址信息。

```
civic location information:
-----
Identifier          :1
country             :CH
device type         :1
city                :Fuzhou
postal-code         :350000
```

常见配置错误

-

6.4.14 配置设备的紧急电话号码信息

配置效果

- 更改设备的紧急电话号码信息。

注意事项

-

配置方法

- 可选配置。

- 用户可根据实际需要配置设备的紧急电话号码信息。

检验方法

显示本地设备的紧急电话号码信息。

- 检查本地设备的紧急电话号码信息是否和配置的相同。

相关命令

配置设备的紧急电话号码信息

- 【命令格式】 **lldp location elin identifier id elin-location tel-number**
- 【参数说明】 *id* : 表示紧急电话号码信息的配置标识号, 范围为: 1-1024
tel-number : 表示紧急电话号码, 范围: 10 – 25 字节
- 【命令模式】 全局模式
- 【使用指导】 使用此命令来配置紧急电话号码信息。

删除设备的紧急电话号码信息

- 【命令格式】 **no lldp location elin identifier id**
- 【参数说明】 *id* : 表示紧急电话号码信息的配置标识号, 范围为: 1-1024
- 【命令模式】 全局模式
- 【使用指导】 -

配置举例

配置设备的紧急电话号码信息

- 【配置方法】 配置设备接口 1 的紧急电话号码为: 085285555556。

```
Ruijie#config
Ruijie(config)#lldp location elin identifier 1 elin-location 085283671111
```

- 【检验方法】 显示设备接口 1 的紧急电话号码信息。


```
elin location information:
-----
Identifier           :1
elin number          :085283671111
```

常见配置错误

-

6.5 监视与维护

清除各类信息

-  在设备运行过程中执行 **clear** 命令, 可能因为重要信息丢失而导致业务中断。

作用	命令
清除 LLDP 的统计信息。	clear lldp statistics [interface interface-name]
清除 LLDP 的邻居信息。	clear lldp table [interface interface-name]

查看运行情况

作用	命令
----	----

显示本地设备的 LLDP 信息，这些信息将被组织成 TLV 发送给邻居设备。	show lldp local-information [global interface <i>interface-name</i>]
显示本地设备的 LLDP 普通地址信息或者紧急电话号码信息。	show lldp location { civic-location elin-location } { identifier <i>id</i> interface <i>interface-name</i> static }
显示邻居设备的 LLDP 信息。	show lldp neighbors [interface <i>interface-name</i>] [detail]
显示本地设备的 LLDP network-policy 配置策略信息	show lldp network-policy { profile [<i>profile-num</i>] interface <i>interface-name</i> }
显示 LLDP 的统计信息。	show lldp statistics [global interface <i>interface-name</i>]
显示 LLDP 的状态信息。	show lldp status [interface <i>interface-name</i>]
显示端口上可发布的 TLV 配置信息。	show lldp tlv-config [interface <i>interface-name</i>]

查看调试信息

 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
打开 LLDP 错误处理的调试开关。	debug lldp error
打开 LLDP 事件处理的调试开关。	debug lldp event
打开 LLDP 热备份处理的调试开关。	debug lldp ha
打开 LLDP 报文接收的调试开关。	debug lldp packet
打开 LLDP 状态机相关的调试开关。	debug lldp stm



配置指南-IP 地址及应用

本分册介绍 IP 地址及应用配置指南相关内容，包括以下章节：

1. IP 地址与服务
2. ARP
3. DHCP
4. DNS
5. 网络通信检测工具
6. TCP
7. 软件 IPv4 快转

1 IP 地址与服务

1.1 概述

因特网协议（Internet Protocol，IP）使用逻辑虚拟的地址将数据包从源方发送到目的方，即 IP 地址。在网络层，路由设备使用 IP 地址完成数据包转发。

i 以下仅针对 IPv4 地址进行介绍。

协议规范

- RFC 1918 : Address Allocation for Private Internets
- RFC 1166 : Internet Numbers

1.2 典型应用

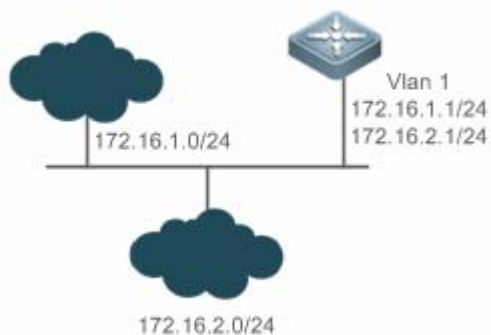
典型应用	场景描述
配置IP地址通信	两个网络使用同一个交换机接口进行通信

1.2.1 配置IP地址通信

应用场景

交换机连接一个局域网，局域网分为两个网段：172.16.1.0/24 和 172.16.2.0/24。要求两个网段的计算机都可以通过交换机和因特网通信，并且两个网段的计算机之间可以互相通信。

图 1-1 IP 地址配置范例



功能部属

- 在 vlan1 口上配置两个 ip 地址，一个主 ip 地址，一个从 ip 地址。
- 在 172.16.1.0/24 网段中的主机上配置网关为 172.16.1.1，在 172.16.2.0/24 网段中的主机上配置网关为 172.16.2.1。

1.3 功能详解

基本概念

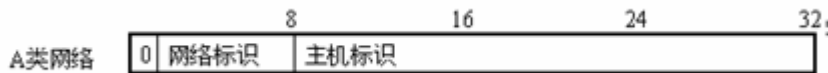
IP 地址

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

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

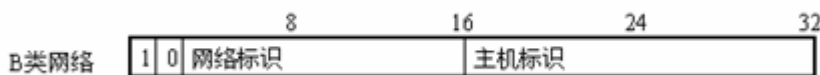
A 类地址，最高比特位为“0”，有 7 个比特位表示网络号，24 个比特位表示本地地址。这样总共有 128 个 A 类网络。

图 1-2



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

图 1-3



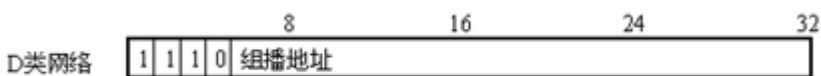
C 类地址，前三个最高比特位为“110”，有 21 个比特位表示网络号，8 个比特位表示本地地址。这样总共有 2,097,152 个 C 类网络。

图 1-4



D 类地址，前四个最高比特位为“1110”，其余比特位为组播地址。

图 1-5



i 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	0.0.0.0~0.255.255.255	保留
	1.0.0.0~126.255.255.255	可用
	127.0.0.0~127.255.255.255	保留
B 类网络	128.0.0.0~191.254.255.255	可用
	191.255.0.0~191.255.255.255	保留
C 类网络	192.0.0.0~192.0.0.255	保留
	192.0.1.0~223.255.254.255	可用
	223.255.255.0~223.255.255.255	保留
D 类网络	224.0.0.0~239.255.255.255	组播地址
E 类网络	240.0.0.0~255.255.255.254	保留
	255.255.255.255	广播地址

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

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

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

子网掩码

网络掩码也是一个 32 比特的数值，标识着该 IP 地址的哪几个比特为网络部分。网络掩码中，值为“1”的比特对应的 IP 地址比特位就是网络部分，值为“0”的比特对应的 IP 地址比特位就是主机地址部分。如 A 类网络对应的网络掩码为“255.0.0.0”。您可以利用网络掩码对一个网络进行子网划分，子网划分就是将主机地址部分的一些比特位也作为网络部分，缩小主机容量，增加网络的数量，这时的网络掩码就称为子网掩码。

广播报文

广播报文是指目标地址为某个物理网络上所有主机的数据包。锐捷产品支持两种类型广播报文：1) 定向广播，是指数据包接收者为一个指定网络的所有主机，目标地址的主机部分全为“1”；2) 淹没广播，是指数据包接收者为所有网络的主机，目标地址 32 比特位全为“1”。

ICMP 报文

ICMP 是 (Internet Control Message Protocol) Internet 控制报文协议。它是 TCP/IP 协议族的一个子协议，用于在 IP 主机、网络设备之间传递控制消息，主要用于网络出现异常的时候通知相应设备。

📌 TTL

TTL (Time-To-Live) , 生存时间。指定数据包被路由器丢弃之前允许通过的网段数量。它是IP协议报文中的一个值, 它告诉网络, 数据包在网络中的时间是否太长而应被丢弃。

功能特性

功能特性	作用
IP地址	用于配置接口 IP 地址, 该接口才允许运行 IP 协议。
广播报文处理	设置 IP 广播地址, 转发处理定向广播报文。
发送ICMP报文	控制 ICMP 协议报文的收发。
控制ICMP差错报文的发送速率	防止拒绝服务攻击。
IP TTL	用于配置单播报文和广播报文的 TTL。
IP源路由	用于对接收报文的源路由进行检查。

1.3.1 IP地址

接口获取 IP 地址有以下方式：

- (1) 手工配置 IP 地址。
- (2) 利用 DHCP 协议获取 IP 地址。
- (3) 通过 PPP 协商获得 IP 地址。
- (4) 借用其它接口的 IP 地址。

这几种方式是互斥的, 配置新的获取 IP 地址方式时会覆盖通过原有方式获取的 IP 地址。

i 利用 DHCP 协议获取 IP 地址请参见“DHCP”章节, 以下仅介绍其他三种获取 IP 地址的方式。

📌 配置接口 IP 地址

一个设备只有配置了 IP 地址, 才可以接收和发送 IP 数据包, 接口配置了 IP 地址, 说明该接口允许运行 IP 协议。

📌 接口配置多个 IP 地址

锐捷产品可以支持一个接口配置多个 IP 地址, 其中一个为主 IP 地址, 其余全部为次 IP 地址。次 IP 地址的配置理论上没有数目限制, 但是次 IP 地址与主 IP 以及次 IP 地址之间必须属于不同网络。在网络建设中, 会经常使用到次 IP 地址, 通常在以下情况下应该考虑使用次 IP 地址：

- 一个网络没有足够多的主机地址。例如, 现在一般局域网需要一个 C 类网络, 可分配 254 台主机。但是当局域网主机超过 254 台时, 一个 C 类网络将不够分配, 有必要分配另一个 C 类网络地址。这样设备就需要连接两个网络, 所以就配置多个 IP 地址。

- 许多旧的网络是基于第二层的桥接网络，没有进行子网的划分。次 IP 地址的使用可以使该网络很容易升级到基于 IP 层的路由网络。对于每个子网，设备都配置一个 IP 地址。
- 一个网络的两个子网被另外一个网络隔离开，可以创建一个被隔离网络的子网，通过配置次 IP 地址的方式，将隔离的子网连接起来。一个子网不能在设备的两个或两个以上接口出现。

i 配置次 IP 地址之前，需要确定已经配置了主 IP 地址。如果网络上的一台设备配置了次 IP 地址，则其它设备也必须配置同一网络的次 IP 地址。当然如果其它设备原先没有分配 IP 地址，可以配置为主地址。

配置通过 PPP 协商获取 IP 地址

i 本命令只在点对点接口上支持。

通过此配置，点对点接口可以通过 PPP 协商接受对端为自己分配的 IP 地址。

配置接口借用 IP 地址

所谓“借用 IP 地址”，是指一个接口上没有配置 IP 地址，但为了使该接口能正常使用，就向同一设备上其它有 IP 地址的接口借用一个 IP 地址。

i 以太网接口、隧道接口和环回接口的 IP 地址可以被其它接口借用，但它们不能借用其它接口的 IP 地址。

i 被借用接口的 IP 地址不能是借用其它接口的 IP 地址。

i 如果被借用接口有多个 IP 地址，只有主 IP 地址被借用。

i 一个接口的 IP 地址可以借给多个接口。

i 借用接口的 IP 地址始终和被借用接口的 IP 地址保持一致，随着被借用接口的 IP 地址变化而变化。

相关配置

配置接口一个或多个 IP 地址

- 缺省情况接口没有配置 IP 地址。
- 通过 **ip address** 命令配置接口 IP 地址。
- 配置后根据冲突检测即可使用该 IP 地址进行通信。
- 通过 **ip address ip-address mask secondary** 可以配置多个次 IP 地址。

1.3.2 广播报文处理

工作原理

广播分两种，全广播，即 IP 地址为 255.255.255.255，由于会被路由器禁止传输，所以也叫本地网络广播。另一种是所有的主机位都为 1 的广播，例如：192.168.1.255/24，这种广播，通过配置是可以被转发的。

如果 IP 网络设备转发淹没广播（一般指目标 IP 地址为全“1”的广播报文），可能会引起网络的超负载，严重影响网络的运行，这种情况称为广播风暴。设备提供了一些办法能够将广播风暴限制在本地网络，阻止其继续扩张。但对于桥和交换机等基于二层网络设备，将转发和传播广播风暴。

解决广播风暴最好的办法就是给每个网络指定一个广播地址，这就是定向广播，这要求使用广播报文的 IP 协议尽可能应用定向广播而不是淹没广播进行数据传播。

关于广播问题的详细描述，请参见 RFC 919 和 RFC 922。

IP 定向广播报文是指目标地址为某个 IP 子网广播地址的 IP 报文，如目标地址为 172.16.16.255 的报文就称为定向广播报文。但是产生该报文的节点又不是目标子网的成员。

没有与目标子网直连的设备接收到 IP 定向广播报文，跟转发单播报文一样处理定向广播报文。当定向广播报文到达直连该子网的设备后，设备将把定向广播报文转换为淹没广播报文（一般指目标 IP 地址为全“1”的广播报文），然后以链路层广播方式发送给目标子网上的所有主机。

相关配置

配置 IP 广播地址

- 缺省情况下接口 IP 广播地址为 255.255.255.255。
- 如果需要定义其它地址的广播报文，可以在接口下配置 `ip broadcast-address` 命令。

允许转发定向广播

- 缺省情况接口不允许转发定向广播。
- 用户可以在指定的接口上，通过 `ip directed-broadcast` 命令配置接口允许转发定向广播，这样该接口就可以转发到直连网络的定向广播了。该命令只影响定向广播报文在目标子网的传输，而不影响其它定向广播报文的正常转发。
- 在接口上，用户还可以通过定义访问控制列表来控制转发某些定向广播。当定义了访问列表时，只有符合访问列表中定义的定向广播才会被转发。

1.3.3 控制ICMP差错报文的发送速率

工作原理

为了防止拒绝服务攻击，对 ICMP 差错报文的发送速率进行限制，采用令牌桶算法。

如果 IP 报文需要分片，但是 IP 首部的不可分片位被设置了，设备会向源 IP 地址发送编号为 4 的 ICMP 目的不可达报文，这种 ICMP 差错报文的主要用途是路径 MTU 发现。为了防止其它 ICMP 差错报文太多导致发不出编号为 4 的 ICMP 目的不可达报文，从而导致路径 MTU 发现功能失效，对编号为 4 的 ICMP 目的不可达报文和其它 ICMP 差错报文分别限速。

相关配置

配置 IP 首部不可分片位触发的 ICMP 目的不可达报文的发送速率

- 缺省速率是 100 毫秒 10 个。
- 可通过 `ip icmp error-interval DF` 配置发送速率。

▾ 配置其它 ICMP 差错报文的发送速率

- 缺省速率是 100 毫秒 10 个。
- 可通过 `ip icmp error-interval` 配置发送速率。

1.3.4 IP TTL

工作原理

IP 数据包从源地址向目的地址经过路由器间传播，设置一个 TTL 数值，每过一个路由器 TTL 值就减一，当减到零的时候，路由器就把这个包丢掉，这样可以防止无用的包在网络上无限传播下去，浪费网络带宽。

相关配置

▾ 设置 IP TTL

- 缺省情况接口 IP TTL 为 64。
- 可通过 `ip ttl` 设置接口的 IP TTL 值。

1.3.5 IP源路由

工作原理

锐捷产品支持 IP 源路由。当设备接收到 IP 数据包时，会对 IP 报头的严格源路由、宽松源路由和记录路由等选项进行检查，这些选项在 RFC 791 中有详细描述。如果检测到该数据包启用了其中一个选项，就会执行响应的动作；如果检测到无效的选项，就会给数据源发送一个 ICMP 参数问题消息，然后丢弃该数据包。

开启 IP 源路由，在 IP 数据报选项中增加源路由选项，可用于测试某特定网络的吞吐率，也可以是数据报绕开出错的网络。然而，可能会导致诸如源地址欺骗(Source Address Spoofing)、IP 欺骗(IP Spoofing)等的网络攻击。

相关配置

▾ 配置 IP 源路由

- 缺省情况开启 IP 源路由功能。
- 可通过 `ip source-route` 开启或关闭该功能。

1.4 配置详解

配置项	配置建议 & 相关命令	
配置接口IP地址	⚠ 必须配置。用于配置 ip 地址，允许接口运行 IP 协议。	
	ip address	手工配置接口 IP 地址
配置广播报文处理方式	⚠ 可选配置。用于设置 IP 广播地址，允许转发定向广播报文。	
	ip broadcast-address	配置 IP 广播地址
	ip directed-broadcast	允许转发定向广播
配置ICMP差错报文的发送速率	⚠ 可选配置。	
	ip icmp error-interval DF	配置 IP 首部不可分片位触发的 ICMP 目的不可达报文的发送速率
	ip icmp error-interval	配置其它 ICMP 差错报文和 ICMP 重定向报文的发送速率
设置IP TTL	⚠ 可选配置。用于配置单播报文和广播报文的 TTL。	
	ip ttl	设置 TTL 值
配置IP源路由	⚠ 可选配置。用于配置对接收报文的源路由进行检查。	
	ip source-route	启用 IP 源路由

1.4.1 配置接口IP地址

配置效果

通过配置接口 IP 地址实现 IP 网络通信。

注意事项

-

配置方法

✚ 手工配置接口 IP 地址

- 必须配置。
- 在三层接口模式下配置。

检验方法

通过 **show ip interface** 可以看到配置的地址生效

相关命令

手工配置接口 IP 地址

【命令格式】 **ip address** *ip-address network-mask* [**secondary**]

【参数说明】 *ip-addr0065ss* : 32 个比特位 IP 地址，8 位一组，以十进制方式表示，组之间用点隔开。

network-mask : 32 个比特位网络掩码，“1”表示掩码位，“0”表示主机位。每 8 位一组，以十进制方式表示，组之间用点隔开。

secondary : 表示配置的次 IP 地址。

【命令模式】 接口模式

【使用指导】 -

配置举例

给接口配置 IP 地址

【配置方法】 在接口 GigabitEthernet 0/0 配置 ip 地址 192.168.23.110 255.255.255.0

```
Ruijie#configure terminal
Ruijie(config)#interface gigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)# no switchport
Ruijie(config-if-GigabitEthernet 0/0)#ip address 192.168.23.110 255.255.255.0
```

【检验方法】 使用 **show ip interface** 可以看到接口 GigabitEthernet 0/0 添加地址成功

```
Ruijie# show ip interface gigabitEthernet 0/0
GigabitEthernet 0/0
  IP interface state is: UP
  IP interface type is: BROADCAST
  IP interface MTU is: 1500
  IP address is:
    192.168.23.110/24 (primary)
```

1.4.2 配置广播报文处理方式

配置效果

配置接口广播地址为 0.0.0.0，并允许转发定向广播报文。

注意事项

-

配置方法

配置 IP 广播地址

- 可选配置，有些老的主机可能只认 0.0.0.0 的广播地址，此时需要配置接口的广播地址为 0.0.0.0。
- 在三层接口模式下配置。

允许转发定向广播

- 可选配置，向处在一个广播域的全部主机发送广播，但是发送者并不处在这个广播域内，此时需要配置允许转发定向广播。
- 在三层接口模式下配置。

检验方法

通过 `show running-config interface` 可以看到配置生效

相关命令

配置 IP 广播地址

【命令格式】 `ip broadcast-address ip-address`

【参数说明】 `ip-address`：IP 网络的广播地址。

【命令模式】 接口模式

【使用指导】 目前 IP 广播报文的目标地址一般为全“1”，表示为 255.255.255.255。RGOS 软件可以通过定义产生其它 IP 地址的广播报文，而且可以同时接收全“1”以及自己定义的广播包。

允许转发定向广播

【命令格式】 `ip directed-broadcast [access-list-number]`

【参数说明】 `access-list-number`：访问列表号，范围从 1-199，1300 - 2699。如果定义了访问列表号，只有匹配该访问列表的 IP 定向广播报文才转换。

【命令模式】 接口模式

【使用指导】 如果在接口上配置了 `no ip directed-broadcast`，RGOS 将丢弃接收到的直连网络的定向广播报文。

配置举例

【配置方法】 在设备端口 gigabitEthernet 0/1 配置 IP 广播报文的目标地址为 0.0.0.0，启用定向广播的转发。

```
Ruijie#configure terminal
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# no switchport
Ruijie(config-if-GigabitEthernet 0/1)# ip broadcast-address 0.0.0.0
Ruijie(config-if-GigabitEthernet 0/1)# ip directed-broadcast
```

【检验方法】 使用 **show ip interface** 可以看到接口 GigabitEthernet 0/1 配置成功

```
Ruijie#show running-config interface gigabitEthernet 0/1
ip directed-broadcast
ip broadcast-address 0.0.0.0
```

1.4.3 配置ICMP报文差错报文的发送速率

配置效果

配置 ICMP 差错报文的发送速率。

注意事项

-

配置方法

▾ 配置 IP 首部不可分片位触发的 ICMP 目的不可达报文的发送速率

- 可选配置。
- 在全局模式下配置。

▾ 配置其它 ICMP 差错报文的发送速率

- 可选配置。
- 在全局模式下配置。

检验方法

执行 **show running-config** 可以看到配置生效。

相关命令

▾ 配置 IP 首部不可分片位触发的 ICMP 目的不可达报文的发送速率

- 【命令格式】 **ip icmp error-interval DF milliseconds [bucket-size]**
- 【参数说明】 *milliseconds* : 令牌桶的刷新周期, 取值范围 0~2147483647, 缺省值为 100, 单位为毫秒。取值为 0 时, 表示不限制 ICMP 差错报文的发送速率。
bucket-size : 令牌桶中容纳的令牌数, 取值范围 1~200, 缺省值为 10。
- 【命令模式】 全局模式
- 【使用指导】 为了防止拒绝服务攻击, 对 ICMP 差错报文的发送速率进行限制, 采用令牌桶算法。
如果 IP 报文需要分片, 但是 IP 首部的不可分片位被设置了, 设备会向源 IP 地址发送编号为 4 的 ICMP 目的不可达报文, 这种 ICMP 差错报文的主要用途是路径 MTU 发现。为了防止其它 ICMP 差错报文太多导致发不出编号为 4 的 ICMP 目的不可达报文, 从而导致路径 MTU 发现功能失效, 对编号为 4 的 ICMP 目的不可达报文和其它 ICMP 差错报文分别限速。
因为定时器的精度是 10 毫秒, 建议用户把令牌桶的刷新周期配置成 10 毫秒的整数倍。如果令牌桶的刷新周期大于 0 小于 10, 实际生效的刷新周期是 10 毫秒, 例如配置 5 毫秒 1 个, 实际效果是 10 毫秒 2 个; 如果令牌桶的刷新周期不是 10 毫秒的整数倍, 实际生效的刷新周期自动换算成 10 毫秒的整数倍, 例如配置 15 毫秒 3 个, 实际效果是 10 毫秒 2 个。

配置其它 ICMP 差错报文的发送速率

- 【命令格式】 **ip icmp error-interval milliseconds [bucket-size]**
- 【参数说明】 *milliseconds* : 令牌桶的刷新周期, 取值范围 0~2147483647, 缺省值为 100, 单位为毫秒。取值为 0 时, 表示不限制 ICMP 差错报文的发送速率。
bucket-size : 令牌桶中容纳的令牌数, 取值范围 1~200, 缺省值为 10。
- 【命令模式】 全局模式
- 【使用指导】 为了防止拒绝服务攻击, 对 ICMP 差错报文的发送速率进行限制, 采用令牌桶算法。
因为定时器的精度是 10 毫秒, 建议用户把令牌桶的刷新周期配置成 10 毫秒的整数倍。如果令牌桶的刷新周期大于 0 小于 10, 实际生效的刷新周期是 10 毫秒, 例如配置 5 毫秒 1 个, 实际效果是 10 毫秒 2 个; 如果令牌桶的刷新周期不是 10 毫秒的整数倍, 实际生效的刷新周期自动换算成 10 毫秒的整数倍, 例如配置 15 毫秒 3 个, 实际效果是 10 毫秒 2 个。

配置举例

- 【配置方法】 配置 IP 首部不可分片位触发的 ICMP 目的不可达报文的发送速率为 1 秒 100 个, 配置其它 ICMP 差错报文的发送速率为 1 秒 10 个。
- ```
Ruijie(config)# ip icmp error-interval DF 1000 100
Ruijie(config)# ip icmp error-interval 1000 10
```
- 【检验方法】 执行 **show running-config** 可以看到配置生效
- ```
Ruijie#show running-config | include ip icmp error-interval
ip icmp error-interval 1000 10
ip icmp error-interval DF 1000 100
```

1.4.4 配置IP TTL

配置效果

修改接口的 IP TTL 值。

注意事项

-

配置方法

- 可选配置。
- 在三层接口模式下配置。

检验方法

通过 **show run-config** 可以看到配置生效

相关命令

▾ 配置 IP TTL

- 【命令格式】 **ip ttl value**
- 【参数说明】 *value* : TTL 值, 取值范围是 0~255。
- 【命令模式】 全局模式
- 【使用指导】 -

配置举例

- 【配置方法】 配置本机发送的单播报文的缺省 TTL 值为 100。

```
Ruijie#configure terminal
Ruijie(config)#ip ttl 100
```

- 【检验方法】 通过 **show run-config** 可以看到配置生效

```
Ruijie#show running-config
ip ttl 100
```

1.4.5 配置IP源路由

配置效果

开启或关闭 IP 源路由信息的处理功能。

注意事项

-

配置方法

- 缺省情况下开启 IP 源路由功能。
- 可选配置，通过 **no ip source-route** 可关闭 IP 源路由功能。

检验方法

通过 **show run-config** 可以看到配置生效。

相关命令

▾ 配置 IP 源路由

【命令格式】 **ip source-route**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 -

配置举例

【配置方法】 关闭了 IP 源路由信息的处理功能。

```
Ruijie#configure terminal
Ruijie(config)# no ip source-route
```

【检验方法】 通过 **show run-config** 可以看到配置生效

```
Ruijie#show running-config
no ip source-route
```

1.5 监视与维护

清除各类信息

-

查看运行情况

作用	命令
显示接口 IP 信息	show ip interface [<i>interface-type interface-number</i> brief]
显示转发表	show ip route [<i>address</i> [<i>mask</i>]]
显示转发表的统计值	show ip route summary
显示 IP 报文统计值	show ip packet statistics [total <i>interface-name</i>]

查看调试信息

-

2 ARP

2.1 概述

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。地址解析的方式有两类：1) 地址解析协议 (ARP)；。关于 ARP，分别在 RFC 826，RFC 1027 文档中描述。

ARP(Address Resolution Protocol，地址解析协议)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 缓存中。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。

协议规范

- RFC826 : An Ethernet Address Resolution Protocol
- RFC1027 : Using ARP to implement transparent subnet gateways

2.2 典型应用

典型应用	场景描述
在局域网内提供地址解析协议服务	在同一段中，主机学习其他设备的 MAC 地址，需要用到地址解析协议。
使用代理ARP实现透明的子网网关	通过代理地址解析服务，允许主机在不知道另一个网络是否存在的情况下和另一网络内的主机直接通讯。

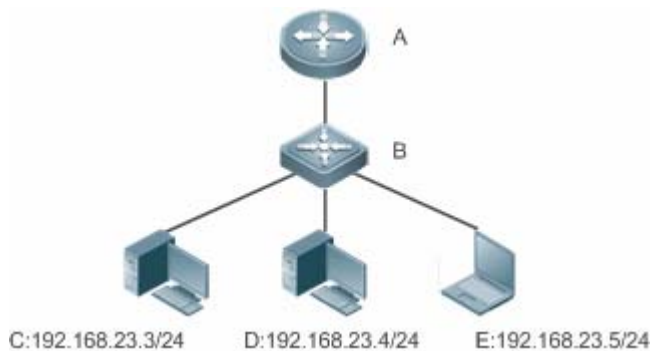
2.2.1 在局域网内提供地址解析协议服务

应用场景

在所有 IPv4 局域网内，都需要用到 ARP 协议。

- 主机需要通过 ARP 协议来学习其他设备的 MAC 地址，只有学到 MAC 地址后，主机才可以和其他设备通信。

图 2-1



- 【注释】 A 为路由器
B 为交换机，作为用户主机网段的网关。
C、D、E 为用户主机

功能部属

- 在局域网内运行 ARP 协议，实现 IP 地址和 MAC 地址的映射。

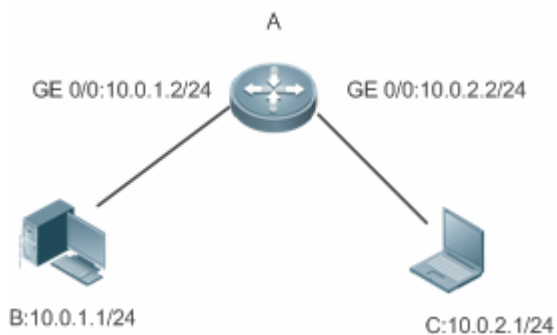
2.2.2 使用代理ARP实现透明的子网网关

应用场景

在不同的 IPv4 局域网内，实现透明的子网网关。

- 通过在设备上配置代理 ARP 的功能，实现不同网段内主机的直接通讯。

图 2-错误!未定义书签。



- 【注释】 A 为路由器，连接两个局域网
B、C 为用户主机，不配置默认网关，在不同的子网

功能部属

- 在子网网关上运行代理 ARP 功能，可以帮助没有路由信息的主机获得其它子网 IP 地址的 MAC 地址。

2.3 功能详解

功能特性

功能特性	作用
静态ARP	用户手工指定 IP 地址和 MAC 地址的映射，防止设备学到错误的 ARP 表项而影响网络。
ARP属性设置	用户指定 ARP 表项的超时时间、ARP 请求重传次数和间隔、未解析 ARP 表项数上限。
免费ARP	检测 IP 地址冲突，以及让外围设备更新本机的 ARP。
ARP可信检测	通过 NDU（邻居不可达探测），保证学习的 ARP 表项正确。
ARP防IP报文攻击	通过设置触发 ARP 设丢弃表项的 IP 报文个数，触发设置丢弃表项到硬件，来防止未知名单播报文大量送 CPU 对 CPU 造成冲击。

2.3.1 静态ARP

静态 ARP 包括手工配置的静态 ARP 和认证下发的静态 ARP。手工配置的静态 ARP 优先级大于认证下发的静态 ARP。静态 ARP 能够防止设备学到错误的 ARP 表项而影响网络。

工作原理

静态 ARP，设备不会再去主动更新 ARP 表项，并且永久存在。

设备转发三层报文时，以太头部的目的 MAC 地址将采用静态配置的 MAC 地址来封装。

相关配置

配置静态 ARP

手工配置的静态 ARP，在全局模式下，使用 `arp ip-address mac-address type` 命令配置静态 ARP 表项。缺省情况下用户没有配置任何静态 ARP 表项。ARP 封装只支持 Ethernet II 类型，用 `arpa` 表示。

2.3.2 ARP属性设置

用户指定 ARP 表项的超时时间、ARP 请求重传次数和间隔、接口 ARP 学习数量限制。

工作原理

ARP 超时设置

ARP 超时设置只对动态学习到的 IP 地址和 MAC 地址映射起作用。当一个 ARP 表项超时后，设备会发送单播 ARP 请求报文探测对方是否在线，假如能收到对方的 ARP 应答，则说明对方仍在线，该 ARP 表项不会删除，否则会删除该 ARP 表项。

超时时间设置得越短，ARP 缓冲中保存的映射表就越真实，但是 ARP 消耗网络带宽也越多。

↘ ARP 请求重传时间间隔和次数

IP 地址解析成 MAC 地址时连续发送 ARP 请求的时间间隔和次数。时间间隔越短，解析速率更快。次数越多，解析成功率更大，但是 ARP 消耗网络带宽也越多。

↘ 接口 ARP 学习数量限制

改成通过配置指定接口的用户 ARP 表项个数，灵活控制 ARP 表项资源的按需分配，防止表项资源浪费。

相关配置

↘ ARP 超时设置

在接口模式下，使用命令 **arp timeout seconds** 配置 ARP 的超时时间。默认情况下超时时间为 3600 秒，用户可以根据实际情况重新调整。

↘ ARP 请求重传时间间隔和次数

- 在全局模式下，使用命令 **arp retry interval seconds** 配置 ARP 的重传时间间隔。默认情况下超时时间为 1 秒，用户可以根据实际情况重新调整。
- 在全局模式下，使用命令 **arp retry times number** 配置 ARP 的重传次数。默认情况下可以连续发送 5 次，用户可以根据实际情况重新调整。

↘ 接口 ARP 学习数量限制

在接口模式下，使用命令 **arp cache interface-limit limit** 配置接口 ARP 的学习数量限制。默认不限制接口上 ARP 学习的数量，用户可以根据实际情况重新调整。此数量限制包含静态 ARP。

2.3.3 免费ARP

工作原理

免费 ARP 报文是一种特殊的 ARP 报文，该报文的发送端 IP 地址和目标 IP 地址都是本机 IP 地址。免费 ARP 的主要用途有：

1. IP 地址冲突检测。当设备收到免费 ARP 报文后，如果发现报文中的 IP 地址和自己的 IP 地址相同，向发送免费 ARP 报文的设备返回一个 ARP 应答，告诉该设备 IP 地址冲突。
2. 当接口的 MAC 地址变化时，发送免费 ARP 通知其它设备更新 ARP 表项。

设备具有免费 ARP 报文学习功能。当设备收到免费 ARP 报文时，设备判断是否存在和免费 ARP 报文源 IP 地址对应的动态 ARP 表项，如果存在，根据免费 ARP 报文中携带的信息更新 ARP 表项。

相关配置

配置免费 ARP

接口模式下，使用命令 **arp gratuitous-send interval seconds [number]** 允许接口定时发送免费 ARP 请求报文。缺省情况下接口上该功能是关闭的。一般在该接口充当下联设备网关时，需要开启这个功能，定时更新使下联设备的网关 mac，防止他人冒充网关。

2.3.4 ARP可信检测

工作原理

该命令用于防止 arp 欺骗导致无用的 arp 表项过多占用设备资源。在三层接口开启 arp 可信检测功能后，从该接口上收到 arp 请求报文：

1. 如果对应表项不存在，则创建动态 arp 表项，并经过 1 到 5 秒的一个随机时间后进入 NUD（邻居不可达探测），即将新学习的 arp 表项设置为老化状态并单播 arp 请求，在老化时间内收到对端 arp 更新，则保存表项，否则直接删除该表项。
2. 如果对应 arp 表项已经存在，则不进行 NUD 探测逻辑。
3. 如果已有的动态 arp 表项的 MAC 地址被更新，也走 NUD 探测逻辑。

该功能由于在 ARP 学习过程中增加了一个严格确认的过程，所以开启该功能会影响到 ARP 的学习性能。

关闭该功能后，arp 表项的学习和更新不再走 NUD 逻辑。

相关配置

配置 ARP 可信检测

接口模式下，使用命令 **arp trust-monitor enable** 命令开启 ARP 可信检查功能，缺省情况下没有开启该功能。

2.3.5 ARP防IP报文攻击

工作原理

在收到未解析的 IP 报文时，交换机设备不能够进行硬件转发，需要把报文送 CPU 进行地址解析，如果此类报文大量送 CPU，就会对 CPU 造成冲击，影响交换机其它业务的运行。

开启 ARP 防 IP 报文攻击后，在 ARP 请求期间，交换机 CPU 会统计收到的目的 IP 命中该 ARP 表项的报文个数，当这个个数等于配置的个数时，会设置一个丢弃表项到硬件，后续硬件收到所有该目的 IP 的报文都不会送 CPU；在地址解析完成时，更新上述表项为转发状态，使得交换机能够对该目的 IP 的报文进行硬件转发。

相关配置

配置 ARP 防 IP 报文攻击

- 全局模式下，使用命令 **arp anti-ip-attack** 配置触发 ARP 丢弃表项的 IP 报文个数。

- 缺省情况下，在 3 个目的 IP 地址相同的未知名单播报文送 CPU 后，就会设置丢弃表项。

2.4 配置详解

配置项	配置建议&相关命令	
配置静态ARP	 可选配置，用于 IP 地址和 MAC 地址的静态绑定。	
	arp	定义静态 ARP
配置ARP属性	 可选配置，用于指定 ARP 表项的超时时间、ARP 请求重传次数和间隔、接口 ARP 学习数量限制	
	arp timeout	配置 ARP 超时时间
	arp retry interval	配置 ARP 请求重传时间间隔
	arp cache interface-limit	配置接口 ARP 学习数量限制
配置免费ARP	 可选配置，用于检测 IP 地址冲突，以及让外围设备更新本机的 ARP。	
	arp gratuitous-send interval	开启定时发送免费 ARP 的功能
配置ARP可信检测	 可选配置，用于发送单播 ARP 请求确认，以保证学习 ARP 表项正确性。	
	arp trusted-monitor enable	开启 ARP 可信检测功能
配置ARP防IP报文攻击	 可选配置，防止 IP 报文大量送 CPU 对 CPU 造成冲击。	
	arp anti-ip-attack	配置触发 ARP 设丢弃表项的 IP 报文个数。

2.4.1 配置静态ARP

配置效果

用户手工指定 IP 地址和 MAC 地址的映射，防止设备学到错误的 ARP 表项而影响网络。

注意事项

对于三层交换机，配置完静态 ARP 表项后，交换机必须在学习到该静态 ARP 表项的 MAC 地址对应的物理端口后才能进行正常的三层路由。

配置方法

▾ 配置静态 ARP

- 可选配置
- 在汇聚设备上，可以通过静态绑定上联设备的 IP 和 MAC 地址的映射，防止设备因受到 ARP 攻击而更改掉上联设备的 ARP 表项的 MAC 地址，导致网络异常。
- 在全局模式下配置

检验方法

使用命令 **show running-config** 查看命令是否生效，或使用命令 **show arp static** 查看是否成功创建了静态 ARP 缓存表。

相关命令

配置静态 ARP

【命令格式】 **arp ip-address mac-address type**

【参数说明】 *ip-address* : 与 MAC 地址对应的 IP 地址，分为四组十进制表示的数值，组之间用点隔开。

mac-address : 数据链路层地址，48 个比特位组成。

type : ARP 封装类型。对于以太网接口，关键字为 arpa。

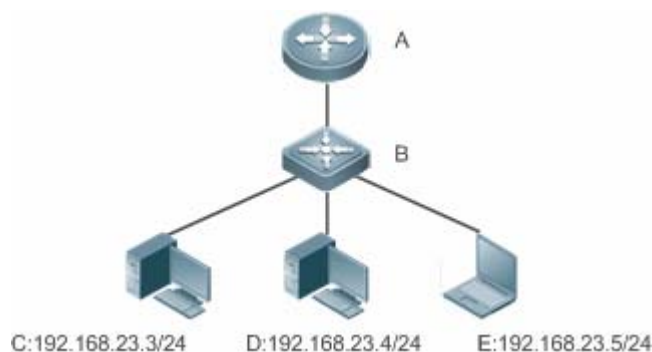
【命令模式】 全局模式

【使用指导】 RGOS 使用 ARP 缓冲表，根据 32 个比特位 IP 地址查找 48 个比特位的 MAC 地址。

由于大多数主机支持动态 ARP 解析，所以通常不需要配置静态 ARP 映射。利用 **clear arp-cache** 命令可以删除动态学习到的 ARP 映射。

配置举例

【网络环境】



【注释】 A 为路由器

B 为交换机，作为用户主机网段的网关。

C、D、E 为用户主机

【配置方法】 在设备 B 上配置静态 ARP 表项，静态绑定设备 A 的 IP 和 MAC 地址映射。

```
Ruijie(config)#arp 192.168.23.1 00D0.F822.334B arpa
```

【检验方法】 通过 **show arp static** 命令可查看静态 ARP 表项：

```
Ruijie(config)#show arp static
```

```
Protocol Address Age(min) Hardware Type Interface
Internet 192.168.23.1<static> 00D0.F822.334B arpa
1 static arp entries exist.
```

常见配置错误

- 静态绑定的 MAC 地址错误。

2.4.2 配置ARP属性

配置效果

用户指定 ARP 表项的超时时间、ARP 请求重传次数和间隔、接口 ARP 学习数量限制。

注意事项

无

配置方法

▾ ARP 超时设置

- 可选配置
- 局域网中如果用户上下线较频繁，则可以将 ARP 超时时间设置小一点，可以将无效的 ARP 表项尽早删除。
- 在接口模式下配置

▾ ARP 请求重传时间间隔和次数

- 可选配置
- 在网络带宽资源不足时，可以将重传时间间隔配大，次数配小，以减少网络带宽的消耗。
- 在全局模式下配置

▾ 接口 ARP 学习数量限制

- 可选配置
- 在接口模式下配置

检验方法

使用命令 `show arp timeout` 可以查看所有接口的老化超时时间。

使用命令 **show running-config** 查看 ARP 请求重传时间间隔和次数、接口 ARP 学习数量限制命令是否生效。

相关命令

▾ ARP 超时设置

【命令格式】 **arp timeout seconds**

【参数说明】 *seconds* : 超时时间, 以秒为计算单位, 默认值为 3600, 范围 0-2147483。

【命令模式】 接口模式

【使用指导】 ARP 超时设置只对动态学习到的 IP 地址和 MAC 地址映射起作用。超时时间设置得越短, ARP 缓存中保存的映射表就越真实, 但是 ARP 消耗网络带宽也越多, 所以需要权衡利弊。除非有特别的需要, 否则一般不需要配置 ARP 超时时间。

▾ ARP 请求重传时间间隔和次数

【命令格式】 **arp retry interval seconds**

【参数说明】 *seconds* : <1-3600>, ARP 请求的重传时间可以设置为 1~3600 秒, 默认值为 1 秒。

【配置模式】 全局模式

【使用指导】 当发现本设备有频繁的向外发送 ARP 请求, 引起网络繁忙等其它问题时, 可以将 ARP 请求的重传时间设置长一点, 一般不要超过动态 ARP 表项的老化时间。

▾ 接口 ARP 学习数量限制

【命令格式】 **arp cache interface-limit limit**

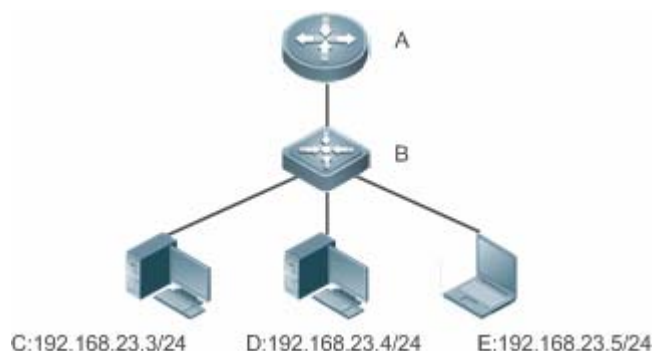
【参数说明】 *limit* : 指定接口所能学习的 ARP 数量最大限制, 包括静态配置和动态学习的 ARP, 取值范围为 0-设备支持的 ARP 表项容量, 0 表示不限制接口 ARP 学习数量。

【配置模式】 接口模式

【使用指导】 限制接口的 ARP 学习数量, 可防止恶意的 ARP 攻击, 让设备生成大量的 ARP 表项, 占用过多的表项资源。配置的值必须不小于当前接口已经学习到的 ARP 表项数量, 否则配置不生效。该限制受限于设备支持的 ARP 容量。

配置举例

【网络环境】



【注释】 A 为路由器

B 为交换机，作为用户主机网段的网关。

C、D、E 为用户主机

- 【配置方法】
- 配置接口 GigabitEthernet 0/1 下的 ARP 超时时间为 60 秒
 - 配置接口 GigabitEthernet 0/1 下的 ARP 学习数量限制为 300
 - 配置 ARP 请求重传时间间隔为 3 秒
 - 配置 ARP 请求重传次数为 4 次

```
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#arp timeout 60
Ruijie(config-if-GigabitEthernet 0/1)#arp cache interface-limit 300
Ruijie(config-if-GigabitEthernet 0/1)#exit
Ruijie(config)#arp retry interval 3
Ruijie(config)#arp retry times 4
```

- 【检验方法】
- 通过 **show arp timeout** 查看接口的老化时间
 - 通过 **show running-config** 查看 ARP 请求重传时间间隔和次数、接口 ARP 学习数量限制

```
Ruijie#show arp timeout
Interface                arp timeout(sec)
-----
GigabitEthernet 0/1      60
GigabitEthernet 0/2      3600
GigabitEthernet 0/4      3600
GigabitEthernet 0/5      3600
GigabitEthernet 0/7      3600
VLAN 100                  3600
VLAN 111                  3600
Mgmt 0                    3600

Ruijie(config)# show running-config
arp retry times 4
arp retry interval 3
!
interface GigabitEthernet 0/1
  arp cache interface-limit 300
```

常见配置错误

无

2.4.3 配置免费ARP

配置效果

接口定时发送免费 ARP 报文。

注意事项

无

配置方法

- 可选配置
- 设备做用户网关时，为了防止因为 ARP 欺骗导致其他用户学习到错误的网关 MAC 后会一直上不了网，需要在接口上开启免费 ARP 功能。
- 在接口模式下配置

检验方法

使用 `show running-config interface [name]` 查看是否配置成功。

相关命令

▾ 开启定时发送免费 ARP 的功能

【命令格式】 `arp gratuitous-send interval seconds [number]`

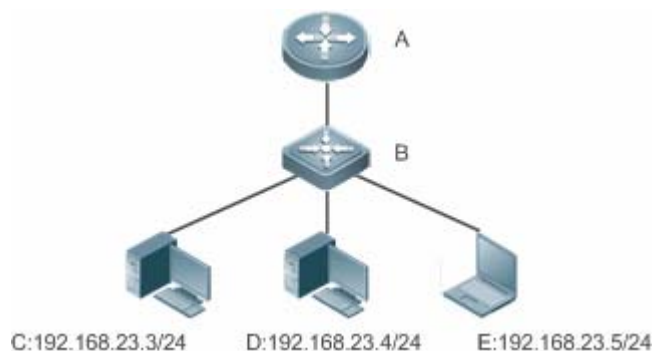
【参数说明】 `seconds`：发送免费 ARP 请求的时间间隔，单位秒，取值范围<1-3600>。
`number`：发送免费 ARP 请求的数量，缺省值是 1，取值范围<1-100>。

【命令模式】 接口模式

【使用指导】 当设备的网络接口作为下联设备的网关时，如果下联设备中有冒充网关的行为，则可以在此接口配置定时发送免费 ARP 请求，公告自己才是真正的网关。

配置举例

【网络环境】



【注释】 A 为路由器

B 为交换机，作为用户主机网段的网关。

C、D、E 为用户主机

【配置方法】 配置 GigabitEthernet 0/0 口发送免费 ARP 功能，频率为每 5 秒发送一个免费 ARP 请求报文。

```
Ruijie(config-if-GigabitEthernet 0/0)#arp gratuitous-send interval 5
```

【检验方法】 使用 **show running-config interface** 命令查看配置是否生效

```
Ruijie#sh running-config interface gigabitEthernet 0/0
```

```
Building configuration...
Current configuration : 127 bytes
!
interface GigabitEthernet 0/0
 duplex auto
 speed auto
 ip address 30.1.1.1 255.255.255.0
 arp gratuitous-send interval 5
```

常见配置错误

无

2.4.4 配置ARP可信检测

配置效果

开启 arp 可信检测功能，在收到 arp 请求报文后，如果对应表项不存在，进入 NUD（邻居不可达探测）。如果已有的动态 arp 表项的 MAC 地址被更新，马上走 NUD 探测逻辑，起到防止 arp 攻击的作用。

注意事项

该功能由于在 ARP 学习过程中增加了一个严格确认的过程，所以开启该功能会影响到 ARP 的学习性能。

配置方法

- 可选配置。
- 如果有要求严格学习 ARP 表项的需求时，设备上可以开启 arp 可信功能，设备在收到 arp 请求报文后，如果之前不存在对应 arp 表项，则需要发送单播 ARP 请求报文，在确认对端真实存在后才学习 ARP 表项，否则不学习 ARP 表项。在 arp 表项的 mac 地址发生了变化后，马上走 NUD 探测，防止 arp 欺骗。
- 在接口模式下配置

检验方法

使用 **show running-config interface [name]**查看是否配置成功。

相关命令

▾ 开启 ARP 可信检测功能

【命令格式】 **arp trust-monitor enable**

【参数说明】 -

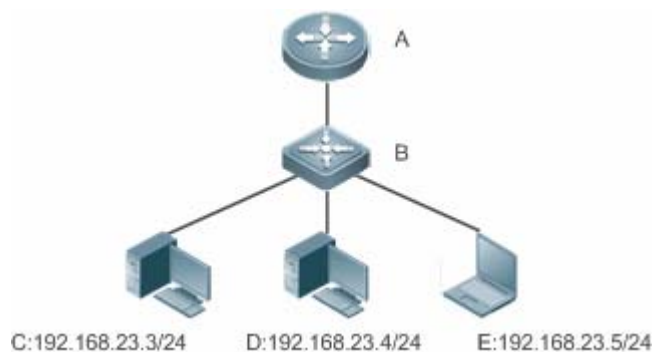
【命令模式】 接口模式

【使用指导】

- ❗ 开启该功能，如果对应 arp 表项已经存在，且 mac 地址没发生更新，则不进行 NUD 探测逻辑。
- ❗ 开启该功能，如果已有的动态 arp 表项的 mac 地址被更新，则马上走 NUD 探测逻辑。
- ❗ 关闭该功能后，arp 表项的学习和更新不需要 NUD 过程。

配置举例

【网络环境】



- 【注释】 A 为路由器
B 为交换机，作为用户主机网段的网关。
C、D、E 为用户主机

【配置方法】 配置 GigabitEthernet 0/0 口开启 ARP 可信检测功能

```
Ruijie(config-if-GigabitEthernet 0/0)#arp trust-monitor enable
```

【检验方法】 使用 **show running-config interface** 查看是否配置是否生效

```
Ruijie#show running-config interface gigabitEthernet 0/0
```

```
Building configuration...
Current configuration : 184 bytes
!
interface GigabitEthernet 0/0
duplex auto
```

```
speed auto
ip address 30.1.1.1 255.255.255.0
arp trust-monitor enable
```

常见配置错误

无

2.4.5 配置ARP防IP报文攻击

配置效果

交换机 CPU 收到配置个数的目的 IP 命中该 ARP 表项的报文时，后续所有该目的 IP 的报文都不会送 CPU。

注意事项

只在交换机产品上支持。

配置方法

- 可选配置。
- 在交换机产品上，默认情况下，在 3 个未知名单播报文送 CPU 后设置丢弃表项。通过此命令用户可以针对具体网络环境调整这个参数，也可以关闭该功能。
- 在全局模式下配置。

检验方法

使用 `show run` 命令查看是否配置成功。

相关命令

配置 ARP 防 IP 报文攻击

【命令格式】 `arp anti-ip-attack num`

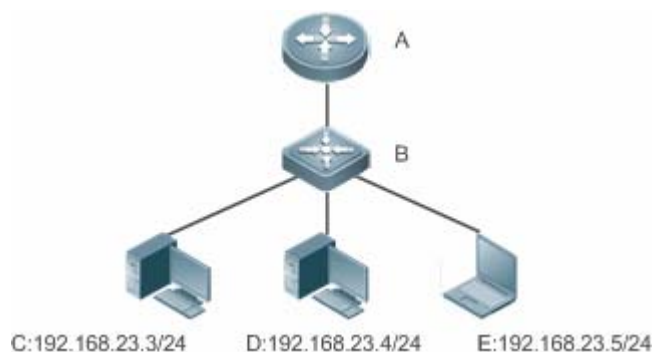
【参数说明】 `num`：设置触发 ARP 丢弃表项的 IP 报文个数，取值范围<0-100>。
0 表示关闭 ARP 防 IP 报文攻击功能。缺省值为 3。

【命令模式】 全局模式

【使用指导】  如果硬件路由资源比较充分，`arp anti-ip-attack num` 可以设置得小一些。在硬件路由资源比较紧张的情况下，要优先满足正常路由的使用，可以将 `arp anti-ip-attack num` 设置得比较大，或者关闭该功能。

配置举例

【网络环境】



- 【注释】 A 为路由器
 B 为交换机，作为用户主机网段的网关。
 C、D、E 为用户主机

【配置方法】 在设备B上配置ARP防IP报文攻击。

```
Ruijie(config)#arp anti-ip-attack 10
```

【检验方法】 使用 **show running-config** 查看配置是否生效

```
Ruijie#show running-config
```

```
Building configuration...
Current configuration : 53 bytes
arp anti-ip-attack 10
```

常见配置错误

无

2.5 监视与维护

清除各类信息

! 在设备运行过程中执行 **clear** 命令，可能因为重要信息丢失而导致业务中断。

作用	命令
清除动态 ARP 表项。在网关认证模式下，不会删除认证 VLAN 下的动态 ARP 表项。	clear arp-cache
清零 ARP 报文统计信息	clear arp-cache packet statistics [<i>interface</i>]

查看运行情况

作用	命令
显示 ARP 表。	show arp [detail] [interface-type interface-number[ip [mask] mac-address static complete incomplete]]
显示 ARP 表	show ip arp
显示 ARP 表项相应计数	show arp counter
显示动态 ARP 表项的老化时间	show arp timeout
查看 ARP 报文统计信息	show arp packet statistics [interface]

查看调试信息

 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
显示 ARP 报文的收发情况	debug arp
显示 ARP 表项的创建删除情况	debug arp event

3 DHCP

3.1 概述

DHCP (Dynamic Host Configuration Protocol , 动态主机设置协议) 是一个局域网的网络协议，使用UDP协议工作，被广泛用来动态分配可重用的网络资源，如IP地址。

DHCP 是基于 Client 工作模式。

协议规范

- RFC2131 : Dynamic Host Configuration Protocol
- RFC2132 : DHCP Options and BOOTP Vendor Extensions

3.2 典型应用

典型应用	场景描述
在局域网内提供DHCP服务	为局域网内下游用户分配地址。
设备启动DHCP Client功能	局域网内下游多设备启动 DHCP Client 功能。

3.2.1 在局域网内提供DHCP服务

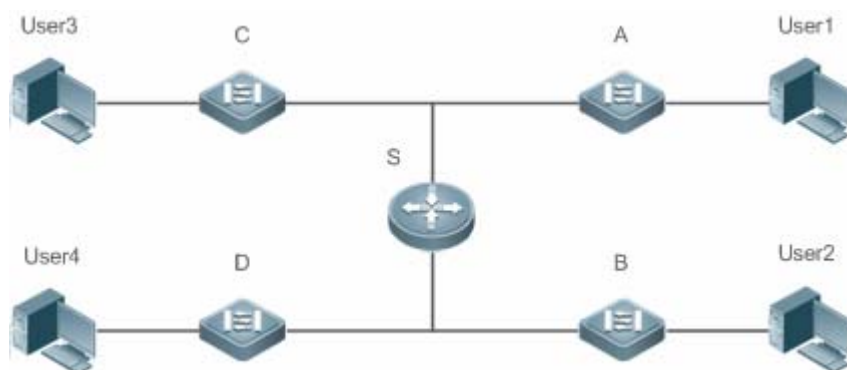
应用场景

在一个局域网内，为四个用户分配 IP 地址。

以下图为例，为 User1、User2、User3 、User4 分配 IP 地址。

- User1、User2、User3 、User4 通过 A、B、C、D 与 Server 相连

图 3-1



- 【注释】 S为出口网关设备，作 DHCP-Server。
A、B、C、D 为接入交换机，作二层透传
User1、User2、User3 、User4 为用户

功能部署

- Server(S)上运行 DHCP-Server 服务
- 在 A、B、C、D 上实行二层 VLAN 透传功能
- User1、User2、User3 、User4 上主动发起 DHCP-Client 请求

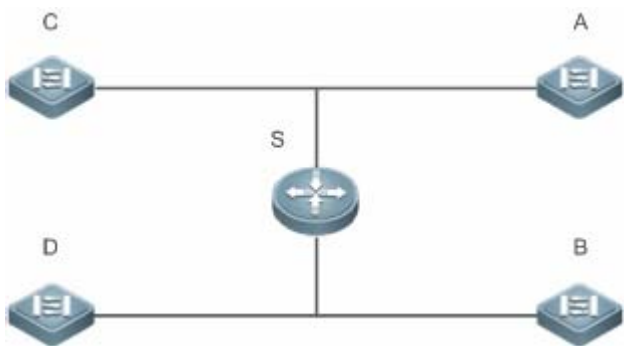
3.2.2 设备启动DHCP Client功能

应用场景

在一个局域网内，A、B、C、D 四个接入设备向 S 请求地址

以下图为例，A、B、C、D 接口上开启 DHCP-Client 功能，请求 IP 地址。

图 3-2



- 【注释】 S为出口网关设备，作 DHCP-Server。
A、B、C、D 为接入交换机，接口启动 DHCP-Client 功能

功能部署

- Server(S)上运行 DHCP-Server 服务
- 在 A、B、C、D 在接口上开启 DHCP-Client 功能

3.3 功能详解

基本概念

📌 DHCP 客户端

DHCP 客户端可以让设备自动地从 DHCP 服务器获得 IP 地址以及其它配置参数。

功能特性

功能特性	作用
DHCP客户端	设备启用 DHCP Client 功能，可以自动从 DHCP 服务器获取 IP 地址以及其它配置参数。

3.3.1 DHCP客户端

工作原理

Client 状态机进入 Init 状态，主动发出广播 Discover 报文，之后 Client 有可能收到多份 Offer，进入 Offer 选择阶段选择一份最优的 Offer 后给予该服务器响应，此后在地址的老化 1/2、4/5 周期内还会发出续租等报文请求对地址的继续使用。

相关配置

📌 接口上启动 DHCP-Client 功能

- 缺省情况下，该服务关闭。
- 接口模式下使用 `ip address dhcp` 开启功能。
- 必须开启客户端功能，才能进行 DHCP 服务。
- 该功能只在三层接口上有效，如 SVI、Router Port 等；

3.4 配置详解

📌 配置 DHCP 客户端

配置项	配置建议 & 相关命令	
配置DHCP客户端	 必须配置，用于启用 DHCP 客户端	
	<table border="1"> <tr> <td><code>ip address dhcp</code></td> <td>使得以太网或者 PPP、HDLC、FR 封装的接口能够通过 DHCP 获得 IP 地址信息</td> </tr> </table>	<code>ip address dhcp</code>
<code>ip address dhcp</code>	使得以太网或者 PPP、HDLC、FR 封装的接口能够通过 DHCP 获得 IP 地址信息	

3.4.1 配置DHCP客户端

配置效果

设备启动 dhcp-client，可动态取得地址及其它需求配置。

注意事项

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

配置方法

在接口上执行 `ip address dhcp` 命令

检验方法

查看接口是否取到 ip 地址

相关命令

配置 DHCP 客户端

【命令格式】 `ip address dhcp`

【参数说明】 -

【命令模式】 接口配置模式

- 【使用指导】
- 锐捷产品支持以太网端口通过 DHCP 获得动态分配的 IP 地址
 - 锐捷产品支持 ppp 封装的端口通过 DHCP 获得动态分配的 IP 地址
 - 锐捷产品支持 FR 封装的端口通过 DHCP 获得动态分配的 IP 地址
 - 锐捷产品支持 HDLC 封装的端口通过 DHCP 获得动态分配的 IP 地址

配置举例

DHCP 客户端配置

【配置方法】 1：为设备接口 FastEthernet 0/0 配置 DHCP 自动分配地址


```
Ruijie(config)# interface FastEthernet0/0
Ruijie(config-if-FastEthernet 0/0)#ip address dhcp
```

【检验方法】 1：show run 查看

```
Ruijie(config)#show run | begin ip address dhcp
ip address dhcp
```

3.5 监视与维护

清除各类信息

 在设备运行过程中执行 **clear** 命令，可能因为重要信息丢失而导致业务中断。

查看运行情况

作用	命令
显示 DHCP 租约信息	show dhcp lease

查看调试信息

 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
DHCP 报文调试开关	debug ip dhcp client

4 DNS

4.1 概述

DNS (Domain Name System , 域名系统) , 因特网上作为域名和IP地址相互映射的一个分布式数据库, 能够使用户更方便的访问互联网, 而不用去记住能够被机器直接读取的IP数串。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) 。

 下文仅介绍 DNS 的相关内容。

协议规范

- RFC1034 : DOMAIN NAMES - CONCEPTS AND FACILITIES
- RFC1035 : DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION

4.2 典型应用

典型应用	场景描述
静态域名解析	直接在本设备上根据预设的域名/IP 对应表进行域名解析
动态域名解析	从网络上的 DNS 服务器动态获取域名对应的地址

4.2.1 静态域名解析

应用场景

- 在设备上预设置域名和 IP 的对应表
- 设备上的一些应用 (比如 Ping , Telnet 等) 进行域名操作时, 直接在设备上就能解析到预设的 IP , 无需连到网络上的服务器。

功能部属

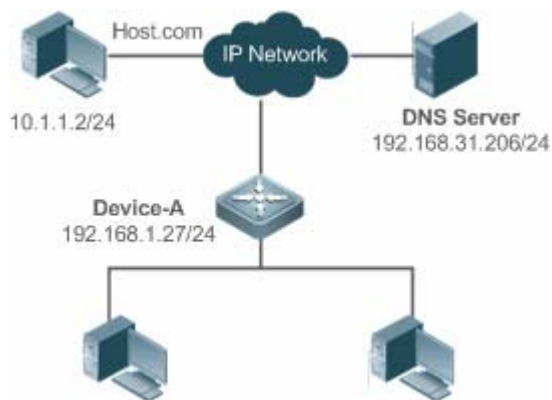
- 在设备上预设置域名和 IP 的对应关系

4.2.2 动态域名解析

应用场景

- “DNS Server” 部署在网络上，对外提供域名服务
- “host.com” 部署在网络上，使用域名(host.com)对外提供服务
- “Device-A”设备指定 “DNS Server” 作为 DNS 服务器，从 “DNS Server” 上获取到 “host.com”的地址

图 4-1 动态域名解析配置组网图



功能部属

- 将 DNS Server 部署为“Device-A”的 DNS 服务器

4.3 功能详解

基本概念

DNS

DNS 由解析器和域名服务器组成。域名服务器是指保存有网络中所有主机的域名和 IP 地址的对应关系，并提供将域名和 IP 互转的服务器。DNS 的 TCP 和 UDP 端口号都是 53，通常使用 UDP。

功能特性

功能特性	作用
域名解析	根据域名从域名服务器或本地数据库获取对应的 IP 地址

4.3.1 域名解析

工作原理

静态域名解析

静态域名解析，就是用户在设备上预先设置好域名和 IP 的对应关系，当用户使用某些应用(比如 Ping、Telnet 等等)进行域名操作时，系统从本设备上解析出域名对应的 IP，而不需要到网络上的 DNS 服务器获取域名对应的 IP。

📌 动态域名解析

动态域名解析，就是当用户使用某些应用进行域名操作时，系统 DNS 解析器查询外部的 DNS 服务器，获取到域名对应的 IP。

动态域名解析过程：

3. 用户应用(Ping、Telnet 等)向系统 DNS 解析器请求域名对应的 IP
4. 系统 DNS 解析器先查找动态缓存，如果动态缓存的域名未过期则返回给应用程序
5. 如果不存在未过期的域名，DNS 解析器向外部的 DNS 服务器发起域名转 IP 的请求
6. DNS 解析器接收到 DNS 服务器的应答，缓存并转发给应用程序

相关配置

📌 开启域名解析功能

- 缺省情况下，设备是开启域名解析功能。
- 通过 `ip domain-lookup` 命令开启域名解析功能。

📌 配置静态域名对应的 IP

- 缺省情况下，没有域名/IP 的静态配置。
- 通过 `ip host` 命令指定域名对应的 IPv4 地址

📌 配置域名服务器

- 缺省情况下，未配置域名服务器。
- 通过 `ip name-server` 命令配置域名服务器。

4.4 配置详解

配置项	配置建议 & 相关命令	
配置静态域名解析	⚠️ 可选配置	
	<code>ip domain-lookup</code>	开启域名解析功能
	<code>ip host</code>	配置域名对应的 IPv4 地址
配置动态域名解析	⚠️ 可选配置	
	<code>ip domain-lookup</code>	开启域名解析功能
	<code>ip name-server</code>	配置域名服务器

4.4.1 配置静态域名解析

配置效果

系统解析器从设备本地解析域名对应的 IP。

配置方法

▾ 开启域名解析功能

- 缺省已开启域名解析功能
- 如果关闭该功能，静态域名解析不生效。

▾ 配置静态域名对应的 IPv4 地址

- 必须配置，用户使用到的域名必须配置对应的 IP。

检验方法

- 通过 **show run** 查看配置信息。
- 通过 **show hosts** 当前的域名和 IP 对应关系

相关命令

▾ 配置域名对应的 IPv4 地址

- 【命令格式】 **ip host** *host-name ip-address*
- 【参数说明】 *host-name* : 域名
ip-address : 对应的 IPv4 地址
- 【命令模式】 全局模式
- 【使用指导】 -

配置举例

▾ 配置静态域名解析

- 【配置方法】 ● 在设备上静态配置域名 `www.test.com` 的 IP 地址为 `192.168.1.1`

```
Ruijie#configure terminal
Ruijie(config)# ip host www.test.com 192.168.1.1
Ruijie(config)# exit
```

- 【检验方法】 通过 **show hosts** 查看是否有所配置的静态域名表项

```
Ruijie#show hosts
```



```
Name servers are:
```

Host	type	Address	TTL(sec)
www.test.com	static	192.168.1.1	---

4.4.2 配置动态域名解析

配置效果

系统解析器从 DNS 服务器解析域名对应的 IP

配置方法

▾ 开启域名解析功能

- 缺省已开启域名解析功能
- 如果关闭该功能，动态域名解析不生效。

▾ 配置 DNS 服务器

- 必须配置，使用动态域名解析必须配置外部的 DNS 服务器。

检验方法

- 通过 **show run** 查看配置信息

相关命令

▾ 配置域名服务器

- 【命令格式】 **ip name-server** { *ip-address* }
- 【参数说明】 *ip-address* : DNS 服务器的 IPv4 地址
- 【命令模式】 全局模式
- 【使用指导】 -

配置举例

▾ 配置动态域名解析

【网络环境】

图 4-2



DEVICE : 从网络上的 DNS 服务器(192.168.10.1)解析域名

【配置方法】

在设备上配置 DNS 服务器地址为 192.168.10.1

```
DEVICE#configure terminal
DEVICE(config)# ip name-server 192.168.10.1
DEVICE(config)# exit
```

【检验方法】

通过 **show hosts** 查看是否配置指定 DNS 服务器

```
Ruijie(config)#show hosts
Name servers are:
192.168.10.1 static
```

Host	type	Address	TTL(sec)
------	------	---------	----------

4.5 监视与维护

清除各类信息

! 在设备运行过程中执行 **clear** 命令，可能因为重要信息丢失而导致业务中断。

作用	命令
清除动态主机名缓存表。	clear host [<i>host-name</i>]

查看运行情况

作用	命令
查看 DNS 的相关参数	show hosts [<i>host-name</i>]

查看调试信息

! 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
打开调试功能	debug ip dns

5 网络通信检测工具

5.1 概述

网络通信检测工具可以用于检查网络是否能够连通，用好网络通信监测工具可以很好地帮助我们分析判定网络故障。网络通信检测工具包括 PING（Packet Internet Groper，因特网包探索器）和 Traceroute（路由侦测）。PING 工具主要用于检测网络通与不通，以及网络的时延，时延值越大，则表示网络速度越慢。Traceroute 工具则可以帮助用户了解网络的物理与逻辑连接的拓扑情况以及数据传输的效率。在网络设备上，这两个工具所对应的命令为 ping 和 traceroute。

协议规范

- RFC792：Internet Control Message Protocol

5.2 典型应用

典型应用	场景描述
端对端连通性检查	网络设备与目标主机都连接在 IP 网络上，都配置有 IP 地址。
主机路由检查	网络设备与目标主机都连接在 IP 网络上，都配置有 IP 地址。

5.2.1 端对端连通性检查

应用场景

图 5-1 网络设备 A 与目标主机 B 都连接在 IP 网络上。

网络设备与目标主机都连接在 IP 网络上，端对端连通性检查就是判定 IP 报文能否在二者之间传输。目标主机可以是网络设备本身，这种情况一般用于检查设备自身网络接口和 TCP/IP 协议配置的正确性。



功能部属

通过在网络设备上运行 Ping 功能。

5.2.2 主机路由检查

应用场景

图 5-2 网络设备 A 与目标主机 B 都连接在 IP 网络上。

网络设备与目标主机都连接在 IP 网络上，主机路由检查就是判定 IP 报文在二者之间传输，究竟需要经过多少网关（路由器）。目标主机通常不是网络设备本身，并且通常与网络设备不在同一个 IP 网段。



功能部属

通过在网络设备上运行 Traceroute 功能。

5.3 功能详解

功能特性

功能特性	作用
Ping连通性测试	检测指定 IPv4 地址是否可达，并输出相关信息。
Traceroute连通性测试	显示 IPv4 数据包从源地址到目的地址所经过的网关。

5.3.1 Ping连通性测试

工作原理

PING 工具向目标 IP 地址发送一个 ICMP 请求（ICMP Request）数据包，要求对方返回一个 ICMP 回声（ICMP Echo）数据包，来确定两台网络机器是否连接相通，时延是多少。

相关配置

- 通过 ping 命令进行配置

5.3.2 Traceroute连通性测试



工作原理

Traceroute 工具利用 ICMP 及 IP 报文头部的 TTL (Time To Live) 字段。首先，网络设备的 Traceroute 工具送出一个 TTL 是 1 的 ICMP Request 到目的主机，当路径上的第一个路由器收到这个报文时，它将 TTL 减 1。此时 TTL 变为 0 了，所以该路由器会将此报文丢弃，并送回一个 ICMP 超时 (ICMP time exceeded) 消息，Traceroute 工具收到这个消息后，便知道这个路由器存在于这个路径上，接着再送出另一个 TTL 是 2 的报文，发现第 2 个路由器。Traceroute 工具每次将送出的报文的 TTL 加 1 来发现另一个路由器，这个重复的动作一直持续到某个数据报文到达目的主机。当报文到达目的主机后，该主机不会送回 ICMP time exceeded 消息，而是送回 ICMP Echo，Traceroute 工具结束探测并显示从网络设备到目的主机的路径信息。

相关配置

- 通过 `traceroute` 命令进行配置

5.4 配置详解

配置项	配置建议 & 相关命令	
Ping连通性测试	 可选配置，用于检测 IPv4 地址是否可达。	
	<code>ping</code>	运行 Ping 功能。
Traceroute连通性测试	 可选配置，显示 IPv4 数据包从源地址到目的地址所经过的网关。	
	<code>traceroute</code>	运行 Traceroute 功能。

5.4.1 Ping连通性测试

配置效果

在网络设备上采用 Ping 连通性测试，可以得知该网络设备和目的主机之间是否保持连通，报文是否可以在网络设备和目的主机之间传输。

注意事项

执行 PING 操作的网络设备本身需要配置 IP 地址。

配置方法

- 如果需要检测 IPv4 地址是否可达，可通过 `Ping IPv4` 命令。

检验方法

输入 **ping** 命令，即可在 CLI 界面显示相关信息。

相关命令

📄 Ping IPv4

【命令格式】 `ping [ip] [address [length length] [ntimes times] [timeout seconds] [data data] [source source] [df-bit] [validate] [detail] [out-interface interface]]`

【参数说明】 `address`：指定目的 IPv4 地址或域名。

`length`：指定发送数据包数据填充段的长度，范围：36~18024，默认填充长度为 100。

`times`：指定发送数据包的个数，范围：1~ 4294967295。

`seconds`：指定超时的时间，范围：1~10（秒）。

`data`：指定报文填充数据，格式为 1-255 长度的字符串，默认填充为 abcd。

`source`：指定报文源 IPv4 地址或源接口。其中，环回接口地址（例如 127.0.0.1）不允许作为源地址。

`df-bit`：设置 IP 的 DF 标识位，当 DF 位被设置为 1 时，表示不对数据包进行分段处理，默认 DF 位为 0。

`validate`：设置是否校验响应报文。

`detail`：设置回显是否显示详细信息，默认只显示 ‘!’ 和 ‘.’ 。

`interface`：指定发送数据报文的出口接口。

【命令模式】 在普通用户模式下，只能运行基本的 **ping** 功能；在特权用户模式下，还可以运行 **ping** 的扩展功能。

在其他模式下，可以通过 `do` 命令执行 **ping** 的扩展功能，具体配置请参考 `do` 命令说明。

【使用指导】 运行 **ping** 功能，如果有应答，则显示出应答的相关信息，最后输出一个统计信息。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，和基本的 **ping** 功能一样，最后也输出一个统计信息。要使用域名功能，则要先配置域名服务器，具体配置请参考 DNS 配置部分。

配置举例

📄 运行普通 Ping 功能

【配置方法】 在特权模式下输入 Ping IPv4 地址 192.168.21.26

常规 ping

```
Ruijie# ping 192.168.21.26
```

```
Sending 5, 100-byte ICMP Echoes to 192.168.21.26, 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
```

显示 detail 的 ping

```
Ruijie#ping 192.168.21.26 detail
```

```
Sending 5, 100-byte ICMP Echoes to 192.168.21.26, timeout is 2 seconds:
```

```
< press Ctrl+C to break >
```

```

Reply from 192.168.21.26: bytes=100 time=4ms TTL=64
Reply from 192.168.21.26: bytes=100 time=3ms TTL=64
Reply from 192.168.21.26: bytes=100 time=1ms TTL=64
Reply from 192.168.21.26: bytes=100 time=1ms TTL=64
Reply from 192.168.21.26: bytes=100 time=1ms TTL=64

```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms.
```

【检验方法】 缺省将 5 个数据段长度为 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，显示相应的探测信息，最后输出一个统计信息。

运行扩展 Ping 功能

【配置方法】 在特权模式下输入 Ping IPv4 地址 192.168.21.26，并指定发送数据包的长度、个数、超时的时间等。

常规 ping

```
Ruijie# ping 192.168.21.26 length 1500 ntimes 100 data ffff source 192.168.21.99 timeout 3
Sending 100, 1500-byte ICMP Echoes to 192.168.21.26, 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
```

显示 detail 的 ping

```
ping 192.168.21.26 length 1500 ntimes 20 data ffff source 192.168.21.99 timeout 3 detail
Sending 20, 1500-byte ICMP Echoes to 192.168.21.26, timeout is 3 seconds:
```

```
< press Ctrl+C to break >
```

```

Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=2ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=3ms TTL=64

```

```
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64

Success rate is 100 percent (20/20), round-trip min/avg/max = 1/1/3 ms.
```

【检验方法】 将 20 个长度为 1500Byte 的数据包发送到指定的 IP 地址，在指定的时间（3 秒）内，如果有应答，显示相应的探测信息，最后输出一个统计信息。

5.4.2 Traceroute 连通性测试

配置效果

在网络设备上采用 Traceroute 连通性测试，可以得知该网络设备和目的主机之间的路由拓扑信息，报文从网络设备到目的主机经过了多少个网关。

注意事项

执行 Traceroute 操作的网络设备本身需要配置 IP 地址。

配置方法

- 如果需要跟踪 IPv4 数据包到达目的主机经过哪些网关，可通过配置 Traceroute IPv4 命令。

检验方法

输入 `traceroute` 命令，即可在 CLI 界面显示相关信息。

相关命令

Traceroute IPv4

【命令格式】 `traceroute [ip] [address [probe number] [source source] [timeout seconds] [ttl minimum maximum] [out-interface interface]`

【参数说明】 `address`：指定目的 IPv4 地址或域名。
`number`：指定发送的探测的数量，范围：1~255。
`source`：指定报文源 IPv4 地址或源接口。其中，环回接口地址（例如 127.0.0.1）不允许作为源地址
`seconds`：指定超时的时间，范围：1~10（秒）。
`minimum maximum`：指定最小和最大 TTL 值，范围：1~255。
`interface`：指定发送数据报文的出口接口。

【命令模式】 在普通用户模式下，只能运行基本的 `traceroute` 功能；在特权用户模式下，还可以运行 `traceroute` 的扩展功

能。

【使用指导】 **Traceroute** 命令主要用于检查网络的连通性，并在网络故障发生时，准确的定位故障发生的位置。要使用域名功能，则要先配置域名服务器，具体配置请参考 DNS 配置部分。

配置举例

网络畅通的 Traceroute 举例

【配置方法】 在特权模式下，输入 Traceroute IPv4 地址 61.154.22.36。

```
Ruijie# traceroute 61.154.22.36
< press Ctrl+C to break >
Tracing the route to 61.154.22.36
 0  192.168.12.1          0 msec  0 msec  0 msec
 1  192.168.9.2           4 msec  4 msec  4 msec
 2  192.168.9.1           8 msec  8 msec  4 msec
 3  192.168.0.10          4 msec  28 msec 12 msec
 4  202.101.143.130       4 msec  16 msec  8 msec
 5  202.101.143.154      12 msec  8 msec  24 msec
 6  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。

网络中某些网关不通的 Traceroute 举例

【配置方法】 在特权模式下，输入 Traceroute IPv4 地址 202.108.37.42。

```
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。

6 TCP

6.1 概述

TCP 协议为应用层提供了一个可靠的、有连接的基于 IP 的传输层协议。

应用层向 TCP 层发送用于网间传输的、用 8 位字节表示的数据流，然后 TCP 把数据流分割成适当长度的报文段，最大分段大小 (MSS) 通常受该计算机连接的网路的数据链路层的最大传送单元 (MTU) 限制。之后 TCP 把报文传给 IP 层，由它来通过网络将报文传送给接收端实体的 TCP 层。

TCP 为了保证不发生丢包，就给每个字节一个序号，同时序号也保证了传送到接收端实体的包的按序接收。然后接收端实体对已成功收到的字节发回一个相应的确认 (ACK)；如果发送端实体在合理的往返时延 (RTT) 内未收到确认，那么对应的数据 (假设丢失了) 将会被重传。

- 在数据正确性与合法性上，TCP 用一个校验和函数来检验数据是否有错误，在发送和接收时都要计算校验和；同时可以使用 MD5 认证对数据进行校验。
- 在保证可靠性上，采用超时重传和捎带确认机制。
- 在流量控制上，采用滑动窗口协议，协议中规定，对于窗口内未经确认的分组需要重传。

协议规范

- RFC 793 : Transmission Control Protocol
- RFC 1122 : Requirements for Internet Hosts -- Communication Layers
- RFC 1191 : Path MTU Discovery
- RFC 1213 : Management Information Base for Network Management of TCP/IP-based internets:MIB-II
- RFC 2385 : Protection of BGP Sessions via the TCP MD5 Signature Option
- RFC 4022 : Management Information Base for the Transmission Control Protocol (TCP)

6.2 典型应用

典型应用	场景描述
TCP性能优化	TCP 传输路径上某一段链路的 MTU 比较小，为了避免 TCP 报文分片，可以开启 TCP 的路径 MTU 发现功能。
TCP连接异常检测	TCP 探测对端是否还在正常工作。

6.2.1 TCP性能优化

应用场景

以下图为例，A 和 D 建立 TCP 连接，A 和 B 之间链路的 MTU 是 1500 字节，B 和 C 之间链路的 MTU 是 1300 字节，C 和 D 之间链路的 MTU 是 1500 字节，为了使 TCP 传输性能达到最优，需要避免 TCP 报文在设备 B 和设备 C 上分片。

图 6-1



【注释】 A、B、C 和 D 为路由器。

功能部署

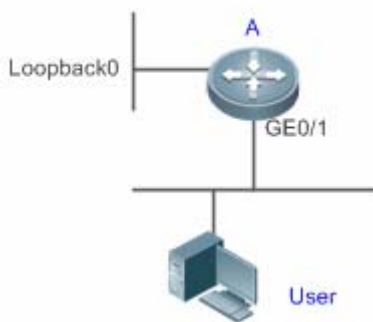
- 在 A 和 D 上开启 TCP 的路径 MTU 发现功能。

6.2.2 TCP连接异常检测

应用场景

以下图为例，用户远程登录到设备 A，用户异常关机，如果设备 A 等待 TCP 重传超时，会导致用户的 TCP 连接残留比较长的一段时间，可以利用 TCP 保活功能快速检测出用户的 TCP 连接异常。

图 6-2



【注释】 A 是路由器。

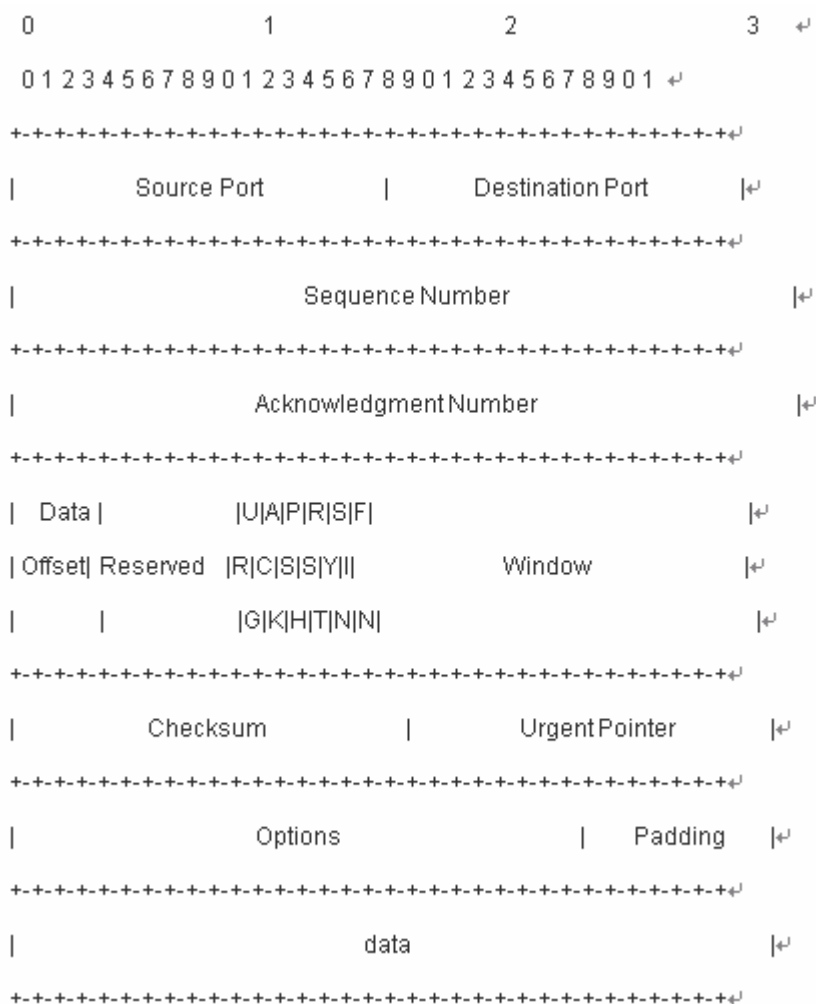
功能部署

- 在设备 A 上开启 TCP 保活功能。

6.3 功能详解

基本概念

TCP 首部格式



- Source Port 是源端口，16 位。
- Destination Port 是目的端口，16 位。
- Sequence Number 是序列号，32 位。

- Acknowledgment Number 是确认序列号，32 位。
- Data Offset 是数据偏移，4 位，该字段的值是 TCP 首部（包括选项）长度除以 4。
- 标志位：6 位，URG 表示 Urgent Pointer 字段有意义，ACK 表示 Acknowledgment Number 字段有意义，PSH 表示 Push 功能，RST 表示复位 TCP 连接，SYN 表示 SYN 报文（在建立 TCP 连接的时候使用），FIN 表示发送方没有数据需要发送了（在关闭 TCP 连接的时候使用）。
- Window 表示接收缓冲区的空闲空间，16 位，用来告诉 TCP 连接对端自己能够接收的最大数据长度。
- Checksum 是校验和，16 位。
- Urgent Pointers 是紧急指针，16 位，只有 URG 标志位被设置时该字段才有意义，表示紧急数据相对序列号（Sequence Number 字段的值）的偏移。

✚ TCP 三次握手

- TCP 三次握手的过程如下：
 - (1) 客户端发送 SYN 报文给服务器端。
 - (2) 服务器端收到 SYN 报文，回应一个 SYN ACK 报文。
 - (3) 客户端收到服务器端的 SYN 报文，回应一个 ACK 报文。
- 三次握手完成，TCP 客户端和服务器端成功地建立连接，可以开始传输数据了。

功能特性

功能特性	作用
配置SYN超时	配置 TCP 发送 SYN 报文或者 SYN ACK 报文后等待应答报文的超时
配置窗口大小	配置窗口大小
配置端口不可达时是否发送 reset 报文	配置在收到端口不可达的 TCP 报文时是否发送 reset 报文
配置MSS	配置 TCP 连接的 MSS
路径MTU发现功能	探测 TCP 传输路径上的最小 MTU，根据最小 MTU 调整发送的 TCP 报文的大小，避免分片
TCP保活功能	探测 TCP 连接对端是否还在正常工作

6.3.1 配置SYN超时

工作原理

建立 TCP 连接需要经过三次握手：发起方先发送 SYN 报文，响应方回应 SYN+ACK 报文，然后发起方再回应 ACK。

- 在发起方发送 SYN 报文后，如果响应方一直不回应 SYN+ACK 报文，发起方会不断的重传 SYN 报文直到超过一定的重传次数或超时时间。

- 在发起方发送 SYN 报文后，响应方回应 SYN+ACK 报文，但发起方不再回复 ACK，响应方也会一直重传直到超过一定的重传次数或超时时间。（SYN 报文攻击会出现这种情况。）

相关配置

设置 TCP SYN 超时时间

- TCP SYN 超时时间的缺省值是 20 秒。
- 用户可以在全局配置模式下使用“`ip tcp synwait-time seconds`”命令设置 SYN 超时时间，取值范围是 5 到 300，单位是秒。
- 如果网络中存在 SYN 攻击，减少 SYN 超时时间可以防止一些资源消耗，但对连续的 SYN 攻击达不到效果。在设备主动与外界请求建立连接时，减少 SYN 超时时间可以减少用户等待时间，如 telnet。如果网络比较差也可以适当增加超时时间。

6.3.2 配置窗口大小

工作原理

TCP 的接收缓冲区用来缓存从对端接收到的数据，这些数据后续会被应用程序读取。一般情况下，TCP 的窗口值反映接收缓冲区的空闲空间的大小。对于带宽比较大、有大量数据的连接，增大窗口可以显著提高 TCP 传输性能。

相关配置

设置窗口大小

- 用户可以在全局配置模式下使用“`ip tcp window-size size`”命令设置窗口大小，单位是字节，取值范围是 128 到(65535<<14)，缺省值是 65535。如果窗口大于 65535 字节，自动开启窗口扩大功能。
- 实际通告给对端的窗口大小是从配置的窗口大小和接收缓冲区的剩余空间取较小值。

6.3.3 配置端口不可达时是否发送 reset 报文

工作原理

TCP 协议在分发 TCP 报文给应用程序时，如果找不到该报文所属的 TCP 连接会主动回复一个 reset 报文以终止对端的 TCP 连接。攻击者可能利用大量的端口不可达的 TCP 报文对设备进行攻击。

相关配置

配置端口不可达时是否发送 reset 报文

收到端口不可达的 TCP 报文时，默认发送 reset 报文。

用户可以在全局配置模式下使用 “no ip tcp send-reset” 命令禁止发送 reset 报文。

如果允许发送 reset 报文，攻击者可能利用大量的端口不可达的 TCP 报文对设备进行攻击。

6.3.4 配置MSS

工作原理

最大分段大小 (Maximum Segment Size, MSS)，指一个 TCP 报文的数据载荷的最大长度，不包括 TCP 选项。

在 TCP 建立连接的三次握手中需要进行 MSS 协商，连接的双方都在 SYN 报文中增加 MSS 选项，其选项值表示本端最大能接收的段大小，即对端最大能发送的段大小。连接的双方取本端发送的 MSS 值和接收对端的 MSS 值的较小者作为本连接最大传输段大小。

- i** 实际生效的 MSS 是从根据 MTU 计算得到的 MSS 和用户配置的 MSS 取较小值。
- i** 如果该连接支持某些选项，那么 MSS 还要减去选项 4 字节对齐后的长度值。如 MD5 选项要减去 20 字节，MD5 选项长度 18 字节，对齐后 20 字节。

相关配置

设置 MSS

- 用户可以在全局配置模式下使用 “ip tcp mss max-segment-size” 命令设置 TCP 连接的 MSS，单位是字节，取值范围是 68 到 10000，默认使用根据 MTU 计算得到的 MSS。如果用户配置了 MSS，实际生效的 MSS 是从根据 MTU 计算得到的 MSS 和用户配置的 MSS 取较小值。
- MSS 太小会降低传输性能，增加 MSS 可以提高传输性能，但不是越大越好，选择 MSS 值可以参考接口的 MTU，如果 MSS 大于接口的 MTU，TCP 报文需要分片重组，会降低传输性能。

6.3.5 路径MTU发现功能

工作原理

RFC1191 规定的 TCP 连接的路径 MTU 发现功能，用来发现 TCP 报文传输路径的最小 MTU，避免分片重组，可以提高网络带宽的利用率。IPv4 TCP 路径 MTU 发现的过程如下：

- TCP 源端将发送的 TCP 报文的外层 IP 首部设置不可分片标志位。
- 如果 TCP 路径上某路由器的出口 MTU 值小于该 IP 报文长度，则会丢弃报文，并向 TCP 源端发送 ICMP 差错报文，报文中会携带该出口 MTU 值。

- (3) TCP 源端通过解析该 ICMP 差错报文，可知 TCP 路径上当前最小的 MTU 值，即路径 MTU。
- (4) 后续 TCP 源端发送数据段的长度不超过 MSS， $MSS = \text{路径 MTU} - \text{IP 头部长度} - \text{TCP 头部长度}$ 。

相关配置

▾ 启用路径 MTU 发现功能

TCP 缺省关闭路径 MTU 发现功能。

用户可以在全局配置模式下使用 “`ip tcp path-mtu-discovery`” 命令开启路径 MTU 发现功能。

6.3.6 TCP保活功能

工作原理

如果 TCP 希望知道对端是否还在正常工作，可以开启保活功能。当 TCP 对端在一段时间内（称为空闲时间）没有发送过报文给本端，本端开始发送保活报文，连续发送若干次，如果没有收到一个应答报文，就认为对端异常，关闭 TCP 连接。

相关配置

▾ 启用保活功能

- TCP 缺省关闭保活功能。
- 用户可以在全局配置模式下使用 “`ip tcp keepalive [interval num1] [times num2] [idle-period num3]`” 命令开启保活功能。interval 是时间间隔，默认值是 75 秒；times 是发送保活报文的最大次数，默认值是 6 次；idle-period 是空闲时间，默认值是 15 分钟。

 该命令不再区分服务器端和客户端，对所有的 TCP 连接都生效。

6.4 配置详解

配置项	配置建议 & 相关命令	
TCP性能优化	 可选配置，用于优化 TCP 连接的性能。	
	<code>ip tcp synwait-time</code>	配置建立 TCP 连接的超时时间。
	<code>ip tcp window-size</code>	配置 TCP 窗口大小。
	<code>ip tcp send-reset</code>	配置收到端口不可达的 TCP 报文时是否发送 reset 报文。
	<code>ip tcp mss</code>	配置 TCP 连接的 MSS。
	<code>ip tcp path-mtu-discovery</code>	开启路径 MTU 发现功能。

TCP连接异常检测	 可选配置，用于检测 TCP 对端是否正常工作。	
	<code>ip tcp keepalive</code>	开启 TCP 保活功能。

6.4.1 TCP性能优化

配置效果

- TCP 连接的传输性能达到最优，避免分片。

注意事项

-

配置方法

▾ 配置 SYN 超时

- 可选配置。
- 在 TCP 连接的两端配置。

▾ 配置 TCP 窗口大小

- 可选配置。
- 在 TCP 连接的两端配置。

▾ 配置端口不可达时是否发送 reset 报文

- 可选配置。
- 在 TCP 连接的两端配置。

▾ 配置 MSS

- 可选配置。
- 在 TCP 连接的两端配置。

▾ 配置 TCP 的路径 MTU 发现功能

- 可选配置。
- 在 TCP 连接的两端配置。

检验方法

相关命令

配置 SYN 超时

【命令格式】 **ip tcp synwait-time seconds**

【参数说明】 *seconds* : SYN 报文超时时间。单位为秒，取值范围是 5 到 300，缺省值是 20。

【命令模式】 全局模式

【使用指导】 如果网络中存在 SYN 攻击，减少 SYN 超时时间可以防止一些资源消耗，但对连续的 SYN 攻击达不到效果。在设备主动与外界请求建立连接时，减少 SYN 超时时间可以减少用户等待时间，如 telnet。如果网络比较差也可以适当增加超时时间。

配置 TCP 窗口大小

【命令格式】 **ip tcp window-size size**

【参数说明】 *size* : 单位是字节，取值范围是 128 到(65535 << 14)，缺省值是 65535。

【命令模式】 全局模式

【使用指导】 -

配置端口不可达时是否发送 reset 报文

【命令格式】 **ip tcp send-reset**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 收到端口不可达的 TCP 报文时，默认发送 reset 报文。

配置 MSS

【命令格式】 **ip tcp mss max-segment-size**

【参数说明】 *max-segment-size* : MSS 的上限值。单位为字节，取值范围是 68 到 10000，默认使用根据 MTU 计算得到的 MSS。

【命令模式】 全局模式

【使用指导】 **ip tcp mss** 的作用就是限制即将建立的 TCP 连接的 MSS 的最大值。任何新建立的连接协商的 MSS 值不能超过配置的值。如果要减小连接的最大 MSS 值，可以配置该命令，一般情况下不需要配置。

配置路径 MTU 发现功能

【命令格式】 **ip tcp path-mtu-discovery [age-timer minutes | age-timer infinite]**

【参数说明】 **age-timer minutes** : TCP 在发现路径 MTU 后，重新进行探测的时间间隔。单位是分钟，取值范围是 10 到 30。缺省值是 10。

age-timer infinite : TCP 在发现路径 MTU 后，不重新探测。

【命令模式】 全局模式

【使用指导】 TCP 的路径 MTU 发现功能是按 RFC1191 实现的，这个功能可以提高网络带宽的利用率。当用户使用 TCP 来批量传输大块数据时，该功能可以使传输性能得到明显提升。

按 RFC1191 的描述，TCP 在发现路径 MTU 后，隔一段时间可以使用更大的 MSS 来探测新的路径 MTU。这

个时间间隔就是使用参数 **age-timer** 来指定。当设备发现的路径 MTU 比 TCP 连接两端协商出来的 MSS 小时，设备就会按上述配置时间间隔，去尝试发现更大的路径 MTU。直到路径 MTU 达到 MSS 的值，或者用户停止这个定时器，这个探测过程才会停止。停止这个定时器，使用 **age-timer infinite** 参数。

配置举例

📌 开启 TCP 的路径 MTU 发现功能。

【配置方法】 在设备上开启 TCP 的路径 MTU 发现功能，重新探测的时间间隔取缺省值。

```
Ruijie# configure terminal
Ruijie(config)# ip tcp path-mtu-discovery
Ruijie(config)# end
```

【检验方法】 用户可以执行命令 **show tcp pmtu** 查看 IPv4 TCP 连接的路径 MTU。

```
Ruijie# show tcp pmtu
```

Number	Local Address	Foreign Address	PMTU
1	192.168.195.212.23	192.168.195.112.13560	1440

常见错误

6.4.2 TCP连接异常检测

配置效果

- TCP 探测对端是否还在正常工作。

注意事项

配置方法

📌 开启保活功能

- 可选配置。

检验方法

相关命令

▾ 开启保活功能

【命令格式】 **ip tcp keepalive [interval num1] [times num2] [idle-period num3]**

【参数说明】 **interval num1** : 发送保活报文的时间间隔, 单位是秒, 取值范围是 1 到 120, 缺省值是 75 秒。

times num2 : 发送保活报文的最大次数, 取值范围是 1 到 10, 缺省值是 6。

idle-period num3 : 空闲时间, 即对端没有向本端发送过报文的时间长度, 单位是秒, 取值范围是 60 到 1800, 缺省值是 15 分钟。

【命令模式】 全局模式

【使用指导】 如果 TCP 希望知道对端是否还在正常工作, 可以开启保活功能, 默认关闭。

假设用户开启保活功能, 时间间隔, 次数和空闲时间都使用缺省值, TCP 在 15 分钟内没有收到过对端发送的报文, 开始发送保活报文, 每隔 75 秒发送一次, 连续发送 6 次, 如果没有收到对方发送的任何 TCP 报文, 就认为 TCP 连接无效, 自动释放 TCP 连接。

配置举例

▾ 开启 TCP 保活功能。

【配置方法】 在设备上开启 TCP 保活功能, 空闲时间是 3 分钟, 发送保活报文的时间间隔是 60 秒, 如果连续发送 4 次保活报文, 没有收到对方发送的任何 TCP 报文, 就认为 TCP 连接无效。

```
Ruijie# configure terminal
Ruijie(config)# ip tcp keepalive interval 60 times 4 idle-period 180
Ruijie(config)# end
```

【检验方法】 用户远程登录到设备, 然后用户异常关机, 在设备上执行 `show tcp connect` 观察用户的 IPv4 TCP 连接被删除的时间。

常见错误

6.5 监视与维护

清除各类信息

查看运行情况

作用	命令
显示 IPv4 TCP 连接的基本信息	show tcp connect [local-ip <i>a.b.c.d</i>] [local-port <i>num</i>] [peer-ip <i>a.b.c.d</i>] [peer-port <i>num</i>]
显示 IPv4 TCP 连接的统计信息	show tcp connect statistics
显示 IPv4 TCP 路径 MTU 的信息	show tcp pmtu [local-ip <i>a.b.c.d</i>] [local-port <i>num</i>] [peer-ip <i>a.b.c.d</i>] [peer-port <i>num</i>]
显示 IPv4 TCP 端口使用情况	show tcp port [<i>num</i>]
显示 IPv4 TCP 参数信息	show tcp parameter
显示 IPv4 TCP 统计信息	show tcp statistics

查看调试信息

 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
查看 IPv4 TCP 报文的调试信息	debug ip tcp packet [in out] [local-ip <i>a.b.c.d</i>] [peer-ip <i>a.b.c.d</i>] [local-port <i>num</i>] [peer-port <i>num</i>] [deeply]
查看 IPv4 TCP 连接的调试信息	debug ip tcp transactions [local-ip <i>a.b.c.d</i>] [peer-ip <i>a.b.c.d</i>] [local-port <i>num</i>] [peer-port <i>num</i>]

7 软件 IPv4 快转

7.1 概述

在不支持硬件转发的产品上，由软件转发 IPv4 报文，为了使软件转发性能达到最优，我司实现了软件 IPv4 快转。

快转主要维护两张表：转发表和邻接表。转发表用来存放路由；邻接表用来存放下一跳的链路层信息，相当于 ARP 表。

快转可以主动解析下一跳，还可以实现流量负载均衡。

i 下文仅介绍软件 IPv4 的相关内容。

协议规范

7.2 典型应用

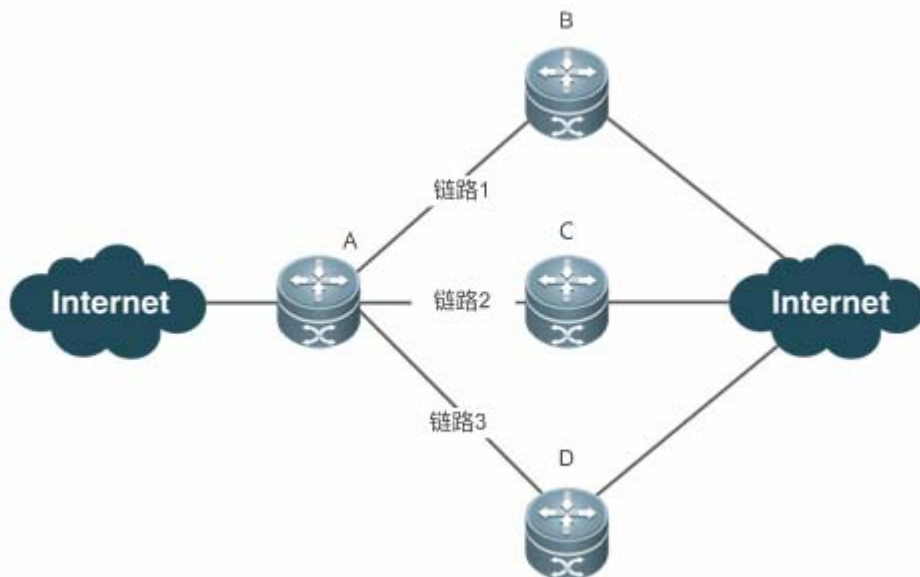
典型应用	场景描述
流量负载均衡	在网络路由中，当路由前缀关联到多个下一跳时，快转可以在多个下一跳中实现流量负载均衡。

7.2.1 流量负载均衡

应用场景

以下图为例，路由器 A 上，对于某条路由前缀关联 3 个下一跳，即链路 1、链路 2 和链路 3。缺省情况下，快转使用目的 IP 地址进行负载均衡，还可以根据源 IP 地址和目的 IP 地址进行负载均衡。

图 7-1



【注释】 A 为运行软件快转的路由器。
B、C、D 可以为其它转发设备。

功能部属

- 路由器 A 上运行软件快转。

7.3 功能详解

基本概念

IPv4 快转主要涉及以下基本概念：

📌 路由表

IPv4 路由表中存储着指向特定网络地址的路径，同时含有网络周边的拓扑信息。在报文转发的过程中 IPv4 快转根据路由表选择报文的传输路径。

📌 邻接节点

邻接节点包含了被路由报文的输出接口信息。例如下一跳列表、下一个处理部件、链路层输出封装等信息。当报文与该邻接节点匹配时，直接对报文进行封装，而后调用该节点的发送函数即可实现转发。为了便于检索和更新，邻接节点构成的表一般组织成哈希表的形式；为了支持路由负载均衡，邻接节点的下一条列表信息被组织为负载均衡表的形式；邻接节点中也可以不包含下一跳信息，也可以包含下一个处理部件的索引号（例如其它线卡，多业务卡）。

📌 主动解析

快转支持主动解析下一跳。对于以太网接口上的下一跳，如果不知道 MAC 地址，快转将主动解析下一跳。IPv4 快转请求 ARP 模块解析下一跳；。

↘ 报文转发路径

报文的路由转发是根据报文的 IPv4 地址，所以如果指定了报文源 IPv4 地址和目的 IPv4 地址，则该报文的转发路径将是确定的。

7.3.1 快转负载均衡策略

快转负载均衡就是利用多个网络设备通道均衡分担流量。

工作原理

快转支持报文的负载均衡处理，目前实现两种基于 IP 地址的负载均衡策略。在快转模型中，当路由前缀关联到多个下一跳时，即多径路由，该路由将关联到一个负载均衡表，并依路由权重实现负载均衡。当 IPv4 报文依最长前缀匹配到该均衡表时，快转根据报文的 IPv4 地址进行散列，选中其中的一条路径转发报文。

IPv4 快转支持两种负载均衡模式，分别是根据报文的源 IP 地址进行均衡、根据报文的源 IP 和目的 IP 地址进行均衡。

7.4 监视与维护

统计快转报文信息

快转报文统计信息即快转所处理的报文统计信息，包括了转发的报文数目，以及各种原因丢弃的报文数目等。快转提供配置信息查看和清除当前的统计信息，以供判断报文的转发行为是否和预期相同。

命令	作用
show ip ref packet statistics	显示 IPv4 快转当前的报文统计信息
clear ip ref packet statistics	清除 IPv4 快转当前的报文统计信息

查看邻接信息

用户可以通过以下命令来查看当前的邻接信息：

命令	作用
show ip ref adjacency [glean local ip-address {interface interface_type interface_number} discard statistics]	可以指定显示 IPv4 快转的集合邻接、本地邻接、指定 IP 对应邻接、指定接口关联邻接及所有邻接节点相关信息。

查看主动解析信息

用户可以通过以下命令来查看需要主动解析的下一跳：

命令	作用
show ip ref resolve-list	查看 IPv4 快转主动解析的下一跳。

查看报文转发路径信息

报文的路由转发是根据报文的 IPv4 地址，所以如果指定了报文源 IPv4 地址和目的 IPv4 地址，则该报文的转发路径将是确定的。执行下面的命令，并指定报文的源 IPv4 地址与目的 IPv4 地址，将会显示该报文的实际转发路径，比如报文丢弃、提交 CPU 或转发，进一步还可以知道从哪个接口转发等等。

命令	作用
show ip ref exact-route <i>source-ipaddress</i> <i>dest_ipaddress</i>	显示某特定报文的实际转发路径。

查看快转表路由信息

通过下面的命令可以查看快转表的路由信息：

命令	作用
show ip ref route [default <i>{ip mask}</i>] statistics]	显示当前 IPv4 快转表中的路由信息，参数 default 表示显示缺省路由。



配置指南-安全

本分册介绍安全配置指南相关内容，包括以下章节：

1. AAA
2. STORM CONTROL
3. PASSWORD-POLICY
4. CPP
5. DHCP Snooping

1 AAA

1.1 概述

AAA 是 Authentication Authorization and Accounting (认证、授权和记账) 的简称，它提供了对认证、授权和记账功能进行配置的一致性框架，锐捷网络设备产品支持使用 AAA。

AAA 以模块方式提供以下服务：

认证：验证用户是否可获得访问权，可选择使用 RADIUS 协议、TACACS+协议或 Local (本地) 等。身份认证是在允许用户访问网络和网络服务之前对其身份进行识别的一种方法。

授权：授权用户可使用哪些服务。AAA 授权通过定义一系列的属性对来实现，这些属性对描述了用户被授权执行的操作。这些属性对可以存放在网络设备上，也可以远程存放在安全服务器上。

记账：记录用户使用网络资源的情况。当 AAA 记账被启用时，网络设备便开始以统计记录的方式向安全服务器发送用户使用网络资源的情况。每个记账记录都是以属性对的方式组成，并存放在安全服务器上，这些记录可以通过专门软件进行读取分析，从而实现对用户使用情况、网络资源的使用情况进行记账、统计、跟踪。

尽管 AAA 是最主要的访问控制方法，锐捷产品同时也提供了在 AAA 范围之外的简单控制访问，如本地用户名身份认证、线路密码身份认证等。不同之处在于它们提供对网络保护程度不一样，AAA 提供更高级别的安全保护。

使用 AAA 有以下优点：

- 灵活性和可控制性强
- 可扩充性
- 标准化认证
- 多个备用系统

协议规范

- 暂无相应规范

1.2 典型应用

典型应用	场景描述
无域环境下的认证、授权、记账	所有用户处于同一个域，进行认证、授权、记账
多域环境下的认证、授权、记账	处于不同域的用户，采用不同的方法进行认证、授权、记账

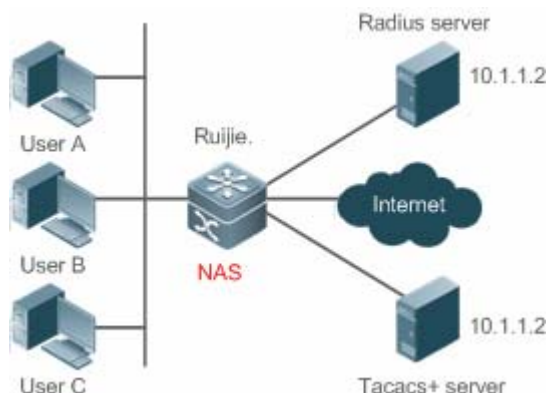
1.2.1 无域环境下的认证、授权、记账

应用场景

在图 1-1所示的网络应用中，为了更好地对网络访问控制器设备（NAS，以下简称网络设备）进行安全管理，需要满足如下应用要求：

1. 不同的管理人员有各自的用户账号，其用户名和口令不能共享，便于帐号管理和防止泄漏。
2. 对网络设备的访问需经过认证，用户认证的实现方式可以分为本地认证和集中认证，应采用集中认证和本地认证相结合的方式，集中认证为主用、本地认证为备用。在集中认证过程中，要求先通过 RADIUS 服务器认证，若无响应再转本地认证。
3. 在认证时，不同的用户可以被限制只能访问特定的网络设备。
4. 对用户进行分权限管理：把网络管理用户分为超级用户和普通用户。其中，超级用户对网络设备拥有查看和配置的权限，普通用户对网络设备只拥有特定的查看权限。
5. 服务器端可将用户的认证信息、授权信息和网络行为记录在服务器中，以供日后查看和审计（本例采用 TACACS+进行记账）。

图 1-1



【注释】 UserA，UserB，UserC 直接或者通过网络和 NAS 相连接。

NAS 通常为接入交换机或者汇聚交换机。

RADIUS 服务器可以是 Windows 2000/2003 Server（IAS）、UNIX 系统所带组件，也可以是一些厂商提供的专用服务器软件。

TACACS+服务器可以是一些厂商提供的专用的服务器软件。

功能部属

- 在 NAS 上启用 AAA
- 在 NAS 上配置安全服务器
- 在 NAS 上配置本地用户

- 在 NAS 上配置认证
- 在 NAS 上配置授权
- 在 NAS 上配置记账

1.3 功能详解

基本概念

本地认证、远程服务器认证

对用户进行认证时，如果使用 NAS 上的用户数据库进行密码校验，就称为本地认证。

对用户进行认证时，如果使用远程服务器上的用户数据库进行密码校验，就称为远程服务器认证。目前，远程服务器认证主要是 RADIUS 服务器认证和 TACACA+服务器认证。

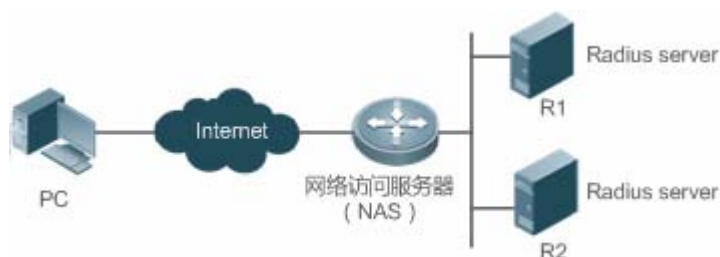
方法列表

由于对用户进行认证、授权和记账可以使用不同的安全方法，您需要使用方法列表定义一个使用不同方法对用户进行认证、授权和记账的前后顺序。方法列表可以定义一个或多个安全协议，这样可以确保在第一个方法失败时，有备用系统可用。锐捷产品使用方法列表中列出的第一个方法时，如果该方法无应答，则选择方法列表中的下一个方法。这个过程一直持续下去，直到与列出的某种安全方法成功地实现通信或用完方法列表。如果用完方法列表而还没有成功实现通信，则该安全功能宣告失败。

方法列表仅是定义将要被依次查询的、并用于认证用户身份的一系列安全方法。方法列表使您能够指定一个或多个用于身份认证的安全协议，这样确保在第一种方法失败的情况下，可以使用身份认证备份系统。我司产品使用第一种方法认证用户的身份，如果该方法无应答，将选择方法列表中的下一种方法。这个过程一直持续下去，直到与列出的某种身份认证方法成功地实现通信或用完方法列表。如果用完方法列表而还没有成功实现通信，则身份认证宣告失败。

⚠ 只有在前一种方法没有应答的情况下，锐捷产品才会尝试下一种方法。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 1-2



上图说明了一个典型的 AAA 网络配置，包含两台安全服务器：R1 和 R2 是 RADIUS 服务器。以及一台网络访问服务器（NAS），可以作为 RADIUS 客户端。

假设系统管理员已定义了一个方法列表，在这个列表中，R1 首先被用来获取身份信息，然后是 R2，最后是访问服务器上的本地用户名数据库。如果一个远程 PC 用户试图拨号进入网络，网络访问服务器首先向 R1 查询身份认证信息，假如用户通过了 R1 的身份认证，R1 将向网络访问服务器发出一个 ACCEPT 应答，这样用户即获准访问网络。如果 R1 返回的是 REJECT 应

答，则拒绝用户访问网络，断开连接。如果 R1 无应答，网络访问服务器就将它看作 TIMEOUT，并向 R2 查询身份认证信息。这个过程会一直在余下的指定方法中持续下去，直到用户通过身份认证、被拒绝或对话被中止。如果所有的方法返回 TIMEOUT，则认证失败，连接将被断开。

- ❗ REJECT 应答不同于 TIMEOUT 应答。REJECT 意味着用户不符合可用身份认证数据库中包含的标准，从而未能通过身份认证，访问请求被拒绝。TIMEOUT 则意味着安全服务器对身份认证查询未作应答，当检测到一个 TIMEOUT 时，AAA 选择身份认证方法列表中定义的下一个身份认证方法将继续进行身份认证过程。
- ❗ 在本文中，与 AAA 安全服务器相关的认证、授权和记账配置，均以 RADIUS 为例，而与 TACACS+ 有关的内容请另外参考“配置 TACACS+”。

AAA 服务器组

定义一个 AAA 服务器组，用于把一个或几个同一类型的服务器划分为同一组。配置方法列表时，引用该服务器组，则使用该方法列表进行认证、授权、记账操作时，首先向被引用服务器组中的服务器发起请求。

功能特性

功能特性	作用
AAA 认证	验证是否允许用户接入网络
AAA 授权	定义用户可以使用哪些服务或拥有哪些权限
AAA 记账	记录用户使用网络资源的情况

1.3.1 AAA 认证

在 AAA 中，认证、授权和计费是三个独立的业务过程。认证是用来验证用户是否可以获得访问权，其职责是完成各接入或服务请求的用户名、密码和用户信息的交互认证过程。在 AAA 中，可以只使用认证，而不使用授权或计费。

- ❗ 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。

AAA 认证方案：

- 不认证 (none)

对用户非常信任，不对其进行合法性检查。一般情况下不采用这种方法。

- 本地认证 (local)

认证过程在 NAS 设备上完成，用户信息（包括用户名、密码和各种属性）直接配置在接入设备上。当配置 local 参数使用本地数据库进行验证时，需要使用 username password 命令预先在本地创建用户数据库。

- 远程服务器组认证 (group)

认证过程在 NAS 和一个远程服务器组之间完成（一个服务器组可包含任意个相同类型的服务器），NAS 和远程服务器之间通过 RADIUS 或 TACACS+ 协议通信。用户信息集中在远程服务器上统一管理，可以实现大容量、高可靠性、支持多设备的集中式统一认证。为提防远程服务器组的服务器均无效时，可配置本地认证作为备选认证方式完成认证。

AAA 认证类型

锐捷产品目前支持以下认证类型：

- Login (登录) 认证

针对 SSH、Telnet、FTP 等终端接入用户，在用户登录到 NAS 命令行界面时进行身份认证。

- Enable 认证

针对的是用户终端登录到 NAS 上的命令行界面以后，提升命令行界面执行权限时进行认证。即对 enable (进入特权模式) 行为进行认证。

相关配置

启动 AAA

缺省情况下，AAA 没有启动。

使用 `aaa new-model` 命令可以启动。

配置 AAA 认证方案

缺省情况下，没有配置任何 AAA 认证方案。

确定使用本地 (Local) 认证还是远程服务器认证。如果用户使用远程服务器认证，则需要先配置 RADIUS 或 TACACS+ 服务器。如果使用 Local 认证，则需要在 NAS 上配置本地用户数据库信息。

配置 AAA 认证方法

缺省情况下，没有配置任何 AAA 认证方法。

确定要配置的接入方式，针对不同接入方式配置不同的认证方法。

1.3.2 AAA 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。

AAA 授权方案

- 直接授权 (none)

对用户非常信任，直接授权用户的权限为接入设备允许用户所使用的默认权限。

- 本地授权 (local)

授权过程在 NAS 设备上完成，根据 NAS 上为本地用户配置的相关属性进行授权。

- 远程服务器授权 (group)

授权过程在 NAS 和远程服务器组之间完成。当远程服务器组的服务器均无效时，可以配置本地授权或直接授权作为备选授权方式完成授权。

AAA 授权类型

- 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）。

- Config-commands 授权

对配置模式（包括全局配置模式及其子模式）下的命令进行授权。

- Console 授权

对通过控制台登录的用户所执行命令的授权。

- Command（命令）授权

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。

- Network（网络）授权

授予网络连接上的用户会话可用的服务。例如 PPP、SLIP 等网络连接接通过 Network 授权，可以获得诸如流量、带宽、超时等服务配置。

相关配置

启动 AAA

缺省情况下，AAA 没有启动。

使用 `aaa new-model` 命令可以启动。

配置 AAA 授权方案

缺省情况下，没有配置任何 AAA 授权方案。

确定使用本地（local）授权还是远程服务器授权。如果用户使用远程服务器授权，则需要先配置 RADIUS 或 TACACS+ 服务器。如果使用 Local 授权，则需要 NAS 上配置本地用户数据库信息。

配置 AAA 授权方法

缺省情况下，没有配置任何 AAA 授权方法。

确定要配置的接入方式，针对不同接入方式配置不同的认证方法。

1.3.3 AAA 记账

在 AAA 中，记账是一个和认证、授权同级别的独立流程，其职责为发送记账开始、更新和结束请求给所配置的记账服务器，由服务器记录用户使用网络资源的情况，实现对用户的活动进行计费、审计以及跟踪等功能。

在 AAA 配置中，记账方案不是必须配置的。

AAA 记账方案

- 不记账 (none)

不对用户记账。

- 本地记账 (local)

记账过程在 NAS 上完成，实现了本地用户连接数的统计和限制，并没有实际的费用统计功能。

- 远程服务器组记账 (group)

记账过程在接入设备和远程的服务器之间完成。当远程服务器组失效时，可配置本地记账作为备选记账方式完成记账。

AAA 记账类型

- Exec 记账

针对的是用户终端登录到 NAS 上的 CLI 界面时，在登入和登出时分别进行记账。

- Command 记账

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。

- Network 记账

记录与网络连接用户会话有关的信息。

相关配置

启动 AAA

缺省情况下，AAA 没有启动。

使用 `aaa new-model` 命令可以启动。

配置 AAA 记账方案

缺省情况下，没有配置任何 AAA 记账方案。

确定使用本地 (Local) 记账还是远程服务器记账。如果用户使用远程服务器记账，则需要先配置 RADIUS 或 TACACS+ 服务器。如果使用 Local 记账，则需要先在 NAS 上配置本地用户数据库信息。




配置 AAA 记账方法

缺省情况下，没有配置任何 AAA 记账方案。

确定要配置的接入方式，针对不同接入方式配置不同的记账方法。

1.4 配置详解

配置项	配置建议 & 相关命令
配置AAA认证	 如果要确认用户的身份，则必须配置。

	aaa new-model	开启 AAA。
	aaa authentication login	定义 Login 认证的认证方法列表。
	aaa authentication enable	定义 enable 认证的方法类型和执行顺序。
	login authentication	在特定终端线路上应用 Login 认证方法。
	aaa local authentication attempts	设置 login 用户尝试登录次数的最大值。
	aaa local authentication lockout-time	设置 login 用户被锁定的时间长度。
配置AAA授权	 如果要对不同用户赋予不同的权限，限制用户可以使用的服务，则必须配置。	
	aaa new-model	开启 AAA。
	aaa authorization exec	定义 exec 授权的方法类型和执行顺序。
	aaa authorization commands	定义 command 授权的方法类型和执行顺序。
	aaa authorization network	为接入用户配置授权方法列表。
	authorization exec	在特定终端线路上应用 exec 授权方法。
	authorization commands	在特定终端线路上应用 command 授权方法。
配置AAA记账	 如果要实现对用户使用网络资源情况的记账、统计和跟踪，则必须配置。	
	aaa new-model	开启 AAA。
	aaa accounting exec	定义 exec 记账的方法类型及方法执行顺序。
	aaa accounting commands	定义 command 记账的方法类型及方法执行顺序。
	accounting exec	在特定终端线路上应用 exec 记账方法。
	accounting commands	在特定终端线路上应用 command 记账方法。
	aaa accounting update	开启记账更新功能。
aaa accounting update periodic	设置记账更新时间间隔。	
配置AAA服务器组	 如果有多台服务器且需要能灵活选择服务器进行认证、授权和记账的处理，则建议配置。	
	aaa group server	创建 AAA 自定义服务器组。
	server	添加 AAA 服务器组成员。

1.4.1 配置 AAA 认证

配置效果

验证用户是否可以获得访问权。

注意事项

- 如果在一个认证方案中使用多种认证方法，则认证方法的执行顺序为配置的先后顺序。只有在当前认证方法没有响应的情况下，才会采用下一种认证方法；如果当前认证方法认证失败，则不会跳转到下一个认证方案进行认证。

- 由于 none 方法使得请求接入的任何用户在所有认证方法都没有应答情况下能通过身份认证，所以仅将它作为备用的身份认证方法。

i 一般情况下，不要使用 none 身份认证。在特殊情况（如所有可能的申请接入用户都是可信任的，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。

- AAA 认证开启的情况下，如果没有配置任何方法且不存在 default 认证方法时，对于控制台允许不认证直接登录；其他接入都要进行 local 认证。
- 如果进入 CLI 界面的时候经过了 Login 身份认证（none 方法除外），将记录当前使用的用户名。此时，进行 Enable 认证的时候，将不再提示输入用户名，直接使用与 Login 认证相同的用户名进行认证，注意输入的口令要与之匹配。
- 如果进入 CLI 界面的时候没有进行 Login 认证，或在 Login 认证的时候使用了 none 方法，将不会记录用户名信息。此时，如果进行 enable 认证，将会要求重新输入用户名。这个用户名信息不会被记录，每次进行 Enable 认证都要重新输入。

配置方法

▾ 开启 AAA

- 必须配置。
- 使用 `aaa new-model` 开启 AAA。
- 缺省情况下，没有启动 AAA。

▾ 定义 Login 认证的方法类型和执行顺序。

- 使用命令 `aaa authentication login` 配置 Login 认证的方法类型和执行顺序。
- 如果为 Login 接入用户配置认证方法列表（包括配置 default 方法列表），则必须配置此命令。
- 缺省情况下，没有配置 Login 认证方法列表。

▾ 定义 Enable 认证的方法类型和执行顺序。

- 使用命令 `aaa authentication enable` 配置 Enable 认证的方法类型和执行顺序。
- 如果为 Enable 过程配置认证方法列表（只能配置 default 方法列表），则必须配置此命令。
- 缺省情况下，没有配置 Enable 认证方法列表。

▾ 在特定终端线路上应用 Login 认证方法。

- 使用 `login authentication(line 模式下)` 命令在特定终端线路上应用 Login 认证方法。
- 如果要在特定线路上应用指定的 Login 认证方法列表，则必须配置此命令。
- 缺省情况下，所有终端线路关联 default 方法列表。

▾ 设置 login 用户尝试登录次数的最大值。

- 可选配置。

- 缺省情况下，允许 login 用户尝试密码的失败次数为 3 次。

📌 设置 login 用户被锁定的时间长度。

- 可选配置。
- 缺省情况下，当 login 用户尝试登录的次数超过最大值，被锁定的时间为 15 分钟。

检验方法

- 使用 show aaa method-list 查看已配置的方法列表信息。
- 使用 show aaa lockout 查看用户尝试登录失败次数的最大值和用户锁定的时间长度的配置信息。
- 使用 show running-config 查看 Login 认证关联认证方法列表的信息。

相关命令

📌 开启 AAA

【命令格式】 **aaa new-model**

【参数说明】 无

【命令模式】 全局模式

【使用指导】 该命令是 AAA 的使能命令，如果您要使用 AAA 安全服务，就必须使用 **aaa new-model** 使能 AAA 安全服务。如果没有启用 AAA，则所有 AAA 命令将是不可配置的。

📌 定义 Login 认证的方法类型和执行顺序。

【命令格式】 **aaa authentication login { default | list-name } method1 [method2...]**

【参数说明】 **default**：使用该参数，则后面定义的方法列表作为 Login 认证的默认方法。

list-name：定义一个 Login 认证的方法列表，可以是任何字符串。

method：必须是“local、none、group”所列关键字之一，一个方法列表最多有 4 个方法。

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：使用服务器组进行身份认证，目前支持 RADIUS 和 TACACS+服务器组。

【命令模式】 全局模式

【使用指导】 如果设备启用 AAA 登录认证安全服务，用户就必须使用 AAA 进行 Login 认证协商。您必须使用 **aaa authentication login** 命令配置默认的或可选的方法列表用于 Login 认证。

只有前面的方法没有响应，才能使用后面的方法进行身份认证。

设置了 Login 认证方法后，必须将其应用在需要进行 Login 认证的终端线路上，否则将不生效。

📌 定义 Enable 认证的方法类型和执行顺序

【命令格式】 **aaa authentication enable default method1 [method2...]**

【参数说明】 **default**：使用该参数，则后面定义的方法列表作为 Enable 认证的默认方法。

list-name：定义一个 Enable 认证的方法列表，可以是任何字符串。

method：必须是“enable、local、none、group”所列关键字之一，一个方法列表最多有 4 个方法。

enable : 使用 enable 命令配置的密码进行认证。

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 : 使用服务器组进行身份认证，目前支持 RADIUS 和 TACACS+服务器组。

【命令模式】 全局模式

【使用指导】 如果设备启用 AAA 登录认证安全服务，用户就必须使用 AAA 进行 Enable 认证协商。您必须使用 **aaa authentication enable** 命令配置默认的或可选的方法列表用于 Enable 认证。只有前面的方法没有响应，才能使用后面的方法进行身份认证。

设置 login 用户尝试登录次数的最大值。

【命令格式】 **aaa local authentication attempts max-attempts**

【参数说明】 *max-attempts* : 最大尝试失败次数，取值范围 1~2147483647

【命令模式】 全局模式

【使用指导】 该命令配置 Login 登录用户尝试登录失败次数。

设置 login 用户被锁定的时间长度。

【命令格式】 **aaa local authentication lockout-time lockout-time**

【参数说明】 *lockout-time* : 锁定时间（单位：分钟），取值范围 1~2147483647

【命令模式】 全局模式

【使用指导】 配置 Login 登录用户尝试超过配置登录失败次数后被锁定的时间长度。

配置举例

i 以下配置举例，仅介绍与 AAA 认证相关的配置。

AAA Login 认证配置示例。对 Login 用户先用 RADIUS 服务器进行认证，在远程服务器没有响应的情况下转本地认证。

【网络环境】

图 1-3



【配置方法】 第一步：开启 AAA。

第二步：如果用户使用远程服务器认证，则需要先配置 RADIUS 或 TACACS+服务器。如果使用 Local 认证，则需要在 NAS 上配置本地用户数据库信息。（本例需要配置 RADIUS 服务器和本地数据库信息）

第三步：根据不同接入用户类型（本例为 Login 用户），配置 AAA 认证方法列表（本例的认证方法是先 RADIUS 认证，无响应后转 Local 认证）。

第四步：将方法应用于某个特定的接口或线路。如果使用的是 default 认证方法，则可以不必配置该步骤。

NAS

```

Ruijie#configure terminal
Ruijie(config)#username user password pass
Ruijie(config)#aaa new-model
Ruijie(config)#radius-server host 10.1.1.1
  
```

```
Ruijie(config)#radius-server key ruijie
Ruijie(config)#aaa authentication login list1 group radius local
Ruijie(config)#line vty 0 20
Ruijie(config-line)#login authentication list1
Ruijie(config-line)#exit
```

【检验方法】 在 NAS 设备上，通过 **show aaa method-list** 命令查看配置效果。

NAS

```
Ruijie#show aaa method-list

Authentication method-list:
aaa authentication login list1 group radius local

Accounting method-list:

Authorization method-list:
```

以 Telnet 用户为例，用户远程登录到 NAS 设备上，CLI 界面提示输入用户名/密码。
输入正确的用户名/密码，才能访问设备。

User

```
User Access Verification

Username:user
Password:pass
```

📌 **AAA enable 认证配置示例。** 对 enable 认证先使用 RADIUS 服务器进行认证，在远程服务器没有响应的情况下转本地认证，在本地认证用户名不存在的情况下转 enable 密码认证。

【网络环境】

图 1-4



【配置方法】

第一步：开启 AAA。

第二步：如果用户使用远程服务器认证，则需要先配置 RADIUS 或 TACACS+服务器。如果使用 Local 认证，则需要 NAS 上配置本地用户数据库信息。如果使用 enable 密码认证，则需要 NAS 上配置 enable 认证密码。

第三步：根据不同接入用户类型，配置 AAA 认证方法列表。

i Enable 认证方法列表全局只能定义一个，因此 Enable 认证不需要定义方法列表的名称，只要配置成默认的方法列表，配置以后，会自动被应用。

NAS

```
Ruijie#configure terminal
Ruijie(config)#username user privilege 15 password pass
Ruijie(config)#enable secret w
Ruijie(config)#aaa new-model
```

```
Ruijie(config)#radius-server host 10.1.1.1
Ruijie(config)#radius-server key ruijie
Ruijie(config)#aaa authentication enable default group radius local enable
```

【检验方法】 在 NAS 设备上，通过 **show aaa method-list** 命令查看配置效果。

NAS

```
Ruijie#show aaa method-list

Authentication method-list:
aaa authentication enable default group radius local enable

Accounting method-list:

Authorization method-list:
```

用户级别切换到 15 级，CLI 提示认证。输入正确的用户名/密码，才能访问设备。

NAS

```
Ruijie>enable
Username:user
Password:pass
Ruijie#
```

常见错误

- 没有配置 RADIUS 服务器或者 TACACS+服务器。
- 没有配置本地数据库用户名和密码。

1.4.2 配置 AAA 授权

配置效果

- 定义用户可以使用哪些服务或拥有哪些权限。

注意事项

- 关于 Exec 授权：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。
- 关于授权方法：如果在一个授权方案中使用多种授权模式，则授权模式的执行顺序为配置的先后顺序。只有在当前授权模式没有响应的情况下，才会采用下一种授权模式；如果当前授权模式失败，则不会采用下一种授权模式进行授权。
- 关于 Command 授权：Command 授权功能目前仅 TACACS+协议支持。

- 关于 Console 授权：RGOS 支持区分通过控制台登录和其他终端登录的用户，可以设置控制台登录的用户，是否需要进行命令授权。如果关闭了控制台的命令授权功能，则已经应用到控制台线路的命令授权方法列表将不生效。

配置方法

▾ 开启 AAA

- 必须配置。
- 使用 **aaa new-model** 开启 AAA。
- 缺省情况下，没有启动 AAA。

▾ 定义 exec 授权的方法类型和执行顺序。

- 使用 **aaa authorization exec** 命令配置 exec 授权的方法类型和执行顺序。
- 如果要为 exec 用户配置授权方法列表（包括配置 default 方法列表），则必须配置此命令。
- 缺省情况下，没有配置授权方法。

i Exec 用户（控制台用户，可以通过 Console 口或者 Telnet 连接设备，每个连接称为一个 EXEC 用户，如 Telnet 用户、SSH 用户）的默认级别为最低权限的访问级别。

▾ 定义 command 授权的方法类型和执行顺序。

- 使用 **aaa authorization commands** 命令配置 command 授权的方法类型和执行顺序。
- 如果要为 command 授权配置授权方法列表（包括配置 default 方法列表），则必须配置此命令。
- 缺省情况下，没有配置授权方法。

▾ 为接入用户配置授权方法列表。

- 使用 **aaa authorization network** 命令为接入用户配置认证方法列表。
- 如果要为 network 用户配置授权列表（包括配置 default 方法列表），则必须配置此命令。
- 缺省情况下，没有配置授权方法。

▾ 在特定终端线路上应用 exec 授权方法。

- 使用 **authorization exec** (line 模式下)命令为特定终端线路上应用 exec 授权方法。
- 如果要在特定线路上应用指定的 exec 授权方法列表，则必须配置此命令。
- 缺省情况下，所有终端线路关联 default 授权方法列表。

▾ 在特定终端线路上应用 command 授权方法。

- 使用 **authorization commands** (line 模式下)命令为特定终端线路上应用 command 授权方法。
- 如果要在特定线路上应用指定的 command 授权方法列表，则必须配置此命令。
- 缺省情况下，所有终端线路关联 default 授权方法列表。

✎ 开启需要对配置模式下的命令进行授权。

- 使用 **aaa authorization config-commands** 命令开启需要对配置模式下的命令进行授权的功能。
- 缺省情况下，对配置模式下的命令不开启授权功能。

✎ 开启对控制台的用户执行的命令进行授权。

- 使用 **aaa authorization console** 命令开启对控制台的用户执行的命令进行授权的功能。
- 缺省情况下，不开启对控制台的用户执行的命令进行授权的功能。

检验方法

使用 **show running-config** 命令查看以上配置是否生效。

相关命令

✎ 开启 AAA。

【命令格式】 **aaa new-model**

【参数说明】 无

【命令模式】 全局模式

【使用指导】 该命令是 AAA 的使能命令，如果您要使用 AAA 安全服务，就必须使用 **aaa new-model** 使能 AAA 安全服务。如果没有启用 AAA，则所有 AAA 命令将是不可配置的。

✎ 定义 exec 授权的方法类型和执行顺序。

【命令格式】 **aaa authorization exec { default | list-name } method1 [method2...]**

【参数说明】 **default**：使用该参数，则后面定义的方法列表作为 exec 授权的默认方法。

list-name：定义一个 exec 授权的方法列表，可以是任何字符串。

method：必须是“local、none、group”所列关键字之一，一个方法列表最多有 4 个方法。

local：使用本地用户名数据库进行 exec 授权。

none：不进行 exec 授权。

group：使用服务器组进行 exec 授权，目前支持 RADIUS 和 TACACS+服务器组。

【命令模式】 全局模式

【使用指导】 RGOS 支持对登录到 NAS 的 CLI 界面的用户进行授权，赋予其 CLI 权限级别（0~15 级）。目前对于通过了 Login 认证的用户，才进行 Exec 授权。如果 Exec 授权失败，则无法进入 CLI 界面。配置了 Exec 授权方法后，必须将其应用在需要进行 Exec 授权的终端线路上，否则将不生效。

✎ 定义 command 授权的方法类型和执行顺序。

【命令格式】 **aaa authorization commands level { default | list-name } method1 [method2...]**

【参数说明】 **default**：使用该参数，则后面定义的方法列表作为 command 授权的默认方法。

list-name：定义一个 command 授权的方法列表，可以是任何字符串。

method：必须是“none、group”所列关键字之一，一个方法列表最多有 4 个方法。

none : 不进行 command 授权。

group : 使用服务器组进行 command 授权, 目前 TACACS+服务器组。

【命令模式】 全局模式

【使用指导】 RGOS 支持对用户可执行的命令进行授权, 当用户输入并试图执行某条命令时, AAA 将该命令发送到安全服务器上, 如果安全服务器允许执行该命令, 则该命令被执行, 否则该命令不执行, 并会给出执行命令被拒绝的提示。

配置命令授权的时候需要指定命令的级别, 这个级别是命令的默认级别 (例如, 某命令对于 14 级以上用户可见, 则该命令的默认级别就是 14 级的)。

配置了命令授权方法后, 必须将其应用在需要进行命令授权的终端线路上, 否则将不生效。

为接入用户配置授权方法列表。

【命令格式】 **aaa authorization network { default | list-name } method1 [method2...]**

【参数说明】 **default** : 使用该参数, 则后面定义的方法列表作为 network 授权的默认方法。

list-name : 定义一个 network 授权的方法列表, 可以是任何字符串。

method : 必须是 "none、group" 所列关键字之一, 一个方法列表最多有 4 个方法。

none : 不进行身份认证。

group : 使用服务器组进行 network 授权, 目前支持 RADIUS 和 TACACS+服务器组。

【命令模式】 全局模式

【使用指导】 RGOS 支持对所有网络有关的服务请求如 PPP、SLIP 等协议进行授权。如果配置了授权, 则对所有的认证用户或接口自动进行授权。

可以指定三种不同的授权方法, 与身份认证一样, 只有当前的授权方法没有响应, 才能继续使用后面的方法进行授权, 如果当前授权方法失败, 则不再使用其他后继的授权方法。

RADIUS 或 TACACS+服务器是通过返回一系列的属性来完成对认证用户的授权。所以网络授权是建立在认证的基础上的, 只有认证通过了才有可能获取网络授权。

开启对配置模式 (包括全局配置模式及其子模式) 下的命令进行授权的功能。

【命令格式】 **aaa authorization config-commands**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 如果只对非配置模式 (如特权模式) 下的命令进行授权, 可以使用该命令的 **no** 模式关闭配置模式的授权功能, 则配置模式及其子模式下的命令不需要进行命令授权就可以执行。

开启对通过控制台登录的用户所执行的命令进行授权的功能。

【命令格式】 **aaa authorization console**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 RGOS 支持区分通过控制台登录和其他终端登录的用户, 可以设置控制台登录的用户, 是否需要进行命令授权。如果关闭了控制台的命令授权功能, 则已经应用到控制台线路的命令授权方法列表将不生效。

配置举例

i 以下配置举例，仅介绍与 AAA 授权相关的配置。

配置 AAA exec 授权。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。

【网络环境】

图 1-5



【配置方法】

第一步：开启 AAA。

第二步：如果用户使用远程服务器授权，则需要先配置 RADIUS 或 TACACS+ 服务器。如果使用 local 授权，则需要先在 NAS 上配置本地用户数据库信息。

第三步：根据不同接入方式和服务类型，配置 AAA 授权方法列表。

第四步：将方法应用于某个特定的接口或线路。如果使用的是 default 认证方法，则可以不配置该步骤。

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。

NAS

```

Ruijie#configure terminal
Ruijie(config)#username user password pass
Ruijie(config)#username user privilege 6
Ruijie(config)#aaa new-model
Ruijie(config)#radius-server host 10.1.1.1
Ruijie(config)#radius-server key test
Ruijie(config)#aaa authentication login list1 group local
Ruijie(config)#aaa authorization exec list2 group radius local
Ruijie(config)#line vty 0 4
Ruijie(config-line)#login authentication list1
Ruijie(config-line)# authorization exec list2
Ruijie(config-line)#exit
  
```

【检验方法】

在 NAS 设备上，通过 **show run**、**show aaa method-list** 命令查看配置效果。

NAS

```

Ruijie#show aaa method-list

Authentication method-list:
aaa authentication login list1 group local

Accounting method-list:

Authorization method-list:
aaa authorization exec list2 group radius local

Ruijie# show running-config
aaa new-model
!
  
```

```

aaa authorization exec list2 group local
aaa authentication login list1 group radius local
!
username user password pass
username user privilege 6
!
radius-server host 10.1.1.1
radius-server key 7 093b100133
!
line con 0
line vty 0 4
  authorization exec list2
  login authentication list1
!
End

```

- ✎ **配置 Command 授权。为 Login 用户设置命令授权，应用 default 授权方法：对 15 级命令进行授权，先使用 tacacs+ 服务器授权，无响应后转 local 授权。授权同时应用于控制台登录用户和其他终端登录的用户。**

【网络环境】

图 1-6



【配置方法】

第一步：开启 AAA。

第二步：如果用户使用远程服务器授权，则需要先配置 RADIUS 或 TACACS+ 服务器。如果使用 local 授权，则需要先在 NAS 上配置本地用户数据库信息。

第三步：根据不同接入方式和服务类型，配置 AAA 授权方法列表。

第四步：将方法应用于某个特定的接口或线路。如果使用的是 default 认证方法，则可以不必配置该步骤。

NAS

```

Ruijie#configure terminal
Ruijie(config)#username user1 password pass1
Ruijie(config)#username user1 privilege 15
Ruijie(config)#aaa new-model
Ruijie(config)#tacacs-server host 192.168.217.10
Ruijie(config)#tacacs-server key aaa
Ruijie(config)#aaa authentication login default local
Ruijie(config)#aaa authorization commands 15 default group tacacs+ local
Ruijie(config)#aaa authorization console

```

【检验方法】

在 NAS 设备上，通过 **show run**、**show aaa method-list** 命令查看配置效果。

NAS

```

Ruijie#show aaa method-list

Authentication method-list:

```

```
aaa authentication login default local

Accounting method-list:

Authorization method-list:
aaa authorization commands 15 default group tacacs+ local

Ruijie#show run
!
aaa new-model
!
aaa authorization console
aaa authorization commands 15 default group tacacs+ local
aaa authentication login default local
!
!
nfpp
!
vlan 1
!
username user1 password 0 pass1
username user1 privilege 15
no service password-encryption
!
tacacs-server host 192.168.217.10
tacacs-server key aaa
!
line con 0
line vty 0 4
!
!
end
```

配置 Network 授权。

【网络环境】

图 1-7



【配置方法】

第一步：开启 AAA。

第二步：如果用户使用远程服务器授权，则需要先配置 RADIUS 或 TACACS+服务器。如果使用 local 授权，则需要先在 NAS 上配置本地用户数据库信息。

第三步：根据不同接入方式和服务类型，配置 AAA 授权方法列表。

第四步：将方法应用于某个特定的接口或线路。如果使用的是 default 认证方法，则可以不必配置该步骤。

NAS

```
Ruijie#configure terminal
Ruijie(config)#aaa new-model
Ruijie(config)#radius-server host 10.1.1.1
Ruijie(config)#radius-server key test
Ruijie(config)#aaa authorization network default group radius none
Ruijie(config)# end
```

【检验方法】 在 NAS 设备上，通过 **show aaa method-list** 命令查看配置效果。

NAS

```
Ruijie#show aaa method-list

Authentication method-list:

Accounting method-list:

Authorization method-list:
aaa authorization network default group radius none
```

常见配置错误

无

1.4.3 配置 AAA 记账

配置效果

- 记录用户使用网络资源的情况。
- 记录用户进行设备管理时登入登出的过程、记录执行过的命令。

注意事项

关于记账方法：

- 如果在一个记账方案中使用多种记账模式，则记账模式的执行顺序为配置的先后顺序。只有在当前记账模式没有响应的情况下，才会采用下一种记账模式；如果当前记账模式失败，则不会采用下一种记账模式进行记账。
- 默认的记账方法（default 方法）列表一旦配置，将自动应用到所有终端上。在线路上应用非默认记账方法列表，将取代默认的方法列表。如果试图应用未定义的方法列表，则会给出一个警告提示信息，该线路上的记账将不会生效，直至定义了该记账方法列表才会生效。

关于 Exec 记账：

- 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。

关于 Command 记账：

- Command 记账功能目前仅 TACACS+协议支持。

配置方法

▾ 开启 AAA。

- 必须配置。
- 使用 `aaa new-model` 开启 AAA。
- 缺省情况下，没有启动 AAA。

▾ 定义 exec 记账的方法类型及方法执行顺序。

- 使用命令 `aaa accounting exec` 配置 exec 记账的方法类型及方法执行顺序。
- 如果要为 exec 用户配置记账方法（包括配置 default 方法列表），则必须配置此命令。
- Exec 用户（控制台用户，可以通过 Console 口或者 Telnet 连接设备，每个连接称为一个 EXEC 用户，如 Telnet 用户、SSH 用户）的默认级别为最低权限的访问级别。
- 缺省情况下，没有配置记账方法。

▾ 定义 command 记账的方法类型及方法执行顺序。

- 使用命令 `aaa accounting commands` 配置 command 记账的方法类型及方法执行顺序。
- 如果要为 command 记账配置记账方法（包括配置 default 方法列表），则必须配置此命令。
- 缺省情况下，没有配置记账方法。命令记账功能目前仅 TACACS+协议支持。

▾ 在特定终端线路上应用 exec 记账方法。

- 使用命令 `accounting exec`(line 模式下)配置在特定终端线路上应用 exec 记账方法。
- 如果要在特定线路上应用指定的 exec 记账方法列表，则必须配置此命令。
- 如果应用的是 default 方法列表，则可不配置此命令。
- 缺省情况下，所有终端线路关联 default 方法列表。

▾ 在特定终端线路上应用 command 记账方法。

- 使用命令 `accounting commands`(line 模式下)配置在特定终端线路上应用 command 记账方法。
- 如果要在特定线路上应用指定的 command 记账方法列表，则必须配置此命令。
- 如果应用的是 default 方法列表，则可不配置此命令。
- 缺省情况下，所有终端线路关联 default 方法列表。

✎ 开启记账更新功能。

- 可选配置。
- 该功能有助于提高记账准确性，建议配置。
- 缺省情况下，记账更新功能关闭。

✎ 设置记账更新时间间隔。

- 可选配置。
- 除非有明确要求，否则不建议配置。

检验方法

使用 `show running-config` 命令查看配置是否生效。

相关命令

✎ 开启 AAA。

【命令格式】 `aaa new-model`

【参数说明】 无

【命令模式】 全局模式

【使用指导】 该命令是 AAA 的使能命令，如果您要使用 AAA 安全服务，就必须使用 `aaa new-model` 使能 AAA 安全服务。如果没有启用 AAA，则所有 AAA 命令将是不可配置的。

✎ 定义 exec 记账的方法类型及方法执行顺序。

【命令格式】 `aaa accounting exec { default | list-name } start-stop method1 [method2...]`

【参数说明】 **default**：使用该参数，则后面定义的方法列表作为 exec 记账的默认方法。

list-name：定义一个 exec 记账的方法列表，可以是任何字符串。

method：必须是“none、group”所列关键字之一，一个方法列表最多有 4 个方法。

none：不进行 exec 记账。

group：使用服务器组进行 exec 记账，目前支持 RADIUS 和 TACACS+服务器组。

【命令模式】 全局模式

【使用指导】 RGOS 只有在用户通过了登录认证后，才会启用 Exec 记账功能，如果用户登录时未进行认证或认证采用的方法为 none，则不会进行 Exec 记账。

启用记账功能后，在用户登录到 NAS 的 CLI 界面时候，发送记账开始（Start）信息给安全服务器，在用户退出登录的时候，发送记账结束（Stop）信息给安全服务器。如果一个用户在登录时没有发出 Start 信息，在退出登录时也不会发出 Stop 信息。

配置了 Exec 记账方法后，必须将其应用在需要进行命令记账的终端线路上，否则将不生效。

✎ 定义 command 记账的方法类型及方法执行顺序。

【命令格式】 `aaa accounting commands level { default | list-name } start-stop method1 [method2...]`

- 【参数说明】 *level* : 要进行记账的命令级别, 范围 0~15, 决定哪个级别的命令执行时, 需要记录信息。
default : 使用该参数, 则后面定义的方法列表作为 command 记账的默认方法。
list-name : 定义一个 command 记账的方法列表, 可以是任何字符串。
method : 必须是 “none、group” 所列关键字之一, 一个方法列表最多有 4 个方法。
none : 不进行 command 记账。
group : 使用服务器组进行 command 记账, 目前支持 TACACS+服务器组。
- 【命令模式】 全局模式
- 【使用指导】 RGOS 只有在用户通过了登录认证后, 才会启用命令记账功能, 如果用户登录时未进行认证或认证采用的方法为 none, 则不会进行命令记账。启用记账功能后, 在用户每次执行指定级别的命令后, 将所执行的命令信息, 发送给安全服务器。
 配置了命令记账方法后, 必须将其应用在需要进行命令记账的终端线路上, 否则将不生效。

✎ 开启记账更新功能。

- 【命令格式】 **aaa accounting update**
- 【参数说明】 无
- 【命令模式】 全局模式
- 【使用指导】 如果没有启用 AAA 安全服务, 则不能使用记账更新。如果已经启用 AAA 安全服务, 则该命令用设置记账更新功能。

✎ 设置记账更新时间间隔。

- 【命令格式】 **aaa accounting update periodic interval**
- 【参数说明】 *Interval* : 记账更新时间间隔, 以分钟为单位, 最小为 1 分钟。
- 【命令模式】 全局模式
- 【使用指导】 如果没有启用 AAA 安全服务, 则不能使用记账更新。如果已经启用 AAA 安全服务, 则该命令用设置记账更新时间间隔。

配置举例

i 以下配置举例, 仅介绍与 AAA 记账相关的配置。

✎ 配置 AAA exec 记账。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 记账。

【网络环境】

图 1-8



【配置方法】

- 第一步：开启 AAA。
- 第二步：如果用户使用远程服务器记账, 则需要先配置 RADIUS 或 TACACS+服务器。
- 第三步：根据不同接入方式和服务类型, 配置 AAA 记账方法列表。
- 第四步：将方法应用于某个特定的接口或线路。如果使用的是 default 认证方法, 则可以不必配置该步骤。

NAS

```
Ruijie#configure terminal
Ruijie(config)#username user password pass
Ruijie(config)#aaa new-model
Ruijie(config)#radius-server host 10.1.1.1
Ruijie(config)#radius-server key test
Ruijie(config)#aaa authentication login list1 group local
Ruijie(config)#aaa accounting exec list3 start-stop group radius
Ruijie(config)#line vty 0 4
Ruijie(config-line)#login authentication list1
Ruijie(config-line)# accounting exec list3
Ruijie(config-line)#exit
```

【检验方法】

在 NAS 设备上，通过 **show run**、**show aaa method-list** 命令查看配置效果。

NAS

```
Ruijie#show aaa method-list

Authentication method-list:
aaa authentication login list1 group local

Accounting method-list:
aaa accounting exec list3 start-stop group radius

Authorization method-list:

Ruijie# show running-config
aaa new-model
!
aaa accounting exec list3 start-stop group radius
aaa authentication login list1 group local
!
username user password pass
!
radius-server host 10.1.1.1
radius-server key 7 093b100133
!
line con 0
line vty 0 4
    accounting exec list3
    login authentication list1
!
End
```

📌 配置 command 记账。为 Login 用户设置命令记账，应用 default 记账方法。其中 Login 认证采用本地认证，使用 tacacs+ 服务器记账。

【网络环境】

图 1-9



【配置方法】

第一步：开启 AAA。

第二步：如果用户使用远程服务器记账，则需要先配置 RADIUS 或 TACACS+服务器。

第三步：根据不同接入方式和服务类型，配置 AAA 记账方法列表。

第四步：将方法应用于某个特定的接口或线路。如果使用的是 default 认证方法，则可以不必配置该步骤。

NAS

```

Ruijie#configure terminal
Ruijie(config)#username user1 password pass1
Ruijie(config)#username user1 privilege 15
Ruijie(config)#aaa new-model
Ruijie(config)#tacacs-server host 192.168.217.10
Ruijie(config)#tacacs-server key aaa
Ruijie(config)#aaa authentication login default local
Ruijie(config)#aaa accounting commands 15 default start-stop group tacacs+
  
```

【检验方法】

在 NAS 设备上，通过 show 命令查看配置效果。

NAS

```

Ruijie#show aaa method-list

Authentication method-list:
aaa authentication login default local

Accounting method-list:
aaa accounting commands 15 default start-stop group tacacs+
Authorization method-list:

Ruijie#show run
!
aaa new-model
!
aaa authorization config-commands
aaa accounting commands 15 default start-stop group tacacs+
aaa authentication login default local
!
!
nfpp
!
vlan 1
!
  
```

```
username user1 password 0 pass1
username user1 privilege 15
no service password-encryption
!
tacacs-server host 192.168.217.10
tacacs-server key aaa
!
line con 0
line vty 0 4
!
!
end
```

常见配置错误

无

1.4.4 配置 AAA 服务器组

配置效果

- 创建自定义服务器组，每个服务器组可添加一台或多台服务器。
- 配置认证、授权、记账方法列表时，引用服务器组的组名作为认证、授权、记账方法，则表示在进行认证、授权、记账请求时使用该服务器组中的服务器。
- 使用自定义服务器组可以实现认证、授权、记账相分离。

注意事项

在自定义服务器组中，只能指定并应用默认服务器组中的服务器。

配置方法

📌 创建 AAA 自定义服务器组。

- 必选配置
- 在创建自定义服务组名的时候，组名尽可能有明确的含义。不可以使用预定义的关键字“radius”和“tacacs+”。

📌 添加 AAA 服务器组成员。

- 必选配置

- 使用 `server` 命令添加 AAA 服务器组的成员。
- 缺省情况下，自定义组中没有添加服务器。

检验方法

使用命令 `show aaa group` 查看配置的服务器组信息。

相关命令

▾ 创建 AAA 自定义服务器组。

【命令格式】 `aaa group server {radius | tacacs+} name`

【参数说明】 `name`：服务器组的取名，目前不能为关键字“radius”，“tacacs+”，因为这是 RADIUS 和 TACACS+默认的服务器组名称。

【命令模式】 全局模式

【使用指导】 该命令配置 AAA 服务器组，目前支持 RADIUS 和 TACACS+服务器组。

▾ 添加 AAA 服务器组成员。

【命令格式】 `server ip-addr [auth-port port1] [acct-port port2]`

【参数说明】 `ip-addr`：服务器 ip 地址


`port1`：服务器认证端口（仅 RADIUS 服务器组支持）

`port2`：服务器记账端口（仅 RADIUS 服务器组支持）

【命令模式】 服务器组配置模式

【使用指导】 往指定服务器中添加服务器，不指定端口时使用默认值。

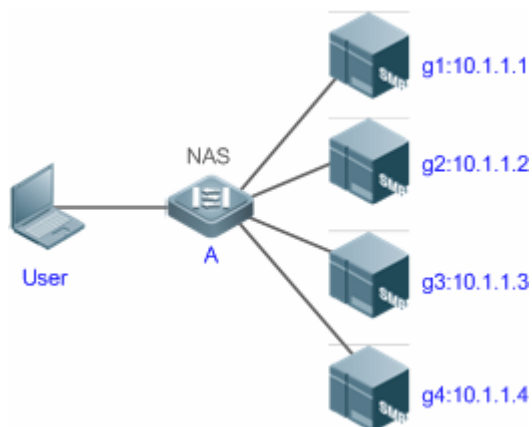
配置举例

 以下配置举例，仅介绍与 AAA 服务器组相关的配置。

- ▾ 创建 AAA 自定义服务器组。RADIUS 服务器组 g1、g2，其中 g1 组的服务器的 IP 为 10.1.1.1 和 10.1.1.2，g2 组的服务器的 IP 为 10.1.1.3 和 10.1.1.4。

【网络环境】

图 1-10



- 【前置任务】
- 1, 网络中已经完成了接口、IP 地址、Vlan 的配置, 网络连通, NAS 设备到服务器的路由可达。
 - 2, 启用 AAA 服务。

【配置方法】 第一步：配置服务器（该服务器属于默认服务器组）

第二步：创建 AAA 自定义服务器组

第三步：在自定义服务器组中添加服务器组成员

NAS

```
Ruijie#configure terminal
Ruijie(config)#radius-server host 10.1.1.1
Ruijie(config)#radius-server host 10.1.1.2
Ruijie(config)#radius-server host 10.1.1.3
Ruijie(config)#radius-server host 10.1.1.4
Ruijie(config)#radius-server key secret
Ruijie(config)#aaa group server radius g1
Ruijie(config-gs-radius)#server 10.1.1.1
Ruijie(config-gs-radius)#server 10.1.1.2
Ruijie(config-gs-radius)#exit
Ruijie(config)#aaa group server radius g2
Ruijie(config-gs-radius)#server 10.1.1.3
Ruijie(config-gs-radius)#server 10.1.1.4
Ruijie(config-gs-radius)#exit
```

【检验方法】 在 NAS 设备上，通过 **show aaa group**、**show run** 命令查看配置效果。

NAS

```
Ruijie#show aaa group
Type      Reference  Name
-----
radius    1         radius
tacacs+   1         tacacs+
radius    1         g1
radius    1         g2
```


```
Ruijie#show run
!
radius-server host 10.1.1.1
radius-server host 10.1.1.2
radius-server host 10.1.1.3
radius-server host 10.1.1.4
radius-server key secret
!
aaa group server radius g1
server 10.1.1.1
server 10.1.1.2
!
aaa group server radius g2
server 10.1.1.3
server 10.1.1.4
!
!
```

常见配置错误

- 对于使用非默认认证、记账端口的 radius 服务器，在使用命令 `server` 添加服务器时要同时指定认证端口或记账端口。

1.5 监视与维护

清除各类信息

 在设备运行过程中执行 `clear` 命令，可能因为重要信息丢失而导致业务中断。

作用	命令
清除被锁定的用户列表。	<code>clear aaa local user lockout {all user-name <i>username</i> }</code>

查看运行情况

作用	命令
显示记账更新相关的信息。	show aaa accounting update
显示当前 login 的锁定配置参数。	show aaa lockout
显示 AAA 配置的所有服务器组。	show aaa group
显示 AAA 所有的方法列表。	show aaa method-lis
显示 AAA 用户相关信息。	show aaa user

查看调试信息

无

2 STORM CONTROL

2.1 概述

当局域网中存在过量的广播、多播或未知名单播数据流时，就会导致网络变慢和报文传输超时机率大大增加。这种情况称之为局域网风暴。拓扑协议的执行错误或对网络的错误配置都有可能产生风暴。

用户可以分别针对广播、多播和未知名单播数据流进行风暴控制。当设备端口接收到的广播、多播或未知名单播数据流的速率超过所设定的带宽、每秒允许通过的报文数或者每秒允许通过的千比特数时，设备将只允许通过所设定带宽、每秒允许通过的报文数或者每秒允许通过的千比特数的数据流，超出限定范围部分的数据流将被丢弃，直到数据流恢复正常，从而避免过量的泛洪数据流进入局域网中形成风暴。

协议规范

无。

2.2 典型应用

典型应用	场景描述
网络防攻击	网络防攻击，开启风暴控制功能，防止泛洪

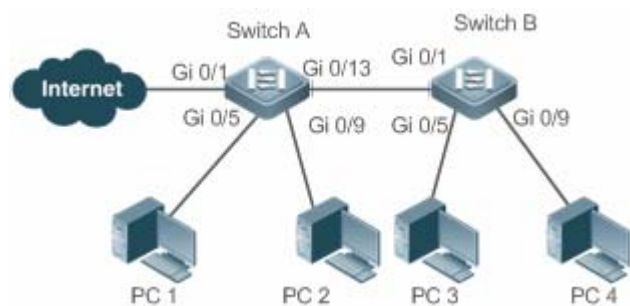
2.2.1 网络防攻击

应用场景

网络防攻击，应用需求如下：

- 防止设备受到广播、多播、未知名单播报文攻击。

图 2-1



【注释】 A、B 为接入设备

PC 1、PC 2、PC 3、PC 4 为台式机。

功能部属

- 所有接入设备（本例为 Switch A、Switch B）的端口上开启风暴控制功能。

2.3 功能详解

基本概念

▾ 风暴控制

当设备端口接收到的未知名单播数据流、组播数据流或者广播数据流的速率超过所设定的对应类型的报文数据流带宽、每秒允许通过的最大报文数或者每秒允许通过的最大千比特数时，设备将只允许通过所设定带宽、每秒最大报文数或者每秒最大千比特数的数据流，超出限定范围部分的数据流将被丢弃，直到数据流恢复正常。

▾ 基于带宽百分比的风暴控制

当设备端口接收到的数据流的速率超过所设定的带宽时，设备将只允许通过所设定带宽的数据流，超出带宽部分的数据流将被丢弃，直到数据流恢复正常。

▾ 基于每秒报文数限制的风暴控制

当设备端口接收到的数据流的速率超过所设定的每秒允许通过的最大报文数时，设备将只允许通过所设定每秒最大报文数的数据流，超出最大允许的每秒报文数部分的数据流将被丢弃，直到数据流恢复正常。

▾ 基于每秒千比特数限制的风暴控制

当设备端口接收到的数据流的速率超过所设定的每秒允许通过的最大每秒千比特数时，设备将只允许通过所设定每秒最大千比特数的数据流，超出最大允许的每秒千比特数部分的数据流将被丢弃，直到数据流恢复正常。

功能特性

功能特性	作用
单播报文风暴控制	开启单播报文风暴控制功能，可以实现对未知名单播报文的流量限制，防止泛洪
组播报文风暴控制	开启组播报文风暴控制功能，可以实现对组播报文的流量限制，防止泛洪
广播报文风暴控制	开启广播报文风暴控制功能，可以实现对广播报文的流量限制，防止泛洪

2.3.1 单播报文风暴控制

单播报文风暴控制功能用于监控设备端口接收到的未知名单播数据流的速率，以实现未知名单播报文在局域网中的流量限制，防止未知名单播报文数据流过大而出现泛洪现象。

工作原理

当设备端口接收到的未知名单播数据流的速率超过所设定的带宽、每秒允许通过的报文数或者每秒允许通过的千比特数时，设备将只允许通过所设定限定范围的未知名单播数据流，超出限定范围部分的未知名单播数据流将被丢弃，直到数据流恢复正常。

相关配置

启动接口上单播报文风暴控制之功能

缺省情况下，接口上的单播报文风暴控制功能关闭。

使用 `storm-control unicast [{ level percent | pps packets | rate-bps }]` 命令可以启动接口上的单播报文风暴控制功能。

使用 `no storm-control unicast` 或者 `default storm-control unicast` 命令可以关闭接口上的单播报文风暴控制功能。

命令默认参数由相关产品决定。

2.3.2 组播报文风暴控制

组播报文风暴控制功能用于监控设备端口接收到的组播数据流的速率，以实现组播报文在局域网中的流量限制，防止组播报文数据流过大而出现泛洪现象。

工作原理

当设备端口接收到的组播数据流的速率超过所设定的带宽、每秒允许通过的报文数或者每秒允许通过的千比特数时，设备将只允许通过所设定限定范围的组播数据流，超出限定范围部分的组播数据流将被丢弃，直到数据流恢复正常。

相关配置

启动接口上组播报文风暴控制之功能

缺省情况下，接口上的组播报文风暴控制功能关闭。

使用 `storm-control multicast [{ level percent | pps packets | rate-bps }]` 命令可以启动接口上的组播报文风暴控制功能。

使用 `no storm-control multicast` 或者 `default storm-control multicast` 命令可以关闭接口上的组播报文风暴控制功能。

命令默认参数由相关产品决定。

2.3.3 广播报文风暴控制

广播报文风暴控制功能用于监控设备端口接收到的广播数据流的速率，以实现广播报文在局域网中的流量限制，防止广播报文数据流过大而出现泛洪现象。

工作原理

当设备端口接收到的广播数据流的速率超过所设定的带宽、每秒允许通过的报文数或者每秒允许通过的千比特数时，设备将只允许通过所设定范围的广播数据流，超出限定范围部分的广播数据流将被丢弃，直到数据流恢复正常。

相关配置

启动接口上广播报文风暴控制之功能


缺省情况下，接口上的单播报文风暴控制功能关闭。

使用 **storm-control broadcast** [{ *level percent* | *pps packets* | *rate-bps* }] 命令可以启动接口上的广播报文风暴控制功能。

使用 **no storm-control broadcast** 或者 **default storm-control broadcast** 命令可以关闭接口上的广播报文风暴控制功能。

命令默认参数由相关产品决定。

2.4 配置详解

配置项	配置建议 & 相关命令
配置风暴控制基本功能	 必须配置。开启风暴控制
	<pre>storm-control { broadcast multicast unicast } [{ level percent pps packets rate-bps }]</pre> 启动风暴控制

2.4.1 配置风波控制基本功能

配置效果

- 可以基于广播、多播、单播开启风暴控制功能，功能开启之后可以实现对广播、组播、未知名单播报文进行风暴控制，防止泛洪。

注意事项

- 功能开启，配置命令可以无需带任何参数，比如命令 **storm-control unicast** 开启基于未知名单播报文的风暴控制，所有命令可选参数使用系统默认值。

配置方法

启动基于单播报文风暴控制

- 必须配置。
- 若无特殊要求，应在每台设备上启动单播报文风暴控制功能。

启动基于组播报文风暴控制

- 必须配置。
- 若无特殊要求，应在每台设备上启动组播报文风暴控制功能。

启动基于广播报文风暴控制

- 必须配置。
- 若无特殊要求，应在每台设备上启动广播报文风暴控制功能。

检验方法

- `show storm-control` 查看命令是否配置成功。

相关命令

启动基于单播报文风暴控制

【命令格式】 `storm-control unicast [{ level percent | pps packets | rate-bps }]`

【参数说明】 `level percent`：指定带宽百分比。

`pps packets`：指定每秒报文数

`rate-bps`：指定速率

【命令模式】 端口模式

【使用指导】 必须是交换口

启动基于组播报文风暴控制

【命令格式】 `storm-control multicast [{ level percent | pps packets | rate-bps }]`

【参数说明】 `level percent`：指定带宽百分比。

`pps packets`：指定每秒报文数

`rate-bps`：指定速率

【命令模式】 接口模式

【使用指导】 必须是交换口

启动基于广播报文风暴控制

【命令格式】 `storm-control broadcast [{ level percent | pps packets | rate-bps }]`

【参数说明】 `level percent`：指定带宽百分比。

`pps packets`：指定每秒报文数

`rate-bps`：指定速率

- 【命令模式】 接口模式
 【使用指导】 必须是交换口

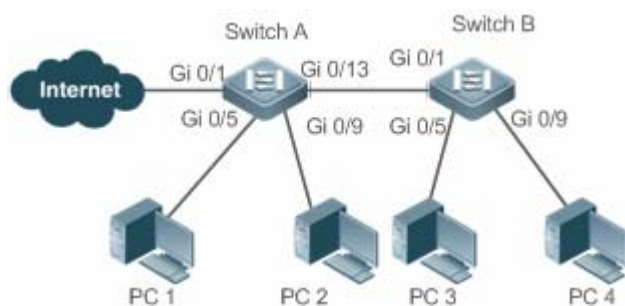
配置举例

i 以下配置举例，仅介绍与风暴控制相关的配置。

在设备上开启风暴控制功能

【网络环境】

图 2-2



【配置方法】 ● 在接入设备 Switch A、Switch B 上配置风暴控制

```
Switch A
Ruijie(config)#interface range gigabitEthernet 0/5,0/9,0/13
Ruijie(config-if-range)#storm-control broadcast
Ruijie(config-if-range)#storm-control multicast
Ruijie(config-if-range)#storm-control unicast

Switch B
Ruijie(config)#interface range gigabitEthernet 0/1,0/5,0/9
Ruijie(config-if-range)#storm-control broadcast
Ruijie(config-if-range)#storm-control multicast
Ruijie(config-if-range)#storm-control unicast
```

【检验方法】 检查 Switch A、Switch B 上是否开启风暴控制

```
Switch A
Ruijie# sho storm-control
Interface          Broadcast Control Multicast Control Unicast Control Action
-----
GigabitEthernet 0/1      Disabled          Disabled          Disabled          none
GigabitEthernet 0/5      default           default           default           none
GigabitEthernet 0/9      default           default           default           none
GigabitEthernet 0/13     default           default           default           none

Switch B
Ruijie#sho storm-control
Interface          Broadcast Control Multicast Control Unicast Control Action
-----
GigabitEthernet 0/1      default           default           default           none
GigabitEthernet 0/5      default           default           default           none
```

GigabitEthernet 0/9	default	default	default	none
---------------------	---------	---------	---------	------

常见错误

- 无。

2.5 监视与维护

清除各类信息

无。

查看运行情况

作用	命令
查看风暴控制信息。	show storm-control [<i>interface-type interface-number</i>]

查看调试信息

无

3 PASSWORD-POLICY

3.1 概述

Password Policy (口令策略) 是设备本地认证时提供的口令安全功能，它依据管理员设置的口令安全策略对用户的登录密码和用户的登录状态进行控制。

 下文仅介绍 Password Policy 的相关内容。

协议规范

暂无可遵循的协议规范或标准。

3.2 功能详解

基本概念

📌 口令最小长度限制

根据系统的安全要求，管理员可设置用户口令的最小长度。当用户配置口令时，如果输入的口令长度小于限定的最小长度，系统将不允许用户设置该口令，并提示出错信息，提醒用户重新设置口令。

📌 强口令检测功能

口令的复杂度越低，其被成功破解的可能性就越大，比如与账号同名的口令、只包含字符或数字的简单口令等。出于安全性考虑，管理员可以打开强口令检测功能，确认用户设置的口令具有较高的复杂度。打开强口令检测功能后，对不符合口令强度检测策略的如下口令提示告警：

- 1、与账号同名的口令；
- 2、只包含字符或数字的简单口令。

📌 口令生存周期

口令生存周期用于限制用户口令的使用时间。当口令的使用时间超过限定值后，需要用户更换口令。

当用户登录时，如果用户输入已经过期的口令，系统将提示该口令已经过期，需要重新设置口令。在重新设置口令时，如果输入的新口令不符合要求，或者连续两次输入的新口令不一致，系统将要求用户继续重新输入。

📌 口令重复使用限制功能

当用户修改口令时，系统会要求用户设置新的口令，旧的口令将被记录下来，形成该用户的历史记录。如果用户新设置的口令以前被使用过，系统将给出错误提示，并要求用户重新设置口令。

可以配置每个用户口令历史记录的最大条数，当口令历史记录的条数超过配置的最大条数时，新的口令历史记录将覆盖该用户最老的一条口令历史记录。

📌 口令加密存储

出于安全考虑，管理员可以打开口令加密存储功能，打开此功能后，进行 **show running-config** 查看配置或 **write** 保存配置文件时，用户设置的各种口令将变成密文；如果再次关闭口令加密存储功能，已经变为密文的口令不会恢复为明文。

3.3 配置详解

配置项	配置建议 & 相关命令	
配置口令安全策略	⚠️ 可选配置。用于配置口令安全相关的策略组合。	
	password policy life-cycle	设置口令生存周期。
	password policy min-size	限制用户口令的最小长度。
	password policy no-repeat-times	限制重复使用最近几次已配置过的口令。
	password policy strong	打开强口令检测功能。
	service password-encryption	设置口令加密存储。

3.3.1 配置口令安全策略基本功能

配置效果

- 为设备的本地认证提供口令安全策略，用户可以配置不同的安全策略来实现口令安全管理的目的。

注意事项

- 配置了口令安全策略后，只对全局口令（通过 **enable password**、**enable secret** 命令配置）和本地用户口令（通过 **username name password password** 命令配置），对于 Line 模式下面的口令不生效。

配置方法

📌 设置口令生存周期

- 可选配置。
- 若无特殊要求，应在每台需要设置口令生存周期的设备上面配置。

📌 限制用户口令的最小长度

- 可选配置。
- 若无特殊要求，应在每台需要限制口令最小长度的设备上面配置。

限制重复使用最近几次已配置过的口令

- 可选配置。
- 若无特殊要求，应在每台需要限制重复使用最近几次已配置过的口令的设备上面配置。

打开强口令检测功能

- 可选配置。
- 若无特殊要求，应在每台需要进行强口令检测的设备上面配置。

设置口令加密存储

- 可选配置。
- 若无特殊要求，应在每台需要设置口令加密存储的设备上面配置。

检验方法

在设备上面配置一个本地用户，并为此用户配置合法、非法口令。

- 配置合法的口令时，设备能否正确添加用户口令。
- 配置非法的口令时，设备能否提示相应的 Log 信息。

相关命令

设置口令生存周期

【命令格式】 **password policy life-cycle days**

【参数说明】 **life-cycle days**：口令生存周期，单位：天，范围：1~65535。

【命令模式】 全局配置模式

【使用指导】 口令生存周期用来限制用户口令的使用时间，当口令超过生存周期后，系统在下次用户登录时，将提示用户修改口令。

限制用户口令的最小长度

【命令格式】 **password policy min-size length**

【参数说明】 **min-size length**：指定口令最小长度，范围：1~31。

【命令模式】 全局配置模式

【使用指导】 此命令用来配置口令的最小长度限制，若没有配置口令的最小长度限制，用户设置口令时将不进行口令最小长度限制。

限制重复使用最近几次已配置过的口令

【命令格式】 **password policy no-repeat-times times**

【参数说明】 **no-repeat-times times**：最近几次已配置过的口令，范围：1~31。

【命令模式】 全局配置模式

【使用指导】 开启此功能后，用户最近几次使用过的旧口令将被记录下来，形成该用户的口令历史记录。如果用户新设置的

口令以前被使用过，系统将给出错误提示，口令更改失败。

可以配置用户口令历史记录的最大条数，当口令历史记录的条数超过配置的最大历史记录条数时，新的口令历史记录将覆盖该用户最老的一条口令历史记录。

📌 打开强口令检测功能

【命令格式】 **password policy strong**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 开启了此功能后，能够在新建用户时对不符合口令强度策略的如下口令配置提示告警：

- 1、与账号同名的口令；
- 2、只包含字符或数字的简单口令。

📌 设置口令加密存储

【命令格式】 **service password-encryption**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 没有设置口令加密存储前，用户配置过程，使用的各种口令均以明文显示和存储，除非是直接使用密文进行配置。出于安全考虑，可以打开口令加密存储功能，打开此功能后，进行 **show running-config** 或 **write** 保存时，用户设置的各​​种口令将变成密文；如果再次关闭口令加密存储功能，已经变为密文的口令不会恢复为明文。

📌 查看用户设置的口令安全策略信息


【命令格式】 **show password policy**

【参数说明】 -

【命令模式】 特权模式、全局模式、接口模式

【使用指导】 查看设备上设置的口令安全策略信息。

配置举例

 以下配置举例，介绍口令安全策略相关的配置。

📌 在设备上

【网络环境】 假设网络环境中，有以下口令安全需求：

- 1、口令最小长度大于等于 8 个字符；
- 2、口令生存时间为 90 天；
- 3、口令使用加密存储和传输；
- 4、口令重复使用历史记录条数 3 条；
- 5、不允许口令与用户名一样或者只包含简的字符或数字。

- 【配置方法】
- 配置口令最小长度：8。
 - 配置口令生存周期：90 天。
 - 开启口令加密存储功能。

- 配置口令重复使用历史记录条数：3。
- 开启强口令检测功能。

```
Ruijie# configure terminal
Ruijie(config)# password policy min-size 8
Ruijie(config)# password policy life-cycle 90
Ruijie(config)# service password-encryption
Ruijie(config)# password policy no-repeat-times 3
Ruijie(config)# password policy strong
```

【检验方法】 用户设置了相关口令安全策略相关的配置后，在新增用户和口令的时候，将会依据口令安全策略进行相关的检测。

- 通过 **show password policy**，查看用户设置的口令安全策略信息。

```
Ruijie# show password policy

Global password policy configurations:

Password encryption:           Enabled
Password strong-check:        Enabled
Password min-size:            Enabled (8 characters)
Password life-cycle:          Enabled (90 days)
Password no-repeat-times:     Enabled (max history record: 3)
```

常见错误

- 设置口令过期前开始提醒的时间大于口令生存周期。

3.4 监视与维护

查看运行情况

作用	命令
查看用户设置的口令安全策略信息	show password policy

4 CPP

4.1 概述

CPP (CPU Protect Policy , CPU 保护策略) 提供了交换机 CPU 保护的策略。

在网络环境中, 有各种攻击报文在网络上传播, 其会导致交换机的 CPU 利用率过高, 影响协议运行, 甚至无法正常管理交换机。针对这种情况, 必须对交换机的 CPU 进行保护, 即对送往交换机的 CPU 处理的各种报文进行流量控制和优先级处理, 保障其正常处理能力。

CPP 功能能够有效的抵御网络中的恶意攻击, 为正常的协议报文提供干净的运行环境。

CPP 缺省情况下已开启, 伴随交换机的整个运行过程, 都在发挥着其保护作用。

4.2 功能详解

基本概念

📌 QoS , DiffServ

QoS (Quality of Service) 服务质量, 是网络的一种安全机制, 是用来解决网络延迟和阻塞等问题的一种技术。

DiffServ 指差分服务模型, 是 QoS 实现模型的一种典型, 通过对业务流进行划分, 以提供差异性的服务。

📌 Bandwidth , Rate

带宽指最大可承载的数据率, 在本文中主要用于指限速阈值, 超过限速阈值的报文将会被丢弃。

速率指实际的数据率, 当速率超过带宽时, 超过部分将被丢弃。速率只能小于等于带宽。

本文中的带宽和速率的单位都为 pps (packets per second , 每秒报文数)。

📌 L2 , L3 , L4

指报文按照 TCP/IP 模型划分的层次结构。

L2 指二层头部, 即以太网封装部分; L3 指三层头部, 即 IP 封装部分; L4 指四层头部, 一般指 TCP/UDP 的头部封装部分。

📌 优先级队列, SP

报文在交换机内部会被缓存, 输出方向即在队列中进行缓存, 优先级队列是与 SP 对应的, 各个队列并非对等, 而是严格划分优先级。

SP (Strict Priority) 严格优先级调度算法, 是 QoS 调度算法的一种, 当高优先级队列中有报文时, 一定调度高优先级队列。调度指从队列中选择报文进行输出, 本文中, 指选择报文的 CPU。

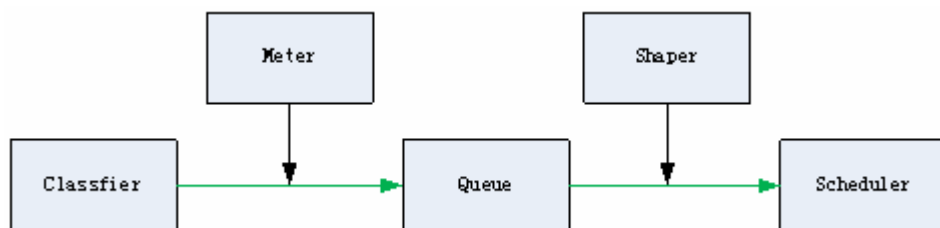
📌 CPU 端口

交换机将报文送 CPU 前，会进行缓存，报文投递 CPU 的过程，实际上类似于报文输出的过程，CPU 端口是一个虚拟端口，报文被送 CPU，即从这个虚拟端口输出，上述的优先级队列，SP 均是针对 CPU 端口的。

功能特性

CPP 功能通过标准的 QOS (服务质量) 差分服务模型 (DiffServ) 实现 CPU 保护。

图 4-1 CPP 实现模型图



功能特性	作用
Classifier	完成对报文类型的分类，为后续的 QOS 策略实施提供保证。
Meter	基于报文类型进行限速处理，控制某种报文类型的带宽。
Queue	对送往 CPU 的报文进行排队，基于报文类型可选择不同的队列进行排队。
Scheduler	选择队列进行报文调度，被调度到的报文被送往 CPU。
Shaper	完成基于优先级队列和 CPU 端口进行限速处理，控制优先级队列和 CPU 端口的带宽。

4.2.1 Classifier

工作原理

Classifier (分类器) 对每个需要送到 CPU 的报文进行分类，分类时根据报文的 L2、L3 以及 L4 信息。对报文进行分类是实施 QOS 策略的基础，在后续动作中根据分类可以实施不同策略，提供区别服务。交换机提供的分类是固定的，按照交换机支持的协议，管理功能固定划分报文类型，比如生成树协议的 BPDU 报文，网络控制报文协议的 ICMP 报文等。不支持自定义报文的分类规则。

i 由于硬件差异性，不同产品对报文的分类有差异，具体参见产品特性文档。

相关配置

4.2.2 Queue

工作原理

Queue (队列) 完成了对报文的二级划分, 可以多种不同的报文类型选择同一个队列; 同时, 队列完成了报文在交换机内部的缓存, 为接下来的 Scheduler 和 Shaper 提供服务。

CPP 对应的队列是严格优先级 (SP) 队列, 通过报文的入队列, 确定报文的严格优先级, 队列号大的优先级高。

4.2.3 Scheduler

工作原理

Scheduler (调度器) 根据优先级队列, 对报文进行严格优先级 (SP) 调度, 即只要更高优先级队列存在报文, 严格优先调度更高优先级队列中的报文。

在调度前, 送 CPU 的报文缓存在队列中, 当被调度时, 报文被送往 CPU 处理。

i 调度策略不可更改, 只支持严格优先级调度。

相关配置

4.2.4 Shaper

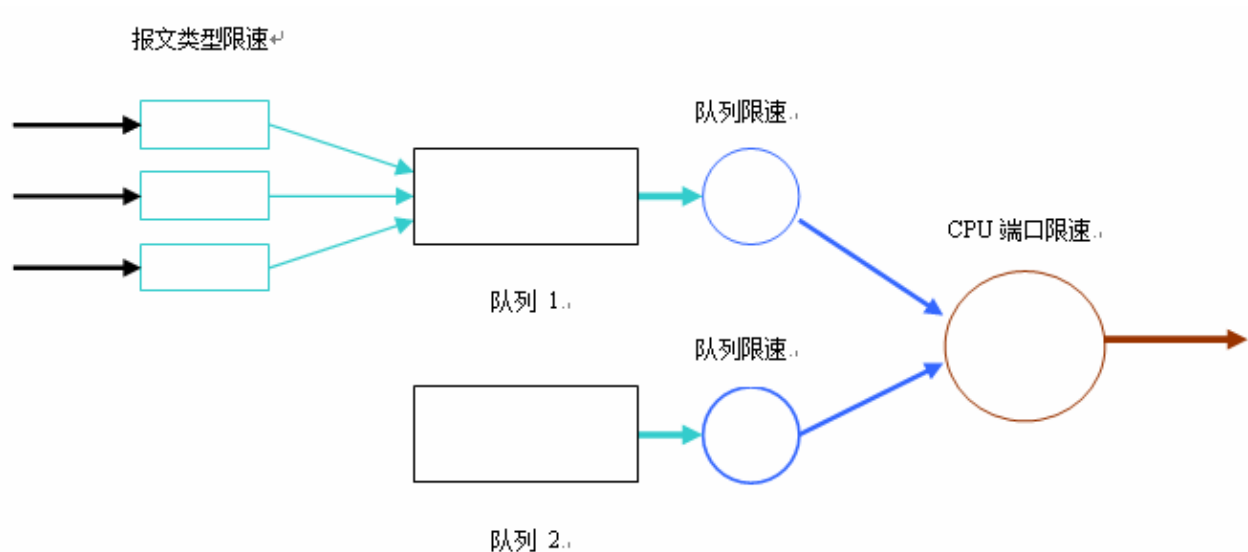
工作原理

Shaper (整形器) 完成对送往 CPU 的报文进行整形, 即当实际速率大于整形阈值时, 报文继续缓存在队列中, 不进行调度, 因此, 在报文速率波动情况下, 通过 Shaper, 可以使得送往 CPU 的报文速率是平滑的(速率小于等于整形阈值)。

在有 Shaper 的情况下, 高优先级队列的报文不一定调度完成才调度低优先级队列, 某个优先级队列报文速率若超过整形阈值, 将会暂时停止调度。因此, 通过 Shaper, 可以避免低优先级队列的报文被饿死(一直调度高优先级队列报文, 低优先级队列报文得不到调度)。

由于 Shaper 通过限制调度报文的速率 实际上也提供了限速的功能。针对优先级队列和所有送 CPU 的报文(CPU 端口) ,Shaper 提供了两级限速。和 Meter 功能一起, 形成三级限速, 为 CPU 提供三级防护。

图 4-2 CPP 的三级限速



4.3 产品说明



NBS2000 系列产品，CPP 对应的队列是加权循环(WRR)调度算法，高优先级队列的报文具具有更高的权重，同时防止低优先级队列报文一直得不到调度。



NBS2000 系列产品中 Shaper 的配置出厂预设，不支持修改。



NBS2000 系列产品不支持 CPP 的任何配置。



NBS2000 系列产品，不支持单独查看某个端口（包括 CPU 端口）、报文类型及优先级队列的配置与查看。



NBS2000 系列产品 CPU Protect 的默认值：

报文类型	带宽(pps)	报文优先级	支持情况
arp	130	1	yes
l2-packet	180	6	yes
local	200	3	yes
other	50	0	yes

各优先级队列的默认带宽值：

队列	默认带宽值
0	200
1	200
2	200
3	200
4	200
5	200
6	200
7	200

CPU 口默认带宽值：200

4.4 监视与维护

清除各类信息

作用	命令
清除 CPP 的统计信息。	clear cpu-protect counters [<i>device device_num</i>]

查看运行情况

作用	命令
查看 CPU 端口的配置值	show cpu-protect cpu

查看调试信息

-
。

5 DHCP Snooping

5.1 概述

DHCP Snooping：意为 DHCP 窥探，通过对 Client 和服务器之间的 DHCP 交互报文进行窥探实现对用户 IP 地址使用情况的记录和监控，同时还可以过滤非法 DHCP 报文，包括客户端的请求报文和服务端的响应报文。

i 下文仅介绍 DHCP Snooping 的相关内容。

协议规范

- RFC2131：Dynamic Host Configuration Protocol
- RFC2132：DHCP Options and BOOTP Vendor Extensions

5.2 典型应用

典型应用	场景描述
DHCP服务欺骗攻击防范	在网络上存在多个 DHCP 服务器，限制 DHCP 客户端只能从合法的 DHCP 服务获取网络配置参数。
DHCP报文泛洪攻击防范	在网络上存在恶意用户，频繁的发送 DHCP 请求报文。
伪造DHCP报文攻击防范	在网络上存在恶意用户，发送伪造的 DHCP 请求报文，比如 DHCP-Release 报文。

5.2.1 DHCP服务欺骗攻击防范

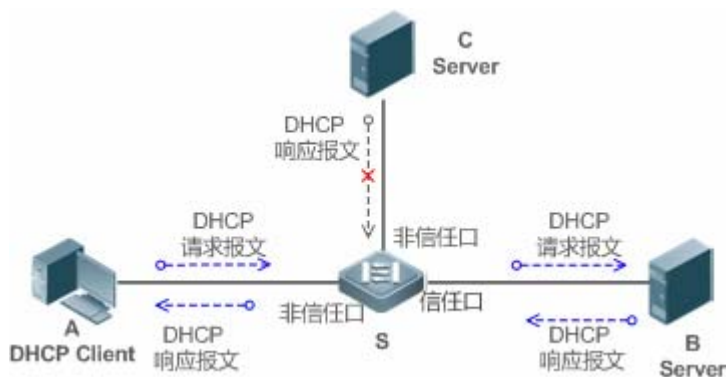
应用场景

在网络中可能存在多个 DHCP 服务器，需要保证用户 PC 只能从控制范围内的 DHCP 服务器获取网络配置参数。

以下图为例，DHCP 客户端仅与可信 DHCP 服务器通信。

- DHCP 客户端的请求报文只会传输到可信任的 DHCP 服务器。
- 只有可信任 DHCP 服务器的响应报文才会传输给客户端。

图 5-1



- 【注释】 S 为接入设备。
 A 为用户 PC。
 B 为控制范围内的 DHCP 服务器。
 C 为不受控的 DHCP 服务器。

功能部署

- 在接入设备 S 上开启 DHCP Snooping 服务，实现 DHCP 报文监控。
- 设置接入设备 S 链接 DHCP 服务器 B 的端口为 DHCP TRUST 口，实现响应报文的转发。
- 设置接入设备 S 的其余端口为 DHCP UNTRUST 口，实现响应报文的过滤。

5.2.2 DHCP报文泛洪攻击防范

应用场景

在网络中可能存在恶意 DHCP 客户，高速率的发送 DHCP 请求报文，造成合法用户无法获得 IP、接入设备高负荷运行甚至瘫痪。需要保证网络系统运行稳定。

应用 DHCP 报文限速，DHCP 客户端仅能以低于规定的速率发送 DHCP 请求报文。

- DHCP 客户端的请求报文发送速率低于规定阈值。
- 超出限定的报文被丢弃。

功能部署

- 在接入设备 S 上开启 DHCP Snooping 服务，实现 DHCP 监控。
- 限制 UNTRUST 口的 DHCP 报文发送速率。

5.2.3 伪造DHCP报文攻击防范

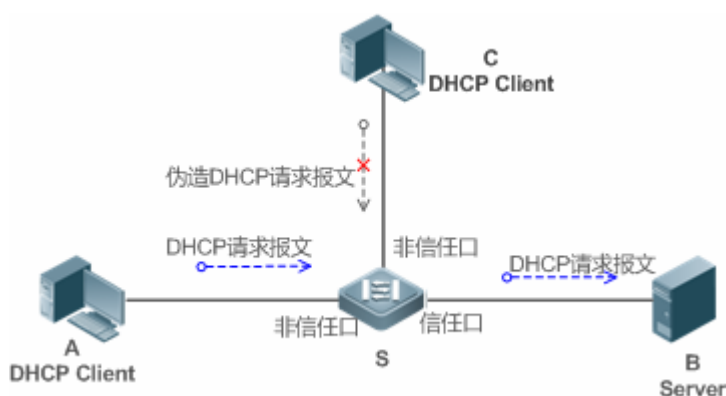
应用场景

在网络中可能存在恶意用户，伪造 DHCP 请求报文，一方面消耗了服务器的可用 IP，另一方面有可能抢夺合法用户的 IP。需要过滤掉接入网络上的非法 DHCP 报文。

以下图为例，DHCP 客户端发送的 DHCP 请求报文将被检查。

- DHCP 客户端的请求报文的源 MAC 字段与 DHCP 报文的客户硬件地址字段必须匹配。
- 客户端的 Release 报文与 Decline 报文必须与 Snooping 内部数据库的记录匹配。

图 5-2



- 【注释】 S 为接入设备。
A、C 为用户 PC。
B 为控制范围内的 DHCP 服务器。

功能部署

- 在接入设备 S 上开启 DHCP Snooping 服务，实现 DHCP 监控。
- 设置接入设备 S 链接 DHCP 服务器 B 的端口为 DHCP TRUST 口，实现响应报文的转发。
- 设置接入设备 S 的其余端口为 DHCP UNTRUST 口，实现 DHCP 报文的过滤。
- 在接入设备 S 上，所有 UNTRUST 口设置 DHCP 源 MAC 检查，过滤非法的 DHCP 报文。

5.3 功能详解

基本概念

DHCP 请求报文

DHCP 客户端发往 DHCP 服务器的报文。包括 DHCP-DISCOVER 报文、DHCP-REQUEST 报文、DHCP-DECLINE 报文、DHCP-RELEASE 报文及 DHCP-INFORM 报文。

📌 DHCP 应答报文

DHCP 服务器发往 DHCP 客户端的报文。包括 DHCP-OFFER 报文、DHCP-ACK 报文及 DHCP-NAK 报文。

📌 DHCP Snooping TRUST 口

由于 DHCP 获取 IP 的交互报文是使用广播的形式，从而存在着非法的 DHCP 服务影响用户正常 IP 的获取，更有甚者通过非法的 DHCP 服务欺骗窃取用户信息的现象，为了防止非法的 DHCP 服务的问题，DHCP Snooping 把端口分为两种类型，TRUST 口和 UNTRUST 口，设备只转发 TRUST 口收到的 DHCP 应答报文，而丢弃所有来自 UNTRUST 口的 DHCP 应答报文，这样我们把合法的 DHCP Server 连接的端口设置为 TRUST 口，则其他口为 UNTRUST 口，就可以实现对非法 DHCP Server 的屏蔽。

在交换机设备上，所有交换口或者 2 层 AP 口默认均为 UNTRUST 口，可以配置指定 TRUST 口。在无线 AP (Access Point) 设备上，所有 WLAN 均为 UNTRUST 口，不可配置指定 TRUST 口；当 AP 为 FAT 模式时，所有 2 层交换口和 2 层封装接口默认均为 UNTRUST 口，可以配置指定为 TRUST 口；当 AP 为 FIT 模式时，所有 2 层交换口默认为 UNTRUST 口，可以配置指定为 TRUST 口，所有 2 层封装接口均为 TRUST 口，不可以配置指定为 UNTRUST 口。在无线 AC (Access Control) 设备上，所有 WLAN 均为 UNTRUST 口，不可配置指定为 TRUST 口，所有交换口和 2 层 AP 口默认为 UNTRUST 口，可以配置指定为 TRUST 口。

📌 DHCP Snooping 报文抑制

在对个别用户禁用 DHCP 报文的情况下，需要屏蔽用户设备发出的任何 DHCP 报文，那么我们可以在 UNTRUST 口配置 DHCP 报文抑制功能，过滤掉该端口收到的所有 DHCP 报文。

📌 DHCP Snooping 速率限制

DHCP Snooping 对 DHCP 报文的速率限制可以选择通过 NFPP 的速率限制命令配置，NFPP 的配置请查看 NFPP 配置指导。

📌 DHCP Option82 选项

DHCP Option82 选项又称为 DHCP 中继代理信息选项 (Relay Agent Information Option)，是 DHCP 报文中的一个选项。因其选项编号为 82，故通常被简称为 Option82 选项。Option82 选项是为了增强 DHCP 服务器的安全性，改善 IP 地址的分配策略而提出的一种 DHCP 选项。该选项功能通常配置在网络接入设备的 DHCP 中继服务组件中，如 DHCP Relay、DHCP Snooping。该选项对 DHCP 客户端透明，由 DHCP 中继组件实现选项的添加与剥离。

📌 非法 DHCP 报文

DHCP Snooping 通过对经过设备的 DHCP 报文进行合法性检查，丢弃不合法的 DHCP 报文，记录用户信息并生成 DHCP Snooping 绑定数据库供其他功能（如：ARP 检测功能）查询使用。以下几种类型的报文被认为是非法的 DHCP 报文

- UNTRUST 口收到的 DHCP 应答报文，包括 DHCPACK、DHCPNACK、DHCP OFFER 等。
- UNTRUST 口收到的带有网关信息【giaddr】的 DHCP request 报文。
- 打开 mac 校验时，源 MAC 与 DHCP 报文携带的【chaddr】字段值为不同的报文。
- DHCPRELEASE 报文中的用户在 DHCP Snooping 绑定数据库中存在，但是 DHCPRELEASE 报文的 UNTRUST 口和保存在 DHCP Snooping 绑定数据库中的 UNTRUST 口不一致，那么这个 DHCPRELEASE 报文是非法的。

- DHCP 报文格式不正确或是不完整的报文。

功能特性

功能特性	作用
过滤非法DHCP报文	对交互的 DHCP 报文进行合法性检查, 丢弃那些非法报文(非法报文的介绍见上节的介绍), 仅向 TRUST 口转发合法的请求报文。
建立Binding数据库	窥探 DHCP 客户端与服务器的交互, 生成 DHCP Snooping Binding 数据库, 为其他安全过滤模块提供依据。

5.3.1 过滤非法DHCP报文

对来自 UNTRUST 口的 DHCP 报文进行合法性检查。依据上节“基本概念”中介绍的非法报文类型, 进行过滤。控制报文的传播范围, 防止恶意用户欺骗。

工作原理

窥探过程中, 检查报文的接收端口、报文字段, 达到过滤报文目的; 修改报文的端口, 达到控制报文传播范围的目的。

▾ 端口检查

接收到 DHCP 报文时, 设备先判断接收报文的端口是否为 DHCP TRUST 口。若是 TRUST 口, 跳过合法性检查、Binding 记录生成阶段, 直接进入报文转发阶段。若是 UNTRUST 口, 需要进行合法性检查。

▾ 检查报文封装及长度是否完整

设备检查报文是否为 UDP 报文, 且目的端口为 67 或 68。检查数据包的实际长度与协议中的长度字段是否匹配。

▾ 检查 DHCP 报文字段及报文类型是否正确

依据上节“基本概念”中介绍的非法报文类型, 先检查报文的【giaddr】、【chaddr】字段, 再依据报文的实际类型, 检查该类型特有的限制条件是否满足。

相关配置

▾ 启动全局 DHCP Snooping 功能

缺省情况下, DHCP Snooping 功能关闭。

使用 `ip dhcp snooping` 命令可以启动设备的 DHCP Snooping 功能。

必须首先开启全局 DHCP Snooping 功能, 才能进一步在不同 VLAN 上启停 DHCP Snooping 功能。

▾ 配置 DHCP 源 MAC 检查功能

缺省情况下, 设备不对报文的二层源 MAC 及 DHCP 报文的【chaddr】字段进行校验。

使用 `ip dhcp snooping verify mac-address` 命令，设备就会对 UNTRUST 口送上来的 DHCP Request 报文进行源 MAC 和【chaddr】字段的 MAC 地址进行校验检查，丢弃 MAC 值不相同的 DHCP 请求报文。

5.3.2 建立Binding数据库

窥探 DHCP 客户端与 DHCP 服务器的交互报文，依据合法 DHCP 报文信息，生成 DHCP Snooping Binding 表项。所有这些表项作为合法用户的信息表，提供给设备的其他安全模块使用，作为网络报文过滤的依据。

工作原理

窥探过程中，依据 DHCP 报文的类型，不断更新 Binding 数据库。

生成 Binding 记录

窥探到 TRUST 口上的 DHCPACK 报文时，提取出报文中的客户端 IP 地址、客户端 MAC 地址、租约时间字段，结合设备记录的客户端所在端口 ID（有线接口索引或者无线 WLAN ID）、客户端所属 VLAN，生成一条 Binding 记录。

删除 Binding 记录


记录的租约时间到期；或是窥探到客户端发送的合法 DHCP-RELEASE/DHCP-DECLINE 报文时；或是接收到来自 TRUST 口的 NAK 报文时；或是用户使用 clear 命令主动删除 Binding 记录时，删除对应的 Binding 记录。

相关配置

无需额外配置，只需要开启 DHCP Snooping 功能即可。

5.4 配置详解

配置项	配置建议 & 相关命令	
配置DHCP Snooping基本功能	 必选配置。用于建立 DHCP Snooping 服务。	
	<code>ip dhcp snooping</code>	启动 DHCP Snooping 功能
	<code>ip dhcp snooping suppression</code>	启动 DHCP 报文抑制功能
	<code>ip dhcp snooping verify mac-address</code>	配置 DHCP 源 MAC 检查功能
	<code>ip dhcp snooping database write-delay</code>	启动 DHCP Snooping Binding 记录定时保存功能
	<code>ip dhcp snooping database write-to-flash</code>	手动保存 DHCP Snooping Binding 记录
	<code>renew ip dhcp snooping database</code>	手动将保存在备份文件中的用户记录导入到 DHCP Snooping Binding 数据库中
	<code>ip dhcp snooping trust</code>	配置 DHCP Snooping TRUST 口
	<code>ip dhcp snooping bootp</code>	启动支持 bootp 功能

	ip dhcp snooping check-giaddr	启动 DHCP Snooping 支持处理 Relay 请求报文功能
配置Option82 选项	 可选配置。用于优化 DHCP 服务器地址分配。	
	ip dhcp snooping information option	在 DHCP 请求报文中加入 Option82 选项功能
	ip dhcp snooping information option format remote-id	设置 Option82 选项的子选项 remote-id 为自定义字符串的功能
	ip dhcp snooping vlan information option format-type circuit-id string	设置 Option82 选项的子选项 circuit-id 为自定义字符串的功能

5.4.1 配置DHCP Snooping基本功能

配置效果

- 开启 DHCP Snooping 服务。
- 生成 DHCP Snooping Binding 数据库。
- 控制 DHCP 报文的传播范围。
- 过滤非法的 DHCP 报文。

注意事项

- 设备连接可信 DHCP 服务器的端口必须设置成 DHCP TRUST 口。
- DHCP Snooping 生效的端口可以是有线的交换口、2 层 AP 口或者 2 层封装子接口，也可以是无线的 WLAN，端口下的配置分为接口模式下的配置以及无线安全模式下的配置。

配置方法

▾ 启动全局 DHCP Snooping 服务

- 必须配置。
- 若无特殊要求，应在接入设备上配置该功能。

▾ 按 VLAN 开关 DHCP Snooping 功能

- 如果有些 VLAN 不需要 DHCP Snooping 功能，可以关闭。
- 若无特殊要求，应在接入设备上配置该功能。

▾ 配置 DHCP TRUST 口

- 必须配置。

- 将设备连接可信 DHCP 服务器的端口设置成 DHCP TRUST 口。

启动 DHCP 源 MAC 地址检查

- 如果要求 DHCP 请求报文的【chaddr】字段必须与数据包的二层源 MAC 地址匹配，则必须配置。
- 若无特殊要求，应在接入设备的所有 UNTRUST 口上开启该功能。

启动 DHCP Snooping Binding 记录定时保存功能

- 如果要求设备重启后，之前窥探的 DHCP Snooping Binding 记录仍然能够生效，需要启动该功能。
- 若无特殊要求，应在接入设备上开启该功能。

启动支持 BOOTP 功能

- 可选配置。

若无特殊要求，应在接入设备上开启该功能。

启动 DHCP Snooping 支持处理 Relay 请求报文功能

- 可选配置。
- 若无特殊要求，应在接入设备上开启该功能。

检验方法

用户配置设备使用 DHCP 协议获取网络配置参数。

- 检查设备上的 DHCP Snooping Binding 数据库是否生成相应用户记录。

相关命令

配置打开和关闭 DHCP Snooping

【命令格式】 [no] ip dhcp snooping

【参数说明】 -。

【命令模式】 全局配置模式

【使用指导】 打开 DHCP Snooping 全局功能后，可以使用 **show ip dhcp snooping** 命令查看 DHCP Snooping 功能是否打开。

配置端口 DHCP 报文抑制

【命令格式】 [no] ip dhcp snooping suppression

【参数说明】 -

【命令模式】 接口配置模式或者无线安全配置模式

【使用指导】 通过配置该命令，可拒绝该端口下所有 DHCP 请求报文，即禁止该端口下的所有用户通过 DHCP 方式申请地址。

配置 DHCP 源 MAC 检查功能

- 【命令格式】 **[no] ip dhcp snooping verify mac-address**
- 【参数说明】 -
- 【命令模式】 全局配置模式
- 【使用指导】 源 MAC 地址检验功能，是对 DHCP CLIENT 发出的请求报文，检查链路层头部 MAC 地址和 DHCP 报文中的 CLIENT MAC 字段是否相同。源 MAC 地址检验失败时，报文将被丢弃。

配置定时写 DHCP Snooping 数据库信息到 flash

- 【命令格式】 **[no] ip dhcp snooping database write-delay [time]**
- 【参数说明】 *time*：两次将 DHCP Snooping 数据库写入 FLASH 的时间间隔。
- 【命令模式】 全局配置模式
- 【使用指导】 通过配置该命令，可以将 DHCP Snooping 数据库写入 FLASH 文件。可以防止设备重新启动后，用户信息丢失，导致用户必须重新获取 IP 地址，才可以正常通讯。

手动把 DHCP Snooping 数据库信息写到 flash

- 【命令格式】 **ip dhcp snooping database write-to-flash**
- 【参数说明】 -
- 【命令模式】 全局配置模式
- 【使用指导】 通过执行此命令，可以实时将 DHCP Snooping 数据库中动态用户信息写入 FLASH 文件。如果设备从非 QINQ 版本升级到 QINQ 版本（反之亦然），则因 flash 文件版本不同，绑定表项不能从 flash 文件恢复。

手动地把当前备份文件中的信息导入 DHCP Snooping 绑定数据库

- 【命令格式】 **renew ip dhcp snooping database**
- 【参数说明】 -
- 【命令模式】 特权模式
- 【使用指导】 通过执行此命令，可以实时将备份文件信息导入 DHCP Snooping 数据库中。

配置端口为 TRUST 口

- 【命令格式】 **[no] ip dhcp snooping trust**
- 【参数说明】 -
- 【命令模式】 接口配置模式
- 【使用指导】 通过配置该命令，将连接合法 DHCP 服务器的端口配置为 TRUST 口。TRUST 端口收到的 DHCP 响应报文被正常转发，UNTRUST 端口收到的 DHCP 响应报文将被丢弃。

配置支持 BOOTP 功能

- 【命令格式】 **[no] ip dhcp snooping bootp-bind**
- 【参数说明】 -
- 【命令模式】 全局配置模式
- 【使用指导】 通过配置该命令，可支持 BOOTP 协议。

配置启动 DHCP Snooping 支持处理 Relay 请求报文功能

【命令格式】 [no] ip dhcp snooping check-giaddr

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 开启此功能后 不能部署使用 Relay 请求生成的 DHCP Snooping 绑定表项的业务 如 IP Source Guard/802.1x 认证等，否则可能导致用户无法上网。

开启此功能后，不能配置 ip dhcp snooping verify mac-address，否则 Relay 的 DHCP 请求报文会被丢弃，导致用户无法获取地址。

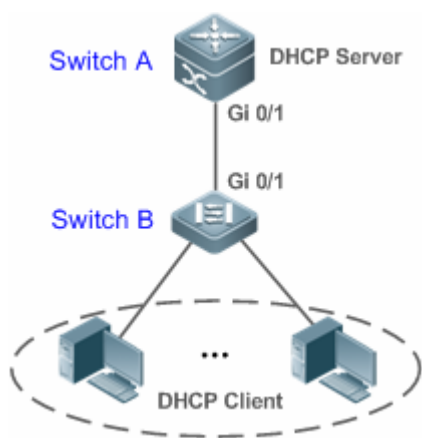
配置举例

i 以下配置举例，仅介绍与 DHCP Snooping 相关的配置。

DHCP 客户端用户通过合法 DHCP 服务器动态获取 IP 地址

【网络环境】

图 5-3



- 【配置方法】
- 在接入设备（本例为 Switch B）上开启 DHCP Snooping 功能
 - 将上链口（本例为端口 Gi 0/1）设置为 TRUST 口。

B

```
B#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
B(config)#ip dhcp snooping
B(config)#interface gigabitEthernet 0/1
B(config-if-GigabitEthernet 0/1)#ip dhcp snooping trust
B(config-if-GigabitEthernet 0/1)#end
```

【检验方法】 确认 Switch B 的配置。

- 是否开启 DHCP Snooping 功能、配置的 DHCP Snooping TRUST 口是否为上链口。
- 查看 Switch B 的 DHCP Snooping 配置情况，关注点为 TRUST 口是否正确。

B

```
B#show running-config
!
ip dhcp snooping
!
```

```
interface GigabitEthernet 0/1
B#show ip dhcp snooping
Switch DHCP Snooping status           : ENABLE
DHCP Snooping Verification of hwaddr status : DISABLE
DHCP Snooping database write-delay time  : 0 seconds
DHCP Snooping option 82 status          : DISABLE
DHCP Snooping Support BOOTP bind status  : DISABLE
Interface                               Trusted      Rate limit (pps)
-----
GigabitEthernet 0/1                    YES        unlimited
B#show ip dhcp snooping binding
Total number of bindings: 1
MacAddress      IPAddress      Lease(sec)  Type           VLAN  Interface
-----
0013.2049.9014  172.16.1.2  86207      DHCP-Snooping 1   GigabitEthernet 0/11
```

常见错误

- 没有将上链口设置为 DHCP TRUST 口。
- 在上链口上配置了其他的接入安全选项，导致配置 DHCP TRUST 口失败。

5.4.2 配置Option82 选项

配置效果

- 让 DHCP 服务器在进行地址分配时，能够获取更多的信息，做出更佳地址分配。
- 选项对 DHCP 客户端透明，客户端无法感知到功能的开启或关闭。

注意事项

- 与 DHCP Relay 的 Option82 选项功能互斥。

配置方法

- 如果需要施加此项优化，则应该执行此配置项。
- 若无特殊要求，应在已经开启 DHCP Snooping 的接入设备上开启该功能。

检验方法

查看 DHCP Snooping 的配置选项，确保功能成功开启。

相关命令

在 DHCP 请求报文中加入 Option82 选项功能

【命令格式】 [no] ip dhcp snooping information option [standard-format]

【参数说明】 **standard-format** : Option82 选项使用标准格式。

【命令模式】 全局配置模式

【使用指导】 通过配置该命令，将在 DHCP 请求报文中添加 Option82 选项信息，DHCP 服务器根据 Option82 选项信息进行地址分配。

设置 Option82 选项的子选项 remote-id 为自定义字符串

【命令格式】 [no] ip dhcp snooping information option format remote-id { string ASCII-string | hostname }

【参数说明】 **string ASCII-string** : Option82 选项 remote-id 扩展格式内容为自定义字符串。

hostname : Option82 选项 remote-id 扩展格式内容为主机名。

【配置模式】 全局配置模式

【使用指导】 通过配置该命令，设置 DHCP 请求报文中添加 Option82 选项的 remote-id 子选项为自定义内容，DHCP 服务器根据 Option82 选项信息进行地址分配。

设置 Option82 选项的子选项 circuit-id 为自定义字符串

【命令格式】 [no] ip dhcp snooping vlan *vlan-id* information option format-type circuit-id string *ascii-string*

【参数说明】 **vlan-id** : DHCP 请求报文所在 VLAN。

ascii-string : Circuit ID 要填充的用户自定义的内容。

【配置模式】 接口配置模式

【使用指导】 通过配置该命令，设置 DHCP 请求报文中添加 Option82 选项的 circuit-id 子选项为自定义内容，DHCP 服务器根据 Option82 选项信息进行地址分配。

配置举例

下面是配置在 DHCP 请求报文中加入 Option82 选项功能的例子。

- 【配置方法】
- 配置 DHCP Snooping 基本功能。略
 - 开启添加 Option82 选项功能。

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

【检验方法】 查看 DHCP Snooping 配置。

```
B#show ip dhcp snooping
```

```

Switch DHCP Snooping status           : ENABLE
DHCP Snooping Verification of hwaddr status : DISABLE
DHCP Snooping database write-delay time  : 0 seconds
DHCP Snooping option 82 status         : ENABLE
DHCP Snooping Support bootp bind status  : DISABLE
Interface Trusted Rate limit (pps)
-----
GigabitEthernet 0/1 YES unlimited


```

常见配置错误

- 无

5.5 监视与维护

清除各类信息

 在设备运行过程中执行 **clear** 命令，可能因为重要信息丢失而导致业务中断。

作用	命令
清空 DHCP Snooping 数据库动态用户信息。	clear ip dhcp snooping binding [ip] [mac] [vlan vlan-id] [interface interface-id]

查看运行情况

作用	命令
显示 DHCP Snooping	show ip dhcp snooping
显示 DHCP Snooping 数据库信息	show ip dhcp snooping binding

查看调试信息

 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
打开 DHCP Snooping 事件的调试开关。	debug snooping ipv4 event
关闭 DHCP Snooping 事件的调试开关。	no debug snooping ipv4 event
打开 DHCP Snooping 报文的调试开关。	debug snooping ipv4 packet
关闭 DHCP Snooping 报文的调试开关。	no debug snooping ipv4 packet
打开 DHCP Snooping 基于 MAC 的调试开关	debug snooping ipv4 mac-address H.H.H
关闭 DHCP Snooping 基于 MAC 的调试	no debug snooping ipv4 mac-address H.H.H

开关	
打开 DHCP Snooping 全部调试开关	debug snooping ipv4 all
关闭 DHCP Snooping 全部调试开关	no debug snooping ipv4 all



配置指南-ACL

本分册介绍可靠性配置指南相关内容，包括以下章节：

1. ACL

1 ACL

1.1 概述

ACLs (Access Control Lists, 接入控制列表), 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。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、丢弃。

根据使用 ACL 目的的不同可分为: 安全 ACLs 和 QoS ACLs。

- 安全 ACLs 用于控制哪些数据流允许从网络设备通过。
- QoS ACLs 对这些数据流进行优先级分类和处理。

配置访问列表的原因比较多, 最主要的主要有以下一些:

- 网络访问控制: 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。
- 优先服务保证: 为一些重要的数据流进行优先分类处理, 这就是 QoS ACLs 作用。有关 QoS ACLs 的使用请参考 QoS 相关的配置手册。

 下文仅介绍 ACL 的相关内容。

协议规范

无

1.2 典型应用

典型应用	场景描述
企业内网访问控制应用	在企业网中根据需要对各个部门的网络访问权限进行控制和限制, 比如服务器的访问限制、QQ 和 MSN 等聊天工具的使用限制等。

1.2.1 企业内网络访问控制应用

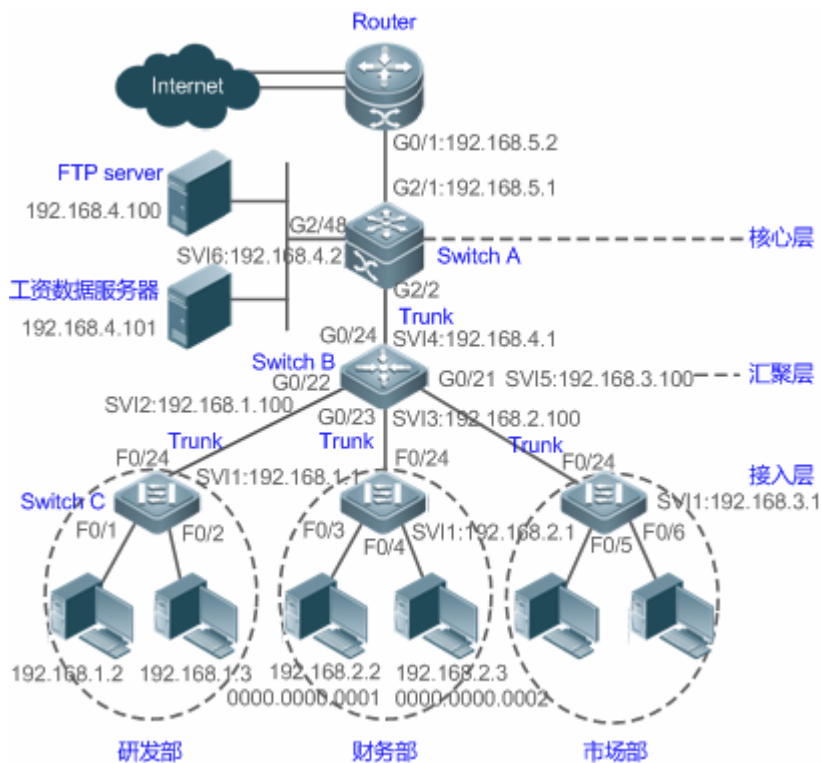
应用场景

Internet 病毒无处不在, 需要封堵各种病毒的常用端口, 以保障内网安全:

- 只允许内部 PC 访问服务器, 不允许外部 PC 访问服务器。

- 不允许非财务部门 PC 访问财务部 PC；不允许非研发部门 PC 访问研发部 PC。
- 不允许研发部门人员在上班时间（即 9:00~18:00）使用 QQ、MSN 等聊天工具。

图 1-1



【注释】 接入层设备 C：连接各部门的 PC，通过千兆光纤(trunk 方式)连接汇聚层设备。

汇聚层设备 B：划分多个 VLAN，每个部门为一个 VLAN，通过万兆光纤(trunk 方式)上连核心层设备。

核心层设备 A：连接各种服务器，如 FTP，HTTP 服务器等，通过防火墙与 Internet 相连。

功能部署

- 通过在核心层设备（本例为设备 A）上联 Router 的端口（本例为 G2/1 口）上设置扩展 ACL 来过滤相关端口的数据包来达到防病毒的目的。
- 要求内部 PC 对服务器进行访问，不允许外部 PC 访问服务器，可以通过定义 IP 扩展 ACL 并应用到核心层设备（本例为设备 A）的下联汇聚层设备和服务器的接口（本例为 G2/2 口/SVI 2）上实现。
- 要求特定部门间不能互访，可通过定义 IP 扩展 ACL 实现（本例中分别在设备 B 的 G0/22、G0/23 上应用 IP 扩展 ACL）；
- 可通过配置时间 IP 扩展 ACL，限制研发部门在特定时间内使用 QQ/MSN 等聊天工具（本例中在设备 B 的 SVI 2 上应用时间 IP 扩展 ACL）。

1.3 功能详解

基本概念

访问列表

访问列表有：基本访问列表和动态访问列表。

用户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。

i 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。

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，或使用子网来定义一类流)
- 目的 IP 地址字段(可以申明全部目的 IP 地址值，或使用子网来定义一类流)
- 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，还可以申明源端口或目的端口的范围。
- 可以申明一个 UDP 的源端口、目的端口或者都申明，还可以申明源端口或目的端口的范围。

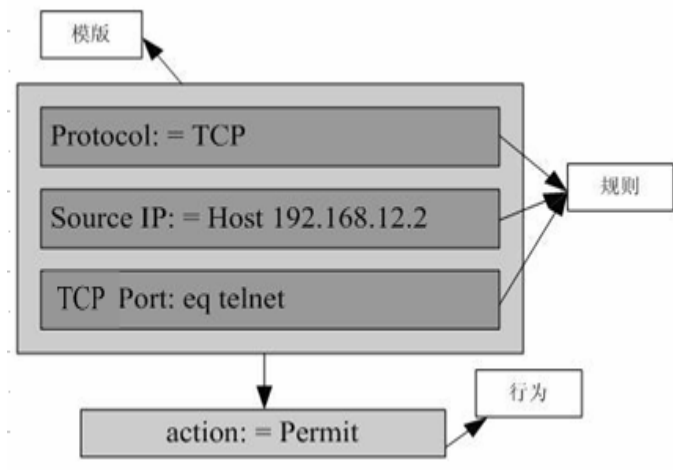
过滤域指的是，在生成一条 ACE 时，根据报文中的哪些字段用以对报文进行识别、分类。过滤域模板就是这些字段组合的定义。比如，在生成某一条 ACE 时希望根据报文的源 IP 字段对报文进行识别、分类，而在生成另一条 ACE 时，希望根据的是报文的源 IP 地址字段和 UDP 的源端口字段，这样，这两条 ACE 就使用了不同的过滤域模板。

规则(Rules)，指的是 ACE 过滤域模板对应的值。比如有一条 ACE 内容如下：

```
permit tcp host 192.168.12.2 any eq telnet
```

在这条 ACE 中，过滤域模板为以下字段的集合：源 IP 地址字段、IP 协议字段、目的 TCP 端口字段。对应的值(Rules)分别为：源 IP 地址 = Host 192.168.12.2；IP 协议 = TCP；TCP 目的端口 = Telnet。

图 1-2 对 ACE : permit tcp host 192.168.12.2 any eq telnet 的分析



- ❗ 过滤域模板可以是三层字段(Layer 3 Field)和四层字段(Layer 4 Field)字段的集合，也可以是多个二层字段(Layer 2 Field)的集合，但标准与扩展的 ACL 的过滤域模板不能是二层和三层、二层和四层、二层和三层、四层字段的集合。要使用二层、三层、四层字段集合，可以应用 Expert 扩展访问控制列表 (Expert ACLs)。
- ❗ OUT 方向 ACL 关联 SVI 的注意事项：支持 IP 标准，IP 扩展，MAC 扩展，专家级 ACL 应用。
- ❗ 对 ACL 中匹配目的 IP 和目的 MAC 有一些限制，如果在 MAC 扩展和专家级 ACL 中匹配目的 MAC，将这样的 ACL 应用到 SVI 的 OUT 方向时，表项会被设置，但无法生效。如果想要在 IP 扩展，专家级 ACL 中匹配目的 IP，而目的 IP 不在所关联的 SVI 的子网 IP 范围内时，该配置的 ACL 将无法生效。比如 VLAN 1 的地址为 192.168.64.1 255.255.255.0，创建一条 IP 扩展的 ACL，ace 为 deny udp any 192.168.65.1 0.0.0.255 eq 255，将该 ACL 应用到 VLAN 1 的出口，将无法生效，因为目的 IP 不在 VLAN 1 子网 IP 范围内，如果 ace 为 deny udp any 192.168.64.1 0.0.0.255 eq 255 将可以生效，因为目的 IP 符合规定。
- ✅ 交换机设备上，作用在物理口和 AP 口上的 OUT 方向 ACL，仅支持匹配知名报文（单播、组播），不支持匹配未知名单播，即对于未知名报文或者广播报文，端口上配置的 OUT 方向 ACL 不生效。
- ✅ 交换机设备上，输入 ACL 和 DOT1X，全局 IP+MAC 绑定，端口安全，IP SOURCE GUARD 共用时，PERMIT 和默认 DENY 的 ACE 不生效，其他 DENY 表项的 ACE 正常生效。

- ✓ 交换机设备上，输入 ACL 和 QOS 共用时，PERMIT ACE 不生效，其他 DENY 表项的 ACE 正常生效；默认 DENY 的表项在 QOS 表项的后面生效。
- ✓ 交换机设备上，通过 **norgos-security compatible** 命令来使得基于端口的输入 ACL 和 DOT1X，全局 IP+MAC 绑定，端口安全，IP SOURCE GUARD 共用时，PERMIT，DENY 表项同时生效。
- ✓ 交换机设备上，ACL 同时应用于多个 SVI 的 IN 方向后，再添加 ACL 中的 ACE，保存配置后重启，由于硬件容量的原因，可能导致某几个 SVI 上的 ACL 无法配置上。

功能特性

功能特性	作用
IP访问列表	可以根据 IPv4 报文头部的三层或四层信息对进出设备的 IPv4 报文进行控制。
MAC扩展访问列表	可以根据以太网报文的二层头部信息对进出设备的二层报文进行控制。

1.3.1 IP访问列表

IP 访问列表主要用于对进出设备的 IPv4 报文进行精细化控制，用户可以根据实际需要阻止或允许特定的 IPv4 报文进入网络，从而实现控制 IP 用户访问网络资源的目的。

工作原理

在 IP 访问列表中定义一系列的 IP 访问规则，然后将访问列表应用在接口的入方向或出方向上，当然还可以对 IP 访问列表进行全局应用，IPv4 报文进出设备时，设备就会通过判断报文是否与规则匹配来决定是否转发或阻断报文。

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

基本访问列表包括标准 IP 访问列表和扩展 IP 访问列表，访问列表中定义的典型规则主要包含以下匹配域：

- 源 IP 地址

- 目的 IP 地址
- IP 协议号
- 四层源端口号或 ICMP type
- 四层目的端口号或 ICMP code

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) 可以对上述匹配域进行组合来控制报文的转发或阻断。

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。

- ✔ 路由类产品上, ACL 规则中的 ICMP code 匹配域对于 ICMP type 为 3 的 ICMP 报文无效。如果 ACL 规则中配置了要匹配 ICMP 报文的 code 字段, 当 type 为 3 的 ICMP 报文进入设备执行 ACL 匹配时, 匹配结果可能与预期的不一样。

📌 隐含“拒绝所有数据流”规则语句

在每个 IP 访问列表的末尾隐含着一条“拒绝所有数据流”规则语句, 因此如果分组与任何规则都不匹配, 将被拒绝。

如下例:

```
access-list 1 permit host 192.168.4.12
```

此列表只允许源主机为 192.168.4.12 的报文通过 其它主机都将被拒绝。因为这条访问列表最后包含了一条规则语句 `access-list 1 deny any`。

又如:

```
access-list 1 deny host 192.168.4.12
```

如果列表只包含以上这一条语句, 则任何主机报文通过该端口时都将被拒绝。

- ❗ 在定义访问列表的时候, 要考虑到路由更新的报文。由于访问列表末尾“拒绝所有数据流”, 可能导致所有的路由更新报文被阻断。

📌 输入规则语句的顺序

加入的每条规则都被追加到访问列表的最后 (但在默认规则语句之前), 访问列表规则语句的输入次序非常重要, 它决定了该规则语句在访问列表中的优先级, 设备在决定转发还是阻断报文时, 是按规则语句创建的次序将进行比较的, 找到匹配的规则语句后, 便不再检查其他规则语句。

假设创建了一条规则语句, 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。

相关配置

配置 IP 访问列表

缺省情况下，设备上无任何 IP 访问列表。

在配置模式下使用 `ip access-list { standard | extended } {acl-name | acl-id}` 命令可以创建一个标准 IP 访问列表或扩展 IP 访问列表，并进入标准或扩展 IP 访问列表模式。

配置 IP 访问列表匹配规则

缺省情况下，创建的 IP 访问列表中会有一条隐含的 deny 所有 IPv4 报文的匹配规则，这条表项对用户不可见，但当将访问列表应用在接口上时，就会生效，也就是会丢弃所有 IPv4 报文，因此，如果用户想允许某些特定的 IPv4 报文进出设备，就得往访问列表中配置一些匹配规则。

对于标准 IP 访问列表，可以通过以下方式配置匹配规则：

对于扩展 IP 访问列表，可以通过以下方式配置匹配规则：

- 不管是命名的扩展 IP 访问列表，还是数值索引的扩展 IP 访问列表，都可以在扩展 IP 访问列表模式下使用 `[sn] { permit | deny } protocol { host source | any | source source-wildcard } { host destination | any | destination destination-wildcard } [precedence precedence] [time-range time-range-name]` 命令为访问列表配置一条匹配规则。
- 数值索引的扩展 IP 访问列表，除了可以在扩展 IP 访问列表模式下使用前面提到的命令配置匹配规则外，还可以在配置模式下使用 `access-list acl-id { permit | deny } protocol { host source | any | source source-wildcard } { host destination | any | destination destination-wildcard } [precedence precedence] [time-range time-range-name]` 命令为标准 IP 访问列表配置一条匹配规则。

应用 IP 访问列表

缺省情况下，设备上的所有接口下都没有应用 IP 访问列表，也就是说 IP 访问列表不会对进出设备的 IP 报文进行匹配过滤。

在接口下使用 `ip access-group {acl-id | acl-name} in` 命令可以让一个标准 IP 访问列表或扩展 IP 访问列表在指定的接口上生效。

1.3.2 MAC 扩展访问列表

MAC 扩展访问列表主要是基于报文的二层头部来对进出设备的报文进行精细化控制，用户可以根据实际需要阻止或允许特定的二层报文进入网络，从而实现控制保护网络资源不受攻击或者基于些控制用户访问网络资源的目的。

工作原理

在 MAC 扩展访问列表中定义一系列的 MAC 访问规则，将访问列表应用在接口的入方向或出方向上，报文进出设备时，设备就会通过判断报文是否与规则匹配来决定是否转发或阻断报文。

要在设备上配置 MAC 扩展访问列表，必须给访问列表指定一个唯一的名称或编号，以便唯一标识每个访问列表。下表列出可以使用编号来指定 MAC 扩展访问列表编号范围。

协议	编号范围

MAC 扩展访问列表	700-799
------------	---------

MAC 扩展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

从上面的规则字段可以看出，MAC 扩展访问列表（编号 700 -799）主要是根据源或目的 MAC 地址以及报文的以太网类型来匹配报文分组的。

对于单一的 MAC 扩展访问列表来说，可以使用多条独立的访问列表语句来定义多种规则，其中所有的语句引用同一个编号或名字，以便将这些语句绑定到同一个访问列表。不过，使用的语句越多，阅读和理解访问列表就越来越困难。

📌 隐含“拒绝所有数据流”规则语句

在每个 MAC 扩展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 700 permit host 00d0.f800.0001 any
```

此列表只允许来自 MAC 地址为 00d0.f800.0001 的主机发出的报文通过，来自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 700 deny any any`。

相关配置

📌 配置 MAC 扩展访问列表

缺省情况下，设备上无任何 MAC 扩展访问列表。

在配置模式下使用 `mac access-list extended{acl-name | acl-id}` 命令可以创建一个 MAC 扩展访问列表，并进入 MAC 扩展访问列表模式。

📌 配置 MAC 扩展访问列表匹配规则

缺省情况下，创建的 MAC 扩展访问列表中会有一条隐含的 deny 所有二层报文的匹配规则，这条表项对用户不可见，但当将访问列表应用在接口上时，就会生效，也就是会丢弃所有二层报文，因此，如果用户想允许某些特定的二层报文进出设备，就得往访问列表中配置一些匹配规则。

可以通过以下方式配置匹配规则：

- 不管是命名的 MAC 扩展访问列表，还是数值索引的 MAC 扩展访问列表，都可以在 MAC 扩展访问列表模式下使用 `[sn]{ permit |deny }{any|hostsrc-mac-addr | src-mac-addrmask}{any|hostdst-mac-addr | dst-mac-addrmask}[ethernet-type] [time-range tm -rng-name]`命令为访问列表配置一条匹配规则。
- 数值索引的 MAC 扩展访问列表，除了可以在 MAC 扩展访问列表模式下使用前面提到的命令配置匹配规则外，还可以在配置模式下使用 `access-list acl-id{ permit |deny }{any|hostsrc-mac-addr | src-mac-addrmask}{any|hostdst-mac-addr | dst-mac-addrmask}[ethernet-type] [time-range $time$ -range-name]`命令为 MAC 扩展访问列表配置一条匹配规则。

应用 MAC 扩展访问列表

缺省情况下，设备上的所有接口都没有应用 MAC 扩展访问列表，也就是说创建的 MAC 扩展访问列表不会对进出设备的二层报文进行匹配过滤。

在接口下使用 `mac access-group {acl-id | acl-name} in` 命令可以让一个 MAC 扩展访问列表在指定的接口上生效。


1.4 产品说明



NBS200/2000 -E 系列产品支持此功能, NBS200/2000 -S 系列产品不支持此功能。

1.5 配置详解

配置项	配置建议&相关命令	
配置IP访问列表功能	可选配置。用于匹配过滤 IPv4 报文。	
	<code>ip access-liststandard</code>	配置 IP 标准访问列表
	<code>ip access-listextended</code>	配置 IP 标准访问列表
	<code>permit host any time-range</code>	配置 permit 类型的 IP 标准访问列表规则
	<code>deny host any time-range</code>	配置 deny 类型的 IP 标准访问列表规则
	<code>deny host any host any tos dscp precedence fragment time-range</code>	配置 deny 类型的 IP 扩展访问列表规则
	<code>ip access-group in</code>	应用 IP 标准或 IP 扩展访问列表
配置 MAC 扩展访问列表	可选配置。用于匹配过滤二层报文	
	<code>mac access-listextended</code>	配置 MAC 扩展访问列表
	<code>deny any host any host cos inner time-range</code>	配置 deny 类型的 MAC 扩展访问列表规则
	<code>mac access-group in</code>	应用 MAC 扩展访问列表

配置访问列表注释信息	 可选配置。用于为访问列表或访问列表规则配置注释信息便于用户识别。	
	<code>access-list list-remark</code>	在全局模式为访问列表配置注释信息。

1.5.1 配置IP访问列表

配置效果

通过配置 IP 访问列表，并将访问列表应用到设备的接口上，就可以对在该接口进出的所有 IPv4 报文进行控制，禁止或允许特定的 IPv4 报文进入网络，从而实现控制 IP 用户访问网络资源的目的。

注意事项

无

配置方法

配置 IP 访问列表

- 必须配置。要实际针对 IPv4 用户访问网络资源的控制，首先必须配置 IP 访问列表。
- 可以根据用户的分布情况，在接入、汇聚或核心设备上配置。IP 访问列表只对被配置的设备上有效，不会影响网络中的其他设备。

配置 IP 访问列表规则

- 可选配置。访问列表里允许无规则，没有配置规则时，默认禁止所有 IPv4 报文进入设备。

应用 IP 访问列表

- 必须配置。要使得 IP 访问列表真正生效，就必须将 IP 访问列表应用到设备的特定接口上。
- 可以根据用户的分布，在接入、汇聚或核心设备的指定接口上应用 IP 访问列表。

检验方法

可以通过以下方法检验 IP 访问列表的配置效果：

- 通过 ping 的方式检查 IP 访问列表是否真的在指定接口上生效。比如，IP 访问列表里配置了禁止某个 IP 主机或某个 IP 范围的主机不允许访问网络，通过 ping 的方式检验是否真的 ping 不通来验证。
- 通过访问网络相关资源的方式来检验 IP 访问列表是否真的在指定接口上生效，比如访问 internet 网，或通过 ftp 访问网络上的 ftp 资源等。

相关命令

配置 IP 访问列表

【命令格式】 **ip access-list { standard | extended } {acl-name | acl-id}**

【参数说明】 **standard**: 该选项若被配置, 表示要创建一个标准 IP 访问列表。

extended: 该选项若被配置, 表示要创建一个扩展 IP 访问列表。

acl-name: 该选项若被配置, 表示创建一个命名的标准 IP 或扩展 IP 访问列表, 长度范围[1, 99]。访问列表名称不能以数字 0 - 9 开头, 也不能为 “in” 或 “out”。

acl-id: 为访问列表编号, 以此来唯一标识一条访问列表, 该选项若被配置, 表示创建一个数值索引的标准 IP 或扩展 IP 访问列表, 如果创建的是标准 IP 访问列表, **acl-id** 的取值范围为 1-99, 1300 - 1999, 如果创建的是扩展 IP 访问列表, **acl-id** 的取值范围为 100-199, 2000 - 2699。

【命令模式】 全局配置模式

【使用指导】 此命令可以用来配置标准 IP 或扩展 IP 访问列表, 并进入标准 IP 或扩展 IP 访问列表配置模式。如果只想通过检查报文的源 IP 地址来控制用户的网络资源访问权限, 那么可以配置标准 IP 访问列表; 如果想通过检查报文的源 IP 地址、目的 IP 地址、报文的协议号、TCP/UDP 源或目的端口号来控制用户的网络资源访问权限, 那么就需要配置扩展 IP 访问列表。

配置 IP 访问列表规则

- 为标准 IP 访问列表配置规则。

有两种方式可以为标准 IP 访问列表配置规则：

【命令格式】 **[sn] { permit | deny } { hostsource | any | source source-wildcard } [time-range time-range-name]**

【参数说明】 **sn**: 为规则表项的序号, 取值范围为[1, 2147483647]。这个序号决定了这条规则表项在该访问列表中的优先级, 序号越小, 优先级越大, 优先级大的会优先去匹配报文。如果配置匹配规则时没有指定序号, 系统会自动分配一个序号, 序号的分配原则为在当前访问列表最后一条匹配规则的序列基础之上加上一个递增值, 递增值默认为 10, 假设当前访问列表最后一条匹配规则的序号为 100, 则缺省情况下新增的这条匹配规则序号就为 11, 此外, 递增值是可以通过命令调整的。

permit: 该选项若被配置, 表示本规则属于允许通过类的;

deny: 该选项若被配置, 关键字表示本规则属于禁止通过类的;

hostsource: 该选项若被配置, 表示要匹配源 IP 为某一台主机发出的 IP 报文;

any: 该选项若被配置, 表示要匹配任意主机发出的 IP 报文;

*source**source-wildcard*: 该选项若被配置, 表示要匹配某一个 IP 网段的内主机发出的报文;

*time-range**time-range-name*: 该选项若被配置, 表示该匹配规则关联了一个时间区, 只有在指定的时间区间内该规则才会生效, 否则不生效, 更多关于关时间区的描述, 请参考 *time range* 的配置手册

【命令模式】 标准 IP 访问列表模式

【使用指导】 此命令在标准 IP 访问列表模式下为访问列表配置规则, 该访问列表可以是命名访问列表, 也可以是数字索引的访问列表。

【命令格式】 **access-list** *acl-id* { **permit** | **deny** } {*host**source*| **any** | *source**source-wildcard* } [*time-range**tm-rng-name*]

【参数说明】 *acl-id*: 数值索引访问列表的编号, 以此来唯一标识一条访问列表。取值范围为: 1-99, 1300 - 1999

permit: 该选项若被配置, 表示本规则属于允许通过类的;

deny: 该选项若被配置, 关键字表示本规则属于禁止通过类的;

*host**source*: 该选项若被配置, 表示要匹配源 IP 为某一台主机发出的 IP 报文;

any: 该选项若被配置, 表示要匹配任意主机发出的 IP 报文;

*source**source-wildcard*: 该选项若被配置, 表示要匹配某一个 IP 网段的内主机发出的报文;

*time-range**time-range-name*: 该选项若被配置, 表示该匹配规则关联了一个时间区, 只有在指定的时间区间内该规则才会生效, 否则不生效, 更多关于关时间区的描述, 请参考 *time range* 的配置手册

【命令模式】 标准 IP 访问列表模式

【使用指导】 此命令在配置模式下为数字索引的 IP 访问列表配置规则。这种配置方式无法为命名的标准 IP 访问列表配置规则。

- 为扩展 IP 访问列表配置规则。

有两种方式可以为扩展 IP 访问列表配置规则:

【命令格式】 [*sn*] { **permit** | **deny** } *protocol*{*host**source*| **any** | *source**source-wildcard* } {*host**destination* | **any** | *destination* *destination-wildcard* }[[**precedence***precedence*] [*time-range**time-range-name*]

【参数说明】 *sn*: 规则表项的序号, 取值范围为[1, 2147483647]。这个序号决定了这条规则表项在该访问列表中的优先级, 序号越小, 优先级越大, 优先级大的会优先去匹配报文。如果配置匹配规则时没有指定序号, 系统会自动分配

一个序号,序号的分配原则为在当前访问列表最后一条匹配规则的序列基础之上加上一个递增值,递增值默认为 10,假设当前访问列表最后一条匹配规则的序号为 100,则缺省情况下新增的这条匹配规则序号就为 11,此外,递增值是可以通过命令调整的

permit: 该选项若被配置,表示本规则属于允许通过类的;

deny: 该选项若被配置,关键字表示本规则属于禁止通过类的;

protocol: IP 协议号,取值范围[0, 255];为方便使用,系统提供了常用 IP 协议号的简称以取代对应的 IP 协议号具体数值,包括 eigrp、gre、icmp、igmp、ip、ipinip、nos、ospf、tcp、udp。

hostsource: 该选项若被配置,表示要匹配源 IP 为某一台主机发出的 IP 报文;

source-source-wildcard: 该选项若被配置,表示要匹配某一个 IP 网段的内主机发出的报文;

hostdestination: 该选项若被配置,表示要匹配目的 IP 为某一台特定主机的 IP 报文;**any** 关键字表示要匹配发往任意主机的 IP 报文。

destination destination-wildcard: 该选项若被配置,表示要匹配目标为某一个 IP 网段主机的报文。

any: 该选项若被配置,表示要匹配任意主机发出的 IP 报文或者要匹配发往任意主机的 IP 报文;

precedenceprecedence: 该选项若被配置,表示要匹配 IP 报文头部中的优先级域。

tos tos: 该选项若被配置,表示要匹配 IP 报文头部中的服务类型域。

dscp dscp: 该选项若被配置,表示要匹配 IP 报文头部的 dscp 域。

fragment: 该选项若被配置,表示只要匹配非首片的 IP 分片报文。

time-range time-range-name: 该选项若被配置,表示该匹配规则关联了一个时间区,只有在指定的时间区间内该规则才会生效,否则不生效,更多关于时间区的描述,请参考 time range 的配置手册

【命令模式】 扩展 IP 访问列表模式

【使用指导】 此命令在扩展 IP 访问列表模式下为访问列表配置规则,该访问列表可以是命名访问列表,也可以是数字索引的访问列表。

【命令格式】 **access-list acl-id { permit | deny } protocol{hostsource| any | source-source-wildcard } {hostdestination | any | destination destination-wildcard }[precedenceprecedence] [time-range time-range-name]**

【参数说明】 **acl-id:** 数值索引访问列表的编号,以此来唯一标识一条访问列表。取值范围为:100-199,2000-2699

sn: 规则表项的序号,取值范围为[1, 2147483647]。这个序号决定了这条规则表项在该访问列表中的优先级,序号越小,优先级越大,优先级大的会优先去匹配报文。如果配置匹配规则时没有指定序号,系统会自动分配一个序号,序号的分配原则为在当前访问列表最后一条匹配规则的序列基础之上加上一个递增值,递增值默认

为 10，假设当前访问列表最后一条匹配规则的序号为 100，则缺省情况下新增的这条匹配规则序号就为 11，此外，递增值是可以通过命令调整的

permit: 该选项若被配置，表示本规则属于允许通过类的；

deny: 该选项若被配置，关键字表示本规则属于禁止通过类的；

protocol: IP 协议号，取值范围[0, 255]；为方便使用，系统提供了常用 IP 协议号的简称以取代对应的 IP 协议号具体数值，包括 eigrp、gre、icmp、igmp、ip、ipinip、nos、ospf、tcp、udp。

hostsource: 该选项若被配置，表示要匹配源 IP 为某一台主机发出的 IP 报文；

source-source-wildcard: 该选项若被配置，表示要匹配某一个 IP 网段的内主机发出的报文；

hostdestination: 该选项若被配置，表示要匹配目的 IP 为某一台特定主机的 IP 报文；**any** 关键字表示要匹配发往任意主机的 IP 报文。

destination destination-wildcard: 该选项若被配置，表示要匹配目标为某一个 IP 网段主机的报文。

any: 该选项若被配置，表示要匹配任意主机发出的 IP 报文或者要匹配发往任意主机的 IP 报文；

precedenceprecedence: 该选项若被配置，表示要匹配 IP 报文头部中的优先级域。

tos tos: 该选项若被配置，表示要匹配 IP 报文头部中的服务类型域。

dscp dscp: 该选项若被配置，表示要匹配 IP 报文头部的 dscp 域。

fragment: 该选项若被配置，表示只要匹配非首片的 IP 分片报文。

time-range time-range-name: 该选项若被配置，表示该匹配规则关联了一个时间区，只有在指定的时间区间内该规则才会生效，否则不生效，更多关于时间区的描述，请参考 time range 的配置手册

【命令模式】 扩展 IP 访问列表模式

【使用指导】 此命令在配置模式下为数字索引的 IP 访问列表配置规则。这种配置方式无法为命名的标准 IP 访问列表配置规则。

应用 IP 访问列表

【命令格式】 **ip access-group {acl-id | acl-name} in**

【参数说明】 **acl-id:** 该选项若被配置，表示要将一个数值索引的标准 IP 或扩展 IP 访问列表应用在接口上。

acl-name: 该选项若被配置，表示要将一个命名的标准 IP 或扩展 IP 访问列表应用在接口上。

in: 该选项若被配置，表示这个访问列表对进入该接口的 IP 报文进行控制。

【命令模式】 接口模式

【使用指导】 此命令可以让 IP 访问列表在指定的接口

上生效，同时需要指定对进入设备的报文生效，还是从设备转发出去的报文生效。

1.5.2 配置MAC扩展访问列表

配置效果

通过配置 MAC 扩展访问列表，并将访问列表应用到设备的接口上，就可以对在该接口上进出的所有二层报文进行控制，禁止或允许特定的二层报文进入网络，从而实现基于二层报文头来控制用户访问网络资源的目的。

注意事项

无

配置方法

▾ 配置 MAC 扩展访问列表

- 必须配置。要基于二层报文头信息（比如用户 PC 的 MAC 地址）控制用户访问网络资源的权限，首先必须配置 MAC 扩展访问列表。
- 可以根据用户的分布情况，在接入、汇聚或核心设备上配置。MAC 扩展访问列表只在被配置的设备上有效，不会影响网络中的其他设备。

▾ 配置 MAC 扩展访问列表规则

- 可选配置。访问列表里允许无规则，没有配置规则时，默认禁止所有以太网二层报文进入设备。

▾ 应用 MAC 扩展访问列表

- 必须配置。要使得 MAC 扩展访问列表真正生效，就必须将 MAC 扩展访问列表应用到设备的特定接口上。
- 可以根据用户的分布，在接入、汇聚或核心设备的指定接口上应用 MAC 扩展访问列表。

检验方法

可以通过以下方法检验 MAC 扩展访问列表的配置效果：

- 如果 MAC 扩展访问列表希望放过或过滤某些 IP 报文，可以通过 ping 的方式检查这样的 MAC 扩展访问列表规则是否真的在指定接口上生效。比如，MAC 扩展访问列表里配置了禁止以太网类型为 0x0800 即 IP 报文从接口进入设备，可以通过 ping 的方式检验是否真的 ping 不通来验证。

- 如果 MAC 扩展访问列表希望放过或过滤某些非 IP 报文，比如 ARP 报文，这种报文也可以通过 ping 的方式检查这样的 MAC 扩展访问列表规则是否真的在指定接口上生效，比如想过滤掉 ARP 报文，可以通过 ping 的方式检验是否真的 ping 不通来验证。
- 另外，还可以通过构造符合指定特征的二层报文来检验 MAC 扩展访问列表是否真的生效。典型地可以使用两台 PC 机，一台构造二层报文并发送，另一台开启抓包软件抓包，根据访问列表规则指定的动作检查报文的转发是否如预期（转发或不转发）。

相关命令

配置 MAC 扩展访问列表

【命令格式】 **mac access-list extended** {*acl-name* | *acl-id*}

【参数说明】 *acl-name*: 该选项若被配置，表示创建一个命名的 MAC 扩展访问列表，长度范围[1, 99]。访问列表名称不能以数字 0 - 9 开头，也不能为 "in" 或 "out"。

acl-id: 为访问列表编号，以此来唯一标识一条访问列表，该选项若被配置，表示创建一个数值索引的 MAC 扩展访问列表，取值范围为 700-799。

【命令模式】 全局配置模式

【使用指导】 此命令可以用来配置 MAC 扩展访问列表，并进入 MAC 扩展访问列表配置模式。如果想通过检查以太网报文的二层信息来控制用户的网络资源访问权限，那么就可以配置 MAC 扩展访问列表。

配置 MAC 扩展访问列表规则

有两种方法为 MAC 扩展访问列表配置规则：

- 在 MAC 扩展访问列表模式中配置规则

【命令格式】 [*sn*] { **permit** | **deny** }{*any*|*host**src-mac-addr* | *src-mac-addr**mask*}{*any*|*host**dst-mac-addr* | *dst-mac-addr**mask*}[*ethernet-type*] [**time-range***tm-rng-name*]

【参数说明】 *sn*: 为规则表项的序号，取值范围为[1, 2147483647]。这个序号决定了这条规则表项在该访问列表中的优先级，序号越小，优先级越大，优先级大的会优先去匹配报文。如果配置匹配规则时没有指定序号，系统会自动分配一个序号，序号的分配原则为在当前访问列表最后一条匹配规则的序列基础之上加上一个递增值，递增值默认为 10，假设当前访问列表最后一条匹配规则的序号为 100，则缺省情况下新增的这条匹配规则序号就为 11，此外，递增值是可以通命令调整的。

permit: 该选项若被配置，表示本规则属于允许通过类的；

deny: 该选项若被配置，关键字表示本规则属于禁止通过类的；

any: 该选项若被配置，表示要匹配任意主机发出的二层报文；

hostsrc-mac-addr: 该选项若被配置, 表示要匹配源 MAC 为某一台主机发出的二层报文;

src-mac-addrmask: 该选项若被配置, 表示对源 MAC 进行取反;

any: 该选项若被配置, 表示要匹配目的为任意主机发出的二层报文;

hostdst-mac-addr: 该选项若被配置, 表示要匹配目的 MAC 为某一台主机的二层报文;

dst-mac-addrmask: 该选项若被配置, 表示对目的 MAC 进行取反;

ethernet-type: 该选项若被配置, 表示要匹配指定以太网类型的二层报文;

time-range*time-range-name*: 该选项若被配置, 表示该匹配规则关联了一个时间区, 只有在指定的时间区间内该规则才会生效, 否则不生效, 更多关于关时间区的描述, 请参考 time range 的配置手册

【命令模式】 MAC 扩展访问列表模式

【使用指导】 此命令在 MAC 扩展访问列表模式下为访问列表配置规则, 该访问列表可以是命名访问列表, 也可以是数字索引的访问列表。

- 在全局模式中为 MAC 扩展访问列表配置规则

【命令格式】 **access-list** *acl-id*{ **deny** }{**any**|**hostsrc-mac-addr** | *src-mac-addrmask*}{**any**|**hostdst-mac-addr** | *dst-mac-addrmask*}[*ethernet-type*] [**time-range***tm-rng-name*]

【参数说明】 *acl-id*: 数值索引访问列表的编号, 以此来唯一标识一条访问列表。取值范围为: 700-799

permit: 该选项若被配置, 表示本规则属于允许通过类的;

deny: 该选项若被配置, 关键字表示本规则属于禁止通过类的;

hostsrc-mac-addr: 该选项若被配置, 表示要匹配源 MAC 为某一台主机发出的二层报文;

src-mac-addrmask: 该选项若被配置, 表示对源 MAC 进行取反;

any: 该选项若被配置, 表示要匹配目的为任意主机发出的二层报文;

hostdst-mac-addr: 该选项若被配置, 表示要匹配目的 MAC 为某一台主机的二层报文;

dst-mac-addrmask: 该选项若被配置, 表示对目的 MAC 进行取反;

ethernet-type: 该选项若被配置, 表示要匹配指定以太网类型的二层报文;

time-range*time-range-name*: 该选项若被配置, 表示该匹配规则关联了一个时间区, 只有在指定的时间区间内该规则才会生效, 否则不生效, 更多关于关时间区的描述, 请参考 time range 的配置手册。

【命令模式】 全局模式

【使用指导】 此命令在配置模式下为数字索引的 MAC 扩展访问列表配置规则。这种配置方式无法为命名的 MAC 扩展访问列表配置规则。

应用 MAC 扩展访问列表

【命令格式】 **mac access-group {acl-id|acl-name } in**

【参数说明】 **acl-id:** 该选项若被配置，表示要将一个数值索引的 MAC 扩展访问列表应用在接口上。

acl-name: 该选项若被配置，表示要将一个命名的 MAC 扩展访问列表应用在接口上。

in: 该选项若被配置，表示这个访问列表对进入该接口的二层报文进行控制。

【命令模式】 接口模式

【使用指导】 此命令可以让 MAC 扩展访问列表在指定的接口上生效，同时需要指定对进入设备的报文生效，还是从设备转发出去的报文生效。

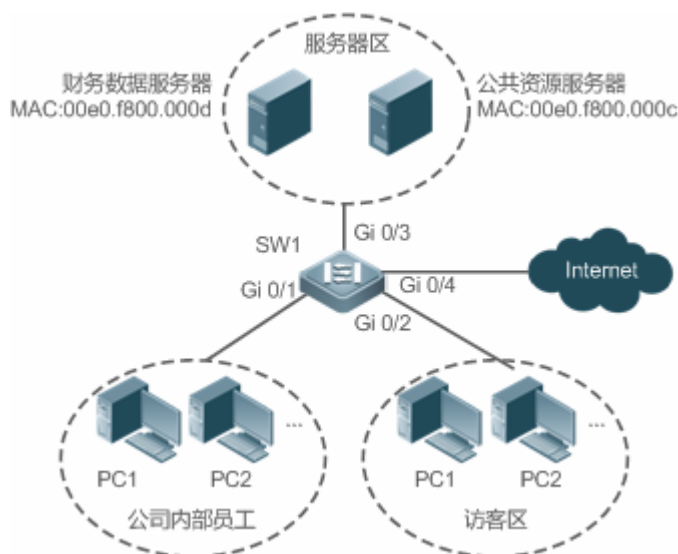
配置举例

以下配置举例，仅介绍与 ACL 相关的配置。

通过 MAC 扩展访问列表，限制来访客户可访问的资源

【网络环境】

图 1-3



- 【配置方法】
- 配置 MAC 扩展访问列表
 - 在 MAC 扩展访问列表中添加访问规则
 - 将 MAC 扩展访问列表应用在连接访客区接口的出方向上,允许访客 PC 访问 Internet 以及公司内部的公共服务器,但不允许访问公司的账务数据服务器,即禁止访问 MAC 地址为 00e0.f800.000d 的服务器。

SW1

```
sw1(config)#mac access-list extended 700
sw1(config-mac-nacl)#deny any host 00e0.f800.000d
sw1(config-mac-nacl)#permit any any
sw1(config-mac-nacl)#exit
sw1(config)#int gigabitEthernet 0/2
sw1(config-if-GigabitEthernet 0/2)#mac access-group 700in
```

- 【检验方法】
- 从访客 PC 机上 ping 财务数据服务器,确认 ping 不通。
 - 从访问 PC 机上 ping 公共资源服务器,确认可以 ping 得通。
 - 在访问 PC 机上访问 Internet,比如访问百度,确认可以打开主页。

SW1

```
sw1(config)#show access-lists
mac access-list extended 700
10 deny any host 00e0.f800.000d etype-any
20 permit any any etype-any
sw1(config)#show access-group
mac access-group 700in
Applied On interface GigabitEthernet 0/2
```

1.5.3 配置访问列表注释信息

配置效果

在实际的网络维护过程中,如果配置了很多访问列表且没有为这些访问列表配置注释信息,时间一长往往会难以区分这些访问列表的用途。为访问列表配置注释信息,可以方便理解 ACL 用途。

注意事项

无

配置方法

配置访问列表

- 必须配置。要实现安全通道功能，首先要配置访问列表，访问列表的配置方法请参考相关章节说明。
- 可以根据用户的分布情况，在接入、汇聚或核心设备上配置。配置仅在本设备上有效，不会影响网络中的其他设备。

配置访问列表注释信息

- 可选配置。为便于管理和理解所配置的访问列表，可以为访问列表配置注释信息。

配置访问列表规则

- 可选配置。访问列表里允许无规则，没有配置规则时，相当于安全通道功能不生效。访问列表规则配置请参考相关章节的说明。

配置访问列表规则注释信息

- 可选配置。为便于理解所配置的访问列表，除了可以为访问列表本身配置注释信息外，还可以为规则配置注释信息。

检验方法

可以通过在设备上使用 **show access-lists** 命令验证访问列表注释信息。

相关命令

配置访问列表

访问列表的配置方法请参考

IP 访问列表、MAC 扩展访问列表的相关章节说明。

配置访问列表注释信息

有以下方式为访问列表配置注释信息：

【命令格式】 **access-list** *acl-id* **list-remark***comment*

【参数说明】 *acl-id*: 访问列表编号

comment: 注释信息。长度[1, 100]，超过 100 个字符将被截短至 100 个字符

【命令模式】 配置模式

【使用指导】 通过该命令为指定的访问列表配置注释信息

配置访问列表规则

访问列表规则的配置方法请参考

IP 访问列表、MAC 扩展访问列表的相关章节说明。

配置访问列表规则注释信息

【命令格式】 **access-list** *acl-id sn remarkcomment*

【参数说明】 *acl-id*: 访问列表编号

comment: 注释信息。长度[1, 100]，超过 100 个字符将被截短至 100 个字符

sn: 需要注释规则的序列号

【命令模式】 配置模式

【使用指导】 通过该命令为访问列表规则添加注释信息，若 *sn* 未配置默认注释访问列表中最后一个规则

有以下方式为访问列表规则配置注释信息：

【命令格式】 **access-list** *acl-id remarkcomment*

【参数说明】 *acl-id*: 访问列表编号

comment: 注释信息。长度[1, 100]，超过 100 个字符将被截短至 100 个字符

【命令模式】 配置模式

【使用指导】 通过该命令为访问列表规则添加注释信息

配置举例

无

1.6 监视与维护


清除各类信息

-

查看运行情况

作用	命令
查看基本访问列表	show access-lists [<i>acl-id</i> <i>acl-ame</i>] [summary]
显示接口上应用的访问列表配置信息。	show access-group [<i>interface</i> <i>interface-name</i>]
显示接口上应用的 IP 访问列表配置信息。	show ip access-group [<i>interface</i> <i>interface-name</i>]
显示接口上应用的 MAC 扩展访问列表配置信息。	show mac access-group [<i>interface</i> <i>interface-name</i>]

查看调试信息

 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
监视访问列表运行过程信息	debug acl acld event
调试查看 ACL 客户端的信息	debug acl acld client-show
调试查看所有 ACL 客户端创建的访问列表信息	debug acl acld acl-show



配置指南-可靠性

本分册介绍可靠性配置指南相关内容，包括以下章节：

1. RLDP

1 RLDP

1.1 概述

RLDP (Rapid Link Detection Protocol , 快速链路检测协议) 是一种以太网链路故障检测协议 , 用于快速检测单向链路故障、双向链路故障以及下联环路故障。如果发现故障存在 , RLDP 会根据用户配置的故障处理方式自动关闭或通知用户手工关闭相关端口 , 以避免流量的错误转发或者防止以太网二层环路。

协议规范

- 无

1.2 典型应用

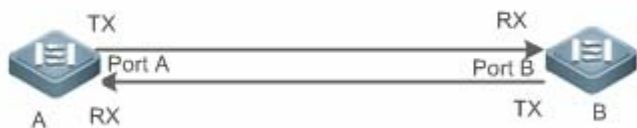
典型应用	场景描述
单向链路检测	检测链路单向故障
双向链路检测	检测链路双向故障
下联环路检测	检测链路环路故障

1.2.1 单向链路检测

应用场景

如下图所示 , 设备 A 与设备 B 之间通过光纤相连 , 图中的两条线分别表示光纤的 Tx 线与 Rx 线 , A 与 B 分别使能 RLDP 的单向链路检测功能。如果端口 A 的 Tx 与端口 B 的 Rx 或者端口 A 的 Rx 与端口 B 的 Tx 中任意一个出现故障 , 那么协议可以检测出单向故障并做出相应的处理。故障如果被恢复 , 管理员可以手工在 A 和 B 上恢复协议状态并重新开始检测。

图 1-1



- 【注释】 A、B 为二层或者三层交换机。
A 上的 Port A 的 TX 与 B 上的 Port B 的 RX 连接。
A 上的 Port A 的 RX 与 B 上的 Port A 的 TX 连接。

功能部署

- 全局配置 RLDP 使能。
- 接口下配置 RLDP 的单向链路检测功能并指定单向故障发生时的处理方式。

1.2.2 双向链路检测

应用场景

如下图所示，设备 A 与设备 B 之间通过光纤相连，图中的两条线分别表示光纤的 Tx 线与 Rx 线，A 与 B 分别使能 RLDP 的双向链路检测功能。如果端口 A 的 Tx 与端口 B 的 Rx 以及端口 A 的 Rx 与端口 B 的 Tx 同时出现故障，那么协议可以检测出双向故障并做出相应的处理。故障如果被恢复，管理员可以手工在 A 和 B 上恢复协议状态并重新开始检测。

图 1-2



- 【注释】 A、B 为二层或者三层交换机。
A 上的 Port A 的 TX 与 B 上的 Port B 的 RX 连接。
A 上的 Port A 的 RX 与 B 上的 Port A 的 TX 连接。

功能部署

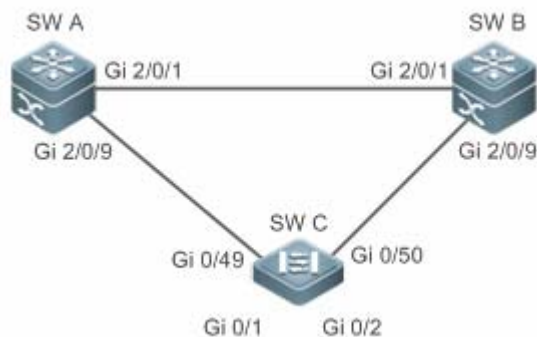
- 全局配置 RLDP 使能。
- 接口下配置 RLDP 的双向链路检测功能并指定双向故障发生时的处理方式。

1.2.3 下联环路链路检测

应用场景

如下图所示，设备 A、设备 B 以及设备 C 之间连成网络环路，A 使能 RLDP 的下联环路检测功能，协议此时可以检测出环路故障并做响应的。

图 1-3



【注释】 A、B、C 为二层或者三层交换机。
A、B、C 通过交换口两两互连。

功能部署

- A 上全局配置 RLDP 使能。
- A 与 B 的连接端口、A 与 C 的连接端口分别配置 RLDP 下联环路检测功能并指定环路故障发生时的处理方式。

1.3 功能详解

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，有些情况下物理层虽然处于连通状态并能正常工作，但是实际对应的二层链路却是无法通信或者存在异常。RLDP 协议通过与邻居设备交互探测报文、探测响应报文或者环路报文来识别邻居设备并检测链路是否存在故障。

基本概念

↘ 链路单向故障

光纤交叉连接、一条光纤未连接、一条光纤断路、双绞线中的一条线路断路或者两台设备之间的中间设备出现单向断路等情况下会出现链路单向故障，这种链路一边能通而另一边不能通会导致流量被错误转发或者环路保护协议（比如 STP）功能失效。

↘ 链路双向故障

两条光纤断路、双绞线中的两条线路断路或者两台设备之间的中间设备出现双向断路等情况下会出现链路双向故障，这种链路双向都不通会导致流量被错误的转发。

↘ 链路环路故障

设备下联被用户错误的接入其他设备形成了环路，这种会在网络中引起广播风暴。

↘ RLDP 协议报文

协议定义了三种类型的报文：探测报文（Prob）、探测响应报文（Echo）以及环路报文（Loop）。

- Prob 报文为二层组播报文，用于邻居协商、单向或者双向链路检测，报文的默认封装格式为 SNAP 类型，如果邻居发出的报文格式为 EthernetII 格式则封装方式自动变更为 EthernetII；
- Echo 报文为响应 Prob 报文的二层单播报文，用于单向或者双向链路检测，报文的默认封装格式为 SNAP 类型，如果邻居发出的报文格式为 EthernetII 格式则封装方式自动变更为 EthernetII；
- Loop 报文为二层组播报文，用于下联环路检测，这类报文只会被发送方所接收，报文的封装格式为 SNAP 封装方式。

▾ RLDP 探测间隔及最大探测次数

RLDP 可以配置探测间隔与最大探测次数。探测间隔决定了 Prob 报文与 Loop 报文的发送周期，设备在接收到 Prob 报文后会立即响应 Echo 报文。探测间隔与最大探测次数决定了单向或者双向链路探测的最大探测时间（探测间隔 × 最大探测次数 + 1），最大探测时间内如果无法正确接收到邻居的 Prob 报文或者 Echo 报文可以触发单向或者双向故障的处理。

▾ RLDP 邻居协商

配置了单向或者双向检测功能的端口可以学习到对端设备作为邻居，一个端口支持学习一个邻居，邻居可变化。协商功能启用后，端口下协商到邻居后才开始单向或者双向检测，协商过程中如果成功接收到邻居发送的 Prob 报文就认为协商成功。但是，在已存在故障的情况下才使能协议，会出现无法正常学习邻居而导致检测不能启动，建议此时先恢复链路的错误状态。

▾ RLDP 端口故障时的处理方式

- warning：只打印相关的 Syslog 说明当前的故障端口和故障类型。
- Shutdown SVI：打印 Syslog 的基础上，如果故障端口为物理交换口或者 L2 AP 成员口，那么会根据端口所属的 Access VLAN 或者 Native VLAN 查询出对应的 SVI 并执行 Shutdown 操作。
- 端口违例：打印 Syslog 的基础上，设置故障端口为违例状态，此时端口物理上会进入 Linkdown 状态。
- Block：打印 Syslog 的基础上，设置故障端口的转发状态为 Block，此时端口不对收到的报文进行转发。

▾ RLDP 端口故障后的恢复方式

- 手工执行 Reset：手工将所有故障端口恢复到初始化状态，此时会重新启动链路检测。
- 手工或者自动执行 Errdisable Recovery：手工或者定时（默认每 30s，可配置）恢复所有故障端口到初始化状态并重新启动链路检测。
- 自动恢复：单向或者双向链路检测的情况下，如果指定的故障处理方式不是端口违例，那么可以依赖与邻居交互的 Prob 报文自动恢复到初始化状态并重新启动链路检测。

▾ RLDP 端口状态

- normal：端口下配置启动检测后的状态。
- error：端口下检测出链路故障后的状态，可以是单向、双向或者环路故障导致。

▾ 功能特性

功能特性	作用
建立 RLDP 检测	启用单向、双向或者下联环路检测功能，永远检测单向、双向或者环路故障并进行相应的故障处理。

1.3.1 建立RLDP检测

RLDP 的链路检测模式主要包括单向链路检测、双向链路检测以及下联环路检测等。

工作原理

↘ RLDP 单向链路检测

单向链路检测启动后，端口后周期的发送 Prob 报文并接收邻居响应的 Echo 报文，同时接收邻居的 Prob 报文并及时响应 Echo 报文给邻居。在最大探测时间内，如果只能接收到邻居的 Prob 报文但无法接收到邻居的 Echo 报文或者既不能接收到邻居的 Prob 报文也不能接收到邻居的 Echo 报文，那么会触发单向故障的处理并停止检测。

↘ RLDP 双向链路检测

双向链路检测启动后，端口后周期的发送 Prob 报文并接收邻居响应的 Echo 报文，同时接收邻居的 Prob 报文并及时响应 Echo 报文给邻居。在最大探测时间内，如果既不能接收到邻居的 Prob 报文也不能接收到邻居的 Echo 报文，那么会触发双向故障的处理并停止检测。

↘ RLDP 下联环路检测

下联环路检测启动后，端口会周期的发送 Loop 报文，同一个设备的相同端口或者不同端口接收到 Loop 报文后，如果报文发送端口与接收端口为路由口或者 L3 AP 成员口并且发送口与接收后相同则触发环路故障，或者报文发送端口与接收端口为交换口或者 L2 AP 成员口并且端口的默认 VLAN 相同同时转发状态均为 Forward 则触发环路故障，故障发生后按相应的故障处理方式来处理并停止检测。

相关配置


- 配置 RLDP 检测功能

缺省情况下，检测功能不生效。

使用 RLDP 全局命令 `rldp enable` 和接口命令 `rldp port` 可以启动 RLDP 检测功能，并指定检测类型与故障处理方式。

用户可以根据实际环境通过 `rldp neighbor-negotiation` 指定邻居协商、`rldp detect-interval` 指定探测间隔、`rldp detect-max` 指定探测次数、`rldp reset` 恢复故障端口状态等。

1.4 配置详解

配置项	配置建议&相关命令
配置 RLDP 基本功能	 全局模式，必须配置。配置全局开启 RLDP 探测功能
	<code>rldp enable</code> 全局下启动 RLDP 检测，生效到所有端口。

 接口模式，必须配置。指定接口下的探测类型以及故障处理方式。	
rldp port	端口下启动 RLDP 检测，指定具体的检测类型以及发生故障后的处理方式。
 全局模式，可选配置。指定探测过程中的探测间隔、探测次数、是否需要邻居协商。	
rldp detect-interval	全局修改 RLDP 配置参数，包括探测间隔、最大探测次数以及邻居协商，可生效到所有端口下的 RLDP 检测。
rldp detect-max	
rldp neighbor-negotiation	
 特权模式，可选配置。	
rldp reset	特权下恢复故障端口的状态，可生效到所有端口下的 RLDP 检测。

1.4.1 配置RLDP基本功能

配置效果

- 启用 RLDP 单向、双向或者下联环路检测，用于发现单向、双向或者环路故障。

注意事项

- 对于 AP 成员口上的 RLDP 配置，如果是配置环路检测，则会同步配置到该 AP 的所有成员口，如果是配置单向链路检测和双向链路检测，则直接在 AP 成员口生效。
- 对于物理口加入 AP 的情况，新加入的 AP 成员口的环路检测配置需要和该 AP 现有的成员口的环路检测配置一致。这里分 3 种情况：1) 如果新加入的 AP 成员口没有配置环路检测，而该 AP 现有的成员口有配置环路检测，则新加入的 AP 成员口同步环路检测的配置和检测结果。2) 如果新加入的 AP 成员口有配置环路检测，而该 AP 现在的所有成员口都没有配置环路检测，则新加入的 AP 成员口清除环路检测配置并加入 AP。3) 如果新加入的 AP 成员口的环路检测配置和该 AP 现有的成员口的环路检测配置不一致，则新加入的 AP 成员口同步环路检测的配置和检测结果。
- AP 成员口配置 RLDP 时，故障处理方法只能配置为“shutdown-port”，如果故障处理方法配置为非“shutdown-port”时，将转换成“shutdown-port”的配置并生效。
- 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 探测，如果用户确认故障已经解决，则可以使用 **rldp reset** 命令或者 **errdisable recovery** 命令来恢复并重新启动检测，**errdisable recovery** 的配置可以参考 <<SWITCH-INTF-SCG.doc>>。

配置方法

▾ 全局配置使能

- 必须配置。

- 全局模式下配置，配置后各端口的检测可以启动。

↘ 全局配置邻居协商

- 可选配置。
- 全局模式下配置，配置后各端口检测的启动依赖于邻居协商的成功。

↘ 全局配置探测间隔

- 可选配置。
- 全局模式下配置，可以指定具体的时间间隔。

↘ 全局配置最大探测次数

- 可选配置。
- 全局模式下配置。
- 可以指定具体的最大探测次数。

↘ 接口下配置检测功能

- 必须配置。
- 接口模式下配置。
- 在接口下配置 RLDP 功能，可以选择单向、双向或者下联环路检测类型，同时指定对应的故障处理方式。

↘ 特权下配置恢复所有故障端口状态

- 可选配置。
- 特权模式下配置，配置后可以恢复所有故障状态端口，重新启动检测。

检验方法

- 查看设备的 RLDP 信息，包括全局、端口以及邻居的相关信息。

相关命令

↘ 全局使能 RLDP 检测功能

- 【命令格式】 `rldp enable`
- 【参数说明】 -
- 【命令模式】 全局模式。

【使用指导】 全局启用 RLDP 检测功能。

▾ 接口下启动 RLDP 检测功能

【命令格式】 `rldp port { unidirection-detect | bidirection-detect | loop-detect } { warning | shutdown-svi | shutdown-port | block }`

【参数说明】 **unidirection-detect**：单向链路检测。
bidirection-detect：双向链路检测。
loop-detect：下联环路检测。
warning：故障处理方式为告警。
shutdown-svi：故障处理方式为关闭接口所在的 SVI 口。
shutdown-port：故障处理方式为端口违例。
block：故障处理方式为关闭端口的学习转发能力。

【命令模式】 接口模式

【使用指导】 接口包括：2 层交换口、3 层路由口、L2AP 下的成员口、L3AP 下的成员口等接口。

▾ 全局修改 RLDP 检测参数

【命令格式】 `rldp {detect-interval interval | detect-max num | neighbor-negotiation }`

【参数说明】 **detect-interval interval**：探测间隔。
detect-max num：最大探测次数。
neighbor-negotiation：邻居协商。

【命令模式】 全局模式

【使用指导】 当实际环境变化，需要修改所有 RLDP 检测的参数时，对所有端口生效。

▾ 恢复 RLDP 故障端口状态

【命令格式】 `rldp reset`

【参数说明】 -

【命令模式】 特权模式

【使用指导】 恢复 RLDP 所有故障端口状态到初始状态并重新启动检测。

▾ 查看 RLDP 状态信息

【命令格式】 `show rldp [interface interface-name]`

【参数说明】 *interface-name*：指定要查看的具体接口

【命令模式】 特权模式、全局模式、接口模式

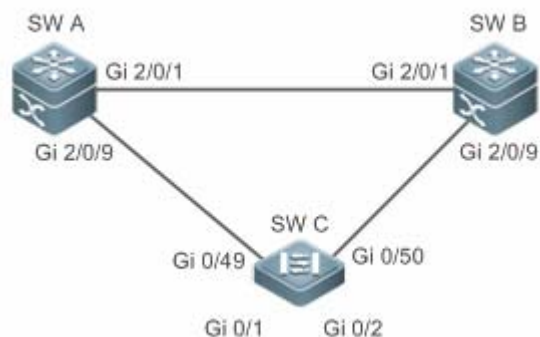
【使用指导】 查看 RLDP 状态信息。

配置举例

▾ 在环网拓扑中开启 RLDP 检测功能

【网络环境】 如下图所示，汇聚与接入为环网拓扑，环网中各设备均开启 STP 来防止环路并提供冗余保护，为了防止环路

图 1-4 中链路出现单向或者双向故障进而导致 STP 协议失效，汇聚设备与汇聚设备之间以及汇聚与接入设备之间启用 RLDP 单向和双向检测，为了防止汇聚设备下联被错误的接入而出现环路，汇聚设备与接入设备的下联端口均开启 RLDP 环路检测；为了防止接入设备下联被错误的接入而出现环路，接入设备的下联端口均开启 RLDP 环路检测



- 【配置方法】
- SW A、SW B 作为汇聚，SW C 作为接入，SW C 下联可以接用户设备，三台设备组成环网拓扑，每台设备开启 STP，STP 配置参考相关配置指南。
 - SW A 开启 RLDP，两个端口需要配置单向和双向链路检测，下联端口需要配置开启环路检测。
 - SW B 开启 RLDP，两个端口需要配置单向和双向链路检测，下联端口需要配置开启环路检测。
 - SW C 开启 RLDP，上联两个端口需要配置单向和双向链路检测，下联两个端口需要配置开启环路检测

A

```
A#configure terminal
A(config)#rldp enable
A(config)#interface GigabitEthernet 2/0/1
A(config-if-GigabitEthernet 2/0/1)#rldp port unidirection-detect shutdown-port
A(config-if-GigabitEthernet 2/0/1)#rldp port bidirection-detect shutdown-port
A(config-if-GigabitEthernet 2/0/1)# exit
A(config)#interface GigabitEthernet 2/0/9
A(config-if-GigabitEthernet 2/0/1)#rldp port unidirection-detect shutdown-port
A(config-if-GigabitEthernet 2/0/1)#rldp port bidirection-detect shutdown-port
A(config-if-GigabitEthernet 2/0/1)#rldp port loop-detect shutdown-port
A(config-if-GigabitEthernet 2/0/1)#exit
```

B

同 A 的配置

C

```
C#configure terminal
C(config)#rldp enable
C(config)#interface GigabitEthernet 0/49
C(config-if-GigabitEthernet 0/49)#rldp port unidirection-detect shutdown-port
C(config-if-GigabitEthernet 0/49)#rldp port bidirection-detect shutdown-port
C(config-if-GigabitEthernet 0/49)# exit
C(config)#interface GigabitEthernet 0/50
C(config-if-GigabitEthernet 0/50)#rldp port unidirection-detect shutdown-port
C(config-if-GigabitEthernet 0/50)#rldp port bidirection-detect shutdown-port
C(config-if-GigabitEthernet 0/50)#exit
```

```
C(config)#interface GigabitEthernet 0/1
C(config-if-GigabitEthernet 0/1)# rldp port loop-detect shutdown-port
C(config-if-GigabitEthernet 0/1)#exit
C(config)#interface GigabitEthernet 0/2
C(config-if-GigabitEthernet 0/2)# rldp port loop-detect shutdown-port
C(config-if-GigabitEthernet 0/2)#exit
```

【检验方法】 ● 检查 A、B、C 设备的 RLDP 状态信息，以 A 为例。

A

```
A#show rldp
rldp state          : enable
rldp hello interval: 3
rldp max hello      : 2
rldp local bridge   : 00d0.f822.33aa
-----

Interface GigabitEthernet 2/0/1
port state          : normal
neighbor bridge    : 00d0.f800.51b1
neighbor port      : GigabitEthernet 2/0/1
unidirection detect information:
  action: shutdown-port
  state : normal
bidirection detect information:
  action: shutdown-port
  state : normal

Interface GigabitEthernet 2/0/9
port state          : normal
neighbor bridge    : 00d0.f800.41b0
neighbor port      : GigabitEthernet 0/49
unidirection detect information:
  action: shutdown-port
  state : normal
bidirection detect information:
  action: shutdown-port
  state : normal
loop detect information:
  action: shutdown-port
  state : normal
```

常见错误

- 与私有组播地址认证或者 TPP 等功能不可以同时开启。

- 配置单双向检测时不指定邻居协商，要求邻居设备在全局和接口下使能 RLDP，否则会被检测为单向或者双向故障。
- 配置单双向检测时如果指定了先协商邻居后开始检测，那么在已存在故障的情况下由于无法学习到邻居而导致不能正常检测，建议先恢复链路错误状态。
- 路由口下建议不要指定故障处理方式为 Shutdown SVI。
- STP 等环路保护协议使能的端口下建议不要指定故障处理方式为 Block。

1.5 监视与维护

查看运行情况

作用	命令
查看 RLDP 运行状态。	<code>show rldp [interface <i>interface-name</i>]</code>



配置指南-网管和监控

本分册介绍网管和监控配置指南相关内容，包括以下章节：

1. SNMP
2. NTP
3. SPAN

1 SNMP

1.1 概述

SNMP 是 Simple Network Management Protocol (简单网络管理协议) 的缩写, 在 1988 年 8 月就成为一个网络管理标准 RFC1157。到目前, 因众多厂家对该协议的支持, SNMP 已成为事实上的网管标准, 适合于在多厂家系统的互连环境中使用。利用 SNMP 协议, 网络管理员可以对网络上的节点进行信息查询、网络配置、故障定位、容量规划, 网络监控和管理是 SNMP 的基本功能。

📌 SNMP 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。
- 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。

协议规范

- RFC 1157 , Simple Network Management Protocol (SNMP)
- RFC 1901 , Introduction to Community-based SNMPv2
- RFC 2578 , Structure of Management Information Version 2 (SMIv2)
- RFC 2579 , Textual Conventions for SMIv2
- RFC 3411 , An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
- RFC 3412 , Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
- RFC 3413 , Simple Network Management Protocol (SNMP) Applications
- RFC 3414 , User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
- RFC 3415 , View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
- RFC 3416 , Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)
- RFC 3417 , Transport Mappings for the Simple Network Management Protocol (SNMP)
- RFC 3418 , Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)
- RFC 3419 , Textual Conventions for Transport Addresses

1.2 典型应用

典型应用	场景描述
通过SNMP管理网络设备	通过 SNMP 网络管理器对网络设备进行管理和监控。

1.2.1 通过SNMP管理网络设备

应用场景

以下图为例，用户通过 SNMP 网络管理器，来对网络设备 A 进行管理和监控。

图 1-1



【注释】 A 为需要被管理的网络设备。
PC 为网络管理站。

功能部属

网络管理站和被管理的网络设备通过网络连接，用户在网络管理站上，通过 SNMP 网络管理器，访问网络设备上的管理信息数据库，以及接收来自网络设备主动发出的消息，来对网络设备进行管理和监控。

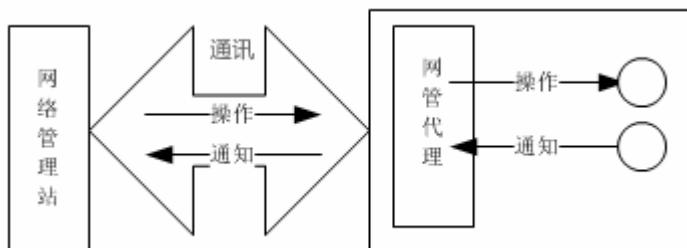
1.3 功能详解

基本概念

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

图 1-2 网络管理站（NMS）与网管代理（Agent）的关系图



SNMP 网络管理器

SNMP 网络管理器，是采用 SNMP 来对网络进行控制和监控系统，也称为 NMS (Network Management System)。

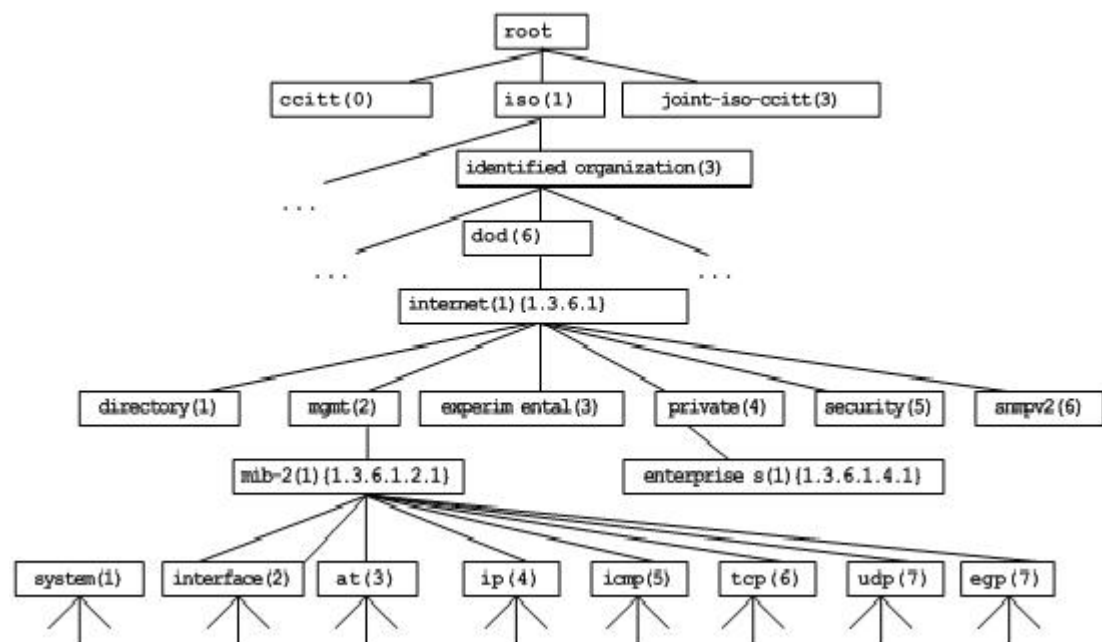
SNMP 代理

SNMP 代理 (SNMP Agent, 下文简称为 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。

MIB

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大量信息，为了能在 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，树的节点表示某个特定的管理单元。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，MIB 则是网络设备的单元标识符的集合。

图 1-3 MIB 树形层次结构



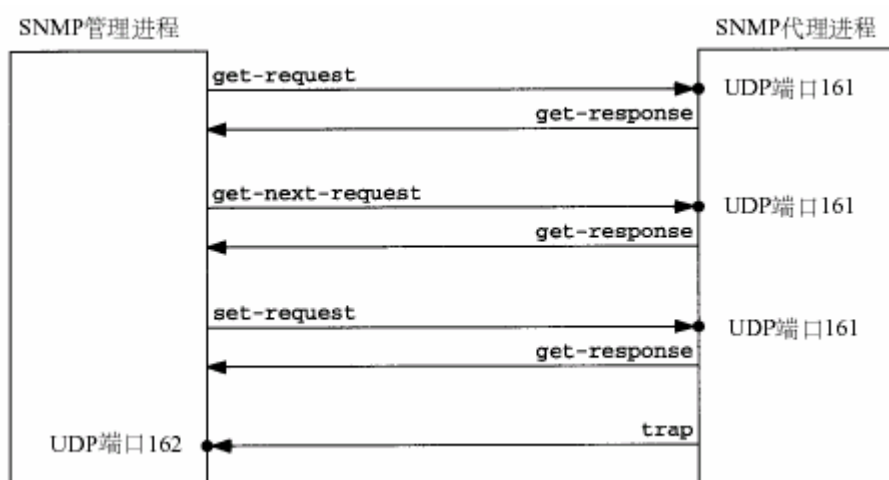
操作类型

SNMP 协议中的 NMS 和 Agent 之间的交互信息，定义了 6 种操作类型：

- Get-request 操作：NMS 从 Agent 提取一个或多个参数值。
- Get-next-request 操作：NMS 从 Agent 提取一个或多个参数的下一个参数值。
- Get-bulk 操作：NMS 从 Agent 提取批量的参数值；
- Set-request 操作：NMS 设置 Agent 的一个或多个参数值。
- 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。
- Trap 操作：Agent 主动发出的报文，通知 NMS 有某些事情发生。

前面的 4 个报文是由 NMS 向 Agent 发出的，后面两个是 Agent 发给 NMS 的（注意：SNMPv1 版本不支持 Get-bulk 操作）。下图描述了这几种操作。

图 1-4 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。

功能特性

功能特性	作用
SNMP基本功能	配置网络设备上的 SNMP 代理，实现对网络上的节点进行信息查询、网络配置、故障定位、容量规划等基本功能。
SNMPv1 及SNMPv2C	采用基于共同体的安全架构，包括认证名和访问权限。
SNMPv3	SNMPv3 重新定义了 SNMP 架构，主要是在安全功能上进行了增强，包括支持基于用户的安全模型，以及支持基于视图的访问控制模型等。SNMPv3 架构内已经包含了 SNMPv1 和 SNMPv2C 所有的功能。

1.3.1 SNMP基本功能

工作原理

▾ 工作过程

SNMP协议交互是应答式的（报文交互参见图 1-4 SNMP的报文类型）。NSM向Agent主动发起请求，包括Get-request、Get-next-request、Get-bulk和Set-request，Agent接收请求并完成操作后以Get-response作为应答。Agent有时候也会向NSM主动发出Trap和Inform消息，其中Trap消息不需要应答，而Inform消息则需要NSM回送一个Inform-response应答，表示收到消息，否则Agent将会重发Inform消息。

相关配置

▾ 屏蔽或关闭 SNMP 代理

缺省时启动 SNMP 功能。

使用 **no snmp-server** 命令屏蔽 SNMP 代理功能。

执行 **no enable service snmp-agent** 命令，直接关闭 SNMP 所有服务。

▾ 设置 SNMP 基本参数

缺省时系统联系方式、序列号缺省值是 60FF60；缺省最大数据报文长度 1572 字节；缺省的 SNMP 服务 UDP 端口号是 161。

使用 **snmp-server contact** 命令配置或删除系统联系方式。

使用 **snmp-server location** 命令配置或删除系统位置。

使用 **snmp-server chassis-id** 命令配置系统序列码或恢复缺省值。

使用 **snmp-server packetsize** 命令配置代理最大数据报文长度或恢复缺省值。

使用 **snmp-server udp-port** 命令设置 SNMP 服务 UDP 端口号或恢复缺省值。

▾ 配置 SNMP 主机地址

缺省情况下，没有 SNMP 主机。

使用 **snmp-server host** 命令配置 Agent 主动发送消息的 NMS 主机地址或删除指定 SNMP 主机地址。发给主机的消息可以绑定 SNMP 的版本、接收端口、认证名或用户。该命令与 **snmp-server enable traps** 命令一起使用，主动给 NMS 发送 Trap 消息。

▾ 设置 Trap 消息参数

缺省情况下，禁止 SNMP 向 NMS 主动发送 Trap 消息；打开接口发送 Link Trap 功能；关闭发送系统重启 Trap 功能。

缺省时，SNMP 报文从哪个接口出去，就使用哪个接口的 IP 地址作为源地址。

缺省时 Trap 消息报文的队列长度为 10，发送 Trap 消息的时间间隔为 30 秒。

使用 **snmp-server enable traps** 命令配置 Agent 主动或禁止向 NMS 发送 Trap 消息。

使用 **snmp trap link-status** 命令打开或关闭接口发送 Link Trap 功能。

使用 **snmp-server trap-source** 命令指定发送消息的源地址或恢复缺省值。

使用 **snmp-server queue-length** 命令设置 Trap 消息报文的队列长度或恢复缺省值。

使用 **snmp-server trap-timeout** 命令设置发送 Trap 消息的时间间隔或恢复缺省值。

使用 **snmp-server system-shutdown** 命令打开或关闭发送系统重启 Trap 功能。

📌 设置对 community 和 user 进行密码字典检查

缺省情况下，关闭对 community 和 user 进行密码字典检查。

使用 **snmp-server enable secret-dictionary-check** 命令对 SNMP 的 community 和 user 进行密码字典检查功能，该命令需与全局配置命令 **password policy** 一起使用。

1.3.2 SNMPv1 及SNMPv2C

SNMPv1 和 SNMPv2C 都采用基于共同体(Community-based)的安全架构。通过定义主机地址以及认证名(Community String)来限定能够对代理的 MIB 进行操作的管理者。

工作原理

SNMPv1 和 SNMPv2 版本使用认证名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。

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。

📌 安全

一个认证名有以下属性：

- 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。

相关配置

📌 设置认证名及访问权限

所有认证名的缺省访问权限为只读。

使用 **snmp-server community** 命令配置或删除认证名和访问权限。

该命令为启用设备 SNMP 代理功能的第一个重要命令，指定了团体的属性、允许访问 MIB 的 NMS 范围等等。

1.3.3 SNMPv3

SNMPv3 重新定义了 SNMP 架构，将之前的 SNMPv1 和 SNMPv2 的功能也纳入到 SNMPv3 体系中。

工作原理

网络管理系统 (NMS) 和 SNMP 代理 (SNMP Agent) 都称为 SNMP 实体。在 SNMPv3 架构中，SNMP 实体分为引擎和应用两大部分，其中 SNMP 引擎用于发送和接收信息、鉴定和加密信息以及对管理对象的控制访问。SNMP 应用指的是 SNMP 内部的应用程序，利用 SNMP 引擎提供的服务进行工作。

SNMPv3 版本使用基于用户的安全模型 (USM) 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) 的用户和安全级别必须同设备中定义的某个 SNMP 用户一致。

SNMPv3 版本规定 NSM 在管理设备的时候，必须先得知设备上 SNMP Agent 的引擎标识。SNMPv3 定义了 Discover 和 Report 操作机制，NSM 在不知道 Agent 引擎标识的情况下，可以先向 Agent 发送 Discover 报文，而 Agent 以 Report 响应，并在响应报文中携带了引擎标识信息。此后，NSM 和 Agent 之间的管理操作必须携带该引擎标识。

安全

- SNMPv3 通过安全模型以及安全级别来确定对数据采用哪种安全机制进行处理。目前可用的安全模型有三种类别：SNMPv1、SNMPv2c、SNMPv3。SNMPv3 将 SNMPv1 和 SNMPv2c 也纳入到安全模型中。

SNMPv1 及 SNMPv2c 安全模型和级别

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 安全模型以及安全级别

安全模型	安全级别	鉴别	加密	说明
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

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 代理必须拥有一个唯一的引擎标识，即 SmpEngineID。

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。
- 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。

相关配置

配置 MIB 视图和组

缺省配置一个 default 视图，允许访问所有的 MIB 对象。

缺省没有配置用户组。

使用 `snmp-server view` 命令配置或删除视图；使用 `snmp-server group` 命令配置或删除用户组。

可以配置一条或者多条指令，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。

配置 SNMP 用户



缺省没有配置用户。

配置 `snmp-server user` 命令配置或删除用户。

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（是否需要进行认证、是否需要进行加密等）、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。

1.4 配置详解

配置项	配置建议 & 相关命令	
配置SNMP基本功能	 必须配置。使用户可以通过 NMS 访问 Agent。	
	<code>enable service snmp-agent</code>	启动 Agent 功能。
	<code>snmp-server community</code>	配置认证名和访问权限。
	<code>snmp-server user</code>	配置 SNMP 用户信息。
	<code>snmp-server view</code>	配置 SNMP 视图。
	<code>snmp-server group</code>	配置 SNMP 用户组。
	<code>snmp-server secret-dectionaty-check</code>	<code>enable</code>
启用Trap功能	 可选配置。使 Agent 主动向 NMS 发送 Trap 消息。	

	snmp-server host	配置 NMS 主机地址。
	snmp-server enable traps	Agent 主动向 NMS 发送 Trap 消息。
	snmp trap link-status	打开接口发送 Link Trap 功能。
	snmp-server system-shutdown	打开发送系统重启 Trap 功能。
	snmp-server trap-source	指定发送 Trap 消息的源地址。
屏蔽Agent功能	⚠️ 可选配置。在不需要 Agent 服务的时候，屏蔽 Agent 功能。	
	no snmp-server	屏蔽 Agent 功能。
设置SNMP控制参数	⚠️ 可选配置。用于设置或修改 SNMP 控制参数。	
	snmp-server contact	设置设备的联系方式。
	snmp-server location	设置设备位置。
	snmp-server chassis-id	设置设备序列码。
	snmp-server packet-size	修改最大数据报文长度。
	snmp-server udp-port	修改 SNMP 服务 UDP 端口号。
	snmp-server queue-length	修改 Trap 消息报文的队列长度。
	snmp-server trap-timeout	修改发送 Trap 消息的时间间隔。

1.4.1 配置SNMP基本功能

配置效果

使用户可以通过 NMS 访问 Agent。

注意事项

- 网络设备上默认没有设置认证名，无法使用 SNMPv1 或 SNMPv2C 访问网络设备的 MIB。设置认证名时，如果没有指定访问权限，则默认的访问权限是只读（Read-only）。

配置方法

配置 SNMP 视图

- 可选配置。
- 使用基于视图的访问控制（VACM）功能时需要进行配置。

配置 SNMP 用户组

- 可选配置。
- 使用基于视图的访问控制（VACM）功能时需要进行配置。

配置认证名和访问权限

- 必选配置。
- 使用 SNMPv1 和 SNMPv2C 管理网络设备必须在 agent 设备上设置认证名。

配置 SNMP 用户信息

- 必选配置。
- 使用 SNMPv3 管理网络设备必须设置用户。

启动 Agent 功能

- 可选配置。
- 默认开启 Agent 功能，在 Agent 功能关闭后需要再次开启时，须使用此命令。

打开 SNMP 攻击防护检测功能

- 可选配置。
- 默认关闭 SNMP 攻击防护检测功能，在需要防止恶意攻击时，在 agent 上使用该配置项。

设置对 community 和 user 进行密码字典检查

- 可选配置。
- 默认不对 community 和 user 进行密码字典检查，如果不希望团体名和用户名太简单而容易被破解，可以启动对 community 和 user 进行密码字典检查，该配置需要与全局配置命令 password policy 一起使用。

检验方法

使用 `show snmp` 命令查看设备上的 snmp 功能。

相关命令

配置 SNMP 视图

【命令格式】 `snmp-server view view-name oid-tree { include | exclude }`

【参数说明】 `view-name`：视图名。

`oid-tree`：视图关联的 MIB 对象，是一棵 MIB 子树。

`include`：标明该 MIB 对象子树被包含在视图之内。

`exclude`：标明该 MIB 对象子树被排除在视图之外。

【命令模式】 全局配置模式

【使用指导】 指定视图的名称，用于基于视图的管理。

配置 SNMP 用户组

- 【命令格式】 **snmp-server group** *groupname* { **v1** | **v2c** | **v3** { **auth** | **noauth** | **priv** } } [**read** *readview*] [**write** *writeview*] [**access** { *aclnum* | *aclname* }]
- 【参数说明】 **v1** | **v2c** | **v3** : 指明 SNMP 版本。
auth : 该组的用户传输的消息需要验证但数据不需要保密, 只对 v3 有效。
noauth : 该组用户传输的消息不需要验证数据也不需要保密, 只对 v3 有效。
priv : 该组用户传输的消息需要验证同时传输的数据需要保密, 只对 v3 有效。
readview : 关联一个只读的视图。
writeview : 关联一个读写视图。
aclnum : 访问列表序列号, 关联指定的访问列表, 指定能访问 MIB 的 ipv4 NMS 地址范围。
aclname : 访问列表名称, 关联指定的访问列表, 指定能访问 MIB 的 ipv4 NMS 地址范围。
- 【命令模式】 全局配置模式
- 【使用指导】 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。通过这种方式判定操作关联的管理对象是否在视图允许之内, 只有在视图允许之内的管理对象才被允许访问。

配置认证名和访问权限

- 【命令格式】 **snmp-server community** [0 | 7] *string* [**view** *view-name*] [[**ro** | **rw**] [**host** *ipaddr*]] [*aclnum* | *aclname*]
- 【参数说明】 0 : 表示输入的团体字符串为明文字符串。
7 : 表示输入的团体字符串为密文字符串。
string : 团体字符串, 相当于 NMS 和 SNMP 代理之间的通信密码。
view-name : 指定视图的名称, 用于基于视图的管理。
ro : 指定 NMS 对 MIB 的变量只能读, 不能修改。
rw : NMS 对 MIB 的变量可读可写。
aclnum : 访问列表序列号, 关联指定的访问列表, 指定能访问 MIB 的 ipv4 NMS 地址范围。
aclname : 访问列表名称, 关联指定的访问列表, 指定能访问 MIB 的 ipv4 NMS 地址范围。
ipaddr : 关联 NMS 地址, 指定访问 MIB 的 NMS 地址。
- 【命令模式】 全局配置模式
- 【使用指导】 该命令为启用设备 SNMP 代理功能的第一个重要命令, 指定了团体的属性、允许访问 MIB 的 NMS 范围等等。要关闭 SNMP 代理功能, 执行 **no snmp-server** 命令即可。

配置 SNMP 用户

- 【命令格式】 **snmp-server user** *username* *groupname* { **v1** | **v2c** | **v3** [**encrypted**] [**auth** { **md5** | **sha** } *auth-password*] [**priv** **des56** *priv-password*] } [**access** { *aclnum* | *aclname* }]
- 【参数说明】 *username* : 用户名。
groupname : 该用户对应的组名。
v1 | **v2c** | **v3** : 指明 SNMP 版本。只有 v3 支持后面的安全参数。
encrypted : 指定的是密码输入的方式为密文输入。否则, 以明文输入。如果选择了以密文输入, 则需要输入连续的 16 进制数字字符表示的密钥。注意使用 MD5 的认证密钥长度为 16 字节, 而 SHA 认证协议密钥长度为 20 字节。以两个字符表示一个字节。加密表示的密钥仅对本引擎有效。
auth : 指定是否使用验证。
md5 : 指定使用 MD5 认证协议。**sha** 指定使用 SHA 认证协议。
auth-password : 配置认证协议使用的口令字符串 (不超过 32 个字符)。系统将这些口令转换成相应的认证密

钥。

priv：指定是否使用保密。**des56** 指明使用 56 位的 DES 加密协议。

priv-password：为加密用的口令字符串（不超过 32 个字符）。系统将这个口令转换成相应的加密密钥。

aclnum：访问列表序列号，关联指定的访问列表，指定能访问 MIB 的 ipv4 NMS 地址范围。

aclname：访问列表名称，关联指定的访问列表，指定能访问 MIB 的 ipv4 NMS 地址范围。

【命令模式】 全局配置模式

【使用指导】 配置用户的信息，以使 NMS 使用合法的用户同代理进行通信。

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。

启动 Agent 功能

【命令格式】 **enable service snmp-agent**

【参数说明】

【配置模式】 全局模式

【使用指导】 该命令用于启动设备的 SNMP 代理功能。

设置对 community 和 user 进行密码字典检查

【命令格式】 **snmp-server enable secret-dictionary-check**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 该命令必须与全局配置命令 **password policy** 一起使用，设置检查规则，比如密码最小长度不小于 6 等。要关闭检查功能，执行 **no snmp-server enable secret-dictionary-check** 命令即可。

显示 SNMP 的状态信息

【命令格式】 **show snmp [mib | user | view | group | host | process-mib-time]**

【参数说明】 **mib**：显示系统中支持的 snmp mib 信息。

user：显示 snmp 用户信息。

view：显示 snmp 视图信息。

group：显示 snmp 用户组信息。

host：显示用户配置的显示信息。

process-mib-time：显示处理时间最长的 mib 节点。

【配置模式】 特权用户模式

【使用指导】 -

配置举例

SNMPv3 配置举例

【网络环境】

图 1-5



- 网络工作站(NMS)基于用户的认证加密模式对网络设备(Agent)进行管理。例如 :使用用户名 “user1” , 认证方式为 MD5 , 认证密码为 123 , 加密算法为 DES56 , 加密密码为 321。
- 网络设备能够控制用户访问 MIB 对象的操作权限。例如 : 用户 “user1” 可以对 System (1.3.6.1.2.1.1) 节点下的 MIB 对象进行读操作 , 其中只能对 SysContact (1.3.6.1.2.1.1.4.0) 节点下的 MIB 对象进行写操作。
- 网络设备能够主动向网管工作站发送验证加密的消息。

【配置方法】

- 第一步, 配置 MIB 视图和组。创建一个 MIB 视图 “view1” , 包含关联的 MIB 对象 (1.3.6.1.2.1.1); 再创建一个 MIB 视图 “view2” , 包含关联的 MIB 对象 (1.3.6.1.2.1.1.4.0)。创建一个组 “g1” , 选择版本号为 “v3” , 配置安全级别为认证加密模式 “priv” , 并可读视图 “view1” , 可写视图 “view2”。
- 第二步, 配置 SNMP 用户。创建用户名 “user1” , 属于组 “g1” , 选择版本号为 “v3” , 配置认证方式为 “md5” , 认证密码为 “123” , 加密方式为 “DES56” , 加密密码为 “321”。
- 第三步, 配置 SNMP 主机地址。配置主机地址为 192.168.3.2 , 选择版本号为 “3” , 配置安全级别为认证加密模式 “priv” , 关联对应的用户名 “user1” 。使能 Agent 主动向 NMS 发送 Trap 消息。
- 第四步, 配置 Agent 的 IP 地址。配置 Gi0/1 的接口地址为 192.168.3.1/24。

Agent

```

Ruijie(config)#snmp-server view view1 1.3.6.1.2.1.1 include
Ruijie(config)#snmp-server view view2 1.3.6.1.2.1.1.4.0 include
Ruijie(config)#snmp-server group g1 v3 priv read view1 write view2
Ruijie(config)#snmp-server user user1 g1 v3 auth md5 123 priv des56 321
Ruijie(config)#snmp-server host 192.168.3.2 traps version 3 priv user1
Ruijie(config)#snmp-server enable traps
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-gigabitEthernet 0/1)#ip address 192.168.3.1 255.255.255.0
Ruijie(config-if-gigabitEthernet 0/1)#exit
  
```

【检验方法】

- 第一步, 通过 **show running-config** 命令查看设备的配置信息。
- 第二步, 通过 **show snmp user** 命令查看 SNMP 用户。
- 第三步, 通过 **show snmp view** 命令查看 SNMP 视图。
- 第四步, 通过 **show snmp group** 命令查看 SNMP 组。
- 第五步, 通过 **show snmp host** 命令查看用户配置的主机信息。
- 第六步, 安装 MIB-Browser 查询。

Agent

```

Ruijie# show running-config
!
interface gigabitEthernet 0/1
  
```

```
no ip proxy-arp
ip address 192.168.3.1 255.255.255.0
!
snmp-server view view1 1.3.6.1.2.1.1 include
snmp-server view view2 1.3.6.1.2.1.1.4.0 include
snmp-server user user1 g1 v3 encrypted auth md5 7EBD6A1287D3548E4E52CF8349CBC93D priv des56
D5CEC4884360373ABBF30AB170E42D03
snmp-server group g1 v3 priv read view1 write view2
snmp-server host 192.168.3.2 traps version 3 priv user1
snmp-server enable traps
```

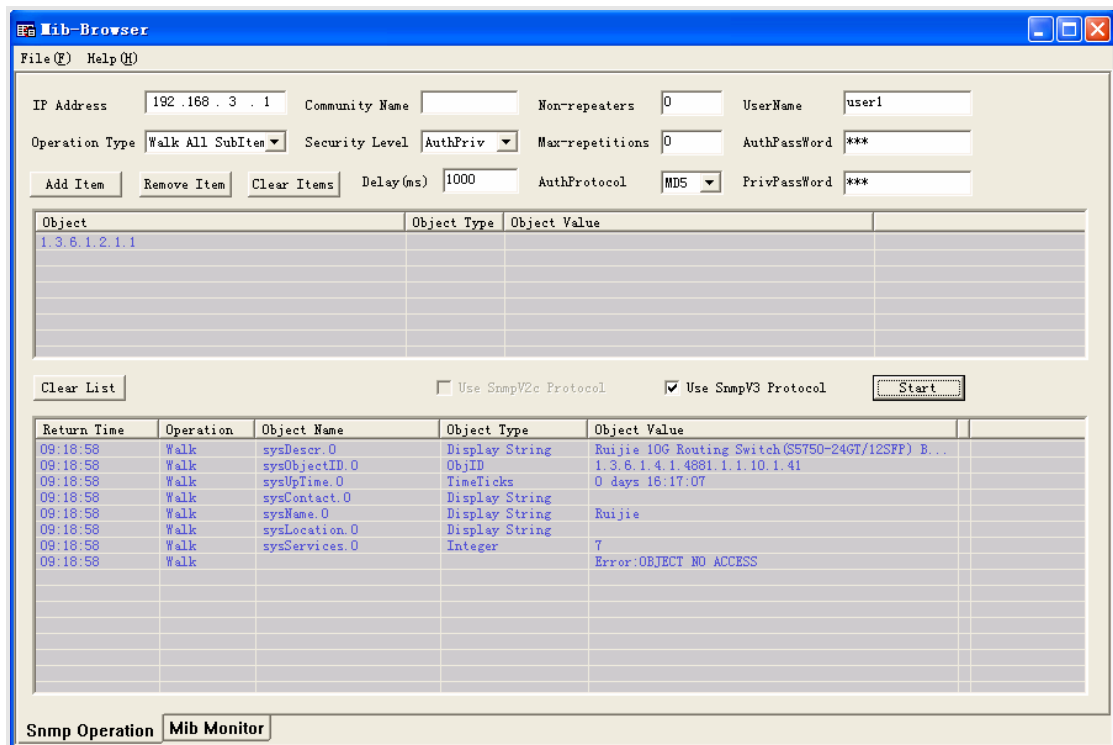
```
Ruijie# show snmp user
User name: user1
Engine ID: 800013110300d0f8221120
storage-type: permanent      active
Security level: auth priv
Auth protocol: MD5
Priv protocol: DES
Group-name: g1
```

```
Ruijie#show snmp view
view1(include) 1.3.6.1.2.1.1
view2(include) 1.3.6.1.2.1.1.4.0
default(include) 1.3.6.1
```

```
Ruijie# show snmp group
groupname: g1
securityModel: v3
securityLevel:authPriv
readview: view1
writeview: view2
notifyview:
```

```
Ruijie#show snmp host
Notification host: 192.168.3.2
udp-port: 162
type: trap
user: user1
security model: v3 authPriv
```

安装 MIB-Browser 在 IP Address 中输入设备的 IP 地址 :192.168.3.1 在 UserName 中输入 “user1” 在 Security Level 中选择 “AuthPriv” ,在 AuthPassWord 中输入 “123” ,在 AuthProtocol 中选择 “MD5” ,在 PrivPassWord 中输入 “321” 。点击 add item 按钮,选择要查询的 MIB 的具体管理单元,比如下图的 System。点击 Start 按钮,便开始对网络设备进行 MIB 的查询了,具体的查询结果见对话框的最下面的窗口 :



常见错误

-

1.4.2 启用Trap功能

配置效果

使 Agent 主动向 NMS 发送 Trap 消息。

注意事项

-

配置方法

配置 snmp 主机地址

- 可选配置。
- 需要 Agent 主动发送消息时需要配置 NWS 的主机地址。

Agent 主动向 NMS 发送 Trap 消息

- 可选配置。
- 当需要 agent 主动向 NMS 发送 Trap 消息时，需在 agent 上配置此项。

📌 打开接口发送 Link Trap 功能

- 可选配置。
- 当需要接口发送 link trap 功能时，需在 agent 上配置接口打开此项。

📌 打开发送系统重启 Trap 功能

- 可选配置。
- 当希望 RGOS 系统在设备 reload/reboot 以前给 NMS 发送 Trap 消息通知系统重启时，需在 agent 上配置此项。

📌 指定发送 Trap 消息的源地址

- 可选配置。
- 当希望固定使用一个本地 IP 地址作为 SNMP 的源地址以便于管理时，需在 agent 上配置此项。

检验方法

通过 `show snmp` 命令显示 SNMP 的状态信息。


通过 `show running-config` 命令查看设备的配置信息。

相关命令

📌 配置 NMS 主机地址

【命令格式】 `snmp-server host { host-addr } [traps | informs] [version { 1 | 2c | 3 { auth | noauth | priv }] community-string [udp-port port-num] [notification-type]`

【参数说明】 `host-addr`：SNMP 主机地址。
`traps | informs`：配置主机发送 trap 报文还是 inform 报文。
`Version`：选择 snmp 版本，V1、V2C、V3。
`auth | noauth | priv`：配置 V3 用户的安全级别。
`community-string`：团体字符串或用户名（V3 版本）。
`port-num`：配置 snmp 主机端口。
`notification-type`：主动发送的 Trap 类型，例如 snmp。

 如果没有指定 Trap 类型，则包括所有 Trap 类型。

【命令模式】 全局配置模式

【使用指导】 该命令与全局配置命令 `snmp-server enable traps` 一起使用，主动给 NMS 发送 Trap 消息。
可以配置多个不同的 SNMP 主机用于接收 Trap 消息，一个主机可以使用不同 Trap 类型组合，不同的端口。

📌 配置 Agent 主动向 NMS 发送 Trap 消息

- 【命令格式】 **snmp-server enable traps** [*notification-type*]
- 【参数说明】 *notification-type* : 启用对应事件的 Trap 通知 , , 有以下类型 :
- snmp: 启动 SNMP 事件的 TRAP 通知 ;
 - bridge: 启动 BRIDGE 事件的 TRAP 通知 ;
 - mac-notification: 启动 MAC 事件的 TRAP 通知 ;
 - urpf: 启动 URPF 事件的 TRAP 通知 ;
 - vrrp: 启动 VRRP 事件的 TRAP 通知 ;
 - web-auth: 启动 WEB 认证事件的 TRAP 通知。
- 【命令模式】 全局配置模式
- 【使用指导】 该命令必须与全局配置命令 **snmp-server host** 一起使用 , 才能发送 Trap 消息。

📌 打开接口发送 Link Trap 功能

- 【命令格式】 **snmp trap link-status**
- 【参数说明】 -
- 【配置模式】 接口配置模式
- 【使用指导】 对于接口 (以太网接口、Ap 接口、SVI 接口) , 当功能打开时 , 如果接口发生 Link 状态变化 , SNMP 将发出 Link Trap , 反之则不发。

📌 打开发送系统重启 Trap 功能

- 【命令格式】 **snmp-server system-shutdown**
- 【参数说明】 -
- 【配置模式】 全局配置模式
- 【使用指导】 打开 SNMP 系统重启通知功能 , 会在设备 **reload/reboot** 以前给 NMS 发送 Trap 消息通知系统重启。

📌 指定发送 Trap 消息的源地址

- 【命令格式】 **snmp-server trap-source interface**
- 【参数说明】 *interface* : 用于作为 SNMP 源地址的接口。
- 【配置模式】 全局配置模式
- 【使用指导】 缺省情况下 , SNMP 报文从哪个接口出去 , 就使用哪个接口的 IP 地址作为源地址 , 为了便于管理和识别 , 可以使用该命令固定使用一个本地 IP 地址作为 SNMP 的源地址。

配置举例

📌 配置启用 trap 功能

【网络环境】

图 1-6



- 网管工作站 (NMS) 基于共同体认证模式对网络设备 (Agent) 进行管理 , 网络设备能够主动向网管工

作站发送消息。

- 【配置方法】
- 第一步，配置 Agent 主动向 NMS 发送消息。配置 SNMP 主机地址为 192.168.3.2，消息格式为 Version 2c，认证名为 “user1”。使能 Agent 主动发送 Trap 消息。
 - 第二步，配置 Agent 的 IP 地址。配置 Gi 0/1 的接口地址为 192.168.3.1/24。

Agent

```
Ruijie(config)#snmp-server host 192.168.3.2 traps version 2c user1
Ruijie(config)#snmp-server enable traps
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-gigabitEthernet 0/1)#ip address 192.168.3.1 255.255.255.0
Ruijie(config-if-gigabitEthernet 0/1)#exit
```

- 【检验方法】
- 通过 **show running-config** 命令查看设备的配置信息。
 - 通过 **show snmp** 命令显示 SNMP 的状态信息。

Agent

```
Ruijie# show running-config
ip access-list standard a1
 10 permit host 192.168.3.2
interface gigabitEthernet 0/1
 no ip proxy-arp
 ip address 192.168.3.1 255.255.255.0
snmp-server view v1 1.3.6.1.2.1.1 include
snmp-server location fuzhou
snmp-server host 192.168.3.2 traps version 2c user1
snmp-server enable traps
snmp-server contact ruijie.com.cn
snmp-server community user1 view v1 rw a1
snmp-server chassis-id 1234567890

Ruijie#show snmp
Chassis: 1234567890
0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Set-request PDUs
0 SNMP packets output
    0 Too big errors (Maximum packet size 1472)
    0 No such name errors
```

```
0 Bad values errors
0 General errors
0 Response PDUs
0 Trap PDUs
SNMP global trap: enabled
SNMP logging: disabled
SNMP agent: enabled
```

常见错误

1.4.3 无屏蔽Agent功能

配置效果

在不需要 Agent 服务的时候，屏蔽 Agent 功能。

注意事项

- 执行 **no snmp-server** 命令，可以在不需要代理服务的时候，屏蔽 SNMP 代理功能。
- 不同于屏蔽命令，执行 **no enable service snmp-agent** 命令，会直接关闭 snmp 所有服务（即 snmp 代理功能被禁用了，不接收报文、不发送响应报文及 trap），不会屏蔽代理的配置信息。

配置方法

📄 配置屏蔽设备 SNMP 代理

- 可选配置。
- 需要屏蔽所有 SNMP 代理服务配置时，可选用此项配置。

📄 配置关闭设备 SNMP 代理

- 可选配置。
- 需要直接关闭所有服务时，应选用此配置项。

检验方法

通过 **show services** 命令查看 snmp 服务的开关状态信息。

通过 **show snmp** 命令显示 SNMP 的状态信息。

通过 **show running-config** 命令查看设备的配置信息。

相关命令

配置屏蔽设备 SNMP 代理功能

【命令格式】 **no snmp-server**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 SNMP 代理功能服务默认关闭，在设置 SNMP 代理参数（例如 NMS 主机地址、认证名和访问权限等）时，会自动打开 SNMP 代理服务，服务开关命令 **enable service snmp-agent** 也必须同时打开，SNMP 代理服务才能生效，但只要关闭了其中的一个，SNMP 代理服务将不会生效。使用 **no snmp-server** 命令可以关闭设备支持的所有版本 SNMP 的代理服务。

使用该命令的同时，将屏蔽所有 SNMP 代理服务配置（即使用 **show running-config** 命令查看时不会显示配置，重新开启 SNMP 代理服务可以恢复），而 **enable service snmp-agent** 命令则不会屏蔽 SNMP 代理配置。

配置关闭设备 SNMP 代理功能

【命令格式】 **no enable service snmp-agent**

【参数说明】 -

【配置模式】 全局配置模式

【使用指导】 关闭 SNMP 服务开关，但不会屏蔽 SNMP 代理参数。

配置举例

配置启用 snmp 服务功能

【网络环境】

图 1-7



通过设置 snmp 服务开关，以及设置 snmp 代理服务器，使得网管工作站（NMS）能通过 snmp 访问设备。

- 【配置方法】
- 配置启用 snmp 服务。
 - 配置 snmp 代理服务器的参数，使服务生效。

A gent Ruijie(config)#enable service snmp-agent

- 【检验方法】
- 通过 **show services** 命令查看 snmp 服务的开关状态信息。

Agent

```

Ruijie#show service
web-server      : disabled
web-server(https): disabled
  
```



```
snmp-agent      : enabled
ssh-server      : disabled
telnet-server   : enabled
```

常见错误

1.4.4 设置SNMP控制参数

配置效果

对 SNMP 的 Agent 的基本参数进行配置，包括设备的联系方式、设备位置、序列号、发送 Trap 消息的参数等，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。

注意事项

配置方法

✚ 配置系统的联系方式

- 可选配置。
- 当需要修改系统的联系方式时，需在 agent 上配置此项。

✚ 配置系统位置

- 可选配置。
- 当需要修改系统的系统位置时，需在 agent 上配置此项。

✚ 配置系统序列码

- 可选配置。
- 当需要修改系统的序列码时，需在 agent 上配置此项。

✚ 配置 SNMP 代理最大数据报文长度

- 可选配置。
- 当需要修改 SNMP 代理最大数据报文长度时，需在 agent 上配置此项。

✚ 配置 SNMP 服务 UDP 端口号

- 可选配置。
- 当需要修改 SNMP 服务的 UDP 端口号时，需在 agent 上配置此项。

配置 Trap 消息报文的队列长度

- 可选配置。
- 当希望通过调整消息队列大小来控制消息发送速度时，需在 agent 上配置此项。

配置发送 Trap 消息的时间间隔

- 可选配置。
- 当需要修改发送 Trap 消息的时间间隔时，需在 agent 上配置此项。

配置 SNMP 流控

- 可选配置。
- 如果 SNMP 的请求报文太多导致 SNMP 任务的 CPU 占用比较高，可以配置 SNMP 流控，限制 SNMP 任务每秒处理的请求报文个数，从而控制 SNMP 任务的 CPU 占用情况。

检验方法

通过 `show snmp` 命令显示 SNMP 的状态信息。

通过 `show running-config` 命令查看设备的配置信息。

相关命令

配置系统的联系方式

- 【命令格式】 `snmp-server contact text`
- 【参数说明】 `text`：描述系统联系方式的字符串。
- 【命令模式】 全局配置模式
- 【使用指导】

配置系统位置

- 【命令格式】 `snmp-server location text`
- 【参数说明】 `text`：描述系统信息的字符串。
- 【配置模式】 全局配置模式
- 【使用指导】

配置系统序列码

- 【命令格式】 `snmp-server chassis-id text`
- 【参数说明】 `text`：系统序列号的文本，可以是数字或字符。
- 【配置模式】 全局配置模式

【使用指导】 SNMP 系统序列号一般使用机器的序列号，以便对设备进行识别。

配置 SNMP 代理最大数据报文长度

【命令格式】 **snmp-server packetsize** *byte-count*

【参数说明】 *byte-count*：数据包大小，从 484 字节到 17876 字节。

【配置模式】 全局模式

【使用指导】

配置 SNMP 服务 UDP 端口号

【命令格式】 **snmp-server udp-port** *port-num*

【参数说明】 *port-num*：指定 SNMP 服务的 UDP 端口号，即接收 SNMP 报文的协议端口号。

【配置模式】 全局模式

【使用指导】 指定接收 SNMP 报文的协议端口号。

配置 Trap 消息报文的队列长度

【命令格式】 **snmp-server queue-length** *length*

【参数说明】 *length*：队列长度，大小从 1 到 1000。

【配置模式】 全局配置模式

【使用指导】 通过调整消息队列大小来控制消息发送速度。

配置发送 Trap 消息的时间间隔

【命令格式】 **snmp-server trap-timeout** *seconds*

【参数说明】 *seconds*：间隔时间，单位为秒，取值范围：1 – 1000。

【配置模式】 全局配置模式

【使用指导】 通过调整发送消息的时间间隔来控制消息发送速度。

配置 SNMP 流控

【命令格式】 **snmp-server flow-control pps** [*count*]

【参数说明】 *count*：每秒处理的 SNMP 请求报文数量，范围<50-65535>。

【命令模式】 全局配置模式

【使用指导】 如果 SNMP 的请求报文太多导致 SNMP 任务的 CPU 占用比较高，可以配置 SNMP 流控，限制 SNMP 任务每秒处理的请求报文个数，从而控制 SNMP 任务的 CPU 占用情况。

配置举例

设置 SNMP 的控制参数

【网络环境】

图 1-8



- 网管工作站（NMS）基于共同体认证模式对网络设备（Agent）进行管理，网管工作站能够获取设备的基本系统信息，如系统的联系方式、位置、序列码。

【配置方法】

- 第一步，配置 SNMP 代理参数。配置系统所处的位置、联系方式、序列码。
- 第二步，配置 Agent 的 IP 地址。配置 Gi 0/1 的接口地址为 192.168.3.1/24。

Agent

```
Ruijie(config)#snmp-server location fuzhou
Ruijie(config)#snmp-server contact ruijie.com.cn
Ruijie(config)#snmp-server chassis-id 1234567890
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-gigabitEthernet 0/1)#ip address 192.168.3.1 255.255.255.0
Ruijie(config-if-gigabitEthernet 0/1)#exit
```

【检验方法】

- 第一步，查看设备的配置信息。
- 第二步，查看 SNMP 视图和组的信息。

Agent

```
Ruijie# show running-config
ip access-list standard al
 10 permit host 192.168.3.2
interface gigabitEthernet 0/1
 no ip proxy-arp
 ip address 192.168.3.1 255.255.255.0
snmp-server view v1 1.3.6.1.2.1.1 include
snmp-server location fuzhou
snmp-server host 192.168.3.2 traps version 2c user1
snmp-server enable traps
snmp-server contact ruijie.com.cn
snmp-server community user1 view v1 rw al
snmp-server chassis-id 1234567890

Ruijie#show snmp view
v1(include) 1.3.6.1.2.1.1
default(include) 1.3.6.1
Ruijie#show snmp group
groupname: user1
securityModel: v1
securityLevel:noAuthNoPriv
```

```
readview: v1
writeview: v1
notifyview:
groupname: user1
securityModel: v2c
securityLevel:noAuthNoPriv
readview: v1
writeview: v1
notifyview:
```

常见错误

-

1.5 监视与维护

清除各类信息

-

查看运行情况

作用	命令
显示 SNMP 的状态信息	show snmp [mib user view group host]

2 NTP

2.1 概述

NTP (Network Time Protocol , 网络时间协议) , 用来使网络设备时间同步化的一种应用层协议。它可以使网络设备对其服务器或时钟源做同步化, 提供高精度度的时间校正 (LAN 上与标准时间差小于 1 毫秒, WAN 上几十毫秒), 且可使用加密确认的方式来防止攻击。

目前我司设备支持 NTP 的客户端与服务器功能, 即设备既可以从时间服务器上同步时间, 也能够作为时间服务器对其他设备进行时间同步。在作为服务器工作时设备仅支持单播 Server 模式。

协议规范

- RFC 1305 : Network Time Protocol (Version 3)

2.2 典型应用

典型应用	场景描述
基于外部时钟参考源同步时间	设备即作为客户端从外部时钟源同步时间, 同步成功后又作为服务器向其他设备提供时间同步服务。

2.2.1 基于外部时钟参考源同步时间

应用场景

如图所示：

- DEVICE-A 作为可靠参考时钟源对外提供时间同步服务
- DEVICE-B 指定 DEVICE-A 为 NTP 服务器, 从 DEVICE-A 同步时间。
- DEVICE-B 同步成功后向 DEVICE-C 提供时间同步服务。

图 2-1



功能部署

将 DEVICE-B 配置为 NTP 外部时钟参考模式

2.3 功能详解

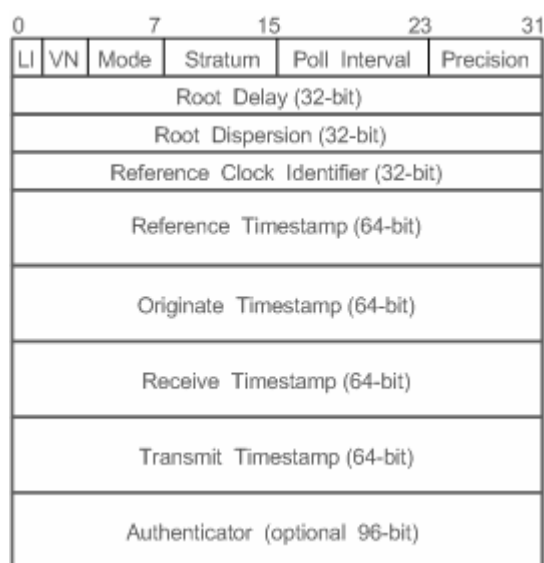
基本概念

▾ NTP 报文

根据 RFC1305 定义，NTP 采用 UDP 报文进行传输，UDP 端口号为 123。

NTP 时间同步报文格式如图 2-2

图2-2 NTP时间同步报文格式



- Leap Indicator (LI): 2 比特，闰秒标志。

i 00-无警告信息 01-上一分钟有 61 秒 10-上一分钟有 59 秒 11-时钟未同步

- Version Number (VN): 3 比特，NTP 版本号，当前版本号为 3。
- Mode : 3 比特，NTP 工作模式。

i 0-未定义 1-主动对等体 2-被动对等体 3-客户端 4-服务器 5-广播 6-控制信息 7-保留

- Stratum : 8 比特，本地时钟的层数 (0-未定义 1-主参考时钟源 其它值-次参考时钟源)。
- Poll Interval : 8 位整数，轮询时间 (秒数)
- Precision : 8 位整数，本地时钟的时间精度 (秒数)
- Root Delay : 32 位整数，到主参考时钟源的往返时间
- Root Dispersion : 32 位整数，相对于主参考时钟源的最大误差
- Reference Clock Identifier : 32 比特，参考时钟源的标识

- Reference Timestamp : 64 位时间戳, 最后一次被设置或者被校正的时间
- Originate Timestamp : 64 位时间戳, 时间同步请求报文离开客户端的本地时间
- Receive Timestamp : 64 位时间戳, 时间同步请求报文到达服务器的本地时间
- Transmit Timestamp : 64 位时间戳, 时间同步响应报文离开服务器的本地时间
- Authenticator (可选): 验证信息

📌 NTP 客户端

设备作为 NTP 客户端从网络中的 NTP 服务器同步时间。

📌 层数 (stratum)

NTP 使用“层数 (stratum)”的概念来描述设备距离权威时钟源的“跳数 (hops)”。一个层数为 1 的时间服务器应当有个直连的原子钟或电波钟；层数为 2 的时间服务器就从层数为 1 的服务器获取时间；层数为 3 的服务器就从层数为 2 的获取时间……如此递推。因此时钟层数数值更低的时钟源即被认为拥有更高的时钟精度。

📌 硬件时钟

硬件时钟根据设备上的石英晶体振荡器频率工作, 由设备的电池为其供电, 设备关机后硬件时钟依然运行。在设备启动运行后, 会从硬件时钟读取时间信息, 作为设备的软件时间。

功能特性

功能特性	作用
NTP 时间同步	使网络设备根据其服务器或可靠时钟源进行时间同步, 以实现高精度度的时间校正。
NTP 安全认证	通过 NTP 报文加密认证方式, 防止非可靠时钟源对设备进行时间同步干扰。

2.3.1 NTP时间同步

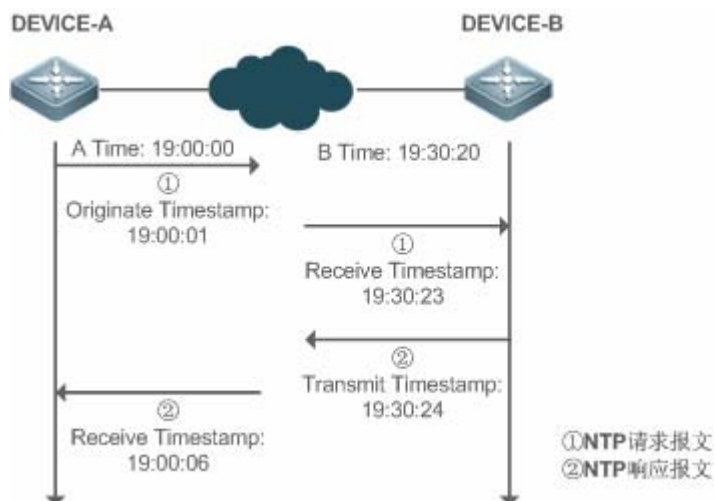
工作原理

NTP 同步时间的方式是通过客户端与服务器之间交互 NTP 报文：

- 客户端每隔 64 秒钟向所有服务器发送时间同步报文。收到服务器响应报文后, 对所有服务器的响应报文进行过滤和选择, 最后和优选服务器的时间进行同步。
- 服务器收时间同步请求报文时, 将本地时钟作为参考源, 按协议要求将本地时间信息填充到响应报文返回给客户端。

NTP 时间同步报文格式如图 2-3

图2-3 NTP基本工作原理图



DEVICE-B (下面简称 B) 作为 NTP 参考时钟源, DEVICE-A (下面简称 A) 作为 NTP 客户端从 DEVICE-B 同步时间, 在某一时刻 A 的本地时钟为 19:00:00, B 的本地时钟为 19:30:20:

4. A 发出 NTP 请求报文, 报文离开 A 的本地时间 (T0) 为 19:00:00, 填充在 Originate Timestamp
5. 经过 2 秒的网络延时, B 收到请求报文的本地时间 (T1) 为 19:30:23, 填充在 Receive Timestamp
6. B 处理 NTP 请求, 1 秒后响应 NTP 报文, 报文离开 B 的本地时间 (T2) 为 19:30:24, 填充在 Transmit Timestamp
7. 经过 2 秒的网络延时, A 接收到响应报文, 响应报文到达 A 的本地时间 (T3) 为 19:00:06

时间同步的具体算法如下:

- A 通过公式 $((T1-T0)+(T2-T3))/2$ 计算出 B 和 A 的时间差为 30 分 20 秒
- A 通过公式 $(T3-T0)-(T2-T1)$ 计算出 A 和 B 的报文往返的延时为 4 秒

▾ NTP 工作模式

- 外部时钟参考模式

在该模式下, 设备即充当服务器又充当客户端, 如果收到来自其它客户端发出的时间同步请求, 必须先从指定服务器同步时间, 同步成功后才可以向其它客户端提供时间同步服务。

相关配置

▾ 配置 NTP 服务器

- 缺省情况下, NTP 功能关闭。
- 通过 `ntp server` 命令指定 NTP 服务器 (即外部时钟参考源), 即可开启 NTP 功能。
- 配置后设备处于外部时钟参考模式。

▾ 实时同步

- 缺省情况下, 设备每隔 64 秒进行一次时间同步。

▾ 更新硬件时钟

- 缺省情况下，设备同步完时间后不会把时间更新到硬件时钟。
- 配置 `ntp update-calendar` 命令可以使设备每次时间同步成功时会自动更新硬件时钟。

2.3.2 NTP安全认证

为防止对时间服务器的恶意破坏，NTP 使用了识别(Authentication)机制，检查时间同步信息是否是真正来自所宣称的服务器并检查资料的返回路径，以提供对抗干扰的保护机制。

工作原理

NTP 客户端和服务器配置相同的密钥。发送请求报文和响应报文时，设备根据指定的密钥和 NTP 报文内容采用 MD5 算法计算出报文的哈希值填充到报文的认证信息。接收设备根据认证信息判断是否报文发送端是否可信的设备或者报文是否被篡改。

相关配置

配置 NTP 全局安全认证机制

- 缺省情况下，没有开启 NTP 安全认证机制。
- 通过 `ntp authenticate` 命令可开启 NTP 安全认证机制。

配置 NTP 全局认证密钥

- 缺省情况下，没有配置全局认证密钥。
- 通过 `ntp authentication-key` 命令可开启 NTP 安全认证机制。

配置 NTP 全局信任密钥 ID

- 缺省情况下，没有配置全局信任密钥。
- 通过 `ntp trusted-key` 命令设备作为参考时钟源对外提供时间同步服务的信任密钥。

配置外部参考时钟源的信任密钥 ID

- 通过 `ntp server` 指定外部参考时钟源的同时可以指定该时钟源的信任密钥。

2.4 配置详解

配置项	配置建议&相关命令	
配置 NTP 基本功能	 必须配置，用于开启 NTP 功能，开启后设备处于外部时钟参考模式。	
	<code>ntp server</code>	配置 NTP 服务器
	<code>ntp update-calendar</code>	自动更新硬件时钟
	 可选配置，用于关闭 NTP 功能。	

	no ntp	关闭所有 NTP 功能，清空 NTP 配置。
	ntp disable	禁止接收指定接口的 NTP 报文
配置 NTP 安全认证	 可选配置，用于防止非可靠时钟源对设备进行时间同步干扰。	
	ntp authenticate	开启安全认证机制
	ntp authentication-key	设置安全认证全局密钥
	ntp trusted-key	配置时间同步服务可信密钥
	ntp server	配置外部参考时钟源的可信密钥

2.4.1 配置NTP基本功能

配置效果

外部时钟参考模式

- 设备作为客户端，从外部参考时钟源同步时间到本地时钟
- 时间同步成功后，设备可作为时间同步服务器，对外提供时间同步服务

注意事项

- 客户端/服务器模式，设备只有从外部的可靠时钟源同步成功后，才能作为时间同步服务器对外提供服务。

配置方法

配置 NTP 服务器

- 必须配置，至少指定一个外部参考时钟源（最多可配置 20 个不同的外部参考时钟源）。
- 如果需要关联配置 NTP 密钥，在配置 NTP 服务器前，必须先配置 NTP 安全认证。

自动更新硬件时钟

- 可选配置
- 默认情况下，时间同步成功后只更新系统时钟，不会更新硬件时钟。
- 配置此命令，时间同步成功后会自动更新硬件时钟。

关闭 NTP 功能

- 如果需要关闭 NTP 功能，并且清空 NTP 配置，可通过 **no ntp** 命令
- 默认情况，开启 NTP 功能后所有接口都可以接收 NTP 报文。如果需要禁止特定接口的 NTP 功能时可通过 **ntp disable** 命令。

检验方法

- 通过 `show ntp status` 查看 NTP 配置信息。
- 通过 `show clock` 查看是否完成时间同步

相关命令

配置 NTP 服务器

【命令格式】 `ntp server { ip-addr | domain | ip domain } [version version] [source if-name] [key keyid] [prefer]`

【参数说明】 `ip-addr` : 参考时钟源的 IPv4 地址

`domain` : 参考时钟源的 IPv4 域名

`version` : NTP 版本号, 取值为 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` : 同参考时钟源通信采用的密钥(1-4294967295)

`prefer` : 参考时钟源是否高优先级

【命令模式】 全局模式

【使用指导】 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。

 如果需要设置认证密钥, 在配置 NTP 服务器前必须先配置 NTP 安全认证。

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。

更新硬件时钟

【命令格式】 `ntp update-calendar`

【参数说明】 -

【命令模式】 全局模式

【使用指导】 -

关闭 NTP 功能

【命令格式】 `no ntp`

【参数说明】 -

【命令模式】 全局模式

【使用指导】 此命令可以快速关闭 NTP 所有功能, 并且清空 NTP 所有配置

禁止接口接收 NTP 报文

【命令格式】 `ntp disable`

【参数说明】 -

【命令模式】 接口模式

【使用指导】 -

2.4.2 配置NTP安全认证

配置效果

-

注意事项

客户端和服务器的认证密钥必须一致。

配置方法

▾ 配置 NTP 全局安全认证机制

- 必须配置
- 默认情况下设备不开启安全认证机制。

▾ 配置 NTP 全局认证密钥

- 必须配置
- 默认情况下设备没有认证密钥。

▾ 配置 NTP 全局信任密钥 ID

- 可选配置
- 给可信设备提供时间同步服务，必须通过密钥 ID 指定可信认证密钥。
- 只允许配置一个信任密钥，所指定的认证密钥必须和可信设备一致。

▾ 配置外部参考时钟源的认证密钥 ID

- 可选配置
- 从可信参考时钟源同步时间，必须通过密钥 ID 指定可信认证密钥。
- 每个可信参考时钟源分别对应一个认证密钥，认证密钥必须和可信参考时钟源的密钥一致。

检验方法

- 通过 **show run** 查看配置是否正确
- 通过 **show clock** 查看是否从可信设备同步时间

相关命令

✎ 开启安全认证机制

【命令格式】 **ntp authenticate**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 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。

✎ 设置全局认证密钥

【命令格式】 **ntp authentication-key** *key-id* **md5** *key-string* [*enc-type*]

【参数说明】 *key-id*：认证密钥的全局 ID（1-4294967295）。

key-string：密钥字符串。

enc-type：可选。输入的密钥是否加密（0 表示无加密，7 表示简单加密，默认为无加密）。

【命令模式】 全局模式

【使用指导】 -

✎ 设置 NTP 服务的可信密钥

【命令格式】 **ntp trusted-key** *key-id*

【参数说明】 *key-id*：认证密钥的全局 ID（1-4294967295）。

【命令模式】 全局模式

【使用指导】 -

✎ 设置外部参考时钟源的可信密钥

参考“[配置NTP服务器](#)”

配置举例

✎ 安全认证

【网络环境】

图2-4



- DEVICE-B：配置为 NTP 客户端/服务器模式，给 DEVICE-C 提供需要安全认证的 NTP 服务，认证密钥为“abcd”
 - DEVICE-A：作为 DEVICE-B 的参考时钟源
 - DEVICE-C：从 DEVICE-B 同步时间
- 【配置方法】
- DEVICE-B 配置 DEVICE-A 为参考时钟源

- DEVICE-C 配置 DEVICE-B 为参考时钟源

```

DEVICE-B B#configure terminal
B(config)# ntp authentication-key 1 md5 abcd
B(config)# ntp trusted-key 1
B(config)# ntp server 192.168.1.1
B(config)# exit

```

```

DEVICE-C C#configure terminal
C(config)# ntp authentication-key 1 md5 abcd
C(config)# ntp server 192.168.2.1 key 1
C(config)# exit

```

- 【检验方法】
- DEVICE-B 会向 192.168.1.1 发送时间同步报文，携带认证信息，从 DEVICE-A 同步时间。
 - 在 DEVICE-B 上通过 **show clock** 命令查看时间是否成功同步。

配置举例

2.5 监视与维护

查看运行情况

作用	命令
show ntp status	显示当前的 NTP 信息

查看调试信息

 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
debug ntp	打开调试功能。
no debug ntp	关闭调试功能。

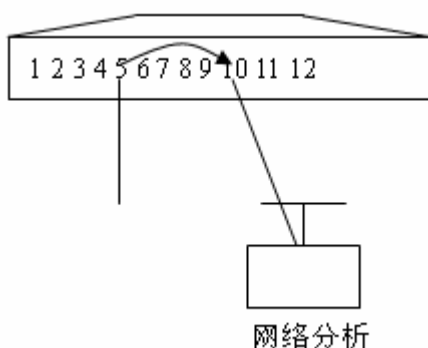
3 SPAN

3.1 概述

镜像(SPAN)是将指定端口的报文复制到交换机上另一个连接有网络监测设备的端口，进行网络监控与故障排除。

通过 SPAN 可以监控所有进入和从源端口输出的报文。例如，在下图中，端口 5 上的所有报文都被映射到了端口 10，连接在端口 10 上的网络分析仪虽然没有和端口 5 直接相连，但是可以接收通过端口 5 上的所有报文。

图 3-1 SPAN 配置实例



镜像功能主要应用于在网络监控和故障排查两种场景中，用于对网络信息的监控和网络故障的解决。

协议规范

- 无

3.2 功能详解

基本概念

▾ SPAN 会话

SPAN 会话是镜像源端口与目的端口之间的数据流，可以监控单个或多个端口的输入、输出、双向的报文。Switched Port、Routed Port 和 AP(聚合端口)等类型的端口都可以配置为 SPAN 会话的源端口和目的端口。端口加入 SPAN 会话后并不影响交换机的正常操作。

用户可以在处于关闭状态的端口上配置 SPAN 会话，但是该 SPAN 会话是非活动的，只有相关的端口被打开后，SPAN 会话才会变为活动状态。另外，SPAN 会话在交换机上电后并不立即生效，直到目的端口处于可操作状态后，SPAN 会话才处于活动状态。用户可以通过 `show monitor [session session-num]` 命令查看 SPAN 会话的操作状态。

▾ 镜像数据流

SPAN 会话包含以下三种方向的数据流：

- 输入数据流：所有源端口上接收到的报文都将被复制一份到目的端口。在一个 SPAN 会话中，用户可以监控一个或多个源端口的输入报文。由于某些原因(如端口安全)，从源端口输入的报文可能被丢弃，但这不影响 SPAN 功能，该报文仍然会镜像到目的端口。
- 输出数据流：所有从源端口发送的报文都将复制一份到目的端口。在一个 SPAN 会话中，用户可以监控一个或多个源端口的输出报文。若由于某些原因，从别的端口发送到源端口的报文可能被丢弃，同样，该报文也不会发送到目的端口。由于某些原因从源端口输出的报文的格式可能改变，例如源端口输出经过路由之后的报文，报文的源 MAC、目的 MAC、VLAN ID 以及 TTL 发生变化，同样，拷贝到目的端口的报文的格式也会变化。
- 双向数据流：包括上面所说的两种数据流。在一个 SPAN 会话中，用户可监控一个或多个源端口的输入和输出方向的数据流。

源端口

源端口也被称为被监控口，在 SPAN 会话中，源端口上的数据流被监控，用于网络分析或故障排除。在单个 SPAN 会话中，用户可以监控输入、输出和双向数据流，且源端口的最大个数没有限制。

源端口具有以下特性：

- 源端口可以是 Switched Port、Routed Port 或 AP。
- 源端口不能同时作为目的端口。
- 源端口和目的端口可以属于同一 VLAN，也可以属于不同 VLAN。

目的端口

SPAN 会话有一个目的端口(也被称为监控口)，用于接收源端口的报文拷贝。

目的端口具有以下特性：

- 目的端口可以是 Switched Port、Routed Port 或 AP。
- 目的端口不能同时作为源端口。

功能特性

功能特性	作用
SPAN	同一设备上端口的镜像。

3.2.1 SPAN

本地镜像主要是用来监控交换机上的数据流。通过将一个端口上的帧拷贝到交换机上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。

工作原理

端口收发报文时检测用户如果有配置该端口作为镜像源时，则会将该端口收发的报文复制到目的端口一份。

配置镜像源端口

用户需要指定镜像会话 ID、源端口名字来配置镜像源端口，并通过镜像方向的可选配置项决定镜像数据流的方向或通过指定 ACL 策略镜像特定数据流。

配置镜像目的端口

用户需要指定镜像会话 ID、目的端口名字来配置镜像目的端口，并通过交换功能可选配置项决定是否在该目的镜像端口上开启交换功能和剥离 TAG 信息功能。

相关配置

系统镜像功能默认是关闭的，只有用户创建会话，并配置源和目的镜像端口才会开启镜像功能。镜像会话可以在配置镜像的源端口或者目的端口的时候进行创建。

配置镜像源端口

缺省情况下，镜像会话中没有镜像源端口。用户通过下面命令配置镜像源端口。

```
monitor session session-num source interface interface-id [ both | rx | tx ]
```

其中，

session-num：镜像会话 ID，针对不同产品支持镜像会话个数会有所不同。

interface-id：待配置的镜像源端口。

rx：配置 **rx** 选项后，只监听源端口接收的报文。

tx：配置 **tx** 选项后，只监听源端口发送的报文。

both：配置 **both** 选项后，源端口收发的报文都会送到目的端口进行监听，即包含 **rx** 和 **tx**。如果用户不配置 **rx**、**tx** 和 **both** 三个选项中的任何一个则默认开启 **both** 选项。

配置镜像目的端口

缺省情况下，镜像会话中没有镜像源端口。用户通过下面命令配置镜像的目的端口。

```
monitor session session-num destination interface interface-id [switch ]
```


其中，

switch：在配置镜像目的的口时，如果没有打开该选项，则镜像目的的口只接收镜像源的镜像报文，其它报文均丢弃。如果打开该选项，除了接收镜像源的镜像报文同时非源端口送过来的报文也不会丢弃，即不影响目的的口和外界的任何其它通信。

配置镜像目的端口时，如果没有配置

switch 选项则默认关闭相应功能。

3.3 配置详解

配置项	配置建议 & 相关命令	
配置SPAN基本功能	 必须配置。用于创建本地镜像。	
	monitor session session-num source interface interface-id [both rx tx]	配置镜像源端口
	monitor session session-num destination interface interface-id [switch]	配置镜像目的端口

3.3.1 配置SPAN基本功能

配置效果

- 配置镜像会话的源和目的端口。
- 目的口可以监控到任何进出源端口的报文。

注意事项

- 如果将源端口或目的端口加入 AP，源端口或目的端口将退出 SPAN 会话。
- 如果镜像目的口没有开启 switch 功能，则目的口只能接收镜像报文，其它流经该端口的报文将被丢弃。开启后可以接收非镜像报文。

配置方法

▾ 镜像会话

- 全局模式。必须配置。
- 可以通过配置镜像的源端口或者目的端口时同时配置镜像会话。还可以通过配置指定某个 VLAN 或者某些 VLAN 作为镜像的数据源时配置镜像会话。

▾ 配置镜像源端口

- 全局模式。必须配置。
- 配置镜像源端口时可以选择配置的镜像方向，缺省是 both 方向，即同时监测报文的接收和发送行为。

▾ 配置镜像目的端口

全局模式。必须配置。

只有同时配置镜像的源端口或者指定 VLAN 作为镜像数据源，以及配置镜像的目的端口时，该镜像会话才真正起作用。

检验方法

- 镜像配置的校验也可以通过 **show monitor** 或者 **show running** 命令查看。也可以在镜像目的口上进行抓包分析，通过抓取的报文查看镜像功能是否生效。

相关命令

配置镜像源端口

【命令格式】 **monitor session session-num source interface interface-id [both | rx | tx]**

【参数说明】 *session-num*：镜像会话 ID

interface-id：接口名字

both：同时监控输入和输出方向的报文，为缺省值

rx：监控输入方向的报文

tx：监控输出方向的报文

【命令模式】 全局模式

【使用指导】 -

配置镜像目的端口

【命令格式】 **monitor session session-num destination interface interface-id [switch]**

【参数说明】 *session-num*：镜像会话 ID

interface-id：接口名字

switch：支持镜像目的口交换功能，缺省为不打开

【命令模式】 全局模式

【使用指导】 -

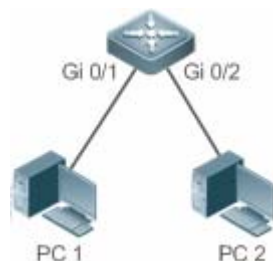
配置举例

i 以下配置举例，仅介绍与本地镜像相关的配置。

下面以本地镜像为例介绍

【网络环境】

图 3-2



【配置方法】

- 如图 1-5，配置设备 A 的 Gi 0/1 和 Gi 0/2 属于 VLAN 1。
- 创建 SVI 1，并配置 SVI 1 地址为 10.10.10.10/24。
- 配置 PC1、PC2 地址为 10.10.10.1/24、10.10.10.2/24，略。
- 配置设备 A 的本地镜像，指定端口 Gi 0/1 和 Gi 0/2 分别为镜像的源端口和目的端口。

```

A      Ruijie# configure
      Ruijie(config)# vlan 1
      Ruijie(config-vlan)# exit
      Ruijie(config)# interface vlan 1
      Ruijie(config-if-VLAN 1)# ip address 10.10.10.10 255.255.255.0
      Ruijie(config-if-VLAN 1)# exit
      Ruijie(config)# monitor session 1 source interface gigabitEthernet 0/1
      Ruijie(config)# monitor session 1 destination interface gigabitEthernet 0/2

```

【检验方法】 首先通过 **show monitor 命令**查看镜像是否正确配置，配置成功后 PC1 向 SVI 1 发送 PING 包，PC2 利用抓包工具进行监控。

```

A      Ruijie# show monitor
      sess-num: 1
      span-type: LOCAL_SPAN
      src-intf:
      GigabitEthernet 0/1          frame-type Both
      dest-intf:
      GigabitEthernet 0/2

```

常见错误

- 用户配置镜像源端口和目的端口时指定的会话 ID 不一致。
- 带宽大的端口被镜像到带宽小的端口可能会造成丢包。

3.4 监视与维护

清除各类信息

无。

查看运行情况

作用	命令
查看系统存在的所有镜像会话。	show monitor
查看具体的镜像会话。	show monitor session session-id

查看调试信息

 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
打开 SPAN 的调试开关。	debug span