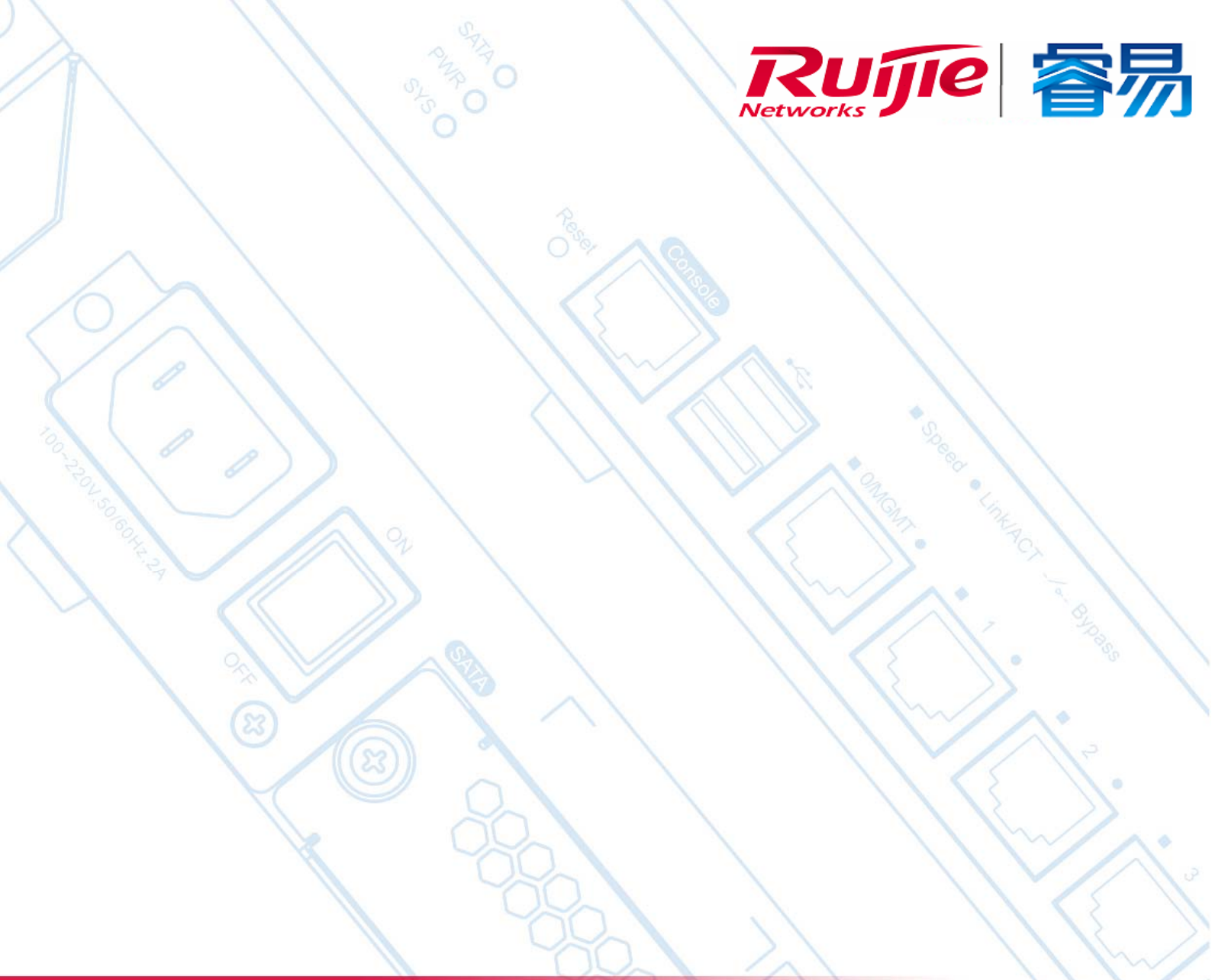


配置手册

RG-NBR 系列出口网关

NBR_RGOS11.9(2)B11P1

文档版本 ：V1.0

copyright © 2019 锐捷网络

版权声明

copyright © 2019 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

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

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-基础配置

本分册介绍基础配置相关内容，包括以下章节：

1. 命令行界面
2. 基础管理
3. LINE
4. PASSWORD-POLICY
5. 软件授权管理
6. PKG_MGMT
7. CWMP
8. 系统日志
9. LED
10. 异常告警
11. HTTP 服务
12. PATCH-UPGRADE
13. WEB-UPGRADE

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

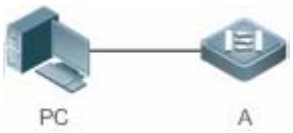
典型应用	场景描述
通过 CLI 配置管理网络设备	通过在命令行界面输入命令对网络设备进行配置管理。

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

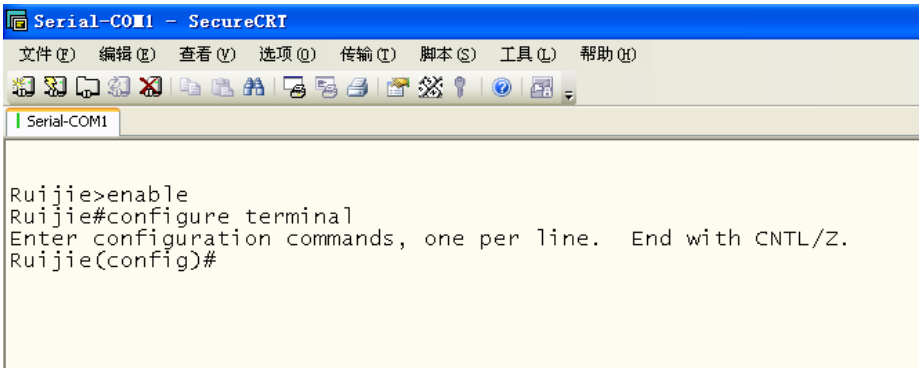


【注释】 A 为需要被管理的网络设备
PC 为用户端。

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



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

1.3.3 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
```

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。

标准的终端支持方向键，例如 VT100 系列。

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
```

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

6. 一个单词代替一条命令。

例如：将“**ip route** *0.0.0.0 0.0.0.0192.1.1.1*”配置别名“mygateway”，执行该命令只要输入“mygateway”即可。

7. 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。

配置方法

系统默认别名

- 在普通或特权用户模式下，部分命令存在默认的别名，可以通过 **show aliases** 命令查看：

```
Ruijie(config)#show aliases
Exec mode alias:
  h                    help
  p                    ping
  s                    show
  u                    undebug
  un                   undebug
```

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。

查看命令别名设置

使用 **show aliases** 命令可以查看系统中的别名设置。

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

8. 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
```

9. 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
```

10. 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。

下文仅介绍基础管理的相关内容。

协议规范

无

2.2 典型应用

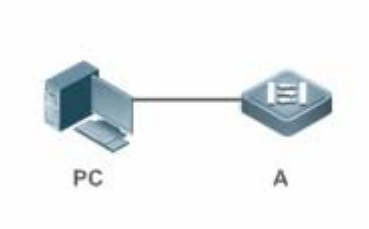
典型应用	场景描述
网络设备的管理	用户通过终端登录网络设备，在命令行界面输入命令实现对设备的配置管理。

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。

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。

AAA 打开时，线路登录允许使用非 AAA 认证方式

- AAA 打开的情况下，全局配置 **login access non-aaa** 命令，可以在 LINE 线路上选择使用非 AAA 服务来进行认证。
- 应在每台设备上配置。

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、以及运行热补丁的过程中，组件处于不稳定状态情况下所收集的系统运行配置会有一定的差异。 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，在系统重新启动后将会导入 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

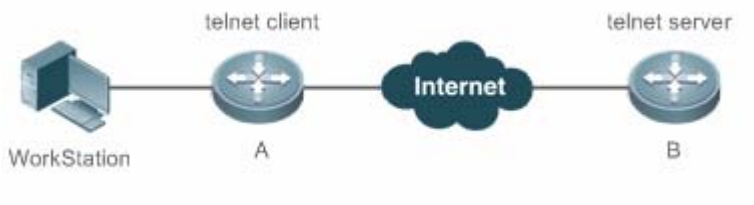
工作原理

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 程序支持使用 IPV4 地址进行通讯。作为 Telnet Server ,可以接受 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,否则有可能会导致设置失效，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。

2.4 产品说明

NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE 支持 V6 功能；NBR800G、NBR950G、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR108G-P、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1500G、NBR2000G 不支持 V6 功能。

2.5 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
设置重启策略	可选配置。设置系统重启时的策略。	
	reload	重启设备。

2.5.1 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。

ℹ 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

2.5.2 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，口令认证成功后，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。

AAA 打开时，线路登录允许使用非 AAA 认证方式

- 可选配置。
- AAA 打开的情况下，全局配置 **login access non-aaa** 命令，可以在 LINE 线路上选择使用非 AAA 服务来进行认证。
- 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** { **aux** | **console** | **ssh** | **telnet** }] [**online amount** *number*] [**permission** *oper-mode path*] [**privilege** *privilege-level*] [**reject remote-login**] [**web-auth**] [**pwd-modify**] [**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。

aux：限制账号的登录方式为 aux。

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。

pwd-modify：允许使用该账号的 web 认证用户修改密码，该选项只有在配置了 **web-auth** 之后才可用。

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】 **login authentication** { **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。

AAA 打开时，线路登录允许使用非 AAA 认证方式

【命令格式】 **login access non-aaa**

【参数说明】 -

【配置模式】 全局配置模式

【使用指导】 如果启用 AAA 安全服务的同时，在 LINE 线路上想采用非 AAA 的认证方式，则需要配置该命令，该功能对所有终端都有效。

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。

#ennif

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；该命令用于打开 IPV4 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。
- Telent 支持在特权模式下配置，do telent 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:
```

【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

2.5.3 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** 来将系统名称恢复位缺省值。

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

2.5.4 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 / T elnet 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，该命令用于打开 IPv4 服务。

telnet-server：打开与关闭 Telnet Server，该命令用于打开 IPv4 服务。

snmp-agent：打开与关闭 Snmp Agent，该命令用于打开 IPv4 服务。

【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

2.5.5 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 h h: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,否则有可能会导致设置失效，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

2.6 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 this	查看系统当前模式下生效的配置信息。
show version [**devices | module | slots**]	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 和 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

【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
!
line con 0
line vty 0 35
 login
```

```
!
end
```

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** *line-num* | **vty** *line-num* **|** *line-num* }

查看运行情况

作用	命令
查看线路的配置信息。	**show line** { **console** *line-num* | **vty** *line-num* **|** *line-num* }
显示当前 line 线路的历史记录命令	**show history**
显示当前 line 线路权限级别	**show privilege**
显示线路登录用户信息	**show user** [**all**]

4 PASSWORD-POLICY

4.1 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。

4.2 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或能，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。

密码字典检测功能

所谓的密码字典，主要是配合密码破译软件所使用，密码字典里包括许多人们习惯性设置的密码，这样可以提高密码破译软件的密码破译成功率和命中率，缩短密码破译的时间。

而密码字典检测功能所做的事情是：在用户配置口令时，通过检测用户所配置的口令，不让用户配置密码字典里面的口令，从而提高用户所配置的口令的安全性，不容易被破解。

密码字典检测功能，主要从以下几个方面对用户配置的口令进行检测：

- 检测系统默认的密码字典列表：若用户配置的口令在系统默认的密码字典当中，则不能通过密码字典检测，提示用户不能使用此口令。

- 检测日期字典，主要为生日字典检测，其检测规则为：针对用户配置的口令进行 4~8 位的组合检测，因为生日日期格式主要格式为：4 位生日密码格式 mmdd、5 位生日密码格式 yymmd 或 yymdd、6 位生日密码格式 yymmdd 或 yyyymd、7 位生日密码格式 yyyymdd 或 yyyymmd、8 位生日密码格式 yyyymmdd。其中：年份 yy 的范围为 00~99、年份 yyyy 的范围为 1900~2100、月份 mm 的范围为 1~12、日期 dd 的范围为 1~31。
- 检测姓氏拼音字典，主要为针对百家姓的姓氏拼音进行检测，此次支持的百家姓主要为近期年份最新的姓氏前 100 名进行检测。
- 检测日期字典和姓氏拼音的组合，对用户输入的口令进行日期字典和姓名拼音字典的组合检测，可以分为：生日+姓氏、姓氏+生日或者纯生日、纯姓氏。

↘ 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。

4.3 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。

4.3.1 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。

↘ 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，系统在下一次用户登录时，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。

4.4 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**

5 软件授权管理

5.1 概述

软件授权是用户使用设备某些扩展功能的中间环节，用户需要在安装上正确的授权文件之后才能使用相应的扩展功能。RGOS 提供的一些扩展功能，包括 AP 支持的用户数量、SSLVPN 支持的并发用户数量。需要经过授权方可使用其功能或使用其扩展功能。

通常，RGOS 所有特性均在出厂时均已安装于设备之中，但某些特性在获取授权前不能使用。

各项特性是否需要授权、授权类型，在各自的配置指南中说明。未加特别说明时，系统的基础功能，是不需要授权的。

5.2 典型应用

5.3 功能详解

基本概念

授权特性

通过授权文件、硬件实体或法律合同等手段获得某项特殊特性的使用许可，该许可规定了允许使用的用户数量、允许使用的实例数目以及允许使用的时间等。

授权软件

授权后才能使用的软件功能。

主机号

每个设备区别于其他设备的唯一的序列号。

在 VSU 环境下，授权可使用任何一台机箱的主机号，但当这台机箱退出 VSU 环境时，相应的授权特性自然随着相应机箱的退出而失效。

按产品授权

一个授权只能用于一台设备，匹配主机号，不支持授权的迁移。

购买凭证

购买授权时的凭证。凭证内包括产品授权码及下载授权的网址。

产品授权码（PAK）

购买凭证的合法所有者登录到下载授权的网址（购买凭证上有列举），利用 PAK 进行注册，之后网页就会提供相应的授权文件供下载或直接发送到注册的邮箱。

授权文件

授权文件用以在设备上进行安装，设备上安装授权文件后，用户即能使用相应的功能。每个授权文件包含数字签名，以防止篡改。授权文件是按产品授权的。

叠加授权

各项授权可叠加在某设备上使用。例如，设备同时有 FCoE 及 TRILL 功能，用户可以同时购买 FCoE 及 TRILL 的授权在同一台设备上使用。

临时授权

该授权有时效性，一段时间后就失效。

评估授权

临时授权的一种，通常是在出厂时已经安装于设备内，主要是提供给用户试用某特性的功能。该授权不依赖于主机号。

永久授权

该授权的使用没有时间限制。

单实例授权

设备上一个特性同一时刻最多只能安装一份授权文件。

⚠ 目前， SSLVPN 支持的并发用户数量等特性均是单实例授权。

多实例授权

设备上一个特性可以同时安装多份授权文件。

⚠ 目前只有 AP 支持的用户数量这一特性是多实例授权。

友好周期警告

友好周期警告是在授权失效数日前通过日志及 TRAP 形式进行通告。设置友好周期警告能防止具有时效的授权在超期后突然停止工作，影响网络运行。

功能特性

功能特性	作用
授权获取及使用	介绍授权的获取及使用。
备份、更新、卸载授权	介绍备份授权、更新授权、卸载授权。

5.3.1 授权获取及使用

授权使用

正式授权需要通过锐捷的网站和销售途径来获取授权，授权是基于每台设备的。依照购买凭证上的网址登陆，按照提示提供产品授权码和主机号，便能获得授权，授权通过直接下载或邮件的形式授予用户。得到授权之后，用户需要对授权文件进行安装。安装成功之后，用户就可以使用该授权所对应的特性。

RGOS 授权方式包括永久授权和临时授权（评估授权是其中一种），当用户第一次启用临时授权使用某特性时，便开始进行授权计时，授权时效过后，特性将被禁用。若想继续使用，用户可以登录锐捷的网站或销售途径通过购买手段获得授权（永久授权或临时授权）。

授权检查

设备运行之后，各个授权特性要进行授权的验证检查。若对应的授权被正确安装，那么该特性的功能便处于就绪状态，用户可以使用；否则，该特性的功能便失效，用户无法使用。

各种特性的授权检查时机有所有不同，有些只在启动时检查、有些是实时检查的。

丢失授权文件

授权文件存储于设备内/data 中，在软件升级中不会丢失。

在产品使用过程中，若出现存储器件损坏或文件系统损坏等情况，在系统修复后，如果此前备份了系统中的授权文件，重新安装这些备份的授权文件即可。如果授权文件未进行备份，则还可以登录锐捷的授权网站，重新获取授权，这一过程与新获得授权过程没有差异（不需要重新购买）。

授权是基于设备的，一项授权给指定设备，授权文件只能在该设备上验证通过。在维修或调换设备时，可能出现主机号发生变化，不再识别此前获取的授权文件，如果出现这种情况，需联系锐捷的产品售后服务人员。

5.3.2 备份、更新、卸载授权

备份授权

当设备发生文件系统存储介质损坏等故障并修理恢复之后，设备上的授权可能已经丢失。所以提前备份系统里的授权文件，以便在故障之后能够重新安装之前的授权。

更新授权

若系统已有的授权不能满足用户对该特性的使用需求，那么用户可以自行登录锐捷的网站购买满足需求的授权，之后在本地进行授权的更新。

卸载授权

当用户不需要某项特性的时候，为了提高内存等资源的利用率，可以选择卸载该特性授权。卸载后如果需要重新使用，再次安装授权文件即可。建议妥善保存授权文件。

5.4 产品说明

NBR3000G-S 支持许可证管理， NBR108G-P、NBR800G、NBR950G、NBR1000G-E、NBR6120-E、NBR1000G-C、NBR1300G-E、NBR1500G、NBR1700G-E、NBR2000G、NBR2000G-C、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 不支持许可证管理。

5.5 配置详解

配置项	配置建议 & 相关命令	
软件授权的基本功能	必须配置。用于授权功能的使用。	
	show license hostid	获取设备主机号。
	license install	安装授权。

5.5.1 软件授权的基本功能

配置效果

安装授权文件，使对应功能生效。

注意事项

- 在指定的网址下载到授权文件后，授权文件需要上传到设备上（也可以放于 usb 设备中）进行安装。安装的过程，设备无需联网。
- 不同设备不能共用授权文件。
- 授权文件在设备上安装后，系统内部自动在/data 下进行了备份（授权文件是以".lic"后缀结尾）。卸载授权时，该备份文件也会删除。

配置方法

获取设备的 host-id

- 必须配置。
- host-id 是主机号。
- 若未授权情况下使用某个授权特性的功能，CLI 会进行提示，说明该特性还未经授权，不能使用，并给出下载授权文件的网址。

【命令格式】 **show license hostid**

【参数说明】 -

【命令模式】 特权模式

【使用指导】

授权文件名不可修改

此命令不需要授权

获取产品授权码

- 必须配置。
- 产品授权码通常在用户购买授权后，锐捷公司会提供纸质的购买凭证。

通过 RUIJIE WEB URL，获取产品授权文件

- 必须配置。
- 在登录至授权网站后，按照提示操作，即可获取授权文件。

将授权文件复制到设备的文件系统中

- 必须配置。
- 采用常规的文件系统操作命令，例如，采用 TFTP 下载、U 盘复制等方式。

安装授权文件

- 可选配置。使用 **license install** 或 **license auto-install** 安装授权文件。VSU 环境下使用 **license install** 命令，若是 cm 管理板，则环境下的所有设备均安装授权文件；若非 cm 管理板，则只在输入命令的设备上安装授权文件。VSU 环境下使用 **license auto-install** 命令，则自动匹配与授权文件相符的设备进行安装。在非 VSU 环境下使用两个命令，作用相同。

【命令格式】 **license install** { **flash: | usb0:** } *filename*

【参数说明】 **flash:** 指定授权文件在内部 flash 文件系统的位置

usb0: 指定授权文件在 USB 文件系统的位置

filename：指定授权文件名字

【缺省配置】 -

【命令模式】 特权模式

【使用指导】 -

检验方法

- 使用 **show license all-license** 命令，查看展示信息中是否有对应的授权功能名来确定是否正确安装。该方法适用于非 VSU 环境下。

【命令格式】 **show license** { **all-license | file** [*license*] }

【参数说明】 **all-license**：显示设备中所有已安装授权文件的列表。

file *filename*：显示一个指定授权名的信息。

【命令模式】 特权模式
【使用指导】 用户可以通过查看特性名称，查看该授权文件是否安装成功。
【命令展示】 -

配置举例

常见错误

- 授权文件不是本设备的
- 环境中没有匹配的设备
- 授权文件已安装
- 系统已安装有更新的授权文件

5.5.2 备份授权文件

配置效果

- 备份系统上的一个或所有特性的授权文件。

注意事项

- 不能备份评估版本的授权
- 必须有足够的存储空间放可备份授权文件。

一般一个授权文件占用空间 4K-10K 不等。

配置方法

备份系统的授权文件

- 备份出的授权文件是普通的常规文件
- 当备份系统中所有授权文件时，生成的是 tar 文件。

【命令格式】 **license** { **copy-all** | **copy-file** *filename* } { **flash: | usb0:** } [*target-filename*]
【参数说明】 **copy-all**：备份系统上的所有永久授权
copy-file *filename*：备份系统上由 *filename* 指定的授权。*filename* 可以是系统已安装的授权文件名，也可以是特性名，当 *filename* 为特性名是，就备份该特性下所有已安装的授权文件。
flash: 指定授权文件在内部 flash 文件系统的位置

usb0: 指定授权文件在 USB 文件系统的位置

filename：指定授权文件名字

【缺省配置】 -

【命令模式】 特权模式

【使用指导】 -

↘ 将授权文件上载至其它系统保存

- 可使用文件系统管理命令将授权文件进一步保存至其它存储设备，例如 USB。

检验方法

- 可使用 **dir** 确定已生成的授权文件，并与 **show license all-license** 中各个永久授权特性的 installed license 字段显示的授权文件名对比，查看备份是否正确。

【命令格式】 **dir** [*filesystem*:] [*file-url*]

【参数说明】 *Filesystem*：文件系统的 url，后面加一个冒号，可能的文件系统包括：**flash:**, **sata:**, **usb:**, **tmp:**。

file-url：路径名，如果是以“/”开头，则表示绝对路径，否则表示相对路径。

【命令模式】 特权模式

【使用指导】 此命令不需要授权

【命令展示】

```
Ruijie#dir usb0:rg-license-lics
Directory of usb0:/rg-license-lics
   1 drwx          4096  Fri Jun 20 12:29:32 2014  .
   2 drwx          4096  Fri Jun 20 12:28:37 2014  ..
   3 -rwx          8704  Fri Jun 20 12:29:12 2014  lics.tar
1 file, 2 directories
536870912 bytes total (740,687,872 bytes free)
```

【命令格式】 **show license** { **all-license | file** [*license*] }

【参数说明】 **all-license**：显示设备中所有已安装授权文件的列表。

file *filename*：显示一个指定授权名的信息。

【命令模式】 特权模式

【使用指导】 用户可以通过查看特性名称，查看该授权文件是否安装成功。

⚠ 命令展示中 installed license 字段只有多实例授权才有，多实例授权系统内部备份的文件名由多实例授权的 id 号决定。单实例授权由于同一时刻系统内最多只有一个授权文件，所以内部授权文件备份直接以特性名命名。

【命令展示】

```
Ruijie#show license all-license
Searching license in the system...
 1. Service name: LIC-AP-64
    Attribute: Permanent, Multiple_instance, Releasable
    [Installed licenses]     [Licensed serial number]
```

```
19881021.lic              LIC-AP-6400000012264966
19881023.lic              LIC-AP-6400000012264988
```

配置举例

备份系统所有授权文件

【网络环境】 备份系统中所有授权文件，并命名为 lics.tar

【配置方法】

- 将 usb 连入设备；
- 将设备上所有永久授权备份到 usb 中，命名为 lics.tar；

```
Ruijie#lic copy-all usb0:rg-license-lics/lics.tar
Success to copy all permanent license.
```

【检验方法】

- 可使用 **dir** 确定已生成的授权文件压缩包，解压后，与 **show license all-license** 中各个永久授权特性的 installed license 字段显示的授权文件名对比，查看备份是否正确。

⚠ installed license 字段只有多实例授权才有，多实例授权系统内部备份的文件名由多实例授权的 id 号决定。单实例授权由于同一时刻系统内最多只有一个授权文件，所以内部授权文件备份直接以特性名命名。

⚠ 本例中 19881021.lic, 19881023.lic 该 id 号是内嵌在授权文件中，由于打包时是根据特性分文件夹存放，所以用户仍然能够区分某个授权文件对应哪个特性。

```
Ruijie#dir usb0:rg-license-lics
Directory of usb0:/rg-license-lics
   1 drwx          4096  Fri Jun 20 12:29:32 2014  .
   2 drwx          4096  Fri Jun 20 12:28:37 2014  ..
   3 -rwx          8704  Fri Jun 20 12:29:12 2014  lics.tar
1 file, 2 directories
536870912 bytes total (740,687,872 bytes free)
 Ruijie#show license all-license

Searching license in the system...

 1. Service name: LIC-AP-64
    Attribute: Permanent, Multiple_instance, Releasable
    [Installed licenses]     [Licensed serial number]
    19881021.lic             LIC-AP-6400000012264966

    19881023.lic             LIC-AP-6400000012264988
```

常见配置错误

- 系统上不存在指定授权或指定文件
- 指定要备份的授权是临时的，不能备份

5.5.3 友好周期警告

配置效果

- 评估授权过期以前，通过日志形式给出告警，使用户可以提前采取应对

注意事项

- 每个授权特性单独设置
- 该项设置会受到设备时间调整的影响
- 永久性授权不需要设置友好周期警告。

配置方法

↘ 设置一个授权的特性的友好周期警告

【命令格式】 **license grace-peroid** *filename days*

【参数说明】 *filename* ：授权特性名字

days ：提前告警的时间。

【缺省配置】 在 120 天、评估授权时间的一半两个值中，缺省值为其中的较小值。

【命令模式】 特权模式

【使用指导】 -

检验方法

- 方法 1：在授权期限小于设置的告警时间时，每隔一段时间便会出现警告的提示信息。
- 方法 2：使用 **show license** 命令查看每个授权对应的 Alarm starting point 字段的告警时间，是否与自己设置的一致。

【命令格式】 **show license** { **all-license | file** [*license*] }

【参数说明】 **all-license**：显示设备中所有已安装授权文件的列表。

file *filename*：显示一个指定授权名的信息。

【命令模式】 特权模式

【使用指导】 此命令不需要授权

【命令展示】 -

常见配置错误

- 设置永久授权的友好周期警告
- 预设置的特性系统中还未安装授权

5.5.4 更新授权

配置效果

- 更新系统上一个特性的授权，通常用于将评估授权更新为临时授权。

注意事项

- 一个正式的永久授权不需要更新。
- 不能将一个新版本的授权更新为旧版本的授权

> 授权文件中有一个生成时间的字段，该字段的值以授权文件从网站生成的时间为准，该字段的值更接近当前时间，则该授权文件的版本更新。

配置方法

更新授权文件

- 可以使用 **license update** 来更新一个特性授权。
- 更新授权，设备无需联网。

【命令格式】 **license update** { **flash: | usb0:** } *filename*

【参数说明】 **flash:** 指定授权文件在内部 flash 文件系统的位置

usb0: 指定授权文件在 USB 文件系统的位置

filename：指定授权文件名字

【缺省配置】 -

【命令模式】 特权模式

【使用指导】 -

检验方法

- 可使用 **show license** 命令，查看 Attribute 字段授权属性是否为永久来确定对应属性是否有更新。

【命令格式】 **show license** { **all-license | file** [*license*] }

【参数说明】 **all-license**：显示设备中所有已安装授权文件的列表。

file *filename*：显示一个指定授权名的信息。

【命令模式】 特权模式

【使用指导】 此命令不需要授权

【命令展示】 -

配置举例

5.5.5 卸载授权

配置效果

- 卸载系统上一个或所有特性授权。

> 当用户不需要某项特性的时候，为了提高内存等资源的利用率，可以选择卸载该特性的授权。卸载后，该特性的功能将失效。

注意事项

- 如果一个特性正在使用，授权卸载后，将在下一次特性使能或启动重启后发生作用。
- 授权卸载后，需要有授权文件方可重新安装，建议卸载前对授权文件进行备份。

配置方法

卸载系统中的一个授权

- 使用 license uninstall 命令卸载系统中的一个授权

【命令格式】 **license uninstall** { **all |** *license [filename]* }
【参数说明】 **all:** 卸载系统内所有授权文件
license：要卸载的授权名
filename：要卸载的文件名
【缺省配置】 -
【命令模式】 特权模式
【使用指导】 当授权相关的特性正在运行时，授权卸载后不会立即生效
授权卸载后不能恢复，建议卸载前先备份授权文件
此命令不需要授权

检验方法

- 可使用 **show license all-license** 命令，查看 Service name 字段，如果未出现已卸载的功能名称，则卸载成功。

【命令格式】 **show license** { **all-license | file** [*license*] }
【参数说明】 **all-license**：显示设备中所有已安装授权文件的列表。
file *filename*：显示一个指定授权名的信息。

【命令模式】 特权模式

【使用指导】 此命令不需要授权

【命令展示】

```
Ruijie#show  license all-license
Searching license in the system...
1. Service name: LIC-FCoE
    Attribute: Permanent, Single_instance, Releasable
    Licensed serial number: LIC-FCOE00000012268889
```

6 PKG_MGMT

6.1 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，还能以热补丁方式升级。

本文描述的组件升级涵盖了盒式设备的组件升级，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

6.2 典型应用

典型应用	场景描述
升降级子系统组件	升降级盒式的 boot，kernel，rootfs 等子系统组件。
升降级单个功能组件包	升降级盒式单个功能组件包。
安装热补丁包	安装热补丁，对功能组件的某一部分进行修补。

6.2.1 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；也可以将 main 包拷贝到 U 盘内，插入设备再执行升级命令完成升级。

6.2.2 一键升级子系统组件

应用场景

也是升降级子系统，一般常用于 VSU 双机系统，在特权模式下通过 upgrade auto 命令执行自动升级，升级过程中用户无须干预，且业务仍可不间断运行。对于单台设备（不论配置为 VSU 模式还是单机模式），执行该命令相当于执行 upgrade 命令后自动整机重启，无法做到业务不间断。

功能部署

如升降级子系统组件。

6.2.3 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。也可将包存放在 U 盘内，插入设备完成升级。

6.2.4 安装热补丁包

应用场景

如果需要在不重启设备的条件下完成软件缺陷的修复，可安装热补丁包。该包仅适用于对特定软件版本的修复。通常只有当用户环境不能重启设备时，才会针对该软件版本发布专门的热补丁包用于缺陷修复。
热补丁升级最显著的特点是：升级完成后，设备无需重启即可修复缺陷。

功能部署

升级热补丁包前，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，也可将包存放在 U 盘内，插入设备完成热补丁升级。

6.3 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。

↘ 热补丁包

热补丁包包含了若干功能组件的热补丁，升级该包可以依次为各功能组件包打上补丁，并且无需重启设备立刻具有新的功能特性。

⚠ 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，查询当前有哪些子系统组件可用。
功能组件升降级及管理	升降级功能组件，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。
热补丁包的升降级及管理	方便用户查询设备中存在的功能组件包及其版本和安装信息。

6.3.1 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。

6.3.2 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。
功能组件及热补丁的管理是利用数据库记录功能组件和热补丁的信息。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。
另外，需要注意当系统进行过补丁升级后，就不能再进行组件升级。

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。

6.3.3 热补丁包的升降级及管理

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。
热补丁包升级原理类似，不同之处在于它只替换需要修订的文件，并且文件替换完成后，新文件自动生效。
另外，需要注意当系统进行过组件升级后，就不能再进行补丁升级。

↘ 管理

热补丁的管理同功能组件一样包含查询、安装、卸载等，这些操作对应着数据库的插入，查询、删除等操作。
热补丁和功能组件的管理是基于同一技术原理实现的，但是热补丁的不同之处在于，热补丁包含未安装，已安装，已激活这三种状态，其中：
已安装仅仅表明设备内存在热补丁，但是该补丁功能并没有真正生效，
已激活状态的热补丁才真正有效。

相关配置

↘ 升级

- 将升级文件存放在设备本地文件系统中后，使用 **upgrade** 命令升级。

↘ 热补丁的激活

- 使用 **patch active** 命令临时激活已安装的补丁，设备重启后补丁作用失效，需重新激活；
- 或使用 **patch running** 命令永久激活已安装的补丁，设备重启后仍然生效。
- 未激活的补丁不会真正生效。

↘ 热补丁的失效

- 如果需要使已激活的补丁失效，可通过 **patch deactive** 命令完成。

卸载热补丁

- patch delete 用于卸载热补丁。

6.4 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，功能组件包及热补丁包的安装，升降级。	
	upgrade *url* ***[force]***	*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。
	upgrade download tftp://*path* ***[force]***	*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

6.4.1 安装包升降级

配置效果

可用安装包包括如下类型。

- 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。
- 升级热补丁包，即在不重启设备的条件下完成软件缺陷修复，该包仅适用于对特定软件版本的升级。

✅ 通常发布 main 包来升级盒式设备。

注意事项

-

配置方法

升级设备对应的 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

一键升级设备对应的 main 安装包

- 可选配置，组成 vsu 的双机设备原先的系统软件全部需要被更新时，且要求业务仍可不间断运行时，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 auto** 命令升级。

通常发 main 包来升级组成 vsu 的设备。

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。

升级热补丁包

- 可选配置。如果需要在不重启设备的条件下完成软件 bug 修订，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。
- 升级后需要激活补丁方能使用，该步骤是必选配置。激活方式有两种：使用 **patch active** 命令临时激活已安装的补丁；或使用 **patch running** 命令永久激活已安装的补丁。

用户场景下通常要求使用 **patch running** 命令永久激活补丁。仅当用户打算临时验证补丁功能时可使用 **patch active** 命令激活补丁。

子系统回滚

- 可选配置。如果需要将子系统回滚到升级前的状态，选择此配置，作用是使系统回归到升级前的状态。
- 使用 **upgrade** 命令升级子系统组件后（如 main 包）该配置才能生效。

用户场景下使用 **upgrade** 命令升级子系统组件成功后，回滚命令仅能生效一次，不可连续回滚。

检验方法

- 完成升级子系统组件后可执行 **show upgrade history** 命令查看是否升级成功。
- 完成升级功能组件后可执行 **show component** 命令查看是否升级成功。
- 完成升级热补丁包后可执行 **show patch** 命令查看是否升级成功。

相关命令

升级

【命令格式】 **upgrade** *url* [**force**]
【参数说明】 **force**：表示强制升级。
【命令模式】 特权模式
【使用指导】 -

【命令格式】 **upgrade download tftp:***/path* [**force**]
【参数说明】 **force**：表示强制升级。
【命令模式】 特权模式
【使用指导】 -

查看设备内存放的安装包文件信息

【命令格式】 **show upgrade file** *url*

【参数说明】 *url* 设备文件系统内安装包存放路径

【命令模式】 特权模式

【使用指导】 -

显示当前系统升级历史信息

【命令格式】 **show upgrade history**

【参数说明】 **无**

【命令模式】 特权模式

【使用指导】 -

子系统组件回滚

【命令格式】 **upgrade rollback**

【命令模式】 特权模式

【使用指导】 该命令撤销上一次子系统升级操作，使子系统返回升级前的状态。只有上次升级的是子系统且子系统升级成功才能进行回滚操作，回滚命令无法连续执行。

显示已安装的功能组件

【命令格式】 **show component**

【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】

显示安装的补丁包信息

【命令格式】 **show patch**

【命令模式】 特权模式

【使用指导】

临时激活已安装的补丁

【命令格式】 **patch active**

【命令模式】 特权模式

【使用指导】 只能对已安装补丁的设备执行该操作。该命令只能临时激活补丁，设备重启后补丁作用失效。

永久激活已安装的补丁

【命令格式】 **patch running**

【命令模式】 特权模式

【使用指导】 只能对已安装补丁的设备执行该操作。该命令可永久激活补丁。

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；
- 将安装包拷入 U 盘内并插入设备，使用 **upgrade** *url* 命令升级位于 U 盘内的安装包。

【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；
- 将安装包拷入 U 盘内并插入设备，使用 **upgrade** *url* 命令升级位于 U 盘内的安装包。
-

【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

```
Ruijie#upgrade sata0://bridge_eg1000m_2.3.1.1252ea-1.mips.rpm
  Upgrade processing is 10%
  Upgrade processing is 60%
  Upgrade processing is 90%

  Upgrade info [OK]
          bridge version[2.0.1.37cd5cda ->2.3.1.1252ea] [OK]
  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
```

↘ VSU 双机系统，使用一键升级命令举例

【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 auto** *url* 升级本地文件系统内的安装包；
- 将安装包拷入 U 盘内并插入设备，使用 **upgrade auto** *url* 命令升级位于 U 盘内的安装包。

【配置方法】
- 执行 upgrade auto 命令
- 升级后主从设备会依次重启

```
2015-04-09_09-56-23 Ruijie#upgrade auto usb0:S6220_RGOS11.0(5)B1_install.bin
```

```
2015-04-09_09-56-24 Ruijie#*Jan  1 00:23:40: %7:
2015-04-09_09-56-24 *Jan  1 00:23:40: %7: [Slot 1/0]:Upgrade processing is 10%
2015-04-09_09-56-26 Ruijie#show upgrade status
2015-04-09_09-56-26 [Slot 1/0]
2015-04-09_09-56-26        dev_type: s6k
2015-04-09_09-56-26        status  : upgrading
2015-04-09_09-56-26 [Slot 2/0]
2015-04-09_09-56-26        dev_type: s6k
2015-04-09_09-56-26        status  : transmission
2015-04-09_09-58-20 *Jan  1 00:25:36: %7: [Slot 2/0]:Upgrade processing is 10%
2015-04-09_09-58-30 Ruijie#show upgrade status
2015-04-09_09-58-30 [Slot 1/0]
2015-04-09_09-58-30        dev_type: s6k
2015-04-09_09-58-30        status  : upgrading
2015-04-09_09-58-30 [Slot 2/0]
2015-04-09_09-58-30        dev_type: s6k
2015-04-09_09-58-30        status  : upgrading
2015-04-09_09-58-39 *Jan  1 00:25:56: %7:
2015-04-09_09-58-39 *Jan  1 00:25:56: %7: [Slot 2/0]:Upgrade processing is 60%
2015-04-09_09-59-19 *Jan  1 00:26:35: %7:
2015-04-09_09-59-19 *Jan  1 00:26:35: %7: [Slot 2/0]:Upgrade processing is 90%
2015-04-09_09-59-19 *Jan  1 00:26:35: %7:
2015-04-09_09-59-19 *Jan  1 00:26:35: %7: [Slot 2/0]:
2015-04-09_09-59-19 *Jan  1 00:26:35: %7: Upgrade info [OK]
2015-04-09_09-59-19 *Jan  1 00:26:36: %7:   Kernel
version[2.6.32.6b311610a8eb91->2.6.32.6b31161115502c]
2015-04-09_09-59-19 *Jan  1 00:26:36: %7:   Rootfs version[1.0.0.eb75cd01->1.0.0.3d978b6c]
2015-04-09_09-59-19 *Jan  1 00:26:36: %7:
2015-04-09_09-59-19 *Jan  1 00:26:36: %7: [Slot 2/0]:Reload system to take effect!
2015-04-09_09-59-21 *Jan  1 00:26:37: %7:
2015-04-09_09-59-21 *Jan  1 00:26:37: %7: [Slot 2/0]:Upgrade processing is 100%
2015-04-09_10-00-28 Ruijie#show upgrade status
2015-04-09_10-00-28 [Slot 1/0]
2015-04-09_10-00-28        dev_type: s6k
2015-04-09_10-00-28        status  : upgrading
2015-04-09_10-00-28 [Slot 2/0]
2015-04-09_10-00-28        dev_type: s6k
2015-04-09_10-00-28        status  : success
2015-04-09_10-01-39 *Jan  1 00:28:56: %7:
2015-04-09_10-01-39 *Jan  1 00:28:56: %7: [Slot 1/0]:Upgrade processing is 60%
2015-04-09_10-02-17 *Jan  1 00:29:33: %7:
```

```
2015-04-09_10-02-17 *Jan  1 00:29:33: %7: [Slot 1/0]:Upgrade processing is 90%
2015-04-09_10-02-17 *Jan  1 00:29:33: %7:
2015-04-09_10-02-17 *Jan  1 00:29:33: %7: [Slot 1/0]:
2015-04-09_10-02-17 *Jan  1 00:29:34: %7: Upgrade info [OK]
2015-04-09_10-02-17 *Jan  1 00:29:34: %7:   Kernel
version[2.6.32.6b311610a8eb91->2.6.32.6b31161115502c]
2015-04-09_10-02-17 *Jan  1 00:29:34: %7:   Rootfs version[1.0.0.eb75cd01->1.0.0.3d978b6c]
2015-04-09_10-02-17 *Jan  1 00:29:34: %7:
2015-04-09_10-02-18 *Jan  1 00:29:34: %7: [Slot 1/0]:Reload system to take effect!
2015-04-09_10-02-19 *Jan  1 00:29:35: %7:
2015-04-09_10-02-19 *Jan  1 00:29:35: %7: [Slot 1/0]:Upgrade processing is 100%
2015-04-09_10-02-19 *Jan  1 00:29:36: %7: %PKG_MGMT:auto-sync config synchronization, Please wait
for a moment....
2015-04-09_10-02-20 *Jan  1 00:29:36: %7:
2015-04-09_10-02-20 [ 1784.116069] rtc-pcf8563 6-0051: retrieved date/time is not valid.
2015-04-09_10-02-20 *Jan  1 00:29:36: %7: [Slot 2/0]:auto sync config: space not enough left
57229312, need 114597815
2015-04-09_10-02-20 *Jan  1 00:29:36: %7:
2015-04-09_10-02-20 *Jan  1 00:29:36: %7: [Slot 2/0]:auto sync package config err
2015-04-09_10-02-20 *Jan  1 00:29:37: %7: [Slot 1/0]
2015-04-09_10-02-21 *Jan  1 00:29:37: %7:   device_name: s6k
2015-04-09_10-02-21 *Jan  1 00:29:37: %7:   status:      SUCCESS
2015-04-09_10-02-21 *Jan  1 00:29:37: %7: [Slot 2/0]
2015-04-09_10-02-21 *Jan  1 00:29:37: %7:   device_name: s6k
2015-04-09_10-02-21 *Jan  1 00:29:37: %7:   status:      SUCCESS
2015-04-09_10-02-21 *Jan  1 00:29:38: %7: %Do with  dtm callback....
2015-04-09_10-02-21 *Jan  1 00:29:38: %VSU-5-DTM_AUTO_UPGRADE: Upgrading the system, wait a moment
please.
```

【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-VSU#show version detail
System description      : Ruijie Full 10G Routing Switch(S6220-48XS4QXS-II) By Ruijie Networks
System start time       : 1970-02-07 00:33:24
System uptime           : 0:00:47:28
System hardware version : 2.00
System software version : S6220_RGOS 11.0(5)B1
System patch number     : NA
System software number  : MO1181304092015
System serial number    : 1234942570019
System boot version     : 1.2.9.f23dcbe(150317)
System core version     : 2.6.32.6b31161115502c
```

```
Module information:
  Slot 2/0 : RG-S6220-48XS4QXS-II
    Hardware version    : 2.00
    System start time   : 1970-02-07 00:33:24
    Boot version        : 1.2.9.f23dcbe(150317)
    Software version    : S6220_RGOS 11.0(5)B1
    Software number     : M01181304092015
    Serial number       : 1234942570019
  Slot 1/0 : RG-S6220-48XS4QXS-II
    Hardware version    : 2.00
    System start time   : 1970-02-07 00:33:47
    Boot version        : 1.2.9.f23dcbe(150317)
    Software version    : S6220_RGOS 11.0(5)B1
    Software number     : M01181304092015
    Serial number       : 1234942570018
```

↘ 盒式设备补丁包安装举例

【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；
- 将安装包拷入 U 盘内并插入设备，使用 **upgrade** *url* 命令升级位于 U 盘内的安装包。

【配置方法】

- 执行升级命令
- 激活热补丁

```
Ruijie#upgrade download tftp://192.168.201.98/eg1000m_RGOS11.0(1C2)_20131008_patch.bin
Accessing tftp://192.168.201.98/eg1000m_RGOS11.0(1C2)_20131008_patch.bin...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!
Transmission finished, file length 9868 bytes.
 Upgrade processing is 10%
 Upgrade processing is 60%

 Upgrade info [OK]
   patch_bridge version[1.0.0.1952]
 Upgrade processing is 90%

 Upgrade info [OK]
   patch_install version[1.0.0.192e35a]
```

```
Ruijie#patch running
 The patch on the system now is in running status
```

【检验方法】

- 查看当前设备安装热补丁信息

```
Ruijie# show patch
:patch package patch_install installed in the system, version:pa1
 Package : patch_bridge
 Status：running
 Version: pa1       Build time: Mon May 13 09:03:07 2013
     Size: 277      Install time: Tue May 21 03:07:17 2013
     Description: a patch for bridge
     Required packages: None
```

↘ 盒式设备子系统升级回滚配置举例

⚠ 只有当上次升级的是子系统且子系统升级成功才能进行子系统回滚操作，回滚命令无法连续执行

【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；
- 将安装包拷入 U 盘内并插入设备，使用 **upgrade** *url* 命令升级位于 U 盘内的安装包。

【配置方法】

- 执行子系统回滚命令
- 设备重启后回滚生效

```
Ruijie#upgrade rollback
 kernel rollback version[2.6.32.9f8b56f->2.6.32.91f9d21][OK]
 rootfs rollback version[1.0.0.1bcc12e8->1.0.0.2ad02537][OK]
 Rollback success!
 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，若版本回复到升级前状态则子系统回滚成功

```
Ruijie#show upgrade history
Last Upgrade Information:
    Time:         2014-08-31 12:15:03
    Method:       LOCAL
Package Name: N18000_RGOS11.0(1)B1_CM_01200616_install.bin
Package Type: Distribution
```

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。
- 设备空间不足：该错误的处理方式是要求用户检查设备是否存在 U 盘，按要求这些设备往往附带 U 盘。

6.4.2 热补丁的失效与卸载

配置效果

使已激活的热补丁失效或者卸载热补丁。

注意事项

未激活的热补丁不生效，所以未激活的热补丁不能使其失效。

配置方法

↘ 使已激活的补丁失效

- 可选配置。如果需要使已激活的补丁失效，可通过 **patch deactive** 命令完成。

↘ 卸载热补丁

- 可选配置。如果需要卸载已安装的热补丁，可使用 **patch delete** 命令完成。

检验方法

- 可使用 **show patch** 命令检测补丁是否被激活或已经被卸载。

相关命令

↘ 使已激活的补丁作用失效

【命令格式】 **patch deactive**

【命令模式】 特权模式

【使用指导】 只有对处于激活状态的补丁才能执行该操作，该操作使对应补丁失效。

↘ 卸载热补丁

【命令格式】 **patch delete**

【命令模式】 特权模式

【使用指导】 用于清除设备上已存在的热补丁包。

配置举例

↘ 盒式设备使补丁作用失效并卸载补丁

【配置方法】
- 执行补丁失效命令
- 执行补丁卸载命令

```
Ruijie#patch deactive
Deactive the patch package success
Ruijie# patch delete
Clear the patch patch_bridge success
Clear the patch success
```

【检验方法】
- 查看补丁状态信息

```
Ruijie#show patch
No patch package installed in the system
```

常见配置错误

- 补丁未处于激活状态时就执行 **patch deactive** 命令。解决方法确认补丁所处的状态，只有当提示 status：running 时，才能执行 **patch deactive** 命令。

6.5 监视与维护

清除各类信息

作用	命令
删除已安装的热补丁包	**patch delete**

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**[*cpmponent _name*]
显示设备中已安装的热补丁包的相关信息。	**show patch** [*patch _name*]
显示升级历史信息	**show upgrade history**

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

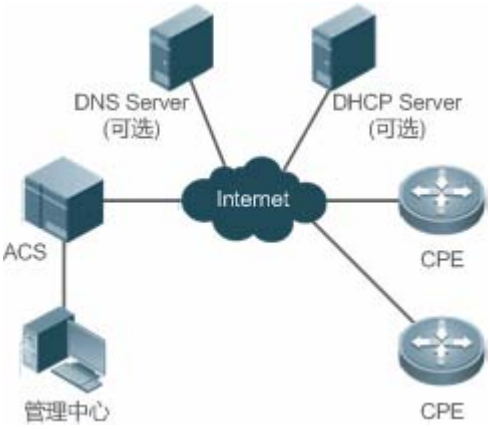
典型应用	场景描述
CWMP 网络应用场景	通过配置 CPE 设备与 ACS 服务器建立连接,以实现 CPE 设备主程序升级 ,配置文件上传，恢复等功能。

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 中直接使用的是 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

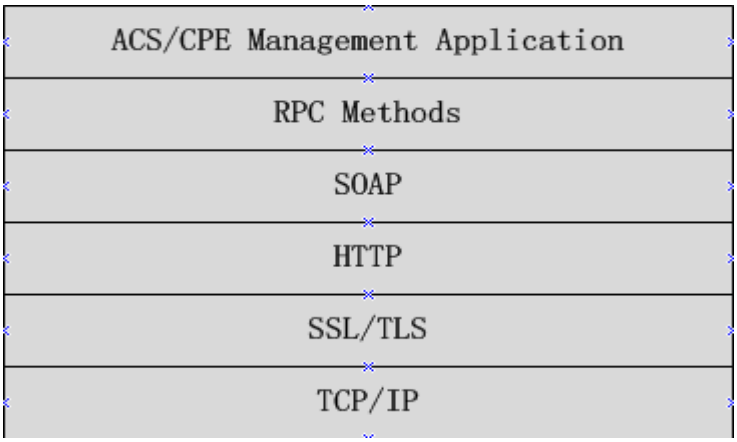
- CPE：Customer Premises Equipment (顾客预置设备)。
- ACS：Auto-Configuration Server (自动配置服务器)。

- 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

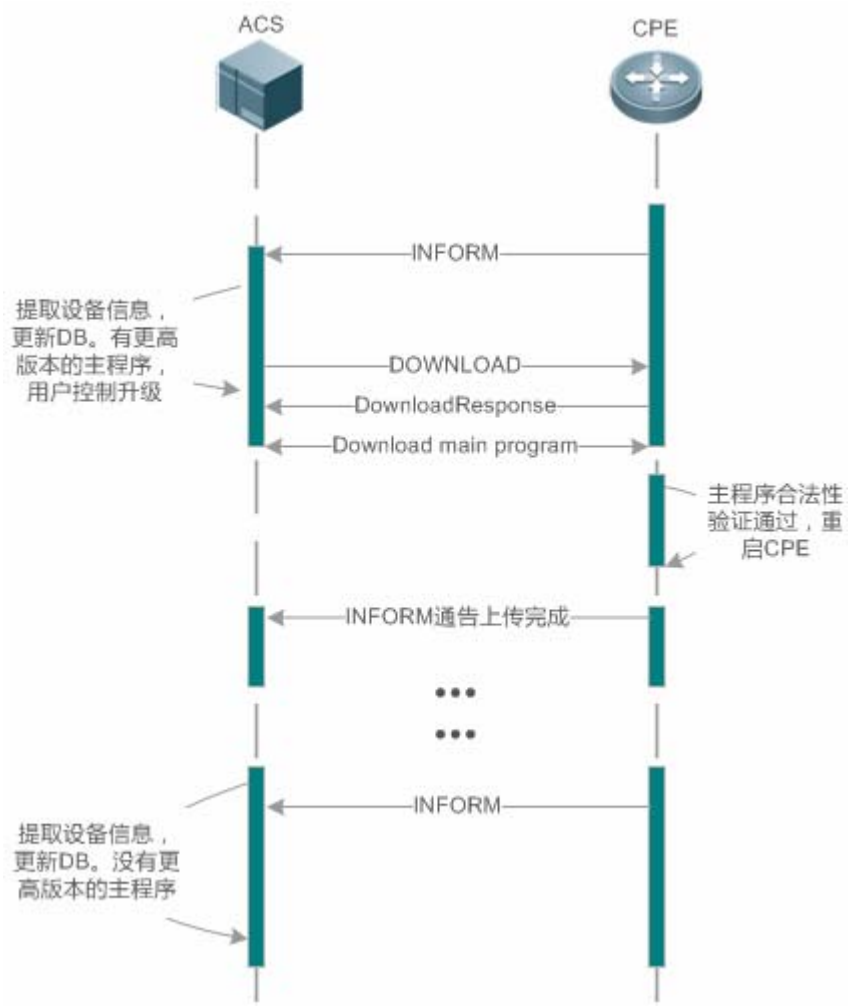
7.3.1 主程序升级

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 DownLoand 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 usrname** 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 usrname** 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

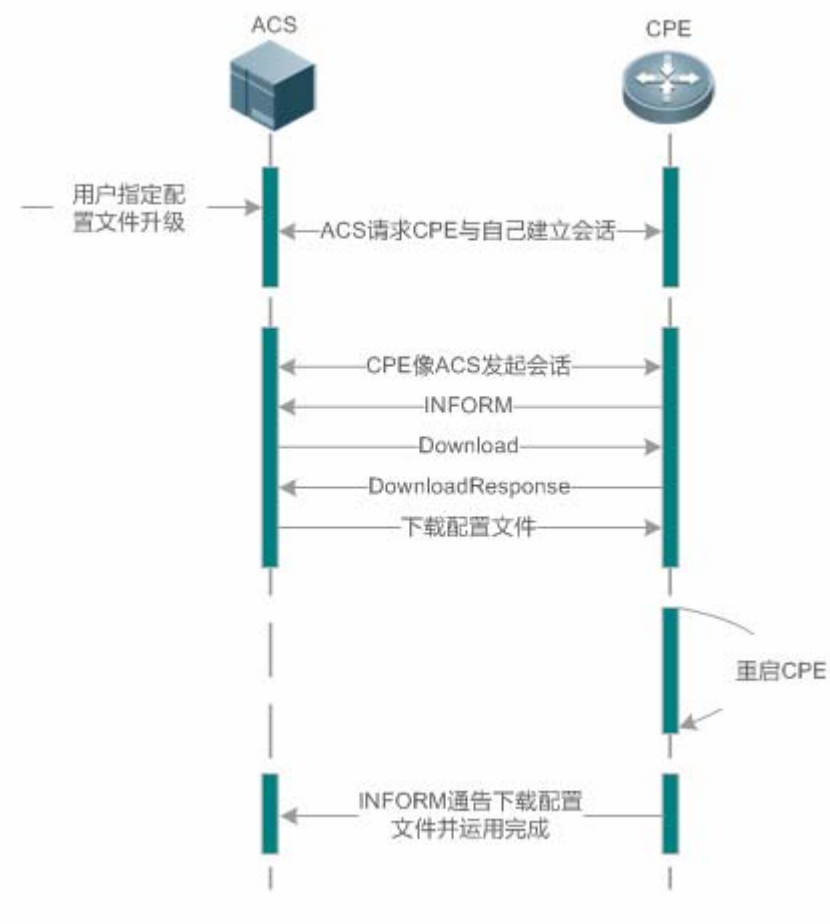
- 缺省情况下，CPE 文件下载功能为默认允许接收。
- 在 CWMP 配置模式下，使用 **no disable download** 命令开启 CPE 接受 ACS 下发的主程序和配置文件下载。

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 DownLoand 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

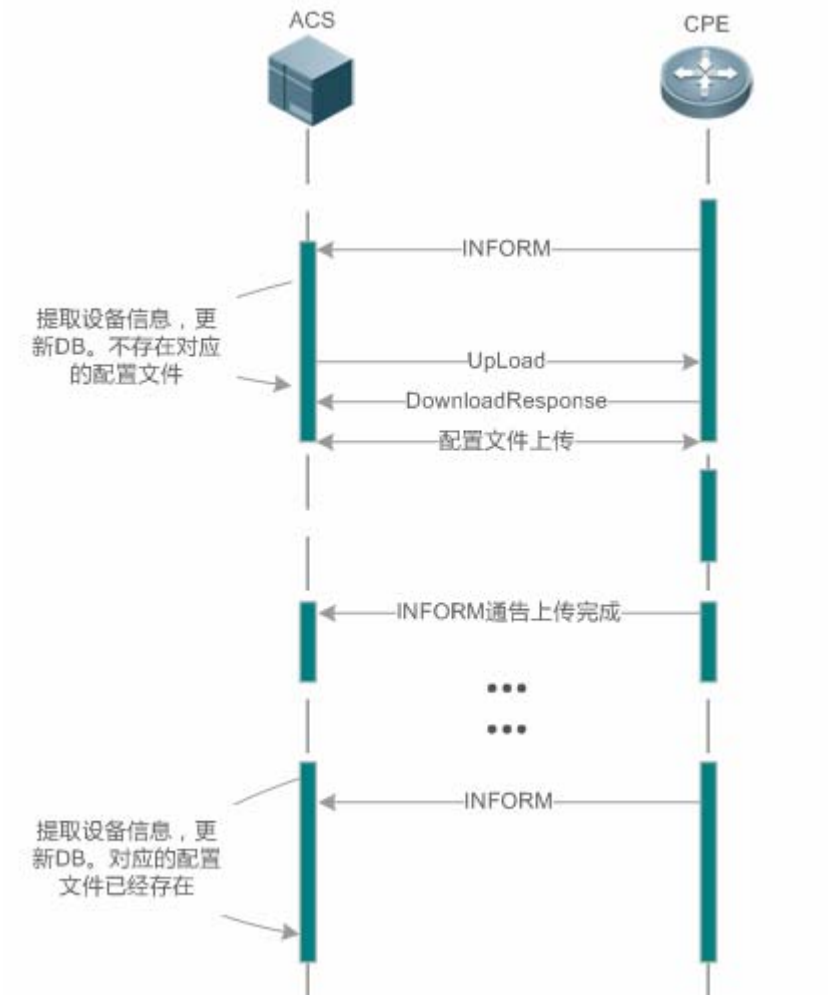
同主程序升级中的配置 cpe 文件下载功能配置

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 usrname	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 usrname	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

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秘码

【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*] [**starttime** *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 系统日志

8.1 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。

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

8.2 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。

8.2.1 系统日志输出到控制台

应用场景

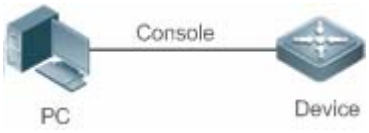
可以将系统日志输出到控制台，方便管理员监控系统的运行状态，网络部署要求如下：

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 8-1 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：

- 设置允许输出到控制台的日志信息级别为 informational（6 级）。
- 设置日志信息的过滤方向为：terminal（终端方向）。
- 设置日志信息的过滤方式为：contains-only（“只包含”过滤方式）。
- 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。

8.2.2 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 8-2 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：

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

8.3 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：

11. 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 (l ocal0)
17	local1	local use 1 (l ocal1)
18	local2	local use 2 (l ocal2)
19	local3	local use 3 (l ocal3)

20	local4	local use 4 (l ocal4)
21	local5	local use 5 (l ocal5)
22	local6	local use 6 (l ocal6)
23	local7	local use 7 (l ocal7)

12. 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。

13. 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。

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：

datatime 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

14. 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。

15. 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。

16. 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。

17. 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。

18. 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.SECFRACZ
```

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。

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。

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。

8.3.1 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、重定向日志开关、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。

8.3.2 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。

切换到旧的日志格式(即 RFC3164 日志格式)，则在 RFC5424 日志格式中使用的命令 **logging delay-send**、**logging policy**、**logging statistic** 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 ‘%’

8.3.3 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** { **sata0:***filename* | **flash:***filename* | **usb0**:*filename* | **usb1**:*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。

8.3.4 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。

如果配置的是服务器方向，可以指定具体的服务器。如可配置 **logging filter direction server 1.1.1.2** ，则过滤方向即为该服务器。当是配置该命令之前，该服务器必须存在，上述中如果服务器 **1.1.1.2** 未配置，则该过滤方向配置失败。

需要注意的是，如果配置了日志服务器全局方向，即配置了 **logging filter direction server ,** 则单独配置的过滤服务器将失效，所有的日志服务器均匹配同一个过滤规则。

↘ 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。

8.3.5 系统日志上送功能设置

日志上送功能分为分级上送、延迟上送及定时上送。在开启 RFC5424 日志格式的情况下，缺省情况下是可以往所有方向输出，并且打开日志延迟上送功能及关闭了定时上送功能；在没有开启 RFC5424 日志开关的情况下，分级上送、延迟上送、定时上送功能均不生效。

工作原理

↘ 分级上送

用户可以使用分级策略功能，将不同模块和严重级别的日志输出到不同目的地，例如：可以在命令行中配置，WLAN 模块的严重级别小于等于 4 的日志，实时发送到日志服务器；同时，WLAN 模块的严重级别大于等于 5 的日志，输出到本地日志文件中。

↘ 延迟上送

所谓的日志延迟上送功能是指：当日志触发后，不直接发送给日志服务器，而是由设备暂时缓存在日志文件中，设备每隔一定时间间隔，主动将日志文件通过 FTP 协议上传到 SYSLOG 服务器。

日志延迟发送功能主要用于：设备产生的日志信息量可能非常庞大，如果全部日志信息实时上送给服务器，设备和 SYSLOG 服务器都会存在性能压力，并对中间网络也会造成负担，而通过延迟上送给服务器的方式可以减少报文传输交互频率。

默认情况下，发送到远端服务器的日志文件名为：文件大小_设备 IP 地址_索引值.txt，若修改延迟上送的文件名，则发送到远端服务器的日志文件名为：配置的文件名前缀_文件大小_设备 IP 地址_索引值.txt；而保存在设备本地 Flash 的文件名则为：配置的文件名前缀_索引值.txt。默认的文件名前缀为 syslog_ftp_server，延迟上送的时间间隔是 3600 秒（1 小时），日志文件大小为 128K。

鉴于日志延迟上送的时间间隔最大可以设置成 65535 秒，即 18 小时，若用户将延迟上送时间间隔配置为较大的值，此时间间隔内产生的日志有可能超过一个文件的大小（128K），为了防止日志丢失，会写一个新的日志文件，并把索引值加 1，等到定时器到期后，会一次性把该时间间隔内缓存的所有日志文件发送到 FTP 或 TFTP 服务器。

由于设备上面用于缓存在本地日志文件的 Flash 空间大小有限，所以限制缓存在设备本地的日志文件个数最多为 8 个，在定时器到期之前，若缓存在设备本地的日志文件超过 8 个，则会先把之前产生的日志文件一次性发送到 FTP 或 TFTP 服务器。

定时上送

定时上送的日志主要是指设备性能统计数据的日志信息。定时上送的所有定时器都由 SYSLOG 模块统一管理，定时器到期，SYSLOG 模块就会调用各模块注册上来的日志处理函数，打印设备的性能统计日志，并实时发送给远端的 SYSLOG 服务器，服务器通过分析这些定时上送的日志来评估设备的性能。

日志定时上送的时间间隔默认为 15 分钟，为了使服务器能在同一时间点上收集到设备上的所有的性能统计日志，需要把不同统计对象的日志定时上送时间间隔设置成倍数关系，目前支持的配置值有 5 个，分别为：0、15、30、60、120，其中 0 代表关闭此统计对象的定时上送功能。

相关配置

设置日志分级上送策略

缺省情况下，设备日志是可以输出到所有方向。

使用 **logging policy module** *module-name* [**not-lesser-than**] *level* **direction** { **all** | **server** | **file** | **console** | **monitor** | **buffer** }命令在全局配置模式下配置日志分级上报时所使用的分级策略。

设置延时上送日志输出到控制台和远程终端开关

缺省情况下，延时上送的日志输出到控制台和远程终端的开关是关闭的。

使用 **logging delay-send terminal** 命令在全局配置模式下打开延时上送日志输出到控制台和远程终端。

设置延时上送日志发往服务器的文件名

缺省情况下，发送到远端服务器的日志文件名为：文件大小_设备 IP 地址_索引值.txt，若修改延迟上送的文件名前缀，则发送到远端服务器的日志文件名为：配置的文件名前缀_文件大小_设备 IP 地址_索引值.txt；而保存在设备本地 Flash 的文件名则为：配置的文件名前缀_索引值.txt，默认的文件名前缀为 syslog_ftp_server。

使用 **logging delay-send file flash:***filename* 命令在全局配置模式下配置延迟上送时缓存在设备本地的日志文件名。

设置延时上送日志发往服务器的时间间隔

缺省情况下，发往远端服务器的时间间隔是 3600 秒（1 小时）。

使用 **logging delay-send interval** *seconds* 命令在全局配置模式下配置延迟上送的时间间隔。

↘ 设置延时上送日志发往服务器的地址和上报方式

缺省情况下，不向任何 FTP 或者 TFTP Server 发送日志信息。

使用 **logging delay-send server** { *ip-address* } **mode** { **ftp user** *username* **password** [**0** | **7**] *password* | **tftp** }命令在全局配置模式下配置日志延迟上送给服务器的地址和上报方式。

↘ 日志定时上送功能开关

缺省情况下，日志定时上送功能是关闭的。

使用 **logging statistic enable** 命令在全局配置模式下开启日志定时上送功能，打开日志定时上送功能后，系统将按一定的时间间隔输出一系列的性能统计数据，方便日志服务器对系统的性能进行跟踪。

↘ 设置定时上送日志输出到控制台和远程终端开关

缺省情况下，定时上送的日志输出到控制台和远程终端的开关是关闭的。

使用 **logging statistic terminal** 命令在全局配置模式下打开定时上送日志（系统性能统计日志）输出到控制台和远程终端。

↘ 设置定时上送的时间间隔

缺省情况下，所有统计对象的定时上送时间间隔都是 15 分钟。

使用 **logging statistic mnemonic** *mnemonic* **interval** *minutes* 命令在全局配置模式下配置日志定时上送的时间间隔。

8.3.6 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。

8.4 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 [*message-type* [**uptime**| **datetime** [**msec**] [**year**]]]	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 [*level*]	设置日志信息允许输出到控制台的级别
	logging rate-limit { *number* | **all** *number* | **console** {*number* | **all** *number* } } [**except** [*severity*]]	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 [*level*]	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 [*buffer-size*] [*level*]	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 { *ip-address* } [**udp-port** *port*]	设置日志发往指定的日志服务器
	logging trap [*level*]	设置允许发往日志服务器的日志级别
	logging facility *facility-type*	设置发往服务器的日志信息的系统设备值
	logging source [**interface**] *interface-type interface-number*	设置发往服务器的日志信息的源接口
	logging source { **ip** *ip-address* }	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** { **sata0:***filename* | **flash:***filename* | **usb0**:*filename* | **usb1**:*filename* } [*max-file-size*] [level]	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
配置系统日志分级上送功能	可选配置，用于设置系统日志分级上送功能的参数信息	
	logging policy module *module-name* [**not-lesser-than**] *level* **direction** { **all** | **server** | **file** | **console** | **monitor** | **buffer** }	配置按模块和严重级别将日志输出到不同目的地
配置系统日志延迟上送功能	可选配置，用于设置系统日志延迟上送功能的参数信息	
	logging delay-send terminal	打开延时上送的日志输出到控制台和远程终端
	logging delay-send file flash:*filename*	配置延迟上送时缓存在设备本地的日志文件名
	logging delay-send interval *seconds*	配置日志延迟上送给服务器的时间间隔
	logging delay-send server { *ip-address* } **mode** { **ftp user** *username* **password** [**0** | **7**] *password* | **tftp** }	配置日志延迟上送的服务器地址和上报方式
配置系统日志定时上送功能	可选配置，用于设置系统日志定时上送功能的参数信息	
	logging statistic enable	打开日志定时上送功能
	logging statistic terminal	打开定时上送的日志输出到控制台和远程终端
	logging statistic mnemonic *mnemonic* **interval** *minutes*	配置系统某个性能统计对象的定时上报时间间隔
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

8.4.1 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系列号

- 可选配置，缺省情况下系统日志的格式中没有添加系列号。
- 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系列号

【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。

切换到旧的日志格式，则在 RFC5424 日志格式中使用的命令 **logging delay-send**、**logging policy**、**logging statistic** 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
```

8.4.2 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面配置。

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面配置。

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面配置。

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，则可以通过设置不同设备日志信息的显示级别来减少日志信息的打印。

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，从命令打开时将对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
```

8.4.3 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面配置。

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。

```
Ruijie#show logging config
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。

8.4.4 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
  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。
```

8.4.5 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】

- 在设备上面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
```

8.4.6 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** { **sata0:***filename* | **flash:***filename* | **usb0**:*filename* | **usb1**:*filename* } [*max-file-size*] [*level*]

【参数说明】 **sata0**: 日志文件选择保存在硬盘当中

flash：日志文件选择保存在扩展 FLASH 当中。

usb0：日志文件选择保存在 USB0 当中，此选项需要设备具有 1 个 USB 接口时才支持，并插入扩展的 USB 设备。

usb1：日志文件选择保存在 USB1 当中，此选项需要设备具有 2 个 USB 接口时才支持，并插入扩展的 USB 设备。

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 flie 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
```

8.4.7 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，则单个匹配规避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面配置。
- 新增可对单个日志服务器进行日志过滤配置。

↘ 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面配置。

↘ 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面配置。

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；

配置 **server** 方向时可指定某个服务器；

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

8.4.8 配置系统日志分级上送功能

配置效果

- 用户可以使用分级策略功能，将不同模块和严重级别的日志输出到不同目的地，例如：可以在命令行中配置，WLAN 模块的严重级别小于等于 4 的日志，实时发送到日志服务器；同时，WLAN 模块的严重级别大于等于 5 的日志，输出到本地日志文件中。

注意事项

- 此功能只有在开启 RFC5424 日志开关的情况下，才会生效。

配置方法

↘ 配置日志分级上送策略

- 可选配置，缺省情况下日志可以输出到所有方向上；
- 若无特殊要求，在需要分级上送策略的设备上配置。

检验方法

- 通过 **show running** 命令可以查看设置的日志分级上送策略参数信息

相关命令

配置日志分级上送策略

【命令格式】 **logging policy module** *module-name* [**not-lesser-than**] *level* **direction** { **all** | **server** | **file** | **console** | **monitor** | **buffer** }

【参数说明】 *module-name*：分级策略的模块名。

not-lesser-than：指定该选项时，代表大于等于所配置的日志级别的日志才会按照所配置的方向输出，小于所配置的日志级别的日志会被过滤掉；没有指定该选项时，代表小于等于所配置的日志级别的日志才会按照所配置的方向输出，大于所配置的日志级别的日志会被过滤掉。

level：所要配置分级策略的日志级别。

all：在所有的方向上都实行日志分级策略

server：只在发往日志服务器方向上实行日志分级策略

file：只在输出到日志文件方向上实行日志分级策略

console：只在输出到控制台方向上实行日志分级策略

monitor：只在输出到远程终端方向上实行日志分级策略

buffer：只在保存到缓冲区方向上实行日志分级策略

【命令模式】 全局配置模式

【使用指导】 用于配置系统日志按模块和严重级别输出到不同的目的地。

配置举例

配置日志分级上送功能

【网络环境】 假设有以下日志信息分级上送功能设置要求：

1、配置 SYS 模块级别大于等于 5 级的日志只往控制台方向输出；

2、配置 SYS 模块级别小于等于 3 级的日志只往缓冲区方向输出。

【配置方法】

- 在设备上面配置分级上送功能

```
Ruijie# configure terminal
Ruijie(config)# logging policy module SYS not-lesser-than 5 direction console
Ruijie(config)# logging policy module SYS 3 direction buffer
```

【检验方法】

- 通过 **show running-config | include logging policy** 命令可以查看用户配置的相关参数信息。
- 通过进入/退出配置模式产生一条模块名为 SYS 的日志，查看输出的方向是否正确。

```
Ruijie#show running-config | include logging policy
logging policy module SYS not-lesser-than 5 direction console
logging policy module SYS 3 direction buffer
```

8.4.9 配置系统日志延迟上送功能

配置效果

- 默认情况下延迟上送的功能是开启的，时间间隔为 3600 秒（1 小时），上送给远端服务器的文件名为：文件大小_设备 IP 地址_索引值.txt，且延迟上送的日志不输出控制台和远程终端；
- 可以根据设备产生延迟上送日志的频率，配置延迟上送的时间间隔，这样子可以减轻设备、SYSLOG 服务器和中间网络的负担，并且可以根据用户需要，配置上送文件的文件名；

注意事项

- 此功能只有在开启 RFC5424 日志开关的情况下，才会生效；
- 一般情况下，最好关闭延时上送的日志输出到控制台和远程终端，避免设备上打印出较多的延迟上送的日志信息，增加网络设备自身的负担；
- 配置的文件名中不能出现字符点号（.），因为系统在生成本地缓存文件时，文件名会增加索引值和后缀（.txt），索引值是以递增形式变化的；也不能出现 PC 文件命名禁止的字符，例如：\/：* “<>|。例如：配置的文件名为 log_server，当前的索引值为 5，文件大小为 1000B，发送日志文件的设备 IP 地址为 10.2.3.5，则发送给远端服务器的日志文件名为：log_server_1000_10.2.3.5_5.txt，但是保存在设备本地的日志文件名为 log_server_5.txt。
- 若网络设备上产生的延迟上送的日志信息较少，可以将延迟上送的时间间隔设置长一点，让更多的延迟上送日志集中在一起发送给远端服务器。

配置方法

↘ 配置日志延迟上送输出到控制台和远程终端

- 可选配置，缺省情况下是关闭延迟上送日志输出到控制台和远程终端；
- 若无特殊要求，在需要查看延迟上送日志的设备上配置。

↘ 配置日志延迟上送的文件名

- 可选配置，缺省情况下延迟上送的文件名为文件大小_设备 IP 地址_索引值.txt；
- 若无特殊要求，在需要修改延迟上送文件名的设备上配置。

↘ 配置日志延迟上送的时间间隔

- 可选配置，缺省情况下延迟上送的时间间隔是 3600 秒（1 小时）；
- 若无特殊要求，在需要修改延迟上送时间间隔的设备上配置。

↘ 配置日志延迟上送的服务器地址和上报方式

- 可选配置，缺省情况下是文件不发往任何远程服务器；

- 若无特殊要求，在需要发送延迟上送日志给远程服务器的设备上配置。

检验方法

- 通过 **show running** 命令可以查看设置的日志延迟上送的参数信息

相关命令

配置日志延迟上送输出到控制台和远程终端

【命令格式】 **logging delay-send terminal**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 用于打开延时上送的日志输出到控制台和远程终端。

配置日志延迟上送的文件名

【命令格式】 **logging delay-send file flash:***filename*

【参数说明】 **flash:***filename*：延迟上送的日志文件名。

【命令模式】 全局配置模式

【使用指导】 用于配置延迟上送时缓存在设备本地的日志文件名。

配置的文件名中不能出现字符点号（.），因为系统在生成本地缓存文件时，文件名会增加索引值和后缀（.txt），索引值是以递增形式改变，也不能出现 PC 文件命名禁止的字符，例如：\/：* “<>|。

例如：用户配置的文件名为 log_server，当前的文件索引值为 5，文件大小为 1000B，发送日志文件的设备 IP 地址为 10.2.3.5，则发送远端服务器的日志文件名为：log_server_1000_10.2.3.5_5.txt，但是保存在本地的日志文件名为 log_server_5.txt。

配置日志延迟上送的时间间隔

【命令格式】 **logging delay-send interval** *seconds*

【参数说明】 *seconds*：延迟上送的时间间隔（单位为秒）

【命令模式】 全局配置模式

【使用指导】 用于配置日志延迟上送给服务器的时间间隔。可以设置的范围为 600 ~ 65535，单位：秒。

配置日志延迟上送的服务器地址和上报方式

【命令格式】 **logging delay-send server** { *ip-address* } **mode** { **ftp user** *username* **password** [**0** | **7**] *password* | **tftp** }

【参数说明】 *ip-address*：接收日志信息的服务器 IP 地址。

username：指定 ftp 服务器的用户名。

password：指定 ftp 服务器的密码。

0：（可选）代表随后跟上的 *password* 为密码明文文本。

7：代表随后跟上的 *password* 为经过简单加密的密文文本。

【命令模式】 全局配置模式

【使用指导】 用于指定一个 FTP 或者 TFTP Server 来接收设备的日志信息。用户总共可以配置 5 个 FTP 或者 TFTP Server，

且每一台服务器只能配置 FTP 或 TFTP 中一种，日志信息将同时发给配置的所有 FTP 或者 TFTP Server。

配置举例

↘ 配置日志延迟上送功能

【网络环境】 假设有以下日志信息延迟上送功能设置要求：

1、开启延迟上送日志输出到控制台和远程终端；

2、延迟上送的时间间隔为 7200 秒（2 小时）；

3、延迟上送的文件名为 syslog_ruijie；

4、延迟上送的服务器 ip 地址为 192.168.23.12、用户名 admin、密码 admin 和上送方式为 FTP。

【配置方法】

- 在设备上面配置延迟上送功能

```
Ruijie# configure terminal
Ruijie(config)# logging delay-send terminal
Ruijie(config)# logging delay-send interval 7200
Ruijie(config)# logging delay-send file flash:syslog_ruijie
Ruijie(config)# logging delay-send server 192.168.23.12 mode ftp user admin password admin
```

【检验方法】

- 通过 **show running-config | include logging delay-send** 命令可以查看用户配置的相关参数信息。
- 通过在延迟上送时间间隔内，产生延迟上送的日志，定时器到期后，查看是否有文件发送到远端的 FTP 服务器。

```
Ruijie#show running-config | include logging delay-send
logging delay-send terminal
logging delay-send interval 7200
logging delay-send file flash:syslog_ruijie
logging delay-send server 192.168.23.12 mode ftp user admin password admin
```

8.4.10 配置系统日志定时上送功能

配置效果

- 默认情况下，定时上送的功能是关闭的，所有统计对象的定时上送时间间隔为 15 分钟，且定时上送的日志不输出控制台和远程终端；
- 根据需要，可以修改统计对象的定时上送时间间隔，服务器将在所有统计对象的时间间隔的最小公倍数时间点上，收集到设备的所有的性能统计日志；

注意事项

- 此功能只有在开启 RFC5424 日志格式的情况下，才会生效；

- 只有打开日志定时上送功能的开关，日志定时上送时间间隔、输出到控制台和远程终端功能设置才会生效；
- 一般情况下，最好关闭定时上送的日志输出到控制台和远程终端，避免设备上日志定时上送功能定时器到期后，打印出较多的性能统计的日志信息，增加网络设备自身的负担
- 为了使服务器能在同一时间点上收集到设备上的所有的性能统计日志，当修改某一个统计对象的时间间隔，都会重新启动所有统计对象的定时上送的定时器。

配置方法

配置日志定时上送功能开关

- 可选配置，缺省情况下日志定时上送功能是关闭的；
- 若无特殊要求，在需要打开定时上送功能的设备上配置。

配置日志定时上送输出到控制台和远程终端

- 可选配置，缺省情况下定时上送日志输出到控制台和远程终端是关闭的；
- 若无特殊要求，在需要查看定时上送日志的设备上配置。

配置日志助记符定时上送的时间间隔

- 可选配置，缺省情况下所有统计对象的定时上送时间间隔都是 15 分钟；
- 若无特殊要求，在需要修改统计对象定时上送时间间隔的设备上配置。

检验方法

- 通过 **show running** 命令可以查看设置的日志定时上送功能参数信息

相关命令

配置日志定时上送功能开关

【命令格式】 **logging statistic enable**
【参数说明】 -
【命令模式】 全局配置模式
【使用指导】 用于打开日志定时上送功能，打开日志定时上送功能后，系统将按一定的时间间隔输出一系列的性能统计数据，方便日志服务器对系统的性能进行跟踪。

配置日志定时上送输出到控制台和远程终端

【命令格式】 **logging statistic terminal**
【参数说明】 -
【命令模式】 全局配置模式
【使用指导】 用于打开定时上送的日志输出到控制台和远程终端。

↘ 配置日志助记符定时上送的时间间隔

【命令格式】 **logging statistic mnemonic** *mnemonic* **interval** *minutes*

【参数说明】 *mnemonic*：日志定时上送的助记符字符串，用于标识系统性能统计对象。

minutes：定时上送的时间间隔，单位：分钟。

【命令模式】 全局配置模式

【使用指导】 用于配置系统某个性能统计对象的定时上报时间间隔。可以设置的时间间隔为 0、15、30、60、120 分钟，其中 0 表示关闭此统计对象的定时上送功能。

配置举例

↘ 配置日志分级上送功能

【网络环境】 假设有以下日志信息定时上送功能设置要求：

1、定时上送的功能是开启的；

2、开启定时上送日志输出到控制台和远程终端；

2、设置统计对象 TUNNEL_STAT 的定时上送的时间间隔为 30 分钟。

【配置方法】

- 在设备上面配置定时上送功能

```
Ruijie# configure terminal
Ruijie(config)# logging statistic enable
Ruijie(config)# logging statistic terminal
Ruijie(config)# logging statistic mnemonic TUNNEL_STAT interval 30
```

【检验方法】

- 通过 **show running-config | include logging statistic** 命令可以查看用户配置的相关参数信息。
- 通过在定时上送功能定时器到期后，查看是否有定时上送的日志产生，且在所有定时上送定时器时间间隔的最小公倍数时间点上，查看是否产生所有性能统计日志。

```
Ruijie#show running-config | include logging statistic
logging statistic enable
logging statistic terminal
logging statistic mnemonic TUNNEL_STAT interval 30
```

8.4.11 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.
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
```

8.4.12 配置系统日志语言

配置效果

- 默认情况下，设备的语言设置为中文，此时设备支持打印中文日志的模块将输出中文日志，可通过配置命令来设置设备当前语言为其他语言。
- 默认情况下，设备的语言设置为英文，此时设备支持打印中文日志的模块将输出中文日志，可通过配置命令来设置设备当前语言为其他语言。

注意事项

- 该配置命令全局配置模式下面进行配置。

配置方法

↘ 设置系统日志当前语言

- 可选配置，缺省情况下系统当前语言为中文。
- 可选配置，缺省情况下系统当前语言为英文。

检验方法

- 通过 **show running** 命令可以查看设置的系统日志当前语言信息

相关命令

设置系统日志语言

【命令格式】 **logging language** { **Chinese** | **English** }

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 此命令设置系统日志语言。

配置举例

配置系统日志语言

【网络环境】 设置当前系统日志语言为英文（默认为中文）。

【配置方法】

- 在全局配置模式下配置

```
Ruijie# configure terminal
Ruijie(config)# logging language English
```

【检验方法】

- 通过 **show running-config | in logging** 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 language English
 login local
```

【网络环境】 设置当前系统日志语言为中文（默认为英文）。

【配置方法】

- 在全局配置模式下配置

```
Ruijie# configure terminal
Ruijie(config)# logging language Chinese
```

【检验方法】

- 通过 **show running-config | in logging** 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 language Chinese
 login local
```

8.4.13 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
```

8.5 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**

9 LED

9.1 概述

LED（LightingEmittingDiode）即发光二极管的简称，是一种半导体固体发光器件。在 AP 上用来做状态指示灯，根据 AP 的不同状态，显示不同的颜色。

下文仅介绍 LED 的相关内容。

协议规范

无

9.2 典型应用

无

9.3 功能详解

我司 AP 上通常都有一个或者多个 LED 灯，用来表示 AP 的工作状态。例如，以太口有数据流的时候，以太口的 LED 灯就会闪烁。通常 LED 灯是通过 GPIO 或者 CPLD 来控制的，通过操作 GPIO 或者 CPLD，来改变灯的颜色状态，例如，绿色常亮、绿色闪烁和红色闪烁等。通过 LED 灯的不同颜色状态，来判断 AP 的工作状态是否正常。当 AP 出现故障时，也可以很容易通过灯的颜色状态来初步得出 AP 是什么故障。

9.4 配置详解

配置项	配置建议 & 相关命令	
配置 AP 定位	可选配置。用于定位 AP 的位置	
	led on	点亮 AP 定位 LED 灯
配置静默模式	可选配置。配置 led 灯为静默状态	
	quiet-mode session	配置 led 静默模式

9.4.1 配置AP定位

配置效果

- AP 上用于定位的 LED 灯会亮起

注意事项

- 完成定位后，必须关闭配置，否则 led 灯的状态将不会再变化

配置方法

↘ 配置 AP 定位灯

- 可选配置。
- 当需要定位某台 AP 的位置时，可开启此配置，定位完后，请关闭此配置。

【命令格式】 **led on**
【参数说明】 -
【缺省配置】 缺省是关闭的
【配置模式】 AP 配置模式
【使用指导】 此命令用来打开 AP 定位灯，以便于定位 AP 的位置。

检验方法

- 检查 AP 定位 LED 灯是否亮起

配置举例

↘ 定位 AP 00d0.f822.33bc 的位置

【网络环境】 无

【配置方法】 在 AC 上配置打开 led 定位灯

AC

```
Ruijie# configure terminal
Ruijie(config)# ap-config 00d0.f822.33bc
Ruijie(ap-config)# led on
```

【检验方法】 检查 AP 上的定位灯是否亮起

常见错误

无

9.4.2 配置静默模式

配置效果

- 配置生效时，AP 上所有 LED 灯都会熄灭。

注意事项

- 必须先配置静默状态生效的时间

配置方法

↘ 配置 session

- 可选配置。
- 配置静默模式时，必须要向创建 session
- 配置 session 生效的时间

【命令格式】 **schedule session** *sid* **time-range** *n* **period** *day1* [**to** *day2*] **time** *hh1:mm1* **to** *hh2:mm2*

【参数说明】 sid：调度 session ID

n：调度 session 时间段编号

day1：调度 session 时间段的周期，day1 表示调度周期开始日期。日期有效值 { sun | mon | tue | wed | thu | fri | sat }

to day2：day2 表示调度周期结束日期，to day2 缺省表示调度时间段的周期只有一天。

time hh1:mm1 to hh2:mm2：调度 session 时间范围：hh1:mm1 和 hh2:mm2 分别是起始时间和结束时间的小时和分钟。小时取值范围[0，23]，分钟取值范围[0，59]

【缺省配置】 调度 session 时间段为空

【命令模式】 全局配置模式

【使用指导】 必现先创建一个 session

↘ 配置静默模式

- 可选配置。
- 配置 led 静默模式的 session

【命令格式】 **quiet-mode session** *session-num*

【参数说明】 session-num：指定 session-id

【缺省配置】 缺省是关闭的

【配置模式】 AP 配置模式

【使用指导】 必须先配置 session

检验方法

- 当系统时间在静默模式的时间范围内时，AP 上的所有 LED 都不亮。

配置举例

↘ 配置每周一晚上 11 点到周二早上 7 点的 LED 灯为静默模式

【配置方法】
- 配置 session
- 配置静默模式使用的 session-id

```
Ruijie# configure terminal
Ruijie(config)#schedule session 1
Ruijie(config)#schedule session 1 time-range 1 period Mon time 23:00 to 7:00
Ruijie(config)#ap-config 00d0.f822.33bc
Ruijie(config-ap)#quiet-mode session 1
```

【检验方法】 当系统时间在 session 配置的时间范围内时，AP 上所有的 LED 灯都会熄灭

常见配置错误

- 配置的 session id 不存在

9.5 监视与维护

清除各类信息

无

查看运行情况

无

查看调试信息

无

10 异常告警

10.1 概述

异常信息告警是当设备出现一些异常情况时，发送邮件给设备管理员。供管理员监控设备运行情况、针对某些异常更改配置或其它处理，让各功能或设备本身更好的工作。

异常告警涉及很多方面如设备受攻击、CPU 温度高、流量接近阈值等。这些都需要各模块配合一起完成监控。如 CPU 温度高，由驱动监控 CPU 温度，当达到一定值时把相关信息通告到异常告警模块； 又如流量接近阈值，由流控模块监控，达到一定值时，通告相关信息。

下文仅介绍异常告警的相关内容。

协议规范

- RFC821：Simple Mail Transfer Protocol, SMTP

10.2 典型应用

典型应用	场景描述
设备受到攻击发出异常告警邮件	设备受到攻击发出异常告警

10.2.1 设备受到攻击发出异常告警邮件

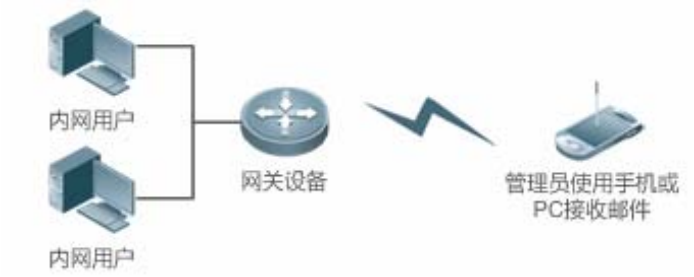
应用场景

1、 设备受到内网某 IP 攻击，首先由防攻击模块检测到攻击，收集信息后通知异常告警模块。

2、 异常告警模块将异常信息封装成邮件正文发送到设置的邮箱。

3、 登录设备 WEB 内网攻击 IP 地址做出处理，如屏蔽该用户。

图 10-1



功能部属

- 设备只需配置 DNS 服务器，并连接到 Intranet 。

10.3 功能详解

基本概念

SMTP 服务器（即发送邮件服务器）

用户发送一封邮件的流程为：

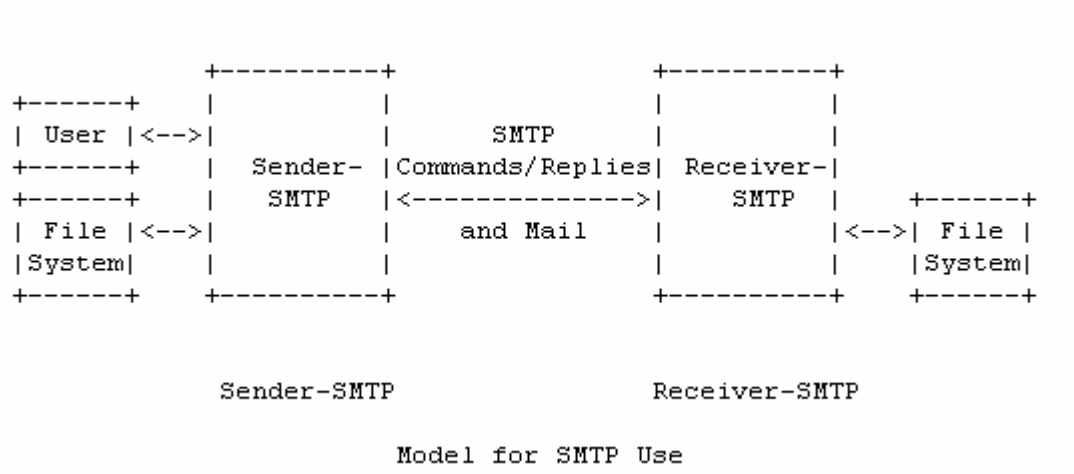
1、 用户的邮件首先投递到 SMTP 服务器

2、 SMTP 服务器将邮件分类处理后再发到收件方的接收邮件服务器。

3、 接收邮件服务器再转发到收件人邮箱。

该过程的工作原理如下：

图 10-2



SMTP 的工作模式

SMTP 服务器就是上图中的 Sender-SMTP，相当于发件方的邮局。

Foxmail、Outlook 等常见的邮件客户端软件，工作在上图中的 User 或 File System。

异常告警功能邮件的发送流程，就跟这些软件类似。特点是需要输入发件人的邮箱帐号、密码，邮件送达的成功率高。

使用异常告警功能，用户必须正确配置 SMTP 服务器和邮箱的帐号密码。

功能特性

功能特性	作用

异常告警	异常告警是通过监控设备或功能的运行参数，发现有异常就发送邮件通知用户。
邮件服务	开启用户发送邮件使用的服务。
接收信息的邮箱	配置用于接收异常告警信息的邮箱
邮件发送频率	告警邮件发送频率觉得信息的实时性，频率越小越能及时收到邮件。但某些情况下可能收到过多邮件，如遇到内网攻击的时候。

10.3.1 异常告警

异常告警是通过监控设备或功能的运行参数，发现有异常就发送邮件通知用户。

工作原理

告警选项

告警选项包括很多，如 CPU 温度高、设备受攻击、总流量超过限制等。这些选项信息由多个模块负责监控。

用户可以配置关注的选项，设备将关注选项出现异常的信息发送到用户邮箱。不关注的选项，即使异常也不发邮件。

相关配置

开启异常告警功能

缺省情况下，功能关闭。

使用 feedback user enable 命令可以开启或关闭异常告警功能。

配置忽略的告警选项

缺省情况下，关注当前支持的所有选项。目前包括：cpu 温度过高、设备受攻击、总带宽超过限制、流控异常、主板温度过高等。

使用 feedback ignore 命令可以配置忽略或关注选项。配置忽略后，该项即使异常也不发邮件。

10.3.2 邮件服务

邮件服务是指设备构造邮件，并发送到指定收件人邮箱。

工作原理

开启邮件服务

功能开关。

SMTP 服务器

根据 SMTP 协议发送服务器就是 Sender-SMTP，用于发送方投递邮件。相当于发送方的邮局。

现在很多常用的邮箱，如 QQ、网易、新浪等，支持 SMTP 协议。但有些需要登录邮箱后手动开通 SMTP 服务才能使用。对应的 SMTP 服务器地址也可以从网页上了解，如 QQ 邮箱的是：qq.smtp.com。

↘ 邮箱帐号、密码

输入的邮箱帐号和密码，是作为发件人信息封装到邮件中。所有支持 SMTP 协议的邮箱帐号均可使用。

相关配置

↘ 开启邮件服务

缺省情况下，功能开启。

使用 mail-service enable 可以开启或关闭邮件服务。

↘ 配置 SMTP 服务器

无缺省配置。

SMTP 服务器地址可以从邮箱网站上查找。

使用 mail-client smtp server 可以配置 SMTP 服务器。

↘ 配置邮箱的帐号、密码

无缺省配置。

目前常用的邮箱都可使用，如 QQ、sina、163 等。

有些邮箱默认开启 SMTP 服务器，有些则默认关闭。如果发现无法发送邮件，请使用浏览器登录邮箱，配置开启 SMTP 服务。

使用 mail-client username 命令可以配置邮箱的帐号、密码。

10.3.3 接收信息的邮箱

接收地址是用于设置接收异常告警邮件。一般是网络管理员的邮箱。

工作原理

设备封装邮件时，作为邮件的收件人。配置多个时，各收件人都能收到告警邮件。

相当于写邮件时填写的收件人，如：

图 10-3



相关配置

配置收件人

无缺省配置。

配置收件人地址，可配置多个，最多 6 个。

10.3.4 邮件发送频率

设备检测到异常信息后，多长时间发送告警邮件，由发送频率决定。

工作原理

邮件发送频率

邮件发送采用定时触发。如，频率设置为 1 小时，则发送 1 小时内检测到的异常信息。

相关配置

配置发送频率

缺省情况下，频率为 1 小时。

可以使用 feedback frequency 配置发送频率，配置范围是<5~10080>，单位为分钟。值越小发送频率越高。因此，如果需要及时收到信息，就需要将该值调整得相对小一些。而网络中存在较多异常，又不想接收过多邮件的用户，可将频率设置大一些。

10.4 配置详解

配置项	配置建议 & 相关命令	
异常告警功能基本配置	⚠ 必须配置。用户配置异常告警功能的基本信息。	
	feedback user enable	开启异常告警功能。
	mail-service enable	开启邮件服务。默认开启。

	mail-client smtp server	配置 SMTP 服务器
	mail-client username	配置邮箱的帐号、密码
	feedback subscriber	配置接收告警信息的邮箱
配置发送邮件频率	⚠ 可选配置。用于调整发送邮件频率。	
	feedback frequency	配置邮件发送邮件频率
公网模式下配置邮件服务源 IP	⚠ 公网模式下必须配置，其他模式不要配置。	
	mail-service source	配置邮件源 IP，公网模式下必须配置，非公网模式下不要配置。

10.4.1 异常告警功能基本配置

配置效果

- 异常告警所需的所有功能，能够让设备封装邮件并发送到指定邮箱。
- 接收邮件的地址可重复多次配置不同帐号，最多支持 6 个。

注意事项

- SMTP 服务器地址和邮箱的帐号密码是在发送邮件时用到，必须正确配置。
- 接收邮件的地址，是指需要收到告警信息的邮箱。可同时配置多个，也可以与输入帐号密码的邮箱是同一个。

配置方法

↘ 开启异常告警功能

- 必须配置。默认关闭。

↘ 开启邮件服务

- 必须配置。默认开启。

↘ 配置 SMTP 服务器

- 必须配置。

↘ 配置邮箱帐号密码

- 必须配置。

↘ 配置接收告警信息的邮箱

- 必须配置。可与上面配置的帐号是同一个邮箱。

- 需要多人接收信息时，可配置多个，最多可配置 6 个。

检验方法

可使用命令 mail-client check，查看邮件相关的配置是否正确。如果正确，配置帐号密码的那个邮箱，将收到一封测试邮件。

相关命令

开启异常告警功能

【命令格式】 **feedback user enable**
【参数说明】 -
【命令模式】 全局配置模式
【使用指导】 -

开启邮件服务

【命令格式】 **mail-service enable**
【参数说明】 -
【命令模式】 全局配置模式
【使用指导】 -

配置 SMTP 服务器

【命令格式】 **mail-client smtp server** *addr*
【参数说明】 **server** *addr* ：smtp 服务器地址。
【命令模式】 全局配置模式
【使用指导】 可从邮箱网页上查找 smtp 服务器。

配置接收信息的邮箱

【命令格式】 **feedback subscriber** *mail-addr*
【参数说明】 **subscriber** *mail-addr* ：接收信息的邮箱地址。
【命令模式】 全局配置模式
【使用指导】 重复该命令可配置多个。
最多可配置 6 个。

配置接收信息的邮箱

【命令格式】 **feedback subscriber** *mail-addr*
【参数说明】 **subscriber** *mail-addr* ：接收信息的邮箱地址。
【命令模式】 全局配置模式
【使用指导】 重复该命令可配置多个。
最多可配置 6 个。

配置举例

↘ 开启异常告警功能，配置基本信息

配置方法 开启异常反馈功能，开启邮件服务。

配置邮箱发送服务器和帐号密码，再配置收件人。

```
Ruijie# configure terminal
Ruijie(config)# feedback user enable
Ruijie(config)# mail-service enable
Ruijie(config)# mail-client smtp server smtp.126.com
Ruijie(config)# mail-client username ruijie@126.com password ******
Ruijie(config)# feedback subscriber UserA@ruijie.com.cn UserB@126.com UserC@qq.com
Ruijie(config)# end
```

【检验方法】 查看相关配置是否正确。

```
Ruijie # mail-client check
Connect to smtp server. OK！
Login to smtp server. OK!
Send a test mail. OK!
Check OK！
```

常见错误

- smtp 服务器错误
- 邮箱帐号或密码错误
- 邮箱未开启 smtp 服务

10.4.2 配置发送邮件频率

配置效果

- 调整异常告警信息邮件的发送频率。数值越小，越能及时收到邮件，数值越大越不及时。

注意事项

- 数值过小如果设备存在异常，会短时间内收到大量邮件。
- 数值过大，设备在异常出现较长时间后，才能收到告警邮件。

配置方法

- 默认 1 小时。如无特殊要求，可不配置。
- 如果设备存在异常，又不希望短时间内收到太多邮件，需要将数值设置大一些。

检验方法

无

相关命令

↘ 配置发送邮件频率

【命令格式】 **feedback frequency** *min*

【参数说明】 **frequency** *min*：发送邮件频率，单位为分钟，可配置范围：5-10080。

【命令模式】 全局模式

【使用指导】 如未配置，默认为 1 小时。

配置举例

↘ 配置发送邮件频率为 1 小时。

【配置方法】
- 配置发送邮件频率为 1 小时。

```
Ruijie# configure terminal
Ruijie(config)# feedback frequency 60
Ruijie(config)# end
```

【检验方法】 -

常见配置错误

- 无

10.4.3 公网模式配置邮件服务源IP

配置效果

- 公网模式下，必须配置，否则告警邮件无法发送。

注意事项

- 公网模式下，必须配置，否则告警邮件无法发送，其他模式不能配置。

配置方法

- 默认未配置。公网模式必须配置。

检验方法

无

相关命令

配置源 IP

【命令格式】 **mail-service source** *ip*

【参数说明】 *ip*：源 IP，典型值为 LAN 口 IP，在 WAN 口 IP 无法访问大网，LAN 口 IP 可以访问大网时配置。

【命令模式】 全局配置模式

【使用指导】 公网模式下必须配置，其他模式不能配置。

配置举例

配置源 IP 为 1.1.1.1。

【配置方法】

- 配置源 IP 为 1.1.1.1。

```
Ruijie# configure terminal
Ruijie(config)# mail-service source 1.1.1.1
Ruijie(config)# end
```

【检验方法】 -

常见配置错误

- 无

10.5 监视与维护

检验配置

⚠ 在配置 SMTP 服务器和邮箱帐号密码后，执行该命令。

作用	命令
检查邮件配置是否正确。	**mail-client check**

查看信息

作用	命令
查看当前支持的	**show feedback items**

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
打开调试开关。	**debug feedback info**

11 HTTP 服务

11.1 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。

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

协议规范

- RFC1945：Hypertext Transfer Protocol -- HTTP/1.0
- RFC2616：Hypertext Transfer Protocol -- HTTP/1.1
- RFC2818：Hypertext Transfer Protocol Over TLS -- HTTPS

11.2 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。
典型应用	场景描述
HTTP 远程升级服务	使用 HTTP 升级功能进行文件升级。

11.2.1 HTTP应用服务

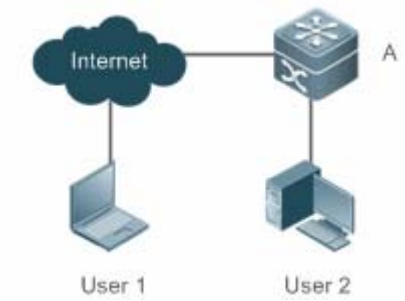
应用场景

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。
- 用户可以根据实际情况，选择在设备上单独启用 HTTPS 服务或者 HTTP 服务，也可以同时启用 HTTPS 和 HTTP 服务。
- 用户还可以再浏览器上设置使用 HTTP/1.0 还是 HTTP/1.1 协议来访问设备的 HTTP 服务。

图 11-1



【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。
- 设备运行 HTTPS 协议，用户在 PC 浏览器中通过 https：//设备的 ip 地址，访问设备。

11.2.2 HTTP远程升级服务

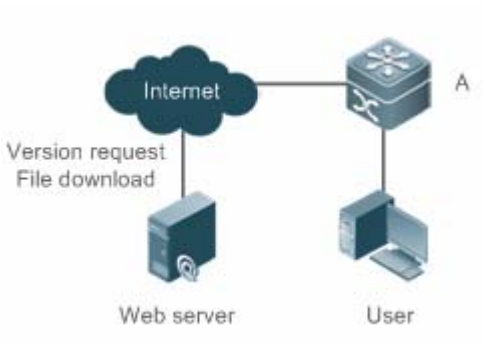
应用场景

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

以下图为例，用户使用 HTTP 远程升级功能进行文件升级。

- 设备每天定时远程获取锐捷服务器中可升级的文件信息。
- 从服务器中下载最新文件，并更新升级设备。

图 11-2



【注释】 A 为锐捷设备。

User 为用户 PC

Web server 为锐捷服务器

功能部署

- 设备运行 HTTP 协议，用户直接通过浏览器向设备下发命令，从 Web server 获取最新版本的可升级文件。

11.3 功能详解

基本概念

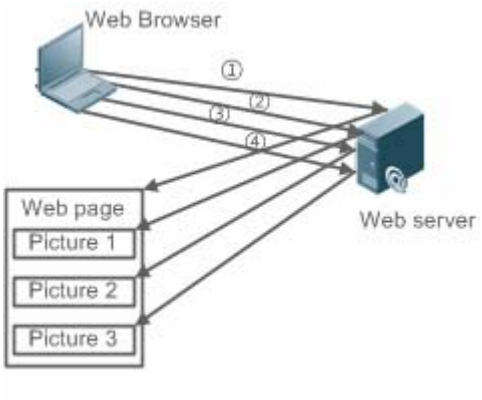
↘ HTTP 服务

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劲的过程，从而严重影响了客户机和服务器的性能，如下图所示。

图 11-3



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 11-4



目前，锐捷设备支持 HTTP/1.0 和 HTTP/1.1 两种协议版本。

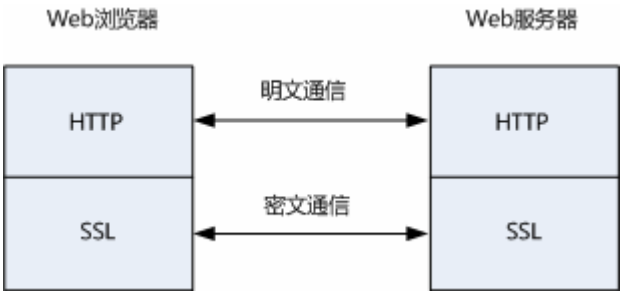
设备使用哪种协议版本由 Web 浏览器决定。

HTTPS 服务

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

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

图 11-5



↘ HTTP 升级服务

HTTP 升级包括 HTTP 本地升级和 HTTP 远程升级两种方式。

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

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 远程升级服务	设备作为客户端连接到远程 HTTP 服务器上，通过获取服务器上的文件来实现本地文件的升级。
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。

11.3.1 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，HTTPS 服务默认端口号是 443。
- 客户端向服务器发送请求消息。
- 服务器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 服务和 HTTPS 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 服务端口

缺省情况下，HTTP 服务端口为 80。

使用 **ip 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。

↘ 配置 HTTPS 服务端口

缺省情况下，HTTPS 服务端口为 4430。

使用 **ip http secure-port** 命令可以配置 HTTPS 服务端口号，取值范围是 443 及 1025-65535。

通过配置 HTTPS 服务端口号，可以减少非法用户对 HTTPS 服务的攻击。

11.3.2 HTTP远程升级服务

设备作为客户端连接到远程 HTTP 服务器上，通过获取服务器上的文件来实现本地文件的升级。

工作原理

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

相关配置

↘ 配置升级服务器地址

缺省情况下，HTTP 远程升级配置的服务器地址是 0.0.0.0，端口号是 80。

使用 **http update server** 命令可以配置 HTTP 远程升级服务器的地址和端口号。

HTTP 升级时，优先连接本命令配置的服务器地址，如果连接不上，则会逐个尝试连接本地记录的服务器地址，如果所有服务器都无法连接，则无法进行升级。

↘ 配置 HTTP 升级模式

缺省情况下，HTTP 采用自动升级模式。

使用 **http update mode** 命令可以配置 HTTP 升级模式为手动升级模式。

↘ 配置 HTTP 自动升级时间

缺省情况下，HTTP 远程自动升级时间是随机的。

使用 **http update time** 命令可以改变自动升级时间，只能配置每天的某一个时间，精确度为分钟。

通过配置该命令，如果升级方式是自动升级模式，设备每天定时在配置的时间对服务器上的文件进行检测升级。

↘ 检测 HTTP 服务器中可升级的文件信息

缺省情况下，检测 HTTP 升级文件信息功能关闭。

使用 **http check-version** 命令可以检测 HTTP 服务器中可升级的文件信息。

通过配置该命令，可以检测到服务器中比本地更新的文件信息。

↘ 手动升级文件

使用 **http update** 命令手动升级文件。

11.3.3 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。

11.4 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
	ip http port	配置 HTTP 服务端口
	ip http secure-port	配置 HTTPS 服务端口
配置 HTTP 远程升级	⚠ 必须配置。用于实现 HTTP 远程升级。	
	http update server	配置 HTTP 升级服务器
	http update mode	配置 HTTP 升级模式
	http update time	配置 HTTP 自动检测时间
	http check-version	检测 HTTP 服务器中可升级的文件信息
	http update	手动升级文件

11.4.1 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。

↘ 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。

↘ 配置 HTTPS 服务端口

- 如果要求改变 HTTPS 服务端口，则必须配置 HTTPS 服务端口。
- 若无特殊要求，可以使用默认的 HTTPS 服务端口 4430 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。
- 用户在浏览器上输入 https：//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** | **https** | **all**]

【参数说明】 **http** | **https** | **all** :打开相应的服务。**http** 为打开 HTTP 服务 ,**https** 为打开 HTTPS 服务 ,**all** 为同时打开 HTTP 和 HTTPS 服务。缺省为同时打开 HTTP 和 HTTPS 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 服务和 HTTPS 服务；如果跟 **http** 关键字，则表示只打开 HTTP 服务；如果跟 **https** 关键字，则表示只打开 HTTPS 服务。

使用 **no enable service web-server** 或者 **default enable service web-server** 用于关闭相应的 HTTP 服务。如果该 **no 命令或 default** 命令后面不跟任何关键字，则表示关闭 HTTP 服务和 HTTPS 服务。

配置 HTTP 服务端口

【命令格式】 **ip 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 HTTPS 服务端口

【命令格式】 **ip http secure-port** *port-number*

【参数说明】 *port-number*：设置 HTTPS 服务端口，取值范围为 443 及 1025-65535。

【命令模式】 全局模式

【使用指导】 使用该命令设置 HTTPS 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，也可以通过 HTTPS 协议访问。
- 要求自己配置 HTTP 服务端口，减少非法用户对 HTTP 的攻击。

【网络环境】

图 11-6



【配置方法】
- 需要配置同时打开 HTTP 和 HTTPS 服务。
- 可以配置 HTTP 服务端口号为 8080；HTTPS 服务端口号为 4430.

A

```
A#configure terminal
A(config)# enable service web-server
A(config)# ip http port 8080
A(config)# ip http secure-port 4430
```

【检验方法】 A

- 查看 HTTP 配置信息。

```
A(config)#show web-service
webservice  :
  http      : enable
            : port(8080)
  https     : enable
            : port(4430)
```

常见错误

- 如果 HTTP 服务端口不是默认的 80 与 4430 ,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。

11.4.2 配置HTTP远程升级

配置效果

- 设备作为客户端连接到远程 HTTP 服务器上，通过获取服务器上的文件来实现本地文件的升级。

注意事项

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

配置方法

↘ **配置 HTTP 升级服务器**

- 如果要求改变 HTTP 远程升级配置的服务器地址和端口号，必须配置。
- 若无特殊要求，不需要在每台设备上配置 HTTP 升级服务器。

↘ **配置 HTTP 升级模式**

- 如果要求 HTTP 升级模式为手动升级模式，则必须配置。
- 若无特殊要求，默认 HTTP 升级模式是自动升级的。

↘ **配置 HTTP 自动升级时间**

- 如果要求改变 HTTP 自动升级时间，则必须配置。
- 若无特殊要求，默认 HTTP 自动升级时间是随机的。

↘ **检测 HTTP 服务器中可升级的文件信息**

- 如果要求检测 HTTP 服务器中可升级的文件信息，则必须配置。
- 若无特殊要求，无需配置，因为默认就是自动升级。

↘ **手动升级文件**

- 必须配置。
- 若无特殊要求，应在每台设备上配置手动升级文件。

检验方法

- 执行 **ping** 命令，验证设备可以与服务器建立连接。
- 执行 **http check-version**，设备可以获取到相关文件的版本信息。

相关命令

配置 HTTP 升级服务器

【命令格式】 **http update server** { *host-name* | *ip-address* } [**port** *port-number*]

【参数说明】 *host-name*：服务器域名。

ip-address：服务器地址。

port *port-number*：服务器端口号，取值范围为 1-65535，缺省为 80。

【命令模式】 全局模式

【使用指导】 通过本命令配置 HTTP 升级的服务器地址和端口号。

HTTP 升级时，优先连接本命令配置的服务器地址，如果连接不上，则会逐个尝试连接本地记录的服务器地址。如果所有服务器都无法连接，则无法进行升级。

系统内部会记录 1 个或多个升级服务器的地址信息，这些地址不允许修改。

⚠ 服务器地址可不配置，因为本地升级记录文件中记录了可能的升级服务器地址。

⚠ 默认需要开启设备的 DNS 功能，并配置 DNS 服务器地址。

配置 HTTP 升级模式

【命令格式】 **http update mode manual**

【参数说明】 **manual**：手动升级模式。

【配置模式】 全局模式

【使用指导】 使用该命令配置 HTTP 升级模式。

配置该命令，HTTP 是手动升级模式。

执行该命令的 **no** 形式，HTTP 是自动升级模式，自动升级时间到，默认会检测服务器可升级的文件信息，并自动下载升级。

配置 HTTP 自动升级时间

【命令格式】 **http update time daily** *hh*:*mm*

【参数说明】 *hh*:*mm*：具体升级时间，格式为小时（24 小时制）:分钟。

【配置模式】 全局模式

【使用指导】 通过本命令配置 HTTP 自动升级时间，设备自动在每天的指定时间连接到 Web 服务器(rgos.ruijie.com.cn)检测是否有可升级的文件信息。获取到的文件信息可以通过 Web 界面查看。

执行该命令的 **no** 形式，设备升级时间是随机。

检测 HTTP 服务器中可升级的文件信息

【命令格式】 **http check-version**

【参数说明】 -

【配置模式】 特权模式

【使用指导】 用户通过本命令检测需要升级的文件类型，检测到的是服务器比本地更新的文件。

手动升级文件

【命令格式】 **http update** { **all** | *string* }

【参数说明】 **all**：升级所有的业务模块

string：需要升级业务模块名称。

【配置模式】 特权模式

【使用指导】 用户通过本命令手动升级指定的业务模块或升级全部的业务模块。

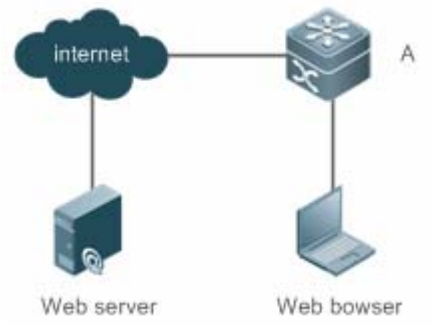
配置举例

使用 HTTP 远程升级功能进行文件升级

- 设备每天凌晨 2 点能定时远程获取锐捷服务器中可升级的文件信息，并下载升级。
- 查看当前可升级的文件信息。
- 从锐捷提供的服务器中下载最新文件，并更新升级设备。

【网络环境】

图 11-7



【配置方法】

- 配置 DNS 信息。
- 开配置设备的定时远程监测时间为凌晨 2 点。
- 获取远程服务器中可更新升级的文件信息。
- 从服务器中下载文件并更新。

A

```
A#configure terminal
A(config)# ip domain-lookup
A(config)# ip name-server 192.168.58.110
A(config)# http update time daily 02:00
A(config)# http check-version
A(config)# end
A# http update all
```

【检验方法】

- -

常见配置错误

- 没有开启 DNS 服务，导致设备与服务器无法建立连接。

11.5 监视与维护

清除各类信息

查看运行情况

作用	命令
查看 Web 服务配置信息和状态。	**show web-service**

查看调试信息

12 PATCH-UPGRADE

12.1 概述

补丁升级功能主要针对设备的补丁包的自动升级管理，和布丁包的手动升级和手动卸载

。

12.2 典型应用

典型应用	场景描述
补丁升级应用场景	描述补丁升级的基本场景及功能

12.2.1 补丁升级典型应用场景

应用场景

补丁升级主要包含如下场景：

- 补丁升级：发布新的热补丁时，从 macc 服务器下载补丁包，并自动升级安装。也可手动删除补丁包或手动升级补丁包。

功能部属

用户无需特殊配置，默认设备开启自动升级

12.3 功能详解

基本概念

↘ 补丁包

补丁包为为修复某些 bug 而生成的补丁文件，升级后可更新部分组件内容。从而达到修复 bug 的目的

↘ 补丁包状态

补丁包包含了四种状态，分别为无补丁状态、安装、加载、永久加载状态。其中加载和永久加载状态时，补丁包真正替换想更新的组件，功能生效

↘ 加载时间段

加载时间段指当设备自动加载补丁包的开始时间段，当设备安装了补丁包后，未在加载时间段内不自动加载补丁

功能特性

功能特性	作用
补丁升级	根据配置对补丁进行升级、回退、卸载

12.3.1 补丁升级

补丁升级可根据服务器配置，下载最新补丁包文件，并根据设备配置，进行补丁升级和回退等功能，并提供异常时的手动升级和卸载。

工作原理

补丁升级模块通过和 macc 服务器交互，获取服务器最新的补丁信息，当服务器上的补丁新于设备时，自动下载补丁。自动模式下，补丁下载成功后，将被自动安装到设备上，但并不马上加载，待到加载时间段时，执行补丁加载。当补丁加载成功超过 5 天后，补丁将被永久加载，5 天内设备，将自动回退到安装状态，并切换为手动模式。手动模式下，不做任何自动更新操作，需手动输入更新或卸载命令后，更新或卸载补丁包。

相关配置

↘ 配置补丁升级

缺省情况下，升级模式为自动升级。

使用 patch-upgrade 命令，修改升级模式、自动加载时间、手动加载、卸载补丁。

↘ 查看补丁升级

使用 **show patch-upgrade** 命令可以查询当前补丁状态、配置、升级日志等信息。

12.4 配置详解

配置项	配置建议 & 相关命令	
配置补丁升级	⚠ 必须配置。	
	patch-upgrade	配置补丁升级

12.4.1 配置补丁升级

配置效果

- 可配置升级模式。
- 可修改自动加载时间。
- 可配置手动升级、卸载补丁

配置方法

配置升级模式

- 可选配置。默认自动升级模式，升级失败时自动切换为手动升级模式。

配置自动加载时间段

- 可选配置。默认每日凌晨 3 点到 4 点。

配置手动升级、卸载

- 可选配置。设备必须在存在已安装的补丁包。

检验方法

- 查看补丁升级配置

相关命令

配置升级模式

【命令格式】 **patch-upgrade set-mode** {**auto** | **manual** }
【参数说明】
【命令模式】 特权模式
【使用指导】 设置当前升级模式为自动升级或手动升级。

配置自动加载时间段

【命令格式】 **patch-upgrade set-active-time start** *hh:mm* **end** *hh:mm*
【参数说明】 *hh:mm*：小时分钟。
【命令模式】 特权模式
【使用指导】 设置补丁自动加载时间段。

配置手动升级

【命令格式】 **patch-upgrade manual-active**
【参数说明】
【命令模式】 特权模式
【使用指导】 使用时必须在手动升级模式下，通常在设备存在已安装补丁包时执行。

配置手动卸载

【命令格式】 **patch-upgrade delete**
【参数说明】
【命令模式】 特权模式
【使用指导】 使用时必须在手动升级模式下，通常在设备存在已安装补丁包时执行。

显示补丁升级配置和状态

【命令格式】 **show patch-upgrade state**
【参数说明】
【命令模式】 特权模式
【使用指导】 使用该命令可以查询补丁升级状态和配置信息。

显示补丁升级日志信息

【命令格式】 **show patch-upgrade log**
【参数说明】
【命令模式】 特权模式
【使用指导】 使用该命令可以查询补丁升级日志信息。

12.5 监视与维护

查看运行情况

作用	命令
查看补丁升级配置和状态信息。	**show patch-upgrade state**
查看补丁升级日志信息。	**show patch-upgrade log**

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
打开补丁升级跟踪的调试开关。	**debug patch-upgrade info**
打开补丁升级错误信息跟踪的调试开关。	**debug patch-upgrade error**
打开补丁升级 http 下载跟踪的调试开关。	**debug patch-upgrade http-info**

13 WEB-UPGRADE

13.1 概述

Web-upgrade 是 RGOS 系统的 WEB 包管理及升级模块，负责对设备 WEB 组件的升级安装，查询。通过堆设备的 WEB 进行升级，用户可以在系统上安装更加稳定的或含有更多特性的 WEB 版本。

下文仅介绍 Web-Upgrade 的相关内容。

协议规范

- 无

13.2 典型应用

典型应用	场景描述
WEB 包升级	升级更新设备 WEB 组件，查看 WEB 包信息

13.2.1 WEB包升级

应用场景

升级 WEB 组件包，完成升级后设备内原先的 WEB 文件被更新，整体 WEB 功能得到增强。

相对于系统组件包的升级，WEB 包升级过程较短，升级完成后设备不需要重启。

功能部属

设备升级前可以将 WEB 包放在 TFTP 服务器程序的根目录下，通过网络下载到设备内，再执行 WEB 包本地升级命令完成升级；也可以将 WEB 包拷贝到 U 盘或 SD 卡内，插入设备再执行升级命令完成升级。

13.3 功能详解

基本概念

无

功能特性

功能特性	作用
WEB 包升级	本地升级 WEB 包

13.3.1 WEB包升级

工作原理

WEB 包升级的原理实际上就是 WEB 文件的替换过程，即 WEB 包内的文件替换设备中的 WEB 文件。

升级完成后，原 WEB 包不会删除，需要手动删除

相关配置

↘ WEB 包升级

将升级文件存放在设备本地文件系统中后，使用 **web-upgrade** 命令升级。

13.4 配置详解

配置项	配置建议 & 相关命令	
WEB 包本地升级	⚠ 基本功能。用于 WEB 包升级	
	web-upgrade *url*	url 为 WEB 包存放的本地路径。该命令用于升级设备内存放的 WEB 包。

13.4.1 WEB包本地升级

配置效果

- 升级更新 WEB 包。

注意事项

- 无

配置方法

WEB 包升级

- 升级前需要先将 WEB 包下载到设备本地。
- 使用 web-upgrade 命令升级
- 手动删除下载的 WEB 包

检验方法

升级完成后可执行 **show web-upgrade** 查看并核对 WEB 包信息

相关命令

本地升级 WEB 包

【命令格式】 **web-upgrade** *url*
【参数说明】 *url*：设备文件系统内 WEB 包存放路径。
【命令模式】 特权模式
【使用指导】 -

查看 WEB 包信息

【命令格式】 **show web-upgrade**
【参数说明】 -
【命令模式】 特权模式，配置模式，接口模式
【使用指导】 -

配置举例

WEB 包本地升级

【网络环境】 升级前必须先将 WEB 包拷入设备内。有以下几种方法：

- 用户首先使用 **copy** 等文件系统命令将 WEB 包拷入设备文件系统，再使用 **web-upgrade** *url*升级本地文件系统内的 WEB 包；
- 将 WEB 包拷入 U 盘或 SD 卡内并插入设备，使用 **web-upgrade** *url*命令升级位于 U 盘或 SD 卡内的安装包。

升级完成后 WEB 包不会删除，如果需要删除，可以使用 **delete** 命令。

【配置方法】

- 通过 **copy tftp** 命令下载 WEB 包到设备本地 tmp 目录

```
ruijie#copy tftp://172.21.3.137/web.gz tmp:web.gz
Press Ctrl+C to quit
!!!!!!!!!!!!!!!
```

```
Copy success.
```

- 通过 WEB 本地升级命令升级 WEB 包

```
Ruijie# web-upgrade tmp:web.gz

Upgrade web package start...

    MD5 a310c329b917fdc992864f8287d83681

    Web version[2018.6.8.07->2018.6.8.10]

Upgrade info [OK]

Upgrade web package succeeded.
```

- 通过 **delete** 命令删除本地 tmp 目录下原 WEB 包

```
ruijie#delete tmp:web.gz
ruijie#
```

【检验方法】 通过命令 **show web-upgrade** 查看当前设备使用的 WEB 包信息，若信息发生变换说明升级成功。

```
ruijie# show web-upgrade

Version      : 2018.6.8.10

Md5          : a310c329b917fdc992864f8287d83681

Size         : 9012807

Build        : 2018-06-08 10:37:41

Compatible   : EG*

Incompatible : EG2100-P|EG680-P
```

常见错误

- 无。

配置指南-接口链路层

本分册介绍接口链路层相关内容，包括以下章节：

1. 接口
2. 模式管理
3. DLDP
4. PCAP
5. PPPOE-CLIENT
6. PPPOE-SERVER
7. Aggregate Port
8. VLAN-TERMINAL

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。

下文仅介绍接口的相关内容。

协议规范

- 无。

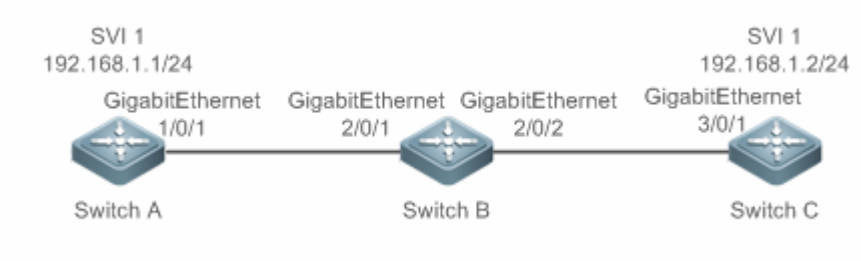
1.2 典型应用

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】 -

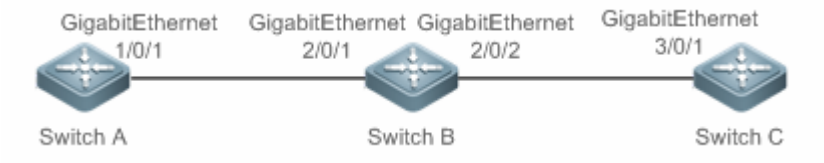
功能部属

- 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 GigabitEthernet3/0/1 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 GigabitEthernet3/0/1 配置为三层路由口。
- 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：

- 三层接口(L3 interface) (三层设备支持)

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）
- Loopback 接口

↘ 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。

↘ 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。

↘ 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。

↘ 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。

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。
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。
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；
- **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 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。

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。

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。

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不一致。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 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。

1.3.10 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。

1.3.11 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，插入的是 SFP 模块，接口工作在千兆模式。

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。

1.3.12 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.。

1.3.13 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。

1.3.14 接口MAC地址

工作原理

缺省情况下，每个以太网口都有一个全球唯一的 MAC 地址。如果需要，以太网接口的 MAC 地址可以修改，但必须保证同一局域网上 MAC 地址的唯一性。

要配置以太网接口的 MAC 地址，在接口配置模式中执行以下命令。

MAC 地址的配置可能会影响了局域网内部的通讯，没有必要的情况下，建议用户不要自行配置 MAC 地址。

相关配置

配置接口的 MAC 地址

缺省情况下，接口有一个全球唯一的 MAC 地址。

在接口模式下使用 **mac-address** *mac-address* 命令可以修改接口的 MAC 地址。

1.3.15 配置VLAN封装标识

工作原理

VLAN（Virtual Local Area Network）即虚拟局域网，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。IEEE 于 1999 年颁布了用以标准化 VLAN 实现方案的 802.1Q 协议标准草案。

VLAN 技术允许网络管理者将一个物理的 LAN 逻辑划分成不同的广播域（或称虚拟 LAN，即 VLAN），每一个 VLAN 都包含一组有着相同需求的计算机工作站，与物理上形成的 LAN 有着相同的属性。但由于它是逻辑划分而不是物理划分，所以同一个 VLAN 内的各个工作站无须被放置在同一个物理空间里，即这些工作站不一定属于同一个物理 LAN 网段。一个 VLAN 内部的广播和单播流量都不会转发到其他 VLAN 中，从而有助于控制流量、减少设备投资、简化网络管理、提高网络的安全性。

VLAN 是为解决以太网的广播问题和安全性而提出的一种协议，它在以太网帧的基础上增加了 VLAN 头，用 VLAN ID 把用户划分为更小的工作组，限制不同工作组间的用户二层互访，每个工作组就是一个虚拟局域网。虚拟局域网的好处是可以限制广播范围，并能够形成虚拟工作组，动态管理网络。

为了能与某个 VLAN 内主机进行通讯，用户可以在以太网接口或以太网子接口上配置 802.1Q（VLAN 协议规范）VLAN 封装标志，以太网口在发包的时候，就会封装上相应的 VLAN 头部，在收包的时候，剥离报文的 VLAN 头部。

相关配置

↘ 配置接口的 VLAN 封装标识

缺省情况下，接口没有开启 802.1Q 封装协议。

在接口模式下使用 encapsulation dot1Q VlanID 命令可以指定接口封装 802.1Q，VlanID 为指定封装的 VLAN 号。

1.3.16 配置接口keepalive报文周期

工作原理

在通常的广域网接口上，封装的链路层协议基本上都需要 keepalive 机制，用以维护链路协议的正常工作，通过配置该命令，就可以设置链路层协议的 keepalive 周期时间，从而控制发送 keepalive 报文的时间。

在 tunnel 接口以及封装了 HDLC、PPP 协议的接口上，还可以设置 keepailve 报文的最大超时次数，如果 keepailve 报文超过设置的最大超时次数都未收到对端的响应，则将断开建立的连接

相关配置

↘ 配置接口 keepalive 报文周期

缺省情况下，以太网口没有启用 keepalive 功能，其他接口 keepalive 周期是 10 秒，可配置范围为 1-32767。
对于 tunnel 接口以及封装了 HDLC、PPP 协议的接口，该命令还携带 keepalive 的最大超时次数的选项，可配置范围为 1-255，缺省情况下，tunnel 接口的缺省值是 3 次，HDLC 协议的缺省值是 3 次，PPP 协议的缺省值是 10 次。
在接口模式下使用 keepalive [keep-period [keep-retries]] 改变接口的 keepalive 报文周期。

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。

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

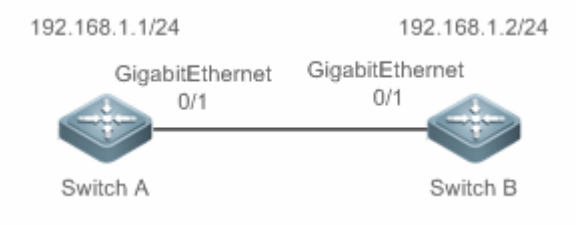
- 在全局配置模式下配置命令，如 logging link-updown 查看接口状态信息。选择一个物理端口，插拔网线，接口将发生两次状态改变，用户可以在控制台上看到接口 link 状态从 up 变为 down 的信息，又从 down 变为 up 的信息，配置 no logging link-updown 后，再次插拔网线，控制台上看不到信息，说明该功能是正常的。

配置举例

配置接口基本属性

【网络环境】

图 1-3



【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 GigabitEthern 0/1 和 SVI 1 在接口 GigabitEthern 0/1 在 **shutdown** 操作后的接口状态是否正确
- 检查接口 GigabitEthern 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 GigabitEthern 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
  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。

> 对于 40G 物理端口，只允许配置接口的速率为 **speed 40G** 和 **speed auto** 两种。

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 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

【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* **down [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。

Down ：设置载波检测信号 DCD 从 Up 状态到 Down 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】 -

配置接口 MAC 地址

- 可选配置。如果需要设置此功能，则应该在接口模式下执行此配置项。
- 接口的 MAC 地址缺省为一固定值。

【命令格式】 **mac-address** *mac-address*

【参数说明】 *Mac-address*：一个合法的 MAC 地址。

【命令模式】 接口配置模式

【使用指导】 -

配置接口 VLAN 封装标识

- 可选配置。如果需要设置此功能，则应该在接口模式下执行此配置项。
- 接口的 VLAN 封装协议默认关闭。

【命令格式】 **encapsulation dot1Q** *VlanID*

【参数说明】 *VlanID*：VLAN ID，范围是 1-4094。

【命令模式】 接口配置模式

【使用指导】 -

配置接口 keepalive 报文周期

- 可选配置。如果需要设置此功能，则应该在接口模式下执行此配置项。
- 缺省情况下，以太网口是没有启用 keepalive 功能的，而对于其他广域网接口，默认 keepalive 时间是 10 秒。

【命令格式】 **keepalive** [*keep-period* [*keep-retries*]]

【参数说明】 *keep-period*：系统发送 keepalive 报文的周期，范围是 1-32767

keep-retries：keepalive 的最大超时次数，范围是 1-255

【命令模式】 接口配置模式

【使用指导】 -

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。

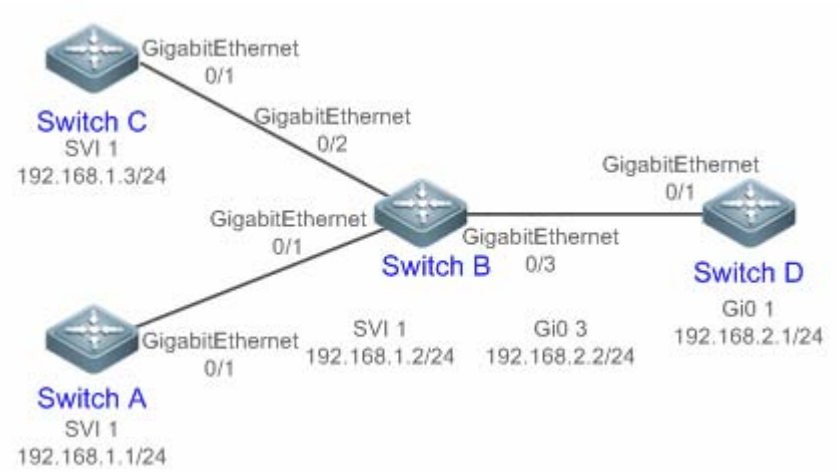
【命令格式】 **show interfaces** [*interface-type interface-number*] [**description**

配置举例

配置接口属性

【网络环境】

图 1-4



【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

```
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

```
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
  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

```
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
  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** [*interface-type interface-number*]
接口硬件复位。	**clear interface** *interface-type interface-number*

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** [*interface-type interface-number*]
显示接口的状态。	**Show interfaces** [*interface-type interface-number*] **status**
显示接口违例状态。	**Show interfaces** [*interface-type interface-number*] **status err-disable**
查看端口链路状态变化时间和次数。	**Show interfaces** [*interface-type interface-number*] **link-state-change statistics**
显示指定接口的描述配置和接口状态。	**show interfaces** [*interface-type interface-number*] **description**
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** [*interface-type interface-number*] **line-detect**
显示接口带宽利用率	**show interfaces** [*interface-type interface-number*] **usage**
显示接口 EEE 状态。	**Show eee interfaces** { *interface-type interface-number* | *status* }
显示 VLAN 子接口信息	**show vlans**

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。

2 模式管理

2.1 概述

模式管理用来统一管理设备的系统模式、网络接口的内外网属性等等。

锐捷的网关系列产品，通常既可作为出口网关设备，此时为网关模式，也可作为桥接设备，此时为网桥模式。这两种系统模式可以通过模式管理切换使用。

用户在使用设备联网时，有内网和外网之分，相应的，设备的网络接口也具有内网或外网的属性，模式管理提供网络接口的内外网属性切换功能，方便用户根据实际情况调整。

协议规范

- 无

2.2 典型应用

典型应用	场景描述
切换接口的内外网模式	用户网络拓扑发生变更，增加一条外网线路。

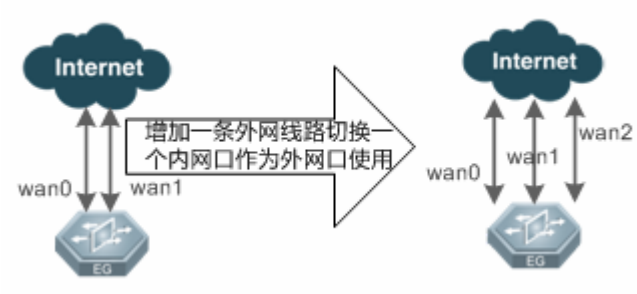
2.2.1 切换接口的内外网模式

应用场景

用户网络拓扑变化，例如，新增一条外网线路，需要连接设备的一个外网端口。

因外网端口已用满，内网端口还有剩余的，可将内网端口切换为外网端口使用，以支持线路的扩展。

图 2-1



【注释】 这个示例中，设备上有 wan0 和 wan1 两个外网口，其他的均为内网口，在增加一条外网线路之后，把空闲的一个

内网口转换为外网口使用，多了 wan2 这个外网口。

功能部属

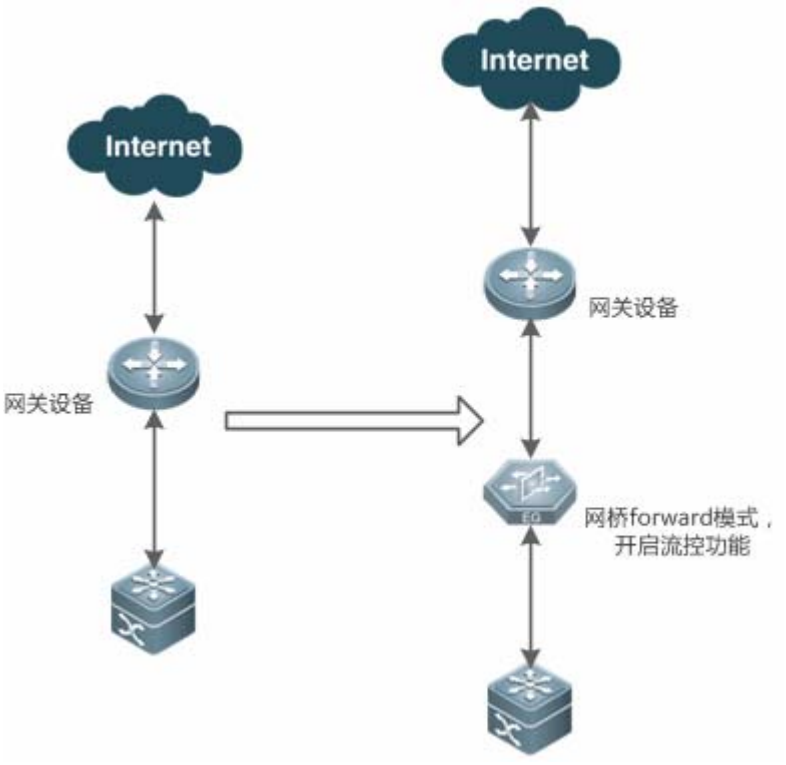
- 确定需要切换的闲置的内网口。
- 执行内外网切换的配置命令，配置该接口为外网口。
- 保存配置，重启生效。

2.2.2 切换网桥下工作模式

应用场景

用户可根据不同用途对设备的系统模式在网关和网桥模式之间自由切换。当用户需要把设备桥接使用时，需要切换至网桥模式，并指定桥的工作模式。网桥下支持四种工作模式（MSC 支持五种），各模式的用途各有差别，用户可根据实际需要选择适当的工作模式。在需要变更时进行调整。

图 2-2



【注释】 这个示例中，用户原有一个网关设备，后来有做流量控制的要求，又想保留原有的网关设备，这时可以把网关设备

切换为网桥模式，串入到当前网络，并配置为 forward 模式，具备流量识别和流量控制的功能。

功能部署

- 确定当前的系统模式，若非网桥，则使用系统模式切换命令切换为非网关模式，保存配置并重启设备。
- 挑选一个内网接口，一个外网接口，建立一个桥映射表，并配置其工作模式，接入网络。
- 若需要多对桥，重复上一步配置。
- 需要变更某对桥的工作模式时，进入桥配置模式修改。

2.3 功能详解

基本概念

系统模式

系统模式有网关和网桥（即，非网关模式）两种。有些设备可以选择工作在网关模式，或者工作在网桥模式。

工作在网关模式下，所有的网络接口都是三层接口，报文根据路由表进行转发。网关模式下的报文处理，为通用路由器的报文处理方式，不再特别说明。

工作在网桥模式下，所有的网络接口都是二层接口，报文根据桥接映射表来进行转发。网桥模式下，报文除了因为策略的原因被阻断丢弃，正常转发的报文不会进行任何修改。

工作在网关模式下，所有的网络接口都是三层接口，报文根据路由表进行转发。网关模式下的报文处理，为通用路由器的报文处理方式，不再特别说明。本产品只支持网关模式。

内外网属性

网关产品中，除了 MGMT 口（管理口），其他网络接口都具备内网属性或外网属性。设备的网络接口需要根据实际情况配置正确的内外网属性：连接用户内网的网络接口为内网口，连接外网线路的网络接口为外网口。

用户可以通过查询模式管理的相关信息，了解当前系统的每个网络接口的内外网属性。通过配置命令来修改网络接口的内网属性或者外网属性。

这里的网络接口，指的是设备上的物理网口。相应的，其上的子接口也会继承其内外网属性，并随着物理口的属性变化而变化；设备上的部分虚接口，如 dialer 口，则只有外网属性，不提供切换功能。

接口的内外网属性切换，需要保存配置并重启设备才能生效。

网桥模式下的工作模式

在网桥模式下，报文根据桥接映射表进行桥接转发，除了因为策略的原因被阻断丢弃，正常转发的报文不会做任何修改。

每个桥接映射表需要关联一个内网口和一个外网口，并指定非网关模式下的工作模式。网桥模式下支持如下几种工作模式：

- forward 工作模式：可以对流经设备的报文做流量识别、流量阻断、流量控制、流量审计。
- sniffer 工作模式：可以对流经设备的报文做流量识别、流量审计。
- bypass 工作模式：只对流经设备的报文做接口报文收发统计。
- receive-only 工作模式：又称单臂模式。可以对流经设备的报文做流量识别、流量审计。与上述工作模式的区别在于处理完直接丢弃报文，而不是转发报文。

桥映射表的数量取决于设备能提供的最大内外网口对数。如，设备有内外网口各 4 个，则最多可以有 4 个桥接映射表。如果设备有 4 个内网口，3 个外网口，则只有 3 个桥接映射表。各设备支持的桥映射表数量会有差别。

桥接映射表不可以删除，需要在配置工作模式后生效。

系统在有多个桥接映射表的情况下，允许各个桥接映射表配置不同的工作模式。

功能特性

功能特性	作用
配置系统模式	配置设备工作在网关模式或者非网关模式。
配置内外网属性	根据实际的网络拓扑配置网络接口的内外网属性。

2.3.1 配置系统模式

配置设备工作在网关模式或者非网关模式。

工作原理

在不同的系统模式下，系统支持的各种业务是有区别的，最大的区别是：网关模式下具备三层路由功能。

相关配置

配置系统模式

本产品只支持网关模式。

2.3.2 配置内外网属性

根据实际的网络拓扑配置网络接口的内外网属性。

工作原理

内网口和外网口上能运行的业务是有差别的，如：流量审计、流量控制的业务是基于外网口的，如果配置不当，该接口的业务就无法有效运行。内外网属性是软件性质的，用户可根据实际的网络拓扑情况进行变更，相关的业务也会根据该配置自动调整。

相关配置

↘ 配置接口内外网属性

缺省情况下，设备各网络接口的内外网属性有区别，是按最典型的用户场景进行设置。用户在 WEB 管理页面或者查询配置文件，可以看到具体的属性。

使用 **specify interface***interface-name***{lan | wan}**命令可以切换接口的内外网属性，保存配置重启后生效。

2.3.3 配置日志信息不保存本地硬盘功能

开启该功能，设备审计日志、流量审计日志、内容审计日志、流日志等信息将不会记录在硬盘。

工作原理

在人数超过一定数量（EG2000X/XE/UE、ACE3000E 为 10000，EG2000G/GE、ACE2000E 为 5000，其他产品不支持）的情况下，大量的信息记录在本地硬盘，会影响设备的使用效果，在这种场景下建议开启日志信息不保存本地硬盘的功能，该功能开启后，相关的日志信息，如内容审计日志、设备审计日志、流量审计日志、流日志，都不会记录在硬盘，可以通过本机的日志服务发送到外置的日志服务器。

相关配置

↘ 配置日志信息不保存本地硬盘功能

不同设备，设备的日志信息不保存本地硬盘功能缺省状态不一样，EG2000X/XE/UE 和 ACE3000E 缺省开启，EG2000G/GE、ACE2000E 缺省关闭，其他网关产品不具备该功能。

使用 **write-db enable** 命令可以关闭日志信息不保存本地硬盘功能，使用 **no write-db enable** 开启。

2.3.4 配置网桥下工作模式

配置网桥设备的一对桥的工作模式，各工作模式支持的业务处理有所差别。

工作原理

桥模式下的 forward、sniffer、bypass 工作模式，对报文的转发是根据桥映射表的规定进行的，从桥映射表的内网口进来的报文，会从对应的外网口转发出去，从外网口进来的报文，由内网口转发。

单臂模式不转发报文，而是丢弃。当然，单臂模式下，需要通过配置内网 IP 段，确定报文方向是上行的还是下行的。

相关配置

↘ 进入桥映射表配置模式

使用 **bridge-map** *bridge-num* 命令可以创建桥接映射表，并进入桥映射表配置模式。

↘ 配置桥映射表的工作模式

缺省情况下，桥映射表的工作模式无配置。

使用 **link-mode***interface-name1 interface-name2* { *forward* | *sniffer* | *bypass*| receive-only}命令可以配置桥映射表并指定其工作模式。

使用 **lan-ip***ip_addresssubnet_mask* 命令可以配置单臂模式下的内网 IP 段，一个单臂模式最多允许配置 100 个内网 IP 段。

2.4 产品说明



NBR108G-P、NBR800G、NBR950G、NBR1500G、NBR2000G、NBR1000G-C、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持二三层口转换， NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR2000G-C、NBR3000G-S 不支持二三层口转换。NBR1500G、NBR2000G、NBR1300G-E、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持端口镜像 ,NBR108G-P、NBR800G、NBR950G、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1000G-E、NBR6120-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE 不支持端口镜像。



NBR3000G-S 、 NBR2000G-C 、 NBR1500G 、 NBR2000G 、 NBR2100G-E 、 NBR2500D-E 、 NBR3000D-E 、 NBR3000D-UE、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持千兆光口， NBR108G-P、NBR800G、NBR950G、NBR1000G-C、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E 不支持千兆光口。

NBR3000G-S 、 NBR2000G-C 、 NBR1500G 、 NBR2000G 、 NBR2100G-E 、 NBR2500D-E 、 NBR3000D-E 、 NBR3000D-UE、NBR108G-P、NBR800G、NBR950G、NBR1000G-C、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR6205-E、NBR6135-E、NBR6210-E 不支持万兆口。NBR6215-E 支持万兆口。



NBR1700G-E 、 NBR2100G-E 、 NBR2500D-E 、 NBR3000D-E 、 NBR3000D-UE 、 NBR6205-E 、 NBR6135-E 、 NBR6210-E、NBR6215-E 支持桥模式，以及桥模式下 BVI 口；NBR108G-P、NBR800G、NBR950G、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR3000G-S、NBR2000G-C、NBR1000G-C、NBR1500G、NBR2000G 不支持桥模式。



NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 NPE 模式；NBR108G-P、NBR800G、NBR950G、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR3000G-S、NBR2000G-C、NBR1000G-C、NBR1500G、NBR2000G、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE 不支持 NPE 模式。

2.5 配置详解

配置项	配置建议&相关命令	
配置系统模式	⚠ 可选配置。配置系统模式为网关模式。	
	sys-mode gateway	配置系统模式为网关模式
配置系统模式	⚠ 可选配置。用于切换当前系统模式，使设备运行于网关模式。 缺省为网关模式。	
	sys-mode gateway	配置系统模式为网关模式
配置内外网属性	⚠ 可选配置。已有缺省配置。用于切换网络接口的内外网属性。	
	specify interface*interface-name*{**lan | wan**}	配置网络接口的内外网属性
配置千兆万兆口的切换	⚠ 可选配置。用于 4 个千兆口与一个万兆口之间的切换。	
	xaui-mode slot *slot-num*	将 4 个千兆口切换为一个万兆口。slot-num：指定要切换的万兆口槽号。
配置日志信息不保存本地硬盘功能	⚠ 可选配置。用于开启或关闭日志信息不保存本地硬盘功能，不同设备缺省状态不一样。	
	no write-db enable	开启日志信息不保存本地硬盘功能
	write-db enable	关闭日志信息不保存本地硬盘功能
配置网桥下工作模式	⚠ 必选配置。用于网桥设备组建桥映射表并指定其工作模式。	
	bridge-map *bridge-num*	配置进入桥接映射表模式层
	link-mode*interface-name1 interface-name2* {**forward | sniffer | bypass | receive-only**}	配置桥接映射表对应的内网口和外网口，及其工作模式
	⚠ 可选配置。缺省 vlan-id 为 1。该编号用于分类识别功能，规定不带 vlan tag 的报文，归类到该 vlan-id 对应的 vlan 分类。	
	native-vlan *vlan-id*	配置该桥接映射表的 native vlan 编号。没有带 vlan-id 的报文将被识别为该 native vlan-id 对应的 vlan 分类对象。

2.5.1 配置系统模式

配置效果

- 切换当前系统模式，使设备运行于网关模式。

注意事项

- 需要保存配置并重启后生效。

配置方法

配置系统模式

- 可选配置。
- 本产品只支持网关模式。
- 在全局配置模式下配置。

检验方法

通过 **show sys-mode** 命令查看当前的系统模式。

相关命令

配置系统模式

【命令格式】 **sys-mode gateway**
【参数说明】 -
【命令模式】 全局模式
【使用指导】 需保存配置重启设备后生效。

查看当前系统模式

【命令格式】 **show sys-mode**
【参数说明】 **-**
【命令模式】 特权模式
【使用指导】 -

配置举例

切换系统模式为网关模式

【配置方法】
- 切换系统模式为网关。
- 保存配置重启。

```
Ruijie#configure terminal
Ruijie(config)#sys-mode gateway
Ruijie(config)# exit
Ruijie#write

Building configuration...
```

```
[OK]
Ruijie#reload
Reload system?(Y/N)y
…
```

【检验方法】 待保存配置重启完成之后，使用 **show sys-mode** 命令检验模式是否生效。

- 查看当前系统模式。

```
Ruijie# show sys-mode
System is gateway mode.
…
LAN: GigabitEthernet 0/0 GigabitEthernet 0/3 GigabitEthernet 0/5
WAN: GigabitEthernet 0/1 GigabitEthernet 0/2 GigabitEthernet 0/4
```

常见错误

- 系统模式切换完之后没有保存配置就重启设备，或保存配置但不重启设备导致没有生效。

2.5.2 配置内外网属性

配置效果

- 配置网络接口的内外网属性，符合实际网络拓扑的情况。
- 通常情况下，用户会在设备上点时或者网络线路变更时需要调整。

注意事项

- 无

配置方法

- 使用内外网属性切换命令完成配置。

检验方法

- 使用模式查看命令查看当前内外网接口属性信息。

相关命令

↘ 配置接口内外网属性

【命令格式】 **specify interface***interface-name*{**lan | wan**}

【参数说明】 **interface***interface-name*：指定要切换内外网属性的接口名称。

【命令模式】 全局模式

【使用指导】 no 命令可以恢复当前接口原有的内外网属性。

↘ 查看当前所有网络接口的内外网属性

【命令格式】 **show sys-mode**

【参数说明】 **-**

【命令模式】 特权模式

【使用指导】 -

配置举例

↘ 用户新增一条外网线路，原先的 3 个外网口已经用光，内网口还有闲置，切换为外网口使用。

【配置方法】

- 配置闲置的内网口作为外网口使用。

```
Ruijie#configure terminal
Ruijie(config)#specify interface GigabitEthernet 0/3wan
Ruijie(config)# end
```

【检验方法】

- 使用 show 命令查看配置结果。

```
Ruijie# show sys-mode
System is bridge mode.
…
LAN: GigabitEthernet 0/0 GigabitEthernet 0/5
WAN: GigabitEthernet 0/1 GigabitEthernet 0/2GigabitEthernet 0/3 GigabitEthernet 0/4
```

常见配置错误

- 无

2.5.3 配置千兆万兆口的切换

配置效果

- 4 个千兆口与一个万兆口之间的切换。

注意事项

- 需要保存配置重启后生效。

配置方法

- 全局模式下，使用 xaui-mode 命令完成配置。

检验方法

- 设备重启生效后，查看接口信息。

相关命令

配置万兆口模式

【命令格式】 **xaui-mode slot** *slot-num*

【参数说明】 *slot-num*：指定要切换的万兆口槽号。

【命令模式】 全局模式

【使用指导】 用 no 命令关闭。

查看当前万兆口模式

【命令格式】 **show interface**

【参数说明】 -

【命令模式】 特权模式

【使用指导】 -

配置举例

用户切换前 4 个千兆口为 1 个万兆口。

【配置方法】

- 配置切换前 4 个千兆口为 1 个万兆口。

```
Ruijie(config)#xaui-mode slot 2
Please save the config, and reload system to take effect!
```

【检验方法】

- 设备重启生效后，使用 show 命令查看配置结果。

```
Ruijie#show interface
…
========================= TenGigabitEthernet 0/2 ========================
…
```

常见配置错误

- 无

2.5.4 配置日志信息不保存本地硬盘功能

配置效果

- 配置开启或关闭日志信息不保存本地硬盘功能。

注意事项

- 无。

配置方法

↘ 配置日志信息不保存本地硬盘功能

- 可选配置。
- 不同设备，缺省状态不一样，EG2000X/XE/UE 和 ACE3000E 缺省开启，EG2000G/GE、ACE2000E 缺省关闭，其他网关产品不具备该功能。
- 在全局配置模式下配置。

检验方法

通过 **show write-db** 命令查看当前设备是否开启日志信息不保存本地硬盘的功能。

相关命令

↘ 配置日志信息不保存本地硬盘功能

【命令格式】 **no write-db enable**
【参数说明】 -
【命令模式】 全局模式
【使用指导】 write-db enable 命令关闭日志信息不保存本地硬盘功能。

↘ 查看当前系统的日志信息是否保存本地硬盘

【命令格式】 **show write-db**
【参数说明】 **-**
【命令模式】 特权模式

【使用指导】 -

配置举例

开启桥接联动功能

【配置方法】

- 开启日志信息不保存本地硬盘功能。

```
Ruijie# configure terminal
Ruijie(config)# no write-db enable
Ruijie(config)# exit
Ruijie#write

Building configuration...

[OK]
Ruijie#reload
Reload system?(Y/N)y
…
```

【检验方法】 待保存配置重启完成之后，使用 **show write-db** 命令检验配置是否生效。

- 查看当前设备日志信息是否保存本地硬盘。

```
Ruijie# show write-db
write-db enable: 0
```

常见错误

日志信息不保存本地硬盘功能配置后没有保存配置就重启，或保存配置但不重启导致没有生效。

2.5.5 配置网桥下工作模式

配置效果

- 用户根据需要配置网桥下的工作模式，不同的工作模式运行不同的业务。

注意事项

- 桥映射表必须由一个内网口和一个外网口组成。且一个网络接口不能同时属于多个桥。
- 必须为桥映射表配置一种工作模式，这个桥才能正常工作。

配置方法

- 进入桥映射表模式配置层
- 网桥模式下 ,每个桥映射表缺省无配置 ,需要用户指定一个内网口和一个外网口组成一对桥 ,并指定其工作模式为 forward、sniffer、bypass、单臂模式中的一种。

检验方法

- 使用桥模式信息的查看命令验证。

相关命令

↘ 进入桥映射表模式配置层

【命令格式】 **bridge-map** *bridge-num*
【参数说明】 *bridge-num*：桥映射表的编号。
【命令模式】 全局模式
【使用指导】 -

↘ 指定桥映射需要的内网口和外网口，及其工作模式

【命令格式】 **link-mode***interface-name1 interface-name2* { **forward | sniffer | bypass | receive-only**}
【参数说明】 *interface-name1*：内网口接口名称。
interface-name2：外网口接口名称
【命令模式】 bridge-map 配置模式
【使用指导】 -

↘ 配置 native vlan 的编号

【命令格式】 **native-vlan** *vlan-id*
【参数说明】 *vlan-id*：该桥接映射表的 native vlan 编号。
【命令模式】 bridge-map 配置模式
【使用指导】 没有带 vlan-id 的报文将被识别为该 native vlan-id 对应的 vlan 分类对象。

↘ 查看当前所有网络接口的内外网属性

【命令格式】 **show bridge-map**[*bridge-num*] [**lan-ip**]
【参数说明】 **-**
【命令模式】 特权模式
【使用指导】 -

配置举例

↘ 用户使用设备作为桥转发设备，要对流经的流量做流量控制，因此需配置设备工作在 forward 模式。

【配置方法】
- 进入桥映射表配置层。
- 创建桥映射并指定其工作在 forward 模式。

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# bridge-map 0
Ruijie(config-bridge-map)# link-mode GigabitEthernet 0/0GigabitEthernet 0/1 forward
Ruijie(config-bridge-map))# end
```

【检验方法】
- 使用 show bridge-map 命令查看配置结果。

```
Ruijie#show bridge-map 0
BRIDGE MAP 0,STATE is DOWN
         Inside interface is GigabitEthernet 0/0,Outside interface is GigabitEthernet 0/1
         Working mode is forward
Native vlan is 1
```

↘ 用户使用设备作为旁路，工作在单臂模式，审计交换机镜像过来的报文。

【配置方法】
- 进入桥映射表配置层。
- 创建桥映射并指定其工作在单臂模式（receive-only）。
- 配置内网 IP 段。

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# bridge-map 0
Ruijie(config-bridge-map)# link-mode GigabitEthernet 0/0GigabitEthernet 0/1 receive-only
Ruijie(config-bridge-map)# lan-ip 192.168.0.0 255.255.255.0
Ruijie(config-bridge-map)# lan-ip 10.10.10.0 255.255.255.0
Ruijie(config-bridge-map))# end
```

【检验方法】
- 使用 show bridge-map 命令查看配置结果。

```
Ruijie#show bridge-map 0
BRIDGE MAP 0,STATE is DOWN
         Inside interface is GigabitEthernet 0/0,Outside interface is GigabitEthernet 0/1
         Working mode is receive-only
Native vlan is 1

Ruijie#show bridge-map 0 lan-ip
IP add              mask add
192.168.0.0        255.255.255.0
10.10.10.0           255.255.255.0
```

常见配置错误

- 桥配置与实际需要不符。如，需要做流量控制，但没有配置工作在 forward 模式下。

2.6 监视与维护

清除各类信息

无

查看运行情况

作用	命令
查看系统模式、网络接口内外网属性相关信息。	**show sys-mode**
查看桥接映射表的相关信息，包括桥关联的内外网接口信息，桥工作模式信息，以及桥的 up/down 状态信息。 单臂模式下，还可以查看配置的内网 IP 段信息	**show bridge-map** *bridge-num*[**lan-ip**]

查看调试信息

无

3 DLDP

3.1 概述

DLDP（Data Link Detection Protocol，数据链路检测协议），是一种基于快速检测以太网链路故障的检测协议。

一般的以太网链路检测机制都只是利用物理连接的状态，通过物理层的自动协商来检测链路的连通性。但是该方法对于三层的数据连通性检测，如物理连接状态正常但三层数据通信异常的场景，存在一定的局限性。

DLDP 在这类场景中，为用户提供可靠的三层链路检测信息。同时，在检测出故障后，DLDP 主动 SHUTDOWN 三层接口的逻辑状态，促使三层协议快速收敛。

协议规范

- 无

3.2 典型应用

典型应用	场景描述
同网段 DLDP 检测	检测端口的源 IP 与检测 IP 属于同一网段。
跨网段 DLDP 检测	检测端口的源 IP 与检测 IP 属不同网段

3.2.1 同网段DLDP检测

应用场景

检测端口的源 IP 与检测 IP 属于同一网段的基本应用场景。

以下图为例，设备 A 上的三层口 Gi 0/1 与设备 C 上的三层口 Gi 0/2 属同网段，若要检测 Gi 0/1 到 Gi 0/2 三层线路的连通性，仅需在 A 或 C 的相应三层口开启 DLDP 检测功能即可。

图 3-1



【注释】 Gi 0/1 与 Gi 0/2 均为三层口，且属同一网段。

B 为同网段网络。

功能部署

- 在 Gi 0/1 或 Gi 0/2 上开启 DLDP 检测即可。

3.2.2 跨网段DLDP检测

应用场景

检测端口的源 IP 与检测 IP 在不同网段的应用场景。

以下图为例 ,设备 A 上的三层口 Gi 0/1 与设备 D 上的三层口 Gi 0/4 在不同网段 ,若要检测 Gi 0/1 到 Gi 0/4 三层线路的连通性，则需在 A 的 GI 0/1 开启 DLDP 功能的同时还需再配置 DLDP 下一跳 IP 地址（设备 B 上的 Gi 0/2 的 IP 地址）。

图 3-2



【注释】 Gi 0/1 与 Gi 0/4 均为三层口，但在不同网段。

功能部署

- 在 Gi 0/1 上开启 DLDP 并配置 DLDP 下一跳 IP 地址。

3.3 功能详解

基本概念

↘ DLDP 的探测间隔及重传次数

探测间隔：指 DLDP 探测报文（ICMP echo）的发送间隔。

重传次数：指 DLDP 探测失效所需的发包次数。

当网络设备在“探测间隔”×“重传次数”的时间周期内没有收到对端的应答报文，则认为三层链路故障，主动 SHUTDOWN 三层接口逻辑状态（实际物理链路还是连通的）。一旦三层链路正常通讯，则恢复三层接口逻辑状态 UP。

↘ DLDP 检测模式

DLDP 的检测模式包括：主动模式和被动模式。

主动模式：指主动发送 ICMP 探测报文的模式，缺省配置为主动模式。

被动模式：指被动接收 ICMP 探测报文的模式。

DLDP 的下一跳

下一跳：指跨网段 DLDP 检测中，检则 IP 对应的路由下一节点。

在某些情形下，DLDP 需要检测非直连网段 IP 的可达性。这时需要配置该接口的下一跳 IP，以便 DLDP 能够通过 ARP 报文获取下一跳 MAC 地址，正确的封装 ICMP 报文并发出。

但在这种情形下，需避免响应报文从其他链路回应的情况，否则会造成 DLDP 误判该接口没有收到 ICMP 应答。

DLDP 的恢复次数

恢复次数：指 DLDP 从故障中恢复需连续收到的响应报文（ICMP reply）次数。

在有些情形下，检测链路可能不太稳定，比如 PING 断了三次，通一次，又断了多次。如果按简单的逻辑，其中的 DLDP 检测就是 UP、DOWN 多次，实际可能加剧环网的不稳定。

恢复次数表示链路从 DOWN 状态为设置为 UP 状态前，需要收到连续的 DLDP 检测报文响应次数。恢复次数缺省为 3 次，即只有该链路上连续 PING 通了 3 次才会设置为 UP。在这种情况下，虽然降低了链路检测的灵敏度，但增加其稳定性，同时相关参数在实际应用中还可根据网络情况进行调整。

DLDP 的绑定 MAC

绑定 MAC：指 DLDP 检测 IP 所绑定的 MAC 地址

在复杂的网络环境下，检测链路中可能存在异常 ARP 报文（ARP 欺骗），使得 DLDP 则获取到非法的 MAC 地址，从而导致检测无法正常工作。

在此种环境下，通过配置绑定 MAC 地址，可将检测 IP(或下一跳 IP)与静态 MAC 地址进行绑定，不再受异常 ARP 报文欺骗而引起 DLDP 功能失效。

功能特性

功能特性	作用
建立 DLDP 检测	实现 DLDP 三层链路连通性检测，在三层链路异常时，主动 SHUTDOWN 掉对应三层口。
绑定 MAC 地址	当网络中存在 ARP 欺骗等异常情况，可将检测 IP 与设备 MAC 地址进行绑定，避免协议异常发生。
DLDP 被动模式	当检测链路两端都开启 DLDP，其中一端可配置为被动模式，以节省带宽资源和设备 CPU 资源。

3.3.1 建立DLDP检测

DLDP 三层链路连通性检测，在检则出三层链路异常时，主动 SHUTDOWN 掉对应三层口。

工作原理

启动 DLDP 功能后，DLDP 会通过 ARP 报文获取被检测设备或者到达被检测设备的下一跳设备的 mac 地址和出接口，然后通过周期性的 IPv4 ICMP echo 报文进行通路检测。如果在指定时间内被检测设备没有回应 IPv4 ICMP reply 报文，则认为这个接口通路出现问题，将该接口设置为“三层接口 DOWN”。

相关配置

- 配置 DLDP 检测功能

缺省情况下，接口上不开启 DLDP 检测功能。

使用 dldp 命令并指定要检测的目的 IP 地址就可以启动 DLDP 检测功能。

用户可以根据实际环境选择是否配置下一跳 IP、MAC 地址、发送间隔、重传次数、恢复次数等参数。

3.3.2 绑定MAC地址

网络中存在 ARP 欺骗等异常情况，可将检测 IP（或下一跳 IP）与设备 MAC 地址进行绑定，避免协议发生异常情况。

工作原理

网络中存在 ARP 欺骗的情况下，通过配置绑定 MAC 地址，可将检测 IP(或下一跳 IP)与静态 MAC 地址进行绑定，不再受异常 ARP 报文欺骗而引起 DLDP 功能失效。

相关配置

缺省情况下开启 DLDP 检测功能时不指定 MAC 地址绑定。

通过 dldp 命令开启检测时并同时指定要绑定的 MAC 地址，若存在下一跳 IP 地址，则配置的是下一跳设备的 MAC 地址，否则配置目的检测设备的 MAC 地址。

配置开启后，DLDP 探测过程中发送的 ARP 报文与 ICMP 报文中的目的 IP 与目的 MAC 是固定的，如果接收的报文中源 IP 与源 MAC 和绑定的 IP 与 MAC 不匹配，则不会进行处理。

3.3.3 DLDP被动模式

当检测链路两端都开启 DLDP，其中一端可配置为被动模式，以节省带宽资源和设备 CPU 资源。

工作原理

一端设备使用 ICMP echo 发包，另一端用同样的检测参数来确认报文的及时可达，一样能达到双方设备检测链路通路的效果，同时也节省了带宽资源和设备 CPU 资源。

相关配置

缺省情况下不开启 DLDP 被动检测模式。

通过 dldp passive 命令开启被动检测。

配置开启后，DLDP 将不再主动发起 ICMP echo 报文进行探测，只需要在接收到 ICMP echo 报文后响应 ICMP Reply 报文即可，在指定时间内如果没有收到 ICMP echo 报文则认为接口通路出现问题。

3.4 配置详解

配置项	配置建议&相关命令	
配置 DLDP 检测功能	⚠ 必须配置，接口模式，开启 DLDP 检测功能	
	dldp	配置 DLDP 检测功能
	⚠ 可选配置，接口模式，开启被动检测功能。	
	dldp passive	配置接口被动模式
	⚠ 可选配置，全局模式，。指定探测过程中的探测间隔、重传次数以及恢复次数。	
	dldp interval	全局修改 DLDP 配置参数，可生效到所有 DLDP 检测
	dldp retry	
	dldp resume	

3.4.1 配置DLDP检测功能

配置效果

- 实现 DLDP 三层链路连通性检测，在三层链路异常时，主动 SHUTDOWN 掉对应三层口。

注意事项

- 一个三层接口下，DLDP 可以配置多个 IP 检测，当所有 IP 都没有 ICMP 响应时，才认为接口 DOWN；而一旦有一个 IP 恢复通讯，则认为接口恢复 UP。
- DLDP 使用该三层接口的第一个 IP 地址作为报文的源 IP 地址进行通讯。

配置方法

启动 DLDP 检测功能

- 必须配置。
- 在接口下配置 DLDP 功能：根据实际环境选择是否配置下一跳 IP、MAC 地址、发送间隔、重传次数、恢复次数等参数。

配置 DLDP 检测模式

- 可选配置。
- 在接口下配置 DLDP 检测模式：根据实际环境选择配置为主动或被动模式。
- 如当三层链路两端都需要开启 DLDP 功能，为节省了带宽资源和设备 CPU 资源，可将其中一端的 DLDP 检测模式改为被动模式。

全局配置 DLDP 参数

- 可选配置。
- 根据需求，可在全局下修改所有 DLDP 检测的参数，包括：检测报文的发送间隔、检测报文的重传次数、恢复次数。

检验方法

- 查看设备的 DLDP 信息，包括所有 DLDP 检测的状态信息以及其统计信息。

相关命令

启动 DLDP 检测功能

【命令格式】 **dldp** *ip-address* [*next-hop-ip*] [**mac-address** *mac-addr*] [**interval** *tick*] [**retry** *retry-num*] [**resume** *resume-num*]

【参数说明】 *ip-address*：DLDP 检测 IP 地址。

next-hop-ip：下一跳 IP 地址。

mac-addr：绑定 MAC 地址，若存在下一跳 IP 地址，则配置的是下一跳设备的 MAC 地址。

tick：检测报文的发送间隔，取值范围：5-6000 tick（1 tick =10 毫秒），缺省值 100 tick（1 秒）。

retry-num：取值范围：1-3600，缺省值 4。

resume-num：恢复次数，取值范围：1-200，缺省值 3。

【命令模式】 接口模式

【使用指导】 接口必须是三层接口，包括：路由口、L3AP、SVI 等接口。

配置 DLDP 检测模式

【命令格式】 **dldp passive**

【参数说明】 -

【命令模式】 接口模式

【使用指导】 接口下必须先开启 DLDP 检测功能后才能配置 DLDP 检测模式。

全局修改 DLDP 检测参数

【命令格式】 **dldp** { **interval** *tick* | **retry** *retry-num* | **resume** *resume-num* }

【参数说明】 *tick*：检测报文的发送间隔，取值范围：5-6000 tick（1 tick =10 毫秒），缺省值 100 tick（1 秒）。

retry-num：检测报文的重传次数，取值范围：1-3600，缺省值 4。

resume-num：恢复次数，取值范围：1-200，缺省值 3。

【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 DLDP 检测的参数时，可使用该命令快速生效。

查看 DLDP 状态信息

【命令格式】 **show dldp statistic** [**interface** *interface-name*]

【参数说明】 *interface-name*：查看信息的三层接口

【命令模式】 特权模式、全局模式、接口模式

【使用指导】 查看接口下的 DLDP 工作状态信息。

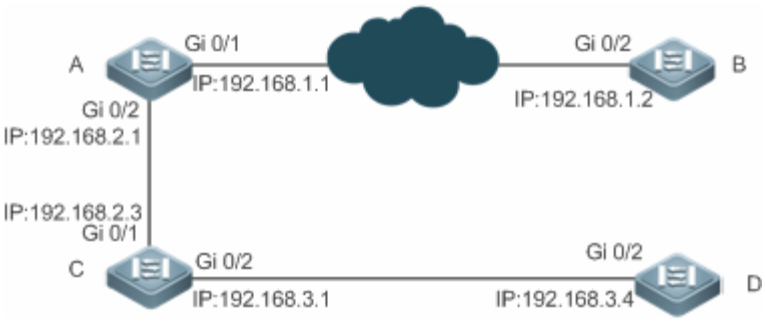
查看所有 DLDP 检测的统计信息。

配置举例

在三层网络上开启 DLDP 检测功能，分别控制 A、B 设备的三层口

【网络环境】

图 3-3



【配置方法】

- 在设备 A 上的路由口（Gi 0/1、Gi 0/2）开启 DLDP 功能，检测 A 到 B 和 D 的三层网络的链通性。
- 若需控制 B 设备的路由口（Gi 0/2），则在该接口上开启 DLDP 功能，并配置为被动模式。

A

```
A#configure terminal
A(config)#interface GigabitEthernet 0/1
A(config-if-GigabitEthernet 0/1)#dldp 192.168.1.2
A(config-if-GigabitEthernet 0/1)# exit
A(config)#interface GigabitEthernet 0/2
A(config-if-GigabitEthernet 0/1)#dldp 192.168.3.4 192.168.2.3
```

B

```
B#configure terminal
B(config)#interface GigabitEthernet 0/2
B(config-if-GigabitEthernet 0/1)#dldp 192.168.1.1
B(config-if-GigabitEthernet 0/1)#dldp passive
```

【检验方法】

- 检查 A、B 设备的 DLDP 状态信息，检测 DLDP 检测是正常开启并工作。

A

```
A# show dldp
Interface  Type         Ip          Next-hop    Interval  Retry  Resume  State
---------  -------  ----------  ----------  --------  -----  ------  ------
Gi0/1      Active   192.168.1.2               100       4      3       Up
Gi0/1      Active   192.168.3.4 192.168.2.3   100       4      3       Up
```

B

```
B# show dldp
Interface  Type         Ip          Next-hop    Interval  Retry  Resume  State
---------  -------  ----------  ----------  --------  -----  ------  ------
Gi0/2      Passive  192.168.1.1               100       4      3       Up
```

常见错误

- IPv4 单播路由不可达，误以为 DLDP 检测失效。
- 对端设备不支持 arp/icmp 回应导致 DLDP 功能失效。
- 跨网段检测没有配置下一跳 IP 地址。

3.5 监视与维护

清除各类信息

作用	命令
清除 DLDP 统计信息。	**clear dldp** [**interface** *interface-name* [*ip-address*]]

查看运行情况

作用	命令
查看 DLDP 运行状态。	**show dldp** [**interface** *interface-name*]
查看 DLDP 的 down/up 统计信息	**show dldp statistic**

4 PCAP

4.1 概述

PCAP（Packet Capture）是网络设备中常用的一种维护功能。

类似运行于个人电脑上的抓包软件，PCAP 功能可以将进入网络设备和从网络设备发出的报文抓取下来，保存在文件中，或者直接显示出来。

协议规范

-

4.2 典型应用

典型应用	场景描述
抓取报文	在日常维护过程中，发现网络内某种报文不通，指定抓包点及抓包方向，输入报文特征，启动抓包，观察报文是否到达设备及被转发走。

4.2.1 抓取报文

应用场景

在日常维护过程中，发现网络内某种报文不通，指定抓包点及抓包方向，输入报文特征，启动抓包，观察报文是否到达设备或从设备发出。

功能部属

用户按照以下步骤操作：

- 创建抓包特征规则，并为规则取名
- 创建抓包点，指定抓包点名称、抓包位置（物理口、Vlan、控制面）、抓包方向、抓包特征
- 指定保存文件名。
- 启动抓包点抓包
- 等待抓包结束。
- 把文件上传到 PC
- 使用 PC 上的抓包软件打开观察抓到的报文内容。

4.3 功能详解

功能特性

功能特性	作用
抓取报文	抓取指定物理端口、VLAN、控制面的收发报文。

4.3.1 抓取报文

用户可以定义抓包点，指定抓包位置、方向、匹配的规则信息、抓包数量、保存文件名称等信息，然后启动抓包过程。

工作原理

用户通过定义抓包点来定义抓包的规则，为了同时抓取多种类型报文，允许用户定义多个抓包点，抓包点间以名称进行区别。这些抓包规则包括：

1) 抓包的位置，可以选择在某个物理端口、VLAN 口、系统控制面作为抓包位置，每个抓包点只能定义一个抓包位置。

2) 抓包方向，可以选择出方向、入方向、双向抓包。

3) 匹配的 7 元组信息，可以匹配源 MAC、目的 MAC、二层协议类型、源 IP、目的 IP、三层协议类型、TCP/UDP 端口信息。

4) 抓包数量，可以选择指定抓包数量或者抓包文件大小。

5) 保存文件名称，指定的抓包文件名称，抓取的报文将保存为 pcap 文件格式。如不指定，默认将在控制台以 syslog 方式输出。

配置好规则后，用户通过命令启动抓包，在达到抓包数量或者文件大小后，抓包将自动停止。用户也可输入命令手动停止抓包。

⚠ 由于报文显示较多，如果不选择抓包文件名，默认在控制台以 syslog 方式输出 30 个抓到的报文。

4.4 配置详解

配置项	配置建议 & 相关命令	
抓取报文	**packet capture rule** *rule-name* **[src-mac** *smac***] [dst-mac** *dmac***] [etype** *type* **| ip | arp] [src-ip** *sip sip-mask***] [dst-ip** *dip dip-mask***]** **[protocol** *protocol* **| tcp | udp] [src-port** *sport* **] [dst-port** *dport***]**	定义抓包匹配规则。

	packet capture point *capture-point-name* **rule** *rule-name* **location {interface** *interface-name* | **vlan** *vlan-id* | **control-plane} {in | out | both}**	创建抓包点，指定抓包位置、匹配规则、抓包方向
	packet capture file *filename* **[buffer-size** *buf-size*] **[packet-num** *pkt-num*]	指定保存的文件名
	packet capture {start | stop}	开始/停止抓包

4.4.1 抓取报文

配置效果

- 定义抓包匹配规则；
- 创建抓包点；
- 指定保存的文件名
- 开始抓包。
- 停止抓包

注意事项

无

配置方法

↘ 定义抓包匹配规则

- 必选配置。用户用此命令定义抓包规则。

【命令格式】 **packet capture rule** *rule-name* **[src-mac** *smac*] **[dst-mac** *dmac*] **[etype** *type* \| **ip** \| **arp**] **[src-ip** *sip sip-mask*] **[dst-ip** *dip dip-mask*] **[protocol** *protocol* \| **tcp** \| **udp] [src-port** *sport*] **[dst-port** *dport*]

【参数说明】 *rule-name*：匹配规则名称

smac：源 MAC

dmac：目的 MAC

type | **ip** | **arp**：二层协议类型

sip：源 IP

sip-mask：源 IP 掩码

dip：目的 IP

dip-mask：目的 IP 掩码

protocol | **tcp** | **udp**：三层协议类型

sport： tcp/udp 协议源端口

dport：tcp/udp 协议目的端口

【缺省配置】 -

【命令模式】 特权模式

【使用指导】 1、用户可以定义多个不同的抓包规则，以规则名称区分不同规则。定义规则以后，规则需要被抓包点引用才会实际生效。

2、删除抓包规则之前，需要删除所有引用该规则的抓包点。

创建抓包点

- 必选配置。本命令用于创建抓包点。

【命令格式】 **packet capture point** *capture-point-name* **rule** *rule-name* **location {interface** *interface-name* | **vlan** *vlan-id* | **control-plane} {in | out | both}**

【参数说明】 *capture-point-name*：抓包点名称

rule-name：匹配的规则名称，由 **packet capture rule** 命令定义。

interface-name：抓包的端口名称

vlan-id：抓包的 vlan id

control-plane： 控制面抓包

in | out | both：抓包方向，入口、出口、或者双向。

【缺省配置】 -

【命令模式】 特权模式

【使用指导】 1、根据需要，用户可以在同一位置定义多个不同的抓包点，匹配不同的抓包规则或者报文方向。多个抓包点可以同时工作，互不影响。

2、抓包过程中，如果修改抓包点定义，不会立即生效，将在下次启动抓包时生效。

指定保存文件名

- 可选配置。本命令用于指定保存文件名。

【命令格式】 **packet capture file** *filename* **[buffer-size** *buf-size***] [packet-num** *pkt-num***]**

【参数说明】 *filename*：保存的文件名

buf-size：缓冲区大小。不选择默认按照 2M 大小存放，文件达到指定大小自动停止抓包。

pkt-num：抓包数量。抓包达到指定数量后，自动停止。不选择默认持续抓取报文。

【缺省配置】 -

【命令模式】 特权模式

【使用指导】 1、设置了保存文件名以后，抓包数据默认保存在文件里。未设置文件名，数据直接以 syslog 形式输出在控制台上。未设置文件名时，默认只能输出 30 个报文。

2、设置保存文件名后，下次启动抓包后生效。

开始/停止抓包

- 必选配置。输入此命令开始或停止抓包。

【命令格式】 **packet capture {start | stop}**

【参数说明】 **start | stop**：开始/停止抓包。

【缺省配置】 -

【命令模式】 特权模式

【使用指导】 1、开始抓包以后，如果不输入停止抓包命令，抓包数量满足后，抓包点将自动停止抓包。如果抓包的停止条件尚未满足，输入该命令后，立即停止抓包。

2、输入开始抓包后，所有抓包点同时开始抓包。

检验方法

使用 **show packet capture status** 命令查看抓包信息。

【命令格式】 **show packet capture status**

【参数说明】 -

【命令模式】 特权用户模式

【使用指导】 执行本命令可以查看抓包的状态信息。

【命令展示】

查看抓包的状态信息

```
Ruijie#show packet capture status


Capture rules:
    Capture rules tcp:
        etype: 0x0800
        source MAC: 2222.2222.2222
        destination  MAC: 1111.1111.1111
        protocol: 0x6
        source IP: 10.10.10.3
        destination  IP: 10.10.10.10
        source port: 5
        destination  port: 10


Capture points:
    Capture point controlplane:
        Capture rules: tcp
        location: control-plane
        direction: all
        status: stopped
        packets captured(in): 200
```

```
        packets captured(out): 200


Capture file:
    filename: /tmp/test.pcap
        buffer size: 2(MB)
        packets limit: 500
    Ruijie#
```

配置举例

抓取报文

【网络环境】
- 用户环境，发现设备端口 0/1 下的设备某应用 TCP 连接不上，需要抓取该端口 TCP 报文进行分析。

【配置方法】
- 使用抓包命令将 TCP 报文保存在 tcp.pcap 文件中，上传到 PC 查看抓取到的内容。

```
Ruijie# packet capture rule tcp etype ip protocol tcp
Ruijie# packet capture point tcppoint rule tcp location interface gi0/1 both
Ruijie# packet capture file flash:tcp.pcap packet-num 1500
Ruijie# packet capture start
```

【检验方法】
- 输入 **show packet capture status** 命令，发现已经开始抓包。

```
Ruijie#show packet capture status


Capture rules:
    Capture rules tcp:
        etype: 0x0800
        protocol: 0x6


Capture points:
    Capture point tcppoint:
        Capture rules: tcp
        location: Gi0/1
        direction: all
        status: running
        packets captured(in): 550
        packets captured(out): 550
```

```
Capture file:
    filename: /data/tcp.pcap
    buffer size: 2(MB)
    packets limit: 1500
```

常见错误

-

4.5 监视与维护

查看运行情况

作用	命令
查看抓包信息	**show packet capture status**

5 PPPOE-CLIENT

5.1 概述

PPPoE（Point-to-point Protocol Over Ethernet）即，基于以太网的点对点协议。

锐捷产品支持在以太网口上运行 PPPoE 客户端，使产品具有了通过简单的桥接访问设备到远程访问集中器来连接主机网络的能力。通过 PPPoE 协议，PPPoE 服务器能够实现对每个接入客户端的控制和计费。

锐捷产品支持的拨号模式：自动拨号（no DDR，永远在线）。

- PPPOE-CLIENT 适用于通过 ADSL 上网的场景。

下文仅介绍 PPPOE-CLIENT 的相关内容。

协议规范

- RFC2516：A Method for Transmitting PPP Over Ethernet (PPPoE)
- RFC1661：The Point-to-Point Protocol (PPP)

5.2 典型应用

典型应用	场景描述
ADSL 场景	在使用 ADSL 上网的场景中，提供拨号和报文转发功能。

5.2.1 ADSL场景

应用场景

在使用 ADSL 上网的场景中，提供拨号和报文转发功能。

以下图为例，讲述设备拨号上网场景。

- 设备启动拨号功能，通过 ADSL 线路，连接到远端 ISP 并获得上网的能力。
- 内网 PC 通过设备上网。

图 5-1



功能部属

- 设备启用拨号功能，通过 ADSL 线路，拨号上网。

5.3 功能详解

基本概念

ISP

ISP(Internet Service Provider) 互联网服务提供商，即向广大用户综合提供互联网接入业务、信息业务和增值业务的网络运营商。

ADSL

ADSL（Asymmetric Digital Subscriber Line）即，非对称数字用户环路，也就是拨号上网线路。

数据流

设备仅对其起转发作用的报文流。

兴趣流

由用户在配置中定义的特定的报文类，这类报文可以刺激设备开始拨号。

功能特性

功能特性	作用
拨号上网	在使用 ADSL 上网的场景中，提供拨号和报文转发功能。

5.3.1 拨号上网

拨号完成之后，设备获得了上网的能力，所以，内网中的主机也都获得了上网的能力。

工作原理

拨号、上网分别对应协商和报文转发两个过程。

其中，协商又可分为：协议协商、协议保活、协议终止三部分。

↘ 协议协商

协议协商分为 PPPoE 协商和 PPP 协商两部分。

在 PPPoE 协商中，协商双方会确认唯一的对方、记录对方 MAC 信息、建立唯一的会话 ID。

在 PPP 协商中，服务器会校验客户端的认证信息。如果校验通过，服务器就会为客户端分配 IP（如果客户端配置了 IP，且符合服务器的要求，服务器会同意这个 IP 为客户端的 IP）。

在两个协议都 UP 之后，设备就获得了上网的能力，也准备好了封装数据流报文所需的二层头。

↘ 协议保活

在 PPP 协议 UP 之后，双方会定期互发 LCP 心跳报文。如果一端在一定时间内没有收到对方回复的心跳报文，这一端就会主动终止协议。

↘ 协议终止

协议双方在一定情况下会主动终止协议。

主动终止协议方会发送 PPP 协议终止报文来结束这个 PPP 会话，然后发送 PPPoE 协议终止报文来结束这个 PPPoE 会话。

被动终止协议方在收到 PPP 协议终止报文后，会发送同意结束 PPP 会话的报文；在收到 PPPoE 协议终止报文后，会发送同意结束 PPPoE 会话的报文。

双方一旦接收到 PPPoE 协议终止报文，即使之前没有收到 PPP 协议终止报文，PPP 和 PPPoE 会话也即刻终止。

↘ 报文转发

报文发送流程：数据流路由到 dialer 口时，设备用已经准备好的二层头信息来封装数据流报文，并最终通过物理口发送出去。

报文接收流程：物理口收到报文之后，设备将报文的三层头位置标好，然后执行下一个业务，并最终发往内网的主机。

相关配置

↘ 配置以太网口

缺省情况下，以下几项都关闭，且没有默认值。

使用 **pppoe enable** 命令可以启用接口上的 PPPoE client 功能。

使用 **no pppoe enable** 命令可以关闭接口上的 PPPoE client 功能。

使用 **pppoe-client dial-pool-number** *pool-number* **no-ddr** 将以太网口绑定到指定的逻辑拨号池 (实现自动拨号的功能 ,永远在线。

使用 **no pppoe-client dial-pool-number** *pool-number* 将以太网口从指定的逻辑拨号池中解除绑定。

使用 **pppoe session mac-address** *H.H.H* 配置 pppoe 会话的 mac 地址。

↘ 配置逻辑接口

缺省情况下，以下几项都关闭。

使用 **interface dialer** *dialer-number* 添加并进入指定逻辑接口。

使用 **no interface dialer** *dialer-number* 删除指定逻辑接口。

使用 **ip address negotiate** 配置 IP 地址由协商获得。

使用 **no ip address negotiate** 取消配置。

使用 **dialer pool** *number* 关联拨号池，与以太网口中拨号池一一对应。

使用 **no dialer pool** *number* 解除与拨号池的关联。

使用 **encapsulation ppp** 配置封装 PPP 协议，PPPoE 是建立在 PPP 基础上的。

使用 **no encapsulatio** 取消封装协议的配置。

使用 **mtu** *1488* 配置最大传输单元的大小为 1488。

使用 **no mtu** 取消 mtu 的配置。

使用 **dialer-group** *dialer-group-number* 关联刺激拨号的规则，与 dialer-list 对应。

使用 **no dialer-group** 取消刺激拨号的规则的配置

使用 **ppp chap hostname** *username* 配置 CHAP 认证使用的用户名。

使用 **no ppp chap hostname** 取消 CHAP 认证使用的用户名。

使用 **ppp chap password** *password* 配置 CHAP 认证使用的密码。

使用 **no ppp chap password** 取消 CHAP 认证使用的密码。

使用 **ppp pap sent-username** *username* **password** *password* 配置 PAP 认证使用的用户名和密码。

使用 **no ppp pap sent-username** 取消 PAP 认证使用的用户名和密码。

↘ 配置必要的全局参数

缺省情况下，以下几项都关闭，要根据实际情况配置以下几项。如果要与其他功能模块合用的话，还要配置其他全局参数。

使用 **dialer-list number protocol** *protocol-name* **ip**{ **permit** | **deny** | **list** *access-list-number* }定义刺激拨号的规则。
使用 **no dialer-list number** 删除刺激拨号的规则。
使用 **ip route** *0.0.0.0 0.0.0.0* **dialer** *dialer-number* [**permanent**]配置路由，permanent 选项使路由一直有效，即使逻辑接口在线路无线时间（enable-timeout）内，此时逻辑接口处于 down 状态。

使用 no **ip route** *0.0.0.0 0.0.0.0* **dialer** *dialer-number* 取消这条路由。

使用 pppoe multi-dial enable 可以全局使能 pppoe client 多拨功能，这样在一个物理口上可以实现多路 pppoe 拨号。

使用 no pppoe multi-dial enable 可以全局关闭 pppoe client 多拨功能。

5.4 配置详解

配置项	配置建议 & 相关命令	
配置 PPPoE client 基本功能	⚠ 必须配置。	
	pppoe enable	启动 PPPoE client 功能
	pppoe-client dial-pool-number *number* **no-ddr**	绑定逻辑拨号池与指定拨号模式
	pppoe session mac-address *H.H.H*	配置 pppoe 会话的 mac 地址
	interface dialer *dialer-number*	添加并进入指定逻辑接口
	ip address { **negotiate** | *ip-addr subnet-mask* }	配置 IP 地址由获得方式
	dialer pool *number*	关联拨号池
	encapsulation ppp	配置封装 PPP 协议
	mtu *1488*	配置最大传输单元的大小为 1488
	dialer-group *dialer-group-number*	关联刺激拨号的规则
	ppp chap hostname *username*	配置 CHAP 认证使用的用户名
	ppp chap password *password*	配置 CHAP 认证使用的密码
	ppp pap sent-username *username* **password** *password*	配置 PAP 认证使用的用户名和密码
	dialer-list number protocol *protocol-name* **ip** { **permit** | **deny** | **list** *access-list-number* }	定义刺激拨号的规则
	⚠ 可选配置。	
	pppoe multi-dial enable	**使能 pppoe client 的多拨功能**

5.4.1 配置PPPoE client基本功能

配置效果

- 设备主动发起 PPPoE 协商，并完成：协商过程、协议保活、协议终止。
- 协商完成之后，获得上网能力，开始转发路由到 dialer 口的数据流。

注意事项

- 内核模块卸载后，用户依然可以继续配置管理，但是将无法完成协商和数据流转发。

配置方法

启用 PPPoE client 功能

- 必须配置。
- 在以太口上配置。
- 启用 PPPoE client 功能。

绑定逻辑拨号池与指定拨号模式

- 必须配置。
- 在以太口上配置。
- 将以太网口绑定到指定的逻辑拨号池，并指定拨号模式。

配置 pppoe 会话的 mac 地址

- 必须配置。
- 在以太口上配置。
- 指定子接口拨号时 pppoe 会话的 mac 地址。

添加并进入指定逻辑接口

- 必须配置。
- 在全局模式配置。
- 添加并进入指定逻辑接口的配置模式。

配置逻辑口 IP 获得方式

- 必须配置。
- 在逻辑口上配置。
- 配置逻辑口 IP 获得方式。

关联拨号池

- 必须配置。
- 在逻辑口上配置。
- 将逻辑接口与特定拨号池关联起来。

配置封装协议

- 必须配置。
- 在逻辑口上配置。
- 为逻辑接口配置 PPP 封装协议。

配置逻辑口 MTU

- 必须配置。
- 在逻辑口上配置。
- 配置逻辑接口的 MTU 为 1488。

关联刺激拨号规则

- 必须配置。
- 在逻辑口上配置。
- 关联刺激拨号的规则。

配置 CHAP 认证使用的用户名

- 必须配置。
- 在逻辑口上配置。
- 配置 CHAP 认证使用的用户名。

配置 CHAP 认证使用的密码

- 必须配置。
- 在逻辑口上配置。
- 配置 CHAP 认证使用的密码。

配置 PAP 认证使用的用户名和密码

- 必须配置。
- 在逻辑口上配置。
- 配置 PAP 认证使用的用户名和密码。

定义刺激拨号规则

- 必须配置。
- 在全局模式配置
- 定义刺激拨号的规则。

开启 pppoe 多拨功能

- 可选配置。
- 在全局模式配置。
- 一旦开启多拨，可以支持在一个物理口上支持多路的 pppoe 拨号。

检验方法

- 检查 dialer 口是否获取到了 IP。
- 检查设备上是否建立了正确的 dialer 口路由表项。

相关命令

启用 PPPoE client 功能

【命令格式】 **pppoe enable**
【参数说明】 **-**
【命令模式】 接口模式
【使用指导】 启用 PPPoE client 接口必须是 WAN 属性的以太口。

绑定逻辑拨号池与指定拨号模式

【命令格式】 **pppoe-client dial-pool-number** *number* **no-ddr**
【参数说明】 *number* ：拨号池编号

【命令模式】 接口模式
【使用指导】 接口必须先启用 PPPoE client 功能。

配置 pppoe 会话的 mac 地址

【命令格式】 **pppoe session mac-address *H.H.H***
【参数说明】 *H.H.H* ：mac 地址
【命令模式】 接口模式
【使用指导】 子接口下必须先启用 PPPoE client 功能。

添加并进入指定逻辑接口

【命令格式】 **interface dialer** *dialer-number*
【参数说明】 *dialer-number*：接口编号。
【命令模式】 全局模式
【使用指导】 -

配置逻辑口 IP 获得方式

【命令格式】 **ip address** { **negotiate** | *ip-addr subnet-mask* }
【参数说明】 *ip-addr*：手动配置 IP。
subnet-mask：手动配置子网掩码。
【命令模式】 接口模式
【使用指导】 如果选择 negotiate，那么 dialer 口的 IP 将协商获得。
如果手动指定 dialer 口的 IP，需要在协商中得到对端同意，才能正常工作。

关联拨号池

【命令格式】 **dialer pool** *number*

【参数说明】 *number*：拨号池编号。
【命令模式】 接口模式
【使用指导】 dialer 口将从这个拨号池中选择以太口进行拨号。

配置封装协议

【命令格式】 **encapsulation ppp**
【参数说明】 **-**
【命令模式】 接口模式
【使用指导】 -

配置逻辑口 MTU

【命令格式】 **mtu** *1488*
【参数说明】 **-**
【命令模式】 接口模式
【使用指导】 因为通过 PPPoE 协议上网，报文的二层头比普通以太报文要长。

关联刺激拨号规则

【命令格式】 **dialer-group** *dialer-group-number*
【参数说明】 *dialer-group-number*: 刺激拨号规则的编号
【命令模式】 接口模式
【使用指导】 如果配置的是 DDR 模式，只有规则内的报文路由到 dialer 口才会刺激设备拨号。
如果配置的是 no-ddr 模式，则这行配置没有作用。

配置 CHAP 认证使用的用户名

【命令格式】 **ppp chap hostname** *username*
【参数说明】 *username*：用户名
【命令模式】 接口模式
【使用指导】 -

配置 CHAP 认证使用的密码

【命令格式】 **ppp chap password** *password*

【参数说明】 *password*：密码
【命令模式】 接口模式
【使用指导】 -

配置 PAP 认证使用的用户名和密码

【命令格式】 **ppp pap sent-username** *username* **password** *password*
【参数说明】 *username*：用户名
password：密码
【命令模式】 接口模式

【使用指导】 -

定义刺激拨号的规则

【命令格式】 **dialer-list number protocol** *protocol-name* **ip{ permit** | **deny** | **list** *access-list-number* }

【参数说明】 *protocol-name*：协议名称

access-list-number：ACL 编号

【命令模式】 全局模式

【使用指导】 -

开启 pppoe 多拨功能

【命令格式】 **pppoe multi-dial enable**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 -

配置举例

以下配置举例，仅介绍与 PPPoE client 相关的配置。

在 ADSL 场景下，启用 PPPoE client 功能，并通过 ADSL 线路上网。

【网络环境】

图 5-2



【配置方法】 ● 在设备上启用 PPPoE client 功能，将 Gi0/5 口放入拨号池。

A

```
A# configure terminal
A(config)# interface GigabitEthernet 0/5
A(config-if)# pppoe enable
A(config-if)# pppoe-client dial-pool-number 1 no-ddr
A(config-if)# exit
A(config)# interface dialer 1
```

```
A(config-if)# ip address negotiate
A(config-if)# mtu 1488
A(config-if)# encapsulation ppp
A(config-if)# ip nat outside
A(config-if)# dialer pool 1
A(config-if)# dialer-group 1
A(config-if)# ppp chap hostname pppoe
A(config-if)# ppp chap password pppoe
A(config-if)# ppp pap sent-username pppoe password pppoe
A(config-if)# exit
A(config)# access-list 1 permit any
A(config)# dialer-list 1 protocol ip permit
A(config)# ip nat inside source list 1 interface dialer 1
A(config)# ip route 0.0.0.0 0.0.0.0 dialer 1
A(config)# end
A#
```

【检验方法】 使用 **show ip interface brief | in dialer** *1* 查看 dialer 口是否获取到 IP。

使用 **show ip route** 查看是否建立了正确的 dialer 口路由表项。

```
A# show ip interface brief | in dialer 1
dialer 1                        49.1.1.127/32        YES       UP
A# show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is 0.0.0.0 to network 0.0.0.0
S*    0.0.0.0/0 is directly connected, dialer 1
C     10.10.3.0/24 is directly connected, GigabitEthernet 0/0
C     10.10.3.1/32 is local host.
C     10.202.172.1/32 is directly connected, dialer 1
C     49.1.1.127/32 is local host.
```

网关产品不支持 BGP,ISIS，配置举例仅作为配置参考，实际请以具体设备配置为准。

【配置方法】 在设备上启用 PPPoE client 多拨功能，将 Gi0/5 口上进行两路拨号

B

```
A# configure terminal
A(config)#pppoe multi-dial enable
```

```
A(config)# interface GigabitEthernet 0/5
A(config-if)# pppoe enable
A(config-if)# pppoe-client dial-pool-number 1 no-ddr
A(config-if)# pppoe-client dial-pool-number 2 no-ddr
A(config-if)#exit
A(config)# interface dialer 1
A(config-if)# ip address negotiate
A(config-if)# mtu 1488
A(config-if)# ip nat outside
A(config-if)# dialer pool 1
A(config-if)# ppp chap hostname pppoe
A(config-if)# ppp chap password pppoe
A(config-if)# ppp pap sent-username pppoe password pppoe
A(config-if)# exit
A(config)# interface dialer 2
A(config-if)# ip address negotiate
A(config-if)# mtu 1488
A(config-if)# ip nat outside
A(config-if)# dialer pool 2
A(config-if)# ppp chap hostname pppoe1
A(config-if)# ppp chap password pppoe1
A(config-if)# ppp pap sent-username pppoe1 password pppoe1
A(config-if)# exit
A(config)# ip nat inside source list 1 interface dialer 1
A(config)# ip nat inside source list 1 interface dialer 2
A(config)# ip route 0.0.0.0 0.0.0.0 dialer 1
A(config)# ip route 0.0.0.0 0.0.0.0 dialer 2
A(config)# end
A#
```

【检验方法】 使用 **show ip route** 查看是否建立了正确的 dialer 口路由表项。

```
A# show ip route
Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is 0.0.0.0 to network 0.0.0.0
S*   0.0.0.0/0 is directly connected, dialer 1
S*   0.0.0.0/0 is directly connected, dialer 2
```

```
C    10.10.3.0/24 is directly connected, GigabitEthernet 0/0
C    10.10.3.1/32 is local host.
C    10.202.172.1/32 is directly connected, dialer 1
C    10.202.172.2/32 is directly connected, dialer 2
C    49.1.1.1  27/32 is local host.
```

网关产品不支持 BGP,ISIS，配置举例仅作为配置参考，实际请以具体设备配置为准。

常见错误

- 用户名、密码不对导致无法协商成功。
- NAT 配置不正确导致内网主机无法上网。
- 路由配置不正确导致内网主机无法上网。

5.5 监视与维护

清除各类信息

在设备运行过程中执行 **clear pppoe tunnel** 命令，会清除隧道而导致报文转发中断。

作用	命令
清除进行 DDR 拨号接口的统计信息。	**clear dialer** [*interface-type interface-number*]
清除隧道。	**clear pppoe tunnel**

查看运行情况

作用	命令
查看 DDR 拨号的相关信息。	**show dialer** [**interface** type number] [**maps**] [**pools**]
查看 PPPoE 状态信息。	**show pppoe** { **ref** | **session** | **tunnel** }

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
打开按需拨号（DDR）的调试开关。	**debug dialer** { **pkt** | **mlp|callback|event** }
打开 PPP 协商的调试开关。	**debug ppp** [**authentication** | **error** | **event** | **negotiation** | **packet**]
打开 PPPoE 协商的调试开关。	**debug pppoe** [**datas** | **errors** | **events** | **packets**]

6 PPPoE-SERVER

6.1 概述

PPPoE 是 point-to-point protocol over ethernet 的简称，可以使以太网的主机通过一个简单的桥接设备连到一个远端的接入集中器上。通过 PPPoE 协议，远端接入设备能够实现对每个接入用户的控制和计费。与传统的接入方式相比，PPPoE 具有较高的性能价格比，它在包括小区组网建设等一系列应用中被广泛采用，目前流行的宽带接入方式 adsl 就使用了 PPPoE 协议。

PPPoE 协议包括 PPPoE CLIENT 和 PPPoE SERVER，这里的 PPPoE-SERVER 就是负责接入 PPPoE 的连接请求，使用户可以接入外网，目前最常见的使用方式比如家庭的宽带连接就是使用了 PC 自带的 PPPoE CLIENT 接入到运营商的 PPPoE SERVER 设备中，是家庭用户可以上网。

协议规范

- RFC2516：A Method for Transmitting PPP Over Ethernet (PPPoE)

6.2 典型应用

典型应用	场景描述
PPPoE SERVER 本地认证	在接入端的设备上启用 PPPoE SERVER 功能，并且通过指定的用户名进行本地认证，PPPoE Client 的 IP 地址由 PPPoE Server 分配。
PPPoE SERVER 远程认证	在接入端的设备上启用 PPPoE SERVER 功能，并且通过 AAA 和 Radius 配合完成远程认证，PPPoE Client 的 IP 地址由 PPPoE Server 分配。

6.2.1 PPPoE SERVER本地认证配置

应用场景

PPPoE CLIENT 通过无线网卡接入无线网络，在接入端的 AC 设备上启用 PPPoE SERVER 功能，并且通过指定的用户名进行本地认证，PPPoE Client 的 IP 地址由 PPPOE Server 分配。

图 6-1



功能部属

- 在接入设备中启用 PPPoE SERVER 功能，实现 PPPoE 拨号服务端功能。
- 在接入设备中配置用户名和密码，实现 PPPoE 拨号时身份认证。
- 在接入设备中配置本地地址池，实现 PPPoE 拨号成功后给用户主机分配 IP。
- 在用户主机启用 PPPoE Client 实现拨号上网。

6.2.2 PPPoE SERVER远程认证配置

应用场景

PPPoE CLIENT 通过无线网卡接入无线网络，在接入端的 AC 设备上启用 PPPoE SERVER 功能，并且通过 AAA 和 Radius 配合完成远程认证，PPPoE Client 的 IP 地址由 PPPoE Server 分配。

图 6-2



功能部属

- 在接入设备中启用 PPPoE SERVER 功能，实现 PPP 拨号服务端功能。
- 在接入设备中启用 radius 认证，实现对 PPP 用户 radius 认证功能。
- 在接入设备中启用 AAA 认证，实现对 PPP 用户 AAA 认证。
- 在用户主机启用 PPPoE Client 实现拨号上网。

6.3 功能详解

基本概念

AC-Cookie Tag

该 TAG 是 PPPoE SEVER 用于防止 DoS 攻击。PPPoE SEVER 可以在 PADO 数据包中包含该 TAG。如果 PPPoE CLIENT 收到了该标签，它必须在接下来的 PADR 中不加改变的包含该标签。TAG_VALUE 是任意长度和值的二进制数据，不能由 PPPoE CLIENT 解释。

功能特性

功能特性	作用
PPPoE SERVER 本地认证	在接入设备本地完成 PPP 认证，PPPOE Client 的 IP 地址由本地地址池分配。
PPPoE SERVER 远程认证	通过 AAA 和 Radius 配合完成远程认证,PPPOE Client 的 IP 地址由 Radius Server 分配。

6.3.1 PPPoE SERVER本地认证

在接入设备本地完成 PPP 认证，PPPOE Client 的 IP 地址由本地地址池分配。

工作原理

PPPOE 协议提供了在广播式的网络（如以太网）中多台主机连接到远端的访问集中器（能完成上述功能的设备也称为宽带接入服务器）上的一种标准。在这种网络模型中，所有用户的主机都需要能独立的初始化自己的 PPP 协议栈，通过 PPP 协议所具有的一些特点，能实现在广播式网络上对用户进行计费和管理。为了能在广播式的网络上建立、维持各主机与访问集中器之间点对点的关系，那么就需要每个主机与访问集中器之间能建立唯一的点到点的会话。

PPPOE 协议共包括两个阶段，即 PPPOE 的发现阶段（PPPOE Discovery Stage）和 PPPOE 的会话阶段（PPPOE Session Stage）。这里更注重对 PPPOE 发现阶段的说明，对于 PPPOE 的会话阶段，可以看成和 PPP 的通信过程是一样的，而两者的主要区别在于只是在 PPP 的数据报文前封装了 PPPOE 的报文头。无论是哪一个阶段的数据报文最终会被封装成以太网的帧进行传送。

当一个主机希望能够开始一个 PPPOE 会话时，它首先会在广播式的网络（协议中是这样说的，但在实际应用中，可能还要跨跃多点访问的网络，如 ATM 等，从而就形成了 PPPOEOA 的数据包）上寻找一个访问集中器，当然可能网络上会存在多个访问集中器时，对于主机而言则会根据各访问集中器（AC，Access Concentration）所能提供的服务或用户的预先的一些配置来进行相应的选择。当主机选择完了所需要的访问集中器后，就开始和访问集中器建立一个 PPPOE 会话进程。在这个过程中访问集中器会为每一个 PPPOE 会话分配一个唯一的会话 ID，会话建立起来后就开始了 PPPOE 的会话阶段，在这个阶段中已建立好点对点连接的双方（这种点对点的结构与 PPP 不一样，它是一种逻辑上的点对点关系）就采用 PPP 协议来交换数据报文，从而完成一系列 PPP 的过程，最终将在协商建立的点对点的逻辑通道上进行网络层数据报的传送。

相关配置

↘ 配置 loopback 接口

缺省情况下，系统未定义 loopback 接口，定义 loopback 接口的目的是让 virtual-template 接口可以借用 loopback 接口的 IP 地址，拷贝到动态创建的 virtual-access 接口上完成 PPP 协商。

使用 **interface loopback** xxx 命令可以创建 loopback 接口，使用 ip address A.B.C.D A.B.C.D 可以为 loopback 接口分配 IP 地址。

必须创建 loopback 口并配置 loopback 接口的 IP 地址，否则 virtual-template 无法借用 loopback 接口的 IP 地址。

↘ 配置认证 username 和 password

为了完成 PPP 的认证，需要在 PPPoE SERVER 端配置 username 和 password。

使用 **username** xxxx **password** xxxx 命令可以配置认证 username 和 password。

如果 PPPoE SERVER 采用 AAA 远程认证，则不需要配置 username 和 password。

↘ 配置本地地址池

为了完成在 PPP 协商过程中为 client 端分配 ip 地址，需要在 PPPoE SERVER 端配置本地地址池。

使用 **ip local pool** pool-name A.B.C.D A.B.C.D 命令可以配置本地地址池。

如果 PPPoE SERVER 采用认证服务器分配地址，则不需要配置该命令。

↘ 配置虚拟模板

缺省情况下，宽带接入服务器未配置可供 PPPoE SERVER 使用的虚拟模板，在启用 PPPoE SERVER 功能时，当会话创建成功后生成的 Virtual-access 接口需要从虚拟模板接口拷贝配置，因此必须首先建立一个虚拟模板接口，并配置接口的相关参数。

使用 **interface virtual-template** number 命令可以创建虚拟模板并进入虚拟模板配置模式。

在 virtual-template 模式下使用 **ip unnumbered loopback** number 可以配置虚拟模板 unnumber 到 loopback 口，从而借用 loopback 口的 IP。

在 virtual-template 模式下使用 **ppp authentication {chap | pap } [**list-name**]**可以配置认证类型为 chap 或 pap 认证。PPPoE 接入认证类型可支持 pap 和 chap 两种认证方法，同时可根据组网方式的不同采取本地认证和远程认证。如果采用远程认证则需要关联设备启用的认证列表名称，具体可参考<AAA-SCG.doc>。

在 viitual-template 模式下使用 **peer default ip address pool** local 可以配置为 client 端分配 ip 的地址池为为 local。

pppoe server 功能必须配置虚拟模板。

↘ 配置 bba-group

要完成 pppoe server 端的功能，启用 pppoe server 功能的接口需要设置关联的 bba-group pppoe 拨号组，在 bba-group 拨号组上设置 pppoe 拨号 server 的配置、连接限制及关联的虚拟模板。

使用 **bba-group pppoe** pppoe_group 命令可以配置 bba-group。

在 bba-group 模式下使用 **virtual-template** number 命令可以关联虚拟模板（必选）。

在 bba-group 模式下使用 **ac-cookie enable** 命令可以启用 ac-cookie 功能(可选)。

在 bba-group 模式下使用 **sessions local-mac limit** count 命令可以设置 PPPoE Client 一个 mac 地址最多接入的会话数(可选)。

在 bba-group 模式下使用 **sessions per-mac limit** count 命令可以设置 PPPoE Server 一个 mac 地址最多接入的会话数(可选)。

在 bba-group 模式下使用 **sessions max limit** count 命令可以设置当前设备最多多接入的会话数(可选)。

↘ 接口启用 PPPoE SERVER 功能

是 PPPoE SERVER 功能的总开关。

在接口配置模式下使用 **pppoe-server enable group** pppoe_group 开启 PPPoE SERER 功能，并关联 bba-group。

PPPoE SERVER 功能在接口下默认关闭。

6.3.2 PPPoE SERVER远程认证

通过 AAA 和 Radius 配合完成远程认证,PPPoE Client 的 IP 地址由 PPPoE Server 分配。

工作原理

原理与本地认证一样，只是认证数据由 PPPoE SERVER 发给 AAA 和 Radius 共同完成远程认证，IP 地址还是由 PPPoE SERVER 分配。相比本地认证方式，不需要配置 username 和 password，而是采用 AAA 认证。

相关配置

PPPoE SERVER 远程认证的基本过程与本地认证一样，只是不需要配置本地 username 和 password。其它的都是需要配置的。

↘ 配置虚拟模板采用 PPP 用户认证方法列表

在全局模式使用 **ppp authentication {chap | pap }** *list-name* 配置虚拟模板采用 PPP 用户认证方法列表，具体命令请参照<PPP-SCG.doc>。

↘ 配置启用 AAA 认证参数

在全局模式使用 **aaa authentication ppp** *list-name* **group radius** 配置对 ppp 认证用户列表明启用 radius 认证。

在全局模式使用 **aaa new-model** 启用 aaa 认证。

具体命令请参照<AAA-SCG.doc>。

↘ 配置 radius 认证参数

在全局模式使用 **radius-server host** *ipv4-address* 配置 radius 安全服务器主机。

在全局模式使用 **radius-server key [**0 | 7**]** *text-string* 配置与 RADIUS 安全服务器进行通信的共享口令。

具体命令请参照<AAA-SCG.doc>。

6.4 产品说明



NBR108G-P、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1500G、NBR2000G 不支持 PPOE SERVER 功能 ;NBR800G、NBR950G、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 PPOE SERVER 功能。

6.5 配置详解

配置项	配置建议 & 相关命令	
配置 PPPoE SERVER 本地认证	⚠ 必须配置。用于配置 PPPoE SERVER 本地认证，如果是选择配置为远程认证，则不必配置 username 和 password，其余项都是必配。	
	interface loopback *number*	配置 loopback 口。
	Ip address *A.B.C.D A.B.C.D*	配置 loopback 口的 IP 地址。
	username *username* **password** *password*	配置认证 username 和 password。如果 PPPoE SERVER 采用 AAA 远程认证，则本项配置不需要。
	ip local pool *pool-name A.B.C.D A.B.C.D*	配置本地地址池。
	interface virtual-template *number*	配置虚拟模板
	ip unnumber loopback *number*	Unnumber 到 loopback 口 ,借用 loopback 口的 IP 地址。在 virtual-template 接口模式下配置。
	ppp authentication {chap | pap }	配置认证类型为 chap 或 pap 认证。PPPOE 接入认证类型可支持 pap 和 chap 两种认证方法 ,同时可根据组网方式的不同采取本地认证和远程认证。如果采用远程认证则需要关联设备启用的认证列表名称，具体可参考 <AAA-SCG.doc>。此命令在 virtual-template 接口模式下配置。
	peer default ip address pool *pool-name*	配置为 client 端分配 ip 的地址池为为 pool-name。此命令在 virtual-template 接口模式下配置。
	bba-group pppoe *pppoe_group*	配置 bba-group。
	virtual-template *number*	关联虚拟模板接口。
	pppoe-server enable group *pppoe_group*	在 PPPoE Client 的接入接口开启 pppoe server 功能，并关联 bba-group。。
配置 PPPoE SERVER 远程认证	⚠ 可选配置。用于配置 PPPoE SERVER 远程认证。这里只描述 username 和 password 替换为 aaa 认证	

	aaa new-model	配置启用 aaa。
	aaa authentication ppp *list-name* **group radius**	配置对 ppp 认证用户列表启用 radius 认证
	ppp authentication {chap | pap } [*list-name*]	配置虚拟模板采用 PPP 用户认证方法列表
	radius-server host *ipv4-address*	配置 radius 认证主机
	radius-server key [0 | 7] *text-string*	配置 radius 认证共享口令

6.5.1 配置PPPoE-SERVER本地认证

配置效果

PPPoE CLIENT 通过指定的用户名进行本地认证，PPPoE Client 的 IP 地址由 PPPOE Server 分配。

注意事项

无

配置方法

↘ 配置 loopback 接口

- 必须配置。
- 用户也可以用其他的三层口替换 loopback 口，但 loopback 口的好处是只要有 IP 地址，永远不会 down。

↘ 配置认证 username 和 password

- 如果采用本地认证，则本项配置必须配置；如果 PPPoE SERVER 采用 AAA 远程认证，则本项配置不需要。

↘ 配置本地地址池

- 必须配置。
- 一般情况下，地址池的范围和 loopback 是同一个网段，减少路由的配置。

↘ 配置虚拟模板

- 必须配置。
- 如果采用远程认证则需要关联设备启用的认证列表名称，具体可参考<AAA-SCG.doc>。
- 在 bba-group 模式下配置关联对应的 virtual-template 接口，在全局模式下配置 virtual-template 接口。

↘ 配置 bba-group

- 必须配置，关联虚拟模板接口。

在接口启用 pppoe 并关联 bba-group

- 必须配置，关联 bba-group。
- 在接口模式下配置，例如 interface vlan 1 接口下。

检验方法

在客户端主机 PPPoE Client 拨号能够成功。

相关命令

创建 loopback 接口

【命令格式】 **interface loopback** *number*
【参数说明】 *number*：新建的 loopback 端口号。
【命令模式】 全局模式
【使用指导】 -

配置 loopback 接口的 IP 地址

【命令格式】 **ip address** *A.B.C.D A.B.C.D*
【参数说明】 *A.B.C.D A.B.C.D*：配置 IP 地址
【命令模式】 接口模式
【使用指导】 -

配置认证 username 和 password

【命令格式】 **username** *username* **password** *password*
【参数说明】 *username*：用户名。
password：用户密码。
【命令模式】 全局模式。
【使用指导】 如果 PPPoE SERVER 采用 AAA 远程认证，则本项配置不需要。

创建本地地址池

【命令格式】 **ip local pool** *pool-name A.B.C.D A.B.C.D*
【参数说明】 *pool-name*：地址池。
A.B.C.D A.B.C.D：IP 地址的范围。
【命令模式】 全局模式。
【使用指导】 -

创建虚拟模板

【命令格式】 **interface virtual-template** *number*

【参数说明】 *number*：新建的虚拟模板编号。
【命令模式】 全局模式
【使用指导】 -

虚拟模板 unnumber 到 loopback 口

【命令格式】 **ip unnumbered loopback** *number*
【参数说明】 *number*：新建的 loopback 接口编号。
【命令模式】 virtual-template 模式
【使用指导】 -

配置认证类型为 chap 或 pap 认证

【命令格式】 **ppp authentication {chap | pap } [***list-name***]**
【参数说明】 *list-name*：认证列表，这个一般 aaa 认证才使用
【命令模式】 virtual-template 模式
【使用指导】 PPPOE 接入认证类型可支持 pap 和 chap 两种认证方法，同时可根据组网方式的不同采取本地认证和远程认证。如果采用远程认证则需要关联设备启用的认证列表名称，具体可参考<AAA-SCG.doc>。

配置为 PPPoE client 端分配 ip 的地址池

【命令格式】 **peer default ip address pool** *pool-name*
【参数说明】 *pool-name*：地址池名字。
【命令模式】 virtual-template 模式
【使用指导】 -

创建 bba-group

【命令格式】 **bba-group pppoe** *group-name*
【参数说明】 *group-name*：bba-group 的名称。
【命令模式】 全局模式
【使用指导】 -

配置 bba-group 关联虚拟模板

【命令格式】 **virtual-template** *number*
【参数说明】 *number*：虚拟模板编号。
【命令模式】 bba-group 模式
【使用指导】

接口启用 PPPoE SERVER 功能

【命令格式】 **pppoe-server enable group** *bba-group*
【参数说明】 *bba-group*：虚拟 bba-group 名称。
【命令模式】 接口模式
【使用指导】 在 PPPOE Client 接入的接口启用 pppoe server 功能，并关联 bba-group

配置举例

↘ 配置 PPPOE 本地认证

【网络环境】
图 6-3



【配置方法】
- 在 PPPoE SERVER 端按基本步骤本地认证
- PPPoE CLINET 通过无线网卡以 PPPOE 认证的方式接入 AC

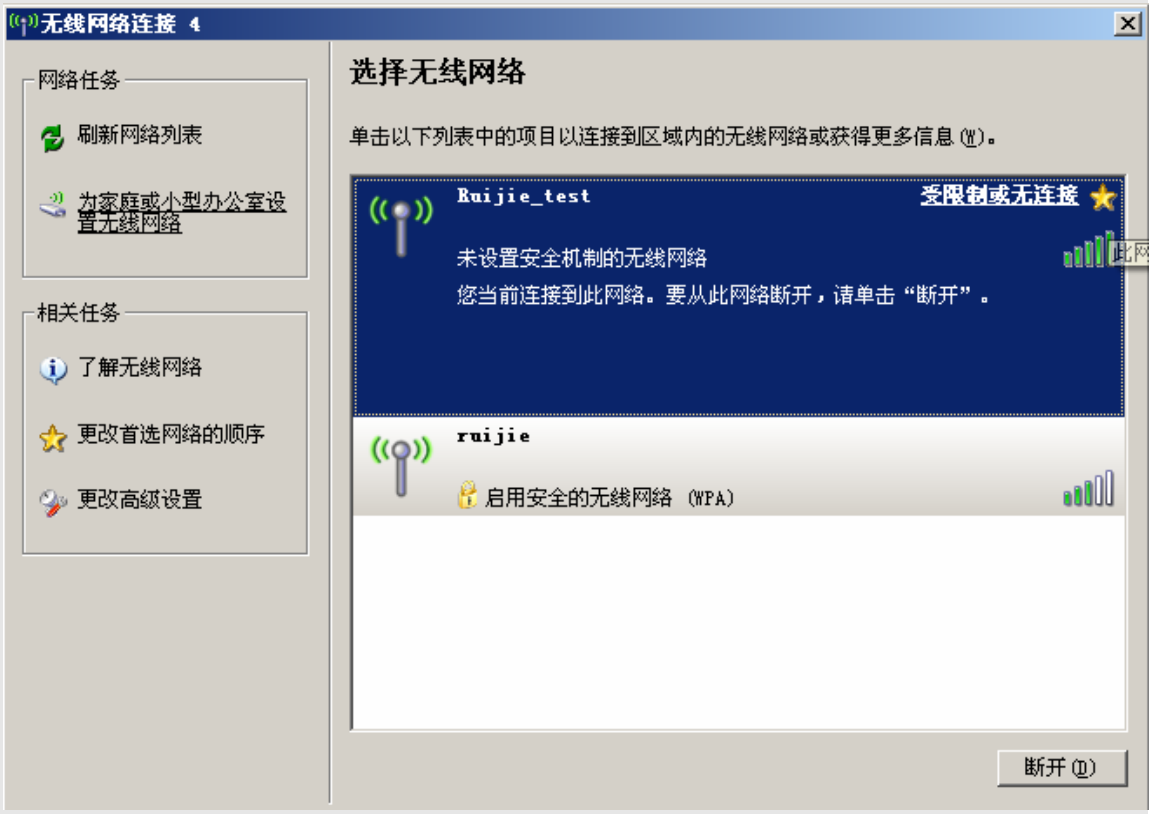
PPPOE SERVER

```
#配置 username 和 password
Ruijie#conf
Ruijie(config)#username ruijie password ruijie
Ruijie(config)#end
Ruijie#

#配置本地地址池
Ruijie#conf
Ruijie(config)#ip local pool pppoe 1.2.3.4 1.2.3.254
Ruijie(config)#end
Ruijie#

#说明：以下配置不分先后顺序

#配置 bba-group
Ruijie#conf
Ruijie(config)#bba-group pppoe pppoe1
Ruijie(config-bba-group)#virtual-template 2
Ruijie(config-bba-group)#exit
Ruijie(config)#end
Ruijie#

#配置 loopback 接口
Ruijie#conf
Ruijie(config)#int loopback 1
Ruijie(config-if-Loopback 1)#ip address 1.2.3.1 24
Ruijie(config-if-Loopback 1)#end
```

```
Ruijie#

#配置虚拟模板
Ruijie#conf
Ruijie(config)#int virtual-template 2
Ruijie(config-if-Virtual-Template 2)#ip unnumbered loopback 1
Ruijie(config-if-Virtual-Template 2)#ppp authentication pap chap
Ruijie(config-if-Virtual-Template 2)#peer default ip address pool pppoe
Ruijie(config-if-Virtual-Template 2)#end
Ruijie#

#配置 vlan 并在接口上使能 pppoe-server 功能
Ruijie#conf
Ruijie(config)#vlan 1
Ruijie(config-vlan)#exit
Ruijie(config)#int vlan 1
Ruijie(config-if-VLAN 1)#pppoe-server enable group pppoe1
Ruijie(config-if-VLAN 1)#end
Ruijie#
Ruijie#
```

PPPOE Client

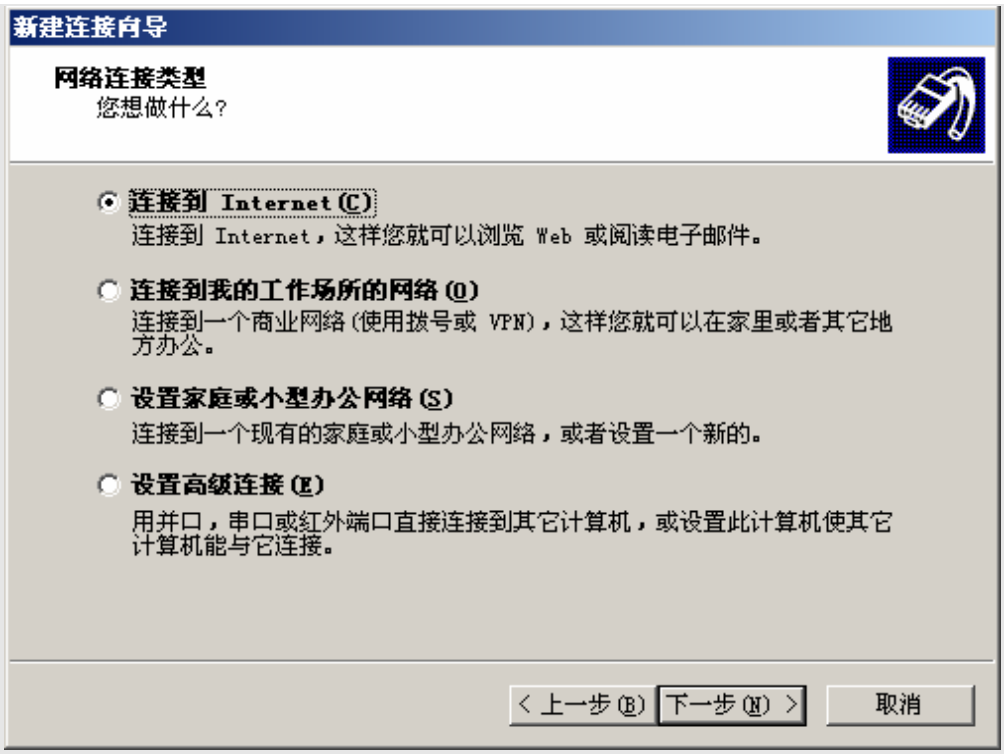
首先保证 PC 上已经安装完成了对应型号的无线网卡驱动，可以搜索到 PPPoE SERVER 端配置的 SSID，并将其设置为首选网络，如下图所示：



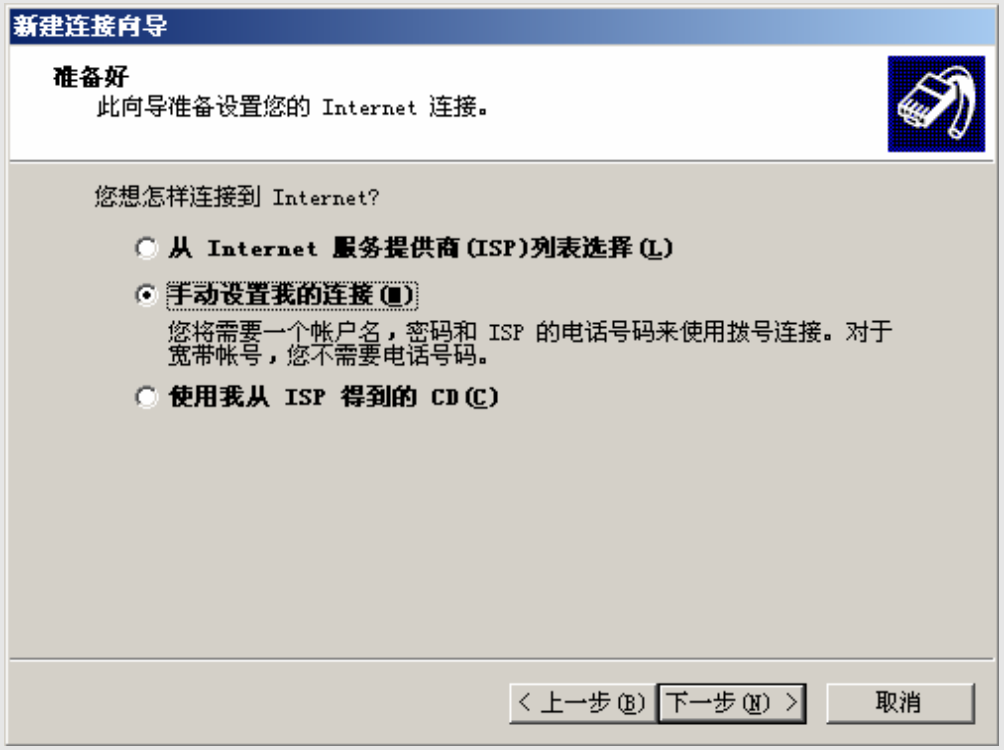
打开网上邻居->查看网络连接->创建一个新的连接



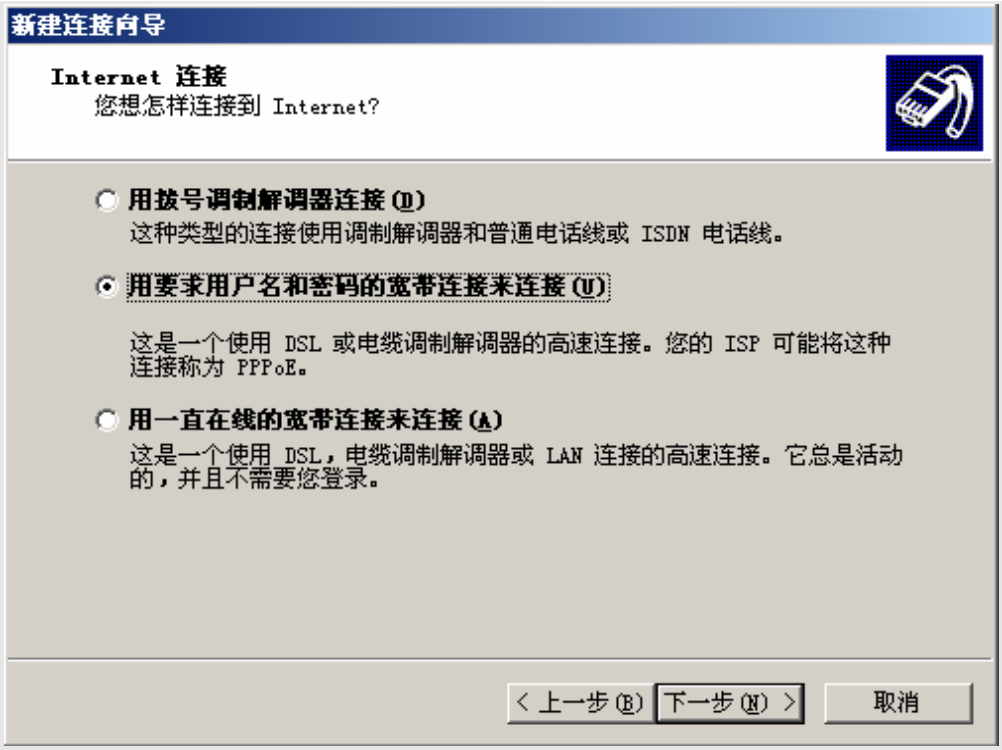
点击下一步，选择：连接到 Internet(C)



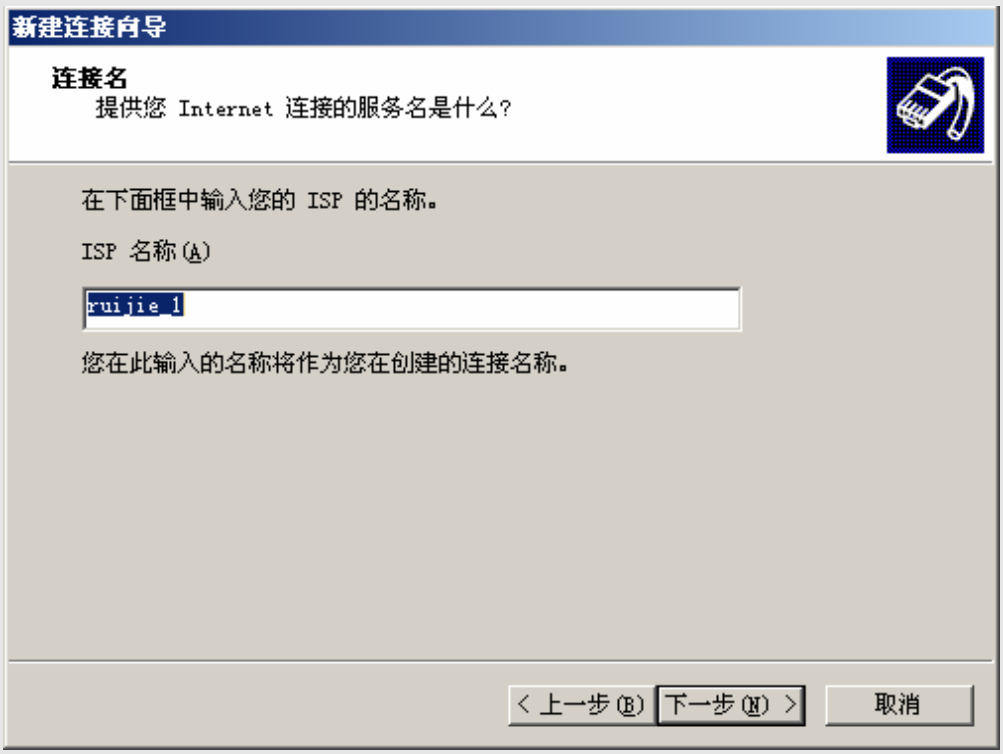
选择：手动设置我的连接(M)



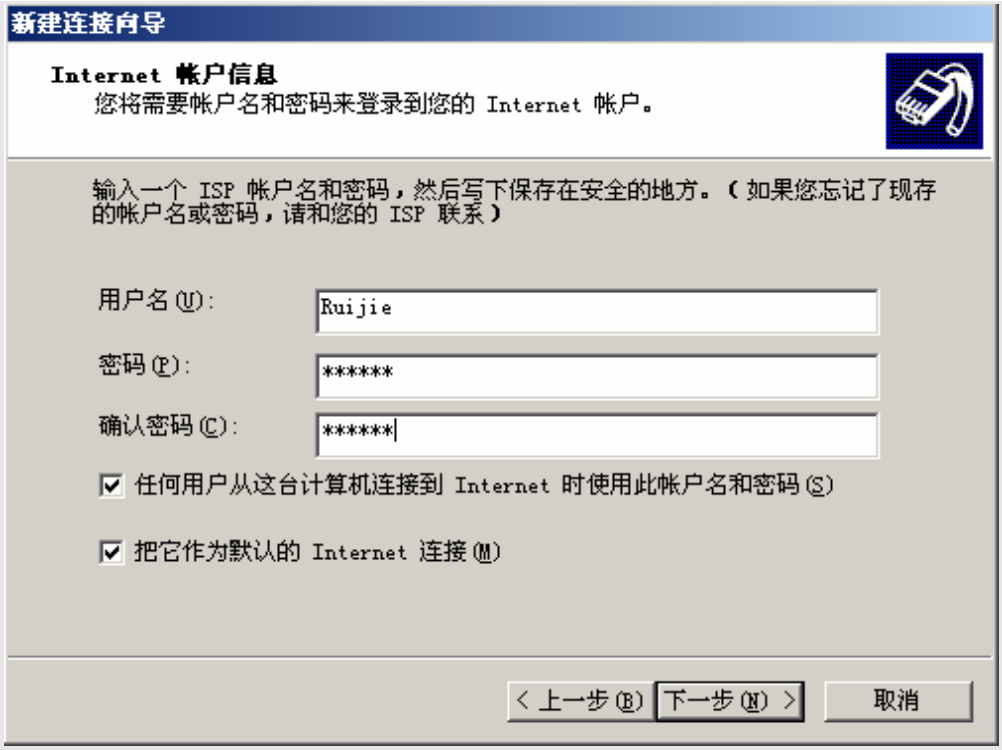
选择：用要求的用户名和密码的宽带连接来连接(U)



输入 ISP 的名称：ruijie_1



输入 PPPOE SERVER 端提供的用户名和密码，本例中用户名及密码均为：Ruijie



点击下一步，完成，通过点击连接即开始通过 PPPOE 的方式接入 AC。




```
B(config)# ip pim bsr-candidate loopback 0
```

【检验方法】

- 在 PPPoE SERVER 端通过 show pppoe session 命令查看连接状态

	● 在 PPPoE CLIENT 端拨号能成功
PPPOE SERVER	Ruijie#show pppoe-server session #以下是 pppoe server 相关的信息 Sid State intf external-vid inner-vid Peer LocalMAC RemoteMAC online time 20 STATE_SESSION virtual-access 5091 1 0 7.7.7.2 00:D0:F8:22:12:81 08:FB:0A:B0:48:AF 0 day(s) 15:16:31 PPPOE Server current sessions count : 1
PPPOE CLIENT	查看 PC 端是否拨号成功

常见错误

无

6.5.2 配置PPPoE SERVER远程认证

配置效果

- PPPoE CLIENT 通过 AAA 和 Radius 配合完成远程认证。

注意事项

- PPPoE SERVER 基本功能，除了本地地址池和 username 与 password，都需要配置。

配置方法

↘ 配置启用 aaa

- 必须配置。
- 开启 aaa 的全局开关。

↘ 配置对 ppp 用户启用 radius 认证

- 必须配置。

↘ 配置虚拟模板采用 ppp 用户认证方法列表

- 必须配置。

- 需要指明认证方式或者认证列表。
- 在 virtual-template 接口模式下配置。

配置 radius 认证参数

- 必须配置。
- 配置 radius 服务器的地址和共享口令。

检验方法

在客户端主机 PPPOE Client 拨号能够成功。

相关命令

配置启用 aaa

【命令格式】 **aaa new-model**
【参数说明】 **-**
【配置模式】 全局模式
【使用指导】 -

配置对 ppp 认证用户列表启用 radius 认证

【命令格式】 **aaa authentication ppp** *list-name* **group radius**
【参数说明】 *list-name*：PPP 认证用户列表。
【命令模式】 全局模式
【使用指导】 -

配置虚拟模板采用 PPP 用户认证方法列表

【命令格式】 **ppp authentication {chap | pap }** *list-name*
【参数说明】 **chap**：认证类型为 chap。
pap：认证类型为 pap
list-name：认证用户列表。
【命令模式】 virtual-template 模式
【使用指导】 -

配置 radius 安全服务器主机

【命令格式】 **radius-server host** *ipv4-address*
【参数说明】 *ipv4-address*：radius 服务器的 IP 地址
【命令模式】 全局模式
【使用指导】 为了使用 RADIUS 实现 AAA 安全服务，必须定义 RADIUS 安全服务器。您可以使用 radius-server host 命令定义一个或多个 RADIUS 安全服务器

定义与 RADIUS 安全服务器进行通信的共享口令

【命令格式】 **radius-server key** [0 | 7] *text-string*

【参数说明】 *text-string*：共享口令的文本

0 | 7：口令的加密类型，0 无加密，7 简单加密。

【命令模式】 全局模式

【使用指导】 共享口令是设备和 RADIUS 安全服务器进行正确通信的基础。为了使设备和 RADIUS 安全服务器能进行通信，必须在设备和 RADIUS 安全服务器上定义相同的共享口令。

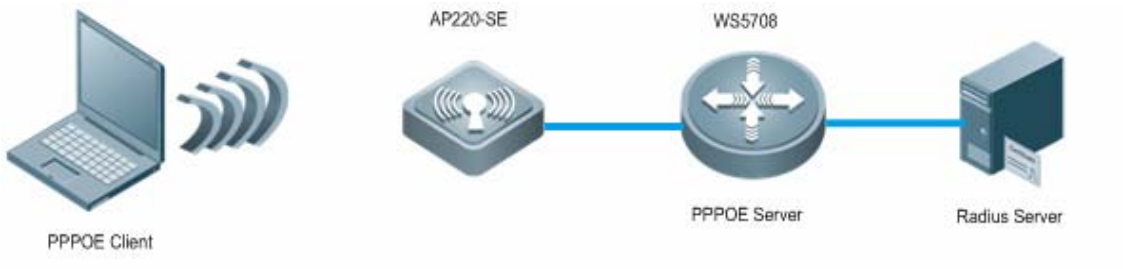
配置举例

以下配置举例，仅介绍 PPPoE SERVER 和 PPPoE CLIENT 的配置。

配置 PPPOE SERVER 远程认证。

【网络环境】

图 1-4



【配置方法】

- 配置 PPPoE SERVER 基本功能。
- 配置 AAA 和 radius。

PPPOE Server

```
#说明：以下配置不分先后顺序

#配置开启 aaa
Ruijie#conf
Ruijie(config)#aaa new-model
Ruijie(config)#exit
Ruijie#
#配置对 ppp 用户启用 radius 认证
Ruijie#conf
Ruijie(config)#aaa authentication ppp default group radius
Ruijie(config)#exit
Ruijie#

#配置 radius 服务器地址和共享口令
Ruijie#conf
Ruijie(config)#radius-server host 192.168.23.71
Ruijie(config)#radius-server key ruijie
```

```
Ruijie(config)#end
Ruijie#

#配置本地地址池
Ruijie#conf
Ruijie(config)#ip local pool pppoe 1.2.3.4 1.2.3.254
Ruijie(config)#end
Ruijie#

#配置 bba-group
Ruijie#conf
Ruijie(config)#bba-group pppoe pppoe1
Ruijie(config-bba-group)#virtual-template 2
Ruijie(config-bba-group)#exit
Ruijie(config)#end
Ruijie#

#配置 loopback 接口
Ruijie#conf
Ruijie(config)#int loopback 1
Ruijie(config-if-Loopback 1)#ip address 1.2.3.1 24
Ruijie(config-if-Loopback 1)#end
Ruijie#

#配置虚拟模板
Ruijie#conf
Ruijie(config)#int virtual-template 2
Ruijie(config-if-Virtual-Template 2)#ip unnumbered loopback 1
Ruijie(config-if-Virtual-Template 2)#ppp authentication pap chap
Ruijie(config-if-Virtual-Template 2)#peer default ip address pool pppoe
Ruijie(config-if-Virtual-Template 2)#end
Ruijie#

#配置 vlan 并在接口上使能 pppoe-server 功能
Ruijie#conf
Ruijie(config)#vlan 1
Ruijie(config-vlan)#exit
Ruijie(config)#int vlan 1
Ruijie(config-if-VLAN 1)#pppoe-server enable group pppoe1
Ruijie(config-if-VLAN 1)#end
Ruijie#
```

	Ruijie#
PPPOE Client	与配置本地认证一样，略
【检验方法】	● 在 PPPoE SERVER 端通过 show pppoe-server session 命令查看连接状态 ● 在 PPPoE CLIENT 端拨号能成功
PPPOE SERVER	Ruijie#show pppoe-server session #以下是 pppoe server 相关的信息 Sid State intf external-vid inner-vid Peer LocalMAC RemoteMAC online time 20 STATE_SESSION virtual-access 5091 1 0 7.7.7.2 00:D0:F8:22:12:81 08:FB:0A:B0:48:AF 0 day(s) 15:16:31 PPPOE Server current sessions count : 1
PPPOE CLIENT	查看 PC 端是否拨号成功

常见错误

- 暂无。

6.6 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
清除系统所有的 pppoe 隧道	**clear pppoe-server tunnel**
清除系统指定 session id 的 pppoe 隧道	**clear pppoe-server tunnel session-id** *id*

查看运行情况

作用	命令
查看当前系统中所有的 Session 信息以及转发面的信息 (注：目前 tunnel 和 session 显示的信息一样。)	**show pppoe-server { tunnel | session | ref }**

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 PPPOE session 报文的调试开关	**debug pppoe datas**
打开 PPPOE 异常信息的输出开关	**debug pppoe errors**
打开 PPPOE 协商的调试开关	**debug pppoe events**
打开 PPPOE 协商报文的调试开关	**debug pppoe packets**
打开 PPP LCP 和 IPCP 阶段的协商调试开关	**debug ppp negotiation**
打开 PPP 认证阶段的协商调试开关	**debug ppp authentication**
打开 PPP 整个协商阶段的错误信息的调试开关	**debug ppp error**

7 Aggregate Port

7.1 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，这条线路上承载的业务就会断掉，而如果将多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，那么在这些端口上承载的业务就不会断掉。

下文仅介绍 AP 的相关内容。

协议规范

- IEEE 802.3ad

7.2 典型应用

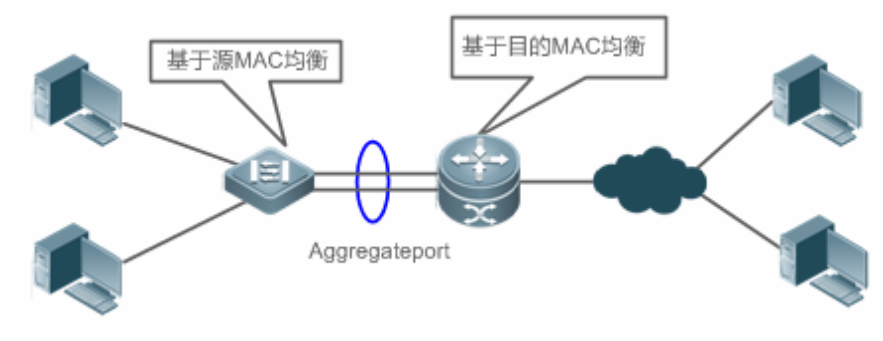
典型应用	场景描述
AP 链路聚合及流量平衡	汇聚和核心设备之间通常存在大量报文流，需要更大的端口带宽来支撑，这时候就可以把设备上多条物理链路聚合成一条逻辑链路，增大链路带宽，并通过配置适当的流量平衡算法，使聚合口上的报文尽可能平衡到每一条物理链路，以提高带宽利用率。

7.2.1 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 7-1 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
- 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

7.3 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。

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。

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。

7.3.1 链路聚合

工作原理

- 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。

7.3.2 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

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。

各种流量平衡模式都是利用流量算法、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。

不同产品，流量均衡支持度可能存在差异。

7.4 产品说明

NBR108G-P 不支持 LAN 口聚合功能 ;NBR800G、NBR950G、NBR1500G、NBR2000G、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 LAN 口聚合功能。

7.5 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。
配置 AP 的 LinkTrap 功能	可选配置。用于打开接口的 LinkTrap 通告功能。	
	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。

7.5.1 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。

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。

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)。

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在接口模式下执行 **no shutdown** 命令重新使能该接口。

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】

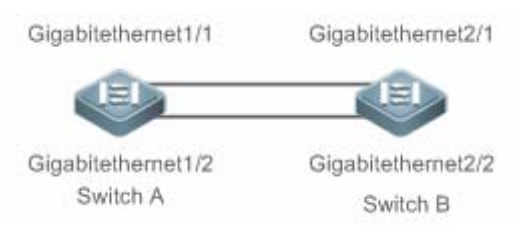
```
Ruijie# show aggregateport 1 summary

AggregatePort  MaxPorts        SwitchPort Mode    Load balance                Ports

-------------  --------------- ---------- ------  --------------------------

------------------------

Ag1            8               Enabled    ACCESS  dst-mac                     Gi0/2
```

配置举例

配置以太网静态 AP

【网络环境】

图 7-2



【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

-

7.5.2 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 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

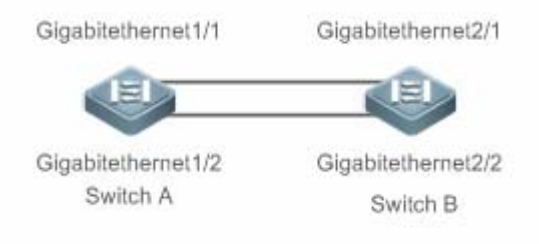
- 通过 **show running** 命令查看相应的配置。
- 打开 LinkTrap 通告的情况下，通过 MIB 软件可以监控到 AP 口或成员口的 LinkTrap 通告。

配置举例

配置 AP 的 LinkTrap 功能

【网络环境】

图 7-3



【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。
- 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 Aggregateport 3
SwitchA(config-if-AggregatePort 3)# no snmp 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 Aggregateport 3
SwitchB(config-if-AggregatePort 3)# no snmp 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

-

7.5.3 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。比如，源 IP 变化的 IPv4 报文要从 AP 口输出，那么 AP 会根据用户指定的 IPv4 报文字段 src-ip 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-dst-ip-l4port** | **src- l4port** | **dst-l4port** | **src-dst-l4port** | **src-ip-src-l4port** | **src-ip-dst-l4port** | **dst-ip-src-l4port** | **dst-ip-dst-l4port** | **src-ip-src-dst-l4port** | **dst-ip-src-dst-l4port** | **src-dst-ip-src-l4port** | **src-dst-ip-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-dst-ip-l4port：根据源 IP 与目的 IP 和 L4 源端口号与 L4 目的端口号进行流量分配。

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。

src-ip-src-l4port： 根据源 IP 与 L4 层源端口号进行流量分配。

src-ip-dst-l4port：根据源 IP 与 L4 层目的端口号进行流量分配。

dst-ip-src-l4port：根据目的 IP 与 L4 层源端口号进行流量分配。

dst-ip-dst-l4port：根据目的 IP 与 L4 层目的端口号进行流量分配。

src-ip-src-dst-l4port：根据源 IP、L4 层源端口号与 L4 层目的端口号进行流量分配。

dst-ip-src-dst-l4port：根据目的 IP、L4 层源端口号与 L4 层目的端口号进行流量分配。

src-dst-ip-src-l4port：根据源 IP、目的 IP 与 L4 层源端口号进行流量分配。

src-dst-ip-dst-l4port：根据源 IP、目的 IP 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)的流量均衡方式或为基于增强模式模板的流量均衡(如使用 CB 线卡的交换机设备)。

【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。

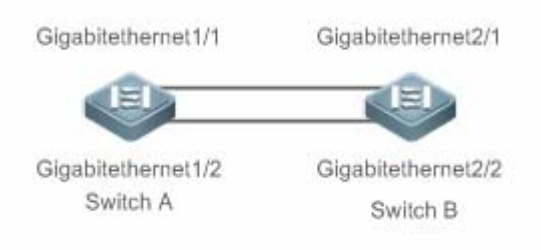
在支持基于 AP 口配置流量均衡的产品上，**aggregateport load-balance** 还支持在 AP 口接口模式下进行配置。

配置举例

配置流量平衡模式

【网络环境】

图 7-4



【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

-

7.6 监视与维护

清除各类信息

-

查看运行情况

作用	命令
显示增强模式模板的设置。	**show load-balance-profile** [*profile-name*]
显示 AP 口摘要信息或流量平衡算法。	**show aggregateport** [*ap-number*] { **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**

8 VLAN-TERMINAL

8.1 概述

vlan 终结就是实现单臂路由功能，即在酒店场景中，每个客户为一个 vlan，交换机配 trunk 口，在不配置子接口的情况下，可以使每个 vlan 的流量都由指定的某一个内网口进出。或者能将指定 VID 或 VID 段通过同一个 lan 口进出。

采用 vlan 终结功能可以给对网络管理带来方便且节省 IP 地址，且管理员便于维护网络，不需要配多个路由，以及减少因 IP 地址增加或变更带来的工作量，由于各个 vlan 的 IP 地址处于同一个网段。

8.2 典型应用

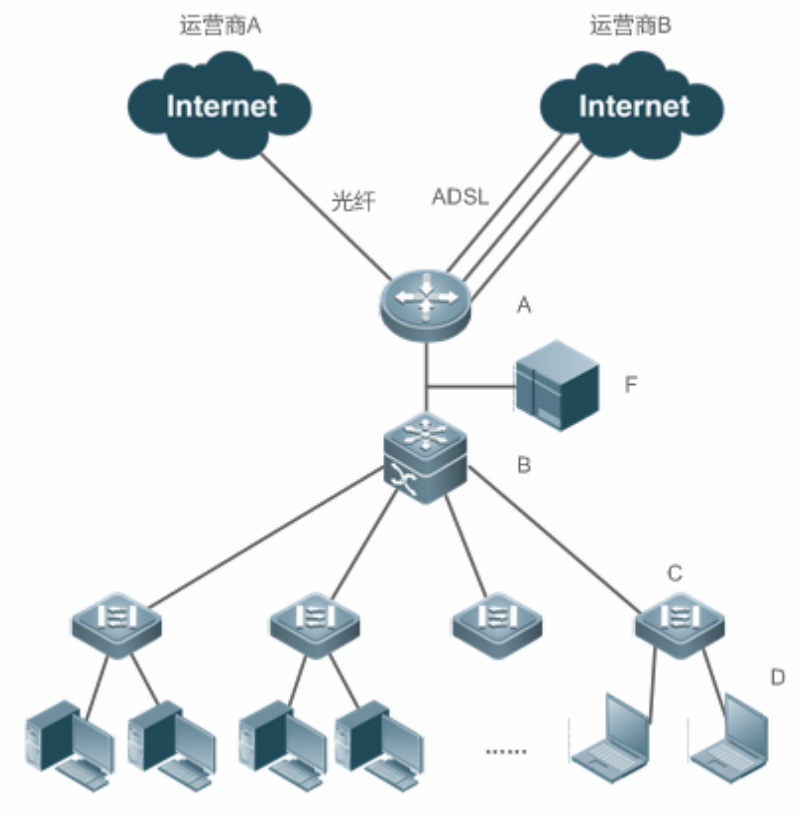
典型应用	场景描述
出口网关部署	出口网关设备部署 vlan 终结功能

8.2.1 出口网关部署

应用场景

酒店场景中出口网关设备只有一个内网口（物理口）与交换机相连，每个房间划分为一个 vlan，交换机没有 supervlan 功能且交换机的镜像口连着网监产品（对各个 vlan 进行监控）

图 8-1 出口网关酒店用户典型的应用场景



【注释】 A 为出口网关设备
B 为核心交换机
C 为交换机
D 为酒店房间的 PC
F 为网监产品

功能部属

- 基本 NAT 上网功能：完成基本的 NAT 地址转换，保障用户正常上网。
- 核心交机的出口配为 trunk 口
- 多链路负载均衡功能：完成数据流在多条链路的合理分配，确保多条链路的带宽利用合理。
- vlan 终结功能：完成带不同 tag 的报文从同一接口进行转发

8.3 功能详解

基本概念

VID

即 vlan id，其作用就是用于区分不同 vlan。

功能特性

功能特性	作用
vlan 终结	开启 vlan 终结。

8.3.1 vlan终结

vlan terminal 功能可以给对网络管理带来方便且节省 IP 地址，且管理员便于维护网络，不需要配多个路由，以及减少因 IP 地址增加或变更带来的工作量，由于各个 vlan 的 IP 地址处于同一个网段。

工作原理

VLAN-TERMINAL 对于其它功能模块来说，是透明的，即不会对其他模块的数据流处理产生影响。通过 CLI 的配置，使驱动能够从交换机上接收配置相应的 VID 报文，这些报文是带 tag 的报文。通过解析这些报文，并把报文中的 TAG 移除，并保存起来；由于报文中已没有 TAG，后续模块就把报文当作普通的报文处理；当要发送报文时，根据流信息，根据映射关系找到对应的 TAG 信息，并对报文进行填充，使报文能正常发送。

相关配置

↘ 开启 vlan 终结功能

缺省情况下，vlan 终结功能是关闭的。

在全局配置模式中，使用 **vlan-terminal enable** 命令可以开启 vlan 终结功能开关。

在全局配置模式中，使用 **no vlan-terminal enable** 命令可以关闭 vlan 终结功能开关。

↘ 配置属于同一个 vlan 的最多上线数

缺省情况下，VID 的上线数为 100 个

使用 vlan-terminal per-vlan *num* 可以调整最多上线数，取值范围为 1~1000 个

要删除相关配置，可以在全局配置模式下执行 no vlan-terminal per-vlan 命令来执行

↘ 配置接口所对应的 VID

可以配置哪些 VID 从哪个接口进出，只支持 lan 口

在接口配置模式下使用 vlan-terminal vlan-list *vlan-list*

删除相关配置使用 no vlan-terminal vlan-list

8.4 产品说明

NBR108G-P、NBR800G、NBR950G、NBR1000G-E、NBR6120-E、NBR2000G-C、NBR3000G-S、NBR1000G-C 不支持 supervlan 终结；NBR1500G、NBR2000G、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 supervlan 终结。

8.5 配置详解

配置项	配置建议 & 相关命令	
开启 vlan 终结功能	必须配置。	
	vlan-terminal enable	开启 vlan 终结功能
配置属于同一个 vlan 的最多上线数	可选配置。	
	vlan-terminal per-vlan *num*	配置属于同一个 VID 的最多上线数,其中配置的范围为 1~1000。
配置接口所对应的 VID	必须配置。	
	vlan-terminal vlan-list *vlan-list*	配置哪些 VID 从哪个接口进出。其中 VID 可能是单个 ,也可以是连续的 ,中间有逗号隔开，其中接口只支持 lan 口。

8.5.1 开启关闭vlan终结功能

配置效果

- 打开 vlan 终结功能，能够完成带不同 tag 的报文从同一接口进行转发。

注意事项

- vlan 终结功能关闭的情况下，功能失效

配置方法

- 全局模式下，通过命令开启 vlan 终结功能。

检验方法

- 检查 vlan 终结功能状态。

相关命令

开启 vlan 终结功能

【命令格式】 **vlan-terminal enable**
【参数说明】 -
【命令模式】 全局模式
【使用指导】 -

配置举例

开启 vlan 终结功能

【配置方法】 在出口网关的设备上（设备 A）

```
Ruijie# configure terminal
Ruijie(config)#vlan-terminal enable
```

【检验方法】
- 查看 vlan 终结功能状态

```
Ruijie#show vlan-terminal
vlan-terminal: enable
```

常见错误

无

8.5.2 配置属于同一个vlan的最多上线数

配置效果

- 属于同一个 VID 的最多上线数，超过这个数，同一个 VID 的就不能新上线。

注意事项

- 是可选的配置
- 缺省情况下，VID 的上线数为 100 个， 可配的范围为 1~1000

配置方法

- 全局模式下，通过命令配置属于同一个 vlan 的最多上线数。

检验方法

- 检查 vlan 的最多上线数。

相关命令

配置属于同一个 vlan 的最多上线数

【命令格式】 **vlan-terminal per-vlan** *num*

【参数说明】 num: 属于同一个 VID 的最多上线数，超过这个数，同一个 VID 的就不能新上线，范围为 1~1000

【命令模式】 全局模式

【使用指导】 -

配置举例

配置 VID 的上线数为 30

【配置方法】 在出口网关的设备上（设备 A）

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# vlan-terminal per-vlan 30
```

【检验方法】

- 查看配置的信息

```
Ruijie#show vlan-terminal
vlan-terminal:  enable
per-vlan:  30
```

常见错误

无

8.5.3 配置接口所对应的VID

配置效果

- 指定哪些 VID 通过哪个接口进行转发

注意事项

- 配置的 VID 与子接口冲突时，以子接口为准

配置方法

- 在接口模式下，通过命令配置接口所对应的 VID。

检验方法

- 检查其配置信息。

相关命令

↘ 配置接口所对应的 VID

【命令格式】 **vlan-terminal vlan-list** *vlan-list*

【参数说明】 *vlan-list*：可以是单个 VID，也可以是连续的 VID，中间有逗号隔开

【命令模式】 接口配置模式

【使用指导】 -

配置举例

↘ 配置从接口 0/1 进出的 VID 为 2，5， 40~80， 100~120

【配置方法】 在出口网关的设备上（设备 A）

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# vlan-terminal vlan-list 2，5，40-80，100-200
```

【检验方法】

- 查看配置的信息

```
Ruijie#show vlan-terminal
vlan-terminal:  enable
per-vlan:        30
Gi0/1:           2,5,40-80,100-200
```

常见错误

- 接口属性错误（只支持 LAN 口）。
- 格式错误。
- VID 冲突。

8.6 监视与维护

清除各类信息

无

查看运行情况

作用	命令
显示 VID 的上线数及对应 VID 的上线 IP。	**show vid-info**
显示 vlan-terminal 的配置信息。	**show vlan-terminal**

查看调试信息

无

配置指南-IP 地址和服务

本分册介绍 IP 地址和服务相关内容，包括以下章节：

1. IP 地址与服务
2. ARP
3. IP Event Dampening
4. TCP
5. 软件 IPv4 快转
6. TUNNEL
7. FPM
8. NAT
9. MLLB
10. WAN-IP

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。

以下仅针对 IPv4 地址进行介绍。

协议规范

- RFC 1918：AddressAllocationforPrivateInternets
- RFC 1166：Internet Numbers

1.2 典型应用

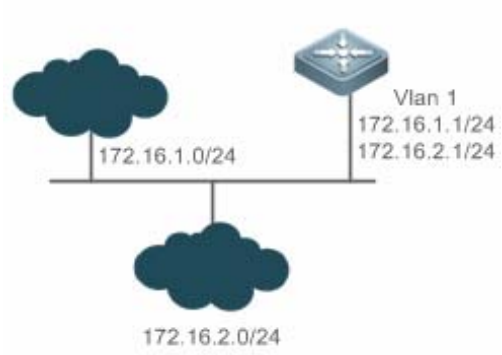
典型应用	场景描述
配置 IP 地址通信	两个网络使用同一个交换机接口进行通信

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

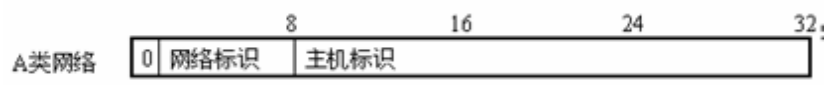
IP 地址

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。

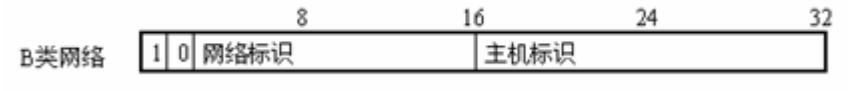
A 类地址，最高比特位为“0”，有 7 个比特位表示网络号，24 个比特位表示本地地址。这样总共有 128 个 A 类网络。

图 1-2



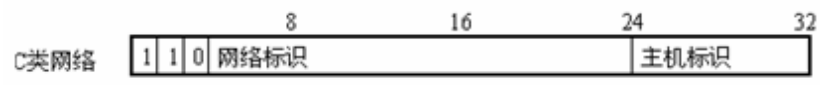
B 类地址，前两个最高比特位为“10”，有 14 个比特位表示网络号，16 个比特位表示本地地址。这样总共有 16,348 个 B 类网络。

图 1-3



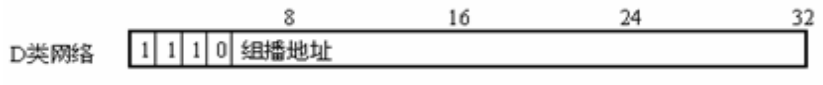
C 类地址，前三个最高比特位为“110”，有 21 个比特位表示网络号，8 个比特位表示本地地址。这样总共有 2,097,152 个 C 类网络。

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



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 MTU	用于配置接口 IP 报文的最大传输单元。
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。
IP 地址池	用于 ppp 协商为对端分配 ip 地址

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。

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 地址或者 SLAVE 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，所以就需要配置多个 IP 地址。
- 许多旧的网络是基于第二层的桥接网络，没有进行子网的划分。次 IP 地址的使用可以使该网络很容易升级到基于 IP 层的路由网络。对于每个子网，设备都配置一个 IP 地址。
- 一个网络的两个子网被另外一个网络隔离开，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。
- SLAVE IP 用在网关集群的场景中，只有配置了主 ip 地址后才允许配置 slave ip。Slave ip 和主 ip 地址都是基于三层口配置的，它们互为备份地址。正常情况下，MASTER 角色的设备使用主 ip 生效，SLAVE 角色的设备使用 slave ip 生效。当 SLAVE 角色设备切换成 MASTER 角色时，其接口实际生效的 IP 将从 Slave ip 更新为主 ip。而当 MASTER 角色设备切换为 SLAVE 角色时，其接口原来实际生效的 IP 将从主 IP 更新为 slave ip。

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 Slave 地址之前，需要确定已经配置了主 IP 地址。Slave IP 和主 IP 在网关集群的场景中互为备份地址。在 MASTER 设备上主地址生效，在 SLAVE 设备上是 Slave 地址生效。且任何时刻，只能有一个地址在接口上生效。

Slave IP 和主 IP 互为备份地址（且总有一个地址不在接口上生效），在部署 dhcp 等应用时，建议将 slave IP 考虑在内，比如不将该 slave IP 分配出去，否则可能导致地址冲突。

同时配置管理 IP 与网关

本命令只在二层设备上支持。

锐捷的二层交换机产品可以配置管理 IP 和网关。用户可以通过 telnet 远程管理二层交换机，并且需要修改二层交换机的管理 IP 与缺省网关。

配置通过 PPP 协商获取 IP 地址

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。

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。

被借用接口的 IP 地址不能是借用其它接口的 IP 地址。

如果被借用接口有多个 IP 地址，只有主 IP 地址被借用。

一个接口的 IP 地址可以借给多个接口。

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。
- 通过 **ip address** *ip-address mask***slave** 可以配置 SLAVE IP 地址。

↘ 配置通过 PPP 协商获取 IP 地址

- 缺省情况接口没有配置通过 PPP 协商获取 ip 地址。
- 通过 **ip address negotiate** 命令配置为点对点接口协商 IP 地址。

↘ 配置接口借用 IP 地址

- 缺省情况接口没有配置 IP 地址。
- 通过 **ip unnumbered** 命令可以向其他接口借用 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 发送ICMP报文

工作原理

ICMP 协议不可达消息

当设备接收到目标为自己的非广播报文，但是该数据包中采用了设备不能处理的 IP 协议，设备就向源地址发送 ICMP 协议不可达消息。另外，如果设备由于不知道路由而不能转发数据包时，也会发送 ICMP 主机不可达消息。

ICMP 重定向消息

路由有时会不够优化，使得设备从一个接口接收到的数据包，还要从该接口发送出去。如果设备将数据包从接收接口重新发送出去，设备就会给数据源发送一个 ICMP 重定向消息，告诉数据源到该目标地址的网关为同一子网上的另外一台设备。这样数据源就会将后续的数据包按照最佳的路径进行发送。

ICMP 掩码应答消息

网络设备有时需要知道互联网上某个子网的子网掩码，为了获取该信息，网络设备可以发送 ICMP 掩码请求消息，接收到 ICMP 掩码请求消息的网络设备就会发送掩码应答消息。

相关配置

启用 ICMP 协议不可达消息

- 缺省情况接口启用 ICMP 协议不可达消息功能。
- 可通过[**no**] **ip unreachables** 命令关闭或启用该功能。

启用 ICMP 重定向消息

- 缺省情况接口启用 ICMP 协议重定向消息功能。
- 可通过[**no**]**ip redirects** 命令关闭或启用该功能。

↘ 启用 ICMP 掩码应答消息

- 缺省情况接口启用 ICMP 掩码应答消息功能。
- 可通过**[no]ip mask-reply** 命令关闭或启用该功能。

1.3.4 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。

1.3.5 IP MTU

工作原理

如果一个 IP 报文超过 IP MTU 的大小 ,RGOS 软件就会对报文进行拆分。所有在同一物理网段上的设备 ,其互联接口的 IP MTU 一定要一致。锐捷产品允许调整接口的链路 MTU 值 ,而且接口的链路 MTU 的变化会引起接口的 IP MTU 的变化 ,接口的 IP MTU 会自动与接口的链路 MTU 保持一致。但是反之不行，如果调整了接口的 IP MTU 值，接口的链路 MTU 不会跟着改变。

相关配置

↘ 设置 IP MTU

- 缺省情况接口 IP MTU 为 1500。
- 可通过 **ip mtu** 设置 IP 包最大传输单元(MTU)。

1.3.6 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。

1.3.7 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。

1.3.8 IP地址池

工作原理

点对点接口可以通过 PPP 协商为对端分配 IP 地址。在 PPP 协商过程中，服务器会校验客户端的认证信息，如果校验通过，服务器就会为客户端分配 IP（如果客户端配置了 IP，且符合服务器的要求，服务器会同意这个 IP 为客户端的 IP），配置可以直接指定对端 IP 地址也可以从地址池获取空闲地址进行分配。

相关配置

使能地址池功能

- 缺省情况已使能地址池功能。
- 可通过 **ip address-pool local** 开启或关闭该功能。

创建地址池

- 缺省情况未配置 IP 地址池。
- 可通过 **ip local pool** 命令创建删除地址池。

配置为 PPP 协商分配 IP 地址给对端

- 缺省情况接口不为对端分配 IP 地址。
- 可通过 **peer default ip address** 命令为对端分配 ip 地址。

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
	ip address negotiate	配置通过 PPP 协商获取 ip 地址
	ip unnumbered	配置接口借用 IP 地址
	ap-interface bvi *num* **ip address**	配置指定 AP 上 BVI 口的 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
配置发送 ICMP 报文	可选配置。用于控制 ICMP 协议报文的收发。	
	ip unreachables	启用 ICMP 协议不可达和主机不可达消息
	ip redirects	启用 ICMP 重定向消息
	ip mask-reply	启用掩码应答消息
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 MTU	⚠ 可选配置。用于配置接口 IP 报文的最大传输单元。	
	ip mtu	设置 MTU 值
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。

↘ 配置通过 PPP 协商获取接口 IP 地址

- 可选配置。
- 如果点对点接口上没有配置 IP 地址，且需要通过 PPP 协商获取 IP 地址时配置。
- 在三层接口模式下配置。

↘ 配置接口借用 IP 地址

- 可选配置。
- 如果接口上没有配置 IP 地址，且需要向其它接口借用 IP 地址时配置。
- 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**] | [**slave**]

【参数说明】 *ip-address*：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。

slave：表示配置的 SLAVE IP 地址。

【命令模式】 接口模式

【使用指导】 -

配置通过 PPP 协商获取接口 IP 地址

【命令格式】 **ip address negotiate**

【参数说明】 -

【命令模式】 接口模式

【使用指导】 只有点对点接口才支持通过 PPP 协商获取 IP 地址，在接口上配置了 **ip address negotiate** 后，对端需要配置 **peer default ip address**。

配置接口借用 IP 地址

【命令格式】 **ip unnumbered***interface-type interface-number*

【参数说明】 *interface-type*：关联接口类型。

interface-number：关联接口编号。

【命令模式】 接口模式

【使用指导】 无编号接口就是只在接口启动 IP 协议，但是不分配 IP 地址，无编号接口需要关联一个具有 IP 地址的接口。无编号接口产生的 IP 数据包，该数据包的源 IP 地址为关联接口的 IP 地址。另外路由协议进程也根据关联接口的 IP 地址，决定是否往无编号接口发送路由更新报文。应用无编号接口，需要注意以下限制：

以太网接口不能配置成无编号接口。

当串行口封装 SLIP、HDLC、PPP、LAPB、Frame-relay 时，可以配置成无编号接口。但是封装帧中继时，只有点到点子接口才允许配置无编号接口。X.25 封装是不允许配置无编号接口的。

不能用 ping 命令来检测无编号接口是否工作正常，因为无编号接口没有 IP 地址。但是通过 SNMP 可以远程监测到无编号接口状态。

不能通过无编号接口进行网络启动。

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)
```

给接口配置 SLAVE IP 地址

【配置方法】 在接口 GigabitEthernet 0/0 配置主 ip 地址 192.168.23.110 255.255.255.0，slave ip 为 192.168.24.110 255.255.255.0

```
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
Ruijie(config-if-GigabitEthernet 0/0)#ip address 192.168.24.110 255.255.255.0 slave
```

【检验方法】 使用 **show running-config interface** 可以看到接口 GigabitEthernet 0/0 添加地址成功

```
Ruijie# show running-config interface gigabitEthernet 0/0
interface GigabitEthernet 0/0
 ip address 192.168.23.110 255.255.255.0
 ip address 192.168.24.110 255.255.255.0 slave
```

给点对点接口配置通过 PPP 协商获取 IP 地址

【配置方法】 在接口点对点接口上配置通过协商获取 ip 地址

```
Ruijie(config)#int virtual-ppp 1
Ruijie(config-if-Virtual-ppp 1)#ip address negotiate
```

【检验方法】 使用 **show run** 可以看到点对点接口相关配置

```
Ruijie#show run interface virtual-ppp 1

Building configuration...
Current configuration: 48 bytes

interface Virtual-ppp 1
 ip address negotiate
```

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 配置发送ICMP报文

配置效果

启用接口 ICMP 协议不可达消息，ICMP 重定向消息以及掩码应答消息。

注意事项

-

配置方法

↘ 启用 ICMP 协议不可达消息

- 缺省开启 ICMP 协议不可达消息。
- 可选配置，通过 **no ip unreachables** 禁止该功能。
- 在三层接口模式下配置。

↘ 启用 ICMP 重定向消息

- 缺省开启 ICMP 重定向消息。
- 可选配置，通过 **no ip redirects** 禁止该功能。
- 在三层接口模式下配置。

↘ 启用 ICMP 掩码应答消息

- 缺省开启 ICMP 掩码应答消息。
- 可选配置，通过 **no ip mask-reply** 禁止该功能。
- 在三层接口模式下配置。

检验方法

通过 **show ip interface** 可以看到配置生效。

相关命令

启用 ICMP 协议不可达消息

【命令格式】 **ip unreachables**
【参数说明】 -
【命令模式】 接口模式
【使用指导】 -

启用 ICMP 重定向消息

【命令格式】 **ip redirects**
【参数说明】 -
【命令模式】 接口模式
【使用指导】 -

启用 ICMP 掩码应答消息

【命令格式】 **ip mask-reply**
【参数说明】 -
【命令模式】 接口模式
【使用指导】 -

配置举例

【配置方法】 在设备端口 gigabitEthernet 0/1 启用 ICMP 协议不可达消息 ,ICMP 重定向消息以及 ICMP 掩码应答消息功能。

```
Ruijie#configure terminal
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# no switchport
Ruijie(config-if-GigabitEthernet 0/1)# ip unreachables
Ruijie(config-if-GigabitEthernet 0/1)# ip redirects
Ruijie(config-if-GigabitEthernet 0/1)# ip mask-reply
```

【检验方法】 使用 **show ip interface** 可以看到接口 GigabitEthernet 0/1 配置成功

```
Ruijie#show ip interface gigabitEthernet 0/1
GigabitEthernet 0/1
  ICMP mask reply is: ON
  Send ICMP redirect is: ON
  Send ICMP unreachabled is: ON
```

1.4.4 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
```

1.4.5 配置IP MTU

配置效果

调整 IP 包最大传输单元。

注意事项

-

配置方法

- 可选配置，所有在同一物理网段上的设备，当互联接口的 IP MTU 不一致时需要配置为一致。
- 在三层接口模式下配置。

检验方法

通过 **show ip interface** 可以看到配置生效

相关命令

↘ 配置 IP MTU

【命令格式】 **ip mtu***bytes*

【参数说明】 *bytes*：IP 包最大传输单元，以字节为单位，范围 68~1500。

【命令模式】 接口模式

【使用指导】 -

配置举例

【配置方法】 将 gigabitEthernet 0/1 接口的 IP MTU 值设为 512 字节

```
Ruijie#configure terminal
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# no switchport
Ruijie(config-if-GigabitEthernet 0/1)#ip mtu 512
```

【检验方法】 使用 **show ip interface** 可以看到接口 GigabitEthernet 0/1 配置成功

```
Ruijie# show ip interface gigabitEthernet 0/1
IP interface MTU is: 512
```

1.4.6 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
```

1.4.7 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
```

1.4.8 配置IP地址池

配置效果

PPP 协议为客户端分配 IP 地址。

注意事项

-

配置方法

↘ 使能 IP 地址池功能

- 可选配置。

- 在全局配置模式下配置。

创建 IP 地址池

- 可选配置。
- 在使能 IP 地址池功能后才能配置，关闭 IP 地址池功能后会自动删除已创建的地址池。
- 在全局模式下配置。

配置 PPP 协商分配 IP 地址给对端

- 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

配置使能 IP 地址池

【命令格式】 **ip address-pool local**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 缺省情况下，IP 地址池功能开启，用户可以配置 IP 地址池，PPP 用户可以用 IP 地址池分配对端的 IP 地址。如果想关闭 IP 地址池功能，可以使用 no ip address-pool local 命令，此时会删除所有之前配置的 IP 地址池。

配置创建 IP 地址池

【命令格式】 **ip local pool** *pool-namelow-ip-address*[*high-ip-address*]

【参数说明】 *pool-name*：指定本地 IP 地址池的名字，**default** 为默认地址池名字。

low-ip-address：IP 地址池中最小的 IP 地址。

high-ip-address：可选，IP 地址池中最大的 IP 地址。如果未指定最大的 IP 地址，则 IP 地址池中只有一个地址，即是 *low-ip-address*

【命令模式】 全局配置模式

【使用指导】 可以用该命令创建一个或多个 IP 地址池，供 PPP 分配 IP 地址给连接的用户。

配置 PPP 协商分配 IP 地址给对端

【命令格式】 **peer default ip address** {*ip-address* | **pool** [*pool-name*] }

【参数说明】 *ip-address*：指定为对端分配的 IP 地址。

pool-name：可选，指定分配 IP 地址的地址池名字，若未配置该参数，则在 default 地址池中分配 IP 地址。

【命令模式】 接口模式

【使用指导】 当对端接口还未配置 IP 地址而本端设备已经有 IP 地址时，可配置本端设备为对端接口分配 IP 地址。这时，需要在对端设备上配置 **ip address negotiate** 命令，在本端设备上配置 **peer default ip address** 命令，使对

端接口接受由 PPP 协商分配的 IP 地址。

该命令仅支持封装 PPP 或 SLIP 协议的点对点接口下配置。

peer default ip address pool 命令 ,是从 IP 地址池里分配出一个 IP 地址给对端 ,这个 IP 地址池是通过 ip local pool 命令配置的地址池。

peer default ip address*ip-address* 命令，直接给对端指定一个 IP 地址，该命令不能在虚拟模板接口及异步口上配置。

配置举例

【配置方法】

- 配置接口 dialer1 从地址池 quark 为对端分配分配 IP 地址

```
Ruijie#configure terminal
Ruijie(config)# ip address-pool local
Ruijie(config)# ip local pool quark 172.16.23.2 172.16.23.255
Ruijie(config)# interface dialer 1
Ruijie(config-if-dialer 1)#peer default ip address pool quark
```

【检验方法】 通过 **show run-config** 可以看到配置生效

```
Ruijie#show running-config
ip local pool quark 172.16.23.2 172.16.23.255
!
interface dialer 1
 peer default ip address pool quark
```

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** [*interface-typeinterface-number* | **brief**]
显示 IP 报文统计值	**show ip packet statistics** [**total |** *interface-name*]
显示协议栈 IP 报文收发统计信息	**show ip packet queue**
显示地址池统计情况	**show ip pool** [*pool-name*]

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）；2）代理地址解析协议（Proxy ARP）。关于 ARP 、Proxy 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	在同一网段中，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。

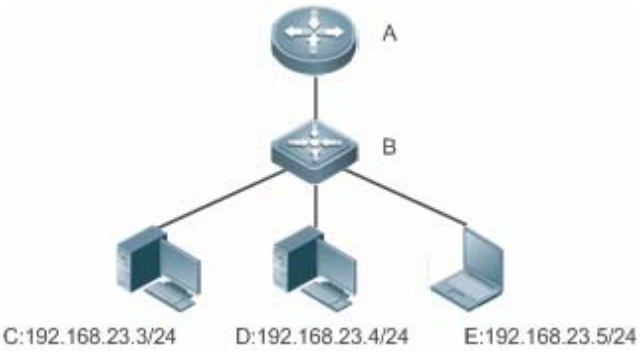
2.2.1 在局域网内提供地址解析协议服务

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。

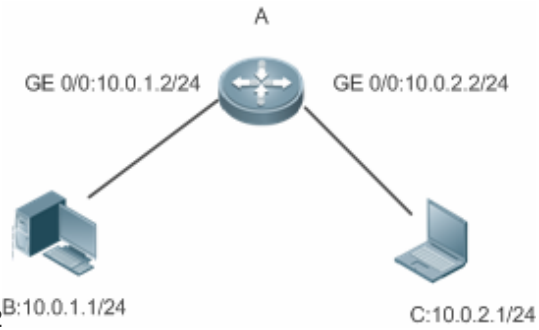


图 2-2

【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。
可信任 ARP	防止 ARP 欺骗。
免费 ARP	检测 IP 地址冲突，以及让外围设备更新本机的 ARP。
代理 ARP	代理应答请求其他设备的 ARP 请求。
any IP ARP	方便用户在不更改 IP 和网关的情况下可以上网。
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。
关闭动态 ARP 学习	关闭动态 ARP 学习功能后，接口不再进行动态 ARP 的学习。
ARP 扫描	根据用户要求，对局域网的邻居进行扫描。

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、未解析 ARP 表项数上限、接口 ARP 学习数量限制、单板 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。

未解析 ARP 表项的数量限制

在局域网中可能存在对网关的攻击，扫描网段，使网关生成大量未解析的 ARP 表项，从而使网关无法正常学习主机的 MAC 地址。为了防止这种攻击，用户可以配置未解析 ARP 表项的数量限制。

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。

单板 ARP 学习数量限制

通过配置指定槽数的 ARP 学习数量，可以限制不同槽数的 ARP 能力，灵活控制 ARP 表项的按槽分配和按需分配。

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。

未解析 ARP 表项的数量限制

在全局模式下，使用命令 **arp unresolve** *number* 配置 ARP 的未解析表项数。默认为 arp 容量的最大值，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。

↘ 单板 ARP 学习数量限制

在全局模式下 ,使用命令 **arp dynamic-entry-limit***slot-id subslot-id limit* 指定单板 ARP 学习的数量限制。默认不限制单板 ARP 学习的数量，用户可以根据实际情况重新调整。

2.3.3 可信任ARP

工作原理

可信任 ARP 作为一类特殊 ARP，添加在交换机端的 ARP 表中，用于防止 ARP 欺骗。可信任 ARP 同时具有静态 ARP 和动态 ARP 两者的特征，其优先级高于动态 ARP 表项、并且低于静态 ARP 表项。可信任 ARP 具有类似于动态 ARP 的老化机制，在 ARP 老化时主动发送 ARP 请求报文探测主机是否存在，如果主机有应答则代表主机还是活动的，那么就更新 ARP 的老化时间，否则删除 ARP 表项。可信任 ARP 具有静态 ARP 的相关特征，即不会通过学习 ARP 报文动态更新 ARP 表项的 MAC、接口等相关字段。

可信任 ARP 是 GSN 客户端用户认证上线时，认证服务端通过接入交换机获取用户真实的 IP-MAC 关联信息，并根据用户的网关信息，在网关交换机上添加的。该过程对于网络管理员来说是透明的，不会对网络管理员的原有网络管理产生任何影响。

综上所述，因为可信任 ARP 来源真实有效，且不会被 ARP 报文动态更新，所以可以有效的防止针对网关的 ARP 欺骗。

相关配置

↘ 配置可信任 ARP 功能

- 全局模式下，使用命令 **service trustedarp** 打开可信任 arp 功能，缺省情况下该功能是关闭的。
- 全局模式下，使用命令 **arp trusted user-vlan***vid1***translated-vlan***vid2* 实现 VLAN 转换，缺省情况下没有任何 VLAN 转换。如果服务器下发的 VLAN 和可信任 ARP 表项生效的 VLAN 不同，则用户需要配置 VLAN 转换。
- 全局模式下，使用命令 **arp trusted aging** 允许可信任 ARP 老化。缺省情况下可信任 ARP 表项不允许老化。
- 全局模式下，使用命令 **arp trusted number** 设置可信任 ARP 表项的容量。缺省情况下为总容量的一半，用户可以根据实际情况更改容量。

2.3.4 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。

2.3.5 代理ARP

工作原理

设备的代理 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。比如设备接收到一个 ARP 请求，ARP 请求的发送者 IP 地址与目标 IP 地址不属于同一网段，而设备又知道所请求 IP 地址的路由，设备就会发送 ARP 响应，响应的 MAC 地址为设备自身的以太网 MAC 地址，这个过程就是代理 ARP 的功能。

相关配置

↘ 配置代理 ARP

- 接口模式下，使用命令 **ip proxy-arp** 开启代理 ARP 功能。
- 缺省情况下路由器上开启了代理 ARP 功能，而交换机上关闭了代理 ARP 功能。

2.3.6 any IP ARP

工作原理

any IP ARP 的意思是使用任意 IP 地址都可以上网，用来满足这一类需求：用户在酒店使用自己的笔记本电脑，希望不修改 IP 地址和网关配置就可以上网。当网关收到主机发来的 ARP 请求时，虽然 ARP 请求的发送者 IP 地址和自己不属于同一个子网，目标 IP 地址可能不是自己，但是网关仍然发送 ARP 应答，并且为主机的 IP 地址生成直连路由。

相关配置

↘ 配置 any IP ARP

接口模式下，使用命令 **arp any-ip** 开启 any IP ARP 功能。缺省情况下接口没有开启该功能。

2.3.7 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。

2.3.8 关闭动态ARP学习

工作原理

配置关闭动态 ARP 学习后，接口上禁止学习动态 ARP。

相关配置

↘ 配置关闭动态 ARP 学习

- 缺省情况下接口使能动态 arp 的学习。
- 在接口模式下，使用命令 **noarp-learning enable** 命令关闭动态 ARP 学习功能。

2.3.9 ARP扫描

工作原理

启用 ARP 扫描功能后，设备会对局域网的邻居进行扫描，学习邻居的 ARP 表项。可以根据用户的需求，对接口下主 IP 地址和从 IP 地址的网段内的邻居进行扫描，或者只扫描用户所指定的地址范围。扫描时间点：在配置时执行一次，执行条件是接口三层 UP（即链路 UP 且配置了 IP 地址）。扫描配置一次，生效一次，不支持配置保存和下次生效。

相关配置

↘ 配置 ARP 扫描

接口模式下，使用命令 **arp scan** [*start-ip-address end-ip-address*]命令开启 ARP 扫描功能，缺省情况下没有开启该功能。

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、未解析 ARP 表项数上限、接口 ARP 学习数量限制、单板 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 unresolve	配置未解析 ARP 表项的数量限制
	arp cache interface-limit	配置接口 ARP 学习数量限制
	arp dynamic-entry-limit	配置单板 ARP 学习数量限制
配置可信任 ARP	⚠ 可选配置，用于防止 ARP 欺骗。	
	service trustedarp	启用可信任 ARP 功能
	arp trusteduser-vlan	添加可信任 ARP 时进行 VLAN 转换
	arp trusted aging	允许可信任 ARP 老化
	arp trusted	调整可信任 ARP 的容量
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
配置代理 ARP	⚠ 可选配置，用于代理应答请求不同子网内其他设备的 ARP 请求。	
	ip proxy-arp	开启代理 ARP 功能。
配置本地代理 ARP	⚠ 可选配置，用于代理应答请求子网内其他设备的 ARP 请求。	
	local-proxy-arp	开启本地代理 ARP 功能。
配置 any IP ARP	⚠ 可选配置，用于用户在不更改 IP 和网关的情况下可以上网。	
	arp any-ip	开启 any IP ARP 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
配置关闭动态 ARP 学习	⚠ 可选配置，用于禁止接口上的动态 ARP 学习。	
	no arp-learning enable	关闭接口的动态 ARP 学习功能
配置 ARP 扫描	⚠ 可选配置，用于启用接口上的 ARP 邻居扫描。	
	arp scan	开启接口上的 ARP 扫描功能

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】 网络拓扑如 图 2-1 所示

【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、未解析 ARP 表项数上限、接口 ARP 学习数量限制、单板 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

未解析 ARP 表项的数量限制

- 可选配置
- 在网络带宽资源不足时，可以将未解析 ARP 表项的数量配小，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

单板 ARP 学习数量限制

- 可选配置
- 在全局模式下配置

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、未解析 ARP 表项是数量限制、接口 ARP 学习数量限制、单板 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。

未解析 ARP 表项的数量限制

【命令格式】 **arp unresolve** *number*

【参数说明】 *number*：未解析 ARP 表项的最大个数，取值范围为< 1-8192>。默认值为 8192。

【配置模式】 全局模式

【使用指导】 当发现 ARP 缓存表中出现大量未解析表项，并且一段时间后还没有消失时，可以用此命令限制未解析表项的个数。

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。

单板 ARP 学习数量限制

【命令格式】 **arp dynamic-entry-limit***slot-id subslot-id limit*

【参数说明】 *slot-id*：分布式设备第一级槽位数；路由器目前最多支持 16 个，取值范围为 1-16。

subslot-id：分布式路由器第二级槽位数；路由器目前最多支持 4 个，取值范围为 0-3。

limit：指定槽数的 ARP 学习数量限制值，取值为<1 –设备支持的最大容量值>。

【配置模式】 全局模式

【使用指导】 限制单板的 ARP 学习数量，分布式设备上支持。

配置举例

【网络环境】 网络拓扑如 图 2-1 所示

【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
- 配置未解析 ARP 表项数量限制为 4096
- 配置 slot 1 subslot 2 的 ARP 学习数量限制为 1000

```
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
Ruijie(config)#arp unresolve 4096
Ruijie(config)#arp dynamic-entry-limit 1 2 1000
```

【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、未解析 ARP 表项是数量限制、接口 ARP 学习数量限制、单板 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 unresolve 4096
arp retry times 4
arp retry interval 3
arp dynamic-entry-limit 1 2 1000
!
interface GigabitEthernet 0/1
 arp cache interface-limit 300
```

常见配置错误

无

2.4.3 配置可信任ARP

配置效果

可以有效的防止针对网关的 ARP 欺骗。

注意事项

可信任 ARP 只在交换机上支持。

配置方法

- 如果需要部署 GSN 方案，则应该执行此配置项。
- 部署 GSN 全局安全网络解决方案时，需要配置开启可信任 ARP 功能。
- 在全局模式下配置

检验方法

使用 **show arp trusted** 命令查看可信 ARP 表项；

使用 **show running** 命令查看可信任 ARP 的相关配置是否生效。

相关命令

↘ 启用可信任 ARP 功能

【命令格式】 **servicetrustedarp**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 设备的可信任 ARP 功能是一种防止 ARP 欺骗的功能，作为 GSN 方案的一部分，需要和 GSN 方案一起使用。

↘ 添加可信任 ARP 时进行 VLAN 转换

【命令格式】 **arp trusteduser-vlan***vid1***translated-vlan***vid2*

【参数说明】 *vid1*：服务器设置的 VID

vid2：转换后的 VID

【配置模式】 全局模式

【使用指导】 要使此命令生效，首先启用可信任 ARP 功能。只有在服务器下发的 VLAN 和可信任 ARP 生效的 VLAN 不同时，才需要配置此命令。

↘ 查看交换机上的可信任 ARP

【命令格式】 **show arp trusted** [*ip* [*mask*]]

【参数说明】 *ip*：IP 地址，显示指定 IP 地址的 ARP 表项；如果指定 trusted 关键字，则只显示可信任 ARP 表项，否则显示非可信任 ARP 表项。

mask：显示 IP 子网内的 ARP 表项; 如果指定 trusted 关键字，则只显示可信任 ARP 表项，否则显示非可信任 ARP 表项。

【配置模式】 特权模式

【使用指导】 -

↘ 删除交换机上的可信任 ARP

【命令格式】 **clear arp trusted** [*ip* [*mask*]]

【参数说明】 *ip*：IP 地址，显示指定 IP 地址的 ARP 表项；如果指定 trusted 关键字，则只显示可信任 ARP 表项，否则显

示非可信任 ARP 表项。

mask：显示 IP 子网内的 ARP 表项; 如果指定 trusted 关键字，则只显示可信任 ARP 表项，否则显示非可信任 ARP 表项。

【配置模式】 特权模式

【使用指导】 执行 **clear arp trusted** 会删除交换机上的所有的可信 ARP，可能导致用户不能上网。

一般情况下使用 **clear arp trusted** *ip* 删除指定的可信任 ARP 表项。

↘ 允许可信任 ARP 老化

【命令格式】 **arp trusted aging**

【参数说明】 -

【配置模式】 全局模式

【使用指导】 使用该命令后可信任 ARP 开始老化，老化时间和动态 ARP 老化时间相同。老化时间可以通过接口模式下 **arp timeout** 命令设置。

↘ 调整可信任 ARP 的容量

【命令格式】 **arp trusted***number*

【参数说明】 *number*：取值范围最小为 10，最大为对应产品 arp 容量减去 1024，缺省可信 arp 的最大表项数为 arp 总容量的一半。

【配置模式】 特权模式

【使用指导】 要使此命令生效，首先启用可信任 ARP 功能。可信任 ARP 表项和其它表项共享内存，如果可信任表项占用过多，可能导致动态 ARP 表项空间不够。一般按需设置，不要设置得太大。

配置举例

【网络环境】 网络拓扑如 图 2-1 所示

【配置方法】
- 开启可信任 ARP 功能
- 配置 VLAN 转换
- 配置可信任 ARP 表项运行老化
- 配置可信任 ARP 表项的容量为 1024

```
Ruijie(config)#servicetrustedarp
Ruijie(config)#arp trusted user-vlan 2-9 translated-vlan 10
Ruijie(config)#arp trusted aging
Ruijie(config)#arp trusted 1024
```

【检验方法】
- 通过 **show running-config** 查看上面的配置是否生效

```
Ruijie(config)# show running-config
servicetrustedarp
arp trusted user-vlan 2-9 translated-vlan 10
arp trusted aging
arp trusted 1024
```

常见配置错误

- 可信任 ARP 功能未开启，导致 ARP 表项下发失败

2.4.4 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】 网络拓扑如 图 2-1 所示

【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

2.4.5 配置代理ARP

配置效果

设备代理应答非本机的 ARP 请求报文。

注意事项

三层交换机缺省关闭代理 ARP 功能，路由器缺省开启代理 ARP 功能。

配置方法

- 可选配置。
- 没有路由信息的主机需要获得其它子网 IP 地址的 MAC 地址，设备需要开启代理 ARP 功能，代理应答 ARP。
- 在接口模式下配置

检验方法

使用 **show ip interface**<*name*>命令查看是否配置成功。

相关命令

↘ 开启代理 ARP 功能

【命令格式】 **ip proxy-arp**

【参数说明】 -

【命令模式】 接口模式

【使用指导】 -

配置举例

【网络环境】 网络拓扑如 图 2-1 所示

【配置方法】 配置 GigabitEthernet 0/0 口开启代理 ARP 功能

```
Ruijie(config-if-GigabitEthernet 0/0)#ip proxy-arp
```

【检验方法】 使用 **show ip interface** 命令查看是否配置成功

```
Ruijie#show ip interface gigabitEthernet 0/0
GigabitEthernet 0/0
  IP interface state is: DOWN
  IP interface type is: BROADCAST
  IP interface MTU is: 1500
  IP address is:
    No address configured
  IP address negotiate is: OFF
  Forward direct-broadcast is: OFF
  ICMP mask reply is: ON
  Send ICMP redirect is: ON
  Send ICMP unreachable is: ON
  DHCP relay is: OFF
  Fast switch is: ON
  Help address is: 0.0.0.0
  Proxy ARP is: ON
ARP packet input number: 0
  Request packet     : 0
  Reply packet       : 0
  Unknown packet     : 0
TTL invalid packet number: 0
ICMP packet input number: 0
 Echo request       : 0
 Echo reply         : 0
 Unreachable        : 0
 Source quench      : 0
 Routing redirect   : 0
```

常见配置错误

无

2.4.6 配置any IP ARP

配置效果

用户使用任意 IP 地址都可以上网。

注意事项

只有出口网关产品支持 any IP ARP 功能。

以下两种情况用户必须修改配置才能上网：

(1) 用户 IP 地址属于和设备直连接口的网段，但配置的网关 IP 地址不是和设备直连接口上配置的 IP 地址。

(2) 用户 IP 地址不属于和设备直连接口的网段，但是属于设备其它接口的网段，即存在冲突的情况。

由于用户 IP 地址不属于和设备直连接口的网段，其动态 ARP 表项和直连路由的生成依赖于用户端首先发起 ARP 请求，因此如下场景(但不仅限于如下场景)会导致用户不能上网，需要用户端清除 ARP 表项然后重新学习网关地址：

(1) 设备代理应答 ARP 请求，用户学习到设备 MAC 地址后，在设备上清除动态 ARP 表项，导致用户动态 ARP 表项和直连路由被删除，应答报文无法到达用户端；

(2) 设备代理应答 ARP 请求，用户学习到设备 MAC 地址后，在接口上关闭 any IP ARP 功能，然后再打开。

注：接口关闭 any IP ARP 功能也会导致用户动态 ARP 表项和直连路由被删除，从而应答报文无法到达用户端。

另外，如果存在对应的静态 ARP 表项或者 VRRP IP 地址的 ARP 表项，any IP ARP 生成的动态 ARP 表项会添加失败或者被覆盖，any IP ARP 功能不生效。

配置方法

- 可选配置。
- 在酒店环境下，网关设备可以开启 any IP ARP 功能，方便用户在不更改 IP 地址的情况下可以上网。
- 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 any IP ARP 功能

【命令格式】 **arp any-ip**

【参数说明】 -

【命令模式】 接口模式

【使用指导】

- 接口关闭 any IP ARP 功能也会导致用户动态 ARP 表项和直连路由被删除，从而应答报文无法到达用户端。
- 如果存在对应的静态 ARP 表项或者 VRRP IP 地址的 ARP 表项，any IP ARP 生成的动态 ARP 表项会添加失败或者被覆盖，any IP ARP 功能不生效。

配置举例

【网络环境】 网络拓扑如图 2-3 所示

【配置方法】 配置 GigabitEthernet 0/0 口开启 any IP ARP 功能

```
Ruijie(config-if-GigabitEthernet 0/0)#arp any-ip
```

【检验方法】 使用 **show running-config interface** 查看是否配置成功

```
Ruijie(config-if-GigabitEthernet 0/0)#sh run int gi0/0

Building configuration...
Current configuration : 140 bytes
!
interface GigabitEthernet 0/0
 duplex auto
 speed auto
 ip address 30.1.1.1 255.255.255.0
 arp gratuitous-send interval 5
 arp any-ip
```

常见配置错误

无

2.4.7 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】 网络拓扑如 图 2-1 所示

【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

2.4.8 配置关闭动态ARP学习功能

配置效果

在接口上关闭动态 ARP 的学习功能后，接口将不能进行动态 ARP 学习。

注意事项

无

配置方法

- 可选配置
- 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

↘ 关闭动态 ARP 学习的功能

【命令格式】 **noarp-learning enable**

【参数说明】 -

【命令模式】 接口模式

【使用指导】 如果确认设备已经学习到需要学习的动态 ARP 表项，通过 web 将动态 ARP 转化为静态 ARP 后，建议开启该功能，否则不建议开启该功能。开启动态 ARP 不学习功能后，存在动态 ARP 表项的话，如果用户需要将动态 ARP 表项转化为静态 ARP 表项，可以通过 web 配置，如果用户需要清除掉该动态 ARP 表项，不允许某一用户上网，则可以通过 clear arp 命令，否则动态 ARP 表项进行正常老化，在老化时间到后，该动态 ARP 表项被清除掉。开启接口停止动态 ARP 学习功能后，则 AnyIP 功能、ARP 可信检测功能失效。

配置举例

【网络环境】 网络拓扑如 图 2-1 所示

【配置方法】 配置 GigabitEthernet 0/0 口禁止动态 ARP 学习功能。

```
Ruijie(config-if-GigabitEthernet 0/0)#no arp-learning enable
```

【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
no arp-learning enable
```

常见配置错误

无

2.4.9 配置ARP扫描

配置效果

在接口上配置 ARP 扫描的功能后，会对指定范围的邻居进行扫描，然后学习这些邻居的 ARP。

注意事项

无

配置方法

- 可选配置
- 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 扫描功能

【命令格式】 **arp scan** [*start-ip-address end-ip-address*]

【参数说明】 *start-ip-address*：ARP 扫描区间的起始 IP 地址，起始 IP 地址必须小于等于终止 IP 地址。

end-ip-address：ARP 扫描区间的终止 IP 地址，终止 IP 地址必须大于等于起始 IP 地址。

【命令模式】 接口模式

【使用指导】 1. ARP 扫描功能一般与 WEB 动态 ARP 转静态 ARP 的功能结合使用。

2. 对于已存在的邻居 ARP 表项的 IP 不进行扫描。

3. 如果用户知道局域网内邻居分配的 IP 地址范围，则可以通过指定 ARP 扫描区间，对该范围内的邻居进行扫描，减少扫描等待的时间。ARP 扫描区间内指定的主机数量必须小于或者等于 1024。

4. ARP 扫描区间的起始 IP 地址和终止 IP 地址必须与接口的 IP 地址（主 IP 地址或从 IP 地址）在同一网段。

5. 如果用户不指定 ARP 扫描区间的起始 IP 地址和终止 IP 地址，则仅对接口下的主 IP 地址网段内的邻居进行扫描。且该主 IP 地址的网段掩码必须大于等于 22 位。

6. ARP 扫描属于即配即用，配置一次，生效一次，不支持配置保存和下次生效。

7. ARP 扫描时间点：在配置时执行一次，执行条件是接口三层 UP（即链路 UP 且配置了 IP 地址）。

配置举例

【网络环境】 网络拓扑如 图 2-1 所示

【配置方法】 配置开启 GigabitEthernet 0/0 口上的 ARP 扫描。

```
Ruijie(config-if-GigabitEthernet 0/0)#arp scan 192.168.23.1 192.168.23.10
```

【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 192.168.23.2 255.255.255.0
 arp scan 192.168.23.1 192.168.23.10
```

常见配置错误

1. 配置的起始 IP 地址大于终止 IP 地址。

2. 配置的起始 IP 地址和终止 IP 地址与接口的 IP 地址不在同一个网段上。

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**

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**
显示可信任 ARP 表	**show arp** [**detail**] **trusted** [*ip* [*mask*]]
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 IP Event Dampening

3.1 概述

对三层设备来说，当三层网络接口由于人为的开启/关闭或者由于其他外在因素导致状态频繁 UP/DOWN 变化时，会造成本设备上路由表的反复震荡。若配置了路由协议，那么路由协议还可能会将这一震荡扩散到整个网络中，造成邻居路由反复进行路由的更新和重新计算，不仅浪费网络带宽，而且导致整个网络不稳定。从设备本身的角度来说，反复的路由更新和计算需要消耗大量的 CPU 资源。这些都会影响客户网络的正常运行。

IP Event Dampening（IP 事件惩罚）功能能够检测异常的 UP/DOWN 翻转，并自动抑制接口状态频繁 UP/DOWN，使单点链路故障不会被路由协议扩散出去；当接口恢复稳定后，抑制状态将自动解除，从而减少网络震荡，降低系统的 CPU 资源消耗，增强整网的稳定性。

协议规范

- RFC2439：BGP Route Flap Damping

IP Event Dampening 采用的抑制算法核心与 RFC2439 所述的 BGP 路由翻转抑制算法一致。

3.2 典型应用

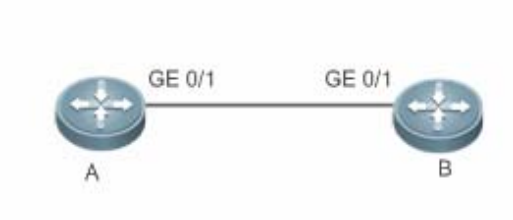
典型应用	场景描述
抑制路由接口震荡	在路由器三层网络接口上监控接口状态变化，对接口的频繁震荡进行抑制。

3.2.1 抑制路由接口震荡

应用场景

在运行路由协议的网络中，两两相连的路由器之间一旦有端口频繁 UP/DOWN，将引起邻居路由反复更新计算路由，进而扩散到整个网络，导致网络震荡。通过在相连的路由口上启用 IP Event Dampening 功能，可以监控接口状态变化，并对接口的频繁振荡进行抑制，减少网络震荡，降低系统的 CPU 资源消耗，增强整网的稳定性。

图 3-1



【注释】 A、B 为普通路由器。

功能部属

以上图为例，可以在路由器 A 和 B 的接口 GE0/1 上配置 IP Event Dampening 功能。

⚠ 路由器上的子接口和接口虚模板 Virtual template，不支持 dampening 功能。

3.3 功能详解

基本概念

↘ 惩罚值（penalty）

IP Event Dampen ing 功能采用了一种对接口状态变化事件计算惩罚值的方式，对接口行为进行感知和控制。接口上每进行一次 up→down 翻转，惩罚值将会累加，待接口稳定时，该惩罚值又会按指数递减。通过这种惩罚值计算，使得接口能智能地感知其自身的状态行为，进行相应处理。

↘ 抑制门限（Suppress Threshold）

为了识别接口震荡事件，IP Event Dampening 功能设置了一个抑制门限，当累积惩罚值超过该门限时，认为该接口处于震荡状态，并对接口实施抑制。

↘ 半衰期（Half-Life Period）

半衰期是指在接口稳定情况下惩罚值衰减到原来一半所需要的时间。它定义了惩罚值按指数衰减的速度，半衰期越短，衰减的越快，探测到接口稳定的速度越快，但震荡检测的灵敏度也越低。

↘ 解除抑制门限（Reuse Threshold）

当接口不再震荡，惩罚值衰减到一定程度（减少到抑制门限以下）时，可认为该接口恢复稳定状态，从而解除接口的抑制状态。

↘ 最大抑制时间（Maximum Suppress Time）

为避免接口长时间震荡后，惩罚值过大，导致过久不能恢复使用，算法定义了一个最大抑制时间，即无论接口震荡多久，接口被抑制的时间不会超过最大抑制时间。

功能特性

功能特性	作用
接口震荡抑制	允许用户在接口上配置接口震荡抑制条件和参数 ,使得交换机或路由器设备能自动对反复震荡的接口进行识别和抑制，确保本机的路由稳定性和避免路由震荡的扩散。

3.3.1 接口震荡抑制

工作原理

当接口上配置了 Dampening 功能时，该接口上会被附上一个与之相关的惩罚值（Penalty）。每当接口 DOWN 的时候，该接口上的 Penalty 增加 1000，该 Penalty 值随时间递减，若递减过程中，接口再次出现 DOWN 事件，则接口上 Penalty 值进行累加，若累计 Penalty 值超过抑制门限（Suppress Threshold）则判断该接口处于抑制（Suppress）状态，之后无论接口的真实状态是什么，对受影响的上层协议来说，该接口始终处于 DOWN 状态。直到 Penalty 递减到解除抑制门限（Reuse Threshold），接口的抑制状态解除，还原接口的真实状态。

当三层接口上未配置 Dampening 功能，或配置了 Dampening 功能但接口未被抑制时，路由协议或其他关心三层接口状态的协议都和正常情况下的行为一样。当接口上配置了 Dampening 且接口被抑制时，上层协议认为接口状态为 down，这期间接口实质上的状态变化不会对路由表以及上层路由协议路由计算和通告造成影响，直到接口解除抑制为止。

相关配置

↘ 配置 IP Event Dampening 功能

- 缺省情况下，三层接口上的 IP Event Dampening 功能关闭。
- 使用 **dampening** [*half-life-period* [*reuse-threshold suppress-threshold max-suppress* [**restart** [*restart-penalty*]]]]命令可以启动或关闭接口上的 IP Event Dampening 功能。

3.4 配置详解

配置项	配置建议 & 相关命令	
启动 IP Event Dampening	⚠ 必须配置。用于抑制三层接口震荡。	
	dampening	配置 IP Event Dampening 功能

3.4.1 启动IP Event Dampening

配置效果

在配置有 IP Event Dampening 的接口上，若发现震荡情况超过用户预先设定的条件参数时，将该接口状态设置为 down。

注意事项

- 对于交换机接口层次转换（三层口转换为 2 层口），如从 routed port 转换为 switch port，该接口上配置的 **dampening** 命令将被删除。

- 对于路由器来说只有主接口可以配置接口事件抑制功能。该功能可以对配有该命令的主接口的所有子接口生效，但不能直接在子接口上配置该命令。该命令也不支持在 virtual template 上配置。

配置方法

↘ 配置 IP Event Dampening 功能

- 必须配置
- 在三层接口模式下配置。
- 配置的时候可以指定半衰期、解除抑制门限、抑制门限、最大抑制时间和初始惩罚值，如果没有指定则使用默认值。

检验方法

可以使用以下两种方法来确认配置是否生效。

- **show running-config。**
- **show interfaces** [*interface-id*] **dampening，**查看接口 IP Event Dampening 配置情况。

相关命令

↘ 打开接口上的 Ip Event Dampening 功能

【命令格式】 **dampening** [*half-life-period* [*reuse-threshold suppress-threshold max-suppress* [**restart** [*restart-penalty*]]]]

【参数说明】 *half-life-period*：半衰期，范围<1-30>，默认 5s。

reuse-threshold：解除抑制门限，范围<1-20000>，默认 1000。

suppress-threshold：抑制门限，范围<1-20000>，默认 2000。

max-suppress：最大抑制时间，范围<1-255>，默认为 half-life-period 的 4 倍。

restart *restart-penalty*：初始惩罚值，范围<1-20000>，默认 2000。

【命令模式】 接口模式

【使用指导】 该功能会影响直连/主机路由，静态路由，动态路由和 VRRP。当一个接口满足命令的配置条件，处于抑制状态时，以上受影响的模块认为该接口状态为 DOWN，从而会删除对应的路由，并且不会从该接口收发数据包。

当在一个已经配置了 **dampening** 命令的接口上，重新配置命令，会使该接口的所有 dampening 信息清空，但接口的翻转次数仍会保留，除非使用 **clear counters** 命令清除接口的统计信息。

如果配置的 *max-suppress* 太小，导致计算得出的最大惩罚值比抑制门限还要小，则该接口将永远得不到抑制。这属于配置错误，此时会打印类似如下的信息，提示用户配置失败：

```
% Maximum penalty (10) is less than suppress penalty (2000). Increase maximum suppress time
```

另外，当配置该命令时，系统内存不足以执行该配置保存，也会打印配置失败的提示：

```
% No memory, configure dampening fail!
```

配置举例

↘ 在三层接口上配置 Ip Event Dampening 功能

【网络环境】

图 3-2



【配置方法】 在路由器 A 和 B 接口 GigabitEthernet 0/1 上开启 IP Event Damp ening 功能，半衰期 30 秒，解除抑制门限 1500，开始抑制门限 10000，以及最长抑制时间为 120 秒。

A

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# dampening 30 1500 10000 100
```

B

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# dampening 30 1500 10000 100
```

【检验方法】 通过 **show interfaces dampening** 命令查看接口的 dampening 的详细信息。

```
Ruijie#show interfaces dampening
GigabitEthernet 0/1
  Flaps Penalty Supp    ReuseTm HalfL   ReuseV  SuppV   MaxSTm  MaxP    Restart
  0     0       FALSE   0       30      1500    1000    100     15119   0
```

常见错误

- 在三层交换机下配置，接口必须先 **no swithport**，转为路由口后才能配置。

3.5 监视与维护

清除各类信息

作用	命令
清除接口的统计信息。	**clear counters**

clear counter 命令相关说明请参考“接口”命令的相关章节。

查看运行情况

作用	命令
显示被惩罚的接口统计信息。	**show dampening interface**
显示接口 IP Event Dampening 配置情况。	**show interfaces dampening**

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 Dampening 功能的调试开关。	**debug dampening interface**

4 TCP

4.1 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络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)

4.2 典型应用

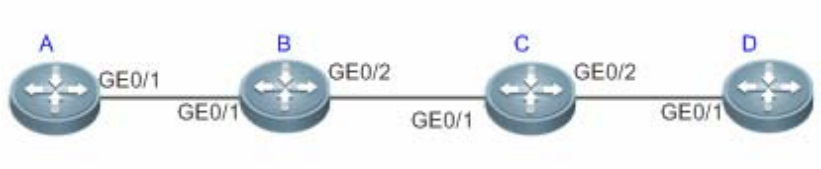
典型应用	场景描述
TCP 性能优化	TCP 传输路径上某一段链路的 MTU 比较小，为了避免 TCP 报文分片，可以开启 TCP 的路径 MTU 发现功能。
TCP 连接异常检测	TCP 探测对端是否还在正常工作。

4.2.1 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 4-1



【注释】 A、B、C 和 D 为路由器。

功能部署

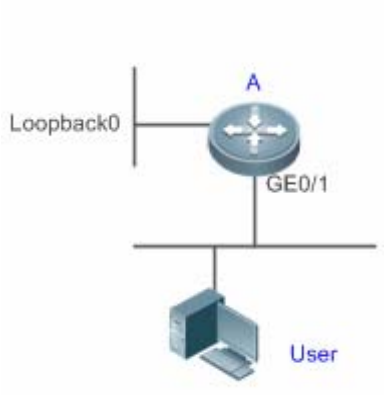
- 在 A 和 D 上开启 TCP 的路径 MTU 发现功能。

4.2.2 TCP连接异常检测

应用场景

以下图为例，用户远程登陆到设备 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 4-2



【注释】 A 是路由器。

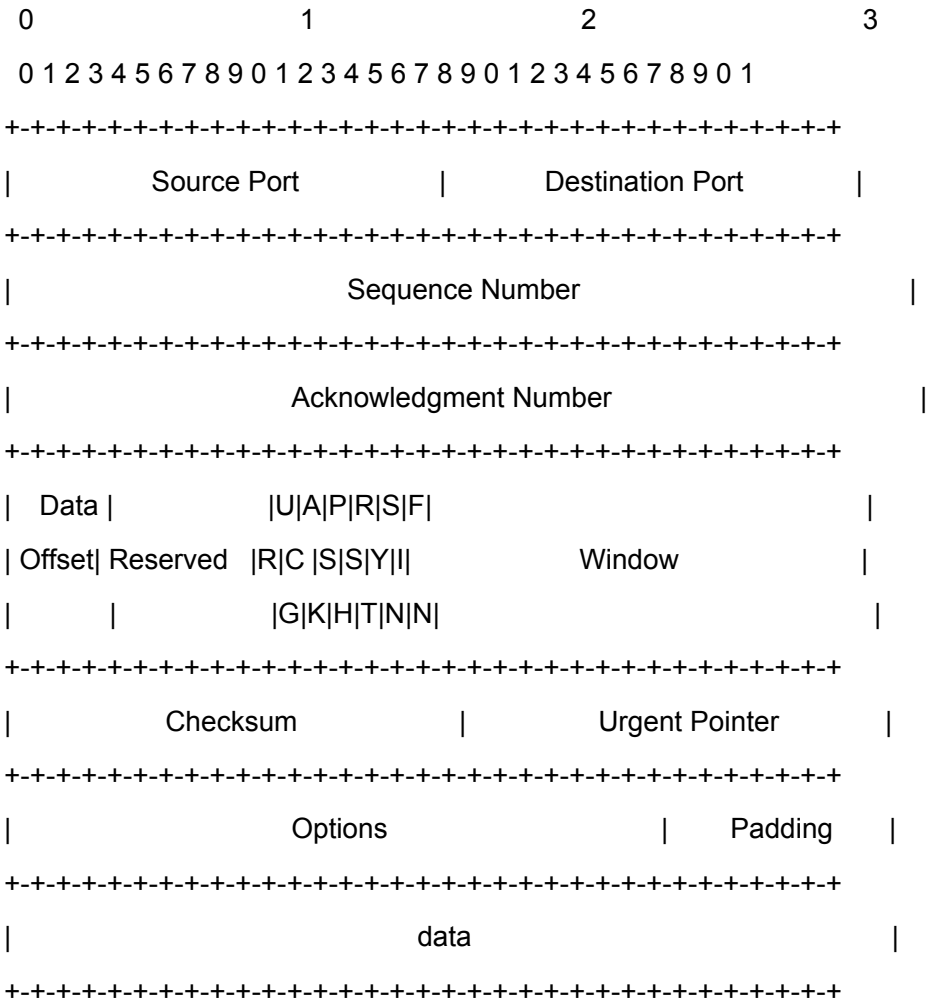
功能部署

- 在设备 A 上开启 TCP 保活功能。

4.3 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
配置转发的 SYN 报文的 MSS 选项值	把转发的 SYN 报文中的 MSS 选项值修改为配置的 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

4.3.1 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。

11.0 版本废弃了 10.x 版本的配置命令“ip tcp s yntime-out”被废弃，但兼容 10.x 版本，如果执行了 10.x 版本的配置命令，将自动转换成 11.0 版本的配置命令。

4.3.2 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、有大批量数据的连接，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。

4.3.3 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。

11.0 版本废弃了 10.x 版本的配置命令“ip tcp not-send-rst”，并且兼容 10.x 版本，如果执行了 10.x 版本的配置命令，将自动转换成 11.0 版本的配置命令。

4.3.4 配置MSS

工作原理

最大分段大小（Maxitum 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。

发送 SYN 报文时 MSS 选项值的计算方法如下：

- IPv4 TCP：MSS = 对端 IP 地址对应的出口的 IP MTU - 20 字节 IP 首部 - 20 字节 TCP 首部。

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。

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。

4.3.5 配置转发的SYN报文的MSS选项值

工作原理

当客户端发起一个 TCP 连接时，它通过 TCP SYN 报文中的 MSS 选项字段协商 TCP 报文数据载荷的最大值，客户端 SYN 报文的 MSS 值表示后续服务器端发送 TCP 报文数据载荷的最大值，反之同理。

如下图所示，PC 与 HTTP 服务器端建立的连接协商的 MSS 是 1460，但数据长度为 1460 字节的 TCP 报文无法直接通过 R1 和 R2，需要分片，因为 R1 和 R2 用隧道相连，隧道的 MTU 小于 1500。这时可以通过在 R2 的（1）口和（2）口上修改 SYN 报文中的 MSS 选项值，从而修改经过（1）口和（2）口的 TCP 连接协商的 MSS 值。

图 4-3



相关配置

↘ 设置转发的 TCPv4 SYN 报文的 MSS 选项值

- 缺省配置是不修改转发的 TCPv4 SYN 报文的选项值。
- 用户可以在接口配置模式下使用“**ip tcp adjust-mss** *max-segment-size*”命令设置转发的 TCPv4 SYN 报文的 MSS 选项值，取值范围是 500 到 1460，单位是字节。
- 如果 TCPv4 报文传输路径中两台设备之间链路的 MTU 比较小，为了避免 TCP 报文分片，用户可以在该设备上设置转发的 TCPv4 SYN 报文的 MSS 选项值，该设备收到 TCPv4 SYN 报文时将会修改 MSS 选项值。用户选择 MSS 值时可以参考接口的 IP MTU。

该配置对于已经存在的 TCP 连接无效，只对新的 TCP 连接有效。

4.3.6 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：

(1) 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。

(2) 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 = 路径 MTU - IP 头部长度 - 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。

4.3.7 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。

10.x 版本提供全局配置模式的配置命令“**service tcp-keepalives-in**”用来开启 TCP 服务器端的保活功能，11.0 版本废弃该命令，该命令隐藏，如果用户执行该命令，将转换成新的配置命令保存。

10.x 版本提供全局配置模式的配置命令“**service tcp-keepalives-out**”用来开启 TCP 客户端的保活功能，11.0 版本废弃该命令，该命令隐藏，如果用户执行该命令，将转换成新的配置命令保存。

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。

4.4 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。	
	ip tcp synwait-time	配置建立 TCP 连接的超时时间。

	ip tcp window-size	配置 TCP 窗口大小。
	ip tcp send-reset	配置收到端口不可达的 TCP 报文时是否发送 reset 报文。
	ip tcp mss	配置 TCP 连接的 MSS。
	ip tcp adjust-mss	配置转发的TCPv4 SYN报文的MSS选项值。

4.4.1 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。

配置转发的 TCPv4 SYN 报文的 MSS 选项值

- 可选配置。
- 如果 TCP 传输路径中两台路由器之间的 MTU 比较小，可以在路由器上配置。

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。

配置转发的 TCPv4 SYN 报文的 MSS 选项值

【命令格式】 **ip tcp adjust-mss** *max-segment-size*

【参数说明】 *max-segment-size*：最大数据段大小，单位为字节，取值范围是 500 到 1460。

【命令模式】 接口模式

【使用指导】 -

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

-

4.4.2 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

-

4.5 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** *a.b.c.d*] [**local-port** *num*] [**peer-ip** *a.b.c.d*] [**peer-port** *num*]
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** *a.b.c.d*] [**local-port** *num*] [**peer-ip** *a.b.c.d*] [**peer-port** *num*]
显示 IPv4 TCP 端口使用情况	**show tcp port** [*num*]
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** *a.b.c.d*] [**peer-ip** *a.b.c.d*] [**global**] [**local-port** *num*] [**peer-port** *num*] [**deeply**]
查看 IPv4 TCP 连接的调试信息	**debug ip tcp transactions** [**local-ip** *a.b.c.d*] [**peer-ip** *a.b.c.d*] [**local-port** *num*] [**peer-port** *num*]

5 软件 IPv4 快转

5.1 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。

下文仅介绍软件 IPv4 的相关内容。

协议规范

-

5.2 典型应用

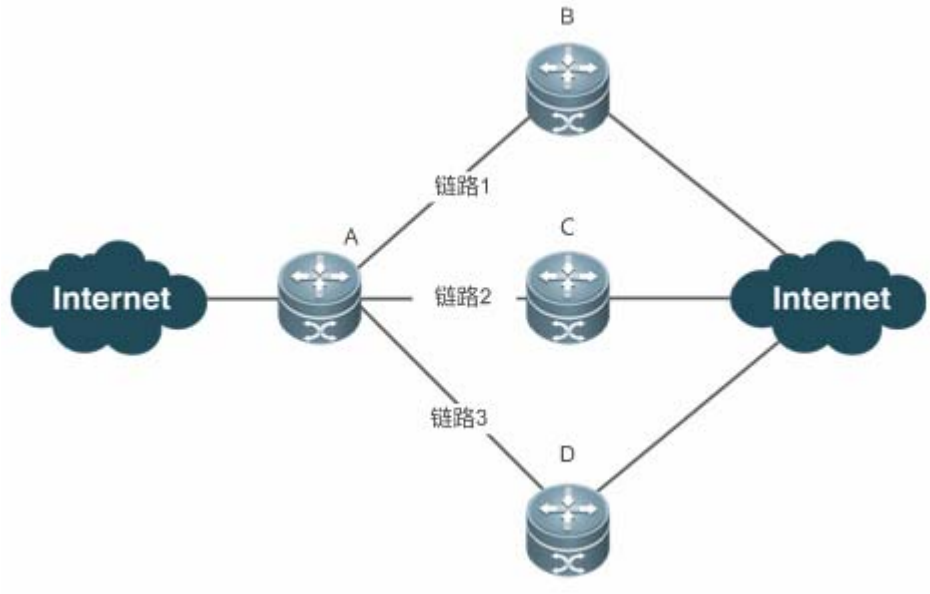
典型应用	场景描述
流量负载均衡	在网络路由中，当路由前缀关联到多个下一跳时，快转可以在多个下一跳中实现流量负载均衡。

5.2.1 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 5-1



【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。

5.3 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。

5.3.1 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，分别是根据报文的目的 IP 地址进行均衡、根据报文的源 IP 和目的 IP 地址进行均衡。

相关配置

↘ 配置 IPv4 源 IP 地址 + 目的 IP 地址负载均衡算法

- 缺省根据 IPv4 报文的目的 IP 地址进行均衡。
- 可以根据 ip ref load-sharing original 配置该负载均衡算法。
- 配置后根据 IPv4 报文的目的 IP 地址和源 IP 地址进行均衡。

5.4 配置详解

配置项	配置建议 & 相关命令	
配置快转负载均衡策略	⚠ 可选配置。	
	ip ref load-sharing original	启动 IPv4 源 IP 地址 + 目的 IP 地址负载均衡算法

✓ 以上命令为路由器专有命令。

5.4.1 配置快转负载均衡策略

配置效果

路由快转支持的两种选路策略如下：

- 按 IPv4 报文的目的 IPv4 地址进行均衡，对报文的目标地址进行散列，权重大的路径被选中的机率大。缺省采用此策略。
    - 按 IPv4 报文的目的 IPv4 地址和源 IPv4 地址进行均衡，对报文的目的 IPv4 地址和源 IPv4 地址进行散列，权重大的路径被选中的机率大。

注意事项

本配置为路由器专有配置。

配置方法

- 可选配置。
- 在 IPv4 环境下，如果需要根据源 IP 地址+目的 IP 地址进行流量均衡，可采用此配置。
- 在连接多条链路的路由设备上配置。

检验方法

使用 show ip ref adjacency statistic 命令可以查看 IPv4 快转的负载均衡策略；

相关命令

配置 IPv4 源 IP 地址 + 目的 IP 地址负载均衡算法

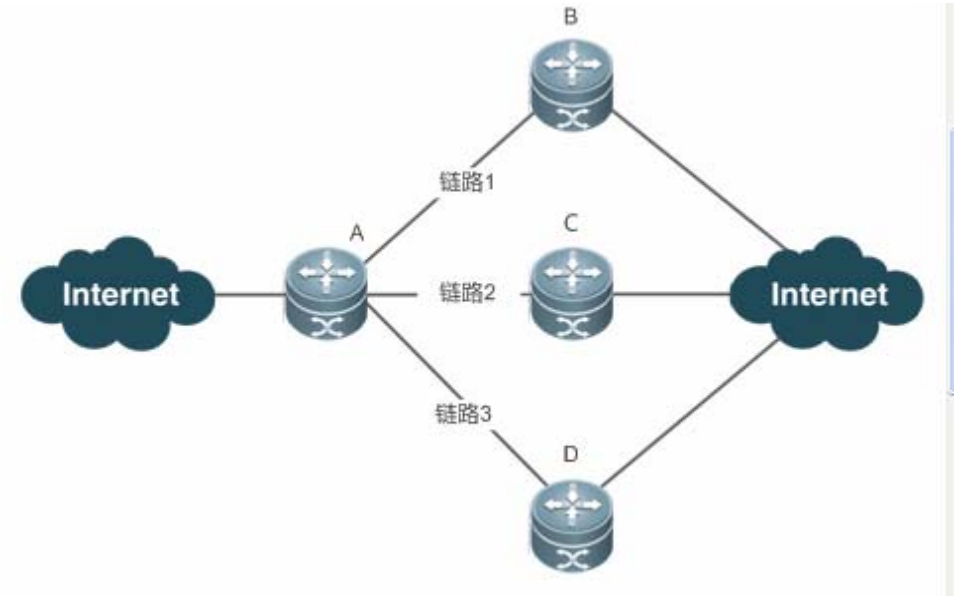
【命令格式】 **ip ref load-sharing original**
【参数说明】 -
【命令模式】 全局模式
【使用指导】

配置举例

配置基于 IPv4 源 IP 地址 + 目的 IP 地址负载均衡

【网络环境】

图 5-2



在路由器 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。

【配置方法】 在路由器 A 上配置 IPv4 源 IP 地址 + 目的 IP 地址负载均衡

A

```
A#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
A(config)#ip ref load-sharing original
```

【检验方法】

```
A #show ip ref adjacency statistics
adjacency balance table statistic:
    source-dest-address load-sharing
    balance: 0

adjacency node table statistic:
    total  : 3
    local  : 1
    glean  : 0
    forward: 0
    discard: 0
    mcast  : 1
    punt   : 1
    bcast  : 0
```

常见配置错误

-

5.5 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。

6 TUNNEL

6.1 概述

Tunnel 接口用于实现隧道功能，是系统虚拟的接口。Tunnel 接口并不特别指定传输协议或者负载协议，它提供的是一个用来实现标准的传输链路。每一个 Tunnel 接口代表一个传输链路。

Tunnel 功能实现包括下面三个主要组成部分：

- 负载协议：通过 Tunnel 传输的负载(网络数据)的封装协议。如 IPv4 和 IPv6 协议作为负载协议，对于 GRE 隧道，可以是不是 IPv4 或者 IPv6 协议；
- 载体协议：用来二次封装并辨识待传输负载的协议。在本文描述的 TUNNEL 中，只有 GRE 隧道有载体协议，即 GRE 协议（也即封装协议）。其他类型的隧道都是 IPv4/IPv6 外面直接封装 IPv4/IPv6；
- 传输协议：实际传输经过载体协议二次封装后的负载的网络协议。锐捷产品使用最广泛应用的 IPv4 和 IPv6 协议作为传输协议。

实际上，如果两个私有同种协议网络需要通过异种公有网络实现互通讯，就可以采用 Tunnel 模式实现。

Tunnel 传输适用于以下情况：

- 允许运行非 IP 协议的本地网络之间通过一个单一网络（IP 网络）通讯，因为 Tunnel 支持多种不同的负载协议；允许那些对路由跳数有限制的协议可以在更广泛的范围内工作，因为 Tunnel 使用的是传输协议（IP）的路由工作；
- 允许通过单一的网络（IP 网络）连接间断子网；
- 允许在广域网上提供 VPN （Virtual Private Network，虚拟专用网络）功能。

由于 Tunnel 将负载封装后传输，这会带来处理上的复杂性，在某些情况下需要注意以下的变化。

- 由于 Tunnel 是逻辑链路，在路由的时候看起来只有一跳（hop），可实际上可能其路由花费不止一跳。在使用 Tunnel 的时候必须注意到 Tunnel 链路的路由与实际路由并不一致。
- 由于 Tunnel 传输将负载封装在传输协议中，在设置防火墙特别是访问控制链表(ACL)的时候，这一点需要考虑；同时必须注意到此时负载协议的传输带宽等(如 MTU)也比理论值更小。

下文仅介绍 Tunnel 的相关内容。

协议规范

- RFC2784：Generic Routing Encapsulation (GRE)
- RFC2890：Key and Sequence Number Extensions to GRE
- RFC3056：Connection of IPv6 Domains via IPv4 Clouds
- RFC4023：Encapsulating MPLS in IP or Generic Routing Encapsulation (GRE)

- RFC4087：IP Tunnel MIB
- RFC4213：Basic Transition Mechanisms for IPv6 Hosts and Routers
- RFC4797：Use of Provider Edge to Provider Edge (PE-PE) Generic Routing Encapsulation (GRE) or IP in BGP/MPLS IP Virtual Private Networks
- RFC5158：6to4 Reverse DNS Delegation Specification
- RFC5214：Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)
- RFC5332：MPLS Multicast Encapsulations
- RFC5579：Transmission of IPv4 Packets over Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) Interfaces
- RFC5845：Generic Routing Encapsulation (GRE) Key Option for Proxy Mobile IPv6
- RFC5969：IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) -- Protocol Specification
- RFC6245：Generic Routing Encapsulation (GRE) Key Extension for Mobile IPv4
- RFC6343：Advisory Guidelines for 6to4 Deployment
- draft-zhou-dhc-gre-option-00 DHCPv4 and DHCPv6 options for GRE
- draft-cai-softwire-6rd-mib-03 Definitions of Managed Objects for 6rd
- draft-howard-isp-ip6rdns-05 Reverse DNS in IPv6 for Internet Service Providers
- draft-tsou-softwire-6rd-multicast-02 IPv6 Multicast Using Native IPv4 Capabilities in a 6rd Deployment
- draft-templin-v6ops-isops-18 Operational Guidance for IPv6 Deployment in IPv4 Sites using ISATAP

6.2 典型应用

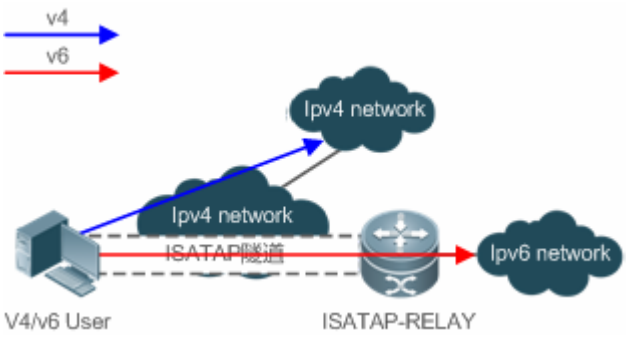
典型应用	场景描述
访问园区网内部的 IPv6 站点	访问园区网内部的 IPv6 站点。
园区网接入 IPv6 骨干网	园区网接入 IPv6 骨干网。

6.2.1 访问园区网内部的IPv6 站点

应用场景

一些园区网有部署 IPv6 服务器，PC 需要能访问这些服务器。可以利用 ISATAP 自动隧道实现这种应用。

图 6-1



【注释】 ISATAP-RELAY 为支持 tunnel 的设备，园区网用户访问 IPv4 的服务器时，直接通过 IPv4 网络访问；访问 IPv6 的服务器时，需通过 ISATAP 隧道访问

功能部属

- V4/V6 用户通过 V4 地址访问 IPv4 网络。
- V4/V6 用户通过 ISATAP 隧道访问 IPv6 网络。
- ISATAP 隧道在 PC 和 ISATAP-RELAY 路由器建建立 ISATAP 隧道。

6.2.2 园区网接入IPv6 骨干网

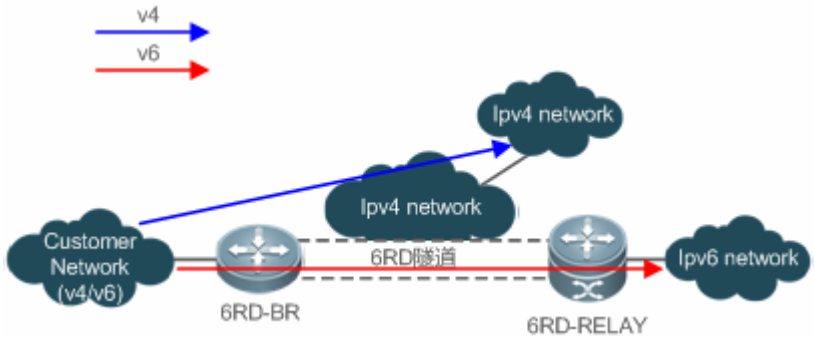
应用场景

将旧的园区网升级成支持 IPv6，或者新建一个支持 IPv6 的园区网。可以使用

6rd 和

6to4 自动隧道实现。

图 6-2



【注释】 6RD-BR 为 6RD 边界路由器

6RD-RELAY 为 6RD 中继路由器，客户网络访问的 IPv6 网络中间隔着 IPv4 网络时，可以通过 6RD 隧道访问

功能部属

- 6RD-BR 和 6RD-RELAY 之间建立 6RD 隧道。
- 6RD 隧道一般由 ISP 部署。
- 6RD-BR 的配置一般通过 DHCP 动态获得。

6.3 功能详解

基本概念

隧道 MTU

- 隧道接口的 MTU（Maximum Transmission Unit，最大传输单元）一般低于普通接口，如普通的 IPv4 over IPv4 的隧道，假定在以太网上传输，那么除去 2 层 IP 头部，每个报文实际能传输的最大数据量是 1460 字节。所以隧道接口的 MTU 为 1480 字节，而不是标准以太网接口的 1500 字节。

隧道路径 MTU

- 隧道接口实际上代表了一个虚拟的链路。以 IPv4 over IPv4 隧道为例。这个隧道接口的 MTU 实际上是隧道链路的 MTU，即隧道本端和对端之间的路径 MTU。当本端和对端之间的路由路径发生变化后，则路径 MTU 可能发生变化，从而影响隧道接口的 MTU

隧道嵌套层数

- 隧道可以嵌套。以 IPv4 over IPv4 隧道为例。可以将原始的 IPv4 报文再封装 2 层 IPv4 首部或者更多层次的 IPv4 首部以后再发送出去。需要隧道嵌套的场景一般不多见，主要是为了更安全的缘故。隧道嵌套后，可以传输的数据更少了。一个隧道接口的对端地址经过 FIB 选路后，如果出口是另一个隧道接口，则会发生隧道嵌套封装；如果选路后出口又是本隧道，那么会出现无穷嵌套（锐捷产品能检测出这种情况，并给出提示）。

功能特性

功能特性	作用
隧道可达性探测	判断隧道链路是否实际可用。
隧道 MTU 自适应调整	根据隧道链路对应的路径 MTU 的变化动态调整隧道接口的 MTU 的值。
隧道嵌套封装层数限制	根据实际需要调大隧道嵌套封装层数限制（很少使用）。
隧道数据有效性校验	对 GRE 隧道传输的数据增加校验和，用于检查数据传输过程中的是否发生错误。

6.4 产品说明



NBR108G-P、NBR800G、NBR950G、NBR1500G、NBR2000G 、NBR1000G-C 不支持 GRE； NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR2000G-C、NBR3000G-S、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 GRE。

NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE 支持 GRE V6 功能，NBR800G、NBR950G、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR108G-P、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1500G、NBR2000G 不支持 GRE V6 功能。

6.5 配置详解

配置项	配置建议 & 相关命令	
配置隧道接口基本功能	⚠ 必须配置。用于建立隧道。	
	Interface tunnel	新建一个隧道接口
	tunnel source	设置隧道的本端地址
配置隧道模式	⚠ 可选配置，用于设置隧道模式	
	tunnel mode	配置隧道封装模式
配置隧道对端地址	⚠ 可选配置，用于设置隧道对端地址	
	tunnel destination	配置隧道对端地址
配置隧道传输网络 TOS	⚠ 可选配置，用于设置传输网络的 TOS	
	tunnel tos	配置隧道传输网络 TOS
配置隧道传输网络 TTL	⚠ 可选配置，用于设置传输网络的 TTL	
	tunnel ttl	配置传输网络的 TTL
配置隧道 6rd br	⚠ 可选配置，用于设置隧道的 br IPv4 地址	
	tunnel 6rd br	配置 6rd 隧道的 br IPv4 地址
配置隧道 6rd br ipv4	⚠ 可选配置，用于设置隧道的 IPv4 通用前缀和通用后缀长度	
	tunnel 6rd ipv4	配置 6rd 隧道的 IPv4 通用前缀和通用后缀长度
配置隧道 6rd br prefix	⚠ 必选配置，用于设置隧道的 IPv6 前缀	

	tunnel 6rd br	配置 6rd 隧道的 IPv6 前缀

6.5.1 配置隧道接口

配置效果

- 新建一个隧道接口。

注意事项

无

配置方法

↘ 新建隧道接口功能

- 在全局配置模式下，使用 **interface tunnel** *number* 新建隧道接口。
- 只有创建了隧道接口，才能使用隧道服务。

检验方法

- 使用 **show interfaces tunnel** *number* 观察是否成功配置。

相关命令

↘ 配置隧道接口

【命令格式】 **interface tunnel** *number*

【参数说明】 *number*：隧道接口编号。

【命令模式】 全局模式

【使用指导】 -

↘ 检查隧道配置

【命令格式】 **show interfaces tunnel** *number*

【参数说明】 *number*：隧道接口编号。

【命令模式】 全局模式

【使用指导】 -

配置举例

↘ 新建一个隧道接口

【配置方法】
- 新建一个隧道接口

```
Ruijie# configure terminal
Ruijie(config)# interface tunnel 1
Ruijie(config-if-Tunnel 1)# end
```

【检验方法】
- 检查隧道接口的配置

```
Ruijie# show interfaces tunnel 1
……
Tunnel attributes:
……
  Tunnel protocol/transport is gre ip
```

常见错误

- 内存不足导致隧道接口创建失败。
- 硬件芯片资源不足导致隧道接口创建失败。

6.5.2 配置隧道封装模式

配置效果

- 需要使用非缺省封装模式的隧道时
- 在隧道接口模式下配置

注意事项

无

配置方法

设置隧道的封装模式

- 可选配置
- 缺省封装模式是 tunnel mode gre ip。
- 在隧道接口模式下，通过 tunnel mode 命令可以修改成其他模式。

检验方法

- 使用 **show interfaces tunnel** *number* 观察是否成功配置。

相关命令

配置隧道封装模式

【命令格式】 **tunnel mode { gre { ip | ipv6 } | ipv6 | ipip | ipv6ip [6rd | 6to4 | isatap] }**

【参数说明】 每一种 mode 代表从此隧道接口发出的报文的封装格式

gre ip 表示，先经过一个 GRE 头部封装，再经过 IPv4 封装，然后在新的 IPv4 网络发送

gre ipv6 表示，先经过一个 GRE 头部封装，再经过 IPv6 封装，然后在新的 IPv6 网络发送

ipv6 表示，从此接口发出的报文直接经过 IPv6 封装后，在新的 IPv6 网络发送

ipip 表示，此接口只能承载 IPv4 报文，并且此报文再经过 IPv4 封装后，在新的 IPv4 网络发送

ipv6ip 表示，此接口只能承载 IPv6 报文，并且报文经过 IPv4 封装后，在新的 IPv4 网络中发送

上述隧道都是手工隧道，而 ipv6ip 6rd/6to4/isatap 是自动隧道，报文封装过程中，目标 IPv4 地址是通过目标 IPv6 地址映射而成。

【命令模式】 接口模式

【使用指导】 隧道的 2 端一般情况下需要配置相同的模式，否则不能正常工作。

配置举例

配置隧道的封装模式为 IPv4 over IPv4。

【配置方法】
- 配置隧道接口的封装模式为 IPv4 over IPv4。

```
Ruijie# configure terminal
Ruijie(config)# interface tunnel 1
Ruijie(config-if-Tunnel 1)# tunnel mode ipip
Ruijie(config)# end
```

【检验方法】

- 检查隧道接口的配置

```
Ruijie# show interfaces tunnel 1
……
Tunnel attributes:
……
  Tunnel protocol/transport is ipv6ip
```

常见错误

- 相同 vrf 已经有一个 6to4 或者 isatap 隧道，继续配置这 2 种隧道。

6.5.3 配置隧道本端地址

配置效果

- 设置隧道的本端地址。

注意事项

- 隧道的本端地址必须同隧道的传输协议匹配。否则隧道口不会 UP(被禁用)。
- 当通过指定另外一个接口间接指定本端地址时，指的是 IPv4 主地址或者 IPv6 第一个全球公网地址。

配置方法

↘ 设置隧道的本端地址

- 必须配置
- 在隧道接口模式下使用 **tunnel source** 命令指定隧道的本端地址。

检验方法

- 通过 **show interfaces tunnel** *number* 命令可以观察隧道的本端地址

相关命令

配置隧道本端地址

【命令格式】 **tunnel source** { *ip-address* | *interface-name interface-number* }

【参数说明】 **ip-address**：可以是 IPv4 地址，也可以是 IPv6 地址。

Interface-name interface-number：可以是各种 3 层接口。

【命令模式】 接口模式

【使用指导】 如果直接指定 IPv4 或者 IPv6 地址，则需要设置成设备自身的地址

配置举例

配置隧道的本端地址。

【配置方法】

- 配置隧道的本端地址为 1.1.1.1

```
Ruijie# configure terminal
Ruijie(config)# interface tunnel 1
Ruijie(config-if-Tunnel 1)# tunnel mode ipv6ip
Ruijie(config-if-Tunnel 1)# tunnel source 1.1.1.1
```

【检验方法】

- 检查隧道接口的配置。

```
Ruijie# show interfaces tunnel 1
……
Tunnel attributes:
  Tunnel source 1.1.1.1, destination UNKNOWN, unrouteable
  Tunnel TOS/Traffic Class not set, Tunnel TTL 254
  Tunnel config nested limit is 0, current nested number is 0
  Tunnel protocol/transport ipv6ip
    Tunnel transport VPN is no set
  ……
```

常见配置错误

无

6.5.4 配置隧道对端地址

配置效果

- 手工隧道，必须配置对端地址后，才能使用（接口才会 UP）。

注意事项

- 自动隧道不能配置对端地址。

配置方法

↘ 配置隧道对端地址

- 6to4, isatap,6rd 隧道不能配置，其他隧道必须配置
- 在接口模式下通过 **tunnel destination** 命令配置对端地址。

检验方法

- **show interfaces tunnel** 命令可以查看是否配置成功。

相关命令

↘ 配置对端地址

【命令格式】 **tunnel destination** { *ip-address* }

【参数说明】 *ip-address*：可以是 ipv4 地址，也可以是 IPv6 地址。

【命令模式】 接口模式

【使用指导】 手工隧道必须配置对端地址。

配置的对端地址的协议族类型必须同传输协议一致，否则隧道接口禁用（不 UP）。

配置举例

↘ 配置隧道对端地址。

【配置方法】
- 配置隧道对端地址为 2.2.2.2

```
Ruijie# configure terminal
Ruijie(config)# interface tunnel 1
Ruijie(config-if-Tunnel 1)# tunnel mode ipv6ip
Ruijie(config-if-Tunnel 1)# tunnel destination 2.2.2.2
```

【检验方法】
- 检查隧道接口的配置

```
Ruijie# show interfaces tunnel 1
……
Tunnel attributes:
  Tunnel source: UNKNOWN, destination 2.2.2.2, unrouteable
  Tunnel TOS/Traffic Class not set, Tunnel TTL 254
  Tunnel config nested limit is 0, current nested number is 0
  Tunnel protocol/transport ipv6ip
  ……
```

常见错误

- 为自动隧道配置对端地址。
- 和另一个隧道的对端地址相同。

6.5.5 配置隧道传输网络TOS

配置效果

- 指定传输协议首部的 tos 或者 traffic class 字段。

注意事项

- 如果不指定，则拷贝承载协议对应的 tos 和 traffic class 字段。

配置方法

↘ 配置传输网络 TOS

- 可选配置
- 如果需要修订隧道数据在网络中的优先级
- 在接口模式下使用 tunnel tos 命令

检验方法

- 使用 **show interfaces tunnel** 命令查看是否成功设置。

相关命令

↘ 配置传输网络 TOS

【命令格式】 **tunnel tos** *number*

【参数说明】 *number*：需要设置的 tos 的值。

【命令模式】 接口模式

【使用指导】 缺省情况下，如果隧道内层承载与外层封装都是 IPv4 协议，则缺省将内层 IPv4 头的 tos 字节拷贝到外层 IPv4 头。如果隧道内层承载与外层封装都是 IPv6 协议，则缺省将内层 IPv6 头的 traffic class8 比特拷贝到外层 IPv6 头。其他情况，外层 IPv4 tos / IPv6 traffic class,为 0

配置举例

↘ 配置传输网络 TOS。

【配置方法】

- 配置传输网络 TOS

```
Ruijie# configure terminal
Ruijie(config)# interface tunnel 1
Ruijie(config-if-Tunnel 1)# tunnel mode ipv6ip
Ruijie(config-if-Tunnel 1)# tunnel tos 2
```

【检验方法】

- 检查隧道接口的配置

```
Ruijie# show interfaces tunnel 1
……
Tunnel attributes:
  Tunnel source 1.1.1.1, destination UNKNOWN, unrouteable
  Tunnel TOS/Traffic Class 0x2, Tunnel TTL 254
  Tunnel config nested limit is 0, current nested number is 0
  Tunnel protocol/transport ipv6ip
  Tunnel transport VPN is VPN1
……
```

常见错误

无

6.5.6 配置隧道传输网络TTL

配置效果

- 指定隧道封装协议首部的 TTL 或者 hoplimit 的值。

注意事项

无

配置方法

↘ 配置传输网络 TTL

- 可选配置
- 缺省 254
- 如果需要将隧道链路的长度修改成特定值
- 使用 tunnel ttl 命令进行设置。

检验方法

- 使用 **show interfaces tunnel** 命令查看是否成功设置。

相关命令

配置传输网络 TTL

【命令格式】 **tunnel ttl** *hop-limit*

【参数说明】 *hop-limit*：传输网络的跳数限制。

【命令模式】 全局模式

【使用指导】 指的是传输网络最多可以经过的路由器数目，缺省是 254。需要修改成特定值，可以使用此命令。

配置举例

配置传输网络 TTL

【配置方法】

- 配置传输网络 TTL。

```
Ruijie# configure terminal
Ruijie(config)# interface tunnel 1
Ruijie(config-if-Tunnel 1)# tunnel mode ipv6ip
Ruijie(config-if-Tunnel 1)# tunnel ttl 3
```

【检验方法】

- 检查隧道接口的配置

```
Ruijie# show interfaces tunnel 1
……
Tunnel attributes:
  Tunnel source 1.1.1.1, destination UNKNOWN, unrouteable
  Tunnel TOS/Traffic Class 0x2, Tunnel TTL 3
  Tunnel config nested limit is 0, current nested number is 0
  Tunnel protocol/transport ipv6ip
  Tunnel transport VPN is VPN1
```

常见错误

无

6.5.7 配置隧道 6rd br

配置效果

- 设置 6rd 隧道的中继路由器的 IPv4 地址 。

注意事项

- 无

配置方法

↘ 配置隧道中继路由

- 可选配置
- 在隧道接口模式下使用此命令达到。

检验方法

- 使用 **show interfaces tunnel** 命令查看是否成功配置。

相关命令

↘ 配置隧道 br 地址

【命令格式】 **tunnel 6rd br** *ipv4-address*

【参数说明】 *ipv4-address*：指定的中继路由的 IP。

【命令模式】 接口模式

【使用指导】 隧道通过 br 地址结合 6rd prefix，6rd ipv4 计算出目的 IPv4 地址。

配置举例

↘ 配置隧道 6rd br 地址。

【配置方法】
- 配置隧道 br 地址。

```
Ruijie# configure terminal
Ruijie(config)# interface tunnel 100
Ruijie(config-if-Tunnel 100)# ipv6 enable
Ruijie(config-if-Tunnel 100)# tunnel 6rd br 10.1.2.1
```

【检验方法】

- 检查隧道接口的配置。

```
Ruijie(config)#show int tunnel 1
……
Tunnel attributes:
  Tunnel source: UNKNOWN, destination UNKNOWN
  Tunnel TOS/Traffic Class not set,
  Tunnel protocol/transport ipv6ip 6rd
    6rd prefix 0.0.0.0/0
    Border relay 1.1.1.1
……
```

常见配置错误

- 无

6.5.8 配置隧道 6rd ipv4

配置效果

- 设置 6rd 隧道的 IPv4 通用前缀和通用后缀长度。

注意事项

- 配置 6rd 域的 IPv4 前缀长度和后缀长度。该命令的有效范围为 0~31，前缀加后缀总长度不能超过 31，若该命令没有配置，则默认为 0

配置方法

↘ 配置 6rd 隧道 ipv4 通用前缀和后缀

- 可选配置
- 在隧道接口模式下使用此命令达到。

检验方法

- 使用 **show interfaces tunnel** 命令查看是否成功配置。

相关命令

↘ 配置隧道 br 地址

【命令格式】 **tunnel 6rd ipv4 prefix-length** *prefix-length* **suffix-length** *suffix-length*

【参数说明】 *prefix-length*：前缀长度

suffix-length：后缀长度

【命令模式】 接口模式

【使用指导】 隧道通过 br 地址结合 6rd prefix，6rd ipv4 计算出目的 IPv4 地址。

配置举例

↘ 配置隧道 6rd ipv4。

【配置方法】
- 设置 tunnel 100 的 6rd ipv4 通用前缀和后缀长度。

```
Ruijie# configure terminal
Ruijie(config)# interface tunnel 100
Ruijie(config-if-Tunnel 100)# ipv6 enable
Ruijie(config-if-Tunnel 100)# tunnel 6rd ipv4 prefix-length 8 suffix-length 8
```

【检验方法】
- 检查隧道接口的配置。

```
Ruijie#show int tunnel 1
……
Tunnel attributes:
  Tunnel source: UNKNOWN, destination UNKNOWN
  Tunnel TOS/Traffic Class not set,
  Tunnel protocol/transport ipv6ip 6rd
    6rd prefix 0.0.0.0/0
    Border relay 1.1.1.1
    ipv4 prefix-len 16,  ipv4 suffix-len:8
  Tunnel transport VPN is no set
……
```

常见配置错误

- 无

6.5.9 配置隧道 6rd prefix

配置效果

- 设置 6rd 域的 IPv6 前缀。

注意事项

- 配置 6rd 的 IPv6 前缀。该命令为使用 6rd 的必须配置，若不配置 6rd IPv6 前缀，6rd 隧道将不能 UP，配置前缀长度为 0 等价于删除 6rd IPv6 前缀

配置方法

↘ 配置 6rd 隧道 IPv6 前缀

- 可选配置
- 在隧道接口模式下使用此命令达到。

检验方法

- 使用 **show interfaces tunnel** 命令查看是否成功配置。

相关命令

配置 6rd 隧道 IPv6 前缀

【命令格式】 **tunnel 6rd prefix** *ipv6-prefix prefix-length*

【参数说明】 *ipv6-prefix*：6rd IPv6 前缀。

prefix-length：前缀长度

【命令模式】 接口模式

【使用指导】 隧道通过 br 地址结合 6rd prefix，6rd ipv4 计算出目的 IPv4 地址。

配置举例

配置隧道 6rd ipv6 前缀

【配置方法】

- 设置 tunnel 100 的 6rd IPv6 前缀。

```
Ruijie# configure terminal
Ruijie# configure terminal
Ruijie(config)# interface tunnel 100
Ruijie(config-if-Tunnel 100)# tunnel 6rd prefix 2001:da8::/32
```

【检验方法】

- 检查隧道接口的配置。

```
Ruijie#show int tunnel 1
……
Tunnel attributes:
  Tunnel source: UNKNOWN, destination UNKNOWN
  Tunnel TOS/Traffic Class not set,
  Tunnel protocol/transport ipv6ip 6rd
    6rd prefix 32.1.0.0/64
    Border relay 1.1.1.1
    ipv4 prefix-len 16,  ipv4 suffix-len:8
  Tunnel transport VPN is no set
……
```

常见配置错误

- 无

6.5.10 配置隧道ipsec profile策略

配置效果

- 隧道封装之后的数据，采用 IPsec 进行加密，以更好的保护数据安全。

注意事项

- 无

配置方法

↘ 配置隧道 ipsec profile 策略

- 可选配置
- 在隧道接口模式下使用此命令达到。

检验方法

- 使用 **show run** 命令查看是否成功配置。

相关命令

建立 ipsec profile 策略

【命令格式】 **crypto ipsec profile** *WORD*

【参数说明】 *WORD*：策略名称。

【命令模式】 全局模式

【使用指导】 需要先建立 ipsec profile 策略，隧道才能关联策略。

交换机产品不支持隧道配置 ipsec profile 策略。

配置隧道 ipsec profile 策略

【命令格式】 **tunnel protection ipsec profile** *WORD*

【参数说明】 *WORD*：策略名称。

【命令模式】 接口模式

【使用指导】 需要先建立 ipsec profile 策略，隧道才能关联策略。

配置举例

配置隧道 ipsec profile 策略

【配置方法】

- 创建 ipsec profile 策略。

```
Ruijie# configure terminal
Ruijie(config)# crypto ipsec profile test
```

- 设置 tunnel 100 的 6rd IPv6 前缀。

```
Ruijie# configure terminal
Ruijie(config)# interface tunnel
Ruijie(config-if-Tunnel 1)# tunnel protection ipsec profile test
```

【检验方法】

- 检查隧道接口的配置。

```
Ruijie#show run int tunnel 1
Building configuration...
Current configuration : 59 bytes
!
interface Tunnel 1
 tunnel protection ipsec profile test
```

常见配置错误

- 无

6.6 监视与维护

清除各类信息

无

查看运行情况

作用	命令
查看隧道接口相关信息。	**show interfaces tunnel *number***

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
打开隧道接口的调试开关	**debug tunnel**

7 FPM

7.1 概述

FPM(Flow Platform)是报文业务处理的加速平台。由于 ip 报文具有流的属性，在业务处理 ip 报文之前，FPM 为业务提供报文的流属性识别，加速业务的处理效率。FPM 是基础平台，系统启机即加载。为了实现配置和管理 FPM，特提供了本配置命令。一般情况下，FPM 的默认配置可以满足实际需求。

下文仅介绍 FPM 的相关内容。

协议规范

无

7.2 典型应用

典型应用	场景描述
配置报文接收水线	单机作为网关设备转发报文
宽松 tcp 状态检查	AS 环境，做主备切换

7.2.1 配置报文接收水线

应用场景

在一个局域网内，当设备收到大量相同 tcp 连接请求报文，这些报文由于收不到对端的响应握手报文，而不能建立合法连接，可能是存在攻击行为。通过 FPM 配置可以限制 TCP 请求连接的报文数量，有效抵抗攻击行为。

功能部属

- 在转发设备上打开严格报文状态追踪
- 配置较小的 tcp-syn-sent 状态报文水线数

7.2.2 宽松tcp状态检查

应用场景

在设备做主备切换时，为了防止期间断流，需要配置宽松 tcp 状态检查。在配置之后，一方单发 ack 报文即可以建立连接并转发报文，使切换期间连接不断开。

功能部署

- 在备份设备上配置宽松 tcp 状态检查

7.3 基本概念

↘ 流表项

流表项是设备识别和管理所有 ip 会话连接的物理资源，在其中会记录当前 ip 会话的基本信息。主要对应的协议类型是 icmp，tcp，udp，rawip 等。

7.4 功能详解

功能特性

功能特性	作用
满流时不建流直接透传	在满流时保证不断流
流老化	回收不再有效的流表项
流允许通过报文数	防止 ip 报文洪水攻击
tcp 状态跟踪	过滤 tcp 非法连接报文
严格报文状态追踪	是否做报文水线数的检查
宽松 tcp 状态检查	是否允许 ack 报文直接建立连接

7.4.1 满流时不建流直接透传

工作原理

当前的 ip 业务做加速处理时，加速逻辑依赖于流表，流表资源是依据当前产品的硬件水平做配置的，一般情况下可以满足环境的应用需求，但是在某些极端环境下，可能会出现流表资源耗尽，不能建流的情况。为了保证业务不断流，在流表满的时候，无线产品上面会不建流，直接透传报文，业务选择执行不做加速处理的逻辑。

7.4.2 流老化

工作原理

流表项的老化是指流表项在一段时间内没有数据交换，需要主动撤消该流表项。流表老化是为了避免异常会话攻击导致系统表项爆满，正常会话无法建立而实现的。不同数据类型的流表项将根据业务的实际情况设定其老化时间；不同的业务数据类型流在其处于不同状态的情况下将设置不同的老化时间。如 TCP SYN 状态流，TCP ESTABLISH 状态流的老化时间是不同的。例如网络中存在端口扫描攻击时，会占用系统比较多的流表资源，依据这些连接建立的流的状态配置合理的老化时间，可以有效回收流表，避免断流。总之配置合理的流老化时间，使得系统流表项中减少“垃圾”表项，满足业务数据流的交换。

7.4.3 流允许通过报文数

工作原理

每个流当前状态下已处理多少报文，会有一个计数，配置相应的流状态允许通过的报文数，可以有效地解决在一种报文的大流量攻击情况下，其他报文无法及时得到处理的问题，满足业务数据流的交换。

7.4.4 tcp状态变迁检查

工作原理

一个 tcp 链接的建立需要有完整的握手过程，否则就是非法连接或者攻击报文。为了能区别对待不同状态的 tcp 会话链接建立的流及判断是否是合法链接，FPM 需要对 tcp 连接进行状态跟踪。但是在一些特殊场景下，比如非对称路由，会导致不能正常做 tcp 链接的状态跟踪，需要关闭这个功能。

7.4.5 流状态报文水线检查

工作原理

当连接建立的流处于某个状态时，一个合法的连接可能通过的报文数会有一个上限，如果通过的报文数超过这个限制，可能是存在有洪水攻击，会占用系统转发资源，所以可以通过配置流状态报文水线检查，有效防御这类攻击。

7.4.6 宽松tcp状态变迁检查

工作原理

一个合法 tcp 连接的建立需要有完整的握手过程，不过在有些情况下，比如热备的切换或者其它场景下，有可能当前的 tcp 连接已经经过握手，只是当前未有对应信息，为了应对这样的情况，需要允许 ack 报文通过，所以 FPM 提供了宽松 tcp 状态检查的命令。

7.5 配置详解

配置项	配置建议 & 相关命令	
配置 FPM 的功能	⚠ 可选配置。用于管理 FPM 的功能	
	Ip session direct-trans-disable	配置满流时不建流不能直接透传报文
	ip session timeout	配置流的老化时间
	ip session threshold	配置流状态允许接收报文水线数
	ip session tcp_state-inspection-disable	配置不做 tcp 的状态变迁检查
	ip session tcp_state-inspection-enable	配置做 tcp 的状态变迁检查
	ip session track-state-strictly	配置是否做流状态报文水线检查
	ip session tcp-loose	配置是否做宽松 tcp 的状态变迁检查

7.5.1 配置满流时不建流不能直接透传报文

配置效果

- 应对在无线产品上面开启某些特殊业务时，如 nat，其要求流平台不建流不能直接透传报文

注意事项

- 本项功能目前只在无线产品上面提供
- 系统默认满流时可以不建流直接透传报文

配置方法

- 可选配置
- 缺省情况下，是允许满流时可以不建流直接透传报文， 通过 **ip session direct-trans-disable** 关闭

【命令格式】 **ip session direct-trans-disable**

【参数说明】

【缺省配置】 缺省允许满流时可以不建流直接透传报文
【命令模式】 全局模式
【使用指导】 恢复开启状态，在相应的配置命令前加 **no** 即可

检验方法

- 通过 **show run** 查看，是否有 **ip session direct-trans-disable** 项配置，如果未有对应配置，则为系统默认的开启状态

配置举例

【网络环境】 如果需要在当前无线设备上面开启 nat 业务 ,nat 业务要求不建流不能直接透传 ip 报文 ,则需要关闭这项功能。
【配置方法】 设置设备上面关闭满流时可以不建流直接透传报文

```
Ruijie# configure terminal
Ruijie(config)# ip session direct-trans-disable
```

【检验方法】 通过 **show run** 查看，配置信息有此项 **ip session direct-trans-disable**

常见错误

-

7.5.2 配置流的老化时间

配置效果

- 可以合理利用系统流表资源，使系统流表项中减少“垃圾”表项，满足业务数据流的交换。

注意事项

- 系统初始化会有一个默认的老化时间，基本可以满足多数场景的需求，所以本配置不是必须的
- 因为系统检测到对应的流会有一定的耗时，所以实际老化时间会稍迟于配置的时间

配置方法

↘ 配置老化时间

- 可选配置

- 缺省情况下，流是按照默认时间来进行老化的，当默认的老化时间不能满足需求的时候，可以使用 **ip session timeout** 来更改对应流的老化时间，时间越大，当前流的存活时间越长。
- 在对应的转发设备上配置。

【命令格式】 **ip session timeout {icmp-closed | icmp-connected | icmp-started | rawip-closed | rawip-connected | rawip-established | rawip-started | tcp-close-wait | tcp-closed | tcp-established | tcp-fin-wait1 | tcp-fin-wait2 | tcp-syn-receive | tcp-syn-sent | tcp-syn-sent2 | tcp-time-wait | udp-closed | udp-started | udp-connected | udp-established}** { *num* }

【参数说明】 **icmp-closed：**设置协议为 ICMP 状态为关闭的流的消亡时间，默认 10s，取值范围 5 – 60
icmp-connected：设置协议为 ICMP 状态为连接的流的消亡时间，默认 10s，取值范围 5-120
icmp-started：设置协议为 ICMP 状态为开始的流的消亡时间默认 10s，取值范围 5-120
rawip-closed：设置协议为其他 ip 协议状态为连接的流的消亡时间，默认 10s，取值范围 5 - 60
rawip-connected：设置协议为其他 ip 协议状态为连接的流的消亡时间默认 300s，取值范围 10-300
rawip-established：设置协议为其他 ip 协议状态为建立的流的消亡时间默认 300s，取值范围 10-600
rawip-started：设置协议为其他 ip 协议状态为开始的流的消亡时间默认 300s，取值范围 10-300
tcp-close-wait：设置协议为 TCP 状态为 tcp-close-wait 的流的消亡时间默认 60s，取值范围 10-120
tcp-closed：设置协议为 TCP 状态为 tcp-closed 的流的消亡时间默认 10s，取值范围 5-20
tcp-established：设置协议为 TCP 状态为 tcp-established 的流的消亡时间默认 1800s ,取值范围 300-604800
tcp-fin-wait1：设置协议为 TCP 状态为 tcp-fin-wait1 的流的消亡时间默认 60s，取值范围 10-120
tcp-fin-wait2：设置协议为 TCP 状态为 tcp-fin-wait2 的流的消亡时间默认 60s，取值范围 10-120
tcp-syn-sent：设置协议为 TCP 状态为 tcp-syn-sent 的流的消亡时间默认 10s，取值范围 5-30
tcp-syn_sent2：设置协议为 TCP 状态为 tcp-syn_sent2 的流的消亡时间默认 10s，取值范围 5-30
tcp-syn-receive：设置协议为 TCP 状态为 tcp-syn-receive 的流的消亡时间默认 10s，取值范围 5-30
tcp-time-wait：设置协议为 TCP 状态为 tcp-time-wait 的流的消亡时间默认 10s，取值范围 5-60
udp-closed： 设置协议为 UDP 状态为关闭的流的消亡时间，默认 10s，取值范围 5 - 60
udp-connected：设置协议为 UDP 状态为连接的流的消亡时间默认 30s，取值范围 10-300
udp-established：设置协议为 UDP 状态为建立的流的消亡时间默认 600s，取值范围 120-600
udp-started：设置协议为 UDP 状态为开始的流的消亡时间默认 10s，取值范围 10-300
num：设置的消亡时间

【缺省配置】 缺省使用默认值。

【命令模式】 全局模式

【使用指导】 恢复默认时间，在相应的配置命令前加 **no** 即可

检验方法

- 通过 **show run** 查看，是否有 **ip session timeout** 配置，如果未有对应配置，则为系统默认的老化时间

配置举例

【网络环境】 如果发现当前的转发设备上面有很多 udp established 状态的流占用大量流表，可以通过减小此状态的流的老

化时间，提供老化效率。

【配置方法】 如果当前转发设备为 FW 卡，其位于设备 1，槽号 2 的位置上面，设置其 udp established 状态的流消亡时间为 120s

```
Ruijie# configure terminal
Ruijie(config)# ip session 1 2 timeout udp-established 120
```

【检验方法】 检查设备 1 槽号为 2 的设备上面的 udp established 状态的流的消亡时间约为 120s

通过 **show run** 查看，配置有此项：

```
ip session 1 2 timeout udp-established 120
```

则相应的状态老化时间为 120s

常见错误

-

7.5.3 配置流允许通过报文数

配置效果

- 可以有效地解决在一种报文的大流量攻击情况下，其他报文无法及时得到处理的问题，满足业务数据流的交换。

注意事项

- 系统初始化会有一个默认的允许报文数，基本可以满足多数场景的需求，所以本配置不是必须的
- 本项检查默认不开启，如果需要开启检查，需要系统有配置流状态报文水线检查

配置方法

- 可选配置。
- 缺省情况下，流是按照默认允许数来进行判断的，当默认允许通过报文数不能满足需求的时候，可以使用 **ip session threshold** 来更改对应流的允许通过报文数，数值越大，允许通过的报文越多。
- 在每台需要配置的转发设备上做相应配置。

【命令格式】 **ip session threshold** {icmp-closed | **icmp-started** | rawip-closed | **tcp-syn-sent | tcp-syn-receive** | **tcp-closed | udp-closed** } { *num* }

【参数说明】 **icmp-closed** ：设置协议为 ICMP 状态为关闭的流的报文通过数，默认 10，取值范围 1 - 2000000000

icmp-started：设置协议为 ICMP 状态为开始的流的报文通过数，默认 300，取值范围 5-2000000000

rawip-closed：**设置协议为其它 ip 协议状态为关闭的流的报文通过数，默认 10，**取值范围 1 - 2000000000

tcp-syn-sent：设置协议为 TCP 状态为 syn-send 的流的报文通过数，默认 10，取值范围 5-2000000000

tcp-syn-receive：设置协议为 TCP 状态为 syn-receive 的流的报文通过数 默认 20 取值范围 5-2000000000

tcp-closed：设置协议为 TCP 状态为 closed 的流的报文通过数，默认 20，取值范围 5-2000000000

udp-closed：设置协议为 UDP 状态为关闭的流的报文通过数，默认 10，取值范围 **1 - 2000000000**

num：设置的报文通过数

【命令模式】 全局模式

【使用指导】 恢复默认允许通过报文数，在相应的配置命令前加 **no** 即可

检验方法

- **通过 show run** 查看，是否有 **ip session threshold** 配置，如果未有对应配置，则为系统默认允许通过报文数

配置举例

【网络环境】 如果网络中存在有大量的 ping 报文洪水攻击，可以配置降低 icmp-start 状态通过的报文水线数，以拒绝这类报文大量通过。

【配置方法】 如果当前转发设备为 fw 卡，其位于设备 1，槽号 2 的位置上面，设置其 **icmp-started** 状态的流报文通过数为 10

```
Ruijie# configure terminal
Ruijie(config)# ip session
threshold icmp-started 10
```

【检验方法】 检查

设备上面的 icmp startd 状态的流报文允许通过数为 10

通过 **show run** 查看，配置有此项：

```
ip session
threshold icmp-started 10
```

则相应状态允许通过报文数为 10

常见错误

-

7.5.4 配置关闭tcp状态变迁检查

配置效果

- 应对特殊场景下，比如非对称路由，所导致不能正常做 tcp 连接状态跟踪引起的问题。

注意事项

- 关闭 tcp 的状态变迁检查，会使 FPM 工作在非正常状态，有些基于 FPM 状态变迁的业务功能可能会不正常，请谨慎配置关闭此项功能。

- 系统默认开启 tcp 状态变迁检查。

配置方法

- 可选配置
- 缺省情况下，是开启 tcp 状态追踪的， 可以通过 **ip session**

  tcp-state-inspection-disable 关闭
- 如果场景需要关闭 tcp 的状态跟踪，比如存在非对称路由，需要在每台需要配置的转发设备上做相应配置。

【命令格式】 **ip session**
tcp-state-inspection-disable

【参数说明】

【缺省配置】 缺省开启 TCP 状态跟踪

【命令模式】 全局模式

【使用指导】 恢复开启状态，在相应的配置命令前加 **no** 即可

检验方法

- 通过 **show run** 查看，是否有 **ip session tcp-state-inspection-disable** 项配置，如果未有对应配置，则为系统默认的开启状态

配置举例

【网络环境】 如果当前转发设备为 FW 卡，其位于设备 1，槽号 2 的位置上面，如果当前转发环境中，FW 卡位于非对称路由路径中，则需要关闭 tcp 状态变迁检查。

【配置方法】 设置设备 1 槽号为 2 的转发设备上面关闭 tcp 的状态跟踪

```
Ruijie# configure terminal
Ruijie(config)# ip session
tcp-state-inspection-disable
```

【检验方法】 通过 **show run** 查看，配置信息有此项 **ip session tcp-state-inspection-disable**

常见错误

-

7.5.5 配置开启tcp状态变迁检查

配置效果

- 应对无线产品需要开启 tcp 状态跟踪的需求。

注意事项

- 无线产品默认关闭 tcp 状态变迁检查。

配置方法

- 可选配置
- 缺省情况下，无线产品是关闭 tcp 状态变迁检查的， 通过 **ip session tcp-state-inspection-enable** 开启

【命令格式】 **ip session tcp-state-inspection-enable**
【参数说明】
【缺省配置】 缺省关闭 TCP 状态变迁检查
【命令模式】 全局模式
【使用指导】 恢复关闭状态，在相应的配置命令前加 **no** 即可

检验方法

- 通过 **show run** 查看，是否有 **ip session tcp-state-inspection-enable** 项配置，如果未有对应配置，则为系统默认的关闭状态

配置举例

【网络环境】 如果当前无线转发设备需要开启 tcp 状态变迁检查的功能。
【配置方法】 设置设备上面开启 tcp 的状态跟踪

```
Ruijie# configure terminal
Ruijie(config)# ip session tcp-state-inspection-enable
```

【检验方法】 通过 **show run** 查看，配置信息有此项 **ip session tcp-state-inspection-enable**

常见错误

-

7.5.6 配置流状态报文水线检查

配置效果

- 本配置主要是使能报文水线的检查及在报文不可达时关闭当前流

注意事项

-

配置方法

- 可选配置
- 可以通过 **ip session**

  track-state-strictly 开启严格报文状态追踪
- 如果场景需要开启报文的水线检查，例如当前存在某种报文的攻击，需要在每台转发设备上做相应配置。

【命令格式】 **ip session track-state-strictly**
【参数说明】
【缺省配置】 关闭严格报文状态追踪
【命令模式】 全局模式
【使用指导】 恢复默认配置，在相应的配置命令前加 no 即可

检验方法

- 通过 **show run** 查看，是否有 **ip session track-state-strictly** 项配置，如果未有对应配置，则为系统默认的关闭状态

配置举例

【网络环境】 如果当前网络环境中存在有 icmp 洪水攻击，需要做报文水线检查，则打开本配置。
【配置方法】 如果当前转发设备为 FW 卡，其位于设备 1，槽号 2 的位置上面，设置在当前转发设备上面严格报文状态追踪

```
Ruijie# configure terminal
Ruijie(config)# ip session
track-state-strictly
```

【检验方法】 通过 **show run** 查看，配置信息有此项 **ip session track-state-strictly**

常见错误

-

7.5.7 配置宽松tcp状态变迁检查

配置效果

- 可以允许 ack 报文可以直接建流。

注意事项

- FW 产品上面默认是不允许 ack 报文直接建流，EG 产品默认是允许 ack 报文直接建流。
- 当前配置非必须。

配置方法

- 可选配置。
- 缺省情况下，FW 产品是关闭宽松 tcp 状态检查的， 可以通过 **ip session tcp-loose** 开启。无线及 EG 产品都是默认打开宽松 tcp 状态检查的
- 如果场景需要配置，例如系统在做热备切换，需要在备机上开启本配置。

【命令格式】 **ip session tcp-loose**
【参数说明】
【命令模式】 全局模式
【使用指导】 恢复默认配置，在相应的配置命令前加 no 即可

检验方法

- 通过 **show run** 查看，是否有此项配置 **ip session tcp-loose，**如果未有对应配置，则为非宽松状态

配置举例

【网络环境】 如果当前作为备份设备的 FW 卡位于设备 1，槽号 2 的位置上面，当前环境需要做主备切换，需要在备份设备上面打开这项配置。
【配置方法】 设置设备 1 槽号为 2 的设备上面的宽松 tcp 状态检查

```
Ruijie# configure terminal
Ruijie(config)# ip session
tcp-loose
```

【检验方法】 通过 **show run** 查看，配置信息有此项 **ip session tcp-loose**

常见错误

-

7.6 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 FPM 处理 ipv4 报文计数	**clear ip fpm counters**

查看运行情况

作用	命令
查看 FPM 处理 ipv4 报文计数	**show ip fpm**
查看 ipv4 报文的流信息	**show ip fpm**
查看 ipv4 流统计信息	**show ip fpm statistics**

8 NAT

8.1 概述

NAT（Network Address Translation，网络地址转换）是将 IP 数据包头中的 IP 地址转换为另一个 IP 地址的过程。在实际应用中，NAT 主要用于实现私有网络访问公共网络的功能。这种通过使用少量的公有 IP 地址代表较多的私有 IP 地址的方式，将有助于减缓可用 IP 地址空间的枯竭。

下文仅介绍 NAT 的相关内容。

协议规范

- RFC 1631：The IP Network Address Translator (NAT)
- RFC 2663：IP Network Address Translator (NAT) Terminology and Considerations
- RFC 2391：Load Sharing using IP Network Address Translation (LSNAT)
- RFC 4008：Definitions of Managed Objects for Network Address Translators (NAT)

8.2 典型应用

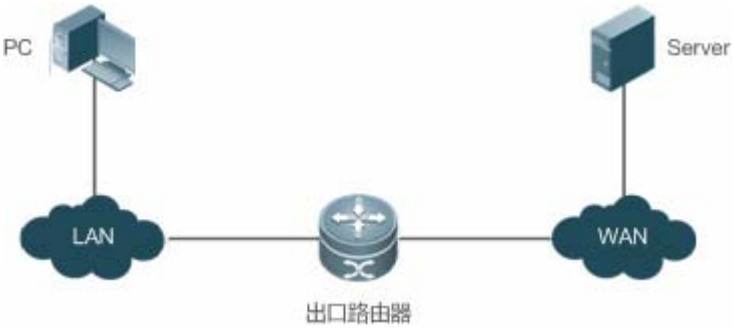
典型应用	场景描述
内网用户访问互联网服务	当内部网络需要与互联网网络通讯时，需要配置 NAT，将内部私有 IP 地址转换成全局唯一 IP 地址。
外部用户访问内网服务器	利用设备将一个或者多个内部主机映射成网络服务器，从而使得外部网络上的网络用户可以获得对应的服务。
内部用户源目的地址转换	两个需要互联的私有网络分配了同样 IP 地址，或者一个私有网络和公有网络分配了同样的全局 IP 地址，两个重叠地址的网络主机之间是不可能通信的，配置了重叠地址 NAT，外部网络主机地址在内部网络表现为另一个网络主机地址，反之一样。
内网服务器负载均衡	当内部网络某台主机 TCP 流量负载过重时，可用多台主机进行 TCP 业务的均衡负载。这时，可以考虑用 NAT 来实现 TCP 流量的负载均衡。

8.2.1 内网用户访问互联网服务

应用场景

以下图为例，PC 位于内网，某服务器位于外网。但由于 IP 地址即将耗尽的问题，整个园区网只分配了一个或者几个外网 IP 地址。出口路由器属于内网，用于连接外网。内网 PC 要访问到外网服务器，需要在出口路由器上开启基本 NAT 功能。

图 8-1



【注释】 出口路由器分别与内网和外网相连

功能部属

- 在内外网口配置 NAT 接口
- 出口网关上配置内部源地址静态地址转换

8.2.2 外部用户访问内网服务器

应用场景

以下图为例，PC 位于外网，某服务器(如 web 服务器)位于内网。但由于 IP 地址即将耗尽的问题，整个园区网只分配了一个外网 IP 地址。出口路由器属于内网，用于连接外网。PC 要访问到内网的服务器，需要在出口路由器上开启 NAPT 功能，即针对 web 服务提供的端口进行的端口映射。

图 8-2



【注释】 出口路由器分别与内网和外网相连
内网部署服务器

功能部属

- 在内外网口配置 NAT 接口

- 出口网关上配置服务器端口地址转换规则

8.2.3 内部用户源目的地址转换

应用场景

以下图为例，PC1 位于私网 1，PC2 位于私网 2。由于 2 个私网以前是单独管理，所以，2 个私网的 IP 地址网段发生了地址重叠，如 PC1 和 PC2 都配置成在 192.168.1.0/24 网段。出口路由器位于私网 1 和私网 2 之间。PC1 和 PC2 要实现实现互访，需要在出口路由器上开启重叠地址 NAT 功能。

图 8-3



【注释】 出口路由器分别与私网 1 和私网 2 相连

功能部属

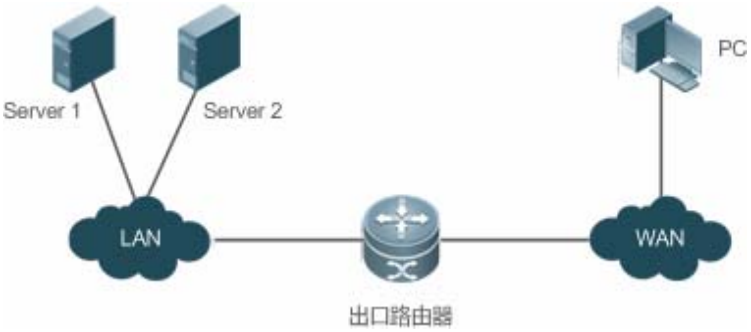
- 在内外网口配置 NAT 接口
- 出口网关上配置内部源地址动态地址转换
- 出口网关上配置外部源地址动态地址转换

8.2.4 内网服务器负载均衡

应用场景

以下图为例，服务器 1 和服务器 2 位于内网，2 台服务器形成集群。PC 位于外网。但由于 IP 地址即将耗尽的问题，整个园区网只分配了一个外网 IP 地址。出口路由器属于内网，用于连接外网。出口路由器要将外网访问服务器的流量分担在 2 台服务器上，需要在出口路由器上开启 NAT 负载均衡功能。

图 8-4



【注释】 出口路由器分别与内网和外网相连
内网部署服务器

功能部属

- 在内外网口配置 NAT 接口
- 出口网关上配置 TCP 负载均衡地址转换

8.3 功能详解

基本概念

私有网络地址和公有网络地址

私有网络地址，是指内部网络或主机的 IP 地址，公有网络地址，是指在互联网上全球唯一的 IP 地址。IANA(Internet Assigned Number Authority)规定将下列的 IP 地址保留用作私有网络地址，不在 Internet 上被分配，可在任何单位或公司内部使用。

A 类私有地址：10.0.0.0~10.255.255.255

B 类私有地址：172.16.0.0~172.31.255.255

C 类私有地址：192.168.0.0~192.168.255.255

NAT 最初的设计目的是用于实现私有网络访问公共网络的功能，后扩展到实现任意两个网络间进行访问时的地址转换应用，本文中将这两个网络分别称为内部网络（内网）和外部网络（外网），通常私网为内部网络，公网为外部网络。

静态 NAT

静态 NAT 是建立内部本地地址和内部全局地址的一对一永久映射。当外部网络需要通过固定的全局可路由地址访问内部主机，静态 NAT 就显得十分重要。

动态 NAT

动态 NAT，是建立内部本地地址和内部全局地址池的临时映射关系，过一段时间没有用就会删除映射关系。当内部网络只访问外网服务，不提供信息服务的主机，内部网络主机数大于全局 IP 地址数时，可以配置动态 NAT。

功能特性

功能特性	作用
基本 NAT	内部私有地址转换成公网可以识别的地址，实现互通
NAPT	可以将多个内部本地地址映射到一个内部全局地址，解决 IP 地址枯竭问题
重叠地址 NAT	重叠私有网络的互相访问
TCP 负载均衡	该功能可以解决某台主机 TCP 流量过载的问题
构建本地服务器	构建本地服务器，以供外部网络的访问
ALG	由于 NAT 只会修改 IP 报文头部，不会去修改应用协议的载荷，引入 ALG，用于支持应用层协议

8.3.1 基本NAT

当内部网络需要与外部网络通讯时，需要配置 NAT，将内部私有 IP 地址转换成全局唯一 IP 地址。可以配置静态或动态的 NAT 来实现互联互通的目的，或者需要同时配置静态和动态的 NAT。

工作原理

3. 内网用户主机（192.168.1.2）向外网服务器（8.8.8.8）发送的 IP 报文通过 NAT 设备。
4. NAT 设备查看报头内容 ,发现该报文是发往外网的 ,将其源 IP 地址字段的的私网地址 192.168.1.2 转换成一个可在 Internet 上选路的公网地址 30.1.1.1，并将该报文发送给外网服务器，同时在 NAT 设备的网络地址转换表中记录这一映射。
5. 外网服务器给内网用户发送的应答报文(其初始目的 IP 地址为 30.1.1.1)到达 NAT 设备后 ,NAT 设备再次查看报头内容，然后查找当前网络地址转换表的记录，用内网私有地址 192.168.1.2 替换初始的目的 IP 地址。

上述的 NAT 过程对终端（如图中的 Host 和 Server）来说是透明的。对外网服务器而言，它认为内网用户主机的 IP 地址就是 30.1.1.1，并不知道有 192.168.1.2 这个地址。因此，NAT “隐藏” 了企业的私有网络。

基本 NAT 包括静态 NAT、动态 NAT。

相关配置

配置 NAT 接口

- 缺省情况下，接口上未执行为 NAT 接口。
- 使用 **ip nat { inside | outside }**命令指定一对 NAT 接口。
- 数据包只有在 outside 接口和 inside 接口之间路由时，并且符合一定规则的，才会进行 NAT 转换。因此必须配置至少一个 inside 接口和一个 outside 接口。

配置静态 NAT

- 缺省情况下，没配置静态 NAT 信息。

- 使用 **ip nat inside source static***local-address global-address* [**permit-inside**] [**netmask** *mask*] [**match** *interface*] [**description** *description-text*]命令可以配置静态一对一 NAT 映射。

配置动态 NAT

- 缺省情况下，没配置动态 NAT 信息。
- 使用 **ip nat inside source list** *access-list-number* **pool***address-pool* [**description** *description-text*]命令可以配置动态 NAT 映射。

8.3.2 NAPT

传统的 NAT 一般是指一对一的地址映射，不能同时满足所有的内部网络主机与外部网络通讯的需要。比如内网缺乏全局 IP 地址 ,甚至没有专门申请全局 IP 地址 ,只有一个连接 ISP 的全局 IP 地址 ,内网要求上网的主机数很多的场景下 ,需要使用 NAPT。

使用 NAPT(网络地址端口转换)，可以将多个内部本地地址映射到一个内部全局地址。

工作原理

NATP,也称之为”多对一地址转换”，它允许多个内部地址映射到同一个公有地址上。NAPT 同时映射 IP 地址和端口号：来自不同内部地址的数据报文的源地址可以映射到同一外部地址，但它们的端口号被转换为该地址的不同端口号，因而仍然能够共享同一地址，也就是“私网 IP 地址＋端口号”与“公网 IP 地址＋端口号”之间的转换。

静态 NAPT

静态 NAPT 一般应用在将内部网指定主机的指定端口映射到全局地址的指定端口上。而前一小节提及的静态 NAT，是将内部主机映射成全局地址。静态 NAPT 适用于内网有提供信息服务的主机，它提供是永久的一对一“IP 地址+端口”映射关系。

动态 NAPT

动态 NAPT 适用于内网只访问外网服务，不提供信息服务的主机。它提供的是临时的一对一”IP 地址+端口”映射关系。

相关配置

配置 NAT 接口

- 缺省情况下，接口上未执行为 NAT 接口。
- 使用 **ip nat** { **inside | outside** }命令指定一对 NAT 接口。
- 数据包只有在 outside 接口和 inside 接口之间路由时，并且符合一定规则的，才会进行 NAT 转换。因此必须配置至少一个 inside 接口和一个 outside 接口。

配置静态 NAPT

- 缺省情况下，没配置静态 NAPT 信息。
- 使用 ip nat inside source static local-ip local-port global-ip global-port [permit-inside] [description description-text]命令可以配置静态一对一 NAPT 映射。

配置动态 NAPT

- 缺省情况下，没配置动态 NAPT 信息。
- 使用 **ip nat inside source list***access-list-number* { [**pool** *address-pool*] | [**interface***interface-type interface-number*] } **overload** [description description-text]命令可以配置动态 NAT 映射。对于 NAPT，一般地址池就定义一个 IP 地址，一个地址最多可以提供 64512 个 NAT 地址转换。如果地址不够，地址池可以多定义几个地址。

8.3.3 重叠地址NAT

两个需要互联的私有网络分配了同样 IP 地址，或者一个私有网络和公有网络分配了同样的全局 IP 地址，这种情况称为地址重叠。两个重叠地址的网络主机之间是不可能通信的，因为它们相互认为对方的主机在本地网络。重叠地址 NAT 就是专门针对重叠地址网络之间通信的问题，配置了重叠地址 NAT，外部网络主机地址在内部网络表现为另一个网络主机地址，反之一样。

工作原理

内部网络和外部网络重叠 IP 地址互访，NAT 必须将内部地址转换成唯一的外部地址，同时还需要将与内部重叠的外部地址转换成内部唯一地址，从而实现互访。

相关配置

配置 NAT 接口

- 缺省情况下，接口上未执行为 NAT 接口。
- 使用 **ip nat** { **inside | outside** }命令指定一对 NAT 接口。
- 数据包只有在 outside 接口和 inside 接口之间路由时，并且符合一定规则的，才会进行 NAT 转换。因此必须配置至少一个 inside 接口和一个 outside 接口。

配置内部源地址转换

- 缺省情况下，没配置内部源地址转换。
- 内部源地址转换，可以使用静态/动态基本 NAT 或者静态/动态 NAPT，详细见“基本 NAT”和“NAPT”章节。

配置外部源静态地址转换

- 缺省情况下，没配置外部源地址转换信息。
- 使用 **ip nat outside source static***global-address local-address* 命令可以配置外部源地址静态 NAT 转换。

配置外部源动态地址转换

- 缺省情况下，没配置外部源动态转换信息。
- 使用 **ip nat outside source list***access-list-number***pool***address-pool* 命令可以外部源地址动态 NAT 转换。

配置访问控制列表

- 缺省情况下，无访问控制列表的配置。
- 使用 **ip access-list {extended | standard}** **{***id* | *name***}**或者 **access-list** 命令配置合适的访问控制列表。

配置静态路由

- 必须配置。
- 使用 **ip route***networknet-mask* {*ip-address* | *interface* [*ip-address*]} [*distance*] [**tag** *tag*] [**permanent | track** *object-number*] [**weight** *number*] [**description***description-text*] [**disabled** | **enabled**] [**global**]命令配置静态路由，用于指定内部目的地址转换后网络的出口。

8.3.4 TCP负载均衡

当内部网络某台主机 TCP 流量负载过重时，可用多台主机进行 TCP 业务的均衡负载。这时，可以考虑用 NAT 来实现 TCP 流量的负载均衡。

工作原理

NAT 创建了一台虚拟主机提供 TCP 服务，该虚拟主机对应内部多台实际的主机，然后对目标地址进行轮询置换，达到负载分流的目的。

相关配置

配置 NAT 接口

- 缺省情况下，接口上未执行为 NAT 接口。
- 使用 **ip nat** { **inside | outside** }命令指定一对 NAT 接口。
- 数据包只有在 outside 接口和 inside 接口之间路由时，并且符合一定规则的，才会进行 NAT 转换。因此必须配置至少一个 inside 接口和一个 outside 接口。

配置地址池

- 缺省情况下，没配置地址池。
- 使用 **ip nat pool** *address-pool start-address end-address* { **netmask** *mask* | **prefix-length** *prefix-length* }配置转换的 IP 地址池。

配置 ACL

- 缺省情况下，没配置 ACL。
- 使用 **access-list** *access-list-number* **permit** *ip-address wildcard* 命令可以配置目标 IP 的扩展 ACL。注意 ACL 必须配置为匹配目标 IP 的扩展 ACL。

配置内部目的地址转换

- 缺省情况下，没配置内部目的地址转换。
- 使用 **ip nat inside destination list***access-list-number***pool** *address-pool* [description description-text]命令可以配置内部目的地址转换。上述配置，只对 TCP 流量产生作用，对其它流量保持不变，除非有另外的 NAT 配置。

8.3.5 构建本地服务器

用户在内部网内设置了三台服务器(FTP 服务器、WEB 服务器以及 E-MAIL 服务器)，希望广域网上的网络主机能够访问这三个服务器。同时内部网的普通用户可以把网关设置成设备来访问 Internet。

工作原理

把内部一个或者多个内部主机映射成网络服务器，从而使得广域网上的网络用户可以获得对应的服务。

相关配置

↘ 配置 NAT 接口

- 缺省情况下，接口上未执行为 NAT 接口。
- 使用 **ip nat** { **inside | outside** }命令指定一对 NAT 接口。
- 数据包只有在 outside 接口和 inside 接口之间路由时，并且符合一定规则的，才会进行 NAT 转换。因此必须配置至少一个 inside 接口和一个 outside 接口。

↘ 配置内部地址端口转换

- 缺省情况下，没配置内部地址端口转换。
- 使用 **ip nat inside source static** { **udp** | **tcp** } **local-address port global-address port** [**permit-inside**] [description description-text]转换内部特定地址和端口，用专属的端口提供对应的服务，比如用 tcp 协议的 20，21 端口构建 ftp 服务器，用 tcp 协议的 80 端口构建 web 服务等
- 当内部有多个服务器且对应的端口是连续的，可通过配置 **ip nat inside source static** { **udp** | **tcp** } **local-address {port-range} port1 port2 global-address {port-range} port3 port4** [**permit-inside**] [description description-text] 转换内部特定地址和多个端口，用专属的多个端口提供对应的服务，比如用 tcp 协议的 20，21 端口构建 ftp 服务器等。

8.3.6 ALG

普通 NAT 实现了对 UDP 或 TCP 报文头中的的 IP 地址及端口转换功能，但对应用层数据载荷中的字段无能为力，在许多应用层协议中，比如多媒体协议（H.323 等）、FTP、SQLNET 等，TCP/UDP 载荷中带有地址或者端口信息，这些内容不能被 NAT 进行有效的转换，就可能导致问题。ALG（Application Level Gateway，应用层网关）

工作原理

ALG（Application Level Gateway，应用层网关）技术能对多通道协议进行应用层报文信息的解析和地址转换，将载荷中需要进行地址转换的 IP 地址和端口或者需特殊处理的字段进行相应的转换和处理，从而保证应用层通信的正确性。NAT 默认开启所有 ALG。当前支持的 ALG 的协议有：dns、ftp、h323、pptp、tftp、rtsp 以及 sip。

相关配置

开启关闭 ALG

- 缺省情况下，开启所有 ALG。
- 使用 **no ip nat translation dns** 命令关闭 DNS ALG。
- 使用 **no ip nat translation ftp** 命令关闭 FTP ALG。
- 使用 **no ip nat translation h323** 命令关闭 H323 ALG。
- 使用 **no ip nat translation pptp** 命令关闭 PPTP ALG。
- 使用 **no ip nat translation tftp** 命令关闭 TFTP ALG。
- 使用 **no ip nat translation rtsp** 命令关闭 RTSP ALG。
- 使用 **no ip nat translation sip** 命令关闭 SIP ALG。

8.4 配置详解

配置项	配置建议 & 相关命令	
配置基本 NAT	⚠ 必须配置。用于内部 PC 连接大网的一对一 NAT 转换	
	ip nat inside	定义该接口连接内部网络
	ip nat inside	定义该接口连接外部网络
	⚠ 可选配置。用于静态 NAT 地址转换	
	ip nat inside source static *local-address global-address* [**permit-inside**] [**netmask***mask*] [**match** interface] [description description-text]	定义内部源地址静态转换关系。
	⚠ 可选配置。用于动态 NAP 地址转换。	

	ip nat pool *address-pool start-address end-address* { **netmask** *mask* | **prefix-length** *prefix-length* } 或者 **ip nat pool** *pool-name* { **netmask** *netmask* | **prefix-length** *prefix-length* } [**type rotary**] **address** *start-ip end-ip* [**match interface** *interface*]	定义全局 IP 地址池，对于 NAT，一般就定义多个 IP 地址，根据内网用户数定义地址池个数。
	access-list *ccess-list-number* **permit** *ip-address wildcard*	定义访问列表，只有匹配该列表的地址才转换。
	ip nat inside source list *access-list-number* { [**pool** *address-pool*] | [**interface** *interface-type interface-number*] } **overload** [description description-text]	定义源地址动态转换关系 ,overload 有和没有是一样的效果，仅是兼容主流厂商的配置。
配置 NAPT	⚠ 必须配置。用于实现 NAPT	
	ip nat inside	定义该接口连接内部网络
	ip nat outside	定义该接口连接外部网络
	⚠ 可选配置。用于静态 NAPT 地址转换。	
	ip nat inside source static { **UDP** *local-address port* | **TCP** *local-address port* } *global-address port* [**permit-inside**] [description description-text]	定义内部源地址静态转换关系。
	⚠ 可选配置。用于动态 NAPT 地址转换。	
	ip nat pool *address-pool start-address end-address* { **netmask** *mask* | **prefix-length** *prefix-length* }	定义全局 IP 地址池，对于 NAPT，一般就定义一个 IP 地址。
	access-list *ccess-list-number* **permit** *ip-address wildcard*	定义访问列表，只有匹配该列表的地址才转换。
	ip nat inside source list *access-list-number* { [**pool** *address-pool*] | [**interface** *interface-type interface-number*] } **overload** [description description-text]	定义源地址动态转换关系 ,overload 有和没有是一样的效果，仅是兼容主流厂商的配置。

配置重叠地址 NAT	必须配置。用于配置重叠地址 NAT。	
	ip nat inside	定义该接口连接内部网络
	ip nat outside	定义该接口连接外部网络
	ip nat inside source static *local-address global-address* [description description-text]	内部源地址转换配置
	⚠ 可选配置。用于静态地址转换	
	ip nat outside source static *global-address local-address*	静态 NAT 配置
	⚠ 可选配置。用于动态地址转换。	
	ip nat pool *address-pool start-address end-address* { **netmask** *mask* | **prefix-length** *prefix-length* }	定义全局 IP 地址池。
	access-list *ccess-list-number* **permit** *ip-address wildcard*	定义访问列表，只有匹配该列表的地址才转换。
	ip nat outside source list *access-list-number* **pool** *address-pool*	定义源地址动态转换关系 ,overload 有和没有是一样的效果，仅是兼容主流厂商的配置。
配置 TCP 负载均衡	⚠ 必须配置。用于实现目标地址的轮询转换	
	ip nat inside	定义该接口连接内部网络
	ip nat outside	定义该接口连接外部网络
	ip nat pool *address-pool start-address end-address* { **netmask** *mask* | **prefix-length** *prefix-length* }	定义 IP 地址池，包含所有实际主机地址。
	access-list *access-list-number* **permit** *ip-address wildcard*	定义访问列表，只匹配虚拟主机地址。 ⚠ 注意应该使用匹配目标 IP 的扩展 ACL。
	ip nat inside destination list *access-list-number* **pool** *address-pool*	定义内部目标地址动态转换关系。
配置 ALG	⚠ 可选配置。用于实现相关协议的 ALG	
	ip nat translation { **dns** [**ttl** *ttl_time*] **| ftp** [**port** *port_num*] **| tftp | pptp | h323 | rtsp | sip** }	定义相关协议的 ALG
配置 NAT 特殊应用	⚠ 可选配置。用于实现 NAT 特殊应用	
	ip nat application source list *list-num* **destination** *dest-ip* { **dest-change** *ip-addr* | **src-change** *ip-addr* }	定义 NAT 特殊应用规则

配置 NAT 发送免费 ARP 间隔	⚠ 可选配置。发送 NAT 本机地址免费 arp 报文的间隔	
	ip nat keepalive [*keealive_out*]	定义发送 NAT 本机地址免费 arp 报文的间隔

8.4.1 配置基本NAT

配置效果

当内部网络需要与外部网络通讯时，需要配置 NAT，将内部私有 IP 地址转换成全局唯一 IP 地址。用户可以配置静态或动态的 NAT 来实现互联互通的目的，或者需要同时配置静态和动态的 NAT。

注意事项

- 配置基本 NAT，必须配置至少一个 inside 接口和一个 outside 接口。
- 新配置的 NAT 规则，只影响新流，对旧流不影响。

配置方法

↘ 配置 NAT inside 口

- 必须配置。
- 若无特殊要求，应在连接内网的 lan 接口下配置为 NAT inside 口。

↘ 配置 NAT outside 口

- 必须配置。
- 若无特殊要求，应在连接外网的 wan 接口下配置为 NAT outside 口。

↘ 配置静态 NAT 地址转换

- 可选配置。
- 若内部网络存在少量固定用户访问外部网络时，，应在全局配置模式下配置静态 NAT 地址转换。

↘ 配置动态 NAT 地址转换

- 可选配置。
- 若内部网络存在大量用户需要访问外部网络，应在全局配置模式下配置动态 NAT 地址转换。

检验方法

无

相关命令

配置 NAT 内外网口

【命令格式】 **ip nat** { **inside | outside** }

【参数说明】 **inside**：内网口

outside：外网口

【命令模式】 接口模式

【使用指导】 数据包只有在 outside 接口和 inside 接口之间路由时，并且符合一定规则的，才会进行 NAT 转换。因此路由器必须配置至少一个 inside 接口和一个 outside 接口。

配置静态 NAT 地址转换

【命令格式】 **ip nat inside source static** *local-address global-address* [**permit-inside**] [**netmask** *mask*] [**match** *interface*] [description description-text]

【参数说明】 *local-address*：内部地址

global-address：外部地址

permit-inside：用于允许内网用户以 global-ip 访问 local-ip 的主机

netmask *mask*：网段到网段地址

match *interface*：指定出接口

description *description-text* ： 描述信息

【命令模式】 全局配置模式

【使用指导】 -

配置地址池

【命令格式】 **ip nat pool** *address-pool start-address end-address* { **netmask** *mask* | **prefix-length** *prefix-length* }

【参数说明】 *address-pool*：地址池名字

start-address：起始 IP 地址

end-address：结束 IP 地址

netmask *mask*：地址网络掩码

prefix-length *prefix-length*：地址网络掩码长度

【命令模式】 全局配置模式

【使用指导】 -

配置动态 NAT 地址转换

【命令格式】 **ip nat inside source list** *access-list-number* **pool** *address-pool* [description description-text]

【参数说明】 *access-list-number*：acl 号。

pool *address-pool*：地址池名字。

description *description-text* ： 描述信息

【命令模式】 全局模式

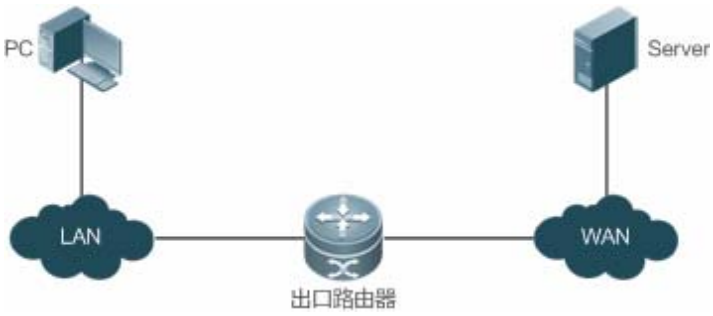
【使用指导】 -

配置举例

内网用户访问外网服务器

【网络环境】

图 8-5



【配置方法】

- 在内网口配置 ip nat inside
- 在外网口配置 ip nat outside
- 配置动态 nat 转换规则

A

```
A# configure terminal
A(config)# interface GigabitEthernet 0/0
A(config-if-GigabitEthernet 0/0)# ip address 192.168.12.1 255.255.255.0
A(config-if-GigabitEthernet 0/0)# ip nat inside
A(config-if-GigabitEthernet 0/0)# exit
A(config)# interface GigabitEthernet 0/1
A(config-if-GigabitEthernet 0/1)# ip address 200.168.12.1 255.255.255.0
A(config-if-GigabitEthernet 0/1)# ip nat outside
A(config-if-GigabitEthernet 0/1)# exit
A(config)# ip nat pool net200 200.168.12.2 200.168.12.100 netmask 255.255.255.0
A(config)# ip nat inside source list 1 pool net200
A(config)# access-list 1 permit 192.168.12.0 0.0.0.255
```

【检验方法】 显示检验。

A

```
Ruijie# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
tcp 200.168.12.200:2063 192.168.12.65:2063 168.168.12.1:23 168.168.12.1:23
```

常见错误

- Inside/outside 口没配置。
- acl 配置不对。

8.4.2 配置NAPT

配置效果

传统的 NAT 一般是指一对一的地址映射，不能同时满足所有的内部网络主机与外部网络通讯的需要。比如内网缺乏全局 IP 地址 ,甚至没有专门申请全局 IP 地址 ,只有一个连接 ISP 的全局 IP 地址 ,内网要求上网的主机数很多的场景下 ,需要使用 NAPT。

使用 NAPT(网络地址端口转换)，可以将多个内部本地地址映射到一个内部全局地址。

注意事项

- 配置 NAPT，必须配置至少一个 inside 接口和一个 outside 接口。
- 新配置的 NAT 规则，只影响新流，对旧流不影响。

配置方法

配置 NAT inside 口

- 必须配置。
- 若无特殊要求，应在连接内网的接口下配置为 NAT inside 口。

配置 NAT outside 口

- 必须配置。
- 若无特殊要求，应在连接外网的接口下配置为 NAT outside 口。

配置静态 NAPT 地址转换

- 可选配置。
- 若内部网络存在少量固定用户访问外部网络时，应在全局配置模式下配置静态 NAPT 地址转换。

配置动态 NAPT 地址转换

- 可选配置。
- 若内部网络存在大量用户需要访问外部网络时，应在全局配置模式下配置动态 NAPT 地址转换。

检验方法

无

相关命令

配置 NAT 内外网口

【命令格式】 **ip nat** { **inside | outside** }

【参数说明】 **inside**：内网口

outside：外网口

【命令模式】 接口模式

【使用指导】 数据包只有在 outside 接口和 inside 接口之间路由时，并且符合一定规则的，才会进行 NAT 转换。因此必须配置至少一个 inside 接口和一个 outside 接口。

配置静态 NAPT 地址转换

【命令格式】 **ip nat inside source static** { **udp** *local-address port* | **tcp** *local-address port* } *global-address port* [**permit-inside**] [description description-text]

【参数说明】 **udp**：udp 协议

tcp：tcp 协议

local-address：内部本地地址

port：内部本地端口

global-address：外部全局地址

port：外部全局端口

permit-inside：允许内网用户以 global-ip 访问 local-ip 的主机。

description *description-text* ： 描述信息

【命令模式】 全局配置模式

【使用指导】 该命令是用来架设内部服务器，用于外部公网访问内部服务器，除非配置 **permit-inside**，才允许内部以 *global-address* 访问该服务器,否则内网只能以 *local-address* 访问该服务器

配置地址池

【命令格式】 **ip nat pool** *address-pool start-address end-address* { **netmask** *mask* | **prefix-length** *prefix-length* }

【参数说明】 *address-pool*：地址池名字

start-address：起始 IP 地址

end-address：结束 IP 地址

netmask *mask*：地址网络掩码

prefix-length *prefix-length*：地址网络掩码长度

【命令模式】 全局配置模式

【使用指导】 -

配置动态 NAPT 地址转换

【命令格式】 **ip nat inside source list** *access-list-number* { [**pool** *address-pool*] | [**interface** *interface-type interface-number*] } **overload** [description description-text]

【参数说明】 *access-list-number*：acl 号。

pool *address-pool*：地址池名字。

interface *interface-type interface-number*：利用 outside 接口的全局地址做 NAPT。

overload: pool 中的每个全局地址都可以复用转换，就是做 NAPT。目前没有配置这个参数，全局地址也是复用。之所以添加这个参数是为了跟 cisco 的命令兼容。

description *description-text* ： 描述信息

【命令模式】 全局配置模式

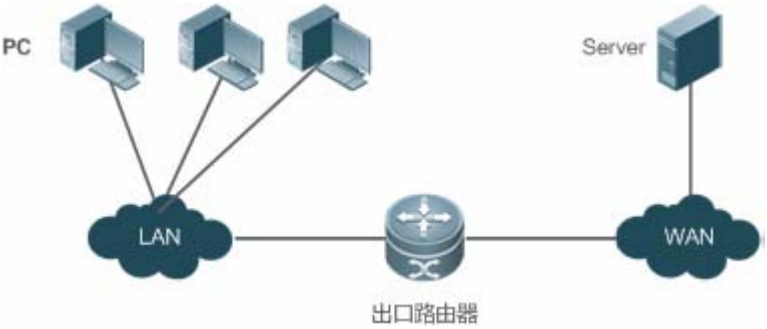
【使用指导】 -

配置举例

↘ 内网用户通过 NAPT 访问外网服务器

【网络环境】

图 8-6



【配置方法】

- 在内网口配置 ip nat inside
- 在外网口配置 ip nat outside
- 配置动态 NAPT 转换规则

A

```
A# configure terminal
A(config)# interface GigabitEthernet 0/0
A(config-if-GigabitEthernet 0/0)# ip address 192.168.12.1 255.255.255.0
A(config-if-GigabitEthernet 0/0)# ip nat inside
A(config-if-GigabitEthernet 0/0)# exit
A(config)# interface GigabitEthernet 0/1
A(config-if-GigabitEthernet 0/1)# ip address 200.198.12.1 255.255.255.0
A(config-if-GigabitEthernet 0/1)# ip nat outside
A(config-if-GigabitEthernet 0/1)# exit
A(config)# ip nat pool net200 200.168.12.1 200.168.12.1 netmask 255.255.255.0
A(config)# ip nat inside source list 1 pool net200
A(config)# access-list 1 permit 192.168.12.0 0.0.0.255
A(config)# ip nat inside source static tcp 192.168.12.3 80 200.198.12.1 80
```

【检验方法】 显示检验。

A

```
Ruijie# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
tcp 200.168.12.200:2063 192.168.12.65:2063 168.168.12.1:23 168.168.12.1:23
icmp 200.168.12.200:2064 192.168.12.66:2063 168.168.12.1:23 168.168.12.1:23
```

```
udp 200.168.12.200:2065 192.168.12.67:2063 168.168.12.1:23 168.168.12.1:23
tcp 200.168.12.200:2066 192.168.12.68:2063 168.168.12.1:23 168.168.12.1:23
tcp 200.168.12.200:2067 192.168.12.69:2063 168.168.12.1:23 168.168.12.1:23
```

常见错误

- Inside/outside 口没配置。
- acl 配置不对。

8.4.3 配置重叠地址NAT

配置效果

两个需要互联的私有网络分配了同样 IP 地址，或者一个私有网络和公有网络分配了同样的全局 IP 地址，这种情况称为地址重叠。两个重叠地址的网络主机之间是不可能通信的，因为它们相互认为对方的主机在本地网络。重叠地址 NAT 就是专门针对重叠地址网络之间通信的问题，配置了重叠地址 NAT，外部网络主机地址在内部网络表现为另一个网络主机地址，反之一样。

注意事项

- 配置重叠地址 NAT，必须先配置内部源地址 NAT 转换。
- 新配置的 NAT 规则，只影响新流，对旧流不影响。

配置方法

↘ 配置 NAT inside 口

- 必须配置。
- 若无特殊要求，应在连接内网的接口下配置为 NAT inside 口。

↘ 配置 NAT outside 口

- 必须配置。
- 若无特殊要求，应在连接外网的接口下配置为 NAT outside 口。

↘ 配置静态外部源地址转换

- 可选配置。
- 若外部网络存在少量用户需要访问内部网络时，应在全局配置模式下配置静态外部源地址转换。

↘ 配置动态外部源地址转换

- 可选配置。
- 若外部网络存在大量用户需要访问内部网络时，应在全局配置模式下配置动态外部源地址转换。

配置访问控制列表

- 使用动态源地址映射时必选。
- 该配置为限制内网需要通过源地址转换用户的范围。

配置静态路由

- 必须配置。
- 用于指定内部目的地址转换后网络的出口。

检验方法

无

相关命令

配置 NAT 内外网口

【命令格式】 **ip nat** { **inside | outside** }

【参数说明】 **inside**：内网口

outside：外网口

【命令模式】 接口模式

【使用指导】 数据包只有在 outside 接口和 inside 接口之间路由时，并且符合一定规则的，才会进行 NAT 转换。因此路由器必须配置至少一个 inside 接口和一个 outside 接口。

配置静态外部源地址转换

【命令格式】 **ip nat outside source static** *global-address local-address*

【参数说明】 *global-address*：外部全局地址

local-address：内部本地**地**址

【命令模式】 全局配置模式

【使用指导】 -

配置静态外部源地址端口转换

【命令格式】 **ip nat outside source static** { **tcp** *global-address global-port* **| udp** *global-address global-port* } *local-iaddress local-port*

【参数说明】 *protocol*：协议号

global-address：外部全局地址

global-port：外部全局端口
local-address：内部本地地址
local-port：内部本地端口

【命令模式】 全局配置模式

【使用指导】 -

配置地址池

【命令格式】 **ip nat pool** *address-pool start-address end-address* { **netmask** *mask* | **prefix-length** *prefix-length* }

【参数说明】 *address-pool*：地址池名字
start-address：起始 IP 地址
end-address：结束 IP 地址
netmask *mask*：地址网络掩码
prefix-length *prefix-length*：地址网络掩码长度

【命令模式】 全局配置模式

【使用指导】 --

配置动态外部源地址转换

【命令格式】 **ip nat outside source list** *access-list-number* **pool** *pool-name*

【参数说明】 *access-list-number*：acl 号。
pool *pool-name*：地址池名字。

【命令模式】 全局配置模式

【使用指导】 -

配置举例

以下配置举例，仅介绍静态外部源地址转换相关的配置。

静态外部源地址转换

【网络环境】
图 8-7



【配置方法】
- 在内网口配置 ip nat inside
- 在外网口配置 ip nat outside

- 配置动态内部源地址 nat 转换规则
- 配置静态外部源地址 nat 转换规则

A

```
A# configure terminal
A(config)# interface GigabitEthernet 0/0
A(config-if-GigabitEthernet 0/0)# ip address 192.168.12.1 255.255.255.0
A(config-if-GigabitEthernet 0/0)# ip nat inside
A(config-if-GigabitEthernet 0/0)# exit
A(config)# interface GigabitEthernet 0/1
A(config-if-GigabitEthernet 0/1)# ip address 200.198.12.1 255.255.255.0
A(config-if-GigabitEthernet 0/1)# ip nat outside
A(config-if-GigabitEthernet 0/1)# exit
A(config)# ip nat pool net200 200.168.12.2 200.168.12.100 netmask 255.255.255.0
A(config)# ip nat inside source list 1 pool net200
A(config)# access-list 1 permit 192.168.12.0 0.0.0.255
A(config)# ip nat outside source static 192.168.12.3 172.16.10.1
A(config)# ip route 172.16.10.0 255.255.255.0 200.198.12.2
```

【检验方法】 显示检验。

A

```
Ruijie# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
tcp 200.168.12.200:2063 192.168.12.65:2063 172.16.10.1:23 168.168.12.3:23
```

常见错误

- Inside/outside 口没配置。
- acl 配置不对。
- 未配置静态路由或者在 outside 接口配置 ip 地址，使得路由器不知道地址转换后该往哪个接口收发数据包。

8.4.4 配置TCP负载均衡

配置效果

当内部网络某台主机 TCP 流量负载过重时，可用多台主机进行 TCP 业务的均衡负载。这时，可以考虑用 NAT 来实现 TCP 流量的负载均衡。在以下的配置中，定义了一个虚拟主机地址，所有来自外部网络访问该虚拟主机的 TCP 连接，将被路由器分配到多台实际主机上，从而实现负载分流的目标。

注意事项

新配置的 NAT 规则，只影响新流，对旧流不影响。

配置方法

配置 NAT inside 口

- 必须配置。
- 若无特殊要求，应在连接内网的接口下配置为 NAT inside 口。

配置 NAT outside 口

- 必须配置。
- 若无特殊要求，应在连接外网的接口下配置为 NAT outside 口。

配置动态内部目的地址转换

- 必须配置。
- 若需要 TCP 负载均衡访问，应在全局配置模式下配置动态内部目的地址转换。

检验方法

无

相关命令

配置 NAT 内外网口

【命令格式】 **ip nat** { **inside | outside** }

【参数说明】 **inside**：内网口

outside：外网口

【命令模式】 接口模式

【使用指导】 数据包只有在 outside 接口和 inside 接口之间路由时，并且符合一定规则的，才会进行 NAT 转换。因此路由器必须配置至少一个 inside 接口和一个 outside 接口。

配置地址池

【命令格式】 **ip nat pool** *pool-name start-ip end-ip* { **netmask** *netmask* | **prefix-length** *prefix-length* } [**type rotary**]

【参数说明】 *address-pool*：地址池名字

start-address：起始 IP 地址

end-address：结束 IP 地址

netmask *mask*：地址网络掩码

prefix-length *prefix-length*：地址网络掩码长度

type rotary：NAT 地址池的类型。rotary 为轮转型，每个地址分配的概率相等。有没有配 rotary 都是轮转型。之所以引入 rotary 参数是与 cisco 命令兼容

【命令模式】 全局配置模式

【使用指导】 -

配置动态内部目的地址转换

【命令格式】 **ip nat inside destination list** *access-list-number* **pool** *address-pool* [**description** *description-text*]

【参数说明】 *access-list-number*：acl 号。

pool *pool-name*：地址池名字。

description *description-text* ： 描述信息

【命令模式】 全局配置模式

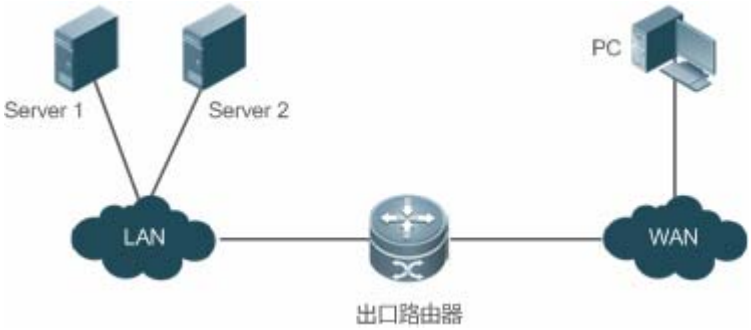
【使用指导】 -

配置举例

外网用户访问内网服务器

【网络环境】

图 8-8



【配置方法】

- 在内网口配置 ip nat inside
- 在外网口配置 ip nat outside
- 配置内部动态目的地址转换规则

A

```
A# configure terminal
A(config)# interface GigabitEthernet 0/0
A(config-if-GigabitEthernet 0/0)# ip address 10.10.10.1 255.255.255.0
A(config-if-GigabitEthernet 0/0)# ip nat inside
A(config-if-GigabitEthernet 0/0)# exit
A(config)# interface GigabitEthernet 0/1
A(config-if-GigabitEthernet 0/1)# ip address 200.198.12.1 255.255.255.0
A(config-if-GigabitEthernet 0/1)# ip nat outside
A(config-if-GigabitEthernet 0/1)# exit
A(config)# ip nat pool realhosts 10.10.10.2 10.10.10.3 netmask 255.255.255.0 type rotary
A(config)# ip nat inside destination list 100 pool realhosts
A(config)# access-list 100 permit ip any host 10.10.10.100
```

【检验方法】 显示检验。

A

```
Ruijie# show ip nat translations
Pro Inside global   Inside local    Outside local           Outside global
tcp 10.10.10.100:23 10.10.10.2:23   100.100.100.100:1178 100.100.100.100:1178
tcp 10.10.10.100:23 10.10.10.3:23   200.200.200.200:1024 200.200.200.200:1024
```

常见错误

- Inside/outside 口没配置。
- acl 配置不对。注意 ACL 必须配置为匹配目标 IP 的扩展 ACL。
- 以上配置，只对 TCP 流量产生作用，对其它流量保持不变，除非有另外的 NAT 配置

8.4.5 配置ALG

配置效果

通常情况下，NAT 只对报文头中的 IP 地址和端口信息进行转换，不对应用层数据载荷中的字段进行分析。然而一些特殊协议，比如 ftp/dns/tftp 等，它们报文的数据载荷中可能包含 IP 地址或端口信息，这些内容不能被 NAT 进行有效的转换，就可能导致问题。而 NAT ALG 技术能对多通道协议进行应用层报文信息的解析和地址转换，将载荷中需要进行地址转换的 IP 地址和端口或者需特殊处理的字段进行相应的转换和处理，从而保证应用层通信的正确性。

注意事项

- 配置 ALG，必须配置至少一个 inside 接口和一个 outside 接口。
- 新配置的 NAT 规则，只影响新流，对旧流不影响。

配置方法

配置 NAT inside 口

- 必须配置。
- 若无特殊要求，应在连接内网的 lan 接口下配置为 NAT inside 口。

配置 NAT outside 口

- 必须配置。
- 若无特殊要求，应在连接外网的 wan 接口下配置为 NAT outside 口。

配置静态 NAT 地址转换

- 可选配置。
- 若内部网络存在少量固定用户访问外部网络时，，应在全局配置模式下配置静态 NAT 地址转换。

配置动态 NAT 地址转换

- 可选配置。
- 若内部网络存在大量用户需要访问外部网络，应在全局配置模式下配置动态 NAT 地址转换。

配置 ALG

- 可选配置。
- 若环境中存在 dns、ftp、tftp、pptp、h323、rtsp 和 sip 协议需要穿透 NAT 进行通信，则需要配置。

检验方法

无

相关命令

配置 NAT 内外网口

【命令格式】 **ip nat** { **inside | outside** }

【参数说明】 **inside**：内网口

outside：外网口

【命令模式】 接口模式

【使用指导】 数据包只有在 outside 接口和 inside 接口之间路由时，并且符合一定规则的，才会进行 NAT 转换。因此路由器必须配置至少一个 inside 接口和一个 outside 接口。

配置静态 NAT 地址转换

【命令格式】 **ip nat inside source static** *local-address global-address* [**permit-inside**] [**netmask** *mask*] [**match** *interface*] [**description** *description-text*]

【参数说明】 *local-address*：内部地址

global-address：外部地址

permit-inside：用于允许内网用户以 global-ip 访问 local-ip 的主机

netmask *mask*：网段到网段地址

match *interface*：指定出接口

description *description-text* ： 描述信息

【命令模式】 全局配置模式

【使用指导】 -

配置地址池

【命令格式】 **ip nat pool** *address-pool start-address end-address* { **netmask** *mask* | **prefix-length**

prefix-length }

【参数说明】 *address-pool*：地址池名字

start-address：起始 IP 地址

end-address：结束 IP 地址

netmask *mask*：地址网络掩码

prefix-length *prefix-length*：地址网络掩码长度

【命令模式】 全局配置模式

【使用指导】 -

配置动态 NAT 地址转换

【命令格式】 **ip nat inside source list** *access-list-number* **pool** *address-pool* [**description** *description-text*]

【参数说明】 *access-list-number*：acl 号。

pool *address-pool*：地址池名字。

description *description-text* ： 描述信息

【命令模式】 全局模式

【使用指导】 -

配置 ALG

【命令格式】 **ip nat translation** { **dns** [**ttl** *ttl_time*] **| ftp** [**port** *port_num*] **| tftp | pptp | h323 | rtsp | sip** }

【参数说明】 ttl：定义 DNS 应用的 UDP 连接转换记录的超时时间。默认是 0。

port_num：定义支持 ftp 应用的端口号，默认是 21。

【命令模式】 全局模式

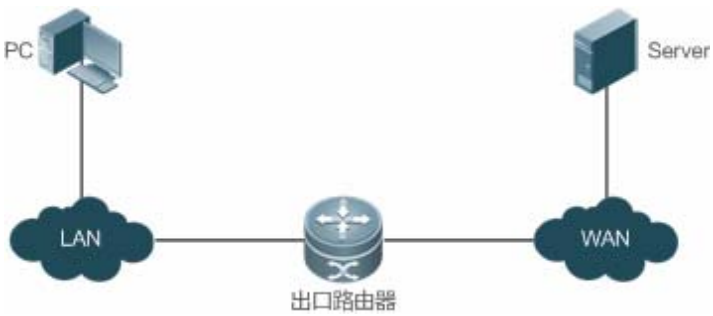
【使用指导】 -

配置举例

内网用户访问外网服务器

【网络环境】

图 8-9



【配置方法】

- 在内网口配置 ip nat inside
- 在外网口配置 ip nat outside
- 配置动态 nat 转换规则
- 配置 ALG

A

```
A# configure terminal
A(config)# interface GigabitEthernet 0/0
A(config-if-GigabitEthernet 0/0)# ip address 192.168.12.1 255.255.255.0
A(config-if-GigabitEthernet 0/0)# ip nat inside
A(config-if-GigabitEthernet 0/0)# exit
A(config)# interface GigabitEthernet 0/1
A(config-if-GigabitEthernet 0/1)# ip address 200.168.12.1 255.255.255.0
A(config-if-GigabitEthernet 0/1)# ip nat outside
A(config-if-GigabitEthernet 0/1)# exit
A(config)# ip nat pool net200 200.168.12.2 200.168.12.100 netmask 255.255.255.0
A(config)# ip nat inside source list 1 pool net200
A(config)# access-list 1 permit 192.168.12.0 0.0.0.255
A(config)# ip nat translation ftp 23
```

【检验方法】 显示检验。

A

```
Ruijie# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
tcp 200.168.12.200:2063 192.168.12.65:2063 168.168.12.1:23 168.168.12.1:23
```

常见错误

- Inside/outside 口没配置。
- acl 配置不对。

8.4.6 配置NAT特殊应用

配置效果

在一些 NAT 的高级应用场合，需要修改一些特定的 IP 报文源地址或者目的地址。

注意事项

- 配置 NAT 特殊应用，必须配置至少一个 inside 接口和一个 outside 接口。
- 新配置的 NAT 规则，只影响新流，对旧流不影响。

配置方法

↘ **配置 NAT inside 口**

- 必须配置。
- 若无特殊要求，应在连接内网的 lan 接口下配置为 NAT inside 口。

配置 NAT outside 口

- 必须配置。
- 若无特殊要求，应在连接外网的 wan 接口下配置为 NAT outside 口。

配置静态 NAT 地址转换

- 可选配置。
- 若内部网络存在少量固定用户访问外部网络时，，应在全局配置模式下配置静态 NAT 地址转换。

配置动态 NAT 地址转换

- 可选配置。
- 若内部网络存在大量用户需要访问外部网络，应在全局配置模式下配置动态 NAT 地址转换。

配置 NAT 特殊应用

- 可选配置。
- 若某些应用需要做特殊的地址转换才能进行通信，则需要配置。

检验方法

无

相关命令

配置 NAT 内外网口

【命令格式】 **ip nat** { **inside | outside** }

【参数说明】 **inside**：内网口

outside：外网口

【命令模式】 接口模式

【使用指导】 数据包只有在 outside 接口和 inside 接口之间路由时，并且符合一定规则的，才会进行 NAT 转换。因此路由器必须配置至少一个 inside 接口和一个 outside 接口。

配置静态 NAT 地址转换

【命令格式】 **ip nat inside source static** *local-address global-address* [**permit-inside**] [**netmask** *mask*] [**match** *interface*] [**description** *description-text*]

【参数说明】 *local-address*：内部地址

global-address：外部地址

permit-inside：用于允许内网用户以 global-ip 访问 local-ip 的主机
netmask *mask*：网段到网段地址
match *interface*：指定出接口
description *description-text* ： 描述信息

【命令模式】 全局配置模式
【使用指导】 -

配置地址池

【命令格式】 **ip nat pool** *address-pool start-address end-address* { **netmask** *mask* | **prefix-length** *prefix-length* }
【参数说明】 *address-pool*：地址池名字
start-address：起始 IP 地址
end-address：结束 IP 地址
netmask *mask*：地址网络掩码
prefix-length *prefix-length*：地址网络掩码长度
【命令模式】 全局配置模式
【使用指导】 -

配置动态 NAT 地址转换

【命令格式】 **ip nat inside source list** *access-list-number* **pool** *address-pool* [**description** *description-text*]
【参数说明】 *access-list-number*：acl 号。
pool *address-pool*：地址池名字。
description *description-text* ： 描述信息
【命令模式】 全局模式
【使用指导】 -

配置 NAT 特殊应用

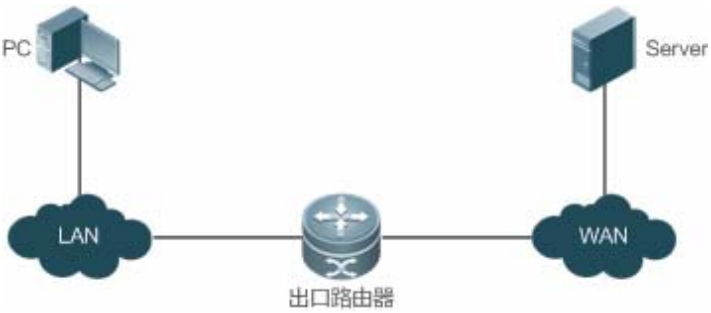
【命令格式】 **ip nat application source list** *list-num* **destination** *dest-ip* { **dest-change** *ip-addr* | **src-change** *ip-addr* }
【参数说明】 *local-address*：内部地址
global-address：外部地址
permit-inside：用于允许内网用户以 global-ip 访问 local-ip 的主机
netmask *mask*：网段到网段地址
match *interface*：指定出接口
【命令模式】 全局配置模式
【使用指导】 -

配置举例

实现域名解析中继服务

【网络环境】

图 8-10



【配置方法】

- 在内网口配置 ip nat inside
- 在外网口配置 ip nat outside
- 配置动态 nat 转换规则
- 配置 NAT 特殊应用

A

```
A#configure terminal
A(config)# interface GigabitEthernet 0/0
A(config-if-GigabitEthernet 0/0)# ip address 192.168.1.1 255.255.255.0
A(config-if-GigabitEthernet 0/0)# ip nat inside
A(config-if-GigabitEthernet 0/0)# exit
A(config)# interface GigabitEthernet 0/1
A(config-if-GigabitEthernet 0/1)# ip address 200.168.12.1 255.255.255.0
A(config-if-GigabitEthernet 0/1)# ip nat outside
A(config-if-GigabitEthernet 0/1.)# exit
A(config)# ip nat pool net200 200.168.12.2 200.168.12.10 netmask 255.255.255.0
A(config)# ip nat inside source list 1 pool net200
A(config)# access-list 1 permit 192.168.12.0 0.0.0.255
A(config)# ip nat application source list 1 destination udp 192.168.1.1 53 dest-change 202.101.98.55
53
A(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

【检验方法】 -

常见错误

- Inside/outside 口没配置。

8.4.7 配置NAT发送免费ARP间隔

配置效果

开启 NAT 地址池中的地址发送免费 ARP 报文的间隔，以防止地址冲突

注意事项

NAT 发送免费 ARP 功能默认关闭。

免费 ARP 的发送仅向外网口方向发送。

配置方法

↘ 配置 NAT inside 口

- 必须配置。
- 若无特殊要求，应在连接内网的 lan 接口下配置为 NAT inside 口。

↘ 配置 NAT outside 口

- 必须配置。
- 若无特殊要求，应在连接外网的 wan 接口下配置为 NAT outside 口。

↘ 配置静态 NAT 地址转换

- 可选配置。
- 若内部网络存在少量固定用户访问外部网络时，，应在全局配置模式下配置静态 NAT 地址转换。

↘ 配置动态 NAT 地址转换

- 可选配置。
- 若内部网络存在大量用户需要访问外部网络，应在全局配置模式下配置动态 NAT 地址转换。

↘ 配置 NAT 发送免费 ARP 间隔

- 可选配置。
- NAT 需要对部分配置规则内的地址当成本机地址，为了防止地址冲突，则需要配置。

检验方法

无

相关命令

配置 NAT 内外网口

【命令格式】 **ip nat** { **inside | outside** }

【参数说明】 **inside**：内网口

outside：外网口

【命令模式】 接口模式

【使用指导】 数据包只有在 outside 接口和 inside 接口之间路由时，并且符合一定规则的，才会进行 NAT 转换。因此路由器必须配置至少一个 inside 接口和一个 outside 接口。

配置静态 NAT 地址转换

【命令格式】 **ip nat inside source static** *local-address global-address* [**permit-inside**] [**netmask** *mask*] [**match** *interface*] [**description** *description-text*]

【参数说明】 *local-address*：内部地址

global-address：外部地址

permit-inside：用于允许内网用户以 global-ip 访问 local-ip 的主机

netmask *mask*：网段到网段地址

match *interface*：指定出接口

description *description-text* ： 描述信息

【命令模式】 全局配置模式

【使用指导】 -

配置地址池

【命令格式】 **ip nat pool** *address-pool start-address end-address* { **netmask** *mask* | **prefix-length** *prefix-length* }

【参数说明】 *address-pool*：地址池名字

start-address：起始 IP 地址

end-address：结束 IP 地址

netmask *mask*：地址网络掩码

prefix-length *prefix-length*：地址网络掩码长度

【命令模式】 全局配置模式

【使用指导】 -

配置动态 NAT 地址转换

【命令格式】 **ip nat inside source list** *access-list-number* **pool** *address-pool* [**description** *description-text*]

【参数说明】 *access-list-number*：acl 号。

pool *address-pool*：地址池名字。

description *description-text* ： 描述信息

【命令模式】 全局模式

【使用指导】 -

配置 NAT 发送免费 ARP 间隔

【命令格式】 **ip nat keepalive** [*keealive_out*]

【参数说明】 *keealive_out*：发送 nat 本机地址免费 arp 报文的间隔

【命令模式】 全局配置模式

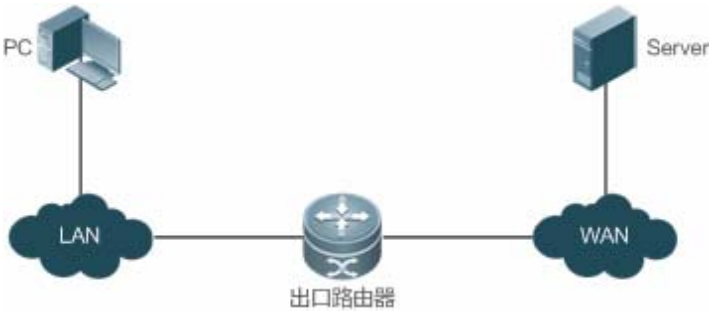
【使用指导】 -

配置举例

实现发送免费 ARP 间隔

【网络环境】

图 8-11



【配置方法】

- 在内网口配置 ip nat inside
- 在外网口配置 ip nat outside
- 配置动态 nat 转换规则
- 配置定时发送免费 ARP

A

```
A#configure terminal
A(config)# interface GigabitEthernet 0/0
A(config-if-GigabitEthernet 0/0)# ip address 192.168.1.1 255.255.255.0
A(config-if-GigabitEthernet 0/0)# ip nat inside
A(config-if-GigabitEthernet 0/0)# exit
A(config)# interface GigabitEthernet 0/1
A(config-if-GigabitEthernet 0/1)# ip address 200.168.12.1 255.255.255.0
A(config-if-GigabitEthernet 0/1)# ip nat outside
A(config-if-GigabitEthernet 0/1.)# exit
A(config)# ip nat pool net200 200.168.12.2 200.168.12.10 netmask 255.255.255.0
A(config)# ip nat inside source list 1 pool net200
```

```
A(config)# access-list 1 permit 192.168.12.0 0.0.0.255
A(config)# ip nat keepalive 10
```

【检验方法】 -

常见错误

- Inside/outside 口没配置。
- 未配置正确的 NAT 转换规则。

8.5 监视与维护

清除各类信息

无

查看运行情况

作用	命令
查看 NAT 转换记录	**show ip nat translations** [*acl_num*] [**icmp** | **tcp** | **udp**] [**verbose**]

查看调试信息

无

9 MLLB

9.1 概述

MLLB（Muliti Link Load Balance，多链路负载均衡）是一种多链路负载解决方案，用于解决多链路负载均衡的问题。

用户多链路出口访问外部网络，可以使用锐捷网关产品解决多链路出口链路带宽负载不均的问题，解决传统依靠配置大量静态路由的问题。

锐捷网关产品 MLLB 模块支持 ECMP（Equal Cost Multipath Routing，等价多路径路由）路由的多条链路上根据一定策略进行合理的流量分配，提高链路资源的利用效率。

MLLB 支持两种策略模式：基于链路带宽策略、基于链路负载策略。

MLLB 适用于多出口网络，相同运营商 ECMP 路由的负载均衡服务。

协议规范

无

9.2 典型应用

典型应用	场景描述
高校多出口基于带宽均衡	由一个或多个 ISP（Internet Service Provider，网络服务提供商）服务商提供多条链路网络服务。

9.2.1 高校多出口基于带宽均衡

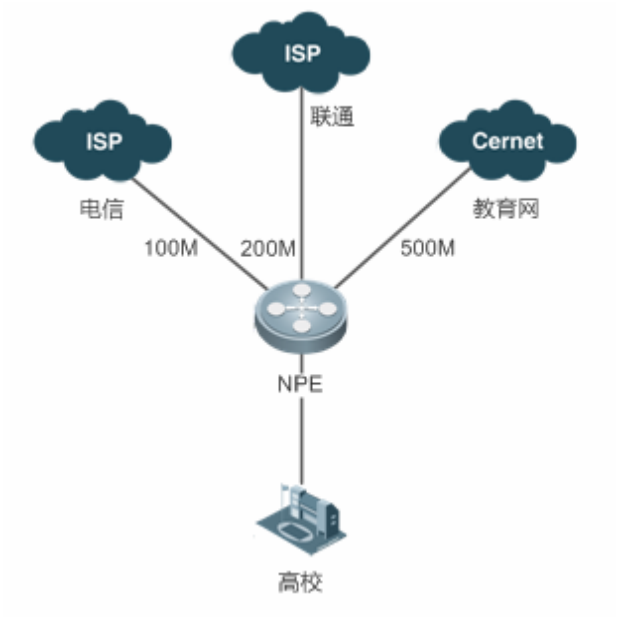
应用场景

由多个 ISP 服务商提供多条链路网络服务。

以下图为例，电信、联通和教育网给某高校提供出口网络服务。

- 高校用户访问外部网络形成 ECMP 路由。
- 基于带宽策略进行均衡负载。

图 9-1



【注释】 -

功能部属

- 配置开启 MLLB 模块开关。
- 配置基于带宽负载策略。
- 配置出口优先。

9.3 功能详解

基本概念

流

流或流会话(session)，即一段时间内一组目的 IP、目的端口、源 IP、源端口、VRF 五元组相同的报文。

ECMP 路由

ECMP 路由称为多重等价路由，对于给定的路由前缀，有一个以上的出口或下一跳。

链路带宽

链路可用资源的衡量指标，不同于物理接口的传输速率，是运营商提供的传输速率上限，通常是指下行带宽。

链路负载

链路负载是指链路当前资源的利用率，通过物理接口接收报文速率 / 链路带宽 计算得到。

阈值

阈值指的是出口带宽利用率阈值，又称负载阈值。用户可以设定阈值作为出口流量的警戒线，当出口流量超过阈值后，多链路负载均衡会采取相应的动作。

MLLB 模块要求：多链路负载均衡不支持 VPN 拨号场景，目前设备无法将 VPN 拨号的不同流识别成父子流，导致多链路负载均衡可能会把 VPN 拨号的不同报文转发到不同的出口，造成 VPN 协商失败。

功能特性

功能特性	作用
MLLB 开关	用于开启/关闭 MLLB 负载均衡模块。
带宽策略	根据 ECMP 出口链路的链路带宽比例进行流量负载均衡。
自定义均衡权重值	指定接口的负载均衡权重值。
负载策略	根据 ECMP 出口链路的当前链路负载，选择最小负载链路进行流量负载均衡。
基于源 IP	基于源 IP 地址选择出口流量负载均衡。（同带宽策略配合使用）
出口优先	当所有出口链路负载都超过阈值时，则会选用出口优先进行流量负载均衡。
负载监控	一般情况下，出口的下行流量是大于上行流量的；但有些用户场景，例如局域网内服务器，则可能上行流量大于下行流，这时可以切换为负载监控上行流量。（同负载策略配合使用）
负载阈值	负载阈值作为链路加入和退出负载均衡的参照，如果链路负载超过阈值上限，不再选择此链路作为负载均衡出口链路；如果链路负载低于阈值下限，重新选择此链路作为负载均衡出口链路。
自动探测网络	自动探测当前的网络。

9.3.1 MLLB开关

MLLB 开关用于开启/关闭 MLLB 负载均衡模块。

工作原理

开启 MLLB 模块开关，将会对 ECMP 出口流按照默认的配置策略（基于链路负载策略）进行负载均衡。

关闭 MLLB 模块开关，将不会对 ECMP 出口流进行负载均衡处理。

相关配置

启动 MLLB 模块功能

缺省情况下，锐捷网关设备 MLLB 模块功能关闭。

全局模式下使用 **mllb enable** 命令开启 MLLB 模块功能。

MLLB 模块功能开启之后，ECMP 出口流将会按照默认配置进行负载均衡。

关闭 MLLB 模块功能

缺省情况下，锐捷网关设备 MLLB 模块功能关闭。

若需要关闭 MLLB 模块功能，则全局模式下使用 **no mllb enable** 命令。

MLLB 模块功能关闭之后，ECMP 出口流将不会进行负载均衡。

9.3.2 带宽策略

带宽策略根据 ECMP 出口的上行或下行带宽比例进行负载均衡，不同出口流量与带宽成比例。

工作原理

对于给定的 ECMP 出口，计算 ECMP 出口链路带宽权重值；带宽越大权重值越大，带宽与权重成比例。

如果一个出口的流量超过阈值，则该出口不参与选路，如果所有出口的流量超过阈值，则 MLLB 模块基于链路带宽策略负载均衡失效，但用户也可以指定出口优先选择某一个出口进行分流。

↘ 计算带宽权重值

统计 ECMP 路由不同出口带宽之和设为 S，各出口带宽为 Bi，基准权重为 base，权重值为 Wi，然后按照如下比例计算：

Wi = Bi × base / S

相关配置

↘ 启动 MLLB 模块带宽策略功能

缺省情况下，锐捷网关设备 MLLB 模块基于带宽策略。

全局模式下使用 **mllb policy bandwidth** 命令启用带宽策略功能。

MLLB 模块启用带宽策略之后，ECMP 出口流会按照链路带宽权重比例进行分流。

9.3.3 自定义均衡权重值

带宽策略默认根据 ECMP 出口的上行或下行带宽比例进行负载均衡，也允许自定义接口的均衡权重值。

工作原理

默认根据接口的下行或者上行带宽比例进行负载均衡，如果需要调整某些接口的带宽利用率，可以自定义该均衡权重值。假设需要提升某个接口的利用率 ,可以在当前带宽值的基础上 ,调高权重值 ,如带宽为 100000 kilobits ,配置自定义权重值为 150000 kilobits。需要降低某个接口的利用率，可以调低权重值，如带宽为 100000 kilobits，配置自定义权重值为 50000 kilobits。

相关配置

↘ 配置自定义均衡权重值

缺省情况下，使用接口下行带宽作为均衡权重值。

全局模式下使用 **mllb interface** *interface-name* **weight** *weight-number* 命令更改接口的均衡权重值。

更好了接口均衡权重值后，将不再使用接口下行带宽作为均衡权重值，不会感知接口下行带宽的变化，直接使用指定的权重值计算负载均衡比值。

9.3.4 负载策略

带宽策略根据 ECMP 出口的上/下行带宽负载情况进行负载均衡，新建流选择最小负载链路分流。

工作原理

对于给定的 ECMP 出口，获取 ECMP 出口链路上行或下行负载情况，负载较小的链路则会被优先分流。

如果一个出口的流量超过阈值，则该出口不参与选路，如果所有出口的流量超过阈值，则 MLLB 模块基于链路负载策略均衡失效，但用户也可以指定出口优先选择某一个出口进行分流。

相关配置

↘ 启动 MLLB 模块负载策略功能

全局模式下使用 **mllb policy load** 命令启用负载策略功能。

MLLB 模块启用负载策略之后，ECMP 出口流会按照当前链路负载进行分流；

9.3.5 基于源IP

MLLB 模块基于源 IP 配置与带宽策略结合使用，可避免同一个用户的流被分流到不同的出口链路，降低网络访问异常风险。

工作原理

对于给定的 ECMP 出口，根据流中源 IP 信息分流到相应的出口链路。

如果一个出口的流量未超过阈值，相同源 IP 的流都会分流到同一个出口链路。

如果一个出口的流量超过阈值，则该出口不参与选路，如果所有出口的流量超过阈值，则 MLLB 模块负载策略均衡失效，但用户也可以指定出口优先选择某一个出口进行分流。

相关配置

↘ 启动 MLLB 模块基于源 IP 功能

缺省情况下，锐捷网关设备 MLLB 模块基于源 IP+目的 IP。

全局模式下使用 **mllb load-sharing original** 命令可以启用 MLLB 模块基于源 IP 功能。

MLLB 模块启用基于源 IP 功能之后，ECMP 出口流会按照源 IP 信息分流，同一个用户流会被分流到相同的出口。

9.3.6 出口优先

MLLB 模块支持出口优先设定，当 ECMP 各出口链路负载达到阈值时，流将根据出口优先进行分流。

工作原理

如果出口的流量未超过阈值，则按照原 MLLB 模块策略进行分流处理。

如果出口的流量超过阈值，则按照出口优先进行分流。

相关配置

↘ 启动 MLLB 模块出口优先功能

缺省情况下，锐捷设备 MLLB 模块出口优先功能关闭。

全局模式下使用 **mllb first-choice** *interface-type interface-number* 命令可以启用 MLLB 模块出口优先功能。

全局模式下使用 **no mllb first-choice** 命令可以关闭 MLLB 模块出口优先功能。

启用 MLLB 模块出口优先功能，当 ECMP 所有出口超过阈值时，出口优先分流，否则 MLLB 模块负载均衡失效。

出口优先功能仅支持 ECMP 默认路由。

9.3.7 负载监控

MLLB 模块支持负载监控设定，可以配置上行或下行监测链路负载情况。

工作原理

如果负载监控链路上行，MLLB 模块负载策略根据链路上行负载，选择最小负载链路进行优先分流。

如果负载监控链路下行，MLLB 模块负载策略根据链路下行负载，选择最小负载链路进行优先分流。

如果一个出口的流量超过阈值，则该出口不参与选路，如果所有出口的流量超过阈值，则 MLLB 模块负载策略均衡失效，但用户也可以指定出口优先选择某一个出口进行分流。

相关配置

↘ 启动 MLLB 模块负载监控功能

缺省情况下，锐捷网关设备 MLLB 模块负载监控链路下行流量。

全局模式下使用 **load-monitor uplink** 命令可以启用 MLLB 模块监控链路上行流量。

全局模式下使用 **no load-monitor** 命令可以启用 MLLB 模块监控链路下行流量。

9.3.8 负载阈值

MLLB 模块支持负载阈值设定，可以配置阈值上限和下限。

工作原理

如果负载监控某链路负载超过阈值上限，此链路置上超载标识，不进行负载均衡出口选路。

如果负载监控某链路负载低于阈值下限，且此链路已经置上了超载标识，则修改标识重新进行负载均衡出口选路。

如果负载监控某链路负载介于阈值上限与下限之间，则维持原状态。

相关配置

↘ 配置 MLLB 模块负载阈值功能

缺省情况下，锐捷网关设备 MLLB 模块负载阈值上限和下限均为 100。

全局模式下使用 **mllb threshold** *percent-upper* | [**lower** *percent-lower*]命令可以启用 MLLB 模块负载阈值上限和下限设置。

全局模式下使用 **no threshold** 命令可以恢复负载阈值默认设置。

9.3.9 自动探测网络

自动探测当前的网络。

工作原理

上网体验的好坏，很大程度上取决 dns 域名的延迟以及解析到 ip 地址是否可通，延迟大小，自动探测网络功能从两个方面量化当前的网络体验情况。从流表信息中获取流量的延迟，半开连接，选路流量的大小，方便量化当前设备网络的整体体验，同时记录下某个时刻的数据信息，方便后期查看；根据指定的 dns 服务器以及出接口，探测指定的主流域名的可访问性，记录 dns 域名解析，tcp 连接，http get 的延迟，量化出该 dns 服务器的稳定性。

相关配置

↘ 开启自动探测网络功能

缺省情况下，没有自动探测功能。

全局模式下使用 **mllb detect domain enable** 命令与 **mllb detect network enable** 命令来开启探测。

全局模式下使用 **no mllb detect domain enable** 命令与 **no mllb detect network enable** 命令来关闭探测。

配置需要探测的域名

配置需要探测的域名，最多支持 32 条域名。

全局模式下使用 **mllb detect domain add** *domain-name* 命令配置需要探测的域名。

全局模式下使用 **no mllb detect domain add** *domain-name* 命令删除需要探测的域名。

配置探测的 dns 服务器与接口

要自动探测域名，必须配置需要探测的域名以及配置探测的 dns 服务器与接口，最多支持 32 条。

全局模式下使用 **mllb detect domain dns-server** *dns-ip interface-name* 命令配置探测的 dns 服务器与接口。

指定源 ip 地址进行探测，使用 **mllb detect domain dns-server** *dns-ip interface-name* **source-ip** *source-ip-address*。

全局模式下使用 **no mllb detect domain dns-server** *dns-ip interface-name* 命令删除。

配置探测域名与检测网络的周期时间

默认探测域名与检测网络的周期时间均为 5 分钟

全局模式下使用 **mllb detect domain interval** *interval-time* 命令配置探测域名的周期时间。

全局模式下使用 **mllb detect network interval** *interval-time* 命令配置探测域名的周期时间。

全局模式下使用 **no mllb detect domain interval** 命令恢复默认的探测域名周期时间。

全局模式下使用 **no mllb detect network interval** 命令恢复默认的检测网络周期时间。

9.4 配置详解

配置项	配置建议 & 相关命令	
配置 MLLB 带宽策略功能	⚠ 必须配置。用于建立基于带宽策略负载均衡服务。	
	mllb enable	启动 MLLB 模块开关
	mllb policy bandwidth	启动 MLLB 模块带宽策略功能
	bandwidth *kilobits*	配置链路带宽
	⚠ 可选配置。 用于配置首选线路和负载门限服务。	
	mllb load-sharing original	设置同一个源 IP 只走同一个出口
	mllb first-choice *interface-type interface-number*	设置某三层口为优选出口
	mllb threshold { *percent-upper* | [**lower** *percent-lower*] }	设置负载均衡链路负载阈值为 *percent*，取值范围 1-100 的整数。percent-upper 为阈值上限，percent-lower 为阈值下限。
配置 MLLB 负载策略功能	⚠ 必须配置。用于建立基于负载策略负载均衡服务。	
	mllb enable	配置链路带宽
	mllb policy load	启动 MLLB 模块负载策略功能
	⚠ 可选配置。用于配置首选线路、负载门限和更新周期服务。	
	load-monitor uplink	配置链路监控方向，默认是下行；uplink 是上行
	mllb first-choice *interface-type interface-number*	设置某三层口为优选出口
	mllb threshold { *percent-upper* | [**lower** *percent-lower*] }	设置负载均衡链路负载阈值为 *percent*，取值范围 1-100 的整数。percent-upper 为阈值上限，percent-lower 为阈值下限。
	mllb load-interval *refresh-time*	设置链路负载监测周期

9.4.1 配置MLLB带宽策略功能

配置效果

按照带宽策略进行负载均衡，对 ECMP 出口流量按照出口带宽比分流。

注意事项

- MLLB 模块对 ECMP 出口流生效。因此，网络中必须存在 ECMP 路由信息。

- 基于带宽策略比例分流，因此，设备接口必须配置带宽值大小。

配置方法

启动 MLLB 模块开关功能

- 必须配置，在全局模式下配置。

配置 MLLB 模块带宽策略功能

- 必须配置，在全局模式下配置。

配置接口带宽大小

- 必须配置，在接口配置模式下，根据实际出口带宽值设置大小。

自定义接口均衡权重值

- 可选配置，在全局模式下配置，在实际出口带宽值基础上进行调整。

配置源 IP 功能

- 可选配置，默认为基于源 IP+目标 IP 分流。若需要配置源 IP 功能，则必须配置。
- 在全局模式下配置。

配置出口优先功能

- 可选配置，默认未开启出口优先功能。若需要配置出口优先功能，则必须配置。
- 在全局模式下配置。

配置负载阈值功能

- 可选配置，默认上限和下限阈值都为 100。若需要改变负载阈值，则必须配置。
- 在全局模式下配置。

检验方法

使网络中的 ECMP 出口流按照 MLLB 模块负载均衡分流。

- 检查设备出口链路流量是否基于带宽策略等比例负载。
- 检查所有 ECMP 出口链路超过阈值之后，是否走出口优先。
- 基于源 IP 配置，检查同一用户流是否走同一出口。
- 检查设备出口链路流量信息统计值。
- 查看 MLLB 模块配置信息是否生效。

相关命令

启动 MLLB 模块开关功能

【命令格式】 **mllb enable**
【参数说明】 -
【命令模式】 全局模式
【使用指导】 -

配置带宽策略功能

【命令格式】 **mllb policy bandwidth**
【参数说明】 -
【命令模式】 全局模式
【使用指导】 带宽策略负载均衡，出口流量按照出口带宽比分担。

配置接口带宽大小

【命令格式】 **bandwidth** *kilobits*
【参数说明】 *kilobits*：指定接口带宽大小。（单位：kilobits）
【命令模式】 接口模式
【使用指导】 此命令用来配置接口出口带宽值。

自定义接口均衡权重值

【命令格式】 **mllb interface** *inteface* **weight** *weight-num*
【参数说明】 *inteface*：接口名称
weight-num：自定义均衡权重值，(单位：kilobits)
【命令模式】 全局模式
【使用指导】 此命令用来自定义接口均衡权重值。

配置源 IP 功能

【命令格式】 **mllb load-sharing original**
【参数说明】 -
【命令模式】 全局模式
【使用指导】 此命令用来保障同一个用户流，被分流到同一个出口，与带宽策略配合使用。

配置出口优先功能

【命令格式】 **mllb first-choice** *interface-type interface-number*
【参数说明】 *interface-type interface-number*：以此接口作为优先出口。
【命令模式】 全局模式
【使用指导】 此命令用来配置出口优先。
如果出口的流量超过阈值，则按照出口优先进行分流。

配置负载阈值功能

【命令格式】 **mllb threshold** { *percent-upper* | [**lower** *percent-lower*] }
【参数说明】 *percent-upper*：指定链路上限值。

percent-lower：指定链路下限值。

上限值与下限制取值范围在 1-100，默认为 100（单位：%）。

【命令模式】 全局模式

【使用指导】 超过阈值上限的出口链路，不再进行分流处理。

查看出口均衡流量信息

【命令格式】 **show mllb statistics**

【参数说明】 -

【命令模式】 特权模式、全局模式、接口模式

【使用指导】 查看所有出口均衡流信息统计。

查看 MLLB 模块配置信息

【命令格式】 **show mllb configure**

【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 MLLB 模块配置信息。

配置举例

以下配置举例，仅介绍与 MLLB 模块相关的配置。

在网络上建立 MLLB 负载均衡服务，支持带宽策略功能

【网络环境】 某网吧配置三条 ADSL 链路，每条链路出口带宽分别为 50M，50M，100M。

按照带宽均衡策略利用 ADSL 链路出口带宽。

【配置方法】

- 全局开启多链路负载均衡功能。

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

- 配置默认路由。

```
Ruijie(config)# ip route 0.0.0.0 0.0.0.0 dialer 1
Ruijie(config)# ip route 0.0.0.0 0.0.0.0 dialer 2
Ruijie(config)# ip route 0.0.0.0 0.0.0.0 dialer 3
```

- 配置 ADSL 链路带宽大小。

```
Ruijie(config)#interface dialer 1
Ruijie(config-if-dialer 1)#bandwidth 50000
Ruijie(config-if-dialer 1)# end
Ruijie(config)# interface dialer 2
Ruijie(config-if-dialer 2)#bandwidth 50000
Ruijie(config-if-dialer 2)# end
Ruijie(config)# interface dialer 3
Ruijie(config-if-dialer 3)#bandwidth 100000
```

```
Ruijie(config-if-dialer 3)# end
```

- 开启基于带宽策略功能。

```
Ruijie(config)#mllb policy bandwidth
```

【检验方法】 网吧用户访问外部网络，查看链路出口均衡信息：

- show mllb configure 查看 MLLB 模块配置是否生效。
- show mllb statistics 查看各出口链路均衡情况。

常见错误

- 未配置 MLLB 模块开启开关功能，导致配置不生效。
- 未配置/配置的出口带宽值与 ISP 提供的网络带宽大小不匹配，导致均衡效果受影响。
- 未配置默认路由信息。

9.4.2 配置MLLB负载策略功能

配置效果

- 按照负载策略进行负载均衡，对 ECMP 出口流量按照当前负载最小出口链路进行分流。

注意事项

- MLLB 模块对 ECMP 出口流生效。因此，网络中必须存在 ECMP 路由信息。

配置方法

启动 MLLB 模块开关功能

- 必须配置，在全局模式下配置。

配置 MLLB 模块负载策略功能

- 必须配置，在全局模式下配置。

配置负载监控

- 可选配置，默认负载监控出口链路下行。
- 配置负载监控需要在全局模式下，根据实际需要选择监控上行或下行方向。

配置出口优先功能

- 可选配置，默认未开启出口优先功能。
- 在全局模式下配置。

配置负载阈值功能

- 可选配置，默认上限和下限阈值都为 100。
- 在全局模式下配置。

配置负载更新周期

- 可选配置，默认更新周期为 5 秒。
- 在全局模式下配置。

检验方法

使网络中的 ECMP 出口流，按照 MLLB 模块负载均衡分流。

- 检查设备出口链路流量是否基于负载策略分流。
- 检查设备出口链路流量信息统计值。
- 检查所有 ECMP 出口链路超过阈值之后，是否走出口优先。
- 查看 MLLB 模块配置信息是否生效。

相关命令

启动 MLLB 模块开关功能

【命令格式】 **mllb enable**
【参数说明】 -
【命令模式】 全局模式
【使用指导】 -

配置负载策略功能

【命令格式】 **mllb policy load**
【参数说明】 -
【配置模式】 全局模式
【使用指导】 负载策略均衡，流量动态根据出口链路的负载状况调整走向使各出口的负载维持均衡。

配置负载监控功能

【命令格式】 **load-monitor uplink**
【参数说明】 -
【配置模式】 全局模式
【使用指导】 用于监控出口链路上行或下行负载情况，默认是下行；uplink 是上行。

配置负载更新周期

【命令格式】 **mllb load-interval** *refresh-time*

【参数说明】 *refresh-time* ：更新周期值，取值范围在 3-30。（单位：秒）

【配置模式】 全局模式

【使用指导】 用于周期性更新出口链路负载。

配置举例

↘ 在网络上建立 MLLB 负载均衡服务，支持负载策略功能

【网络环境】 某高校配置三条出口链路，每条链路出口带宽分别为 50M，50M，100M。

按照负载策略利用链路出口带宽。

【配置方法】

- 全局开启多链路负载均衡功能。

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

- 配置默认路由。

```
Ruijie(config)# ip route 0.0.0.0 0.0.0.0 GigabitEthernet 0/1 202.101.98.54
Ruijie(config)# ip route 0.0.0.0 0.0.0.0 GigabitEthernet 0/2 202.101.98.55
Ruijie(config)# ip route 0.0.0.0 0.0.0.0 GigabitEthernet 0/3 202.101.98.56
```

- 开启基于负载策略功能。

```
Ruijie(config)#mllb policy load
```

- 开启出口优先功能。

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

【检验方法】 高校用户访问外部网络，查看链路出口均衡信息：

- show mllb configure 查看 MLLB 模块配置是否生效。
- show mllb statistics 查看各出口链路均衡情况。

常见配置错误

- 未配置 MLLB 模块开启开关功能，导致配置不生效。
- 未配置默认路由信息。
- 出口优先配置为非 ECMP 出口。

9.4.3 配置自动探测网络功能

配置效果

- 开启后会定时检测当前网络的半开连接数，延迟大小，选路流量信息，以及指定 dns 服务器与出口探测指定域名的可通性，并记录在数据库中。

注意事项

- 探测域名的可通性与检测当前网络，使用两个独立的开关控制其开启。

配置方法

打开自动检测网络开关

- 必须配置，在全局模式下配置。

打开自动探测域名开关

- 必须配置，在全局模式下配置。

配置 dns 服务器 ip 地址与接口

- 必须配置，在全局模式下配置。

配置需要探测的域名

- 必须配置，在全局模式下配置。

配置检测与探测周期时间

- 可选配置，默认值为 5 分钟。
- 在全局模式下配置。

检验方法

- 查看自动探测网络配置信息是否生效。

相关命令

打开自动检测网络开关

【命令格式】 **mllb detect network enable**
【参数说明】 -
【命令模式】 全局模式
【使用指导】 -

打开自动探测域名开关

【命令格式】 **mllb detect domain enable**
【参数说明】 -

【配置模式】 全局模式
【使用指导】 -

配置 dns 服务器 ip 地址与接口

【命令格式】 **mllb detect domain dns-server** *dns-ip interface* **source-ip** *source-ip-address*
【参数说明】 *dns-ip*：dns 服务器的 ip 地址
interface：出接口的名称
source-ip-address：指定探测的源 ip 地址
【配置模式】 全局模式
【使用指导】 -

配置需要探测的域名

【命令格式】 **mllb detect domain add** *domain-name*
【参数说明】 *domain-name*：需要探测的域名名称
【配置模式】 全局模式
【使用指导】 -

配置检测与探测周期时间

【命令格式】 **mllb detect** {**domain | network**} **interval** *interval-time*
【参数说明】 *interval-time*：周期时间，范围在 1-1440（单位：分钟）
【配置模式】 全局模式
【使用指导】 -

配置举例

配置自动探测网络

【网络环境】 某企业配置 2 条出口链路，分别为 100M 电信，50M 联通。客户内网使用 8.8.8.8 域名服务器上网，经常发现网页打开比较缓慢，怀疑联通线路存在问题，同时也怀疑 dns 域名服务器存在问题。配置自动探测网络功能来发现是否存在上述问题。

【配置方法】
- 开启自动探测网络功能。

```
Ruijie(config)# mllb detect domain enable
Ruijie(config)# mllb detect network enable
```

- 配置域名。

```
Ruijie(config)# mllb detect domain add www.qq.com
Ruijie(config)# mllb detect domain add www.tmall.com
Ruijie(config)# mllb detect domain add www.jd.com
```

- 配置 dns 服务器与接口。

```
Ruijie(config)# mllb detect domain dns-server 8.8.8.8 GigabitEthernet 0/1
Ruijie(config)# mllb detect domain dns-server 8.8.8.8 GigabitEthernet 0/2 source-ip 192.168.197.16
```

【检验方法】 可以通过 show mllb detect configure 查看配置是否生效。

常见配置错误

- 未开启探测域名与检测网络功能开关，导致配置不生效。
- 域名与 dns 服务器添加，达到了容量上限，添加失败。

9.5 监视与维护

清除各类信息

无

查看运行情况

作用	命令
查看 MLLB 配置信息。	**show mllb configure**
查看 MLLB 出口均衡统计信息。	**show mllb statistics**
查看 MLLB 探测功能配置信息。	**show mllb detect configure**

查看调试信息

无

10 WAN-IP

10.1 概述

WAN-IP：多 WAN 同网段。本功能适用于这样的场景：用户申请了 N 条线路，且所有 IP 地址均在同网段，而由于 RGOS 本身的限制，不同接口的 IP 地址是不能配置成同一个网段的，多 WAN 同网段就是为了在这种场景下使用的。通过配置使用多 WAN 同网段，网关上就可以配置除不同接口属于同一个网段的效果。

下文仅介绍 WAN-IP 的相关内容。

协议规范

-

10.2 典型应用

典型应用	场景描述
多 WAN 同网段	一台设备，多个 wan 口属于同个网段。

10.2.1 多WAN同网段

应用场景

一个运营商提供了两个（多个）同网段的 IP，IP1 a.b.c.2/24，IP2 a.b.c.3/24，下一跳均为 a.b.c.1/24。

图 10-1



【注释】 D 为内网网络。
A 为出口设备。
B 为运营商交换机。
C 为运营商网关。

功能部属

- 其他功能正常配置即可。

10.3 功能详解

基本概念

RGOS IP 冲突

RGOS 平台是不允许在不通的接口上配置属于同一个网段的 IP 的(如 Gi0/0 配置了 192.168.1.1/24，其他任意接口都不允许配置 192.168.1.0/24 中任意的地址)，如果配置就会提示“Primary IP address conflict with "GigabitEthernet 0/x".”。

功能特性

功能特性	作用
ARP 篡改	在设备的上层模块与运营商之间做一层 ARP 篡改，让他们可以学习到想要的 MAC 地址。

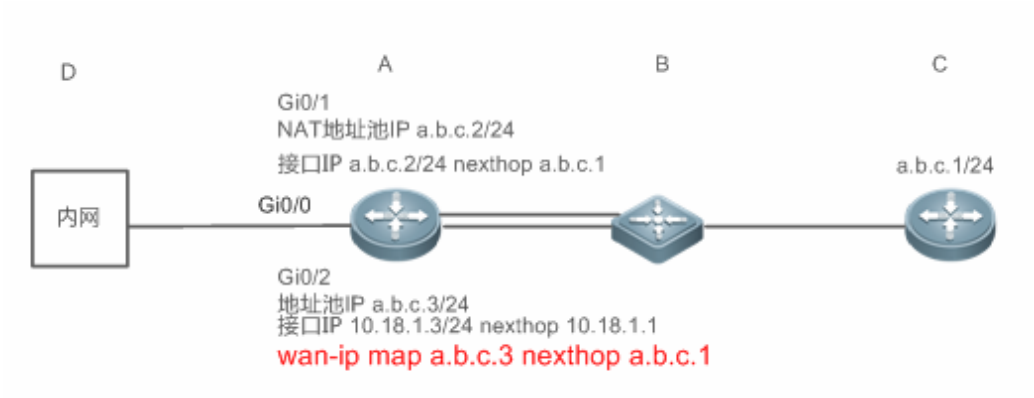
10.3.1 ARP篡改

通过拦截、篡改上层模块发送给运营商的 ARP 报文，让运营商可以学习到本端的 MAC 地址。

通过拦截、篡改运营商发送给设备的 ARP 报文，让设备上层模块可以学习到对端的 MAC。

工作原理

功能部署拓扑如下图 10-2：



【注释】 D 为内网网络。
A 为出口设备。
B 为运营商交换机。
C 为运营商网关。

运营商分配了两个 IP 地址：IP1 a.b.c.2/24，IP2 a.b.c.3/24，下一跳均为 a.b.c.1/24。这样部署：

1. Gi0/1 相关配置：
   a) Gi0/1 上配置运营商分配的 IP1 ip address a.b.c.2 255.255.255.0
   b) Gi0/1 上配置 nexthop a.b.c.1
   c) NAT 地址池中 address a.b.c.2 a.b.c.2 match interface GigabitEthernet 0/1
2. Gi0/2 相关配置：
   a) Gi0/2 上配置一个本设备没有使用的私网地址如 ip address 10.18.1.3 255.255.255.0
   b) Gi0/2 上配置 nexthop 10.18.1.1
   c) NAT 地址池中配置 address a.b.c.3 a.b.c.3 match interface GigabitEthernet 0/2
   d) Gi0/2 上配置 wan-ip map a.b.c.3 255.255.255.0 nexthop a.b.c.1
   e) 生成转换表 1，ARP 报文中如果是 10.18.1.3 发送给 10.18.1.1，那么将 10.18.1.3 替换成 a.b.c.3，将 10.18.1.1 替换成 a.b.c.1
   f) 生成转换表 2 ,ARP 报文中如果是 a.b.c.1 发送给 a.b.c.3 ,那么将 a.b.c.1 替换成 10.18.1.1 ,将 a.b.c.3 替换成 10.18.1.3

↘ 网关学习对端 MAC

对于 Gi0/1 来说，所有流程正常，不再叙述。

对于 Gi0/2 来说，设备主动学习对端的 MAC 流程：

1. ARP 模块广播请求 10.18.1.1 的 MAC，该 ARP 请求被 WAN-IP 模块拦截，WAN-IP 发现源 ip 为 10.18.1.3，目的 ip 为 10.18.1.1，该报文匹配转换表 1，所以将 10.18.1.3 替换成 a.b.c.3，将 10.18.1.1 替换成 a.b.c.1。
2. 运营商收到 a.b.c.1 的 ARP 请求，响应对应的 MAC 给设备。
3. WAN-IP 在收到这个应答后 ,发现源 ip 为 a.b.c.1 ,目的 ip 为 a.b.c.3 ,该报文匹配转换表 2 ,所有将 a.b.c.1 替换成 10.18.1.1，将 a.b.c.3 替换成 10.18.1.3。
4. ARP 模块收到 ARP 应答，学习到 10.18.1.1 的 MAC 二层打通。
5. 内网流量经过设备后，源地址被 NAT 模块修改成 a.b.c.3，发送给网关 10.18.1.1，由于已经在 4 步学习到了 10.18.1.1 的 MAC 就是实际 a.b.c.1 的 MAC，所以报文直接被送到 a.b.c.1 去，到此转发打通。

对于运营商主动学习设备的 MAC，这一流程与以上类似，就不在此重复叙述。

10.4 产品说明



NBR108G-P 不支持配置不同接口配置同网段地址 ;NBR800G、NBR950G、NBR1500G、NBR2000G、NBR1000G-E、NBR6120-E、 NBR1300G-E、 NBR1700G-E、 NBR2100G-E、 NBR2500D-E、 NBR3000D-E、 NBR3000D-UE、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持配置不同接口配置同网段地址。

10.5 配置详解

配置项	配置建议 & 相关命令	
配置多 wan 同网段	⚠ 必须配置。	
	wan-ip enable	开启多 wan 同网段功能开关
	wan-ip map	配置接口下的多 wan 同网段功能

10.5.1 配置多wan同网段

配置效果

- 网关设备可以使用在运营商提供了多个同网段 IP 的场景，内网用户上网正常。

注意事项

- -

配置方法

↘ 开启多 wan 同网段功能开关

- 必须配置。未开启多 WAN 同网段功能开关，则对应的配置无法工作。

【命令格式】 **wan-ip enable**
【参数说明】 **-**
【缺省配置】 功能关闭
【命令模式】 全局模式
【使用指导】 -

↘ 配置接口下的多 wan 同网段功能

- 必须配置。作为策略规则，用于转发报文匹配 ARP。

【命令格式】 **wan-ip map** *ip-address1 mask* **next-hop** *ip-address2*
【参数说明】 *ip-address1*：运营商分配的 ip
mask：掩码
ip-address2：运营商网关
【缺省配置】 无配置
【命令模式】 接口模式
【使用指导】 使用前要确认好运营商分配的 ip 与运营商的网关地址。

↘ 检验方法

使两端都可以学习到需要的 MAC 地址。

- 检查内网用户通过配置 WAN-IP 的出接口上网是否正常，如果正常，那么表示功能成功。
- 使用 **show wan-ip config** 命令检查配置是否正确。

【命令格式】 **show wan-ip config**

【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 wan-ip 的当前配置。

【命令展示】

```
Ruijie(config)#show wan-ip config
Enable: True
GigabitEthernet 0/7: wan-ip map 10.10.0.56 255.255.255.0 nexthop 10.10.0.1
Ruijie(config)#
```

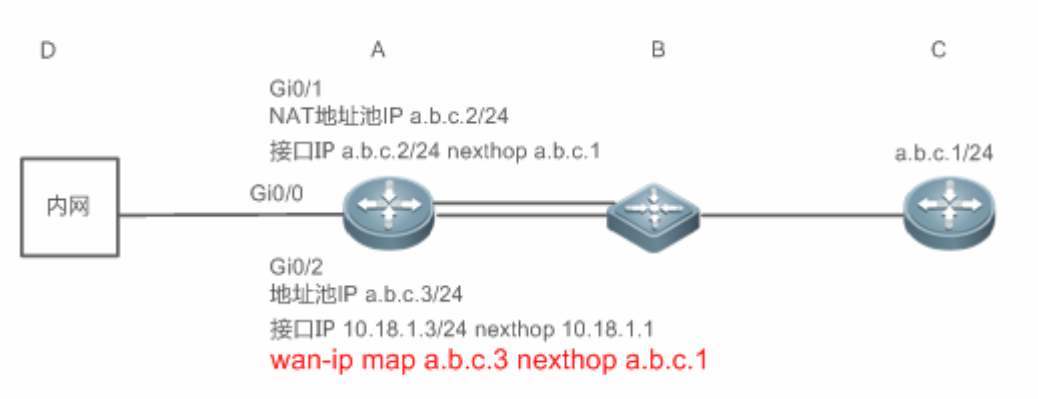
关于 show 信息的详细解释请参看对应功能的命令手册。

配置举例

多 wan 同网段

【网络环境】

图 10-3



【配置方法】

- 在 Gi0/1 上配置如上图的 IP 地址、nexthop、NAT。略
- 在 Gi0/2 上配置如上图的 IP 地址、nexthop、NAT。略

```
A# configure terminal
A(config)# wan-ip enable
A(config)# interface GigabitEthernet 0/2
A(config-if-GigabitEthernet 0/2)# wan-ip map a.b.c.3 255.255.255.0 nexthop a.b.c.1
A(config-if-GigabitEthernet 0/2)# exit
A(config)#
```

【检验方法】

- 通过 Gi0/2 可以正常上网。
- 使用 **show wan-ip config** 命令检查配置表项 a.b.c.3 为运营商分配的 ip，a.b.c.1 为运营商的网关。

A

```
Ruijie(config)#show wan-ip config
Enable: True
GigabitEthernet 0/2: wan-ip map a.b.c.3 255.255.255.0 nexthop a.b.c.1
Ruijie(config)#
```

常见错误

- 接口 nexthop 没有配置。

10.6 监视与维护

查看运行情况

作用	命令
查看转换表。	**show wan-ip config**

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
打开管理面 debug 开关。	**debug wan-ip config**
打开转发面 debug 开关	**debug wan-ip pkt**

配置指南-行为管理

本分册介绍行为管理相关内容，包括以下章节：

1. 二三层分类识别
2. APP-IDENTIFY
3. APP-ROUTE
4. APP-PROXY
5. 全局会话数限制
6. 流量控制
7. FLOW-AUDIT
8. CONTENT-AUDIT
9. LINE-QUALITY

1 二三层分类识别

1.1 概述

设备要对内网用户进行行为控制，首先要对内网用户的数据流进行识别。二三层分类识别就是一种基于报文中的 vlan tag、源 IP 地址和目的 IP 地址对数据流进行检测识别，从而对数据流进行不同对象的划分，设备根据不同对象进行相应的处理达到对内网用户行为控制的目的。

二三层对象包括 vlan 对象、用户对象、网络对象、认证对象：

vlan 对象：基于内网用户所属 vlan id 配置的对象。支持根据报文携带的 vlan tag 进行数据流分类。网关模式下，vlan 对象不生效。网桥模式下，所有的数据流默认匹配中桥的 native vlan 所对应的 vlan 对象，若 native vlan 没有对应的 vlan 对象，则数据流匹配中默认 vlan 对象“any”。

用户对象：基于内网用户 ip 地址和 mac 地址配置的对象。支持根据报文的源 ip 地址、源 mac 地址进行数据流分类。当未匹配中配置的用户对象时，则匹配中系统默认用户对象“any”。当基于 mac 地址和 ip 地址分别匹配中不同的用户对象时，以 mac 地址匹配中的用户对象为最终结果。

网络对象：基于内外用户访问的外网地址配置的对象。支持根据报文的目的 ip 地址进行数据流分类。当未匹配中配置的网络对象时，则匹配中系统默认网络对象“any”。

认证对象：基于外部服务器同步的账号、ip 自动生成的对策。支持根据报文的源 ip 地址进行数据流分类。当没有外部服务器用户同步到设备，则匹配中系统默认认证对象”any’。

- 内置认证：使用设备端内置的 portal 服务器及数据库进行 web 认证。其中本地数据库包括 subs 及 local 两种数据库，本模块描述只针对 subs 数据库。二三层分类识别适用于中小企业，支持根据不同职能部门所属不同 vlan 或 ip 段进行行为控制及审计。

一个 vlan id 只属于一个 vlan 对象，一个 ip 地址也只属于一个用户对象和网络对象。

协议规范

无

1.2 典型应用

典型应用	场景描述
办公网络限制访问外网	部分办公室网络中除了领导外全部禁止访问外部网络
特定用户免于审计和流控	高校场景中，除老师外的所有学生进行内容审计和流量控制
访问外部服务器优先保障	保障访问总部服务器的下载和上传速度
MAC 绑定过滤	只允许手动绑定 MAC+IP 的用户才允许访网络

1.2.1 办公网络限制访问外网

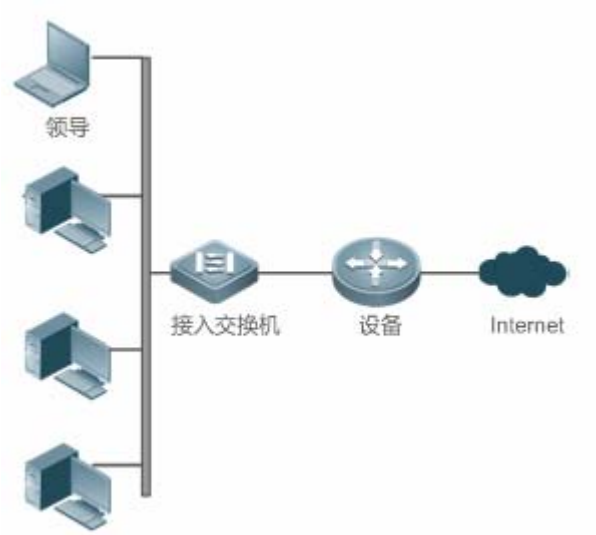
应用场景

禁止所有访问外网的数据流，识别出领导数据流并根据所属对象作特殊处理即放行。

以下图为例，小型的办公网络中，对内网用户访问外部 internet 进行控制。

- 内网用户之间可以通信，但是不能访问外部 internet。
- 领导可以正常访问外部 internet 不受影响。

图 1-1



【注释】 设备内部需要二层网络环境，不能有 nat 否则会导致无法识别。

功能部属

- 设备上开启二三层分类识别命令。
- 设备上启用二三层全局屏蔽模式。
- 配置基于领导 ip 地址或者 mac 地址的用户对象 A。
- 对用户对象 A 设置白名单属性。

1.2.2 特定用户免于审计和流控

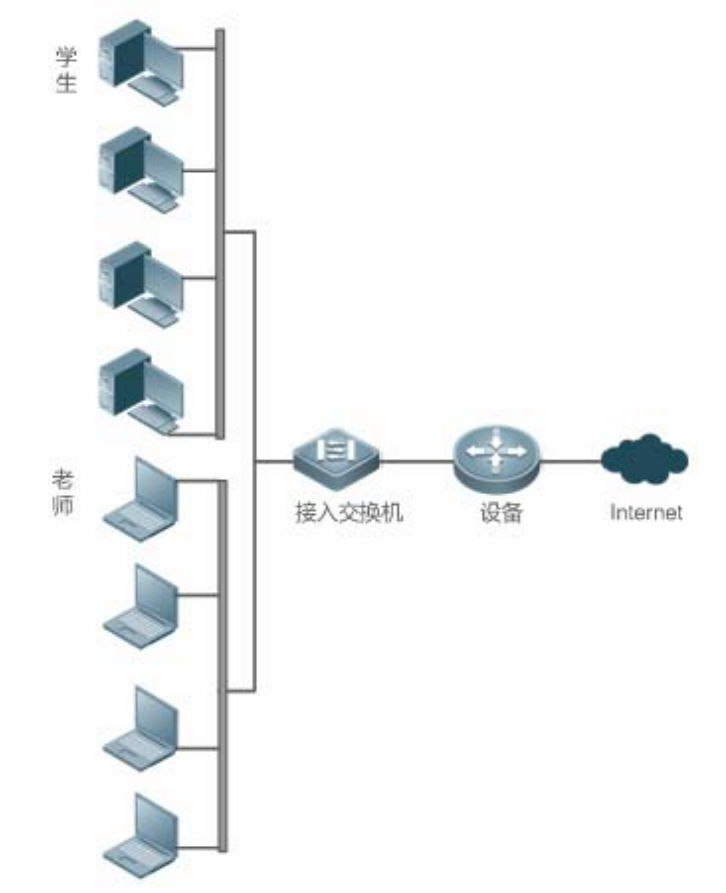
应用场景

识别出学生和老师网段所属的数据流，分别作不同处理。

以下图为例，高校场景中需要对学生的上网行为进行审计和流量控制，但是对老师的上网行为不审计。

- 识别出学生的数据流进行内容审计和流量控制。
- 识别出老师的数据流不进行内容审计和流量控制。

图 1-2



【注释】 设备内部需要二层网络环境，不能有 nat 否则会导致无法识别。

功能部属

- 设备上开启二三层分类识别、内容审计和流量控制。
- 设备上配置基于所有用户的全局内容审计和流控策略。
- 配置基于老师所属 ip 段的用户对象 A。
- 对用户对象 A 设置免监控属性。

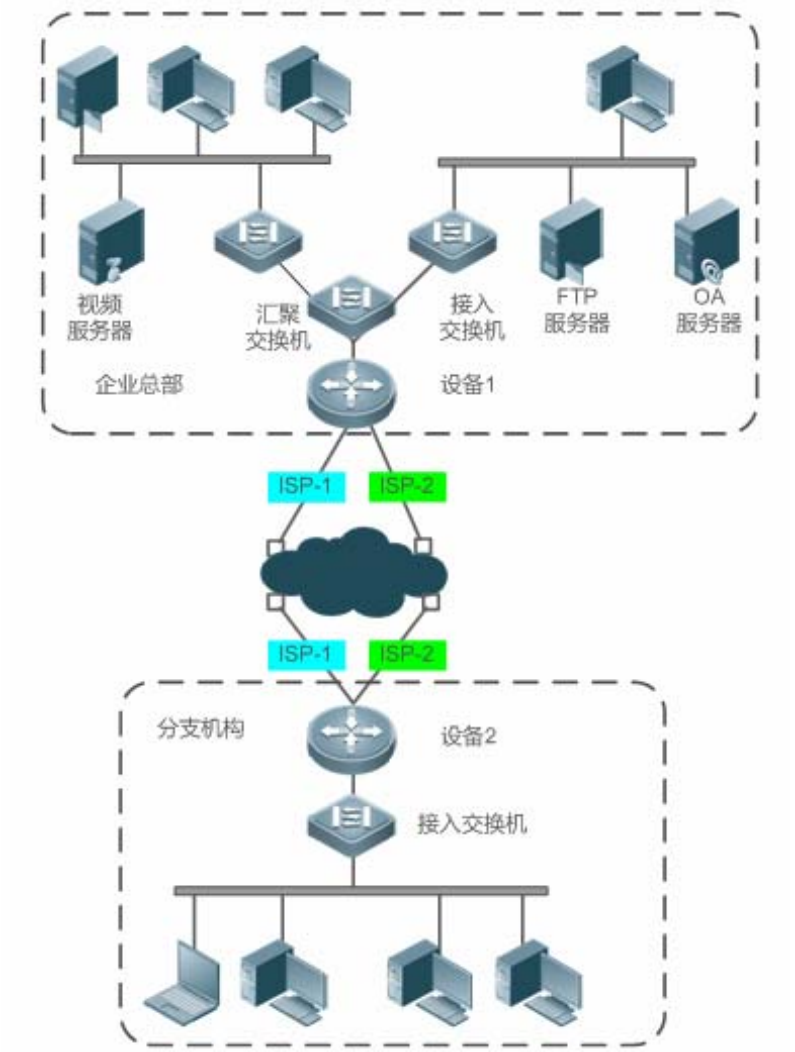
1.2.3 访问外部服务器优先保障

应用场景

以下图为例，企业总部-分布机构场景中，分支机构中需要对访问总部服务器的数据流优先保障。

- 企业分支机构访问外网进行流控限速。
- 企业分支机构访问总部服务器的上传和下载速度优先保障。

图 1-3



【注释】 设备内部需要二层网络环境，不能有 nat 否则会导致无法识别。

功能部属

- 设备上开启二三层分类识别、流量控制。
- 设备上配置基于所有用户的全局流控策略。
- 设备 2 通过 vpn 拨入设备 1。
- 设备 2 上配置基于总部内部服务器 IP 地址的网络对象 A。

- 基于网络对象 A 配置流控策略并调整优先级最高

1.2.4 同步实名账号

应用场景

支持同步外部服务器的实名账号，包括 SAM/SMP/ESS 服务器。

功能部属

- 设备上开启二三层分类识别命令。
- 开启服务器联动功能，配置 link-sam 或 snmp。

1.2.5 MAC 绑定过滤

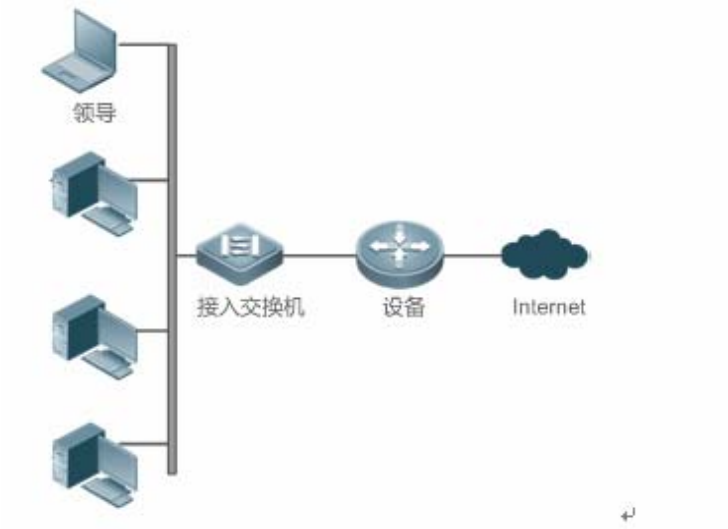
应用场景

网络管理员希望所有的接入终端必须手动 IP+MAC 绑定，不允许非法终端接入访问网络。

以下图为例，限制非法终端接入网络。

- 严格校验模式开启后，配置 MAC+IP 绑定的终端可以正常接入访问网络。。
- 未绑定 IP+MAC 的终端不允许接入网络。

图 1-5



【注释】 -

功能部属

- 设备上开启严格校验模式。
- 设备上将合法的终端手动配置 IP+MAC 绑定。

1.3 功能详解

基本概念

↘ vlan 对象、用户对象、网络对象、认证对象

vlan 对象是基于内网用户所属 vlan id 配置的对象。

用户对象是基于内网用户所属 ip 地址和 mac 配置的对象。

网络对象是基于内网用户所访问的外网地址配置的对象。

认证对象是基于外部服务器同步的账号、ip 自动生成的对象。

↘ 对象、对象组

vlan 对象没有组织层次，因此没有组概念。

网络对象包括单 ip 网络对象，range 网络对象以及网络对象组，网络对象组指未配置 ip 地址的网络对象。

用户对象包括配置了密码、ip 地址、mac 地址任意一种的用户对象以及三项都未配置的用户对象组。

认证对象 ip 节点对应惟一的实名账号和账号组信息，自动生成。

↘ 冲突对象

配置的名称、ip 地址、mac 地址已经存在或者配置的路径和实际组织机构中存在层次关系不符，都称为配置的该对象和已有的对象冲突。

↘ 账号、单双向绑定

用户对象可以配置密码作为认证账号使用，作为账号后，配置的 ip 和 mac 地址被该账号绑定，可以配置单双向绑定。

单向绑定，该账号仅限于绑定 ip 地址和 mac 地址使用，但是该 ip，mac 地址还可以使用其他账号。

双向绑定，该账号仅限于绑定的 ip 和 mac 地址使用，该 ip 和 mac 地址也仅限于使用该账号。不绑定的账号，不受使用 ip 和 mac 地址的限制。

↘ 对象索引值

对象索引值用来惟一标识一个对象节点，是根据内核创建对象成功之后所在的内存地址计算而来，内核和用户空间对象索引值保持一致，数据流经过识别之后根据所属不同对象记录不同索引值，后续流控或者审计模块根据数据流记录的索引值来用户管理模块查询该数据流对应的对象信息。

↘ 数据流分类识别

根据报文中携带的 vlan tag，源目的 ip 地址，以及 mac 地址信息结合配置的各对象信息，将数据流划分属于不同的对象。

用户自定义组

用户对象组织树外，支持配置自定义组对象可以关联任意 IP 段，且 IP 段之间允许冲突，提升配置的易用性。

严格校验模式

该模式下，只有 IP+MAC 绑定且能都能正确识别的用户才能正常接入访问网络。

功能特性

功能特性	作用
数据流分类识别	对不同用户的数据流进行识别，从而达到对不同用户行为控制的目的。

1.3.1 数据流分类识别

根据不同对象配置的 ip，mac 等信息将数据流划分属于不同的对象，通过对不同对象的策略控制达到对不同对象所属数据流差异化行为控制的目的。

工作原理

数据流的分类识别包括对象管理、对象识别两个过程。

对象管理

管理员根据内网用户所属的 ip 地址，mac 地址配置用户对象，根据内网用户访问的外网地址配置网络对象等，将对象名称和 ip 地址，对象索引值等信息关联起来保存在内存中。

对象识别

二三层识别通过对报文中的 vlan tag、ip 地址、mac 地址等信息查询匹配配置的对象数据，对不同的数据流分类划分所属不同的对象，并记录在流私有空间中，报文中也记录所属对象的索引值。后续流量控制和内容审计模块，通过数据流中记录的索引值来用户管理处查询相应的信息，再根据不同对象的差异化策略从而达到对不同数据流差异化控制的目的。

相关配置

启用二三层分类识别功能

缺省情况下，二三层分类识别功能是开启的。

使用 **layer23 classify enable** 命令启动二三层分类识别功能。

使用 **no layer23 classify enable** 命令关闭二三层分类识别功能。

配置用户对象、网络对象、vlan 对象

缺省情况下，系统默认配置 Defalut_Group 和 Vpn_Group 用户对象组和 Out_Server 网络对象组。

使用 **subscriber staticname***namestr***parent** *parstr* [[[**ip-host** *ip-addr*] [**mac** *mac-addr*] | **ip-subnet** *subnetmask* **| ip-range** *start end*] [**password** *pwd_str*{ **two-way-bind** | **single-way-bind**}] | [**password***pwd_str*]]配置用户对象。
使用 **no subscriber staticname***namestr* 删除用户对象。
使用 **network-groupname***namestr*[**parent** *parent*] [**ip-host** *ip-addr*|**ip-subnet** *subnet mask*| **ip-range** *start end*]]配置网络对象。
使用 **nonetwork-groupname***namestr* 删除网络对象。
使用 **vlan-group***name***vlan***vid-list* 配置 vlan 对象。
使用 **novlan-group***name* 删除 vlan 对象。

↘ 配置用户自定义组

缺省情况下，系统不配置用户自定义组。

使用 **subscriber custom-group** *namestr* **relate ip-range** *ip_starip_end* 命令配置自定义组关联 IP/IP 段。

使用 **no subscriber custom-group** *namestr* **[relate ip-range** *ip_starip_end***]**命令删除自定义组或自定义组关联的 IP/IP 段。

↘ 配置用户自定义组属性

缺省情况下，系统不设置用户自定义组属性。

使用 **subscriber custom-group** *namestr* **attribute {deny | avoid-audit | avoid-fc | release | vip}**命令配置自定义组属性。

使用**no subscriber custom-group** *namestr* **attribute {deny | avoid-audit | avoid-fc | release | vip}**命令删除自定义组属性。

↘ 配置严格校验模式

缺省情况下，不启用该模式。

使用 **layer23 strict-verification enable** 命令开启严格校验模式。

使用 **no layer23 strict-verification enable** 命令关闭严格校验模式。

1.3.2 内置无感知认证

使用 subs 静态对象进行 web 认证的首次用户名和密码校验，校验通过后记录 MAC 地址。后续接入认证后无需再次使用用户名和密码，MAC 地址校验通过直接放行。

工作原理

首次接入认证使用用户名密码校验，后续接入使用 MAC 地址校验。

↘ 校验过程

用户输入用户名和密码进行 web 认证，3A 根据认证方法 subs 选择到用户对象进行用户名和密码校验。subs 校验通过后，记录 MAC 地址。当后续用户再次接入网络后，IPOE 获取 MAC 地址通过 3A 到 subs 进行校验，MAC 校验通过后返回认证通过，用户可以正常接入访问网络。

相关配置

↘ 配置 subs 库无感知模式

缺省情况下，subs 库不开启无感知模式。

使用 **layer23 subs-mab enable** 命令开启 subs 库无感知模式。

使用 **no layer23 subs-mab enable** 命令关闭 subs 库无感知模式。

1.4 产品说明

NBR3000G-S 、NBR1500G、NBR2000G、NBR1000G-C、NBR2000G-C 支持自定义用户对象， NBR108G-P、NBR800G、NBR950G、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 不支持自定义用户对象。

NBR3000G-S 、NBR1000G-C、NBR2000G-C 不支持认证对象和网络实名功能； NBR108G-P、NBR800G、NBR950G、NBR1500G、NBR2000G、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持认证对象和网络实名功能。

NBR3000G-S 、NBR1500G、NBR2000G、NBR1000G-C、NBR2000G-C 不支持通过 mac 地址进行用户校验，NBR108G-P、NBR800G、NBR950G、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持通过 mac 地址进行用户校验。

NBR108G-P 不支持 VLAN 对象。NBR800G、NBR950G、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E 、 NBR2500D-E 、 NBR3000D-E 、 NBR3000D-UE 、 NBR3000G-S 、 NBR1500G 、 NBR2000G 、 NBR1000G-C、NBR2000G-C、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 VLAN 对象。

1.5 配置详解

配置项	配置建议&相关命令	
配置二三层分类识别功能	⚠ 必须配置。用于对数据流进行用户对象识别，否则基于用户的审计和流控策略无法生效。	
	layer23 classify enable	启用二三层分类识别功能
配置二三层全局屏蔽模式	⚠ 可选配置。除非用户加入白名单属性，否则报文默认全部丢弃。	
	layer23 deny-mode enable	开启二三层全局屏蔽模式
配置严格校验模式	⚠ 可选配置。开启后将会丢弃未绑定未正确绑定 IP+MAC 的用户，谨慎使用。	
	layer23 strict-verification enable	开启严格校验模式

配置 subs 库无感知模式	可选配置。开启 web 认证后使用。	
	layer23 subs-mab enable	开启 subs 库无感知模式
配置二三层流量监测功能	可选配置。开启后，特定时间间隔内未达到流量阈值，设备端强制下线。	
	layer23 flow-detect enable	开启二三层流量检测测
	layer23 flow-detect flow 0	配置无流量下线
	layer23 flow-detect time-interval 15	配置 15 分钟内无流量下线
配置网络对象	可选配置。	
	network-group *str1* **move to parent** *str2*	移动网络对象。
	network-groupexport { **txt** | **csv** } *filename*	导出当前网络对象配置到文件中。
	network-groupimport { **txt** | **csv** } *filename*[**overwrite**]	导入网络对象信息到当前配置中。
	network-groupname*namestr*[**parent** *parent*] [**ip-host** *ip-addr* | **ip-subnet** *subnet mask*| **ip-range** *start end*]]	配置网络对象。
	network-grouprename *oldname newname*	重命名网络对象。
配置用户对象	可选配置。	
	subscriber *str1* **move to parent** *str2*	移动用户对象。
	subscriber allow *string* **privilege** { **none** | { [**webauth**] [**vpn**] [**login**] } }	设置用户账号权限。
	subscriber export { **txt** | **csv** } *filename*	用户对象文件导入到配置中。
	subscriber import { **txt** | **csv** } *filename*[**overwrite**]	导出用户对象配置到文件中。
	subscriber rename *oldname newname*	重命名用户对象。
	subscriber set *namestr* **attribute** { **avoid-monitor** [**flow-monitor**] | **deny** | **release | vip** | **auth-deny** | **pwd-edit | ssl-auth-deny | ssl-radius-verify**}	设置用户对象特殊属性。
	subscriber static name *namestr***parent** *parstr* [[[**ip-host** *ip-addr*] [**mac** *mac-addr*] | **ip-subnet** *subnet mask* **| ip-range** *start end*] [**password** *pwd_str* { **two-way-bind** | **single-way-bind**}] | [**password** *pwd_str*]]	配置用户对象。
配置用户自定义对象	**subscriber custom-group** *namestr* **relate ip-range** *ip_starip_end*	配置用户对象自定义组
	subscriber custom-group *namestr* **attribute {deny | avoid-audit | avoid-fc | release | vip}**	设置用户自定义组属性
配置 vlan 对象	可选配置	

	vlan-group*name***vlan***vid-list*	配置 vlan 对象。

1.5.1 配置二三层分类识别功能

配置效果

- 对数据流分类识别成不同的对象。
- 基于不同对象作相应的行为控制策略。

注意事项

- 二三层分类识别关闭后，基于用户的审计策略和流控策略等将失效。
- 内核模块卸载后，对象依然可以继续配置管理，但是将无法识别。

配置方法

↘ 开启二三层分类识别开关

- 必须配置。
- 若无特殊要求，设备上不要关闭该功能否则将无法基于用户审计和流控。

检验方法

配置基于某个 ip 地址的对象，然后使用该 ip 经过设备访问外网。

- 检查二三层流私有空间中该数据流是否识别成正确的对象。
- 检查对象显示信息该对象是否关联正确的流数量。

相关命令

↘ 开启二三层分类识别开关

【命令格式】 **layer23 classify enable**
【参数说明】 -
【命令模式】 全局模式
【使用指导】 启用二三层分类识别功能后支持基于 vid，基于源 ip 或源 mac，基于目的 ip 的对象识别。

配置举例

↘ 在设备上启用二三层分类识别功能

【配置方法】 设备上开启二三层分类识别开关。

```
Ruijie#configure terminal
Ruijie(config)# layer23 classify enable
Ruijie(config)#end
```

【检验方法】 show run 查看配置文件中，是否有 **layer23 classify enable 命令。**

常见错误

- 基于用户的策略无法生效，二三层分类识别开关被关闭。

1.5.2 配置二三层全局屏蔽模式

配置效果

- 禁止内网用户访问外部网络。
- 允许少部分加入白名单的用户访问外部网络。

注意事项

- 二三层识别功能必须开启。

配置方法

- 可选配置。
- 设备上开启二三层分类识别功能后，开启二三层全局屏蔽模式。

检验方法

使用 show run 查看配置中，是否含有 **layer23 deny-mode enable 命令。**

相关命令

↘ 二三层全局屏蔽模式

【命令格式】 **layer23 deny-mode enable**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 启用二三层全局屏蔽模式后，默认丢弃所有报文，除非用户对象排除屏蔽，即加入到白名单中。

配置举例

↘ 开启二三层全局屏蔽模式，用户对象 A 允许访问外部网络

【配置方法】 设备上开启全局屏蔽模式开关，用户对象 A 设置白名单属性

```
Ruijie#configure terminal
Ruijie(config)# layer23 deny-mode enable
Ruijie(config)# subscriber static name A parent / ip-host 192.168.1.2
Ruijie(config)#subscriber set A attribute release
Ruijie(config)# end
```

【检验方法】 使用不同的 ip 地址访问外部网络。

- 使用任意一个非 192.168.1.2 的 ip 地址，应该不能访问外部网络。
- 使用 192.168.1.2 可以访问外部网络。

常见配置错误

- 误配置二三层全局屏蔽模式，导致全部无法访问外网。

1.5.3 配置严格校验模式

配置效果

- 该模式下，未绑定或未正确绑定 IP+MAC 的用户将被限制无法正常接入网络。

注意事项

- 开启该模式前，请先绑定 IP+MAC 用户。

配置方法

- 可选配置。
- 开启该模式后，将合法终端加入 IP+MAC 绑定用户中。

检验方法

使用 show layer23 strict-verification 查看开关是否正常开启。

相关命令

↘ 严格校验模式

【命令格式】 **layer23 strict-verification enable**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 启用该模式后，未绑定或未正确绑定 IP+MAC 的用户的报文将被直接丢弃。

配置举例

↘ 开启严格校验模式，只允许 test 账号（1.1.1.1, 00d0.f822.33ef）上网。

【配置方法】 设备上开启严格校验模式，将 test 加入 IP+MAC 绑定用户。

```
Ruijie#configure terminal
Ruijie(config)# layer23 strict-verification enable
Ruijie(config)# subs static name test parent / ip-host 1.1.1.1 mac 00d0.f822.33ef
Ruijie(config)# end
```

【检验方法】 test 用户可以正常上网，其他用户都无法正常上网。

- test 可以正常接入网络上网。
- test 手动更改终端 IP 地址，将无法上网。
- 其他终端使用 1.1.1.1 也无法正常上网。

常见配置错误

- IP/MAC/用户冲突。

1.5.4 配置内置无感知模式

配置效果

- 首次接入网络进行 web 认证后，后续接入网络不需要再次认证。

注意事项

- 和 web 认证功能同时使用。

配置方法

- 可选配置。
- 设备上开启 web 认证后，开启 subs 无感知模式。

检验方法

使用 show run 查看配置中，是否含有 **layer23 subs-mab enable 命令。**

相关命令

↘ subs 无感知模式

【命令格式】 **layer23 subs-mab enable**

【参数说明】 **-**

【命令模式】 全局模式

【使用指导】 启用 subs 无感知模式后，首次 web 认证通过后会记录 MAC 地址，后续接入后直接 MAC 地址校验无需输入用户名和密码进行认证。

配置举例

↘ 开启 subs 无感知模式，用户对象 A 首次认证后，后续无需再进行 web 认证。

【配置方法】 设备上开启内置 web 认证后，配置相关用户名和密码后，配置 subs 无感知模式

```
Ruijie#configure terminal
Ruijie(config)# layer23 subs-mab enable
Ruijie(config)# end
```

【检验方法】 用户首次接入进行 web 认证后，下线再次上线。

- 首次接入需要输入用户名密码进行 web 认证。
- 下线后再次上线无需输入用户名和密码，直接可以上网。

常见配置错误

- 无。

1.5.5 配置二三层流量检测下线

配置效果

- 认证上线的 ip 特定时间内无流量将强制下线。

注意事项

- 流量检测下线只针对认证上线且同步到二三层的账号。

- 需要同时开启流量审计功能。

配置方法

- 可选配置。
- 设备上开启流量审计功能和二三层识别功能后，配置 web 认证并且认证成功上线后，配置流量检测功能。

检验方法

使用 show run 查看配置中，是否含有 **layer23 flow-detect enable** 及对应的流量和时间参数。

开启 web 认证功能认证上线后，配置流量检测下线后，等待特定时间内未达到流量参数，观察设备已经将该 ip 踢下线。

相关命令

↘ 二三层流量检测开关

【命令格式】 **layer23 flow-detect enable**
【参数说明】 -
【命令模式】 全局模式
【使用指导】 启用二三层流量检测功能后，特定时间间隔内未达到流量的在线节点将被强制下线。

↘ 二三层流量检测流量参数配置

【命令格式】 **layer23 flow-detectflow** *flowrate*
【参数说明】 *flowrate* 流量参数，单位 bit/s
【命令模式】 全局模式
【使用指导】 流量参数取 30s 内流量总和的平均值。

↘ 二三层流量检测时间间隔参数配置

【命令格式】 **layer23 flow-detecttime-interval** *time*
【参数说明】 *time* 时间参数
【命令模式】 全局模式
【使用指导】 时间间隔内连续未达到流量的在线节点将被踢下线。

配置举例

↘ 开启二三层流量监测功能，配置 15 分钟内无流量下线

【配置方法】 设备上开启全局屏蔽模式开关，配置二三层流量检测下线参数

```
Ruijie#configure terminal
Ruijie(config)# layer23 flow-detect enable
Ruijie(config)# layer23 flow-detect flow 0
Ruijie(config)#layer23 flow-detect time-interval
Ruijie(config)# end
```

【检验方法】 开启 web 认证功能，同时开启二三层流量检测下线功能。

- 192.168.1.2 使用账号 1，认证在线。
- PC 更改 ip 地址为 192.168.1.3，使用账号 2 认证上线。
- 192.168.1.2 没有流量，等待 15 分钟后，观察 192.168.1.2 已经被设备剔除下线。

常见配置错误

- 流量参数理解错误，单位是 bit/s 不是累加总和的流量。
- 流量检测下线需要依赖流量审计功能。

1.5.6 配置支持 sam 同账号分属不同组功能

配置效果

- 同一个 sam 账号同属多个运营商组信息下发到设备端，支持全部显示。

注意事项

- 该功能只针对 sam 服务器同步的账号。

配置方法

- 可选配置。
- 设备上开启 link-sam 联动后，配置该命令后支持 sam 同账号分属不同的信息下发。

检验方法

使用 show run 查看配置中，是否含有 **layer23 sam-accip-relate enable。**

开启该功能后，show auth-subs brief 查看显示 sam 账号名称是否组合了组名称信息。

```
root(auth-subs group)
    smp_root(auth-subs group)
    sam_root(auth-subs group)
        CMII(auth-subs group)
            CMII:111:111(auth-subs group)
        CMCC(auth-subs group)
            CMCC:111:111(auth-subs group)
    webauth_root(auth-subs group)
```

相关命令

sam 同账号分属不同组功能开关

【命令格式】 **layer23 sam-accip-relate enable**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 启用该功能后，二三层识别会将 sam 服务器同步过来的实名信息，包括 ip、账号、组。由于设备端名称惟一性不能属于多个父组，因此在设备端将账号名称组合为**组名:姓名:账号**的形式来保证名称的惟一性，此功能只针对 sam 服务器同步的用户生效。

配置举例

开启 sam 同账号分属不同组功能

【配置方法】 开启 sam 联动功能后，开启 sam 同账号分属不同组功能

```
Ruijie#configure terminal
Ruijie(config)#layer23 sam-accip-relate enable
Ruijie(config)# end
```

【检验方法】 开启 sam 联动功能，同时开启 sam 同账号分属不同组功能。

- show layer23 sam-acc 查看功能开发状态。
- 使用 sam 端账号认证上线后，观察 sam 端同步的账号名称信息是否含有组名称。
- 基于 sam 账号的账号组配置策略，观察策略是否生效。

常见配置错误

- 该功能无法单独使用，需要同时开启 sam 联动功能。
- 不支持非 sam 服务器账号。

1.5.7 配置支持实名信息设置 scc 功能

配置效果

- 将实名账号信息设置到 scc 后，实名信息也可以用于认证 ip 的放行。

注意事项

- 一般情况下，大批量的认证用户为了设备性能考虑，除非存在二次认证的场景，该功能不开启。

配置方法

- cli 下可选配置。
- 一般开启 link-sam 联动或者 snmp 联动，接受实名信息后该功能才生效。

检验方法

使用 show run 查看配置中，是否含有 **layer23 scc-attention enable。**

开启该功能后，show layer23 state 查看开启状态。

相关命令

↘ 实名账号信息设置 scc 功能开关

【命令格式】 **layer23 scc-attention enable**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 启用该功能后，二三层识别会将服务器同步过来的实名信息，全部设置到 scc 模块。
为了性能优化，一般场景下该功能可以不开启。
二次认证的场景下，接入交换机和设备同时开启认证，接入交换机认证通过后不需要再进行二次认证，此时该功能需要开启。

配置举例

↘ 开启实名账号信息设置 scc 功能

【配置方法】 开启 sam 联动功能后，开启 sam 同账号分属不同组功能

```
Ruijie#configure terminal
Ruijie(config)#layer23 scc-attention enable
Ruijie(config)# end
```

【检验方法】 开启实名账号信息设置 scc 功能。

- show layer23 state 查看功能开发状态。
- show run 查看 layer23 scc-attention enable 命令。
- 开启关闭该功能，debug scc user author 查看 scc 表项中是否存在用户管理同步的认证 ip。

常见配置错误

- 该功能一般和实名账号信息联动功能一起使用，SAM/SMP/ESS 服务器。

1.5.8 配置网络对象

配置效果

- 将 ip 地址和网络对象名称关联起来。
- 基于不同网络对象作特殊行为控制。

注意事项

- 基于网络对象的策略生效必须要开启二三层分类识别功能。
- 网络对象名称不允许相同，且一个 IP 地址只能属于一个网络对象。

配置方法

↘ 移动网络对象

- 可选配置。
- 设备上移动网络对象改变当前网络对象所属路径。

↘ 导出网络对象

- 可选配置。
- 设备上将当前网络对象配置导出到文件中。

↘ 导入网络对象

- 可选配置。
- 设备上将文件中的网络对象信息导入到当前配置中。

↘ 配置网络对象

- 可选配置。
- 设备上配置网络对象将对象名称和 ip 地址信息关联起来。

重命名网络对象

- 可选配置。
- 设备上不改变对象属性及组织结构的基础上更改其名称。

检验方法

配置一个网络对象关联一个 ip 地址，使用内网任一 PC 访问该网络对象配置的 IP 地址。

- 检查 show run 中是否含有网络对象的配置信息。
- 检查二三层流私有空间中该流是否正确匹配中网络对象。

相关命令

移动网络对象

【命令格式】 **network-group** *str1* **move to parent** *str2*

【参数说明】 *str1*-需要移动的网络对象名称

str2-移动之后的所在父对象名称

【命令模式】 特权模式

【使用指导】 该命令主要用于不改变原网络对象下其他属性以及其子节点层次结构的情况下，改变其所属路径。

导出网络对象

【命令格式】 **network-groupexport** { **txt** | **csv** } *filename*

【参数说明】 *filename*-文件名

【命令模式】 特权模式

【使用指导】 该命令主要用于批量导出网络对象，将目前系统中的网络对象配置导出到外部文件中。

导入网络对象

【命令格式】 **network-groupimport** { **txt** | **csv** } *filename*[**overwrite**]

【参数说明】 *filename*-文件名

【命令模式】 特权模式

【使用指导】 该命令主要用于批量导入网络对象到当前配置宏去。

txt 格式文件里编写网络对象格式如下：文件每行代表一个网络对象，对象的各个元素的顺序如：路径、对象名称、ip 地址。网络对象中每个元素用“,”隔开，没有内容的项可以空着，但是“,”要保留，如：最后一列不存在，那么保留“,”在行末。

下面是“.txt”网络对象文件中的一条网络对象记录的举例：

/所有用户/用户组 1,用户 1,192.168.197.1

csv 格式的文件在 Microsoft Excel 中编辑后点击另存为“.csv”格式即可得到该格式的文件。文件中记录的编辑格式为：一条记录分为 4 列，分别为：父对象路径、对象名称、对象 ip 地址。

正常模式下，冲突网络对象会创建失败。overwrite 模式下，将删除一切冲突的网络对象包括名称冲突，ip 冲突然后创建新对象。

配置网络对象

【命令格式】 **network-groupname***namestr*[**parent** *parent*] [**ip-host** *ip-addr* | **ip-subnet** *subnet mask*| **ip-range** *start end*]]

【参数说明】 *namestr*-网络对象名称

parent-父对象所属路径

ip-addr-单 IP 地址

subnet-ip 段起始地址

mask-掩码

start-ip-range 起始地址

end-ip-range 结束地址

【命令模式】 全局模式

【使用指导】 网络对象只有 ip 地址信息，分为单 ip 地址网络对象、ip 地址段网络对象及 ip 地址范围网络对象三种。

默认存在一个默认对象“/”，当启用二三层分类识别时，报文目的 ip 地址匹配不中其他任意一个网络对象则默认匹配中默认对象“/”。当 parent 字段不设置时，默认在根目录下。

网络对象名称是惟一的，不同网络对象名称之间不能相同。

重命名网络对象

【命令格式】 **network-grouprename** *oldname newname*

【参数说明】 *oldname*-原网络对象名称

newname-新网络对象名称

【命令模式】 特权模式

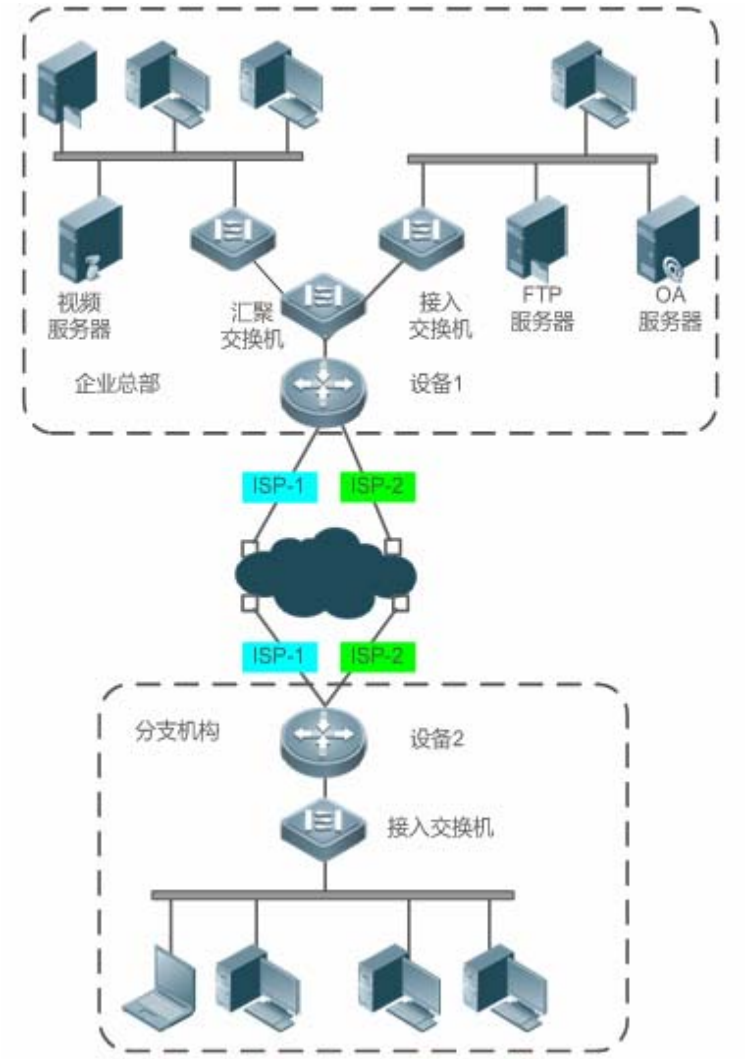
【使用指导】 该命令主要用于不改变原网络对象下其他属性的同时，改变该网络对象的名称。

配置举例

以下仅介绍二三层分类识别相关的命令。

访问外部服务器优先保障，总部内部服务器 IP 地址为 123.123.123.123

【网络环境】



【配置方法】 开启二三层分类识别开关。

设备 2 通过 vpn 拨入设备 1。

配置基于总部设备内部服务器 IP 地址的网络对象 A。

配置基于网络对象 A 的流控保障策略

EG2

```
Ruijie#configure terminal
Ruijie(config)# layer23 classify enable
Ruijie(config)# network-group name A parent / ip-host 123.123.123.123
Ruijie(config)#end
```

【检验方法】 使用 **show network-group by-name** *A* **kernel** 查看该对象是否有关联的流数量。

```
name                              flow dir index ip
A                                 5      0  37160   123.123.123.123
```

常见错误

- 配置网络对象后，二三层分类识别功能未开启导致无法识别。
- 网络对象配置错误配置成基于内网用户的 IP 地址导致无法匹配命中。

1.5.9 配置用户对象

配置效果

- 将 ip 地址、mac 地址、密码、手机号码和用户对象名称关联起来。
- 基于不同用户对象作特殊行为控制。

注意事项

- 基于用户对象的策略生效必须要开启二三层分类识别功能。
- 用户对象名称不允许相同，且一个双向绑定的 IP 地址或 MAC 地址只能属于一个用户对象。

配置方法

↘ 移动用户对象

- 可选配置。
- 设备上移动用户对象改变当前用户对象所属路径。

↘ 导出用户对象

- 可选配置。
- 设备上将当前用户对象配置导出到文件中。

↘ 导入用户对象

- 可选配置。
- 设备上将文件中的用户对象信息导入到当前配置中。

↘ 配置用户对象

- 可选配置。
- 设备上配置用户对象将对象名称和 ip 地址、mac 地址和密码等信息关联起来。

↘ 重命名用户对象

- 可选配置。
- 设备上不改变对象属性及组织结构的基础上更改用户对象名称。

↘ 设置用户对象权限

- 可选配置。
- 设备上对配置了密码的用户账号设置使用权限，是否允许 web 认证、vpn 认证使用。

设置用户对象特殊属性

- 可选配置。
- 设备上对用户对象设置特殊标志以便作特殊处理。

检验方法

配置一个用户对象双向绑定一个 ip 地址并对该对象设置屏蔽属性，使用该 IP 地址经过网关访问外网。

- 检查 show run 中是否含有用户对象的配置信息。
- 检查二三层流私有空间中该流是否正确匹配中用户对象。
- 使用该 IP 地址应该不能访问外网，使用其他 IP 地址可以正常访问外部网络。

相关命令

移动用户对象

【命令格式】 **subscriber***str1* **move to parent** *str2*
【参数说明】 *str1*-需要移动的用户对象名称
str2-移动之后的所在父对象名称
【命令模式】 特权模式
【使用指导】 该命令主要用于不改变原用户对象下其他属性以及其子节点层次结构的情况下，改变其所属路径。

导出用户对象

【命令格式】 **subscriberexport** { **txt** | **csv** } *filename*
【参数说明】 *filename*-文件名
【命令模式】 特权模式
【使用指导】 该命令主要用于批量导出用户对象，将目前系统中的用户对象配置导出到外部文件中。

导入用户对象

【命令格式】 **Subscriber import** { **txt** | **csv** } *filename*[**overwrite**]
【参数说明】 *filename*-文件名
【命令模式】 特权模式
【使用指导】 该命令主要用于批量导入用户对象到当前配置宏去。
txt 格式文件里编写用户对象格式如下：文件每行代表一个用户对象，对象的各个元素的顺序如：路径、账号名称、密码、ip 地址、MAC 地址、是否双向绑定标志、是否免识别、审计，是否免流控(设置为 Y 时 免识别自动设置为 Y)，是否 VIP 用户，是否设置为白名单，是否禁止上网，是否允许修改密码，是否禁止 web 认证登录，是否作为 vpn 分支机账号(一般情况下用户不要编辑该标志)，是否允许 web 认证账号权限，是否允许 vpn 认证账号权限，是否禁止 sslvpn 认证登录，sslvpn 账号本地密码是否不校验，手机号码(选填)。用户对象中每

个元素用“,”隔开，没有内容的项可以空着，但是“,”要保留，如：最后一列不存在，那么保留“,”在行末。

下面是“.txt”用户对象文件中的一条用户对象记录的举例：

/所有用户/用户组 1,用户 1,,192.168.197.1,,

csv 格式的文件在 Microsoft Excel 中编辑后点击另存为“.csv”格式即可得到该格式的文件。文件中记录的编辑格式为：一条记录分为 4 列，分别为：父对象路径、对象名称、密码、对象 ip 地址、mac、是否双向绑定标志、是否免识别、审计，是否免流控(设置为 Y 时 免识别自动设置为 Y)，是否 VIP 用户，是否设置为白名单，是否禁止上网，是否允许修改密码，是否禁止 web 认证登录，是否作为 vpn 分支机账号(一般情况下用户不要编辑该标志)，是否允许 web 认证账号权限，是否允许 vpn 认证账号权限，是否禁止 sslvpn 认证登录，sslvpn 账号本地密码是否不校验，手机号码(选填)。

正常模式下，冲突用户会创建失败。overwrite 模式下，将删除一切冲突的用户对象包括用户名称冲突，ip 冲突，mac 冲突然后创建新对象。

配置用户对象

【命令格式】 **subscriber static name** *namestr* **parent** *parstr* [[[**ip-host** *ip-addr*] [**mac** *mac-addr*] | **ip-subnet** *subnet mask* **|** **ip-range** *start end*] [**password [0 | 6 | 7]** *pwd_str* { **two-way-bind** | **single-way-bind** }] | [**password [0 | 6 | 7]** *pwd_str*]] [**phone** *phone_number*]

【参数说明】 *namestr*-网络对象名称

parstr-父对象所属路径

ip-addr-单 IP 地址

mac-addr-mac 地址

subnet-ip 段起始地址

mask-掩码

start-ip-range 起始地址

end-ip-range 结束地址

pwd_str-密码，其中 0 明文密码，6 为 md5 密码，7 为密文密码

phone_number-密码

【命令模式】 全局模式

【使用指导】 用户对象的 ip 地址不能和除父对象之外的用户对象存在冲突，mac 地址则不能和其他任何用户对象冲突。

用户对象以 ip 地址分类有单 ip 地址用户对象、ip 地址段用户对象和 ip 地址范围用户对象三种，以 mac 地址分类有包含 mac 地址的用户对象和不包含 mac 地址的用户对象两种，其中单 ip 地址的用户对象可以同时包含 mac 地址 ,ip 地址段和 ip 地址范围用户对象不可以同时包含 mac 地址。当 mac 地址和 ip 地址同时匹配中，以 mac 地址的匹配结果为准。

默认存在一个默认用户对象“/”,开启二三层分类识别功能时，若报文的源 ip 地址匹配不中其他任意一个用户对象则默认匹配中默认对象。

普通用户对象设置密码后可以作为账号使用，单双向绑定只针对含有 ip 或者 mac 的账号，双向绑定时，账号和 ip 或 mac 之间双向绑定 ,账号只能使用某段 IP 或者 mac ,而 ip 或 mac 也只能被该账号使用。单向绑定时，该账号只能使用绑定 ip 或者 mac，但是该段 ip 或者 mac 地址还可能被其他账号使用。

不绑定 ip 和 mac 的账号表示该账号不受使用的 ip 或 mac 地址的限制 ,含有 ip 和 mac 的账号默认为双向绑定。

内置认证下，使用其中账号上线后，会自动添加在账号下，不是使用该树中的账号上线的 ip 还是添加在 webauth_root 下。

配置了手机号码的用户，支持本地短信认证进行校验，校验通过后可以正常接入网络。

用户对象名称是惟一的，不同用户对象之间名称不能相同。

重命名用户对象

【命令格式】 **Subscriber rename** *oldname newname*

【参数说明】 *oldname*-原用户对象名称

newname-新用户对象名称

【命令模式】 特权模式

【使用指导】 该命令主要用于不改变原用户对象下其他属性的同时，改变该用户对象的名称。

设置用户对象权限

【命令格式】 **subscriber allow** *string* **privilege** { **none**| { [**webauth**] [**vpn**] [**login**] } }

【参数说明】 *string*-用户对象名称

【命令模式】 全局模式

【使用指导】 设置账号的使用权限，可以都不允许使用或者允许 login 认证，vpn 认证和 web 认证之一，之二，之三。

设置用户对象特殊属性

【命令格式】 **subscriber set** *namestr* **attribute** {**avoid-monitor**[**flow-monitor**] | **deny** | **release | vip** | **auth-deny** | **pwd-edit | ssl-auth-deny | ssl-radius-verify**}

【参数说明】 *namestr*-用户对象名称

【命令模式】 全局模式

【使用指导】 设置免监控属性后默认不对该用户进行流量控制、内容审计和应用识别，但可以设置 flow-monitor 对该用户开启流量控制。

屏蔽属性在屏蔽模式下不生效，正常模式下设置了屏蔽属性则丢弃该用户的报文。

屏蔽属性只在非屏蔽模式下生效，非屏蔽模式下如果免监控和屏蔽属性同时设置，以屏蔽属性作为优先。

白名单属性只在屏蔽模式下生效，开启屏蔽模式后，默认所有用户都不能上网，除非设置用户的白名单属性“release”。

vip 属性用来对用户做流控统一处理，设置了 vip 属性的静态用户对象可以统一做流控处理。

auth-deny 属性用来设置账号的认证屏蔽属性，只在开启内置认证情况下有效。设置后，使用该账号无法认证上线，已经使用该账号在线的用户，也会被下线。

pwd-edit 属性用例设置账号的认证修改密码属性，只在开启内置认证情况下有效。设置后，使用该账号上线的用户可以自行修改密码。

ssl-auth-deny 属性用于设置账号（组）的 sslvpn 认证属性。设置后，配置该属性的账号或继承了配置该属性的账号组下的账号，将在 sslvpn 认证过程中无法认证通过.

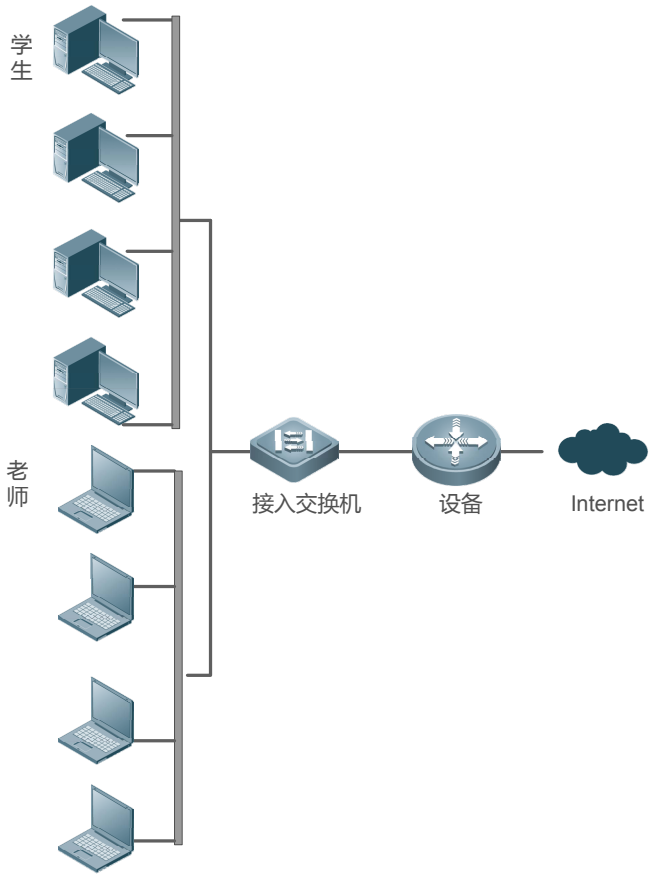
ssl-radius-verify 属性用于设置账号（组）的 sslvpn 本地账号密码不校验认证属性。设置后，sslvpn 的本地账号即使存在依然不对密码进行校验，返回超时便于接下来在 radius 服务器端进行账号和密码校验。

配置举例

以下仅介绍二三层分类识别相关的命令。

↘ 高校场景中，对所有学生的上网行为进行审计和控制，老师不受限制，老师所使用的 ip 段地址为 192.168.100.2-192.168.200.254

【网络环境】



【配置方法】 开启二三层分类识别开关。配置基于老师所属 IP 段地址的用户对象 A。
配置全局审计和流控策略。
设置用户对象 A 的免监控属性。
配置自定义组 B，关联 192.168.100.2-192.168.100.3
针对自定义组 B 配置流控策略

网关

```
Ruijie#configure terminal
Ruijie(config)# layer23 classify enable
Ruijie(config)# subscriber static name A parent / ip-range 192.168.100.2 192.168.200.254
Ruijie(config)# subscriber set A attribute avoid-monitor
Ruijie(config)# subscriber custom-group B relate ip-range 192.168.100.2 192.168.100.3
Ruijie(config)#end
```

【检验方法】 使用学生所属的 IP 地址上网收到审计和流量控制，使用老师所属 IP 地址不受限制。

```
name                              mac              flow  dir dym av-fc av-con vip rel deny bind
h-pwd on-line on-del index          ssl-radius ip
A                                 0000.0000.0000   20     0    0   1     1      0   0   0    2
0     0       0     1233483802  0            192.168.100.2 - 192.168.200.254

Ruijie#show subscriber custom-group all
name                               custom cnt  index
B                                 1      1    2973161921

Ruijie#show subscriber custom-group name B relate-all
b relate-all:
192.168.100.2—192.168.100.3
```

常见错误

- 配置用户对象后，二三层分类识别功能未开启导致无法识别。
- 用户对象特殊属性错误配置，导致功能无法生效。

1.5.10 配置用户自定义组

配置效果

- 将 ip 地址、mac 地址和用户对象自定义组名称关联起来。
- 对自定组名称设置特殊属性
- 基于不同用户自定义组名称的流控、行为审计策略。

注意事项

- 基于用户自定义组的策略生效必须要开启二三层分类识别功能。
- 自定义组名称和用户对象名称不允许相同。

配置方法

↘ 配置用户自定义组

- 可选配置。
- 设备上配置用户自定义组将名称和 ip 地址/ip 段关联起来，且 IP 段之间允许冲突，配置易用性提升。

↘ 设置用户自定义组特殊属性

- 可选配置。
- 设备上对已识别的用户自定义组对象做特殊行为处理。

检验方法

配置一个用户自定义组关联 IP 端 192.168.1.2 – 192.168.1.4 并设置屏蔽属性，使用该 IP 地址段经过网关访问外网。

- 检查 show run 中是否含有用户自定义组的配置信息。
- 使用该 192.168.1.2 – 192.168.1.4 不能访问外网，使用其他 IP 地址可以正常访问外部网络。

相关命令

↘ 配置用户对象自定义组

【命令格式】 **subscriber custom-group** *namestr* **relate ip-range** *ip_starip_end*

【参数说明】 *Namestr*：用户对象名称

ip_star：IP 起始地址

ip_end：IP 结束地址

【命令模式】 全局模式

【使用指导】 配置用户对象自定组对象可以关联任意用户组织上存在或者不存在的 IP 段，允许关联的 IP 段冲突。

↘ 设置用户自定义特殊属性

【命令格式】 **subscriber custom-group** *namestr* **attribute attribute {deny | avoid-audit | avoid-fc | release | vip}**

【参数说明】 *namestr*-用户对象名称

【命令模式】 全局模式

【使用指导】 设置免流控属性后默认不对该用户进行流量控制。

设置免审计属性后，默认不对该用户进行内容审计和应用识别。

屏蔽属性在屏蔽模式下不生效，正常模式下设置了屏蔽属性则丢弃该用户的报文。

屏蔽属性只在非屏蔽模式下生效，非屏蔽模式下如果免监控和屏蔽属性同时设置，以屏蔽属性作为优先。

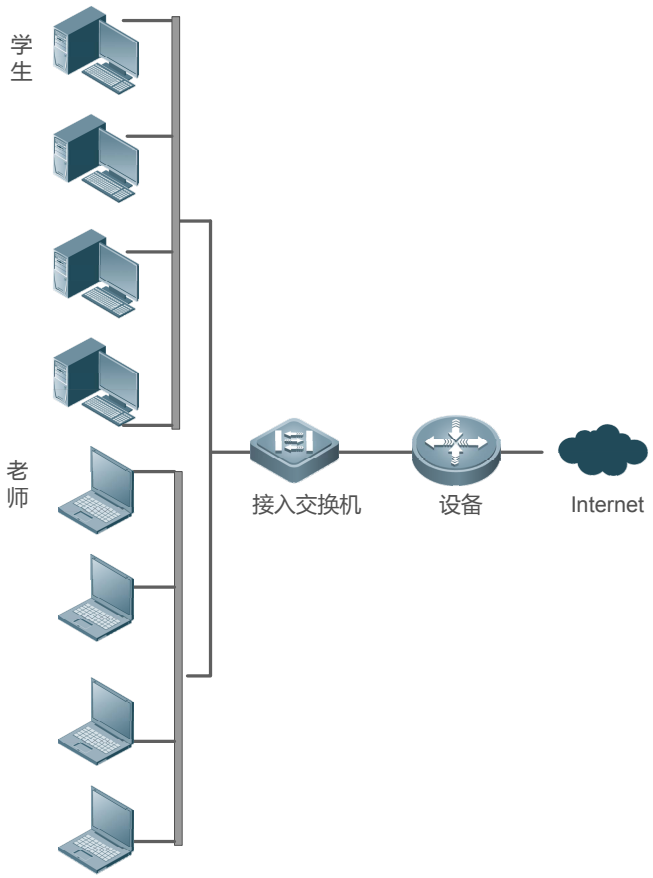
白名单属性只在屏蔽模式下生效，开启屏蔽模式后，默认所有用户都不能上网，除非设置用户的白名单属性“release”。

配置举例

以下仅介绍二三层分类识别相关的命令。

↘ 高校场景中，对所有学生的上网行为进行审计和控制，老师不受限制，老师所使用的 ip 段地址为 192.168.100.2-192.168.200.254

【网络环境】



【配置方法】 开启二三层分类识别开关。配置基于老师所属 IP 段地址的用户对象 B。

配置全局审计和流控策略。

设置用户对象 B 的免流控控属性和免审计属性。

网关

```
Ruijie#configure terminal
Ruijie(config)# layer23 classify enable
Ruijie(config)# subscriber custom-group B relate ip-range 192.168.100.2 192.168.100.4
Ruijie(config)# subscriber custom-group B attribute avoid-fc
Ruijie(config)# subscriber custom-group B attribute avoid-audit
Ruijie(config)#end
```

【检验方法】 使用学生所属的 IP 地址上网收到审计和流量控制，使用老师所属 IP 地址不受限制。

```
Ruijie#show subscriber custom-group all
name                              custom cnt   deny  av-au  av-fc  release  vip  index
B                               1      1     0     1     1     0      0     2973161921

Ruijie#show subscriber custom-group name B relate-all
b relate-all:
192.168.100.2-192.168.100.4
```

常见错误

- 配置用户自定义组后，二三层分类识别功能未开启导致无法识别。

1.5.11 配置 vlan 对象

配置效果

- 将 vlan id 和二层对象名称关联起来。
- 基于不同 vlan 对象作特殊行为控制。

注意事项

- 基于 vlan 对象的策略生效必须要开启二三层分类识别功能。
- vlan 对象名称不允许相同，且一个 vid 只能属于一个 vlan 对象。

配置方法

↘ 配置 vlan 对象

- 可选配置。
- 网关上配置 vlan 对象将名称和 vid 关联起来。

检验方法

配置一个 vlan 对象关联一个 vid，使用 pc 属于该 vid 访问外网。

- 检查 show run 中是否含有 vlan 对象的配置信息。
- 检查二三层流私有空间中该流是否正确匹配中 vlan 对象。

相关命令

↘ 配置 vlan 对象

【命令格式】 **vlan-group***name***vlan***vid-list*

【参数说明】 *name*-vlan 对象名称

vid-list-vlan 对象所属 vid

【命令模式】 全局模式

【使用指导】 启用二三层分类识别功能后支持基于 vid，基于源 ip 或源 mac，基于目的 ip 的对象识别。

配置举例

配置 vid 1-7 都属于 vlan 对象 A

【配置方法】 网关上开启二三层分类识别开关，配置 vlan 对象。

```
Ruijie#configure terminal
Ruijie(config)# vlan-group A vlan 1-7
Ruijie(config)#end
```

【检验方法】 show run 查看配置文件中，是否有 **layer23 classify enable 命令。**

常见错误

- 基于 vlan 对象的策略无法生效，二三层分类识别开关被关闭。

1.6 监视与维护

清除各类信息

无

查看运行情况

作用	命令
显示网络对象信息。	**show network-group** [**all** | **brief** | **parent** [*name* |**root**]]
显示用户对象所有信息。	**show subscriber** { **all** | **brief** | **parent** [*name* |**root**]}
显示用户自定义信息	**show subscriber custom-group {all | name** *namestr* **relate-all}**
根据名称显示 vlan 对象信息。	**show vlan-group** [*name-str*]
显示认证对象信息	**show auth-subs** [**all** | **brief** |**parent** [*name* |**root**] | **dynamic** { **all** | **by-parent** xxx }]
显示 subs 库无感知模式状态	**show subs-mab state**
显示严格校验模式状态	**show layer23 strict-verification**

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
打开用户对象的用户空间调试开关。	**debug subscriber proc-info**
打开用户对象的内核空间调试开关。	**debug subscriber ker-info**
打开网络对象的用户空间调试开关。	**debug network proc-info**

打开网络对象的内核空间调试开关。	**debug network ker-info**

2 APP-IDENTIFY

2.1 概述

应用识别是指对网络中的数据流按照应用特征进行分类识别。应用识别的识别过程主要是分析数据流的报文载荷特征和报文流量特征，从而获知数据流的应用协议类型。应用识别为其他功能模块（如流量控制，流量审计等）提供应用分类信息。应用识别在出口设备中作为基础功能模块使用。

当前应用路由模块实现的应用分流，依赖于流的首包识别技术。对于 TCP 流，因为它前面的握手报文没有载荷，很难通过 DPI (Deep Packet Inspection，深度包检测)规则实现首包识别。

2.2 典型应用

典型应用	场景描述
出口网关部署	出口网关设备部署应用识别

2.2.1 出口网关部署

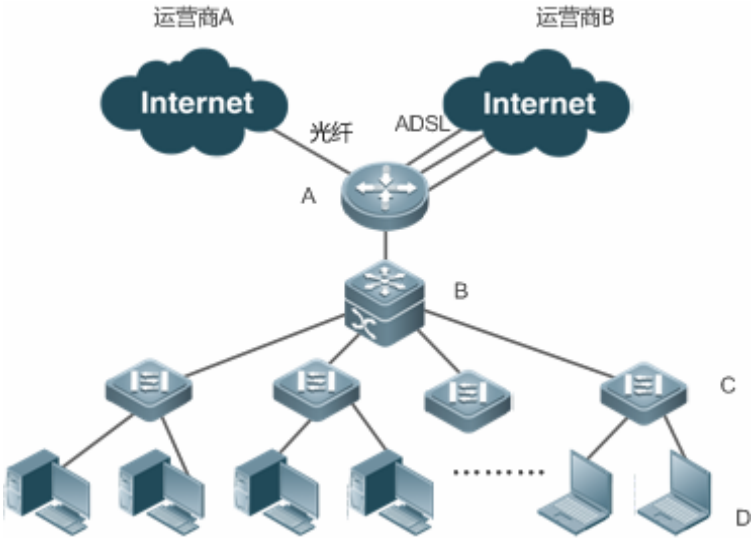
应用场景

出口网关可以连接多条运营商线路，比如一条电信光纤线路和一条联通 ADSL（Asymmetric Digital Subscriber Line ，非对称数字用户环路）线路，或者一条电信光纤线路和多条联通 ADSL 线路。

依赖应用识别的功能有：

- 流量控制功能
- 流量审计功能
- 应用路由功能
- 内容审计功能

图 2-1 出口网关典型应用场景



【注释】 A 为出口网关设备
B 为核心交换机。
C 为接入交换机。
D 为内网用户 PC。

功能部属

- 基本 NAT 上网功能：完成基本的 NAT 地址转换，保障用户正常上网。
- 应用识别功能：完成转发流量的应用识别，配合流控功能实现基于应用的流量控制等功能。
- 应用路由功能：以应用识别为基础，实现大流量应用或者重点应用的流量能够走指定的出口。
- 多链路负载均衡功能：完成数据流在多条链路的合理分配，确保多条链路的带宽利用合理。
- 流量控制功能：和应用识别结合，实现对 P2P 下载流量的抑制，实现对重点应用流量的保障等功能。
- 流量审计功能：和应用识别结合，提供基于应用的流量报表，让用户了解出口的网络带宽是否够用，是否需要扩容。

2.3 功能详解

基本概念

↘ 数据流

数据流的含义为报文的五元组相同的报文流。根据协议的不同通常定义的数据流有三种不同类别：TCP 流、UCP 流、IP 流（专门针对非 TCP/UDP 应用）。五元组分别定于如下：

流类别	五元组标识
TCP 流	源 IP 地址|目的 IP 地址|IP 协议|TCP 源端口|TCP 目的端口
UDP 流	源 IP 地址|目的 IP 地址|IP 协议|UDP 源端口|UDP 目的端口

IP 流	源 IP 地址|目的 IP 地址

↘ 应用路由

为了有效利用网络资源，业界提出一种有效的方法，就是为企业、网吧租用两条（或多条）广域网链路，其中一条高质量线路用于传输对网络传输时延、抖动等特性敏感的关键应用，另一条低质量线路用于传输 P2P 等下载应用。此种情况，就需要出口网关设备能够根据应用进行报文路由。基于应用的路由，简称应用路由，区别于传统的基于报文目的 IP 选路的 IP 路由技术，是一种根据数据流的应用类型进行路由转发的技术。基于这种技术，可以将不同应用类型的数据流分流到不同的出口，以达关键业务与抑制业务各行其道，减少影响的目的。应用路由的最大问题就是如何实现数据流的首报文识别。应用路由相关请参看相关解释。

↘ 首包识别

首包识别要求在每个流的第一个报文实现对这个流的识别。做到首包识别才能保证应用路由的效果。因为如果在数据流中间识别再去应用路由的话，必然导致一个流从至少两个不同线路对外通信，会导致断流。注意区分首包识别与第一个载荷报文，对于 TCP 流，首包为握手报文，而第一个载荷报文为请求报文。

功能特性

功能特性	作用
特征库升级	更新设备的特征库。
应用协议对象管理	管理应用协议对象。
应用识别	开启应用识别。

2.3.1 特征库升级

随着软件版本的更新升级，应用软件产生的报文特征有可能会发生变化。通过特征库升级，更新匹配的报文特征，使得应用识别在不需要更新软件版本的前提下，能够保持准确有效的识别能力。

工作原理

锐捷已有专门的特征库分析团队，并制定出了成熟的特征分析流程。该团队根据流程，分析各个应用的报文特征，并不断地更新到特征库中。

可以通过 WEB 页面提供的下载应用分类库地址下载特征库，或者通过客服获取特征库，然后通过 WEB 页面升级本地特征库；另外，也可以通过 WEB 设置自动更新特征库，自动从锐捷特征库服务器上更新最新版本的特征库，更为方便，并能自动及时更新特征库。

特征库升级是将特征库压缩包（app_signature.upd）进行分析处理，形成应用识别相关的匹配规则。

特征库升级成功后，应用识别模块会将特征库保持到 FLASH 中，当设备重启后，则主动升级 FLASH 中保存的特征库。

相关配置

↘ 升级特征库

缺省情况下，模块加载后大约一分钟开始解析 FLASH 中的特征库。

通过 **show identify-application version** 可以查看当前特征库版本。

特征库升级不成功，则设备使用原有的特征库。若模块加载后，FLASH 中无特征库，则解析特征库失败。若设备无特征库，应用识别模块由于无匹配规则，不会进行应用识别，包括自定义应用规则匹配。保持设备使用最新版本的特征库，能够使得应用识别准确率更高。

2.3.2 应用协议对象管理

通过对应用协议对象进行分组，方便应用协议对象管理。通过配置自定义应用，用户可以根据五元组信息定义应用协议对象，并将自定义应用协议对象加入应用分组中进行管理。

工作原理

↘ 特征库协议对象

通过特征库解析，生成应用识别的分类对象，并形成特征库协议树，其组织形式如下图：

图 2-2 协议树



按照应用协议分类->应用软件->应用软件子类这 3 个层次组织。在系统中以树形式组织。

↘ 自定义应用

符合特定五元组属性的报文，定义为一应用类型，成该类型为自定义应用。

用户自定义应用的匹配，是针对 TCP、UDP 和 IP 协议报文的处理，在报文中提取出源 ip，目的 ip，协议号，源端口信息，目的端口信息后，快速的查找用户自定义应用数据结构，判断是否有匹配的自定义应用。

用户自定义应用在配置时和应用共同与特征解析的应用使用同一颗树，整个系统只有一颗应用树，该树中包含了应用和用户自定义应用。

↘ 应用分组

应用分组有两种模式：

- 一种是按缺省系统支持的应用分类分组（至少应用分类有：“即时通讯软件”、“"IP 网络电话”，“网络游戏软件”、“视频流媒体软件”、“P2P 应用软件”、“股票软件”、“互联网文件传输”、“电子邮件协议”、“数据库”、“网络管理协议”、“路由协议”、“安全协议”、“隧道应用软件”、“远程访问协议”、“网络应用更新”、“网银软件”、“网络硬盘软件”、“软件更新类”、“移动互联网下载工具”、“移动互联网视频影音”、“移动互联网网盘”、“移动互联网软件更新”、“移动互联网即时通讯”、“移动互联网游戏”、“移动互联网社交软件”、“移动互联网 WEB 浏览,”、“移动互联网股票”、“RFC” 等）；
- 一种是按用户自己的需求创建的应用分组，称自定义应用分组。自定义应用分组分为如下两类：

1. 系统预设的用户自定义应用分组：系统预设了关键应用组、抑制应用组、阻断应用组、IP 协议组四个应用组分组，用户不可以修改这些应用分组的名字，用户可以把缺省系统支持的各种应用分组，或者是应用分组下的某种应用，加入到以上四个用户自定义应用分组中。
2. 普通的用户自定义应用分组：用户按照自己的需求自定义的应用分组，在自定义应用分组中，用户可以把缺省系统支持的各种应用分组，或者是应用分组下的某种应用，加入自定义的应用分组中，没有特别的限制。

相关配置

↘ 查看应用及应用分组

通过 **show identify-application** 可以查看当前应用树，包括特征库解析出来的应用协议对象和自定义应用。

通过 **show identify-application custom-group** 显示分组信息。

↘ 自定义应用

默认情况下无自定义应用。

用户自定义支持配置如下几种类型的用户自定义应用：

1. 协议类型、源端口、目的端口
2. 协议类型、源 ip、源端口
3. 协议类型、源 ip、目的 ip
4. 协议类型、目的 ip、目的端口

通过 **identity-application custom name** 可以配置自定义应用。对规则有如下限制：

- 对于“协议类型、源端口、目的端口”类型规则，源端口和目的端口不能同时为 any。
- 对于“协议类型、源 ip、源端口”类型规则，源 ip、源端口都不能为 any。
- 对于“协议类型、源 ip、目的 ip”类型规则，源 ip 和目的 ip 不能同时为 any。
- 对于“协议类型、目的 ip、目的端口”类型规则，目的 ip、目的端口都不能为 any。
- ip 可以配置单个 ip 或者一个 ip 段，但 ip 段的范围不能超过 32 个 ip，且 ip 段必须是连续的。

- 用户自定义应用可以在已有的软件分类上新增应用或已有应用上补充特征。其他情况用户自定义应用软件名称不能与已有的应用软件名称或应用分类名称一样。
- 用户自定义应用分类名称最长支持 31 个字符，用户自定义软件名称最长支持 27 个字符。

↘ 应用分组

默认情况下系统是按照第一种分组模式分组的，可以通过 **show identify-application group-state** 命令来查看当前模式。

使用 **identify-application clear key-inhibitive-block-other group** 可以清除关键应用组，抑制应用组和阻断应用组中的所有应用，系统按第二中模式分组。

在第一种分组模式下，当把某个应用加入了关键应用组，抑制应用组或者阻断应用组后系统就会产生第二种分组模式视图。当把某个应用加入到普通的用户自定义应用分组中，也会产生第二种分组模式视图。

在第二种分组模式下，可识别的应用（即特征库中存在相对应的规则或者用户自定义规则中存在相对应规则）在没有配置加入关键应用组，抑制应用组和阻断应用组的情况下默认属于 IP 协议组，如加入关键应用组则属于关键应用组，加入抑制应用组则属于抑制应用组。不可识别的应用（即特征库中不存在相对应的规则或者用户自定义规则中不存在相对应规则）默认情况下属于 IP 协议组，也可将其加入关键应用组或抑制应用组，这时它们则属于关键应用组或抑制应用组。

在第二种分组模式下，一个系统缺省的应用分组或者应用，可以加入多个自定义的应用分组。例如电子邮件协议可以加入用户自定义应用分组 1，也可以加入用户自定义应用分组 2。

第一种分组模式下通过 **identify-application block**、**identify-application inhibitive**、**identify-application key** 可以将应用或应用分类加入阻断应用组、抑制应用组、关键应用组。

通过 **identify-application custom-group** 命令创建自定义应用分组。创建分组后进入 app-group 配置命令模式 ,通过 **app-add** 和 **app-del** 命令新增和删除应用或应用分类。

一个应用不能同时既加入关键应用组又加入抑制应用组，但其本身和其父应用可以加入不同的应用组，如：腾讯 QQ 和即时通软件，其中腾讯 QQ 为即时通软件分类下的一个子应用，可以将即时通软件加入关键应用组而腾讯 QQ 加入抑制应用组。而如果只将即时通软件加入关键应用组，腾讯 QQ 不加入任何应用组则腾讯 QQ 默认也是加入关键应用组。

应用识别有用户自定义的应用识别协议和特征库的应用识别协议。在系统中，用户自定义的协议特征优先级比特征库的协议特征高。如果对于同一款应用协议，同时存在用户自定义协议特征和特征库协议特征，则系统采用用户自定义协议特征。

用户可最多自定义 100 类用户自定义应用组。

2.3.3 应用识别

应用识别组件识别出数据流的应用属性，其他模块根据数据流的应用属性执行策略动作。

工作原理

整个应用识别主要通过协议预期识别、DPI、协议探测识别、DFI（Deep/Dynamic Flow Inspection，深度/动态流检测）、长度序列识别等识别手段识别出数据流的应用属性。

↘ 协议预期识别

协议预期识别指的是，某些应用协议具有比较明显的流特征，例如，在双方的通讯过程中的流可能包含用于后续对话的 IP、端口等信息，通过分析这些流的信息，提取并记录其特征，后续符合该特征的流，就可以快速识别成该应用。预期的特征在一段时间后会老化，用户可以配置缺省的老化时间。

协议探测识别

协议探测识别指的是，某些应用协议的数据流可能是未知加密的数据流，我们设备会通过一些探测机制，识别出这种加密数据流的应用类型。

DPI 识别

DPI 识别主要是针对报文载荷特征的识别，对报文按照协议层次对协议进行解析识别出报文的协议类型及其端口，在协议和端口的识别基础上对载荷进行解码，再对载荷内容与特征库中的特征串进行匹配，通过多种匹配的模型对应用载荷特征进行匹配和识别，并对识别的结果根据优先级等进行决策选出最后的识别结果。对于某些应用必须通过多个报文的特征识别才能确定协议类型，状态跟踪模块会进行状态的跟踪，经过多个报文后的特征识别后确定出协议的类型。

DFI 识别

DFI 识别采用的是一种基于流量特征的应用识别技术。通常，不同的应用类型的会话连接或数据流状态会有所不同，比如 P2P 下载流和语音流。DFI 识别技术就是要分析出这些数据流的特征，建立流量分类器。然后用分类器对数据流进行分类识别，从而达到智能识别应用类型的目的。

长度序列识别

某些应用通信过程中产生的报文载荷虽然加密 ,但是长度呈现出固定的规律。通过长度序列特征来识别某些加密的 p2p 下载流，典型的是电驴加密下载流。

相关配置

开启应用识别功能

缺省情况下，应用识别开启。

使用 **identify-application enable** 命令可以开启或关闭应用识别全局开关。

应用识别开关开启的情况下，上述的各个识别手段方可生效。在全局开关开启的情况下，上述各个识别手段可单独关闭。

协议预期识别

应用识别开启的情况下，缺省协议预期识别默认开启。

使用 **identify-application proto-expect enable** 开启或关闭协议预期识别。

协议预期识别关闭后，可能会导致整个应用识别的识别能力大幅度下降。一般情况下，不建议关闭协议预期识别。

动态分析获取的协议预期信息需要指定老化时间，当规则中未指定具体时间时，则使用系统默认的老化时间。

默认情况下，协议预期节点老化时间为 60 秒。

使用 **identify-application proto-expect timeout** 可以配置协议预期老化时间。

当配置的时间越长，则协议预期生存时间越长。一般情况下，默认老化时间即可，参数设置越大，预期能力可能有所提高，但是也容易带来误判。

↘ DPI 识别

应用识别开启的情况下，缺省 DPI 识别开启。

使用 **identify-application dpi enable** 开启或关闭 DPI 识别。

DPI 识别关闭后，可能会导致整个应用识别的识别能力大幅度下降。一般情况下，不建议关闭 DPI 识别。

↘ 长度序列识别

应用识别开启的情况下，缺省长度序列识别开启。

使用 **identify-application len-seq enable** 开启或关闭长度序列识别。

长度序列识别关闭后，可能会导致 P2P 加密流识别率。一般情况下，不建议关闭长度序列识别。

2.4 配置详解

配置项	配置建议 & 相关命令	
升级特征库	⚠ 必须配置。用于建立特征库协议树及规则。	
	Identify-application signature update	触发特征库升级
配置自定义应用	⚠ 可选配置。用于自定义应用规则。	
	identity-application custom name	配置应用自定义规则
配置应用分组	⚠ 可选配置。用于管理应用协议对象。	
	identify-application clear key-inhibitive-block-other group	清除关键应用组 ,抑制应用组和阻断应用组中的所有应用。
	identify-application custom-group	新增用户自定义应用组。
	app-add	新增用户自定义应用组中的应用。
	app-del	删除用户自定义组中的应用。
	identify-application block	删除用户自定义组中的应用。
	identify-application key	将某个应用加入关键应用组。
	identify-application inhibitive	将某个应用加入抑制应用组。
配置应用识别功能	⚠ 必须配置。开启应用识别功能。	
	identify-application enable	开启应用识别
	identify-application proto-detect enable	开启协议探测识别
	identify-application proto-expect enable	开启协议预期识别
	identify-application proto-expect timeout	设置协议预期老化时间
	identify-application dpi enable	开启 DPI 识别
	identify-application dfi enable	开启 DFI 识别

	identify-application len-seq enable	开启长度序列识别
	identify-application app-db enable	开启应用收集功能

2.4.1 升级特征库

配置效果

- 建立特征库协议树。
- 创建或更新特征库规则。

注意事项

- 升级的特征库版本与设备当期特征库版本号一样的情况下，升级失败。

配置方法

↘ 升级特征库

- 必须配置。
- 在出口网关设备上升级特征库。先从官网上获取特征库到本地电脑，将特征库压缩包下载到设备上，然后通过 WEB 页面升级本地特征库；也可以通过 HTTP 升级的方式更新特征库。

⚠ 关于 HTTP 升级详见相关的配置文档。该文档中主要描述本地升级相关的配置方法。通过 WEB 升级或者自动更新的方式，则不需要执行相关命令触发特征库解析。

检验方法

- 通过检查特征库版本号是否更新，判断特征库升级是否成功。

相关命令

↘ 升级特征库

【命令格式】 **Identify-application signature update**
【参数说明】 **-**
【命令模式】 全局模式
【使用指导】 将特征库压缩包下载到设备上，通过该命令触发特征库升级。

↘ 查看特征库版本号

【命令格式】 **show identify-application version**
【参数说明】 **-**

【命令模式】 特权模式、全局模式、接口模式

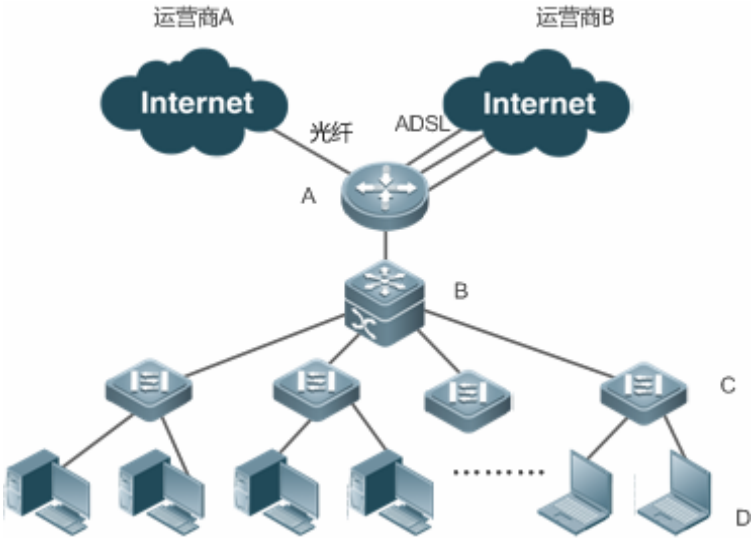
【使用指导】 -。

配置举例

↘ 升级特征库

【网络环境】

图 2-3



【配置方法】

- 通过 WEB 页面高级>系统升级>特征库下载>下载应用分类库，将特征库下载到设备上。
- 解压后，通过 WEB 页面高级>系统升级>本地升级选择解压目录下的 app_signature.upd 文件，点击开始升级即可。等待弹出升级成功提示。

A

```
Ruijie#*Apr 25 14:08:55: %DPI-5-LOCAL_UPDATE: Local signature database upgrading.
Ruijie#*Apr 25 14:10:14: %DPI-5-SIGNATURE_UPDATE: Signature database is upgraded successfully!
```

【检验方法】

- 使用 **show identify-application version** 查看特征库版本号

A

```
Ruijie#show identify-application version
Version:2013.05.22.13.05.22(V2.0)
```

常见错误

- 当前设备的特征库版本和下载的特征库版本一致，升级失败。

2.4.2 配置自定义应用

配置效果

- 配置自定义应用，根据五元组信息识别应用流量。

⚠ 设备中不存在有效的特征库时，自定义应用同样不能识别。

注意事项

↘ 用户自定义应用要能够配置如下几种类型的用户自定义应用：

- 协议类型、源端口、目的端口
- 协议类型、源 ip、源端口
- 协议类型、源 ip、目的 ip
- 协议类型、目的 ip、目的端口

↘ 用户自定义应用对规则有如下限制：

- 对于“协议类型、源端口、目的端口”类型规则，源端口和目的端口不能同时为 any。
- 对于“协议类型、源 ip、源端口”类型规则，源 ip、源端口都不能为 any
- 对于“协议类型、源 ip、目的 ip”类型规则，源 ip 和目的 ip 不能同时为 any
- 对于“协议类型、目的 ip、目的端口”类型规则，目的 ip、目的端口都不能为 any
- 可以配置单个 ip 或者一个 ip 段，但 ip 段的范围不能超过 32 个 ip，且 ip 段必须是连续的。
- 系统已有的应用分类名称和应用名称下，可以新增用户自定义应用特征。已有的系统应用分类特征和系统应用特征不受影响，只是优先级没有用户自定义的高。
- 用户自定义应用分类名称最长支持 31 个字符，用户自定义软件名称最长支持 27 个字符
- 自定义应用同一源 ip 或目的 ip，最多可以配置不连续目的端口或源端口数 example:目的 ip+目的端口类型，ip:1.1.1.1 + port:80， ip:1. 1.1.1 + port:100, ...ip:1.1.1.1 + port:200,这样同一个 ip 的 ip+port 对最多只能配置 16 个。

配置方法

- 全局模式下，通过命令创建自定义应用。

检验方法

- 检查当前自定义应用，查看是否创建成功。

相关命令

↘ 配置一条用户自定义规则

【命令格式】 **identity-application custom name** *software-name* **class** *class-name* **{ ip sip { any any |** *sip-low sip-high* **} dip { any any |** *dip-low dip-high* **} | { tcp | udp } { sport { any any |** *sport-low sport-high* **} dport { any any |** *dport-low dport-high* **} | { sip { any any |** *sip-low sip-high* **} { sport { any any |** *sport-low sport-high* **} | dip { any any |** *dip-low dip-high* **} } | dip { any any |** *dip-low dip-high* **} dport { any any |** *dport-low*

dport-high **} } } }**

【参数说明】 software-name:应用软件名称。

class-name:应用分类名称。

sport-low:起始源端口。范围 0-65535 或 any。

sport-high:结束源端口。范围 0-65535 或 any。

dport-low:起始目的端口。范围 0-65535 或 any。

dport-high:结束目的端口。范围 0-65535 或 any。

sip-low:起始源 ip。

sip-high:结束源 ip。

dip-low:起始目的 ip。

dip-high:结束目的 ip。

【命令模式】 全局模式

【使用指导】 -

查看自定义应用规则

【命令格式】 **show identify-application custom- rule**

【参数说明】 -

【命令模式】 特权模式

【使用指导】 -

配置举例

创建自定义应用规则

【配置方法】

- 创建一条自定义规则

```
Ruijie# configure terminal
Ruijie(config)#identify-application custom name 迅雷游戏 class 自定义游戏 tcp sport 1 10 dport 1 100
```

【检验方法】

- 查看设备中的自定义规则。

```
Ruijie#show identify-application custom-rule
TYPE NAME                          CLASS                           SPL    SPH    DPL    DPH    SIPL
SIPH            DIPL            DIPH
---- ----------------------------- ------------------------------- ------ ------ ------ ------
--------------- --------------- --------------- ---------------
TCP  迅雷游戏                      自定义游戏                        1      10     1      100    any
         any             any             any
```

常见错误

- 自定义应用配置时，未满足限制条件，导致配置失败。限制条件详见注意事项。

2.4.3 配置应用分组

配置效果

- 配置应用分组，流量控制、应用路由等模块可以将策略关联应用分组。

注意事项

- 一个应用不能同时既加入关键应用组又加入抑制应用组，但其本身和其父应用可以加入不同的应用组，如：腾讯 QQ 和即时通软件，其中腾讯 QQ 为即时通软件分类下的一个子应用，可以将即时通软件加入关键应用组而腾讯 QQ 加入抑制应用组。而如果只将即时通软件加入关键应用组，腾讯 QQ 不加入任何应用组则腾讯 QQ 默认也是加入关键应用组。
- 应用识别有用户自定义的应用识别协议和特征库的应用识别协议。在系统中，用户自定义的协议特征优先级比特征库的协议特征高。如果对于同一款应用协议，同时存在用户自定义协议特征和特征库协议特征，则系统采用用户自定义协议特征。
- 用户可最多自定义 100 类用户自定义应用组。。

配置方法

- 确定使用的分组模式。
- 创建应用分组。
- 将应用或应用分类加入应用分组中。

检验方法

- 检查当前应用分组模式。
- 查看应用分组，确认应用分组创建成功。
- 查看应用分组下的各个应用或应用分类。

相关命令

↘ 配置当前应用分组模式

【命令格式】 **identify-application clear key-inhibitive-block-other group**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 某个应用可以加入关键应用组，也可以加入抑制应用组，也可以加入阻断应用组，但不能同时既加入关键应用组又加入抑制应用组，通过这条命令可以将关键应用组，抑制应用组和阻断应用组中的应用删除。

创建应用分组

【命令格式】 **identify-application custom-group** *group-name*
【参数说明】 group-name：应用组名
【命令模式】 全局模式
【使用指导】 通过此命令可以新增用户自定义应用组。
用户可最多自定义 100 类用户自定义应用组。
配置该命令后，命令配置模式转入 group-group 配置命令层。

新增用户自定义分组的应用

【命令格式】 **app-add** *app-name*
【参数说明】 app-name：应用名称。
【命令模式】 app-group 配置命令模式
【使用指导】 通过此命令可以往用户自定义应用组里面增加应用。用户自定义应用组中的应用可以是系统支持的应用，也可以是系统支持的应用分组。

删除用户自定义分组的应用

【命令格式】 **app-del** *app-name*
【参数说明】 app-name：应用名称。
【命令模式】 app-group 配置命令模式
【使用指导】 通过此命令可以删除用户自定义应用组里面应用。

配置阻断应用组

【命令格式】 **identify-application block** *app-name*
【参数说明】 app-name：应用名称。
【命令模式】 全局配置模式
【使用指导】 -

配置关键应用组

【命令格式】 **identify-application key** *app-name*
【参数说明】 app-name：应用名称。
【命令模式】 全局配置模式
【使用指导】 -

配置抑制应用组

【命令格式】 **identify-application inhibitive** *app-name*
【参数说明】 app-name：应用名称。
【命令模式】 全局配置模式
【使用指导】 -

查看应用协议树

【命令格式】 **show identify-application**

【参数说明】 -
【配置模式】 特权模式
【使用指导】 -

查看应用分类

【命令格式】 **show identify-application class [class-name]**
【参数说明】 **class-name:应用分类名称**
【配置模式】 特权模式
【使用指导】 -

查看当前分组模式

【命令格式】 **show identify-application group-state**
【参数说明】 **-**
【配置模式】 特权模式
【使用指导】 -

查看应用分组及分组下的应用或应用分类

【命令格式】 **show identify-application custom-group**
【参数说明】 **-**
【配置模式】 特权模式
【使用指导】 -

查看阻断应用组

【命令格式】 **show identify-application block**
【参数说明】 **-**
【配置模式】 特权模式
【使用指导】 -

查看关键应用组

【命令格式】 **show identify-application key**
【参数说明】 **-**
【配置模式】 特权模式
【使用指导】 -

查看抑制应用组

【命令格式】 **show identify-application inhibitive**
【参数说明】 **-**
【配置模式】 特权模式
【使用指导】 -

查看其他应用组

【命令格式】 **show identify-application other**

【参数说明】 -

【配置模式】 特权模式

【使用指导】 -

配置举例

创建应用分组，并添加应用

【配置方法】

- 创建应用分组
- 在 app-group 配置命令模式下，添加应用。

```
Ruijie# configure terminal
Ruijie(config)#identify-application custom-group mygroup
Ruijie(config-custom-group)#app-add BQQ
Ruijie(config-custom-group)#app-add MSN
Ruijie(config-custom-group)#exit
```

【检验方法】

- 查看应用分组及各个分组下的应用。

```
Ruijie#show identify-application custom-group
system-group: Key_Group
system-group: Unkey_Group
system-group: Block_Group
    application: HTTP-单线程
system-group: Other_Group
custom-group: mygroup
    application: BQQ
    application: MSN (group)
```

配置系统应用组

以关键应用组配置为例

【配置方法】

- 添加应用或者应用分类到关键应用组中。

```
Ruijie# configure terminal
Ruijie(config)#identify-application key BQQ
```

【检验方法】

- 查看应用分组及各个分组下的应用。

```
Ruijie#show identify-application key
BQQ
Ruijie#
```

常见错误

- 配置应用分组时，未满足限制条件，导致配置失败。限制条件详见注意事项。

2.4.4 配置应用识别功能

配置效果

- 配置应用识别后，能够识别出数据流的应用类别，并能收集反馈应用识别信息。

注意事项

- 应用识别开关关闭的情况下，所有的应用识别手段将失效
- 应用识别各个手段依赖于应用特征库。当设备中无特征库时，应用识别失效。
- 应用识别开启的情况，缺省各种识别手段均开启。

配置方法

- 全局模式下，通过命令开启应用识别，及各种识别手段。

检验方法

- 检查应用识别状态，及各个识别手段状态。

相关命令

↘ 开启应用识别

【命令格式】 **identify-application enable**
【参数说明】 -
【命令模式】 全局模式
【使用指导】 -

↘ 开启协议探测识别功能

【命令格式】 **identify-application proto-detect enable**
【参数说明】 -
【命令模式】 全局模式
【使用指导】 -

↘ 开启协议预期识别

【命令格式】 **identify-application proto-expect enable**
【参数说明】 -

【命令模式】 全局模式
【使用指导】 -

设置协议预期识别老化时间

【命令格式】 **identify-application proto-expect timeout** *time-seconds*
【参数说明】 time-seconds：老化的秒数，参数范围 10 - 3600
【命令模式】 全局模式
【使用指导】 -

开启 DPI 识别

【命令格式】 **identify-application dpi enable**
【参数说明】 -
【命令模式】 全局模式
【使用指导】 -

开启 DFI 识别

【命令格式】 **identify-application dfi enable**
【参数说明】 -
【命令模式】 全局模式
【使用指导】 -

开启长度序列识别

【命令格式】 **identify-application len-seq enable**
【参数说明】 -
【命令模式】 全局模式
【使用指导】 -

开启应用收集功能

【命令格式】 **identify-application app-db enable**
【参数说明】 -
【命令模式】 全局模式
【使用指导】 -

查看应用识别功能

【命令格式】 **show identify-application enable**
【参数说明】 -
【命令模式】 特权模式
【使用指导】 -

查看协议预期识别功能

【命令格式】 **show identify-application proto-expect enable**

【参数说明】 -

【命令模式】 特权模式

【使用指导】 使用该命令可以查看预期状态及默认老化时间

查看 DFI 识别功能

【命令格式】 **show identify-application dfi enable**

【参数说明】 -

【命令模式】 特权模式

【使用指导】 使用该命令可以查看预期状态及默认老化时间

配置举例

开启应用识别

【配置方法】
- 开启应用识别
- 根据需要单独关闭某个识别手段

以开启应用识别，关闭 DFI 识别为例：

```
Ruijie# configure terminal
Ruijie(config)#no identify-application dfi enable
```

【检验方法】
- 查看应用识别，查看 dfi 识别。

```
Ruijie#show identify-application enable
on
Ruijie#show identify-application dfi enable
dfi unable!
```

开启应用识别预期识别

【配置方法】
- 开启协议识别功能
- 开启应用收集功能

```
Ruijie# configure terminal
Ruijie(config)#identify-application proto-expect enable
Ruijie(config)#identify-application app-db enable
```

【检验方法】
- 查看协议预期识别。

```
Ruijie#show identify-application proto-expect enable
Proto-expect is enable
Proto-expect app_db is enable
Proto-expect timeout is not set[0s]
```

常见错误

- 单独识别手段功能开启，但应用识别未开启，此时单独的识别手段未能生效。

2.5 监视与维护

清除各类信息

无

查看运行情况

作用	命令
显示应用规则树信息。	**show identify-application**
显示加入阻断应用组的应用或分类。	**show identify-application block**
显示应用分类信息。	**show identify-application class**
显示应用分组信息。	**show identify-application custom-group**
显示自定义应用规则。	**show identify-application custom- rule**
查看应用识别功能。	**show identify-application enable**
显示分组模式。	**show identify-application group-state**
显示加入抑制应用组的应用或分类。	**show identify-application inhibitive**
显示加入关键应用组的应用或分类。	**show identify-application key**
显示其它应用组的应用或分类。	**show identify-application other**
显示协议预期的信息。	**show identify-application proto-expect enable**
显示协议探测的信息。	**show identify-application proto-detect enable**
显示特征库版本号信息。	**show identify-application version**

查看调试信息

无

3 APP-ROUTE

3.1 概述

基于应用的路由，下面简称应用路由，区别于传统的基于报文目的 IP 选路的 IP 路由技术，是一种根据数据流的应用类型进行路由转发的技术。基于这种技术，可以将不同应用类型的数据流分流到不同的出口，保证关键业务与抑制业务各行其道。

锐捷网关产品应用路由主要适用于如下的应用场景：

由于运营商光纤专线和 ADSL（Asymmetric Digital Subscriber Line，非对称数字用户环路）线路的价格差距很大，有些地区每 M 价格差距达到 7-8 倍，为了提高性价比，用户通常采取光纤+ADSL 线路搭配的方式。应用路由可满足用户将抑制应用分流到 ADSL 线路，而关键应用走光纤。这样可以确保关键应用获得更好的线路资源，从而提升网络使用体验，使带宽投入成本和使用体验之间取得最高性价比。

协议规范

无

3.2 典型应用

典型应用	场景描述
网吧多出口基于应用分流	网吧出口采取光纤+ADSL 线路搭配方式。

3.2.1 网吧多出口基于应用分流

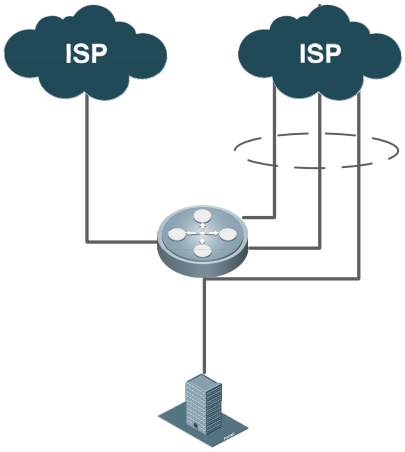
应用场景

网吧的网络平台上可以运行各种业务，但存在关键应用（如游戏、网页浏览、即时通讯等）和抑制应用（在线影视、P2P（Peer to Peer，对等连接）下载）区分。关键业务是网吧的核心竞争力，抑制应用重要性则较低。

以下图为例，电信运营商提供给网吧一条光纤和三条 ADSL 线路。

- 网吧用户需要保证关键应用走光纤线路，影视娱乐及下载相关走 ADSL 线路。

图 3-1



【注释】 - ADS

功能部属 50M 300M

- 配置开启应用路由模块功能。
- 配置 web 应用的选路策略
- 配置视频应用的选路策略
- 配置 P2P 等抑制应用线路的应用路由策略，一般建议是走 ADSL 线路。
- 配置接口组功能。

网关设备

3.3 功能详解

基本概念

应用识别

应用识别是指对网络中的数据流按照应用特征进行流量分类识别，从而识别出数据流的应用协议类型。应用识别的识别过程主要是分析数据流的报文载荷特征和报文流量特征，从而获知数据流的应用协议类型。其识别结果会在报文转发时被应用路由用作判断依据。

应用类别

应用路由根据配置的应用类型进行匹配和分流。应用路由支持的应用类型包括“应用分类”，“应用软件”，“应用软件子类”和“应用分组”。

“应用分组”与前三种是不同维度的概念。可以将应用分组理解为一个容器，用户可以将前三种类型划分到不同的“应用分组”中。系统预定义了“关键应用组”，“抑制应用组”，“阻断应用组”和“其他应用组”四个“应用分组”，用户还可以自定义新的“应用分组”。应用路由支持针对所有的“应用分组”指定路由。

“应用分类”，“应用软件”和“应用软件子类”是逐级细分的关系。“应用分类”下包含若干“应用软件”，应用软件下又分为（也可能没有）若干“应用软件子类”。应用识别特征库已经预定义了大量的“应用分类”，“应用软件”和“应用软件子类”，例如：“HTTP 应用分类”下面包含“HTTP 视频流媒体软件”，“HTTP 视频流媒体软件”又包含“优酷”，“土豆视频”等应用软件子类。可以认为“优酷”是“HTTP 视频流媒体软件”的子集，“HTTP 视频流媒体软件”是“优酷”的超集。除了预定义的类型，用户还可以自行定义新的分类，软件和子类。应用路由支持的“应用分类”，“应用软件”和“应用软件子类”种类见下表。

应用分类	应用软件	应用软件子类	支持应用路由
P2P 下载软件	(all)	(all)	Y
视频流媒体软件	(all)	(all)	Y
HTTP 应用			
	HTTP 视频流媒体	(all)	Y
网络应用更新	(all)	(all)	Y
网络硬盘	(all)	(all)	Y
互联网文件传输(包括 IM 文件传输)	(all)	(all)	Y

应用类别说明：若上一级类别支持应用路由，则其所有下级或更下级也都支持。反之，下级支持，上级则不一定。例如：应用路由支持“HTTP 视频流媒体”及其下子类，但不支持“HTTP 应用”。应用路由支持用户自定义分组，若用户自定义分组中包含有无法首报文识别的应用类型，这部分路由的分流效果无法得到保证。

应用路由支持的应用分类、应用软件和应用软件子类需要参考应用识别 SRS 或 WEB 说明。

Url-group

应用路由支持根据 DNS 请求报文所带的 url 地址进行分流。即 url-group，是一组特定域名的组合，既可以用户自定义，也有系统默认生成的。比如设备自带有 url 组“视频~sys”，该 url-group 包含常见的视频 url 地址，例如”k.youku.com”。该功能针对的是 DNS 请求报文，需要配合 DNS 代理使用。配置 url-group 时，还可以指定是否要修改 DNS 请求报文的目的 IP。

优先级

应用路由与普通 IP 路由，用户路由、策略路由和默认路由都可以作为报文转发的依据。在这些路由策略同时存在的情况下，它们的优先级关系如下：

策略路由(set ip nexthop) > 用户路由 > 应用路由 > 普通 IP 路由 > 策略路由(set ip default nexthop) > 默认路由

在配置了多条应用路由的情况下，各应用路由自身之间也存在优先级关系。

应用路由自身之间的优先级关系与配置顺序相关，后配置的优先级高于先配置的。

命中

命中，是指数据流匹配上应用路由选路策略，并按策略转发。由于应用路由的首报文选路特点，非首报文识别的应用数据流，将无法命中应用路由策略。

状态

应用路由的状态，也称为活动性，是指应用路由是否生效。如果配置的应用路由，出接口状态为 DOWN，则该应用路由状态也为 DOWN。

如果没有打开应用路由转发功能，所有应用路由策略都是 DOWN 状态。

↘ 接口及接口组

应用路由支持 WAN 口作为出接口。

接口组，是指多个 WAN 接口的组合。为了支持应用路由走多链路出口，并简化配置，抽象出一个接口组的概念。用户可以为接口组指定名称，包含接口组接口成员和均衡策略。

应用路由的出口可以指定为接口或接口组。

↘ Ip-group 地址表

应用路由支持指定源或目的 ip 地址做应用选路，ip-group 可以定义各种地址，包括地址库，ip 地址，ip 掩码等。

指定地址后，只有符合该指定源或目的 ip 地址的流量才会进行应用路由选路。

比如指定应用类型为 any，目的 ip 地址为电信地址库的应用路由，可以实现配置电信地址库的效果。

指定应用类型为 any，源 ip 地址为内网服务器的应用路由，可以实现类型配置策略路由的效果。

↘ Ip 协议号与端口号范围

应用路由支持指定 ip 协议号，当选择 tcp 或者 udp 协议的时候，允许指定源与目的端口的范围。指定后，只有符合该协议、且端口号范围的流量才会命中该条策略。当应用路由策略有关联应用对象组、ip 地址表等时，需要全部匹配才认为是匹配这条策略。

功能特性

功能特性	作用
配置应用路由	根据应用路由策略进行分流处理。
配置接口组	将多个出口组合在一起，供应用路由出口选路。

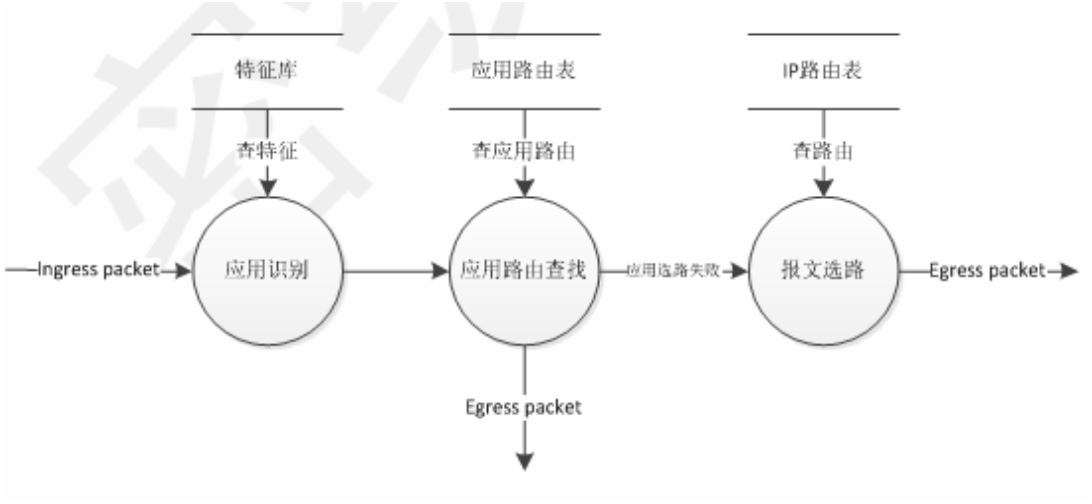
3.3.1 配置应用路由

配置应用路由相关策略，可以对应用进行出口分流处理。

工作原理

应用路由与普通 IP 路由一样，内部有一张“应用路由表”，当新建一个数据流的时候，应用识别模块首先对该数据包进行分析，确定其所属的应用类型，然后当数据包到达路由模块，应用路由查找“应用路由表”，确定下一跳和出口，进行转发（如下图）。如果未匹配任何应用路由，则按普通 IP 选路转发。

图 3-2



应用路由表

“应用路由表”记录满足应用路由数据报文的相关信息，以便于应用路由转发，主要记录出口及下一跳信息。

相关配置

启动应用路由模块转发使能开关

缺省情况下，锐捷网关设备应用路由模块转发使能功能关闭。

全局模式下使用 **app-route enable** 命令开启应用路由模块转发使能功能。

全局模式下可使用 **no app-route enable** 命令关闭应用路由转发模块使能功能。

配置应用路由模块策略功能

缺省情况下，设备中不存在任何策略。

全局模式下使用 **app route** [**priority-num** *priority-num*] *app-name* [**protocol** {**tcp** [**sport** *s-begin* [*s-end*]] [**dport** *d-begin* [*d-end*]] | **udp** [**sport** *s-begin* [*s-end*]] [**dport** *d-begin* [*d-end*]] | **icmp** | *protocol-num*}] [**sip-group** *sip-group-number*] [**dip-group** *dip-group-number*] [**url-group** *url-group-name* [**change-dest** *dest-ip-address*]] {**interface** *interface-name* | **interface-group** *group-name*} [**time-range** *time-rang-name*] [**track** *track-id*] [**description** *description-name*]命令完成应用路由策略配置。

报文匹配规则由 *app-name* ，*sip-group-number* ，*dip-group-number*， *url-group-name* 等关键字指定。

匹配规则的报文的处理方法由 *dest-ip-address*，*interface*，*interface-group* 等关键字指定。

如果某个匹配规则不填写，默认为不关注。

应用路由模块完成策略配置，应用路由生效之后，数据报文将按照应用进行分流处理。

应用路由模块支持后配置的应用路由策略优先级更高，用户可通过优先级调整命令对应用路由策略进行调整。

配置应用路由模块策略优先级调整功能

缺省情况下，策略优先级遵循“后配置先生效”的原则。也可配置时指定优先级。

全局模式下使用 **app route priority-num** *priority-number* **priority** { **increase** | **decrease** } [*1-1999*]命令调整应用路由策略优先级。

策略优先级越大则优先匹配。

应用路由仅支持网关模式，不支持网桥模式。

3.3.1.1 配置指定源目的IP

应用路由支持指定源/目的 IP 的报文走特定路由，通过配置 ip-group 关联 IP 地址(参见 ip-group 的配置文档)，应用路由再关联该 ip-group 选路走指定出口

相关配置

配置 ip-group

全局模式下，可使用 ip-group 配置指定的 ip 范围

配置应用路由模块策略

全局模式下，可使用 **app route** [**priority-num** *priority-num*] *app-name* [**protocol** {**tcp** [**sport** *s-begin* [*s-end*]] [**dport** *d-begin* [*d-end*]] | **udp** [**sport** *s-begin* [*s-end*]] [**dport** *d-begin* [*d-end*]] | **icmp** | *protocol-num*}] [**sip-group** *sip-group-number*] [**dip-group** *dip-group-number*] [**url-group** *url-group-name* [**change-dest** *dest-ip-address*]] {**interface** *interface-name* | **interface-group** *group-name*} [**time-range** *time-rang-name*] [**track** *track-id*] [**description** *description-name*]命令完成应用路由策略配置

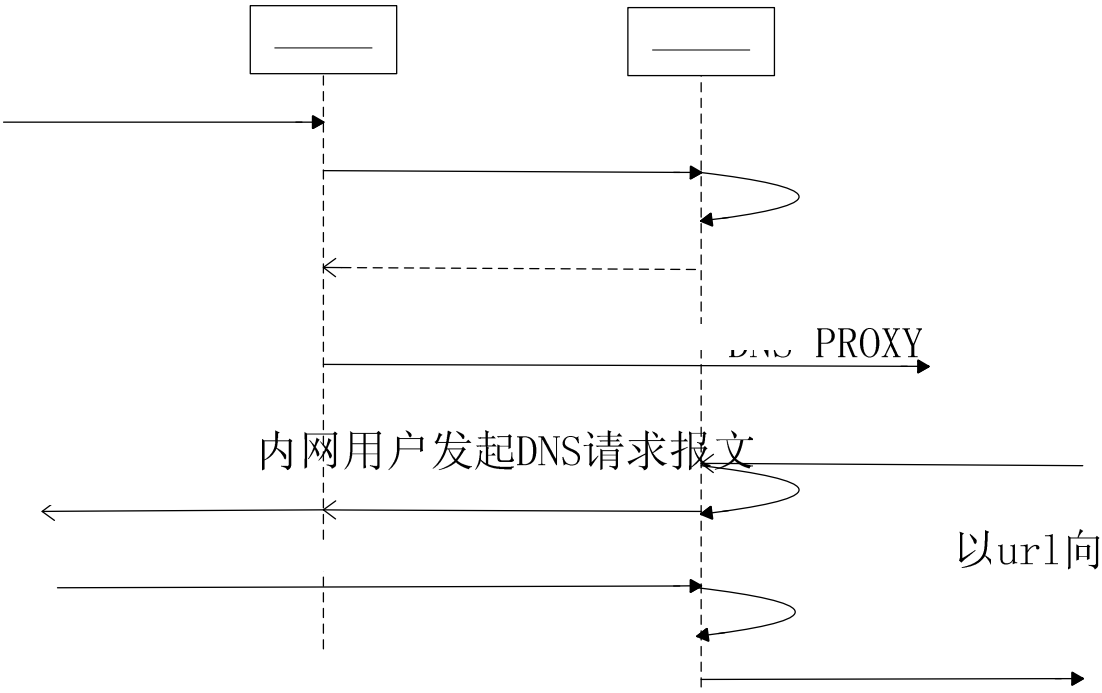
3.3.1.2 配置域名路由

应用路由支持指定域名的报文走特定路由。通过配置 url-group 关联 url 域名(参见 url-group 的配置文档)，应用路由再关联该 url-group 选路走指定出口。

工作原理

应用路由配置 url-group 时，要配合正向 dns 代理功能使用。因为对域名请求报文的处理主要是 DNS 代理来完成，应用路由负责提供路由表项和对域名解析之后的 IP 的处理。

例如：内网某 PC 发起一个请求域名为”k.youku.com”的 DNS 请求报文，DNS 代理拦截到该报文之后，提取域名向应用路由查询，应用路由发现该域名在系统自带的”视频~sys”域名组里，同时配置了 url-group “视频~sys“走选路出口 1，则向 DNS 代理返回出口 1，DNS 代理于是将该 DNS 请求报文选路到该出口。当外网 DNS 服务器应答 DNS 请求时，应用路由会监听从服务器收到的该域名的 DNS 应答报文 ,并提取其中的域名对应的 IP 地址 ,缓存在 “域名 IP 预期表中”,假设为这里 k.youku.com 对应的 IP 为 “119.167.145.107..”。后续当内网 PC 发起的请求报文目的 IP 与该 IP 相同时，则应用路由将该请求报文也重定向到出口 1。



应用路由还支持配置域名路由是否要修改域名请求报文的目的 IP。

相关配置

↘ 配置 ip-group

全局模式下，可使用 **app-proxy url group** *url-group-name* 配置指定的 url

↘ 配置应用路由模块策略

全局模式下，可使用 **app route** [**priority-num** *priority-num*] *app-name* [**protocol** {**tcp** [**sport** *s-begin* [*s-end*]] [**dport** *d-begin* [*d-end*]] | **udp** [**sport** *s-begin* [*s-end*]] [**dport** *d-begin* [*d-end*]] | **icmp** | *protocol-num*}] [**sip-group** *sip-group-number*] [**dip-group** *dip-group-number*] [**url-group** *url-group-name*] [**change-dest** *dest-ip-address*] {**interface** *interface-name* | **interface-group** *group-name*} [**time-range** *time-rang-name*] [**track** *track-id*] [**description** *description-name*]命令完成应用路由策略配置

3.3.2 配置接口组

多个网络出口聚合在一起，形成接口组。

工作原理

一个接口组最多由 32 个接口组成员构成，每个接口组成员就是一个网络出口。接口组可以配置不同的线路负载策略，基于带宽策略的接口组，接口成员按照带宽来计算权重；基于负载策略的接口组，按照负载周期更新，并计算最小负载。

计算带宽权重值

统计接口组不同出口带宽之和设为 S，各出口带宽为 Bi，基准权重为 base，权重值为 Wi，然后按照如下比例计算：

Wi = Bi × base / S

相关配置

配置接口组功能

缺省情况下，设备中不存在任何接口组。

全局模式下使用 **interface-group** *interface-group-name* 命令配置接口组对象。

全局模式下使用 **no interface-group** *interface-group-name* 命令删除接口组对象。

配置接口组接口成员功能

缺省情况下，接口组内成员为空。

接口组模式下，配置 **interface-member** *interface-name* 命令配置接口组成员。

接口组模式下，配置 **no interface-member** *interface-name* 命令删除接口组成员。

配置接口组负载策略功能

缺省情况下，接口组基于线路负载进行均衡。

接口组模式下，配置 **load-balance policy** { **bandwidth** | **load** }命令配置接口组负载策略。

bandwidth 是基于线路带宽，load 是基于线路负载。

接口组默认负载策略为 load。

配置接口网关功能

默认情况下，接口上没有配置 nexthop。

接口模式下，配置 **nexthop** *ip-address* 命令配置接口下一跳信息。

接口网关功能，提供给接口组中接口成员路由选路出口。

3.4 产品说明

NBR800G、NBR950G 不支持应用路由；NBR3000G-S 、NBR1500G、NBR2000G、NBR1000G-C、NBR2000G-C、NBR1000G-E 、 NBR6120-E 、 NBR108G-P 、 NBR1300G-E 、 NBR1700G-E 、 NBR2100G-E 、 NBR2500D-E 、 NBR3000D-E、NBR3000D-UE、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持应用路由。

NBR3000G-S 、NBR1500G、NBR2000G、NBR1000G-C、NBR2000G-C、NBR1000G-E、NBR6120-E、NBR108G-P、

NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE 支持 URL 路由，NBR800G、NBR950G、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 不支持 URL 路由。

NBR800G、NBR950G 不支持 P2P 下载选路；NBR3000G-S 、NBR1500G、NBR2000G、NBR1000G-C、NBR2000G-C 、NBR1000G-E 、NBR6120-E 、NBR108G-P 、NBR1300G-E 、NBR1700G-E 、NBR2100G-E 、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 P2P 下载选路。

NBR800G、NBR950G 不支持网页/视频选路；NBR108G-P 、NBR1000G-E 、NBR6120-E 、NBR1300G-E 、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR3000G-S 、NBR1500G、NBR2000G、NBR1000G-C、NBR2000G-C、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持网页/视频选路。

NBR800G、NBR950G 不支持游戏选路；NBR108G-P、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E 、NBR2500D-E 、NBR3000D-E 、NBR3000D-UE 、NBR3000G-S 、NBR1500G 、NBR2000G 、NBR1000G-C、NBR2000G-C、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持游戏选路。

NBR800G、NBR950G 不支持协议代理；NBR3000G-S 、NBR1500G、NBR2000G、NBR1000G-C、NBR2000G-C、NBR1000G-E 、NBR6120-E 、NBR108G-P 、NBR1300G-E 、NBR1700G-E 、NBR2100G-E 、NBR2500D-E 、NBR3000D-E 、NBR3000D-UE 、NBR6205-E 、NBR6135-E 、NBR6210-E 、NBR6215-E 支持协议代理。其中 NBR3000G-S 、NBR1500G、NBR2000G、NBR1000G-C、NBR2000G-C 的协议代理支持 L2TP、L2TP OVER IPSEC；NBR1000G-E 、NBR6120-E 、NBR108G-P 、NBR1300G-E 、NBR1700G-E 、NBR2100G-E 、NBR2500D-E 、NBR3000D-E、NBR3000D-UE、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 的协议代理不支持 L2TP、L2TP OVER IPSEC。

3.5 配置详解

配置项	配置建议 & 相关命令	
配置应用路由功能	⚠ 必须配置。应用路由策略生效，对满足策略的相关应用进行分流处理。	
	app-route enable	启动应用路由模块转发使能开关
	app route [**priority-num** *priority-num*] *app-name* [**protocol** {**tcp** [**sport** *s-begin* [*s-end*]] [**dport** *d-begin* [*d-end*]] | **udp** [**sport** *s-begin* [*s-end*]] [**dport** *d-begin* [*d-end*]] | **icmp** | *protocol-num*}] [**sip-group** *sip-group-number*] [**dip-group** *dip-group-number*] [**url-group** *url-group-name* [**change-dest** *dest-ip-address*]] {**interface** *interface-name* | **interface-group** *group-name*} [**time-range** *time-rang-name*] [**track** *track-id*] [**description** *description-name*]]	配置应用路由模块策略功能
	nexthop *ip-address*	配置接口网关功能
	⚠ 可选配置。调整应用路由优先级。	
	app route priority-num *priority-number* **priority** { **increase** | **decrease** } [*1-1999*]	调整应用路由策略优先级功能
配置接口组功能	⚠ 必须配置。配置接口组的基本元素。	
	interface-group *interface-group-name*	配置接口组模块名
	interface-member *interface-name*	添加接口组成员
	nexthop *ip-address*	配置接口网关功能
	⚠ 可选配置。配置接口组的高级元素。	
	load-balance policy { **bandwidth** | **load** }	配置接口组负载策略
	bandwidth *kilobits*	配置接口带宽大小

3.5.1 配置应用路由功能

配置效果

应用路由策略生效，对满足策略的相关应用进行分流处理。

注意事项

- 接口需要配置网关。
- 应用对象需要支持首报文识别。
- url-group 需要配合 dns 代理开启
- 应用路由关联的 time-range 对象需要配置生效。

配置方法

启动应用路由模块转发使能开关功能

- 必须配置
- 通过全局开关控制应用路由

配置应用路由模块策略功能

- 必须配置
- 在全局配置应用路由的策略，从而决定哪些应用进行应用路由

配置接口网关功能

- 必须配置
- 只能在 WAN 口上配置网关功能

配置应用路由策略优先级功能

- 可选配置，当需要改变策略优先级时执行该功能。
- 通过该功能，可以改变应用路由策略的优先级，优先级遵循“后配置先匹配”的原则。

检验方法

网络中匹配应用路由策略应用对象的数据报文按照应用路由分流。

- 检查应用路由中应用对象是否按照应用路由出口进行分流。
- 检查应用路由模块配置信息是否生效
- 查看应用路由出口数据统计值。

相关命令

启动应用路由模块转发使能开关功能

【命令格式】 **app-route enable**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 -

配置应用路由模块策略功能

【命令格式】 **app route** [**priority-num** *priority-num*] *app-name* [**protocol** {**tcp** [**sport** *s-begin* [*s-end*]] [**dport** *d-begin* [*d-end*]] | **udp** [**sport** *s-begin* [*s-end*]] [**dport** *d-begin* [*d-end*]] | **icmp** | *protocol-num*}] [**sip-group** *sip-group-number*] [**dip-group** *dip-group-number*] [**url-group** *url-group-name* [**change-dest** *dest-ip-address*]] {**interface** *interface-name* | **interface-group** *group-name*} [**time-range** *time-rang-name*] [**track** *track-id*] [**description** *description-name*]]

【参数说明】 *app -name*：应用名称，可以是“应用分类”，“应用软件”，“应用软件子类”或用户自定义“应用分组”名称，或者“any”。

priority-num：应用路由优先级，唯一标识这条策略，取值范围在 1-10000。

protocol-num：ip 协议号，应用路由指定的 ip 协议号，取值范围在 1-255。

s-begin：源端口号范围的开始值，取值范围在 1-65535。

s-end：源端口号范围的结束值，取值范围在 1-65535，可以不配置，配置后必需大于开始值，即 *s-begin*。

d-begin：目的端口号范围的开始值，取值范围在 1-65535。

d-end：目的端口号范围的结束值，取值范围在 1-65535，可以不配置，配置后必需大于开始值，即 *d-begin*。

sip-group-number：ip-group 的 id 号，配置后，可以指定源 ip 地址来做应用路由选路。取值范围在 1-1000。

dip-group-number：ip-group 的 id 号，配置后，可以指定目的 ip 地址来做应用路由选路。取值范围在 1-1000。

url-group-name：url-group 的名称，配置后，可以指定 url 来作应用路由选。

dest-ip-address：匹配 url-group 的 dns 请求报文重定向的 DNS 服务器 IP 地址，配置之后对于命中 url-group 的 DNS 请求报文，应用路由选路的同时还会把该报文的目的 IP 修改为指定的 IP 地址

interface-name：指定接口名。

group-name：指定接口组名。

time-rang-name：规则关联的 time-rang 对象的名称。

track-id：track 的 id 号，配置之后，应用路由策略的生效状态，将和 track 联动，当 track 通告状态 down 时，本条应用路由策略不生效.

【命令模式】 全局模式

【使用指导】 该命令用于配置一条应用路由，其作用是指定特定应用从特定出口发送。应用路由仅支持可首报文识别的应用类型。

应用路由命令支持的接口类型包含 WAN 口和接口组。一个应用类型的路由只能配置一条，若需要配置多出口的应用路由，必须采用接口组方式配置。

应用路由允许指定路由生效的时间段，通过指定 time-range 参数，定义路由生效的时间。

应用路由生效的条件包括：打开应用路由转发开关；满足 time-range 指定的时间；出接口/接口组至少有一个接口状态为 UP。

配置接口网关功能

【命令格式】 **nexthop** *ip-address*

【参数说明】 *ip-address*：指定接口网关 IP 地址。

【命令模式】 接口模式

【使用指导】 此命令用来配置接口的网关，只有非点到点接口才需要配置网关。应用路由选中该接口时，会使用此处配置的网关地址进行下一跳转发。

配置应用路由策略优先级功能

【命令格式】 **app route priority-num** priority-number **priority** { **increase** | **decrease** } [1-1999]

【参数说明】 priority-number：应用路由优先级，唯一标识这条策略，取值范围在 1-10000。

1-1999：调整的优先级间隔，若调整距离数值超出该路由可调整的范围，可以自动适配到最大值，相当于快速移动到顶端或底端。

【命令模式】 全局模式

【使用指导】 多条应用路由间的优先级顺序与它们配置的先后顺序相关，后配置的策略优先级高于先配置的。如果需要修改已经配置好的应用路由的优先级，可以使用该命令进行优先级调整。

配置举例

以下配置举例，仅介绍与应用路由模块相关的配置。

在设备上开启应用路由功能

【网络环境】 某网吧出口有一条光纤链路 50M，联通运营商，三条 ADSL 链路，电信运营商，每条链路出口带宽都为 100M。需要抑制的大流量应用全部走 ADSL 分流，核心业务走光纤。视频流媒体软件和 HTTP 视频类型的应用在午夜时间不进行抑制，可以走光纤线路。电信运营商的流量需要从电信出口出去，不能跨运营商

【配置方法】

- 配置光纤线路默认路由。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#ip route 0.0.0.0 0.0.0.0 202.100.12.5
```

- 配置接口组，dialer 1,2,3 构成接口组。

```
Ruijie (config)#interface-group intf_group
Ruijie (config-intf-group)# interface-member dialer 1
Ruijie (config-intf-group)# interface-member dialer 2
Ruijie (config-intf-group)# interface-member dialer 3
```

- 配置接口 DNS 代理。光纤联通线路为高优先级，拨号口为低优先级

```
Ruijie(config)#interface gigabitEthernet 0/5
Ruijie(config-if-GigabitEthernet 0/5)# ip name-server 58.22.96.66 track 1
Ruijie(config-if-GigabitEthernet 0/5)# dns-proxy priority high
Ruijie(config)#interface dialer 1
Ruijie(config-if-dialer 1)# ip name-server 218.85.157.99 track 2
Ruijie(config)#interface dialer 2
Ruijie(config-if-dialer 2)# ip name-server 218.85.157.99 track 3
Ruijie(config)#interface dialer 3
Ruijie(config-if-dialer 3)# ip name-server 218.85.157.99 track 4
```

- 配置 ip-group，指定电信地址库。

```
Ruijie(config)#ip-group 1
Ruijie(config-ip-group)# route-db cnii
```

- 配置时间对象。

```
Ruijie (config)#time-range no_midnight
Ruijie (config-time-range)#periodic daily 9:00 to 23:00
Ruijie (config-time-range)#exit
```

- 配置应用识别对象功能。

```
#配置抑制应用对象：
Ruijie(config)#identify-application custom-group 抑制流量~route
Ruijie(config-custom-group)#app-add P2P 应用软件
Ruijie(config-custom-group)#app-add 软件更新
Ruijie(config-custom-group)#app-add 网络硬盘
Ruijie(config-custom-group)#app-add 视频|影音_MOBILE
Ruijie(config-custom-group)#app-add 下载工具_MOBILE
Ruijie(config-custom-group)#app-add HTTP 下载
Ruijie(config-custom-group)#app-add HTTP 上载
Ruijie(config-custom-group)#exit
#配置流媒体对象：
Ruijie(config)#identify-application custom-group 流媒体~route
Ruijie(config-custom-group)#app-add 视频流媒体软件
Ruijie(config-custom-group)#app-add HTTP 视频
Ruijie(config-custom-group)#exit
```

- 配置应用路由

```
#启用应用路由模块开关：
Ruijie (config)#app route enable
#抑制应用走抑制接口组，但视频流媒体，http 视频流媒体，午夜时间不抑制
Ruijie (config)# app route priority-num 10 抑制流量~route interface-group intf_group time-range any

Ruijie (config)# app route priority-num 20 流媒体~route url-group 视频~sys interface intf_group time-range no_midnight

Ruijie (config)# app route priority-num 30 any dst-grp 1 interface-group intf_group time-range any
```

【检验方法】 网吧用户访问外部网络，查看应用路由配置信息及应用出口流量信息：

- show app route 查看应用路由配置生效情况。
- show app route statistics 查看应用路由总体统计情况。
- show app route priority-num 10 session 查看流媒体会话情况。

常见错误

- 未开启应用路由模块转发使能开关功能，导致配置不生效。
- 未配置 time-range 对象，导致配置不生效。
- 未配置默认路由信息。

- 未配置 nexthop 信息。

3.5.2 配置接口组功能

配置效果

- 按照接口组负载策略，选择可转发的接口组成员出口。

注意事项

- 接口成员需要配置网关地址。
- 基于带宽的负载策略需要在接口下配置接口带宽大小。

配置方法

↘ 配置接口组功能

- 必须配置
- 通过全局配置接口组，可以将几个接口捆绑在一起作为应用路由的出口

↘ 配置接口组接口成员功能

- 必须配置
- 将指定接口加入接口组

↘ 配置接口网关功能

- 必须配置
- 只能在 WAN 口配置

↘ 配置接口组负载策略功能

- 可选配置，当需要改变现有负载策略时，使用该功能。
- 默认采用基于链路负载策略。

↘ 配置接口带宽功能

- 可选配置，当协商带宽错误或者不能满足需求时，使用该功能。
- 默认基于线路协商带宽大小。

检验方法

网络出口按照接口组进行分流处理。

- 检查接口组配置信息。

相关命令

配置接口组模块功能

【命令格式】 **interface-group** *interface-group-name*

【参数说明】 *interface-group-name*：接口组名

【命令模式】 全局模式

【使用指导】 接口组用于支持应用路由的多出口配置。

若应用路由的出口指定为接口组，匹配路由将会在接口组包含的多个出口中按一定策略进行均衡。

配置接口组接口成员功能

【命令格式】 **interface-member** *interface-name*

【参数说明】 *interface-name*：接口名

【配置模式】 接口组模式

【使用指导】 该命令将指定的接口加入接口组。

接口组内的接口必须是非 LAN 口，虚拟 dialer 口默认属非 LAN 口，可以加入接口组。

配置接口网关功能

【命令格式】 **nexthop** *ip-address*

【参数说明】 *ip-address*：指定接口网关 IP 地址。

【命令模式】 接口模式

【使用指导】 此命令用来配置 WAN 接口的网关，只有非点到点接口才需要配置网关。应用路由选中该接口时，会使用此处配置的网关地址进行下一跳转发。

配置接口组负载策略功能

【命令格式】 **load-balance policy** { **bandwidth** | **load** }

【参数说明】 -

【配置模式】 接口组模式

【使用指导】 应用路由在新建数据流时进行均衡处理。当配置根据“带宽”均衡时，应用路由根据组内各出口的带宽情况，按比例进行均衡。当配置根据“负载”均衡时，应用路由根据组内各出口当前的负载情况进行均衡。

配置接口带宽功能

【命令格式】 **bandwidth** *kilobits*

【参数说明】 *kilobits*：指定接口带宽大小。（单位：kbits）

【命令模式】 接口模式

【使用指导】 此命令用来配置接口出口带宽值。

接口组模块策略设置为基于带宽策略时，需要配置接口组成员出口带宽值。

配置举例

以下配置举例，仅介绍与接口组模块相关的配置。

在网络上建立接口组服务

【网络环境】 某高校存在多个网络出口，分别为 GigabitEthernet 0/1、0/2 和 0/3，出口流量基于接口组链路负载策略出口选路。

【配置方法】

- 配置全局接口组功能。

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

- 接口组模式下配置接口组接口成员功能。

```
Ruijie (config-intf-group)# interface-member GigabitEthernet 0/1
Ruijie (config-intf-group)# interface-member GigabitEthernet 0/2
Ruijie (config-intf-group)# interface-member GigabitEthernet 0/3
```

- 接口组模式下开启基于负载策略功能。

```
Ruijie(config-intf-group)# load-balance policy load
```

- 接口模式下配置接口网关。

```
Ruijie(config)#interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# nexthop 202.101.98.54
Ruijie(config-if-GigabitEthernet 0/1)# end
Ruijie(config)# interface GigabitEthernet 0/2
Ruijie(config-if-GigabitEthernet 0/2)# nexthop 202.101.98.55
Ruijie(config-if-GigabitEthernet 0/2)# end
Ruijie(config)# interface GigabitEthernet 0/3
Ruijie(config-if-GigabitEthernet 0/3)# nexthop 202.101.98.56
Ruijie(config-if-GigabitEthernet 0/3)# end
```

【检验方法】 查看接口组配置信息：

- show interface-group 查看接口组信息。

常见配置错误

- 未配置接口网关。

3.6 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
清除应用路由统计信息。	**clear app route statistic**

查看运行情况

作用	命令
查看接口组配置信息。	**show interface-group**
查看应用路由信息。	#查看应用路由配置信息 **show app route** #查看应用路由统计信息 **show app route statistics** #查看某个应用路由会话信息 **show app route priority-num** *priority-num* **session**

查看调试信息

无

4 APP-PROXY

4.1 概述

当前应用路由模块实现的应用分流，依赖于流的首包识别技术。对于 TCP 流，因为它前面的握手报文没有载荷，很难通过 DPI (Deep Packet Inspection，深度包检测)规则实现首包识别。应用代理技术是根据识别的结果，通过代理的手段，将某个应用的流量引导到路由链路上，从而提高应用路由效果。该技术用于 TCP 流的应用路由分流效果增强，一般在出口网关模式下，配合应用路由模块一起使用。

协议规范

无

4.2 典型应用

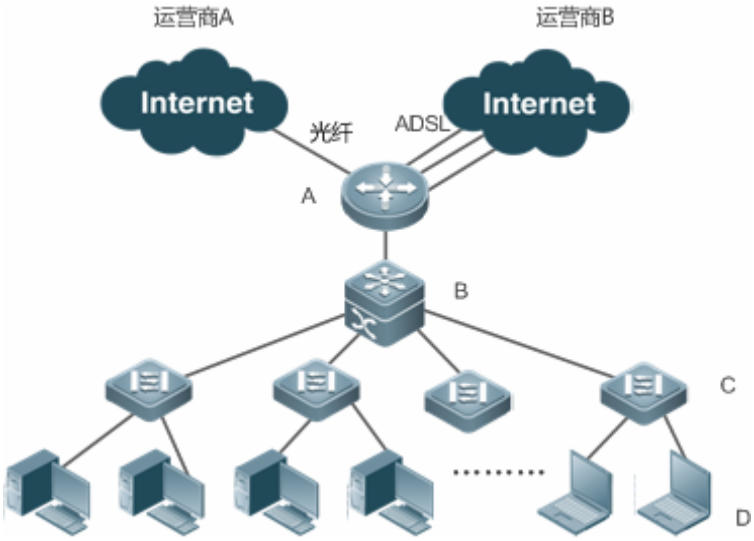
典型应用	场景描述
出口网关部署	出口网关设备部署应用代理

4.2.1 出口网关部署

应用场景

出口网关可以连接多条运营商线路，比如一条电信光纤线路和一条联通 ADSL（Asymmetric Digital Subscriber Line ，非对称数字用户环路）线路，或者一条电信光纤线路和多条联通 ADSL 线路。

图 4-1 出口网关典型应用场景



【注释】 A 为出口网关设备
B 为核心交换机。
C 为接入交换机。
D 为内网用户 PC。

功能部属

- 基本 NAT 上网功能：完成基本的 NAT 地址转换，保障用户正常上网。
- 应用识别功能：完成转发流量的应用识别，配合流控功能实现基于应用的流量控制等功能。
- 应用路由功能（包括应用代理功能）：以应用识别为基础，实现大流量应用或者重点应用的流量能够走指定的出口。
- 多链路负载均衡功能：完成数据流在多条链路的合理分配，确保多条链路的带宽利用合理。
- 流量控制功能：和应用识别结合，实现对 P2P 下载流量的抑制，实现对重点应用流量的保障等功能。
- 流量审计功能：和应用识别结合，提供基于应用的流量报表，让用户了解出口的网络带宽是否够用，是否需要扩容。

4.3 功能详解

基本概念

↘ 数据流

数据流的含义为报文的五元组相同的报文流。根据协议的不同通常定义的数据流有三种不同类别：TCP 流、UCP 流、IP 流（专门针对非 TCP/UDP 应用）。五元组分别定于如下：

流类别	五元组标识
TCP 流	源 IP 地址|目的 IP 地址|IP 协议|TCP 源端口|TCP 目的端口
UDP 流	源 IP 地址|目的 IP 地址|IP 协议|UDP 源端口|UDP 目的端口

IP 流	源 IP 地址|目的 IP 地址

↘ 应用路由

为了有效利用网络资源，业界提出一种有效的方法，就是为企业、网吧租用两条（或多条）广域网链路，其中一条高质量线路用于传输对网络传输时延、抖动等特性敏感的关键应用，另一条低质量线路用于传输 P2P 等下载应用。此种情况，就需要出口网关设备能够根据应用进行报文路由。基于应用的路由，简称应用路由，区别于传统的基于报文目的 IP 选路的 IP 路由技术，是一种根据数据流的应用类型进行路由转发的技术。基于这种技术，可以将不同应用类型的数据流分流到不同的出口，以达关键业务与抑制业务各行其道，减少影响的目的。应用路由的最大问题就是如何实现数据流的首报文识别。

↘ 首包识别

首包识别要求在每个流的第一个报文实现对这个流的识别。做到首包识别才能保证应用路由的效果。因为如果在数据流中间识别再去应用路由的话，必然导致一个流从至少两个不同线路对外通信，会导致断流。注意区分首包识别与第一个载荷报文，对于 TCP 流，首包为握手报文，而第一个载荷报文为请求报文。

功能特性

功能特性	作用
应用代理	配置应用代理。

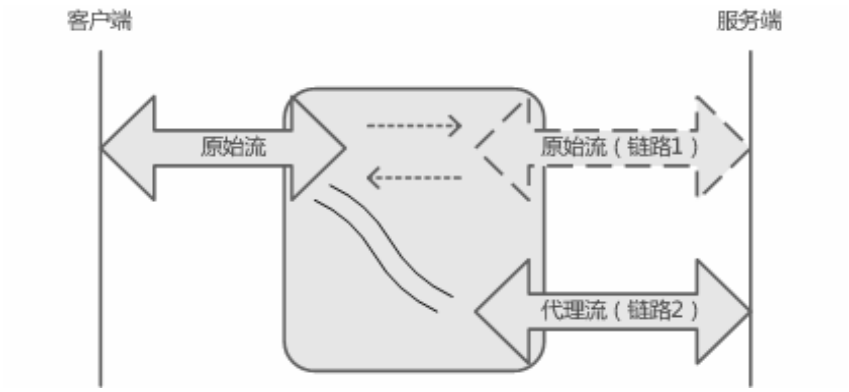
4.3.1 应用代理

应用代理是通过代理技术实现应用分流，能够显著提高应用路由分流能力。

工作原理

↘ 应用代理

应用代理功能是指设备识别出具体应用后，代理客户端通过应用路由的链路同服务端进行通信，从而实现根据应用将流量引导到不同出口，增强应用路由的目的。应用代理主要针对 TCP 流进行处理。为了提高对 HTTP1.1 流的支持，对这类流进行更加精细的应用代理处理。下图中在应用识别成功之前，通过链路 1（链路 1 为普通路由指定的链路）和服务端进行数据交互；在应用识别成功之后，通过应用代理后，通过链路 2（链路 2 为应用路由指定的链路）和服务端进行数据交互。



⚠ 应用代理工作在网关模式，不支持网桥模式；应用代理不支持 VPN 流量；应用代理只支持内网发起的 TCP 流（SYN 报文和第一个有载荷报文由内网发起）

应用代理由 HTTP 应用代理和 TCP 应用代理组成。一条 TCP 流，如果为 HTTP1.1 连接，则采用 HTTP 应用代理处理，否则由 TCP 应用代理处理。

应用代理依赖于应用路由模块。从功能角度上看，应用代理属于应用路由的子模块。在应用路由关闭的情况下，应用代理模块不起作用。

相关配置

↘ 开启应用代理

应用识别开启的情况下，缺省开启应用代理，包括 HTTP 应用代理。

使用 [**no**] **app-proxy enable** 可以开启或关闭应用代理。

使用 [**no**] **app-proxy http enable** 可以开启或单独关闭 HTTP 应用代理。

当应用路由生效且应用代理开启，而 HTTP 应用代理关闭的情况下，所有 TCP 流（包括 HTTP1.1 连接）将被 TCP 应用代理处理；TCP 代理关闭，HTTP 代理失效。

4.4 配置详解

配置项	配置建议 & 相关命令	
配置应用代理	**app-proxy enable**	开启应用代理
	app-proxy http enable	开启 HTTP 应用代理

4.4.1 配置应用代理

配置效果

- 配置应用代理后，在应用路由的状态下，应用分流效果显著提高。

注意事项

- 应用代理依赖于应用识别和应用路由。应用识别或者应用路由关闭的情况下，应用代理不生效。
- 应用代理包括 TCP 应用代理和 HTTP 应用代理，但只有应用代理开关和 HTTP 应用代理开关。

配置方法

- 全局模式下，通过开启应用代理命令开启功能。

检验方法

- 通过查看应用代理状态命令检查应用代理的状态

相关命令

开启应用代理

【命令格式】 **app-proxy enable**
【参数说明】 -
【命令模式】 全局模式
【使用指导】 -

开启 HTTP 应用代理

【命令格式】 **app-proxy http enable**
【参数说明】 -
【命令模式】 全局模式
【使用指导】 -

查看应用代理状态

【命令格式】 **show app-proxy enable**
【参数说明】 -
【命令模式】 特权模式、全局配置模式、接口模式
【使用指导】 -

配置举例

开启应用代理

【配置方法】
- 开启应用代理
- 开启 HTTP 应用代理

```
Ruijie# configure terminal
Ruijie(config)#app-proxy enable
Ruijie(config)#app-proxy http enable
```

【检验方法】
- 查看应用代理状态。

```
Ruijie#show app-proxy enable
app-proxy                              :   Y
app-proxy http                         :   Y
```

常见错误

- 配置了应用路由后，应用路由未生效，即使应用代理功能是开启状态，也不会生效。

4.5 监视与维护

清除各类信息

无

查看运行情况

作用	命令
显示应用代理信息。	**show app-proxy enable**

查看调试信息

无

5 全局会话数限制

5.1 概述

互联网技术的高速发展使得广域网上承载的应用种类和应用数量在不断增加，例如网络游戏、视频会议、VOIP（Voice Over Internet Protocol，网络电话）、电子邮件、P2P（Peer-to-Peer，点对点）应用等等。P2P 应用以其对流会话资源以及带宽资源的大需求，使得企业、网吧、高校原本还算充裕的带宽一下子变得紧张起来，也同时对网关设备提出了更多更高的要求。全局会话数限制主要在如下场景中使用

- 如何有效的分配有限的出口链路带宽，避免因为个人下载而导致整网卡。除了 QOS 或其他流量控制，全局会话数限制在一定程度上也可以达到控制出口链路带宽使用的目的。
- 如何有效的分配有限的网关/网桥设备会话资源（因为每一个会话都需要消耗网关/网桥设备一定的内存资源，而网关/网桥设备的内存资源是有限的，因此会话资源也是有限的）。在如下场景中，我们可以通过全局会话数限制来达成目的。
  a) 避免因为个人 P2P 下载而消耗太多的会话资源而导致网关/网桥设备的资源被耗尽；
  b) 避免因内网 PC 中毒发起大量会话而消耗过多的会话资源。
  c) 避免设备创建没有实际意义的会话资源而白白浪费会话资源。

下文仅介绍全局会话数限制的相关内容。

协议规范

无

5.2 典型应用

典型应用	场景描述
限制内网会话数的建立	典型企业环境，限制每个 IP 的会话数

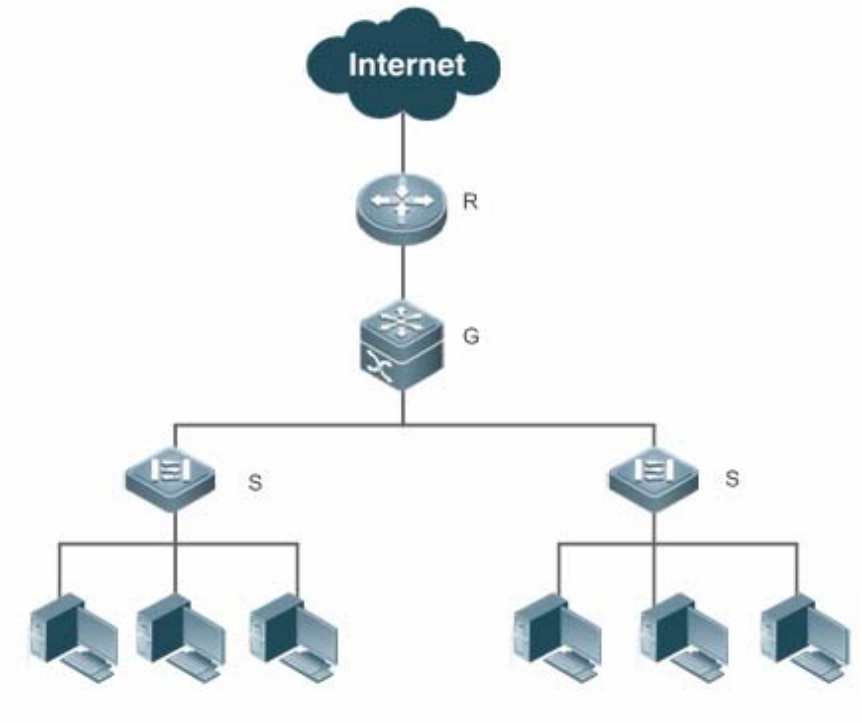
5.2.1 限制内网会话数的建立

应用场景

在一个典型的企业环境中，实现如下功能：

- 允许创建的流会话数控制在 20 万以内；
- 每个 IP 允许创建的流会话数控制在 500 以内；
- 公司领导每个 IP 允许创建的流会话数控制在 1000 以内。

图 5-1



【注释】 R 为出口网关设备。
G 为核心交换机。
S 为接入设备。

功能部属

- 配置公司领导所属的用户组以及用户信息。
- 设定默认的全局 IP 会话数限制。
- 为公司领导单独设置会话数限制值。

5.3 功能详解

基本概念

↘ 会话

五元组（内网 IP、内网端口、外网 IP、外网端口、协议）相同的报文属于同一个会话，通常情况下，锐捷网关产品会为每一条正常通信的会话分配会话资源，保证通信会话的正常进行。

功能特性

功能特性	作用
全局会话数限制开关	可以快速开启或关闭全局会话数功能
总会话数限制	限制设备整机允许创建的会话数。
基于用户/用户组进行会话数限制	基于用户/用户组设置会话数限制信息，比如用户 A，限制会话数为 300 个，用户 B 限制会话数为 500 个。
基于 ACL 进行会话数限制	基于 ACL 设置会话数限制信息，符合指定 ACL 的会话数将被受限。
限制上行报文速率	对内网 IP 的上行报文速率进行限制。
对设备进行新建防护	防止设备因新建新能不足，影响整网的体验。
端口会话数限制	防止来自特定端口的流攻击

5.3.1 全局会话数限制开关

该功能开关适用于在不删除已有的全局会话数限制规则的情况下关闭全局会话数限制功能。

工作原理

在进行全局会话数限制之前，判断开关是否已经关闭，如果是关闭状态，则不进行会话数限制。

相关配置

↘ 设置全局会话数限制开关

缺省情况下，全局会话数开关处于开启状态，只要配置了会话数限制规则，即可启动全局会话数限制。

使用 **no flow-pre-mgr enable** 来关闭全局会话数限制开关，使用 **flow-pre-mgr enable** 来开启全局会话数限制开关。

5.3.2 总会话数限制

正常情况下，每一个会话都将消耗设备一定的资源。某些情况下，为了将这种资源消耗控制在一定的范围，需要为设备整机设定一个会话数限制值。

工作原理

设备在为一条会话申请资源时，判断会话数是否已经达到限制值，如果达到，则不予创建。

相关配置

↘ 设置总会话数限制值

缺省情况下，设备所支持的会话数是由系统资源（流表容量）所决定的。

使用 **flow-pre-mgr total-limit** 来设定限制值。通常情况下无需设定该参数。

5.3.3 基于用户/用户组进行会话数限制

基于用户/用户组设置会话数限制信息，比如用户 A，限制会话数为 300 个，用户 B 限制会话数为 500 个。

工作原理

依赖于用户识别，当一个会话所属的用户/用户组信息识别出来后，我们判断这个用户/用户组的会话有没有超过限制值，如果已经超过，则不允许创建。否则正常创建会话信息。

相关配置

↘ 设置基于用户/用户组的会话数限制值

缺省无相关配置。

使用 **flow-pre-mgr** *rule-id* **subscriber** *subs_name* **action** { **block** | **by-pass** | { **trust total-limit** *total-limit-number* **per-ip-limit** *per-limit-number* } } 来设置用户/用户组的限制值。通常情况，每个 IP 的限制值建议为 500~1000。

5.3.4 基于用户/用户组进行 UDP 会话数限制

基于用户/用户组设置每用户 UDP 会话数占总会话数的比例限制值，比如用户/用户组 A 限制每用户会话数设置为 3000，再设置 UDP 流会话数所占的比例值为 50%，则该用户/用户组 UDP 的流会话数不超过 3000*50%=1500。

工作原理

依赖基于用户/用户组的流会话数的控制方式为 trust 的每 IP 流会话数限制规则，当一个会话所属的用户/用户组信息识别出来后，我们判断这个用户/用户组的 UDP 会话数有没有超过限制值，如果已经超过，则不允许创建。否则正常创建 UDP 会话信息。

相关配置

↘ 设置基于用户/用户组的会话数限制值

缺省 UDP 会话数占总会话数的比例限制值配置为 0，即不限制。

使用 **flow-pre-mgr per-ip-limit udp-ratio** *ratio* 来设置用户/用户组的 UDP 会话数占总会话数的比例限制值。通常情况，比例值建议配置为 50%。

5.3.5 基于 ACL 进行会话数限制

基于 ACL 设置会话数限制信息，符合指定 ACL 的会话数将被受限。

工作原理

判断符合指定 ACL 的会话是否已经达到限制值，如果已经达到限制值，则不允许创建。否则正常创建会话信息。

相关配置

↘ 设置基于 ACL 的会话数限制值

缺省无相关配置。

使用 **flow-pre-mgr** *rule-id* **access-list** *acl-number* **action** { **block** | **by-pass** | { **trust total-limit** *total-limit-number* } }来设置基于 ACL 的会话数限制信息。基于 ACL 的会话数限制不能配置每 IP 的会话数限制。通常本功能是用来为某一类（如攻击）会话设定一个限制值，避免其消耗太多的系统资源。

5.3.6 基于 IP 对每 IP 上行包速限制

基于 IP 对每 IP 上行包速限制，比如设置每 IP 每秒最多允许 5000 个上行报文。通常用于防上行流量攻击的场合。

工作原理

基于 IP 对每 IP 上行包速进行限制，当超过限制值时，将丢弃超限的报文。

相关配置

↘ 设置 IP 的上行包速限制值

缺省无相关配置。

使用 **flow-pre-mgr upload-pps-limit** *limit-number* 来设置真实 IP 的上行报文速率限制值。

使用 **flow-pre-mgr upload-pps-limit virtual-host limit** *limit-number* 来设置虚拟 IP 的上行报文速率限制值。

使用 **flow-pre-mgr upload-pps-limit** { **specify** *ip-addr* | **specify-range** *ip-start ip-end* | **specify-subnet** *ip-subnet ip-mask* } **limit** *limit-number* 来为指定的单 IP、IP 范围、IP 网段设置限制值。

5.3.7 对设备进行新建防护

基于 ACL 对新建报文进行过滤，阻断无意义的报文建流；基于 IP 对每 IP 新建连接速率进行限制，IP 根据攻击源区分为虚拟 IP（构造 IP）和真实 IP，所有识别成虚拟 IP 的 IP 共用一个新建连接速率限制值，每个真实 IP 有各自的新建连接限制值。通常用于防内网新建攻击的场合。

工作原理

控制新建报文的速率，当超过限制值时，将丢弃超限的报文。

相关配置

↘ 设置每 IP 的新建连接限制值

缺省无相关配置。

使用 **ip session filter** *acl-id* 来对过滤设备允许创建的流。

使用 **flow-pre-mgr protocol-enable** 来放行 OSPF、VRRP、RIP 协议。

使用 **flow-pre-mgr** { **up-deny** | **up-permit** } *id* { **{** { ip | icmp | ospf } { **src-host** *ip-addr* | **src-range** *ip-start ip-end* | **src-subnet** *ip-subnet ip-mask* } { **dst-host** { *ip-addr* | **any** } | **dst-range** { *ip-start ip-end* | **any** } | **dst-subnet** { *ip-subnet ip-mask* | **any** } } } | { { tcp | udp } { **src-host** *ip-addr* | **src-range** *ip-start ip-end* | **src-subnet** *ip-subnet ip-mask* } { **src-port** { *port* | **any** } | **sport-range** { *port-srart port-end* | **any** } } { **dst-host** {*ip-addr* | **any**} | **dst-range** { *ip-start ip-end* | **any** } | **dst-subnet** { *ip-subnet ip-mask* | **any** } } { **dst-port** { *port* | **any** } | **dport-range** { *port-srart port-end* | **any** } } } }来放行或者阻断上行报文建流。

使用 **flow-pre-mgr** { **down -deny** | **down -permit** } *id* { **{** { ip | icmp | ospf } { **src-host** { *ip-addr* | **any** } | **src-range** { *ip-start ip-end* | **any** } | **src-subnet** { *ip-subnet ip-mask* | **any** } } { **dst-host** *ip-addr* | **dst-range** *ip-start ip-end* | **dst-subnet** *ip-subnet ip-mask* } } | { { tcp | udp } { **src-host** { *ip-addr* | **any** } | **src-range** { *ip-start ip-end* | **any** } | **src-subnet** { *ip-subnet ip-mask* | **any** } } { **src-port** { *port* | **any** } | **sport-range** { *port-srart port-end* | **any** } } { **dst-host** *ip-addr* | **dst-range** *ip-start ip-end* | **dst-subnet** *ip-subnet ip-mask* } { **dst-port** { *port* | **any** } | **dport-range** { *port-srart port-end* | **any** } } } }来放行或者阻断下行报文建流。

使用 **flow-pre-mgr new-session-limit** { **start-up** | **virtual-host | real-host** } **limit** *limit-number* 来设置设备启机三分钟内、虚拟 IP、真实 IP 的新建速率限制值。

使用 **flow-pre-mgr new-session-limit** { **specify** *ip-addr* | **specify-range** *ip-start ip-end* | **specify-subnet** *ip-subnet ip-mask* } **limit** *limit-number* 来指定具体 IP、IP 范围、IP 网段的新建速率限制值。

5.3.8 端口会话数限制

对特定协议和端口的总会话数、新建会话数（真实 ip、特殊 ip 和虚拟 ip）、基于 acl 的总会话数、基于用户的每 ip 会话数做限制。

工作原理

当存在总会话数、新建会话数（真实 ip、特殊 ip 和虚拟 ip）、基于 acl 的总会话数、基于用户的每 ip 会话数的相关配置时，判定特定协议端口的会话数是否超限，超限则无法创建会话。

相关配置

↘ 设置全局端口范围和端口限制百分比

默认配置的端口为 tcp 445 端口，默认限制的百分比为 5%。

使用 **flow-pre-mgr port-limit range** { **tcp** | **udp** } *port-start port-end* 来配置端口范围。

使用 **flow-pre-mgr port-limit ratio** *num* 来配置端口限制百分比。

5.4 配置详解

配置项	配置建议 & 相关命令	
配置全局会话数限制功能	⚠ 实现全局会话数的限制功能必须配置。IP 上行包速限制值和新建连接限制值根据实际网络情况来配置。	
	flow-pre-mgr enable	启动全局会话数限制功能
	flow-pre-mgr total-limit	配置总的会话数限制值
	flow-pre-mgr subscriber	配置基于用户/用户组的会话数限制值
	flow-pre-mgr access-list	配置基于 ACL 的会话数限制值
	flow-pre-mgr priority-swap	切换两条规则的优先级
	flow-pre-mgr protocol-enable	放行协议
	flow-pre-mgr upload-pps-limit	设置真实 IP 的上行包速限制值
	flow-pre-mgr upload-pps-limit virtual-host limit	设置虚拟 IP 的上行包速限制值
	flow-pre-mgr upload-pps-limit specify	指定具体 IP 的真实主机的上行包速限制值
	flow-pre-mgr upload-pps-limit specify-range	指定具体 IP 范围的真实主机的上行包速限制值
	flow-pre-mgr upload-pps-limit specify-subnet	指定具体 IP 网段的真实主机的上行包速限制值
	flow-pre-mgr new-session-limit start-up	设置设备启机三分钟内，虚拟 IP 的新建连接限制值
	flow-pre-mgr new-session-limit virtual-host	设置设备正常运行时，虚拟 IP 的新建连接限制
	flow-pre-mgr new-session-limit real-host	设置真实 IP 的新建连接限制
	flow-pre-mgr new-session-limit specify	设置指定 IP 的真实主机的新建连接限制

	flow-pre-mgr new-session-limit specify-range	设置指定 IP 范围的真实主机的新建连接限制
	flow-pre-mgr new-session-limit specify-subnet	设置指定 IP 网段的真实主机的新建连接限制
	Ip session filter	设置设备过滤新建报文
	flow-pre-mgr up-deny	设置阻断上行新建流
	flow-pre-mgr up-permit	设置放行上行新建流
	flow-pre-mgr down-deny	设置阻断下行新建流
	flow-pre-mgr down-permit	设置放行下行新建流
	flow-pre-mgr port-limit range	添加端口限制范围
	Flow-pre-mgr port-limit ratio	设置端口限制百分比

5.4.1 配置全局会话数限制功能

配置效果

- 实现设备总的会话数限制。
- 实现基于用户/用户组的会话数限制。
- 实现基于 ACL 的会话数限制。

注意事项

- 配置基于用户/用户组的会话数限制时，需要先开启二三层用户识别功能以及配置对应的用户/用户组信息。
- 系统所配置的规则，采用后配置先生效的原则，也即最后配置的规则，其优先级最高。

配置方法

↘ 启动/关闭全局会话数限制功能

- 可选配置，默认即为开启状态。如果需要在不删除全局会话数限制规则的前提下关闭功能，则可以通过开关关闭功能。
- 在无需该功能的网关设备上关闭该功能，需要该功能的设备无需配置。

↘ 配置总的会话数限制

- 可选配置。
- 如果需要对总的会话数也进行限制，则必须配置。
- 对需要限制总的会话数的每一台网关设备进行配置，若无特殊要求，无需配置该功能。

↘ 配置基于用户/用户组的会话数限制值

- 可选配置。
- 如果需要基于用户/用户组进行会话数限制，则必须配置。
- 在需要基于用户/用户组进行会话数限制的每一台网关设备上进行如下配置：首先开启二三层用户识别，并配置具体的用户/用户组信息，然后为指定用户/用户组配置会话数限制值。通常情况下，每个 IP 的限制值设定在 500~1000 之间比较合理。

配置基于 ACL 的会话数限制值

- 可选配置。
- 如果需要基于 ACL 进行会话数限制，则必须配置。
- 在需要基于 ACL 进行会话数限制的每一台网关设备上进行如下配置：为指定 ACL 配置会话数限制值。基于 ACL 的会话数限制不能配置每 IP 的会话数限制。通常本功能是用来为某一类（如攻击）会话设定一个限制值，避免其消耗太多的系统资源。

切换两条规则的优先级

- 可选配置。
- 当需要切换某台设备两条规则的优先级时，必须使用该配置。
- 规则配置采用后配置先生效的原则，当需要切换两条规则优先级时，使用本配置来实现。

设置内网 IP 的上行包速限制值

- 可选配置。
- 当需要防上行流量攻击时，开启本功能。

设置内网 IP 的新建连接速率的限制值

- 可选配置。
- 当需要防新建攻击时，开启本功能。

设置新建流过滤的条件

- 可选配置。
- 当环境中存在大量无意义的流（如攻击流），开启本功能。

设置端口限制范围

- 可选配置，默认加入 tcp 445 端口。
- 当环境中存在大量目的端口相同的流，可使用本配置添加端口限制。
- 配合端口限制百分比使用。

设置端口限制百分比

- 可选配置，默认为 5%。
- 当环境中存在大量目的端口相同的流时，可使用本配置添加端口限制。

- 配合端口限制范围使用。

检验方法

在设备有大量会话的情况下，检查如下信息：

- 检查规则配置情况以及每个规则的会话匹配情况。
- 检查每个 IP 的会话以及限制情况。
- 检查是否存在攻击日志。

相关命令

启动/关闭全局会话数限制功能

【命令格式】 **flow-pre-mgr enable**

【参数说明】 无

【命令模式】 全局模式

【使用指导】 使用此命令开启全局会话数限制功能，默认开关为开启状态。使用 **no flow-pre-mgr enable** 来关闭全局会话数功能。

配置总的会话数限制

【命令格式】 **flow-pre-mgr total-limit** *limit-number*

【参数说明】 limit-number：全局的流会话数限制值，取值跟设备内存大小有关，其中 0 表示不限制。

【命令模式】 全局模式

【使用指导】 1） 要删除相关的配置，在全局配置模式下通过执行 no flow-pre-mgr total-limit 即可。

2） 设备所能支持的最大流会话数与设备的内存有关，配置该命令时，允许输入的最大值即为设备最多支持的流会话数。

3） 网关模式下，对于上一级路由器的路由错误导致的源进源出的数据流，我们不做限制。

配置基于用户的会话数限制值

【命令格式】 **flow-pre-mgr** *rule-id* **subscriber** *subs_name* **action** { **block** | **by-pass** | { **trust total-limit** *total-limit-number* **per-ip-limit** *per-limit-number* } }

【参数说明】 *rule-id*：规则的标识号，取值范围为 1~50，当配置的标识号已经被使用时，则会提示冲突，无法配置成功；

subs_name：规则关联的静态用户或静态用户组；

total-limit-number：用户/用户组总的流会话数限制值，取值跟设备内存有关，其中 0 表示不限制。

per-limit-number：该用户/用户组下每 IP 的流会话数限制值，取值范围与设备内存有关，不能大于 total-limit-number，其中 0 表示不限制。

【命令模式】 全局模式

【使用指导】 1） 配置基于用户/用户组的流会话数的控制方式：block、by-pass 或 trust，要删除相关的配置，在全局配置模式下通过执行 no flow-pre-mgr *id* 即可。

2） 配置的规则具有优先级，优先级按照最后配置的规则优先级最高的原则来定义。

3） action 的说明，block 表示不允许流会话通信；by-pass 表示不需要创建流会话，直接根据桥的映射关系转发报文（该命令关键字只有在桥接模式、单臂模式下才会出现，网关模式下是不会有该命令关键字的）；trust 表示允许配置用户/用户组的流会话数限制以及每 IP 的流会话数限制，流会话超过指定的限制值后不再允许新建流会话通信。

4） 设备所能支持的最大流会话数与设备的内存有关，配置该命令时，允许输入的最大值即为设备最多支持的流会话数。

5） 网关模式下，对于上一级路由器的路由错误导致的源进源出的数据流，我们不做限制。

配置基于 ACL 的会话数限制值

【命令格式】 **flow-pre-mgr** *rule-id* **access-list** *acl-number* **action** { **block** | **by-pass** | { **trust total-limit** *total-limit-number* } }

【参数说明】 *rule-id*：规则的标识号，取值范围为 1~50，当配置的标识号已经被使用时，则会提示冲突，无法配置成功；

acl-number：规则关联的 ACL 号，取值范围为 1~199；

total-limit-number：ACL 总的流会话数限制值，取值范围与设备内存有关，其中 0 表示不限制。

【命令模式】 全局模式

【使用指导】 1） 配置基于 ACL 的流会话数控制方式：block、by-pass 或 trust，要删除相关的配置，在全局配置模式下通过执行 no flow-pre-mgr id 即可。

2） 配置的规则具有优先级，优先级按照最后配置的规则优先级最高的原则来定义。

3） 基于 ACL 的流会话数限制不允许用户配置每 IP 的流会话数限制。

4） action 的说明，block 表示不允许流会话通信；by-pass 表示不需要创建流会话，直接根据桥的映射关系转发报文（该命令关键字只有在桥接模式、单臂模式下才会出现，网关模式下是不会有该命令关键字的）；trust 表示允许配置该 ACL 的总流会话数限制，流会话超过指定的限制值后不再允许新建流会话通信。

5） 所述 ACL 中的源 IP 对应内网 IP，源端口对应内网端口，目的 IP 对应外网 IP，目的端口对应外网端口。

6） 设备所能支持的最大流会话数与设备的内存有关，配置该命令时，允许输入的最大值即为设备最多支持的流会话数。

7） 基于 ACL 的流会话数限制规则对性能影响较大，不能配置太多。本规则通常用于避免设备创建无意义的流会话，参考示例。

8） 规则关联的 ACL，其包含的 ACL 条目仅支持配置源 IP、源端口、目的 IP、目的端口、协议号，否则该条 ACL 条目在本模块是无法生效的。

9） 网关模式下，对于上一级路由器的路由错误导致的源进源出的数据流，我们不做限制。

切换两条规则的优先级

【命令格式】 **flow-pre-mgr priority-swap** *rule-id1 rule-id2*

【参数说明】 *rule-id1* 和 *rule-id2* 是要切换的两个规则 ID。

【命令模式】 全局模式

【使用指导】 rule-id1 和 rule-id2 都必须已经存在，否则命令不会实际生效。

如果 rule-id1 和 rule-id2 是一样的，则不做任何处理。

设置每 IP 上行包速限制值

【命令格式】 **flow-pre-mgr upload-pps-limit** *limit-number*

【参数说明】 *limit-number：*上行包速限制值，取值范围：0-100000

【命令模式】 全局模式

【使用指导】 所有真实 IP 的上行包速限制值都相同，但是基于 IP 计算各自的上行包速。

不宜配置过大或者过小，否则可能导致网络异常，建议设置为 3000~5000，0 是不限制。服务器之类的要使用 specify 命令单独配置。

↘ 设置指定 IP 上行包速限制值

【命令格式】 **flow-pre-mgr upload-pps-limit** { **specify** *ip-addr* | **specify-range** *ip-start ip-end* | **specify-subnet** *ip-subnet ip-mask* } **limit** *limit-number*

【参数说明】 *ip-addr：指定的具体 IP*

ip-start：指定 IP 范围的开始 IP

ip-end：指定 IP 范围的结束 IP

ip-subnet：指定子网网段

ip-mask：指定掩码

*limit-number：*上行包速限制值，取值范围：0-100000

【命令模式】 全局模式

【使用指导】 如果有一些 IP 比较特殊（比如服务器之类的 IP），real-host 的限制值不适用是，可以使用此命令，对这些 IP 单独限制。

不宜配置过大或者过小，过大可能起不到保护作用，过小则可能引起这些 IP 的访问异常，建议设置为 10000~20000，具体还要看实际网络环境。

另外，如果发现某个真实 IP 被识别成了虚拟 IP，也可以通过该命令把该 IP 加入真实 IP 中。

↘ 过滤新建报文，阻断非法报文建流

【命令格式】 **ip session filter** *acl-id*

【参数说明】 *acl-id：*ACL 的 ID

【命令模式】 全局模式

【使用指导】 新建报文过滤的原理是放行网络环境中合法报文，阻断非法访问的报文。

合法是指网络环境是实际存在的 IP 发出的报文。

非法是指网络中不存在的 IP 发出来的报文，比如 D/DOS 攻击伪造出来的 IP。

↘ 过滤上行新建报文，阻断非法报文建流

【命令格式】 **flow-pre-mgr** { **up-deny** | **up-permit** } *id* { { { ip | icmp | ospf } { **src-host** *ip-addr* | **src-range** *ip-start ip-end* | **src-subnet** *ip-subnet ip-mask* } { **dst-host** { *ip-addr* | **any** } | **dst-range** { *ip-start ip-end* | **any** } | **dst-subnet** { *ip-subnet ip-mask* | **any** } } } | { { tcp | udp } { **src-host** *ip-addr* | **src-range** *ip-start ip-end* | **src-subnet** *ip-subnet ip-mask* } { **src-port** { *port* | **any** } | **sport-range** { *port-srart port-end* | **any** } } { **dst-host** {*ip-addr* | **any**} | **dst-range** { *ip-start ip-end* | **any** } | **dst-subnet** { *ip-subnet ip-mask* | **any** } } { **dst-port** { *port* | **any** } | **dport-range** { *port-srart port-end* | **any** } } } }

【参数说明】 *ip-addr：指定的具体 IP*

ip-start：指定 IP 范围的开始 IP

ip-end：指定 IP 范围的结束 IP

ip-subnet：指定子网网段

ip-mask：指定掩码

port：端口

port-srart：端口范围的起始端口

port-end：端口范围的结束端口

【命令模式】 全局模式

【使用指导】 新建报文过滤的原理是放行网络环境中合法报文，阻断非法访问的报文。

合法是指网络环境是实际存在的 IP 发出的报文。

非法是指网络中不存在的 IP 发出来的报文，比如 D/DOS 攻击伪造出来的 IP。

这个命令的作用和 ip session filter 作用一样，只是用来过滤上行报文。有这条命令的原因是 ip session filter 过滤的性能比较差，存在大量 ACE 的情况下，可以用这条命令和下行新建报文过滤的命令配合起来用。

配置该命令时源 IP 不能为 any。

↘ 过滤下行新建报文，阻断非法报文建流

【命令格式】 **flow-pre-mgr** { **down -deny** | **down -permit** } *id* { { { ip | icmp | ospf } { **src-host** { *ip-addr* | **any** } | **src-range** { *ip-start ip-end* | **any** } | **src-subnet** { *ip-subnet ip-mask* | **any** } } { **dst-host** *ip-addr* | **dst-range** *ip-start ip-end* | **dst-subnet** *ip-subnet ip-mask* } } | { { tcp | udp } { **src-host** { *ip-addr* | **any** } | **src-range** { *ip-start ip-end* | **any** } | **src-subnet** { *ip-subnet ip-mask* | **any** } } { **src-port** { *port* | **any** } | **sport-range** { *port-srart port-end* | **any** } } { **dst-host** *ip-addr* | **dst-range** *ip-start ip-end* | **dst-subnet** *ip-subnet ip-mask* } { **dst-port** { *port* | **any** } | **dport-range** { *port-srart port-end* | **any** } } } }

【参数说明】 *ip-addr：指定的具体 IP*

ip-start：指定 IP 范围的开始 IP

ip-end：指定 IP 范围的结束 IP

ip-subnet：指定子网网段

ip-mask：指定掩码

port：端口

port-srart：端口范围的起始端口

port-end：端口范围的结束端口

【命令模式】 全局模式

【使用指导】 新建报文过滤的原理是放行网络环境中合法报文，阻断非法访问的报文。

合法是指网络环境是实际存在的 IP 发出的报文。

非法是指网络中不存在的 IP 发出来的报文，比如 D/DOS 攻击伪造出来的 IP。

这个命令的作用和 ip session filter 作用一样，只是用来过滤下行报文。有这条命令的原因是 ip session filter 过滤的性能比较差，存在大量 ACE 的情况下，可以用这条命令和上行新建报文过滤的命令配合起来用。

配置该命令时，目的 IP 不能为 any。

↘ 设置放行 OSPF、VRRP、RIP 协议

【命令格式】 **flow-pre-mgr protocol-enable**

【参数说明】 *无*

【命令模式】 全局模式

【使用指导】 放行 OSPF、VRRP、RIP 协议，使其不受新建速率限制，不受并发会话数限制。

设置 IP 的新建连接限制

【命令格式】 **flow-pre-mgr new-session-limit** { **start-up** | **virtual-host | real-host** } **limit** *limit-number*

【参数说明】 *limit-number：* IP 的新建连接限制值，取值范围：0-100000

【命令模式】 全局模式

【使用指导】 start-up：IP 上线时，在有建立 TCP 流之前都当成虚拟 IP 处理，所有虚拟 IP 的新建速率是累加到一起的；设备启机的时候，内网 IP 集中上线，如果限制值设置太小，会影响内网 IP 上线，所以，该条命令的限制值可以设置大些，20000-30000。

Virtual-host：设备正常运行时，正常的内网 IP 基本上都会有 TCP 连接建立，不再属于虚拟 IP，如果还是有 IP 识别成虚拟 IP，则该 IP 有可能就是一个攻击源，所以设备正常运行时，虚拟 IP 的新建连接速度可以比开机三分钟内的配置稍微小一点。因为新上线的正常 IP，一开始也是看成虚拟 IP 处理的，如果限制值配置的太小，被攻击耗光了，则会影响该 IP 的上线，所以设备正常运行时，虚拟 IP 的限制值也不宜过小，也不宜太大，经验值 3000 左右即可。

Real-host：

Real-host：内网 IP 有 TCP 连接建立后，设备就把该 IP 标识成真实 IP，然后采用默认的新建连接限制。该命令就是用于配置所有真实 IP 的默认新建连接限制值。

设置指定 IP 的真实主机的新建连接限制

【命令格式】 **flow-pre-mgr new-session-limit** { **specify** *ip-addr* | **specify-range** *ip-start ip-end* | **specify-subnet** *ip-subnet ip-mask* } **limit** *limit-number*

【参数说明】 *ip-addr：指定的具体 IP*

ip-start：指定 IP 范围的开始 IP

ip-end：指定 IP 范围的结束 IP

ip-subnet：指定子网网段

ip-mask：指定掩码

*limit-number：*上行包速限制值，取值范围：0-100000

【命令模式】 全局模式

【使用指导】 所有真实 IP 可以配置一个默认的限制值，但是针对一些特殊的真实 IP，如服务器，它们的新建连接一般都比较大，需要另外配置。另外，如果发现某个真实 IP 被识别成了虚拟 IP，也可以通过该命令把该 IP 加入真实 IP 中。

设置端口限制范围

【命令格式】 **flow-pre-mgr port-limit range** { **tcp** | **udp** } *port-start port-end*

【参数说明】 *port-start*：端口范围的起始端口

port-end：端口范围的结束端口

【命令模式】 全局模式

【使用指导】 当环境中存在大量目的端口相同的流时，可通过改命令添加端口限制范围；该范围作用于总会话数限制、新建会话数限制（真实 ip、特定 ip、虚拟 ip）、基于 acl 的总会话数限制、基于用户的每 ip 会话数限制；配合端口限制百分比使用。

设置端口限制百分比

【命令格式】 **flow-pre-mgr port-limit ratio** *num*

【参数说明】 *num*：百分比数值

【命令模式】 全局模式

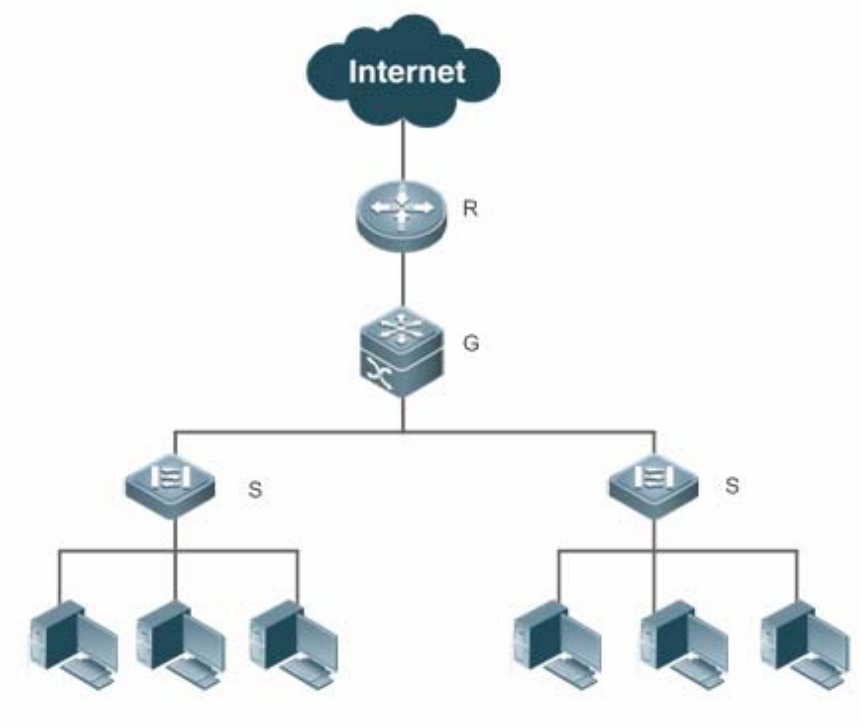
【使用指导】 当环境中存在大量目的端口相同的流时，可通过改命令添加端口限制范围；该百分比作用于总会话数限制、新建会话数限制（真实 ip、特定 ip、虚拟 ip）、基于 acl 的总会话数限制、基于用户的每 ip 会话数限制；配合端口限制范围使用。

配置举例

以下配置举例，仅介绍与全局会话数限制相关的配置。

典型企业环境设置全局会话数功能

【网络环境】



【配置方法】

- 允许创建的流会话数控制在 20 万以内；
- 每个 IP 允许创建的流会话数控制在 500 以内；
- 公司领导每个 IP 允许创建的流会话数控制在 1000 以内。
- 公司普通 PC 新建速率限制在每秒 300
- 公司服务器网段的新建速率放大到 1000，服务器网段：192.168.4.0/24

R

1）配置用户信息

```
# 进入全局配置模式层
R# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
# 配置公司领导的用户组
R(config)# subscriber static name LeaderGroup parent /
# 配置公司领导的用户信息
R(config)# subscriber static name LeaderA parent /LeaderGroup ip-host 192.168.5.11
R(config)# subscriber static name LeaderB parent /LeaderGroup ip-host 192.168.5.12
2）配置流会话数预创建限制与管理的规则
# 配置全局流会话数限制
R(config)# flow-pre-mgr total-limit 200000
#配置所有用户的流会话数限制
R(config)# flow-pre-mgr subscriber any action trust total-limit 0 per-ip-limit 500
#配置公司领导的流会话数限制
R(config)# flow-pre-mgr subscriber LeaderGroup action trust total-limit 0 per-ip-limit 1000
3）配置普通 PC 的新建速率限制
# 配置启机三分钟内的新建连接速率
R(config)# flow-pre-mgr new-session-limit start-up limit 20000
#配置虚拟 IP 的新建连接限制限制
R(config)# flow-pre-mgr new-session-limit virtual-host limit 3000
#配置普通 PC 的新建连接限制
R(config)# flow-pre-mgr new-session-limit real-host limit 300
4）配置服务器的新建速率限制
# 配置指定网段的新建连接速率
R(config)# flow-pre-mgr new-session-limit specify-subnet 192.168.4.0 255.255.255.0 limit 1000
```

【检验方法】 在设备有大量会话的情况下，检查如下信息：

- 检查规则配置情况以及每个规则的会话匹配情况。
- 检查每个 IP 的会话以及限制情况。

```
R# show flow-pre-mgr rule-info
R# show flow-pre-mgr ip-info
R# show flow-pre-mgr new-session-limit attack
R# show flow-pre-mgr drop-count
```

常见错误

- 配置基于用户/用户组的会话数限制功能前没有配置相应的用户/用户组信息或没有开启二三层用户识别。
- 配置了基于 ACL 的会话数限制规则，但是却没有配置相应的 ACL。
- 基于 ACL 的会话数限制仅支持五元组（内网 IP、内网端口、外网 IP、外网端口、协议）的 ACL，如果配置了其他的，则实际上会不生效。

5.5 监视与维护

清除各类信息

无

查看运行情况

作用	命令
查看配置的规则	**show flow-pre-mgr rule-info**
查看 IP 的会话数（包括 UDP 会话数）以及限制参数	**show flow-pre-mgr ip-info** [*ip-address*]
查看防上行流量攻击的配置参数	**show flow-pre-mgr upload-pps-limit**
查看防新建连接攻击的配置参数	**show flow-pre-mgr new-session-limit**
查看最近一次新建连接攻击的记录	**show flow-pre-mgr new-session-limit attack**
查看防攻击丢包情况	**show flow-pre-mgr drop-count**

查看调试信息

无

6 流量控制

6.1 概述

流量控制，简称流控，是将流量按照一定的规则进行分类，并进行有区别的转发和丢包的机制。

通过实施流控方案，可以保障关键流量，抑制恶意流量。

可以在带宽不够充分、需要合理分配流量时，启用流控。

协议规范

无

6.2 典型应用

流控对流量进行分类的方法有以下几种：

- 基于二层（VID）的分类
- 基于用户的分类，这里的用户分类对象包含了用户名和内网源 IP 的映射关系
- 基于网络的分类
- 基于认证对象分类，默认匹配所有认证对象
- 基于应用识别的分类，支持用户自定义的协议分类对象
- 基于是否为 vpn 报文进行分类
- 基于时间段的分类
- 基于帐号的分类

以上分类可以叠加使用，比如可以同时指定网络分类和应用分类。因此，可以组合非常多的分类，实现很多不同场景。下表罗列了流控的典型应用场景：

典型应用	场景描述
基于应用进行流控_在一个 AS 内提供组播服务	将应用区分优先级，高优先级的应用优先保障。比如优先保证游戏，然后照顾视频。
基于 IP 进行流控	将用户区分优先级，高优先级的用户优先保障。比如 VIP 客户优先保障，然后照顾普通客户。
基于时间段的流控	将流量按照时间段分类，以区分对待。比如可以配置上班时间不允许上网。
基于帐号进行流控	基于帐号带宽分配，比如学生帐号带宽限速 4M，不管多少终端都是加起来限速 4M

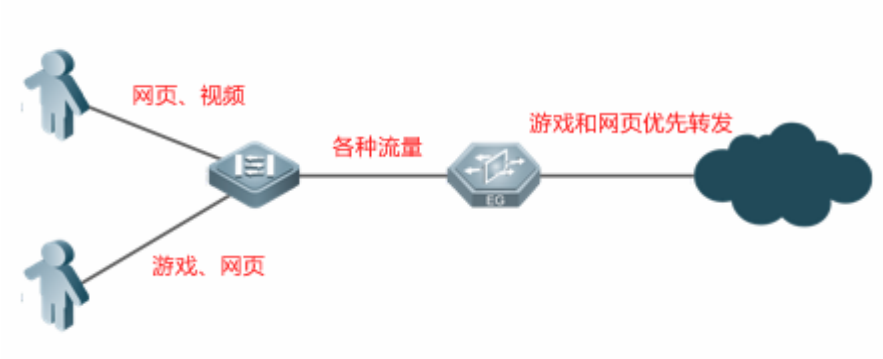
6.2.1 基于应用的流控

应用场景

在某些环境下，用户希望为应用划分优先级，对高优先级的应用，优先保障。

以网吧为例，游戏和上网的优先级最高，视频的优先级最低。这时候，可以配置基于应用的流控，将优先保证游戏和上网等关键应用。如下图所示：

图 6-1



功能部属

- 配置流控通道。
- 配置流控策略。
- 开启应用识别功能。

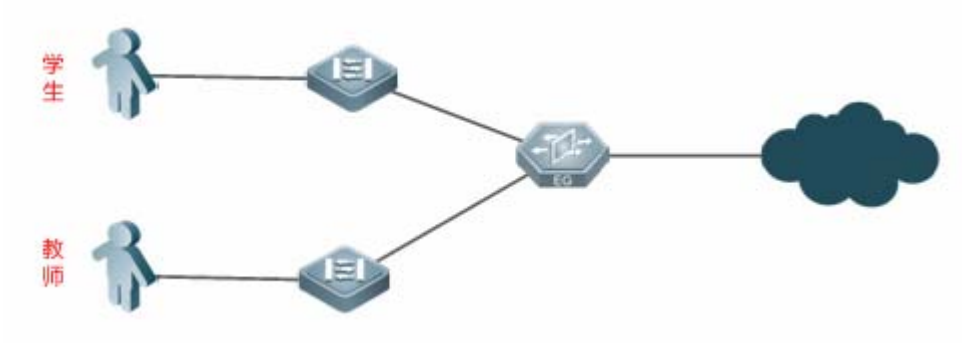
6.2.2 基于每 IP 的流控

应用场景

在某些环境下，用户希望按照用户划分优先级，对重要客户优先保障。

这种场景，可以配置基于 IP 的流控。举例：用户有两种客户，学生和教师， 用户想实现教师分配 10M 带宽、学生分配 2M 带宽的效果。如下图所示：

图 6-2



功能部属

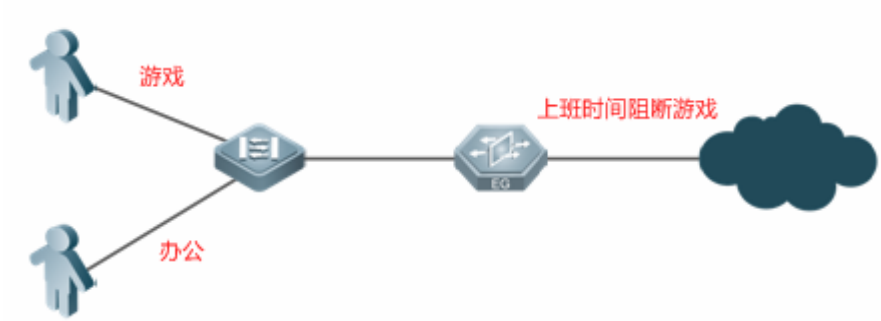
- 配置流控通道。
- 配置流控策略。
- 开启用户识别功能。

6.2.3 基于时间段的流控

应用场景

在某些场景下，用户需要在不同的时间段设置不同的流控方案。这时候可以配置基于时间段的流控，比如公司可以限制员工在上班时间不能玩游戏。如下图所示：

图 6-3



功能部属

- 配置流控通道。
- 配置流控策略。
- 配置时间段对象。

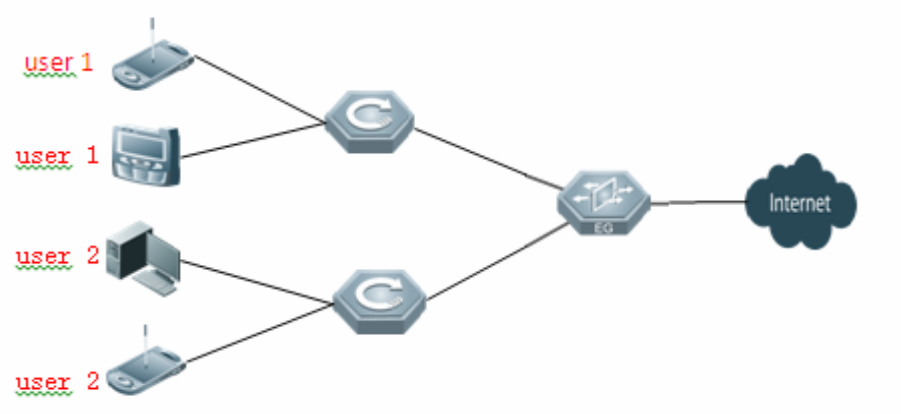
6.2.4 基于每帐号的流控

应用场景

在某些环境下，要基于帐号分配带宽。多个终端(如 pad、笔记本、手机等)使用同一个帐号。

这种场景，可以配置基于帐号的流控。举例：用户有两个帐号，user 1 和 user 2， 用户想实现 user 1 帐号分配 10M 带宽、user 2 帐号分配 2M 带宽的效果。如下图所示：

图 6-4



功能部属

- 配置流控通道。
- 配置流控策略。
- 开启帐号识别功能。

6.3 功能详解

基本概念

↘ ‘流控组’和‘流控树’

锐捷出口网关系列产品，可以在设备的 wan 口上起用流控功能：在接口上应用流控组。

流控组包含了上行流控树和下行流控树，分别对上下行流量进行控制。在流控树中，定义一些流控通道用来缓存报文。同时流控组内可以配置一系列流控策略，用来指明报文行为和进入的通道。

↘ 流控通道

设备根据流控通道的属性，来缓存和转发报文。

↘ 保证带宽（CIR）

cir 为分配给流控通道的带宽额度。

↘ 最大带宽（CIR）

pir 为允许通道最大可以占用的带宽额度。

↘ 每 IP 最大带宽（PER-CIR）

如果通道配置为 per-ip 类型，则可以设置每 IP 的最大带宽：per-cir。

↘ 流控策略

流控策略，负责规划指定流量进入指定的流控通道。比如可以创建一条策略，指定游戏进入关键通道。再创建一条策略，指定 P2P 视频进入抑制通道。

↘ 流控模版

为了降低配置的难度，在空配置起机情况下流量控制会生成默认的配置模板。这些配置模板支持修订，保存重启后相关修订不会丢失。

功能特性

功能特性	作用
流控基本功能	实现流量控制
auto-pir 功能	保证关键应用及时抢占带宽
共享池限速	共享池允许流控通道加入，通过影响加入通道的发包调度，从而实现更加灵活的流量控制

6.3.1 流控基本功能

流控基本功能即流量控制。

工作原理

流量控制，包含以下几个步骤：

1. 将设备待转发的报文送入不同的队列进行缓存，这些队列被称为“通道”；
2. 根据通道的属性，对队列中的报文进行调度发送。

流控基本功能有两部分，“流控策略”和“流控通道”。流控通道用来实际缓存和转发报文，流控策略用来决定报文是否应该被丢弃。如果不丢弃，则流控策略决定报文应该进入的通道。

↘ 报文分类缓存

设备根据配置的流控策略，将待转发的报文缓存在流控的通道中。

目前，流控设置支持以下数据流的分类方法：

- 基于二层（VID）的分类
- 基于用户的分类，这里的用户分类对象包含了用户名和内网源 IP 的映射关系
- 基于网络的分类
- 基于认证对象分类，默认匹配所有认证对象
- 基于应用识别的分类，支持用户自定义的协议分类对象
- 基于是否为 vpn 报文进行分类
- 基于时间段的分类
- 基于帐号的分类

流量控制策略就是基于上述对数据流的几类类分类方法来实现的，将分类对象进行组合构成一条策略规则的关键字，加上策略规则所要对数据流采取的动作(阻断、限速等)就基本上构成了一条策略规则了，所有策略规则的集合就形成了流量控制策略。

↘ 报文发送

设备按照流控通道的属性进行报文转发，流控通道有一系列属性

1. 父通道。和现实环境中带宽划分模型对应，流控通道最终组成一个树形结构。因此，流控通道必定有一个父通道（root 通道除外）；同时，可以多个流控通道共有一个父通道，这些流控通道之间为兄弟关系。

⚠ 如果流控通道不存在父通道，则表明该通道为根通道；

⚠ 一个流控通道树只能有一个根通道。

2. 带宽。流控通道带宽包括两部分：承诺信息速率 cir 和峰值信息速率 pir，pir 必须大于等于 cir。cir 为分配给流控通道的带宽额度，pir 为允许通道最大可以占用的带宽额度，pir 的存在允许流控通道超过 cir 的带宽限制发送报文，从而实现所谓的弹性带宽。弹性带宽的意义在于实现带宽的充分利用，如某个公司出口 10M，公司部门一分配带宽 cir：5M pir：10M，当出口带宽没有其它部门使用时，部门一最大可以占用全部的 10M 带宽。

3. 优先级。流控通道之间的调度采用绝对优先级，高优先级的通道总是优先得到调度，从而拥塞情况下丢包的概率更低。

⚠ 流控通道优先级支持 0～7，其中 0 优先级最高，7 优先级最低；

⚠ 需要注意的是，通道优先级与带宽借用效果并无直接关联；

4. 通道类型。流控通道支持内部实现不同的调度队列和算法，包括先进先出队列、公平队列等。先进先出队列最为简单，入队报文加入队列尾部，出队报文从队列头部获取，实现报文的顺序发送。

   公平队列，顾名思义，其意义在于保证发包机会的公平性，适用于拥塞的情况，保证大流量的连接不会占用所有带宽，小流量的连接也能获取到发包机会。目前流量控制支持两种类型的公平队列： Per-net 队列和 Per-user 队列。

   Per-net 是基于网段公平的队列，其根据用户配置的网段数创建对应个数的队列，报文基于所属网段入对应队列，然后对所有队列轮转发包。为了避免某个网段占用过多的带宽，Per-net 可以指定每个内部队列的承诺带宽和峰值带宽。默认针对内网网段限速，可以配置反向 Per-net 以实现针对外网网段限速。

   Per-user 是基于帐号公平的队列，其根据用户配置的帐号数创建对应个数的队列，报文基于所属帐号入对应队列，然后对所有队列轮转发包。为了避免某个帐号占用过多的带宽，Per-user 可以指定每个帐号的承诺带宽和峰值带宽。

相关配置

↘ 配置流控组

缺省情况下，设备中存在一些流控模版。可以以已有的流控组为模板，拷贝一份新的配置，并可以更新带宽大小，用于部署阶段根据模板或者其它流控组快速生成新的配置：

flow-template copy *Src_name Dst_name* **[bandwith**_*In_bandwith Out_bandwith* **[perpir-update]] [force]**

如果流控模版满足不了用户需求，可以自己配置流控组：

1. 使用 **flow-control** { *name* [**update bandwith**_*In_bandwith Out_bandwith* [**perpir-update**]] }命令可以创建一个流控组。
2. 使用 **channel-tree** { **inbound** | **outbound** }创建流控通道树；
3. 使用 **channel-group** *name* **parent** { **NULL** | *parent_name*} [**cir** *cir_num*] **pir** *pir_num* [**pri** *pri_num*] [ ] { **fifo** | { **per-net** [**per-mask** *mask*] | **per-user** } **per-pir** *ppir_num* [**limit** *limit_num*] [**session-limit** *session_limit_num*] [**reverse**] } 创建流控通道；
4. 使用 **flow-rule** *num* [**vlan-group** *vlan-group-name*] [**subscriber** *subscriber-name*] [**auth-group** *auth-group-name*] [**network-group** *network-group-name*] [**app-group** *app-group-name*] **time-range** *time-rang-name* [**vpn**] 和 **flow-rule** *num* **action** { **drop** | **log-drop** | **pass** [**in-channel** *in-channel-name*] [**out-channel** *out-channel-name*] } [**default**] [**commet** *string*]创建流控策略。

↘ 启动 WAN 口上的流控功能

缺省情况下，WAN 口上的流控功能关闭。

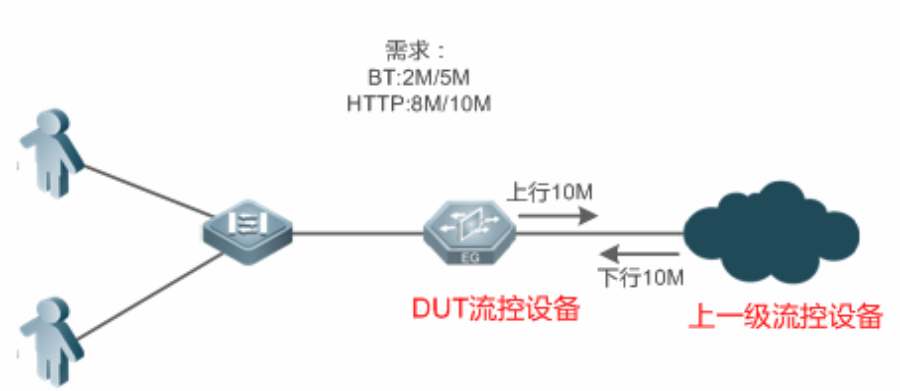
使用 **flow-policy** *name* 命令可以启动 WAN 口上的流控功能，使用 **no flow-policy** 可以取消某个特定的流量组在接口上的应用。

必须在接口上启用流控功能。

6.3.2 auto-pir 功能

工作原理

auto-pir 的场景如下：



针对 DUT 流控设备，需求如下：

1. BT 保证带宽(CIR)为 2M，最大带宽（PIR）为 5M；

2. HTTP 保证带宽(CIR)为 8M，最大带宽（PIR）为 10M；

需要说明的是，该场景下上一级流控设备对下行流量限速 10M，对于超出的流量进行无差别的丢包。该场景具有的普适意义在于，无论是企业、学校还是金融行业，接入 Internet 时，ISP(Internet Service Provider，网络服务器提供商)都是承诺了最大支持的带宽，如 2M、10M 等等。

测试时，先开始 BT 下载，达到预期结果：最大可以达到 5M 的流量；然后开始 HTTP 流量下载，预期结果：HTTP 达到保证的 8M 带宽，BT 流量为 2M，但实测结果：BT 流量 5M，HTTP 流量 5M。原因分析如下：

1) 上一级流控设备限制下行 10M，针对 BT 和 HTTP 进行无差别、成比例的丢包；

2) BT 流量由于连接数众多、报文数量大，在上一级流控设备抢占大量带宽，导致 HTTP 流量出现丢包，实际到达 DUT 设备的 HTTP 流量只有 5M，从而无法抢占更多带宽；

PIR 动态调整功能通过识别上述场景：在总带宽紧张的前提下，如果存在通道速率超过 CIR，则针对速率超过 CIR 的通道，降低其 PIR。以上述场景为例，通过压制 BT 流量 PIR 为 2M，使通过 DUT 设备下行 BT 流量从原来的 5M 降低为 2M，大量的丢包使得 BT 对端降低发送速率，从而到达上一级流控设备 BT 流量大量减少，HTTP 流量得以占用更多带宽。

相关配置

↘ 配置 auto-pir

缺省情况下，NPE 产品默认关闭，其它 EG、NBR、AG 等网关设备默认开启。

可以通过 **auto-pir enable** [**interval** *NUM* [**root-rate** *Percentage*]] [**exclude-pass**] 这条命令，使能流控通道树的 PIR 动态调整功能。使用 **no auto-pir enable** 关闭流控通道数的 PIR 动态调整功能。

6.3.3 共享池限速

工作原理

共享池允许流控通道加入，通过影响加入通道的发包调度，从而实现更加灵活的流量控制。共享池有如下两个属性：

1. 带宽

   即共享池限速值，共享池为 Normal 类型时，针对加入共享池所有流控通道的总流量限速；共享池为 Per-IP 时，针对加入共享池所有流控通道的每用户流量限速。

2. 共享池类型

   共享池有 Normal 和 Per-IP 两种类型，含义见上面说明。当共享池为 Per-IP 类型时，有如下注意事项：

   a. 必须配置用户数限制 Limit 值，超出限制用户的流将会被阻断；

   b. 加入 Per-IP 类型共享池的通道必须为 Per-net 类型，且 per-mask 为 32，即 Per-IP 类型，并且通道 Limit 限制必须小于等于共享池 Limit 限制；

⚠ 只支持流控树最下面两层的通道加入共享池，即只有叶子通道及其上一级的父通道允许加入共享池，并且叶子通道和其父通道不能加入同一个共享池

⚠ 共享池最大只支持 8 个成员通道，如果某成员通道为非叶子节点，该通道的子通道数也必须小于等于 8 个

⚠ 加入共享池的通道如果优先级不同，最坏情况下高优先级通道会抢占共享池所有带宽，配置时需注意是否为想要的效果

⚠ NPE 产品不支持共享池功能，其它 EG、NBR、AG 等网关设备支持

相关配置

缺省情况下，没有配置共享池。

可以通过命令 **share-pool** *Name* **rate** *num1* [**type** { **normal** | **per-ip** [**limit** *num2*l }]配置共享池。通过命令 **no share-pool** *Name* 删除共享池。

6.4 配置详解

配置项	配置建议 & 相关命令	
配置流控基本功能	⚠ 必须配置。用于建立流控组。	
	flow-control { *name* [**update bandwith** *_In_bandwith Out_bandwith* [**perpir-update**]] }	配置流量控制组(简称流控组)
	channel-tree { inbound | outbound }	创建流控通道树
	channel-group *name* **parent** { **NULL** | *parent_name* } [**cir** *cir_num*] **pir** *pir_num* [**pri** *pri_num*] [ ] { **fifo** | { **per-net** [**per-mask** *mask*] | **per-user** } **per-pir** *ppir_num* [**limit** *limit_num*] [**session-limit** *session_limit_num*] [**reverse**] }	创建流控通道
	flow-rule *num* [**vlan-group** *vlan-group-name*] [**subscriber** *subscriber-name*] [**auth-group** *auth-group-name*] [**network-group** *network-group-name*] [**app-group** *app-group-name*] **time-range** *time-rang-name* [**vpn**] **flow-rule** *num* **action** { **drop** | **log-drop** | **pass** [**in-channel** *in-channel-name*] [**out-channel** *out-channel-name*] } [**default**] [**commet** *string*]	配置一条流控策略规则，需要分成两部分进行配置，前半部分表示策略规则的关键字，后半部分表示策略规则的动作

	flow-policy *name*	将流量控制组应用到 wan 口上
配置 auto-pir	⚠ 可选配置。通过配置 auto-pir，可以在带宽用满时，关键流量还可以快速抢占带宽。	
	auto-pir enable [**interval** *NUM* [**root-rate** *Percentage*]] [**exclude-pass**]	使能流控通道树的 PIR 动态调整功能
配置共享池限速	⚠ 可选配置。共享池允许流控通道加入，通过影响加入通道的发包调度，从而实现更加灵活的流量控制。	
	share-pool *Name* **rate** *num1* [**type** { **normal** | **per-ip** [**limit** *num2* **l** }]	创建共享池

6.4.1 配置流控基本功能

配置效果

- 创建流控组并在接口上启用，可以实现基本的流控功能。

注意事项

- 如果配置基于应用的流控，需要开启应用识别功能。
- 如果配置基于用户的流控，需要开启用户识别功能。
- 如果配置基于时间段的流控，需要配置相应的时间段对象。
- 如果配置基于帐号的流控，需要帐号是认证用户并且开启二三层识别。

配置方法

↘ 使用模版拷贝功能

- 非必须配置
- 使用模版拷贝功能，可以直接拷贝得到一个流控组。

↘ 创建流控组

- 除非使用模版拷贝功能，否则必须配置。
- 每个 WAN 口上可以启用一个流控组。

↘ 创建流控树

- 除非使用模版拷贝功能，否则必须配置。
- 每个流控组包含上行流控树和下行流控树，分别对上行和下行流量进行控制。

创建流控通道

- 除非使用模版拷贝功能，否则必须配置。
- 在流控树下面配置流控通道，用于缓存和转发报文。

创建流控策略

- 一般情况下，需要配置流控策略。否则报文进入默认通道进行转发。
- 如果流控策略中指明 vlan、应用识别等流控对象，还需要到相关模块下创建相应的对象。

在接口上启用流控

- 必须配置。

检验方法

可以通过查看策略有效性和通道的速率来判断流控是否生效。

- 查看策略有效性。
- 查看通道的速率。

相关命令

模版拷贝

【命令格式】 **flow-template copy** *Src_name Dst_name* [**bandwith**_*In_bandwith Out_bandwith* [**perpir-update**]] [**force**]

【参数说明】 *Src_name*：拷贝的源流控组，即作为模板的流控组名字。

Dst_name：新创建的流控组名字，不允许与 *Src_name 相同*。

In_bandwith：期望更新的下行带宽大小，输入范围：500~ 10000000，单位：kbps，不输入默认取源配置组下行带宽大小。

Out_bandwith：期望更新的上行带宽大小，输入范围：500~ 10000000，单位：kbps，不输入默认取源配置组上行带宽大小。

perpir-update：输入则 Per-PIR 始终随带宽等比例调整，不输入情况下当带宽大于基准带宽 10M 时不等比例调整。

force：如果目标流控组已经存在，不输入 force 则会拷贝失败，而输入 force 则会先删除存在的流控组再开始拷贝

【命令模式】 全局模式

【使用指导】 -

创建流控组

【命令格式】 **flow-control** { *name* [**update bandwith**_*In_bandwith Out_bandwith* [**perpir-update**]] }

【参数说明】 *name*：流量控制组的名称。

In_bandwith：期望更新的下行带宽大小。

*Out_bandwith：*期望更新的上行带宽大小。

创建流控组，只需要执行 **flow-control {***name***}**即可

【命令模式】 Flow-control 模式

【使用指导】 -

创建流控树

【命令格式】 **channel-tree** { **inbound | outbound** }

【参数说明】 **inbound**：下行流控树。

outbound：上行流控树

【命令模式】 特权模式

【使用指导】 -

创建流控通道

【命令格式】 **channel-group** *name* **parent** { **NULL** | *parent_name*} [**cir** *cir_num*] **pir** *pir_num* [**pri** *pri_num*] [ ] { **fifo** | { **per-net** [**per-mask** *mask*] | **per-user** } **per-pir** *ppir_num* [**limit** *limit_num*] [**session-limit** *session_limit_num*] [**reverse**] }

【参数说明】 *name*：流量控制组的名称。

parent：创建通道的父通道。

NULL：不存在父通道，则创建通道为流控树的根通道。

*parent_name：*创建通道的父通道名字，必须为已经创建的通道

cir *cir_num：*承认信息速率，即保证的最小带宽，输入范围为 100～10000000，单位：kbps，不输入默认为 0，带宽紧张时不承诺分配带宽。

pir *pir_num：*峰值信息速率，即最大可以占用带宽，必须大于等于 **cir**，超出 **cir** 的部分为向父通道借用的带宽大小，输入范围为 100～10000000，单位：kbps。

pri *pri_num：*优先级，输入范围 0～7，0 优先级最高，高优先级的通道会优先得到调度。

fifo：先进先出队列。

per-net: 每网段公平队列，内部队列个数不定，基于网段实现公平的发包机会，适用于拥塞的通道，其还需要配置如下参数.

per-mask *mask:* 网段掩码，输入范围 1～32，32 时即基于每 IP 公平，不输入默认为 32.

per-user: 每帐号公平队列，内部队列个数不定，基于帐号实现公平的发包机会，适用于拥塞的通道。

per-pir *ppir_num：*每个网段的峰值信息速率，即最大可以占用带宽，输入范围为 1～10000000，单位：kbps。

limit *limit_num* .限制网段的个数，输入范围 1～65535，不输入则根据总带宽大小取默认值，总带宽小于 100M 则取 1000，总带宽大于等于 100M 则取 10000。

session-limit *session_limit_num：*用于限制每个网段(IP)的连接数目，输入范围 1～65535，默认不限制每个 IP 的连接数目。

pool *pool_name：*配置流控通道加入共享池的名字，NPE 产品不支持，其它 EG、NBR、AG 等网关设备支持。

reverse：(可选)反向 Per-net，针对外网网段(IP)进行限速，VPN 场景下针对接入分支机构公网网段(IP)限速，默认为正向 Per-net。

【命令模式】 **channel-tree** 配置模式

【使用指导】 -

创建流控策略

【命令格式】 **flow-rule** *num* [**vlan-group** *vlan-group-name*] [**subscriber** *subscriber-name*] [**auth-group** *auth-group-name*] [**network-group** *network-group-name*] [**app-group** *app-group-name*] **time-range** *time-rang-name* [**vpn**]

flow-rule *num* **action** {**drop** | **log-drop** | **pass** [**in-channel** *in-channel-name*] [**out-channel** *out-channel-name*] } [**default**] [**commet** *string*]

【参数说明】 num：流控策略规则的编号，输入范围 1～8192。

vlan-group-name：策略规则关联的 vlan-group 对象的名称，any 表示匹配任何对象。

subscriber-name：策略规则关联的 subscriber 对象的名称，any 表示匹配任何对象。

auth-group-name：策略规则关联的认证对象名称，any 表示匹配任何认证对象。

network-group-name：策略规则关联的 network-group 对象的名称，any 表示匹配任何对象。

app-group-name：策略规则关联的 app-group 对象的名称，any 表示匹配任何对象。

time-rang-name：策略规则关联的 time-rang 对象的名称。

in-channel-name：策略规则关联的 in-channel 通道的名称。

out-channel-name：策略规则关联的 out-channel 通道的名称。

string：策略规则的注释。

Disable：禁用该策略规则，缺省是非禁用的。

Vpn：配置 VPN 策略，只匹配 VPDN 流量，缺省是非 VPN 策略。

Default：默认策略，优先级最低，默认策略之间基于越细越优先生效原则。

【命令模式】 flow-control 模式

【使用指导】 配置一条流控策略规则，需要分成两部分进行配置，前半部分表示策略规则的关键字，后半部分表示策略规则的动作

在接口上启用流控

【命令格式】 **flow-policy** *name*

【参数说明】 *name*：流量控制组的名称。

【命令模式】 接口配置模式

【使用指导】 -

显示流控策略规则的详细信息

【命令格式】 **show flow-control-policy rule** [**group** *name*]

【参数说明】 *name*：流量控制组的名称。

【命令模式】 特权模式

【使用指导】 -

查看通道的速率

【命令格式】 **show flow-control** *Name* [**inbound | outbound**] **auto-pir**

【参数说明】 *Name*：流控组的名字

【命令模式】 特权模式

【使用指导】 -

配置举例

使用模版配置基于应用的流控

【网络环境】 某网吧业务需求：出口带宽为 100M。需要保证网页、游戏等关键应用，对于 P2P 视频要求不高。

【配置方法】
- 根据网吧模版拷贝流控组
- 将拷贝得到的流控组应用到接口

```
Ruijie(config)#flow-template copy tpl-ibar Gi0/1 bandwith 100000 100000
Ruijie(config)#int Gi0/1
Ruijie(config-if-GigabitEthernet 0/1)#flow-policy Gi0/1
```

【检验方法】 使用一下两条命令进行检查：
- show flow-control-policy rule Gi0/1。可以查看策略是否生效。
- show flow-control Gi0/1 auto-pir。可以查看通道速率是否正常。

配置基于用户的流控

【网络环境】 某公司网络出口带宽为 10M。公司内部划分 3 个部门：department1、department 2 和 department 3，网段分别为：192.168.1.0/24、192.168.2.0/24 和 192.168.3.0/24，分别分配带宽 5M、3M 和 2M。

【配置方法】
- 根据实际需求，分别创建上行和下行的流控通道树
- 配置应用识别相关配置，识别出各个部门的流量
- 配置流控策略，决定各个部门流量入对应的流控通道
- 应用流控组到 Wan 口

1） 配置流控组和流控通道树

```
Ruijie# configure terminal
# 创建流控组
Ruijie(config)# flow-control Corp
# 创建下行方向流控树
Ruijie(config-flow-control)# channel-tree inbound
Ruijie(config-channel-tree)# channel-group root parent null cir 10000 pir 10000 pri 4 fifo
Ruijie(config-channel-tree)# channel-group department1 parent root cir 5000 pir 10000 pri 4 fifo
Ruijie(config-channel-tree)# channel-group department2 parent root cir 3000 pir 10000 pri 4 fifo
Ruijie(config-channel-tree)# channel-group department3 parent root cir 2000 pir 10000 pri 4 fifo
Ruijie(config-channel-tree)# exit
# 创建上行方向流控树
Ruijie(config-flow-control)# channel-tree outbound
Ruijie(config-channel-tree)# channel-group root parent null cir 10000 pir 10000 pri 4 fifo
Ruijie(config-channel-tree)# channel-group department1 parent root cir 5000 pir 10000 pri 4 fifo
Ruijie(config-channel-tree)# channel-group department2 parent root cir 3000 pir 10000 pri 4 fifo
Ruijie(config-channel-tree)# channel-group department3 parent root cir 2000 pir 10000 pri 4 fifo
Ruijie(config-channel-tree)# exit
```

```
Ruijie(config-flow-control)# exit
```

B

2） 配置二三层对象识别

```
Ruijie# configure terminal
# 使能二三层对象功能
Ruijie(config)# layer23 classify enable
# 部门识别的配置
Ruijie(config)# subscriber static name department1 parent / ip-subnet 192.168.1.0 255.255.255.0
Ruijie(config)# subscriber static name department2 parent / ip-subnet 192.168.2.0 255.255.255.0
Ruijie(config)# subscriber static name department3 parent / ip-subnet 192.168.3.0 255.255.255.0
# 时间对象不支持 any 关键字，显示定义 any 内容
Ruijie(config)# time-range any
Ruijie(config-time-range)# periodic Daily 0:00 to 23:59
```

C

3） 配置流控策略

```
Ruijie# configure terminal
Ruijie(config)# flow-control Corp
# 部门 1、2、3 分别入流控通道 department1、department2 和 department3
Ruijie(config-flow-control)# flow-rule 1 vlan-group any subscriber department1 network-group any app-group any time-rang any
Ruijie(config-flow-control)# flow-rule 1 action pass in-channel department1 out-channel department1
Ruijie(config-flow-control)# flow-rule 2 vlan-group any subscriber department2 network-group any app-group any time-rang any
Ruijie(config-flow-control)# flow-rule 2 action pass in-channel department2 out-channel department2
Ruijie(config-flow-control)# flow-rule 3 vlan-group any subscriber department3 network-group any app-group any time-rang any
Ruijie(config-flow-control)# flow-rule 3 action pass in-channel department3 out-channel department3
```

D

4） 应用流控组到接口

```
Ruijie# configure terminal
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# flow-policy Corp
```

【检验方法】 使用一下两条命令进行检查：

- **show flow-control-policy rule** *Corp*。可以查看策略是否生效。
- **show flow-control** *Corp* **auto-pir**。可以查看通道速率是否正常。

常见错误

- 一条流量控制策略规则包括关键字和行为部分，两部分都配置才是一条完整的规则，不允许在关键字部分没有配置的情况下就配置行为部分。为了使得配置的策略生效，请先配置好策略规则关联的各个对象。

6.4.2 配置 auto-pir

配置效果

- 通过配置 auto-pir，可以在带宽用满时，关键流量还可以快速抢占带宽。

注意事项

无

配置方法

- 在 channel-tree 模式下开启或者关闭 auto-pir。

检验方法

可以通过命令查看 auto-pir 的详细信息，包括是否开启，阀值大小等。该命令是：**show flow-control** *Name* **auto-pir**

相关命令

↘ 配置 auto-pir

【命令格式】 **auto-pir enable** [**interval** *NUM* [**root-rate** *Percentage*]] [**exclude-pass**]

【参数说明】 *NUM*：调整间隔，单位：秒，不配置默认为 1 秒，配置范围为 1～3600。

Percentage：PIR 压制或恢复的阀值。

exclude-pass：**root-rate** 阀值计算默认包括放行流量，输入 **exclude-pass** 关键字后不包括 pass 流量。

【命令模式】 **channel-tree** 配置模式

【使用指导】 适用于存在上一级流控设备的场景，如果点到点流量占用带宽居高不下，而其它应用带宽得不到保证时，可以使能该功能。

这里计算的根带宽利用率为实际利用率，包括流量控制转发和丢弃的流量。

↘ 查看 auto-pir 信息

【命令格式】 **show flow-control** *Name* [**inbound** | **outbound**] **auto-pir**

【参数说明】 *Name*：流控组的名字

【命令模式】 特权模式

【使用指导】 -

配置举例

↘ 使能流控组 group1 下行 auto-pir 功能

【配置方法】
- 配置流控基本功能。略
- 使能策略组 group1 的 inbound 通道树 PIR 调节功能

```
Ruijie(config)# config
Ruijie(config)# flow-control group1
Ruijie(config-flow-control)# channel-tree inbound
Ruijie(config-channel-tree)# auto-pir enable
```

【检验方法】 使用 show flow-control *group1* auto-pir 可以 auto-pir 是否生效

常见配置错误

无

6.4.3 配置共享池限速

配置效果

- 共享池允许流控通道加入，通过影响加入通道的发包调度，从而实现更加灵活的流量控制。

注意事项

- NPE 产品不支持共享池功能，其它 EG、NBR、AG 等网关设备支持

配置方法

- 在 channel-tree 模式下，将指定的通道加入共享池。

检验方法

可以通过命令查看共享池的配置信息。该命令是：**show flow-control** *Name* { **inbound** | **outbound** } [**share-pool** [*pool-name*]]

相关命令

↘ 创建共享池

【命令格式】 **share-pool** *Name* **rate** *num1* [**type** { **normal** | **per-ip** [**limit** *num2***l** }]

【参数说明】 *Name*：共享池名字。

num1：创建共享池带宽。

type：创建共享池类型，不输入默认为 **normal** 类型

normal：normal 类型，针对所有用户总带宽限速。

per-ip：per-ip 类型，针对每用户带宽限速。

num2： **per-ip** 类型共享池的用户数限制

【命令模式】 **channel-tree** 配置模式

【使用指导】 1、Normal 类型共享池基于加入共享池通道的所有用户限制带宽，即所有用户带宽不能超过配置的 Rate；

2、Per-IP 类型共享池基于加入共享池通道的每个用户限制带宽，即每个用户带宽不能超过配置的 Rate。

3、如果超出 Per-IP 类型共享池 Limit 限制的用户，流量将会被截断。Limit 不输入情况下会自动生成一个 Limit 值；

4、加入共享池通道之间优先级不同，最坏情况下高优先级的通道会强占共享池所有带宽，可以用于不同业务需要区分优先级的场景；

↘ 通道加入共享池

【命令格式】 **channel-group** *name* **parent** { **NULL** | *parent_name* } [**cir** *cir_num*] **pir** *pir_num* [**pri** *pri_num*] [ ] { **fifo** | { **per-net** [**per-mask** *mask*] | **per-user** } **per-pir** *ppir_num* [**limit** *limit_num*] [**session-limit** *session_limit_num*] [**reverse**] }

【参数说明】 -

【命令模式】 **channel-tree** 配置模式

【使用指导】 -

配置举例

↘ 在流量控制组 group1 的 inbound 流控树下，创建 Normal 类型、带宽为 1000kbps 的共享池 *test*：

【配置方法】

- 配置共享池举例

```
Ruijie#config
Ruijie(config)#flow-control group1
Ruijie(config-flow-control)# channel-tree inbound
Ruijie(config-channel-tree)# share-pool test rate 1000 type normal
```

【检验方法】 使用 **show flow-control** *group1***inbound share-pool** *test* 查看共享池的配置。

常见配置错误

无

6.5 监视与维护

清除各类信息

无

查看运行情况

作用	命令
显示当前设备中 ,流量控制组的详细信息。	**show flow-control-policy group**
显示流控策略规则的详细信息	**show flow-control-policy rule** [**group** *name*]
查看指定流控组的流量信息	**show flow-control** *Name* [**inbound** | **outbound**] **auto-pir**
显示流控组配置信息 ,不指定流控组则显示所有流控组配置	**show flow-control** [*Name*]
显示流控通道的配置信息	**show flow-control** *Name* { **inbound** | **outbound** } [**channel-group** *channel-name* [**detail**]]
显示共享池的配置信息	**show flow-control** *Name* { **inbound** | **outbound** } [**share-pool** [*pool-name*]]

查看调试信息

无

7 FLOW-AUDIT

7.1 概述

流量监控就是监控网络用户上网行为的一种基本方法，通过流量监控可以使用户网络应用透明化。通过流量监控，网络管理人员能观察到 IP 会话数，IP 在线时长，IP 应用上网时长，某个用户的流量，某个应用的流量，某个用户的应用流量，某个应用组的流量，某个应用类型的流量，以及用户组的流量。在出口网关设备上，可以使用流量审计功能查看上述各种类型的流量信息。

7.2 典型应用

典型应用	场景描述
出口网关部署	出口网关设备部署流量监控审计

7.2.1 出口网关部署

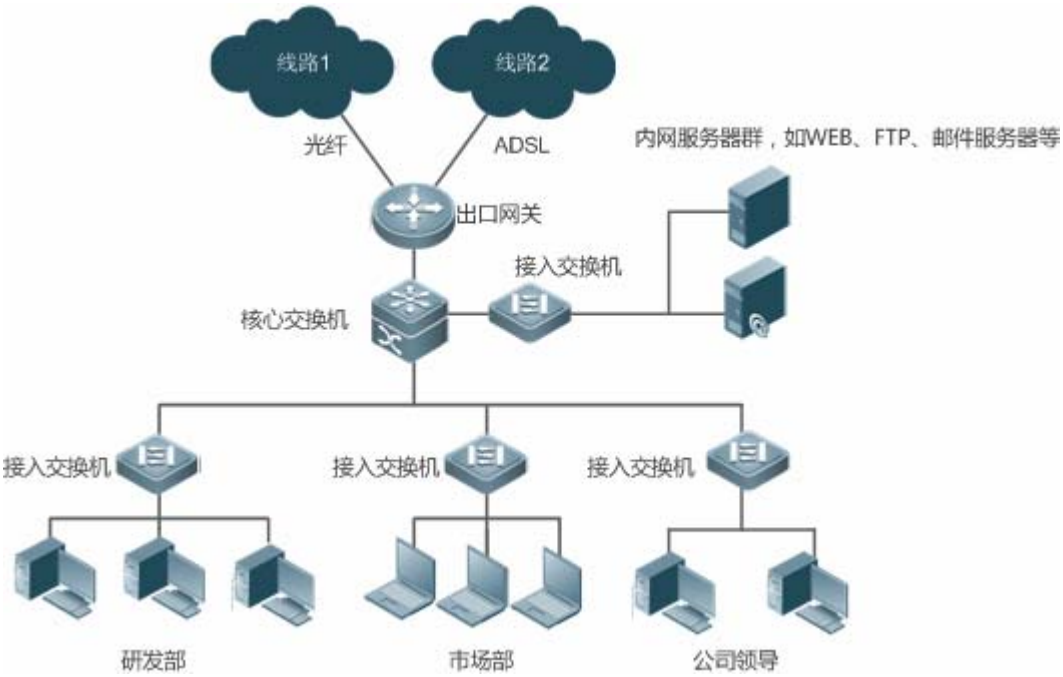
应用场景

流量监控审计对拓扑没有明确的限制，以下只是罗列企业用户的典型拓扑。

依赖流量审计的功能有：

- 应用识别功能

图 7-1 出口网关企业用户典型的应用场景



【注释】 企业内部通常都会部署各种服务器，如 WEB 服务器、FTP 服务器、邮件服务器等等。内部通常都会划分为很多部门，如研发部、市场部、公司领导等，有大量的网络应用通过网关设备连接互联网，如网页浏览、邮件等等。

功能部属

- 基本 NAT 上网功能：完成基本的 NAT 地址转换，保障用户正常上网。
- 应用识别功能：完成转发流量的应用识别。
- 流量控制功能：和应用识别结合，实现对重点应用流量的保障等功能。
- 二三层识别功能：完成转发流量的用户、用户组识别。
- 多链路负载均衡功能：完成数据流在多条链路的合理分配，确保多条链路的带宽利用合理。
- 流量审计功能：流量审计即是对流经网关设备的各种流量进行统计，有基于用户的流量统计，也有基于应用的流量统计等等，从而使得网络的流量可视化。

7.3 功能详解

基本概念

↘ 通路

网桥模式下，一对网桥对应一个通路。网关模式下，一个 WAN 口对应一个通路。

↘ 应用明细

应用下面的子类，如应用“腾讯 QQ”下的明细“QQ 文件传输”

应用类型

为关键应用、抑制应用等

应用组

如“即时通讯软件”

用户组

用户树级结构中是“root/1 级用户组/2 级用户组/3 级用户组/用户”

功能特性

功能特性	作用
流量监控审计	开启流量审计。

7.3.1 流量监控审计

流量审计是对流经网关设备的各种流量进行统计，有基于用户的流量统计，也有基于应用的流量统计等等，从而使得网络的流量可视化。

工作原理

流量监控审计基本原理是通过累计转发面获取的报文数和报文长度来实现统计，报文基于通路，IP，IP 应用，用户组，应用明细，应用组，应用类型，接口，VWAN 分别进行统计，并定时存储到数据库。

相关配置

开启流量监控审计功能

缺省情况下，流量监控审计功能是开启的。

在全局配置模式中，使用 **flow-audit enable** 命令可以开启流量监控审计功能开关。

在全局配置模式中，使用 **no flow-audit enable** 命令可以关闭流量监控审计功能开关。

配置 VPN 流量监控方式

缺省情况下，VPN 的流量监控都是基于外网 IP 的。

使用 flow-audit vpn {inside-ip | outside-ip} 可以调整控方式，inside-ip 表示基于内网 IP 进行监控，outside-ip 表示基于外网 IP 进行监控.。

如果要恢复默认配置，则通过执行命令 flow-audit vpn outside-ip 即可。

7.4 产品说明



NBR2500D-E、NBR3000D-E、NBR3000D-UE 带硬盘设备支持审计记录在本地 ,支持历史流量审计； NBR108G-P 、NBR800G、NBR950G、NBR1500G、NBR2000G、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E 不支持本地记录，不支持历史流量审计；NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 带硬盘时支持本地记录、支持历史流量审计，默认不带硬盘时不支持。

7.5 配置详解

配置项	配置建议 & 相关命令	
开启关闭流量监控审计功能	⚠ 必须配置。打开流量审计功能。	
	flow-audit enable	开启流量监控审计。
配置历史数据保留天数	⚠ 可选配置。配置历史数据保存的天数。	
	flow-audit data-store *num*	配置流量监控审计除天表、周表、月表外其它信息表数据保留天数。
	flow-audit data-store day-report *num*	配置天表历史数据保留天数。
	flow-audit data-store week-report *num*	配置周表历史数据保留天数。
	flow-audit data-store month-report *num*	配置月表历史数据保留天数。
配置报表预生成时间	⚠ 可选配置。配置报表预生成时间 （修改系统时间，会导致异常）。	
	flow-audit generate-report *hour*	配置历史报表预生成的时间点,其中配置的时间为 24 小时制的。
配置硬盘配额	⚠ 可选配置。配置流量审计可以使用硬盘的配额。	
	flow-audit hard-disk-quota *percent*	配置流量监控的硬盘配额，其中参数 percent 为总硬盘容量的百分比，取值范围为 1~100。
配置 VPN 监控方式	⚠ 可选配置。配置 VPN 监控的方式 。	
	flow-audit vpn {inside-ip | outside-ip}	配置 VPN 流量的监控方式，inside-ip 表示基于内网 IP 进行监控 ,outside-ip 表示基于外网 IP 进行监控.。

7.5.1 开启关闭流量监控审计功能

配置效果

- 打开流量审计功能，能够对流经网关设备的各种流量进行统计，并能呈现各种流量信息。

注意事项

- 流量监控审计开关关闭的情况下，功能失效。
- 流量监控审计依赖于应用识别和二三层识别，应用识别和二三层开关关闭时，审计就无法基于应用和用户进行流量统计。

配置方法

- 全局模式下，通过命令开启流量监控审计。

检验方法

- 检查流量监控审计状态。

相关命令

↘ 开启流量监控审计

【命令格式】 **flow-audit enable**
【参数说明】 -
【命令模式】 全局模式
【使用指导】 -

配置举例

↘ 开启流量监控审计

【配置方法】 在出口网关设备上配置。

```
Ruijie# configure terminal
Ruijie(config)#flow-audit enable
```

【检验方法】
- 查看流量监控审计的状态。

```
Ruijie#show run | in flow-audit
flow-audit enable
```

常见错误

无

7.5.2 配置历史数据保留天数

配置效果

- 配置历史数据保留的天数，超过了时间，相关的数据就会被删除。

注意事项

- 是可选的配置。
- 系统从 10.x 升级到模块化时，数据信息会全部丢失。
- 流量信息是根据采样的时间内的总流量， 小时表为 5 分钟采集一次，天表为半小时采集一次，周表的采集粒度为 2 小时，月表的采集粒度为 8 小时。
- 流量监控审计开关关闭的情况下，功能失效，过期的数据也不会被删除。
- 配置流量监控审计除天表、周表、月表外其它信息表数据保留天数范围为 10-90，缺省为 60，单位为天。
- 配置天表历史数据保留天数范围为 10-90，缺省为 60，单位为天。
- 配置周表历史数据保留周数范围为 1-52， 缺省为 8，单位来周。
- 配置月表历史数据保留月数范围为 1-12，缺省为 12，单位为月。

配置方法

- 全局模式下，通过命令配置各个历史数据的保留天数。

检验方法

- 检查各个历史数据的保留天数。

相关命令

↘ 配置流量监控审计除天表、周表、月表外其它信息表数据保留天数

【命令格式】 **flow-audit data-store** *num*
【参数说明】 num: 历史数据保留天数，取值范围为 10~90 天
【命令模式】 全局模式
【使用指导】 -

↘ 配置天表历史数据保留天数

【命令格式】 **flow-audit data-store day-report** *num*
【参数说明】 num: 历史数据保留天数，取值范围为 10~90 天

【命令模式】 全局模式
【使用指导】 -

配置周表历史数据保留天数

【命令格式】 **flow-audit data-store week-report** *num*
【参数说明】 num: 历史数据保留天数，取值范围为 1~52 周
【命令模式】 全局模式
【使用指导】 -

配置月表历史数据保留天数

【命令格式】 **flow-audit data-store month-report** *num*
【参数说明】 num: 历史数据保留天数，取值范围为 1~12 个月
【命令模式】 全局模式
【使用指导】 -

配置举例

修改除天表、周表、月表外其它信息表数据保留天数为 12 天

【配置方法】 在出口网关设备上配置。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# flow-audit data-store 12
```

【检验方法】
- 查看配置的信息。

```
Ruijie#show run | in flow-audit
flow-audit enable
flow-audit data-store 12
```

修改天表历史数据保留天数为 12 天

【配置方法】 在出口网关设备上配置。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# flow-audit data-store day-report 12
```

【检验方法】
- 查看配置的信息。

```
Ruijie#show run | in flow-audit
flow-audit enable
flow-audit data-store day-report 12
```

修改周表历史数据保留周数为 12 周

【配置方法】 在出口网关设备上配置。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# flow-audit data-store week-report 12
```

【检验方法】

- 查看配置的信息。

```
Ruijie#show run | in flow-audit
flow-audit enable
flow-audit data-store week-report 12
```

↘ 修改月表历史数据保留月数为 8 个月

【配置方法】 在出口网关设备上配置。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# flow-audit data-store month-report 8
```

【检验方法】

- 查看配置的信息。

```
Ruijie#show run | in flow-audit
flow-audit enable
flow-audit data-store month-report 8
```

常见错误

无

7.5.3 配置报表预生成时间

配置效果

- 会在指定的时间会有历史报表预生成。

注意事项

- 流量监控审计开关关闭的情况下，功能失效，到了时间也不会有报表生成。

配置方法

- 全局模式下，通过命令配置报表预生成时间。

检验方法

- 检查报表预生成时间。

相关命令

配置报表预生成时间

【命令格式】 **flow-audit generate-report** *hour*

【参数说明】 *hour*： 历史报表预生成的时间点，为 24 小时制的

【命令模式】 全局模式

【使用指导】 -

配置举例

配置日报表/周报表/月报表预生成的时间点为 12 点

【配置方法】 在出口网关设备上配置。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# flow-audit generate-report 12
```

【检验方法】

- 查看报表预生成时间。

```
Ruijie#show run | in flow-audit
flow-audit enable
flow-audit generate-report 12
```

常见错误

无

7.5.4 配置流量监控的硬盘配额

配置效果

- 指定流量监控审计允许使用的硬盘配额

注意事项

- 缺省情况下，流量监控允许使用的硬盘配额为硬盘总容量的 50%，可以根据实际情况进行调整，范围为 1-100。
- 当流量监控所使用的硬盘空间超出配额后，设备将会自动删除流量监控最老的数据以腾出硬盘空间。

配置方法

- 全局模式下，通过命令配置流量监控的硬盘配额。

检验方法

- 检查报流量监控的硬盘配额。

相关命令

↘ 配置流量监控的硬盘配额

【命令格式】 **flow-audit hard-disk-quota** *percent*

【参数说明】 *percent*： 流量监控的硬盘配额，为总硬盘容量的百分比，取值范围为 1~100。

【命令模式】 全局模式

【使用指导】 -

配置举例

↘ 将硬盘的配额调整为 80%

【配置方法】 在出口网关设备上配置。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# flow-audit hard-disk-quota 80
```

【检验方法】

- 查看硬盘配额的配置。

```
Ruijie#show run | in flow-audit
flow-audit enable
flow-audit hard-disk-quota 80
```

常见错误

无

7.5.5 配置 VPN 监控方式

配置效果

- 可以根据自己的审计需求，指定 VPN 的流量监控方式，即基于外网 IP 或内网的 IP。

注意事项

- 缺省情况下，VPN 的流量监控都是基于外网 IP 的

检验方法

- 检查 VPN 的流量监控方式。

相关命令

配置流量监控的 VPN 监控方式

【命令格式】 **flow-audit vpn { inside-ip | outside-ip }**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 -

配置举例

公司总部作为 VPN 服务端，希望查看各个分支机构（通过 VPN 拨号上来的）IP 的流量情况

【配置方法】 在出口网关设备上配置。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# flow-audit vpn outside-ip
```

【检验方法】

- 查看 VPN 监控方式。

```
Ruijie#show run | in flow-audit
flow-audit enable
flow-audit flow-audit vpn outside-ip
```

分公司作为 VPN 客户端，希望看到分公司内部每个员工访问 VPN 资源的流量情况，则需要修改为基于内网 IP 进行监控

【配置方法】 在出口网关设备上配置。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# flow-audit vpn inside-ip
```

【检验方法】

- 查看 VPN 监控方式。

```
Ruijie#show run | in flow-audit
flow-audit enable
flow-audit vpn inside-ip
```

常见错误

无

7.6 监视与维护

清除各类信息

无

查看运行情况

作用	命令
显示整机当前，最近 hour 小时内或指定时间段的在线 IP 数。	**show online statistics** { **global** | **interface** *interface-name* } [{ **detail** [**offset** *start-record* { **limit** *record-num* }] **| recent** *hour* | **minute interval** *begin-year begin-month begin-day begin-hour:begin-minute* **to** *end-year end-month end-day end-hour:end-minute* | [**month | week**] **time-interval** *begin-year begin-month begin-day begin-hour* **to** *end-year end-month end-day end-hour* | **day** *begin-year begin-month begin-day* [**hour-interval** *begin-hour1* **to** *end-hour1* [*begin-hour2* **to** *end-hour2*]] }]
显示整机或指定通路下当前在线 IP 的上网时长、流量信息及指定时间段的 IP 上网时长的信息。	**show online ip** { **global** | **interface** *interface-name*} [[**subscriber** *subscriber-name*] [**subscriber-group** *subscriber-group*] [**vip**] | { **by-auth** } **[auth-subs-group** *auth-group-name* **] [auth-subs** *auth-name* **]]]** [**ip** *ip-address*] [{ **minute-interval** *begin-year begin-month begin-day begin-hour: begin-minute* **to** *end-year end-month end-day end-hour:end-minute* | { [**month** | **week**] **day-interval** *begin-year begin-month begin-day* **to** *end-year end-month end-day* | **day** *begin-year begin-month begin-day* } [**hour-interva** l *begin-hour* **to** *end-hour* [*begin-hour2* **to** *end-hour2* **]] }]** [**order-by** { { **pass** | **drop** } { **upload** | **download** } | **ip** | **subscriber-group** | **subscriber** | **auth-subs-group** | **auth-subs** } { **desc** | **asc** } [**top** n]]
显示整机或指定通路下当前在线 IP、应用的上网时长、流量信息。	**show online ip-application** { **global** | **interface** *interface-name* } [[**subscriber** *subscriber-name*] [**subscriber-group** *subscriber-group*] [**vip**] | { **by-auth** } **[auth-subs-group** *auth-group-name* **] [auth-subs** *auth-name* **]]** [**ip** *ip-address*] [**application** *application-name*] [**application-group** *application-group*] [**application-type** *application-type*] [**order-by** { { **pass** | **drop** } { **upload** | **download** } | **ip** | **subscriber-group** | **subscriber** | **auth-subs-group | auth-subs** | **application** } { **desc** | **asc** }] [**offset** *start –record* { **limit** record-num }]
显示整机或指定接口某个时间段内或最近几小时内或当前的流量信息	**show flowrate** { **global** | **interface** *interface-name* } [{ **recent** *hour* | **minute_interval** *begin-year begin-month begin-day begin-hour:begin-minute* **to** *end-year end-month end-day end-hour:end-minute* | [**month** | **week**] **time-interval** *begin-year begin-month begin-day begin-hour* **to** *end-year end-month end-day end-hour* | { [**month | week**] **day-interval** *begin-year begin-month begin-day* **to** *end-year end-month end-day* | **day** *begin-year begin-month begin-day* } [**hour-interval** *begin-hour* **to** *end-hour* [*begin-hour2* **to** *end-hour2*]] } [**detail**]]

显示整机或指定通路下指定时间段或最近几个小时的用户流量统计信息 ,或当前的用户流量统计信息	**show flowrate ip** { **global** | { **interface** *interface-name*} [**by-vpn**] | **vwan** } [**subscriber-group** *subscriber-group* **by-group** | [[**subscriber-group** *subscriber-group*] [**subscriber** *subscriber-name*] [**vip**] | { **by-auth** } [**auth-subs-group** *auth-group-name*] [**auth-subs** *auth-name*]] [**ip** *ip-address*] [**application** *application-name*] [**application-group** *application-group*] [**application-type** *application-type*]] [{ **recent** *hour* | **minute-interval** *begin-year begin-month begin-day begin-hour:begin-minute* **to** *end-year end-month end-day end-hour: end-minute* | { [**month** | **week**] **day-interval** *begin-year begin-month begin-day* **to** *end-year end-month end-day* | **day** *begin-year begin-month begin-day* } [**hour-interval** *begin-hour1* **to** *end-hour1* [*begin-hour2* **to** *end-hour2*]] }] [**order-by** { { **pass** | **drop** } { **upload** | **download** } | **ip** | **subscriber-group** | **subscriber** | **auth-subs-group** | **auth-subs** } { **desc** | **asc** } [**top** *n* [**detail**]]] [{ **detail** | **by-user** }]
显示整机或指定通路下当前或者时间段内应用、应用组、应用类型相关的流量信息	**show flowrate application** { **global** | **interface** *interface-name* | **vwan** } [[**subscriber** *subscriber-name*] [**subscriber-group** *subscriber-group*] | { **by-auth** } [**auth-subs-group** *auth-group-name*] [**auth-subs** *auth-name*]] [**ip** *ip-address*] [**application-group** *application-group*] [{ [**by-group**] | [**application-type** *application-type*] [{ **by-type** | **application** *application-name* }] }] [{ **recent** *hour* | **minute-interval** *begin-year begin-month begin-day begin-hour:begin-minute* **to** *end-year end-month end-day end-hour:end-minute* | { [**month** | **week**] **day-interval** *begin-year begin-month begin-day* **to** *end-year end-month end-day* | **day** *begin-year begin-month begin-day* } [**hour-interval** *begin-hour1* **to** *end-hour1* [*begin-hour2* **to** *end-hour2*] }] [**order-by** { { **pass** | **drop** } { **upload** | **download** } | **application** } { **desc** | **asc** } [**top** *n*]] [**detail**]
显示整机或指定通路下当前 IP、应用流量信息	**show flowrate ip-application** { **global** | { **interface** *interface-name* } [**by-vpn**] } [[**subscriber** *subscriber-name*] [**subscriber-group** *subscriber-group*] [**vip**] | { **by-auth** } [**auth-subs-group** *auth-group-name*] [**auth-subs** *auth-name*]] [**ip** *ip-address*] [**application** *application-name*] [**application-group** *application-group*] [**application-type** *application-type*] [**order-by** { { **pass** | **drop** } { **upload** | **download** } | **ip** | **application** | **subscriber-group** | **subscriber** | **auth-subs-group** | **auth-subs** } { **desc** | **asc** } [**top** *n*]]

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
开启预报生成时的 debug 信息。	**debug flow-audit flowrate-report**

8 CONTENT-AUDIT

8.1 概述

行为审计功能主要针对企业，学校等出口网络。主要是对内网用户的上网行为进行监督。避免出现工作时间使用聊天工具，上无关的网站，炒股或者玩游戏，上非法的 bbs 论坛，收发非法邮件的这些行为。

出口设备开启行为审计功能，能够防范信息机密外泄、保护组织信息资产安全；能够保证正常的上网行为，避免法律风险。

行为审计包括应用控制审计、URL 访问控制审计、即时通讯过滤审计、客户端邮件过滤审计、WEB 邮件过滤审计、论坛发帖行为过滤审计、搜索引擎关键词过滤审计、虚拟身份审计、外发信息过滤审计、外发文件过滤审计、QQ 聊天内容审计等十一个业务，其中 URL 访问控制审计支持 HTTPS 加密流的域名审计。

MSC 产品仅支持 URL 访问控制审计， NBR-E 全系列支持所有业务，其他无内置存储的网关产品和 ACE 系列产品支持应用控制审计、URL 访问控制审计、即时通讯过滤审计、URL 重定向四个业务，其他有内置存储的网关产品支持所有业务。

8.2 典型应用

典型应用	场景描述
行为审计典型应用场景	描述行为审计的基本场景及功能

8.2.1 行为审计典型应用场景

应用场景

行为审计主要包含如下场景：

- 应用控制审计：主要针对各种应用的网络行为进行监控，根据需要来放行或阻断相应的应用数据流，并对控制行为进行审计。
- URL 过滤审计：主要针对 URL 访问进行监控，对内网的 URL 访问进行分类和审计，并根据需要对相应的 URL 访问行为进行过滤。
- URL 重定向：即网页重定向，将用户的网络请求重新定向到其它位置，以满足用户的网络访问需求。
- IM 过滤审计：主要针对主流的 IM 聊天系统（如 QQ，MSN），对账号和聊天记录进行审计，并对账号进行过滤。
- MAIL 过滤审计：主要针对主流的邮件系统（如 Outlook，Foxmail）对邮件进行收发审计，信息过滤，有内置存储的设备还可以保存邮件的附件内容。
- PLUGIN 审计：主要用于审计 QQ 聊天内容，要求内网 PC 安装插件，无法对内容进行过滤。
- POST FILE 过滤审计：主要针对外发文件的行为进行管理和审计，防止内网文件泄密。
- POST 过滤审计：主要针对 HTTP POST 方式外发信息进行管理和审计，监管地方论坛等外发信息行为。

- WEB-MAIL 过滤审计：主要针对主流的 WEB 邮件系统（如新浪邮箱，网易邮箱，QQ 邮箱）对邮件进行发送审计，信息过滤。
- WEB-BBS 过滤审计：主要针对主流 WEB BBS 站点（如天涯社区，猫扑社区）和微博（如新浪微博、腾讯微博），对用户的发帖内容进行审计，并对用户的发帖内容进行过滤。
- WEB-SEARCH 过滤审计：主要针对主流 WEB 搜索引擎站点（如百度，谷歌），对用户的搜索行为进行审计，并对搜索引擎关键字进行过滤。
- 虚拟身份审计：主要针对主流的社交应用（如微信，微博），对账号 ID 和上下线行为进行审计。
- TELNET 过滤审计：针对 TELNET 协议，对 TELNET 数据流进行审计处理，审计的字段包括内网 IP、内网端口、服务器 IP、服务器端口、行为动作“连接 or 断开”。
- FTP 过滤审计：主要针对 FTP 传输协议，对上传、下载的文件名进行审计，对上传文件进行阻断或审计。

功能部属

用户可以按照如下方式定制行为审计策略：

- 用户可以定制一个策略组表示一组行为审计规则。
- 用户可以基于应用、内容、时间段定制策略组内的各项行为审计规则。
- 用户可以将策略组与静态用户、认证用户相关联，让行为审计策略生效。

8.3 功能详解

基本概念

URL 分类

根据网页内容，因特网上的 URL 可以划分为军事、新闻、体育等，目前系统已经自带了一定的 URL 分类库，用户还可以根据自己的需要对 URL 进行归类。

URL 对象

URL 对象包含了一组相关的 URL，用户可以通过正则表达式来表示 URL 对象所包含的 URL，也可以将 URL 分类（包括系统自带的 URL 分类以及用户自定义的 URL 分类）包含到该 URL 对象中。结合下文，您会发现 URL 对象实际上是作为一种 URL 访问控制的集合而使用的。

URL 分类与 URL 对象的区别：

1、URL 分类通常是根据网页的内容来进行划分的，它不能直接应用于 URL 访问控制规则。

2、URL 对象通常是为了 URL 规则而定义的一个集合，如“URL 白名单”，里面包含的 URL 条目可能并没有直接的联系。

关键字

关键字指用户所关注的上网行为中包含的短语或者词组。

↘ 内容对象

内容对象包含了一系列关键字及正则表达式。与 URL 对象相似，内容对象实际上是作为一种关键字的集合而使用的。

↘ 规则

设备对内网的网络访问行为如何做监控，是由一系列内容审计规则决定的，如应用控制规则、URL 规则、IM 规则、MAIL 规则、WEB-BBS 规则、WEB-MAIL 规则、WEB-SEARCH 规则。用户在对内网的网络访问行为进行监控前，需要先根据自己的需要，基于应用、内容、时间段等条件来配置相应的内容审计规则。

↘ 策略组

策略组是一系列规则的集合，一个策略组表示一组行为审计规则。用户可以将策略组与静态用户、认证用户相关联，让行为审计对相应的用户生效。

功能特性

功能特性	作用
应用控制审计	根据应用分类对用户上网行为进行审计、阻断
URL 审计	根据 URL 分类对用户的 URL 访问行为进行审计、阻断
URL 重定向	将用户的网络请求重新定向到其它位置，以满足用户的网络访问需求
IM 审计	对用户使用即时通讯的行为进行审计、阻断
MAIL 审计	对用户使用邮件客户端的邮件收发行为进行审计、阻断
WEB-BBS 审计	对用户的论坛发帖行为进行审计、阻断
WEB-MAIL 审计	对用户发送 WEB 邮件的行为进行审计、阻断
WEB-SEARCH 审计	对用户使用搜索引擎的行为进行审计、阻断
虚拟身份审计	对用户使用社交应用的行为进行审计
TELNET 审计	对 TELNET 客户端和服务端的的 IP、端口号、行为进行审计、阻断
FTP 审计	对用户使用 FTP 传输的文件名进行审计、阻断

8.3.1 应用控制审计

应用控制审计可以按照应用分类来对网络行为进行监控，根据配置的规则来放行或阻断指定用户的相应应用数据流，并对控制行为进行审计。

工作原理

应用控制审计根据应用识别的结果来对应用数据流进行监控。应用识别模块是出口设备中的基础功能模块，识别过程主要是分析数据流的报文载荷特征和报文流量特征，从而获知数据流的应用协议类型。

应用控制审计规则包含在策略组内，可指定对应用数据流的控制和审计方式。规则可以由表示生效时间段的时间对象、表示待控制应用类型的应用组名、放行还是阻断数据流、是否需要审计等条件自由组合实现，规则间存在优先级关系。

策略组也存在优先级关系，可以关联到静态用户和认证用户。应用控制审计根据策略组与规则的优先级来匹配最终生效的规则，对指定用户的上网行为进行监控和审计。

对于有内置存储的网关设备，审计记录保存在设备的本地存储上，可以通过相应的查询命令来查看应用控制审计记录的明细信息、统计信息。

当审计信息有发送到外面 log 服务器时，可以选择不记录到设备本地存储上，以减轻设备负担。

相关配置

↘ 配置应用控制审计规则

缺省情况下，无应用控制审计规则，应用控制审计功能自动关闭。

使用 **app-rule** 命令可以配置应用控制审计规则。配置有效规则后，应用控制审计功能自动开启。

配置规则的参数决定了应用控制审计对上网行为的监控和审计方式。

↘ 查看应用控制审计的审计信息

缺省情况下，审计记录在设备本地存储上的保存天数是 60 天。

使用 **show app-audit** 命令可以查询应用控制审计记录的明细信息、统计信息。

可通过指定所需的时间范围、过滤条件等配置参数来查询满足指定条件的审计记录信息。

当审计信息有发送到外面 log 服务器的时候，可以通过 **no content-audit write-db app-control** 关闭应用控制审计信息写本地存储的开关。

8.3.2 URL 审计

URL 审计主要针对 URL 访问进行监控，对内网的 URL 访问进行分类和审计，并根据需要对指定用户相应的 URL 访问行为进行过滤。

工作原理

URL 全称是 Uniform Resource Locator，即统一资源定位符，也被称为网页地址。根据网页内容，因特网上的 URL 可以划分为军事、新闻、体育等，目前系统已经自带了一套 URL 分类库，包含五十几个分类。用户还可以根据自己的需要对 URL 进行自定义分类。

URL 审计可以识别出数据流中 HTTP 头包含的 URL 信息，识别出来的 URL 按照系统 URL 分类和自定义 URL 分类进行匹配，确定出 URL 所属类别，再根据 URL 规则对该 URL 进行审计和过滤。

URL 审计还可以识别出 HTTPS 加密的网页数据流包含的域名信息，识别出来的域名按照系统 URL 分类和自定义 URL 分类进行匹配，确定出域名所属类别，再根据 URL 规则对该域名进行审计和过滤。

URL 审计规则包含在策略组内，可指定对 URL 访问的控制和审计方式。规则可以由表示生效时间段的时间对象、表示待控制 URL 分类的 URL 对象、放行还是阻断数据流、是否需要审计等条件自由组合实现，规则间存在优先级关系。

策略组也存在优先级关系，可以关联到静态用户和认证用户。URL 审计根据策略组与规则的优先级来匹配最终生效的规则，对指定用户的 URL 访问行为进行监控和审计。

对于有内置存储的网关设备，审计记录保存在设备的本地存储上，可以通过相应的查询命令来查看 URL 审计记录的明细信息、统计信息、站点排名信息。

当审计信息有发送到外面 log 服务器时，可以选择不记录到设备本地存储上，以减轻设备负担。

相关配置

↘ 配置 URL 审计规则

缺省情况下，无 URL 审计规则，URL 审计功能自动关闭。

使用 **url-rule** 命令可以配置 URL 审计规则。配置有效规则后，URL 审计功能自动开启。

配置规则的参数决定了 URL 审计对 URL 访问行为的监控和审计方式。

缺省情况下，URL 审计规则只对普通网页浏览有效，若要对 HTTPS 加密的数据流也生效，需同时开启 HTTPS 域名审计使能开关。HTTPS 域名审计使能开关缺省关闭。

↘ 查看 URL 审计的审计信息

缺省情况下，审计记录在设备本地存储上的保存天数是 60 天。

使用 **show url-audit** 命令可以查询 URL 审计记录的明细信息、统计信息、站点排名信息。普通网站审计记录和 HTTPS 加密网站记录是一致的，其中的 URL 信息以**错误！超链接引用无效。**前缀和 **错误！超链接引用无效。**前缀区分。

可通过指定所需的时间范围、过滤条件等配置参数来查询满足指定条件的审计记录信息。

当审计信息有发送到外面 log 服务器的时候，可以通过 **no content-audit write-db url** 关闭 url 审计信息写本地存储的开关。

8.3.3 URL 重定向

URL 重定向，即网页重定向，将用户的网络请求重新定向到其它位置，以满足用户的网络访问需求。

工作原理

URL 重定向可以识别出数据流中 HTTP 头包含的 URL 信息，根据 URL 重定向规则对该 URL 进行匹配，若有匹配中规则，则按照规则将用户的请求重定向到另一个网站。

URL 重定向规则包含在策略组内，可指定将某个网站 A 重定向到另一个网站 B，并可指定生效时间段，规则间存在优先级关系。

策略组可以关联到静态用户和认证用户，网吧版 NBR 产品还可以关联自定义用户组。策略组之间也存在优先级关系。

URL 重定向根据策略组与规则的优先级来匹配最终生效的规则，对指定用户的网站访问进行重定向。

相关配置

↘ 配置 URL 重定向规则

缺省情况下，无 URL 重定向规则，URL 重定向功能自动关闭。

使用 **url-redirect-rule** 命令可以配置 URL 重定向规则。配置有效规则后，URL 重定向功能自动开启。

配置规则的参数决定了 URL 重定向的用户对象和生效时间段。

8.3.4 IM 审计

IM 审计主要针对主流的 IM 聊天系统（目前支持 QQ，MSN），对账号和聊天记录进行审计，并对账号进行过滤。

工作原理

MSN 审计支持对账号和聊天记录进行审计。IM 审计可以识别出 MSN 数据流中包含的账号信息和聊天记录信息，并进行审计。通过对指定 MSN 账号数据流的阻断，能够实现账号过滤；通过对聊天记录信息进行关键字匹配，根据匹配结果阻断相应报文，能够实现聊天记录过滤。

QQ 审计支持对账号进行审计。QQ 聊天为加密信息，目前不支持内容过滤审计（配置命令中 QQ 规则的 message 不允许被配置）。QQ 审计可以识别出 PC 端 QQ 账号的上下线行为和移动终端 QQ 账号的在线行为，并进行审计。通过对指定 QQ 账号数据流的阻断，能够实现账号过滤。

IM 审计规则包含在策略组内，可指定对 IM 访问的控制和审计方式。规则可以由表示生效时间段的时间对象、待控制 IM 的类别、待控制 IM 的账号和关键字、放行还是阻断数据流、是否需要审计等条件自由组合实现，规则间存在优先级关系。

策略组也存在优先级关系，可以关联到静态用户和认证用户。IM 审计根据策略组与规则的优先级来匹配最终生效的规则，对指定用户的 IM 访问行为进行监控和审计。

对于有内置存储的网关设备，审计记录保存在设备的本地存储上，可以通过相应的查询命令来查看 IM 审计记录的明细信息、统计信息。

当审计信息有发送到外面 log 服务器时，可以选择不记录到设备本地存储上，以减轻设备负担。

相关配置

↘ 配置 IM 审计规则

缺省情况下，无 IM 审计规则，IM 审计功能自动关闭。

使用 **im-rule** 命令可以配置 IM 审计规则。配置有效规则后，IM 审计功能自动开启。

配置规则的参数决定了 IM 审计对 IM 访问行为的监控和审计方式。

↘ 查看 IM 审计的审计信息

缺省情况下，审计记录在设备本地存储上的保存天数是 60 天。

使用 **show im-audit** 命令可以查询 IM 审计记录的明细信息、统计信息、站点排名信息。

可通过指定所需的时间范围、过滤条件等配置参数来查询满足指定条件的审计记录信息。

当审计信息有发送到外面 log 服务器的时候，可以通过 **no content-audit write-db im** 关闭 im 审计信息写本地存储的开关。

8.3.5 MAIL 审计

MAIL 审计主要针对主流的邮件系统（如 Outlook，Foxmail）对邮件进行收发审计，信息过滤，并保存邮件的附件到本地存储。

工作原理

MAIL 审计的基本工作原理是对未加密的 SMTP 和 POP3 协议数据流进行解析，识别出数据流中相应的发件人、收件人、主题、正文、附件等信息，根据规则对信息进行关键字匹配和审计，放行或阻断相应数据流，从而实现对邮件进行收发审计和信息过滤。

MAIL 审计规则包含在策略组内，可指定对 MAIL 访问的控制和审计方式。规则可以由表示生效时间段的时间对象、MAIL 数据流的方向、表示关键字的内容对象、放行还是阻断数据流、是否需要审计等条件自由组合实现，规则间存在优先级关系。

策略组也存在优先级关系，可以关联到静态用户和认证用户。MAIL 审计根据策略组与规则的优先级来匹配最终生效的规则，对指定用户的 MAIL 访问行为进行监控和审计。

对于有内置存储的网关设备，审计记录保存在设备的本地存储上，可以通过相应的查询命令来查看 MAIL 审计记录的明细信息、统计信息、附件信息。

当审计信息有发送到外面 log 服务器时，可以选择不记录到设备本地存储上，以减轻设备负担。

相关配置

↘ 配置 MAIL 审计规则

缺省情况下，无 MAIL 审计规则，MAIL 审计功能自动关闭。

使用 **mail-rule** 命令可以配置 MAIL 审计规则。配置有效规则后，MAIL 审计功能自动开启。

配置规则的参数决定了 MAIL 审计对客户端邮件访问行为的监控和审计方式。

↘ 查看 MAIL 审计的审计信息

缺省情况下，审计记录在设备本地存储上的保存天数是 60 天。

使用 **show mail-audit** 命令可以查询 MAIL 审计记录的明细信息、统计信息、附件信息。

可通过指定所需的时间范围、过滤条件等配置参数来查询满足指定条件的审计记录信息。

当审计信息有发送到外面 log 服务器的时候，可以通过 **no content-audit write-db mail** 关闭 mail 审计信息写本地存储的开关。

8.3.6 WEB-BBS 审计

WEB-BBS 审计主要针对主流 WEB BBS 站点（如天涯社区，猫扑社区）和微博（如新浪微博、腾讯微博），对用户的发帖内容进行审计，并对用户的发帖内容进行过滤。

工作原理

WEB-BBS 审计的基本工作原理是对未加密的包含论坛发帖或发微博的 HTTP 数据流进行解析，识别出数据流中相应的主题和正文信息，根据规则对信息进行关键字匹配和审计，放行或阻断相应数据流，从而实现对用户的发帖内容进行审计和信息过滤。WEB-BBS 审计目前不支持移动终端的微博客户端（如新浪微博客户端、腾讯微博客户端）。

WEB-BBS 审计规则包含在策略组内，可指定对 WEB-BBS 访问的控制和审计方式。规则可以由表示生效时间段的时间对象、表示关键字的内容对象、放行还是阻断数据流、是否需要审计等条件自由组合实现，规则间存在优先级关系。

策略组也存在优先级关系，可以关联到静态用户和认证用户。WEB-BBS 审计根据策略组与规则的优先级来匹配最终生效的规则，对指定用户的 WEB-BBS 访问行为进行监控和审计。

对于有内置存储的网关设备，审计记录保存在设备的本地存储上，可以通过相应的查询命令来查看 WEB-BBS 审计记录的明细信息、统计信息。

当审计信息有发送到外面 log 服务器时，可以选择不记录到设备本地存储上，以减轻设备负担。

相关配置

↘ 配置 WEB-BBS 审计规则

缺省情况下，无 WEB-BBS 审计规则，WEB-BBS 审计功能自动关闭。

使用 **web-bbs-rule** 命令可以配置 WEB-BBS 审计规则。配置有效规则后，WEB-BBS 审计功能自动开启。

配置规则的参数决定了 WEB-BBS 审计对客户端邮件访问行为的监控和审计方式。

↘ 查看 WEB-BBS 审计的审计信息

缺省情况下，审计记录在设备本地存储上的保存天数是 60 天。

使用 **show web-bbs-audit** 命令可以查询 WEB-BBS 审计记录的明细信息、统计信息。

可通过指定所需的时间范围、过滤条件等配置参数来查询满足指定条件的审计记录信息。

当审计信息有发送到外面 log 服务器的时候，可以通过 **no content-audit write-db web-bbs** 关闭 web-bbs 审计信息写本地存储的开关。

8.3.7 WEB-MAIL 审计

WEB-MAIL 审计主要针对主流的 WEB 邮件系统（如新浪邮箱，网易邮箱，QQ 邮箱）对邮件进行发送审计，信息过滤，并保存邮件的附件至本地存储。

工作原理

WEB-MAIL 审计的基本工作原理是对未加密的包含 MAIL 发送信息的 HTTP 数据流进行解析，识别出数据流中相应的发件人、收件人、主题、正文、附件等信息，根据规则对信息进行关键字匹配和审计，放行或阻断相应数据流，从而实现对邮件进行发送审计和信息过滤。WEB-MAIL 审计目前不支持对邮件接收行为的审计。

WEB-MAIL 审计规则包含在策略组内，可指定对 WEB-MAIL 访问的控制和审计方式。规则可以由表示生效时间段的时间对象、表示关键字的内容对象、放行还是阻断数据流、是否需要审计等条件自由组合实现，规则间存在优先级关系。

策略组也存在优先级关系，可以关联到静态用户和认证用户。WEB-MAIL 审计根据策略组与规则的优先级来匹配最终生效的规则，对指定用户的 WEB-MAIL 访问行为进行监控和审计。

对于有内置存储的网关设备，审计记录保存在设备的本地存储上，可以通过相应的查询命令来查看 WEB-MAIL 审计记录的明细信息、统计信息、附件信息。

当审计信息有发送到外面 log 服务器时，可以选择不记录到设备本地存储上，以减轻设备负担。

相关配置

↘ 配置 WEB-MAIL 审计规则

缺省情况下，无 WEB-MAIL 审计规则，WEB-MAIL 审计功能自动关闭。

使用 **web-mail-rule** 命令可以配置 WEB-MAIL 审计规则。配置有效规则后，WEB-MAIL 审计功能自动开启。

配置规则的参数决定了 WEB-MAIL 审计对客户端邮件访问行为的监控和审计方式。

↘ 查看 WEB-MAIL 审计的审计信息

缺省情况下，审计记录在设备本地存储上的保存天数是 60 天。

使用 **show web-mail-audit** 命令可以查询 WEB-MAIL 审计记录的明细信息、统计信息、附件信息。

可通过指定所需的时间范围、过滤条件等配置参数来查询满足指定条件的审计记录信息。

当审计信息有发送到外面 log 服务器的时候，可以通过 **no content-audit write-db web-mail** 关闭 web-mail 审计信息写本地存储的开关。

8.3.8 WEB-SEARCH 审计

WEB-SEARCH 审计主要针对主流 WEB 搜索引擎站点（如百度，谷歌），对用户的搜索行为进行审计，并对搜索引擎关键字进行过滤。

工作原理

WEB-SEARCH 审计的基本工作原理是利用 URL 审计识别出来的 URL 信息，对属于搜索引擎的 URL 进一步识别出 URL 中相应的搜索关键字，根据规则对信息进行关键字匹配和审计，放行或阻断相应数据流，从而实现对用户的搜索行为进行审计和信息过滤。

WEB-SEARCH 审计规则包含在策略组内，可指定对 WEB-SEARCH 访问的控制和审计方式。规则可以由表示生效时间段的时间对象、表示关键字的内容对象、放行还是阻断数据流、是否需要审计等条件自由组合实现，规则间存在优先级关系。

策略组也存在优先级关系，可以关联到静态用户和认证用户。WEB-SEARCH 审计根据策略组与规则的优先级来匹配最终生效的规则，对指定用户的 WEB-SEARCH 访问行为进行监控和审计。

对于有内置存储的网关设备，审计记录保存在设备的本地存储上，可以通过相应的查询命令来查看 WEB-SEARCH 审计记录的明细信息、统计信息。

当审计信息有发送到外面 log 服务器时，可以选择不记录到设备本地存储上，以减轻设备负担。

相关配置

配置 WEB-SEARCH 审计规则

缺省情况下，无 WEB-SEARCH 审计规则，WEB-SEARCH 审计功能自动关闭。

使用 **web-search-rule** 命令可以配置 WEB-SEARCH 审计规则。配置有效规则后，WEB-SEARCH 审计功能自动开启。

配置规则的参数决定了 WEB-SEARCH 审计对客户端邮件访问行为的监控和审计方式。

查看 WEB-SEARCH 审计的审计信息

缺省情况下，审计记录在设备本地存储上的保存天数是 60 天。

使用 **show web-search-audit** 命令可以查询 WEB-SEARCH 审计记录的明细信息、统计信息。

可通过指定所需的时间范围、过滤条件等配置参数来查询满足指定条件的审计记录信息。

当审计信息有发送到外面 log 服务器的时候，可以通过 **no content-audit write-db web-search** 关闭 web-search 审计信息写本地存储的开关。

8.3.9 虚拟身份审计

虚拟身份审计主要针对主流的社交应用（目前支持微信，微博），对账号 ID 和昵称进行审计。

工作原理

虚拟身份审计支持对账号 ID 进行审计。可以识别出账号的上下线行为，并进行审计。

对于有内置存储的网关设备，审计记录保存在设备的本地存储上，可以通过相应的查询命令来查看虚拟身份审计记录的明细信息、统计信息。

当审计信息有发送到外面 log 服务器时，可以选择不记录到设备本地存储上，以减轻设备负担。

相关配置

配置虚拟身份审计规则

缺省情况下，无虚拟身份审计规则，虚拟身份审计功能自动关闭。

使用 **vid-rule** 命令可以开启虚拟身份审计功能。

配置规则的参数决定了 IM 审计对 IM 访问行为的监控和审计方式。

查看虚拟身份审计的审计信息

缺省情况下，审计记录在设备本地存储上的保存天数是 60 天。

使用 **show vid-audit** 命令可以查询虚拟身份审计记录的明细信息、统计信息、站点排名信息。

可通过指定所需的时间范围、过滤条件等配置参数来查询满足指定条件的审计记录信息。

8.3.10 QQ 聊天内容审计

QQ 聊天内容审计主要针对 PC 端 QQ 软件，对用户的聊天内容进行审计。PC 端需要安装插件用于监控 QQ 软件行为。

工作原理

PC 端插件审计到 QQ 聊天内容，通过 UDP 发送给设备进行记录。

相关配置

↘ 配置 PLUGIN 审计规则

缺省情况下，无 PLUGIN 审计规则，PLUGIN 审计功能自动关闭。

使用 **plugin-rule** 命令可以配置 PLUGIN 审计规则。配置有效规则后，PLUGIN 审计功能自动开启。

↘ 查看 PLUGIN 审计的审计信息

缺省情况下，审计记录在设备本地存储上的保存天数是 60 天。

使用 **show plugin-audit** 命令可以查询 PLUGIN 审计记录的明细信息、统计信息。

可通过指定所需的时间范围、过滤条件等配置参数来查询满足指定条件的审计记录信息。

当审计信息有发送到外面 log 服务器的时候，可以通过 **no content-audit write-db plugin** 关闭 plugin 审计信息写本地存储的开关。

8.3.11 外发文件审计

POST FILE 审计主要针对主流网盘（如百度文库、网易网盘），对用户发送的文件进行审计，并对文件名进行过滤。

工作原理

POST FILE 审计的基本工作原理是对 HTTP 上传文件的数据流进行解析，识别出数据流中的文件名、文件内容。根据规则对信息进行关键字匹配和审计，放行或阻断相应数据流，从而实现对用户的外发文件进行审计和过滤。POST FILE 审计目前不支持移动终端。

POST FILE 审计规则包含在策略组内，可指定对 POST FILE 访问的控制和审计方式。规则可以由表示生效时间段的时间对象、表示关键字的内容对象、放行还是阻断数据流、是否需要审计等条件自由组合实现，规则间存在优先级关系。

策略组也存在优先级关系，可以关联到静态用户和认证用户。POST FILE 审计根据策略组与规则的优先级来匹配最终生效的规则，对指定用户的 POST FILE 访问行为进行监控和审计。

对于有内置存储的网关设备，审计记录保存在设备的本地存储上，可以通过相应的查询命令来查看 POST FILE 审计记录的明细信息、统计信息。

当审计信息有发送到外面 log 服务器时，可以选择不记录到设备本地存储上，以减轻设备负担。

相关配置

↘ 配置 POST FILE 审计规则

缺省情况下，无 POST FILE 审计规则，POST FILE 审计功能自动关闭。

使用 **postfile-rule** 命令可以配置 POST FILE 审计规则。配置有效规则后，POST FILE 审计功能自动开启。

配置规则的参数决定了 POST FILE 审计对客户端邮件访问行为的监控和审计方式。

↘ 查看 POST FILE 审计的审计信息

缺省情况下，审计记录在设备本地存储上的保存天数是 60 天。

使用 **show postfile-audit** 命令可以查询 POST FILE 审计记录的明细信息、统计信息。

可通过指定所需的时间范围、过滤条件等配置参数来查询满足指定条件的审计记录信息。

当审计信息有发送到外面 log 服务器的时候，可以通过 **no content-audit write-db postfile** 关闭 postfile 审计信息写本地存储的开关。

8.3.12 HTTP-POST 审计

POST 审计主要针对主流 WEB BBS 站点（如天涯社区，猫扑社区）和微博（如新浪微博、腾讯微博），对用户的发帖内容进行审计，并对用户的发帖内容进行过滤。

工作原理

POST 审计的基本工作原理是对未加密的包含所有的 HTTP POST 数据流进行解析，识别出数据流中外发的 HTTP 内容，根据规则对信息进行关键字匹配和审计，放行或阻断相应数据流，从而实现对用户的外发信息内容进行审计和过滤。

POST 审计规则包含在策略组内，可指定对 POST 访问的控制和审计方式。规则可以由表示生效时间段的时间对象、表示关键字的内容对象、放行还是阻断数据流、是否需要审计等条件自由组合实现，规则间存在优先级关系。

策略组也存在优先级关系，可以关联到静态用户和认证用户。POST 审计根据策略组与规则的优先级来匹配最终生效的规则，对指定用户的 POST 访问行为进行监控和审计。

对于有内置存储的网关设备 ,审计记录保存在设备的本地存储上 ,可以通过相应的查询命令来查看 POST 审计记录的明细信息、统计信息。

当审计信息有发送到外面 log 服务器时，可以选择不记录到设备本地存储上，以减轻设备负担。

相关配置

↘ 配置 POST 审计规则

缺省情况下，无 POST 审计规则，POST 审计功能自动关闭。

使用 **post-rule** 命令可以配置 POST 审计规则。配置有效规则后，POST 审计功能自动开启。

配置规则的参数决定了 POST 审计对 HTTP POST 行为的监控和审计方式。

↘ 查看 POST 审计的审计信息

缺省情况下，审计记录在设备本地存储上的保存天数是 60 天。

使用 **show post-audit** 命令可以查询 POST 审计记录的明细信息、统计信息。

可通过指定所需的时间范围、过滤条件等配置参数来查询满足指定条件的审计记录信息。

当审计信息有发送到外面 log 服务器的时候 ,可以通过 **no content-audit write-db post** 关闭 post 审计信息写本地存储的开关。

8.3.13 加密类审计

加密类审计针对 SSL 协议加密的流量进行审计 ,主要是使用 HTTPS 协议的应用 ,包括 WEB-BBS、WEB-MAIL、WEB-SEARCH、虚拟身份、外发文件等各种应用类型。

工作原理

加密类审计的工作原理是通过 SSL 代理功能获取到用户的明文流量，然后进行上述审计业务处理。功能开启后，内容审计负责对各种应用的 DNS 域名解析结果进行学习，确定需要进行 SSL 代理的数据流。由于 SSL 代理需要使用我司签发的 SSL 证书对代理的数据流进行加解密，因此需要在终端安装 SSL 根证书，避免功能开启后部分应用由于证书不受信任导致无法使用。

相关配置

↘ 配置开启加密类审计功能

缺省情况下，加密类审计功能不开启。

在默认审计策略下，使用 **ssl-audit** 命令可以配置开启加密类审计功能，并结合 WEB-BBS、WEB-MAIL、WEB-SEARCH、虚拟身份、外发文件等各种应用类型的审计策略一同生效。

加密类审计结果的查看方式同上述各种应用类型的查看方式相同。

8.3.14 阻断信息实时统计

阻断信息实时统计，主要是对阻断的审计信息进行实时统计。

工作原理

进行行为审计，匹配到需要阻断的策略，则在记录数据库前进行记录的统计。

相关配置

↘ 配置开启加密类审计功能

缺省情况下，本功能开启。

8.3.15 TELNET 审计

针对 TELNET 协议，对 TELNET 数据流进行审计处理，审计的字段包括内网 IP、内网端口、服务器 IP、服务器端口、行为动作“连接 or 断开”。

工作原理

TELNET 审计的工作原理是通过获取 TELNET 流量，进行上述审计业务处理。功能开启后，通过数据流，获取 TELNET 客户端和服务端的 IP、端口号和行为动作。

相关配置

↘ 配置开启 TELNET 审计功能

缺省情况下，TELNET 审计功能不开启。

使用 **telnet-rule** 命令可以配置 TELNET 审计规则。配置有效规则后，TELNET 审计功能自动开启。

配置规则的参数决定了 TELNET 审计对 TELNET 行为的监控和审计方式。

↘ 查看 TELNET 审计的审计信息

使用 **show telnet-audit** 命令可以查询 TELNET 审计记录的明细信息、统计信息。

可通过指定所需的时间范围、过滤条件等配置参数来查询满足指定条件的审计记录信息。

可以通过 **no content-audit write-db telnet** 关闭 TELNET 审计信息写本地存储的开关。

8.3.16 FTP 审计

主要针对 FTP 协议，对使用 FTP 协议进行传输的文件名和上传的文件进行审计和过滤。

工作原理

FTP 审计的基本工作原理是对 FTP 上传、下载文件的数据流进行解析，识别出数据流中的文件名。根据规则对文件名进行关键字匹配和审计，放行或阻断相应数据流，从而实现对用户的 FTP 上传、下载的文件名和上传的文件内容进行审计和过滤。

FTP 审计规则包含在策略组内，可指定对 FTP 访问的控制和审计方式。规则可以由表示生效时间段的时间对象、表示文件名关键字的对象、放行还是阻断数据流、是否需要审计等条件自由组合实现，规则间存在优先级关系。

策略组也存在优先级关系，可以关联到静态用户和认证用户。FTP 审计根据策略组与规则的优先级来匹配最终生效的规则，对指定用户的 FTP 访问行为进行监控和审计。

对于有内置存储的网关设备，审计记录保存在设备的本地存储上，可以通过相应的查询命令来查看 FTP 审计记录的明细信息、统计信息。

是否审计上传文件内容由 ftp 文件审计总开关决定，默认为关闭，开启后审计上传文件内容。

可以选择不记录到设备本地存储上，以减轻设备负担。

相关配置

↘ 配置开启 FTP 审计功能

缺省情况下，FTP 审计功能不开启。

使用 **ftp-rule** 命令可以配置 FTP 审计规则。配置有效规则后，FTP 审计功能自动开启。

配置规则的参数决定了 FTP 审计对 FTP 行为的监控和审计方式。

↘ 查看 FTP 审计的审计信息

使用 **show ftp-audit** 命令可以查询 ftp 审计记录的明细信息、统计信息。

可通过指定所需的时间范围、过滤条件等配置参数来查询满足指定条件的审计记录信息。

当审计信息有发送到外面 log 服务器的时候，可以通过 **no content-audit write-db ftp** 关闭 ftp 审计信息写本地存储的开关。

8.3.17 FILE 过滤

主要针对网页邮箱附件、网页论坛附件、外发文件进行文件类型及文件名的过滤。

工作原理

postfile\webmail\bbs 邮件也有自己的附件名过滤规则，文件精细化控制这部分会有冲突。为了解决冲突，处理方法是：模块自己的规则优先级高，文件精细化控制优先级低。

相关配置

↘ 配置开启 FILE 过滤功能

缺省情况下，FILE 过滤功能不开启。

使用 **file-rule** 命令可以配置 FILE 过滤规则。配置有效规则后，FILE 过滤功能自动开启。

配置规则的参数决定了 FILE 对文件行为的监控方式。

8.3.18 内容审计关键字订阅

针对内容审计中需要告警的内容，发送邮件告警给用户。

工作原理

定期查询当前内容审计告警记录，进行汇总后，发送告警邮件给关注人。

相关配置

↘ 配置开启内容审计阻断邮件告警功能

缺省情况下，功能不开启。

8.3.19 内容审计报表统计

针对内容审计记录进行报表统计

工作原理

定期后台生成数据，定时或手动创建统计报表

可根据用户自定义的规则后台统计相应的报表数据

相关配置

↘ 配置报表数据后台生成时间

缺省情况下，功能不开启。

8.4 产品说明



NBR2500D-E、NBR3000D-E、NBR3000D-UE 带硬盘设备支持审计记录在本地；NBR800G、NBR950G、NBR1500G、NBR2000G 、 NBR1000G-C 、 NBR2000G-C 、 NBR3000G-S 、 NBR1000G-E 、 NBR6120-E 、 NBR1300G-E 、 NBR1700G-E、NBR2100G-E 不支持本地记录。NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 默认无硬盘，不支持本地记录，带硬盘时支持本地记录。

NBR800G、NBR950G、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 URL 分类； NBR1500G、NBR2000G、NBR1000G-C、NBR2000G-C、NBR3000G-S 不支持 URL 分类。

NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR800G、NBR950G、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 HTTP URL 审计、BSS、微博审计、webmail 审计、mail 审计、HTTPS 域名审计、IM 审计、HTTPS 加密内容审计、关键字告警；NBR1500G、NBR2000G、NBR1000G-C、NBR2000G-C、NBR3000G-S 不支持 HTTP URL 审计、BSS、微博审计、webmail 审计、mail 审计、HTTPS 域名审计、IM 审计、HTTPS 加密内容审计、关键字告警。

NBR800G、NBR950G、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持搜索审计功能 ;NBR1500G、NBR2000G、NBR1000G-C、NBR2000G-C、NBR3000G-S 不支持搜索审计功能

NBR800G、NBR950G、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持关键字过滤、应用控制；NBR1500G、NBR2000G、NBR1000G-C、NBR2000G-C、NBR3000G-S 不支持关键字过滤、应用控制

NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持外发信息审计、外发文件审计、QQ 聊天内容审计、HTTPS 加密内容审计、文件精细化控制、FTP 审计、Telnet 审计、；NBR800G、NBR950G、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR1500G、NBR2000G、NBR1000G-C、NBR2000G-C、NBR3000G-S 不支持外发信息审计、外发文件审计、QQ 聊天内容审计、文件精细化控制、FTP 审计、Telnet 审计。



NBR800G、NBR950G、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持虚拟身份 ID 识别；NBR1500G、NBR2000G、NBR2000G-C、NBR3000G-S、NBR1000G-C 不持虚拟身份 ID 识别。

NBR800G、NBR950G、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 HTTPS URL 审计，NBR1500G、NBR2000G、NBR2000G-C、NBR3000G-S、NBR1000G-C 不支持 HTTPS URL 审计。

NBR1500G、NBR2000G、NBR2000G-C、NBR3000G-S、NBR1000G-C 不支持实时审计记录和阻断信息记录，NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR800G、NBR950G、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持实时审计记录和阻断信息记录。

NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持虚拟身份、搜索引擎、论坛发帖、外发文件、网站分类、网站域名、WEBMAIL、MAIL、IM、自定义的审计报表，同时支持审计报表以 PDF 的方式导出 ;NBR800G、NBR950G、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR1500G、NBR2000G、NBR2000G-C、NBR3000G-S、NBR1000G-C 不支持虚拟身份、搜索引擎、论坛发帖、外发文件、网站分类、网站域名、WEBMAIL、MAIL、IM、自定义的审计报表。

NRB108G-P 不支持内容审计所有功能。

8.5 配置详解

配置项	配置建议 & 相关命令
配置 URL 分类	⚠ 可选配置。供 URL 对象引用。

	url class	配置 URL 分类
	url	添加 URL 条目
	comment	配置描述
配置 URL 对象	⚠ 必须配置。供 URL 规则引用。	
	url-object	配置 URL 对象
	class	添加 URL 分类
	regexp	添加正则表达式
	comment	配置描述
配置内容对象	⚠ 必须配置。供各内容审计规则引用。	
	content-object	配置内容对象
	keyword	添加关键字
	regexp	添加正则表达式
	comment	配置描述
配置策略组	⚠ 必须配置。用于建立基于用户的行为管理。	
	content-policy	配置策略组
	content-policy-config	配置策略组属性
	content-policy-relate	将策略组关联到用户
配置应用控制审计规则	⚠ 必须配置。用于建立应用控制审计策略。	
	app-rule	配置应用控制审计规则
	app-audit	配置应用控制审计优化
配置 URL 规则	⚠ 必须配置。用于建立 URL 审计策略。	
	url-rule	配置 URL 审计规则
	url-audit	配置 URL 审计优化
配置 URL 重定向规则	⚠ 必须配置。用于建立 URL 重定向策略。	
	url-redirect-rule	配置 URL 重定向规则
配置 IM 规则	⚠ 必须配置。用于建立 IM 审计策略。	
	im-rule	配置 IM 审计规则
配置 MAIL 规则	⚠ 必须配置。用于建立 MAIL 审计策略。	
	mail-rule	配置 MAIL 审计规则
配置 WEB-BBS 规则	⚠ 必须配置。用于建立 WEB-BBS 审计策略。	
	web-bbs-rule	配置 WEB-BBS 审计规则
配置 WEB-MAIL 规则	⚠ 必须配置。用于建立 WEB-MAIL 审计策略。	
	web-mail-rule	配置 WEB-MAIL 审计规则

配置 WEB-SEARCH 规则	⚠ 必须配置。用于建立 WEB-SEARCH 审计策略。	
	web-search-rule	配置 WEB-SEARCH 审计规则
配置虚拟身份规则	⚠ 必须配置。用于建立虚拟身份审计策略。	
	vid-rule	配置虚拟身份审计规则
配置 QQ 聊天内容规则	⚠ 必须配置。用于建立 QQ 聊天内容审计策略。	
	plugin-rule	配置 QQ 聊天内容审计规则
配置外发文件规则	⚠ 必须配置。用于建立外发信息审计策略。	
	postfile-rule	配置外发文件审计规则
配置 HTTP POST 规则	⚠ 必须配置。用于建立 HTTP POST 审计策略。	
	post-rule	配置 HTTP POST 审计规则
配置内容审计信息写本地存储的开关	⚠ 可选配置。用于控制内容审计各业务的审计信息是否写本地存储。	
	content-audit write-db {url | web-search | web-bbs | web-mail | mail | im | app-control | vid | ftp | telnet }	配置内容审计信息写本地存储的开关
配置 HTTP 端口	⚠ 可选配置。不开启应用识别时，支持 TCP 80、8080 端口以外的 HTTP 端口流的 URL 审计。	
	content-audit http-port *port-num*	配置 HTTP 端口
配置 HTTPS 端口	⚠ 可选配置。不开启应用识别时，支持 TCP 443 端口以外的 HTTPS 端口流的域名审计。	
	content-audit https-port *port-num*	配置 HTTPS 端口
配置 HTTPS 审计使能开关	⚠ 可选配置。用于控制是否对 HTTPS 网站进行审计和过滤。	
	https-audit enable	配置 HTTPS 审计的使能开关
配置 TELNET 规则	⚠ 必须配置。用于建立 TELNET 审计策略。	
	telnet-rule	配置 TELNET 审计规则
配置 FTP 规则	⚠ 必须配置。用于建立 FTP 审计策略。	
	ftp-rule	配置 FTP 审计规则
配置 FILE 规则	⚠ 必须配置。用于建立 FILE 过滤策略。	
	file-rule	配置 FILE 过滤规则
配置附件上传 elog 的使能开关	⚠ 可选配置。NPE 模式有硬盘的情况下，开启此开关，可以支持附件上传 elog。	
	content-attach-to-elog enable	配置附件上传 elog 的使能开关

8.5.1 配置 URL 分类

配置效果

- 可配置自定义 URL 分类及包含的 URL 条目。
- 可修改系统 URL 分类包含的 URL 条目。
- 可查询具体 URL 所属的 URL 系统类和自定义分类。
- 配置的 URL 分类供 URL 对象引用。

注意事项

- 配置的 URL 分类需要被具体的 URL 对象引用才能生效。

配置方法

↘ 配置 URL 分类

- 必须配置。

↘ 配置 URL 条目

- 可选配置。若需要包含或修改 URL 条目则可配置。

↘ 配置描述

- 可选配置。若需要对 URL 分类进行描述说明则可添加。

检验方法

- 查看系统 URL 分类
- 查看自定义 URL 分类
- 查看指定 URL 的分类

相关命令

↘ 配置 URL 分类

【命令格式】 **url-class** *class-name*
【参数说明】 *class-name*：URL 分类名称。
【命令模式】 全局模式
【使用指导】 生成 URL 分类，并进入 URL 分类配置模式。删除 URL 分类，可以在全局配置模式下执行 no url-class

class-name。

配置 URL 条目

【命令格式】 **url** *url-string*

【参数说明】 *url-string*：URL 分类所包含的 URL 条目，支持模式匹配：1、若自定义网站分类中包含的 URL 为域名下的子目录，则匹配该子目录下的所有文件。例如：URL 为“ietf.org/2006”，则匹配“ietf.org/2006”目录下所有的内容。 2、若自定义网站分类中包含的 URL 为域名且不含路径，则匹配所有对该域名及其子域名的访问，例如：URL 为“ietf.org”，则匹配对“www.ieft.org”及“download.ietf.org”、 “news.ietf.org”等子域的访问。

【命令模式】 URL 分类配置模式

【使用指导】 向 URL 分类中添加 URL 条目。使用 **no url** *url-string* 删除。

配置描述

【命令格式】 **comment** *comment-string*

【参数说明】 *comment-string*：URL 分类的描述，最长支持 100 个字符。

【命令模式】 URL 分类配置模式

【使用指导】 描述通常是用来说明 URL 分类的用途。使用 **no comment** 删除。

显示系统 URL 库分类名

【命令格式】 **show url-class system** [**class** { **id** *class-id* | **name** *class-name* }]

【参数说明】 *class-name*：查看指定系统分类名 class-name 的信息；未指定 class 表示查看所有系统 URL 分类信息。
class-id：查看指定系统分类 ID class-id 的信息。

【命令模式】 特权模式

【使用指导】 使用该命令可以查询系统 URL 库分类名。

显示系统 URL 库描述信息

【命令格式】 **show url-class system comment** [**class** { **id** *class-id* | **name** *class-name* }]

【参数说明】 *class-name*：查看指定系统分类名 class-name 的信息；未指定 class 表示查看所有系统 URL 分类信息。
class-id：查看指定系统分类 ID class-id 的信息。

【命令模式】 特权模式

【使用指导】 使用该命令可以查询系统 URL 库描述信息。

显示系统 URL 库的当前自定义修改信息

【命令格式】 **show url-class system custom** [**class** { **id** *class-id* | **name** *class-name* }]

【参数说明】 *class-name*：查看指定系统分类名 class-name 的信息；未指定 class 表示查看所有系统 URL 分类信息。
class-id：查看指定系统分类 ID class-id 的信息。

【命令模式】 特权模式

【使用指导】 使用该命令可以查询系统 URL 库的当前自定义修改信息。。

显示精准过滤库相关信息

【命令格式】 **show url-class system exact**

【参数说明】 -

【命令模式】 特权模式

【使用指导】 使用该命令可以查询精准过滤库相关信息。

显示 URL 所属分类

【命令格式】 **show url-class url** *url-string*

【参数说明】 *url-string*：代表 URL 的字符串。

【命令模式】 特权模式

【使用指导】 使用该命令可以查询指定 url-string 所属的系统 url 分类和当前配置下实际的 url 分类。

显示自定义 URL 分类的配置信息

【命令格式】 **show url-class user-cfg** [*class-name*]

【参数说明】 *class-name*：自定义的分类名。

【命令模式】 特权模式

【使用指导】 使用该命令可以查询自定义 URL 分类的配置信息

配置举例

配置自定义 URL 分类

【配置方法】

- 配置分类 CLASSA。
- 配置 URL 条目，用于匹配 ietf.org 子域名的所有 URL。
- 配置描述 NEW-CLASSA

```
Ruijie# configure terminal
Ruijie(config)# url-class CLASSA
Ruijie(url-cls-config)# url ietf.org
Ruijie(url-cls-config)# comment NEW-CLASSA
Ruijie(url-cls-config)# end
```

【检验方法】

- 使用 show running-config 命令可以查看配置状态。

```
Ruijie# show running-config
……
url-class CLASSA
 url ietf.org
 comment NEW-CLASSA
!……
```

修改系统 URL 分类

【配置方法】

- 进入系统分类搜索引擎
- 添加 URL 条目 ietf.org。

```
Ruijie# configure terminal
Ruijie(config)# url-class 搜索引擎
```

```
Ruijie(url-cls-config)# url ietf.org
Ruijie(url-cls-config)# end
```

【检验方法】

- 使用 show running-config 命令可以查看配置状态。

```
Ruijie# show running-config
……
url-class 搜索引擎
 url ietf.org
!……
```

显示指定 url-string 所属的系统 url 分类和当前配置下实际的 url 分类

【配置方法】

- 显示 URL 为 ruijie.com.cn 的分类信息。

```
Ruijie# show url-class user-cfg CLASSA
url-class:CLASSA
url:ietf.org
comment:comment for CLASSA
```

【检验方法】 查看命令的运行结果。

常见错误

- 正则表达式不满足语法要求。

8.5.2 配置 URL 对象

配置效果

- 建立 URL 对象，供 URL 规则引用。

注意事项

- 配置的 URL 对象需要被具体的规则引用才能生效。

配置方法

配置 URL 对象

- 必须配置。

配置 URL 分类

- 可选配置。若包含 URL 分类则可添加。

配置正则表达式

- 可选配置。若包含正则表达式则可添加。。

配置描述

- 可选配置。若需要对 URL 对象进行描述说明则可添加。

检验方法

使用 show running-config 命令可以查看配置状态。

相关命令

配置 URL 对象

【命令格式】 **url-object** *object-name*
【参数说明】 *object-name*：URL 对象名称。
【命令模式】 全局模式
【使用指导】 生成 URL 对象，并进入 URL 对象配置模式。删除 URL 对象及所包含的所有内容，可以在全局配置模式下执行 **no url-object** *object-name*。

配置 URL 分类

【命令格式】 **class** *class-name*
【参数说明】 *class-name*：URL 分类的名称，可以是用户自定义的 URL 分类，也可以是系统自带的 URL 分类。
【命令模式】 URL 对象配置模式
【使用指导】 向 URL 对象中添加关键字。使用 **no class** *class-name* 删除。

配置正则表达式

【命令格式】 **regexp** *url-regexp*
【参数说明】 *url-regexp*：URL 正则表达式，支持标准的正则表示法。
【命令模式】 URL 对象配置模式
【使用指导】 向 URL 对象中添加 URL 正则表达式。使用 **no regexp** *url-regexp* 删除。

配置描述

【命令格式】 **comment** *comment-string*
【参数说明】 *comment-string*：URL 对象的描述，最长支持 100 个字符。
【命令模式】 URL 对象配置模式
【使用指导】 描述通常是用来说明 URL 对象的用途。使用 **no comment** 删除。

配置举例

配置一个用于免审计的 URL 对象

【配置方法】
- 配置 url 对象 un_audit_object。
- 配置分类 un_audit_class、软件更新、脚本未知、软件升级。
- 配置描述 un_audit。

```
Ruijie# configure terminal
Ruijie(config)# url-object objA
Ruijie(url-obj-config)# class un_audit_class
Ruijie(url-obj-config)# class 软件更新
Ruijie(url-obj-config)# class 脚本未知
Ruijie(url-obj-config)# class 软件升级
Ruijie(url-obj-config)# comment un_audit
Ruijie(url-obj-config)# end
```

【检验方法】
- 使用 show running-config 命令可以查看配置状态。

```
Ruijie# show running-config
……
url-object un_audit_object
 class un_audit_class
 class 软件更新
 class 脚本未知
 class 软件升级
 comment un_audit
!……
```

配置一个用于文件阻断的 URL 对象

【配置方法】
- 配置 url 对象 file_deny。
- 配置正则表达式。

```
Ruijie# configure terminal
Ruijie(config)# url-object file_deny
Ruijie(url-obj-config)# regexp (\.exe$)|(\.bat$)|(\.rmvb$)
Ruijie(url-obj-config)# end
```

【检验方法】
- 使用 show running-config 命令可以查看配置状态。

```
Ruijie# show running-config
……
url-object file_deny
 regexp (\.exe$)|(\.bat$)|(\.rmvb$)
!……
```

常见错误

- 正则表达式不满足语法要求。

8.5.3 配置内容对象

配置效果

- 建立内容对象，供各内容审计规则引用。

注意事项

- 配置的内容对象需要被具体的规则引用才能生效。

配置方法

↘ 配置内容对象

- 必须配置。

↘ 配置关键字

- 可选配置。若包含关键字则可添加。

↘ 配置正则表达式

- 可选配置。若包含正则表达式则可添加。

↘ 配置描述

- 可选配置。若需要对内容对象进行描述说明则可添加。

检验方法

使用 show running-config 命令可以查看配置状态。

相关命令

↘ 配置内容对象

【命令格式】 **content-object** *object-name*
【参数说明】 *object-name*：内容对象名称。
【命令模式】 全局模式
【使用指导】 生成内容对象，并进入内容对象配置模式。删除内容对象及所包含的所有内容，可以在全局配置模式下执行 **no content-object** *object-name*。

配置关键字

【命令格式】 **keyword** *string*

【参数说明】 *string*：内容对象包含的关键字。

【命令模式】 内容对象配置模式

【使用指导】 向内容对象中添加关键字。使用 **no keyword** *string* 删除。

配置正则表达式

【命令格式】 **regexp** *regexp*

【参数说明】 *regexp*：关键字正则表达式，支持标准的正则表示法。

【命令模式】 内容对象配置模式

【使用指导】 向内容对象中添加关键字正则表达式。使用 **no regexp** *regexp* 删除。

配置描述

【命令格式】 **comment** *comment-string*

【参数说明】 *comment-string*：内容对象的描述，最长支持 100 个字符。

【命令模式】 内容对象配置模式

【使用指导】 描述通常是用来说明内容对象的用途。使用 **no comment** 删除。

配置举例

配置一个内容对象

【配置方法】

- 配置内容对象 objA。
- 配置关键字 hello。
- 配置正则匹配 .ietf.org。
- 配置描述 commentA。

```
Ruijie# configure terminal
Ruijie(config)# content-object objA
Ruijie(content-obj-config)# keyword hello
Ruijie(content-obj-config)# regexp .*\.ietf\.org
Ruijie(content-obj-config)# comment commentA
Ruijie(content-obj-config)# end
```

【检验方法】

- 使用 show running-config 命令可以查看配置状态。

```
Ruijie# show running-config
......
content-object objA
 keyword hello
 regexp .*\.ietf\.org
 comment commentA
!
```

```
.....
```

常见错误

- 正则表达式不满足语法要求。

8.5.4 配置策略组

配置效果

- 建立策略组。
- 可配置策略组属性。
- 可将策略组关联到用户。

注意事项

- 配置的策略组需要关联到有效的用户才能生效。
- 策略匹配的优先级顺序是先比较策略组的优先级，再比较策略组内规则的优先级。
- 策略匹配时认证用户的优先级比静态用户高。

配置方法

↘ 配置策略组

- 必须配置。

↘ 配置策略组属性

- 可选配置。若需要修改策略组属性则可配置。

↘ 将策略组关联到用户

- 必须配置。

检验方法

使用 show running-config 命令可以查看配置状态。

相关命令

↘ 配置策略组

【命令格式】 **content-policy** *policy-name*

【参数说明】 *policy-name*：内容审计策略组名称。

【命令模式】 全局模式

【使用指导】 指定内容审计策略组名，并进入内容审计策略组配置模式。策略组容量为 100。删除策略组及所包含的所有内容，可以在全局配置模式下执行 **no content-policy** *policy-name*。

全局禁用策略组

【命令格式】 **content-policy-config disable-all**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 1：全局禁用只对自定义策略组起作用，对内置策略组无效。

2：使用命令 **no content-policy-config disable-all** 取消禁用。

禁用策略组

【命令格式】 **content-policy-config disable-policy** *policy-name*

【参数说明】 *policy-name*：内容审计策略组名称。

【命令模式】 全局模式

【使用指导】 1：策略组默认都是有效的。禁用策略组提供了一种可以保留策略组配置，但是不使用该策略组的方式。要想禁用某个策略组，需要显式地配置一条禁用命令。

2：禁用策略组不会删除策略组内容和与用户的关联。

3：配置禁用策略组命令时，如果指定的策略组名不存在，则该命令不会生效。

4：删除策略组后，禁用策略组配置也会同时被删除。

5：使用命令 **no content-policy-config disable-policy** *policy-name* 取消禁用。

交换策略组优先级

【命令格式】 **content-policy-config priority-swap** *policy-name1 policy-name2*

【参数说明】 *policy-name1*：需要对调优先级的策略组名。

policy-name2：需要对调优先级的另一策略组名。

【命令模式】 全局模式

【使用指导】 配置交换两个策略组的优先级后，show running 中可以看到两个策略组排序发生了变化，但 show running 不会出现该命令。

将策略组关联到用户

【命令格式】 **content-policy-relate relate** { **subscriber** { *subs-name1* | **any** } | **auth-subscriber** { *subs-name2* | **any** } } **policy** *policy-name*

【参数说明】 *subs-name1*：策略组关联的静态用户或者自定义用户组。

subs-name2：策略组关联的认证用户。

policy-name：策略组名。

【命令模式】 全局模式

【使用指导】 1：配置关联规则时，如果策略组名不存在，则关联操作不会生效，命令也不会存在。

2：配置关联规则时，所关联的用户 subs-name1、subs-name2 可以不存在，此时该命令可以存在，只是规

则不生效。

3：配置关联规则时，subscriber 或 auth-subscriber 允许指定多个用户名，用户名之间以逗号分割，表示多个用户与该策略组关联。policy-name 也允许指定多个策略组，策略组之间以逗号分割。

4：使用命令 **no content-policy-relate relate** { **subscriber** { *subs-name1* | **any** } | **auth-subscriber** { *subs-name2* | **any** } } **policy** *policy-name* 取消关联。

设置用户不继承父用户组的策略

【命令格式】 **content-policy-relate no-inherit** { **subscriber** { *subs-name1* | **any** } | **auth-subscriber** { *subs-name2* | **any** } }

【参数说明】 *subs-name1*：策略组关联的静态用户。

subs-name2：策略组关联的认证用户。

【命令模式】 全局模式

【使用指导】 1：配置用户的策略继承属性时，所指定的用户 subs-name1、subs-name2 可以不存在，如果此时有策略关联存在，那么该命令可以存在，只是规则不生效。删除用户与所有策略组的关联后，用户的禁止策略继承属性也会同时被删除。

2：使用命令 **no content-policy-relate no-inherit** { **subscriber** { *subs-name1* | **any** } | **auth-subscriber** { *subs-name2* | **any** } }恢复用户的策略继承属性。

配置举例

配置策略组

【配置方法】

- 配置一个内容审计策略组 policyA。

```
Ruijie# configure terminal
Ruijie(config)# content-policy policyA
Ruijie(cont-plcy-config)# end
```

【检验方法】

- 使用 show running-config 命令可以查看配置状态。

配置策略组属性

【配置方法】

- 关闭所有自定义策略组。

```
Ruijie# configure terminal
Ruijie(config)# content-policy-config disable-all
Ruijie(config)# end
```

- 禁用内容审计策略组 policyA。

```
Ruijie# configure terminal
Ruijie(config)# content-policy-config disable-policy policyA
Ruijie(config)# end
```

- 交换两个策略组 policyA、policyB 的优先级。

```
Ruijie# configure terminal
```

```
Ruijie(config)# content-policy-config policy-swap policyA policyB
Ruijie(config)# end
```

【检验方法】 ● 使用 show running-config 命令可以查看配置状态。

常见错误

- 策略的优先级关系未理清导致实际审计结果与预期有差异。

8.5.5 配置应用控制审计规则

配置效果

- 向内容审计策略组中添加应用控制审计规则。
- 交换应用控制审计规则的优先级。
- 配置应用控制审计审计优化。

注意事项

- 应用控制审计规则的生效状态取决于引用的应用分类是否存在、时间对象是否生效、所属的策略组是否关联有效用户。
- 同一个策略组内的规则优先级为后配先生效。
- 应用控制审计无默认审计规则。
- 应用控制审计的阻断规则与其它审计相冲突时，应用控制审计的优先级最高。被应用控制审计阻断的数据流不会再进行其它内容审计。

配置方法

↘ 配置应用控制审计规则

- 必须配置。

↘ 交换应用控制审计规则的优先级

- 可选配置。若需要交换应用控制审计规则的优先级则可配置。

↘ 配置应用控制审计审计优化

- 可选配置。若需要改变默认设置则可配置。

检验方法

使用 show running-config 命令可以查看配置状态。

相关命令

配置应用控制审计规则

【命令格式】 **app-rule** *rule-id* **time-range** *time-name* **app-group** *app-group-name* **action** { **permit** | **deny** } [**audit**] [**vpn**] [**vip**] [**comment** *comment-string*]

【参数说明】 *rule-id*：规则的 ID 标识，取值范围（1~200）。规则容量为 200。

app-group-name：规则要控制的应用组名。

time-name：代表规则生效时间段的时间对象名。

comment-string：该规则的描述。

【命令模式】 内容审计策略组配置模式

【使用指导】 1：规则的 rule-id 在同一个内容审计策略组中不允许重复，在不同的内容审计策略组中允许重复。

2：一个内容审计策略组中的访问控制规则都有相应的优先级，最后配的那条规则优先级最高。

3：规则所关联的 time-name、app-group-name 可以不存在，此时规则不生效。

4：删除应用控制审计规则可使用命令 **no app-rule** *rule-id*。

删除策略组下所有应用控制审计规则

【命令格式】 **app-rule delete-all**

【参数说明】 -

【命令模式】 内容审计策略组配置模式

【使用指导】 只能删除当前策略组下的所有应用控制审计规则，不影响其它策略组。

交换应用控制审计规则的优先级

【命令格式】 **app-rule priority-swap** *rule-id1 rule-id2*

【参数说明】 *rule-id1*：待交换优先级的规则 1 的 ID。

rule-id2：待交换优先级的规则 2 的 ID。

【命令模式】 内容审计策略组配置模式

【使用指导】 交换优先级命令是用于对调两条访问控制规则的优先级，运行该命令后，show running 中可以看到两个规则的排序发生了变化，但 show running 不会出现该命令。

配置应用控制审计优化

【命令格式】 **app-audit** { **optimize-cache** [*time*] | **optimize-deny** }

【参数说明】 *time*：该参数的单位是秒，开启该功能后，不重复审计同一个 IP 在 *time* 时间内的相同应用阻断动作。

【命令模式】 全局模式

【使用指导】 1：开启优化审计功能后，同一个 IP 在一定时间内的同一个应用阻断动作不会被重复审计。默认时间长度为 300s，范围为 5~1800 秒。

2：对于 TCP 流，应用阻断有两种方式：一是直接丢包，二是发送 rst 报文主动断开连接。这两种方式可以通过优化阻断配置切换。

3：缺省为开启状态。关闭相应的应用控制审计优化功能可使用命令 **no no app-audit** { **optimize-cache** | **optimize-deny** }。

配置举例

配置应用控制审计规则

【配置方法】

- 为策略组 policyA 添加一条应用控制审计规则，过滤用户进行视频播放和 P2P 下载，并且审计相应的过滤信息。

```
Ruijie# configure terminal
Ruijie(config)# content-policy policyA
Ruijie(cont-plcy-config)# app-rule 2 time-range any direction double app-group VideoAndP2PGroup action deny audit comment DenyVideoAndP2P
Ruijie(cont-plcy-config)# end
```

- 删除策略组 policyA 中的所有应用控制审计规则。

```
Ruijie# configure terminal
Ruijie(config)# content-policy policyA
Ruijie(cont-plcy-config)# app-rule delete-all
Ruijie(cont-plcy-config)# end
```

【检验方法】

- 使用 show running-config 命令可以查看配置状态。

交换应用控制审计规则的优先级

【配置方法】

- 交换策略组 policyA 内应用控制审计访问控制规则 10 和规则 20 的优先级。

```
Ruijie# configure terminal
Ruijie(config)# content-policy policyA
Ruijie(cont-plcy-config)# app-rule priority-swap 10 20
Ruijie(cont-plcy-config)# end
```

【检验方法】

- 使用 show running-config 命令可以查看配置状态。

配置应用控制审计审计优化

【配置方法】

- 配置指定 120s 内，同一个 IP 的重复应用阻断不审计。

```
Ruijie# configure terminal
Ruijie(config)# app-audit optimize-cache 120
Ruijie(config)# end
```

- 关闭应用控制审计的优化阻断功能。

```
Ruijie# configure terminal
Ruijie(config)# no app-audit optimize-deny
Ruijie(config)# end
```

【检验方法】

- 使用 show running-config 命令可以查看配置状态。

常见错误

- 规则 id 重复导致配置失败。
- 规则引用的对象未存在导致规则不生效。
- 规则优先级未理清导致实际审计结果与预期有差异。

8.5.6 配置 URL 规则

配置效果

- 启用 URL 默认审计功能。
- 向内容审计策略组中添加 URL 规则。
- 交换 URL 规则的优先级。
- 配置 URL 审计优化。
- 配置 URL 过滤提示页面显示的内容。

注意事项

- URL 规则的生效状态取决于引用的 URL 对象是否存在、时间对象是否生效、所属的策略组是否关联有效用户。
- 同一个策略组内的规则优先级为后配先生效。

配置方法

↘ 配置 URL 规则

- 必须配置。

↘ 配置 URL 默认审计

- 可选配置。若需要开启默认审计功能则可配置。

↘ 交换 URL 规则的优先级

- 可选配置。若需要交换 URL 规则的优先级则可配置。

↘ 配置 URL 审计优化

- 可选配置。若需要改变默认设置则可配置。

↘ 配置 URL 过滤提示页面显示的内容

- 可选配置。若需要改变默认设置则可配置。

检验方法

使用 show running-config 命令可以查看配置状态。

相关命令

配置 URL 规则

【命令格式】 **url-rule** *rule-id* **url-object** *url-obj-name* **time-range** *time-name* **action** { **permit** | **deny** } [**audit**] [**comment** *comment-string*]

【参数说明】 *rule-id*：规则的 ID 标识，取值范围（1~200）。规则容量为 200。

url-obj-name：规则关联的 URL 对象。

time-name：代表规则生效时间段的时间对象名。

comment-string：该规则的描述。

【命令模式】 内容审计策略组配置模式

【使用指导】 1：规则的 rule-id 在同一个内容审计策略组中不允许重复，在不同的内容审计策略组中允许重复。

2：一个内容审计策略组中的访问控制规则都有相应的优先级，最后配的那条规则优先级最高。

3：规则所关联的 time-name、url-obj-name 可以不存在，此时规则不生效。

4：删除 URL 规则可使用命令 **no url-rule** *rule-id*。

配置 URL 默认审计

【命令格式】 **url-rule audit-default-enable**

【参数说明】 -

【命令模式】 内容审计策略组配置模式

【使用指导】 1：默认审计只能在策略组名为_AUDIT_DEFAULT 的默认审计组内进行配置，在其它策略组内配置该命令则不生效。

2：关闭 URL 默认审计功能可使用命令 **no url-rule audit-default-enable**。

删除策略组下所有 URL 规则

【命令格式】 **url-rule delete-all**

【参数说明】 -

【命令模式】 内容审计策略组配置模式

【使用指导】 只能删除当前策略组下的所有 URL 规则，不影响其它策略组。

交换 URL 规则的优先级

【命令格式】 **url-rule priority-swap** *rule-id1 rule-id2*

【参数说明】 *rule-id1*：待交换优先级的规则 1 的 ID。

rule-id2：待交换优先级的规则 2 的 ID。

【命令模式】 内容审计策略组配置模式

【使用指导】 交换优先级命令是用于对调两条访问控制规则的优先级，运行该命令后，show running 中可以看到两个规则的排序发生了变化，但 show running 不会出现该命令。

配置 URL 审计优化

【命令格式】 **url-audit** { **apply-referer** | **exact-filter** | **except-postfix** | **except-regexp** [*regexp*] | **only-get** | **optimize-cache** [*time*] }

【参数说明】 *regexp*：该参数是一个正则表达式，开启该功能后，匹配该正则表达式的 URL 不会被审计。

time：该参数的单位是秒，开启该功能后，time 时间内不重复审计同一个 URL 以及从该 URL 网页上打开的链接页。

【命令模式】 全局模式

【使用指导】 1：如果在开启 url-audit except-regexp 时没有指定正则表达式，则默认指定为 ".*=.*&.*=.*"。

2：开启 url-audit except-postfix，将不审计下面这些后缀的 URL，jpg、css、js、gif、png、swf、bmp、ico、ng、dll、GIF、JPG、xml、ini。

3：开启 url-audit optimize-cache，默认时间为 30s。

4：url-audit apply-referer 是需要与 URL 审计过滤策略相配合的。配置完成后，URL 规则在匹配时除了匹配对应的 URL 外，还会用 referer 字段去匹配规则。若只配置该命令，而不开启对应的 URL 审计过滤规则，则无实际效果。

5：缺省为开启状态。关闭相应的 URL 优化审计功能可使用命令 **no url-audit** { **apply-referer** | **exact-filter** | **except-postfix** | **except-regexp** [*regexp*] | **only-get** | **optimize-cache** [*time*] }。

配置 URL 过滤提示页面显示的内容

【命令格式】 **url-filter-notice display** [*text*]

【参数说明】 *text*：URL 过滤提示页面上显示的信息。不输入显示默认信息。

【命令模式】 全局模式

【使用指导】 通过此命令可以配置 URL 过滤提示页面显示的内容。默认开启，显示内容为：

"You are forbidden to visit the website, please contact webmaster!"

配置举例

配置 URL 规则

【配置方法】

- 为内容审计策略组 policyA 添加一个 URL 访问审计规则，不允许访问 URL 对象 url-objA 中的 URL，并且需要审计该类 URL 访问。

```
Ruijie# configure terminal
Ruijie(config)# content-policy policyA
Ruijie(cont-plcy-config)# url-rule 2 url-object url-objA time-range any action deny audit
Ruijie(cont-plcy-config)# end
```

- 删除策略组 policyA 中的所有 URL 规则。

```
Ruijie# configure terminal
Ruijie(config)# content-policy policyA
Ruijie(cont-plcy-config)# url-rule delete-all
Ruijie(cont-plcy-config)# end
```

【检验方法】 ● 使用 show running-config 命令可以查看配置状态。

配置 URL 默认审计

【配置方法】 ● 启用 URL 默认审计。

```
Ruijie# configure terminal
Ruijie(config)# content-policy _AUDIT_DEFAULT
Ruijie(cont-plcy-config)# url-rule audit-default-enable
Ruijie(cont-plcy-config)# end
```

【检验方法】 ● 使用 show running-config 命令可以查看配置状态。

交换 URL 规则的优先级

【配置方法】 ● 交换策略组 policyA 内 URL 访问控制规则 10 和规则 20 的优先级。

```
Ruijie# configure terminal
Ruijie(config)# content-policy policyA
Ruijie(cont-plcy-config)# url-rule priority-swap 10 20
Ruijie(cont-plcy-config)# end
```

【检验方法】 ● 使用 show running-config 命令可以查看配置状态。

配置 URL 审计优化

【配置方法】 ● 开启只审计 HTTP 的 GET。

```
Ruijie# configure terminal
Ruijie(config)# url-audit only-get
Ruijie(config)#end
```

● 配置符合默认正则表达式（.*=.*&.*=.*）的 URL 访问不审计。

```
Ruijie# configure terminal
Ruijie(config)# url-audit except-regexp
Ruijie(config)# end
```

● 配置图片等后缀的 URL 访问不审计。

```
Ruijie# configure terminal
Ruijie(config)# url-audit except-postfix
Ruijie(config)# end
```

● 配置指定 60s 内，同一个 IP 的重复 URL 访问不审计以及从该 URL 页面点开的链接也不审计。

```
Ruijie# configure terminal
Ruijie(config)# url-audit optimize-cache 60
Ruijie(config)# end
```

- 先配置 URL 规则，再开启 URL 宽松白名单功能。

```
Ruijie# configure terminal
Ruijie(config)# content-policy policyA
Ruijie(cont-plcy-config)# url-rule 2 url-object url-objA time-range any action permit audit
Ruijie(cont-plcy-config)# exit
Ruijie(config)#url-rule apply-referer
Ruijie(config)#end
```

【检验方法】

- 使用 show running-config 命令可以查看配置状态。

配置 URL 过滤提示页面显示的内容

【配置方法】

- 配置 URL 过滤提示页面显示的信息：

```
Ruijie# configure terminal
Ruijie(config)# url-filter-notice display 您访问的网站已被禁止，请与管理员联系！
Ruijie(config)#end
```

【检验方法】

- 使用 show running-config 命令可以查看配置状态。

常见错误

- 规则 id 重复导致配置失败。
- 规则引用的对象未存在导致规则不生效。
- 规则优先级未理清导致实际审计结果与预期有差异。

8.5.7 配置 URL 重定向规则

配置效果

- 向内容审计策略组中添加 URL 重定向规则。
- 交换 URL 重定向规则的优先级。

注意事项

- URL 重定向规则的生效状态取决于引用的时间对象是否生效、所属的策略组是否关联有效用户。
- 同一个策略组内的规则优先级为后配先生效。

配置方法

配置 URL 重定向规则

- 必须配置。

交换 URL 重定向规则的优先级

- 可选配置。若需要交换 URL 重定向规则的优先级则可配置。

检验方法

使用 show running-config 命令可以查看配置状态。

相关命令

配置 URL 规则

【命令格式】 **url-redirect-rule** *rule-id* **time-range** *time-name* **from** *url-1* **to** *url-2* [**comment** *comment-string*]

【参数说明】 *rule-id*：规则的 ID 标识，取值范围（1~200）。规则容量为 200。

time-name：代表规则生效时间段的时间对象名。

url-1：需要重定向的 url 地址。

url-2：重定向后的 url 地址。

comment-string：该规则的描述。

【命令模式】 内容审计策略组配置模式

【使用指导】 1：规则的 rule-id 在同一个内容审计策略组中不允许重复，在不同的内容审计策略组中允许重复。

2：一个内容审计策略组中的 URL 重定向规则都有相应的优先级，最后配的那条规则优先级最高。

3：规则所关联的 time-name 可以不存在，此时规则不生效。

4：删除 URL 重定向规则可使用命令 **no url-redirect-rule** *rule-id*。

删除策略组下所有 URL 重定向规则

【命令格式】 **url-redirect-rule delete-all**

【参数说明】 -

【命令模式】 内容审计策略组配置模式

【使用指导】 只能删除当前策略组下的所有 URL 重定向规则，不影响其它策略组。

交换 URL 重定向规则的优先级

【命令格式】 **url-redirect-rule priority-swap** *rule-id1 rule-id2*

【参数说明】 *rule-id1*：待交换优先级的规则 1 的 ID。

rule-id2：待交换优先级的规则 2 的 ID。

【命令模式】 内容审计策略组配置模式

【使用指导】 交换优先级命令是用于对调两条访问控制规则的优先级，运行该命令后，show running 中可以看到两个规则的排序发生了变化，但 show running 不会出现该命令。

配置举例

↘ 配置 URL 重定向规则

【配置方法】

- 为内容审计策略组 policyA 添加一个 URL 重定向规则 将 www.sina.com.cn 重定向到 www.ruijie.com.cn。

```
Ruijie# configure terminal
Ruijie(config)# content-policy policyA
Ruijie(cont-plcy-config)# url-redirect-rule 2 time-range any from www.sina.com.cn to
www.ruijie.com.cn comment sina-redirect
Ruijie(cont-plcy-config)# end
```

- 删除策略组 policyA 中的所有 URL 重定向规则。

```
Ruijie# configure terminal
Ruijie(config)# content-policy policyA
Ruijie(cont-plcy-config)# url-redirect-rule delete-all
Ruijie(cont-plcy-config)# end
```

【检验方法】

- 使用 show running-config 命令可以查看配置状态。

↘ 交换 URL 重定向规则的优先级

【配置方法】

- 交换策略组 policyA 内 URL 重定向规则 10 和规则 20 的优先级。

```
Ruijie# configure terminal
Ruijie(config)# content-policy policyA
Ruijie(cont-plcy-config)# url-redirect-rule priority-swap 10 20
Ruijie(cont-plcy-config)# end
```

【检验方法】

- 使用 show running-config 命令可以查看配置状态。

常见错误

- 规则 id 重复导致配置失败。
- 规则引用的对象未存在导致规则不生效。

8.5.8 配置 IM 规则

配置效果

- 启用 IM 默认审计功能。
- 向内容审计策略组中添加 IM 规则。
- 交换 IM 规则的优先级。

注意事项

- IM 规则的生效状态取决于引用的内容对象是否存在、时间对象是否生效、所属的策略组是否关联有效用户。
- 同一个策略组内的规则优先级为后配先生效。

配置方法

配置 IM 规则

- 必须配置。

配置 IM 默认审计

- 可选配置。若需要开启默认审计功能则可配置。

交换 IM 规则的优先级

- 可选配置。若需要交换 IM 规则的优先级则可配置。

检验方法

使用 show running-config 命令可以查看配置状态。

相关命令

配置 IM 规则的公共部分

【命令格式】 **im-rule** *rule-id* **time-range** *time-name* **action** { **permit** | **deny** } [**audit**] [**comment** *comment-string*]

【参数说明】 *rule-id*：规则的 ID 标识，取值范围（1~200）。

time-name：代表规则生效时间段的时间对象名。

comment-string：该规则的描述。

【命令模式】 内容审计策略组配置模式

【使用指导】 1：规则的 rule-id 在同一个内容审计策略组中不允许重复，在不同的内容审计策略组中允许重复。

2：一个内容审计策略组中的访问控制规则都有相应的优先级，最后配的那条规则优先级最高。

3：规则所关联的 time-name、content-object-name 可以不存在，此时规则不生效。

4：删除 IM 规则可使用命令 **no im-rule** *rule-id*。

配置 IM 规则的进一步描述

【命令格式】 **im-rule** *rule-id* **im-type** *im-name* [**relation** { **and** | **or** } [**account** *content-object-name1*] [**message** *content-object-name2*]]

【参数说明】 *rule-id*：规则的 ID 标识，取值范围（1~200）。规则容量为 200。

im-name：指明审计的 IM 软件。im-name 表示特定的 string 字符串。例如 string 字符串为”qq”表示本规则只审计 QQ 软件；string 字符串为”qq,msn” 或”msn,qq” 表示本规则只审计 QQ 软件和 MSN 软件。

content-object-name1：IM 账号，缺失该项表示不用匹配该项。

content-object-name2：聊天记录，缺失该项表示不用匹配该项。

【命令模式】 内容审计策略组配置模式

【使用指导】 QQ 聊天为加密信息，目前不支持内容过滤审计（如果 im-name 为 QQ 则 message 不允许被配置）。

配置 IM 默认审计

【命令格式】 **im-rule audit-default-enable**

【参数说明】 -

【命令模式】 内容审计策略组配置模式

【使用指导】 1：默认审计只能在策略组名为_AUDIT_DEFAULT 的默认审计组内进行配置，在其它策略组内配置该命令则不生效。

2：关闭 IM 默认审计功能可使用命令 **no im-rule audit-default-enable**。

删除策略组下所有 IM 规则

【命令格式】 **im-rule delete-all**

【参数说明】 -

【命令模式】 内容审计策略组配置模式

【使用指导】 只能删除当前策略组下的所有 IM 规则，不影响其它策略组。

交换 IM 规则的优先级

【命令格式】 **im-rule priority-swap** *rule-id1 rule-id2*

【参数说明】 *rule-id1*：待交换优先级的规则 1 的 ID。

rule-id2：待交换优先级的规则 2 的 ID。

【命令模式】 内容审计策略组配置模式

【使用指导】 交换优先级命令是用于对调两条访问控制规则的优先级，运行该命令后，show running 中可以看到两个规则的排序发生了变化，但 show running 不会出现该命令。

配置举例

配置 IM 规则

【配置方法】

- 为内容审计策略组 policyA 添加一个 MSN 访问审计规则，允许用户进行 MSN 聊天，并且需要审计该用户的某些特定账号 accountA 或特定聊天关键字 keyA 信息。

```
Ruijie# configure terminal
Ruijie(config)# content-policy policyA
Ruijie(cont-plcy-config)# im-rule 2 time-range any action permit audit comment PermitUserAMSN
Ruijie(cont-plcy-config)# im-rule 2 im-type msn relation or  account accountA message keyA
Ruijie(cont-plcy-config)# end
```

- 删除策略组 policyA 中的所有 IM 规则。

```
Ruijie# configure terminal
Ruijie(config)# content-policy policyA
```

```
Ruijie(cont-plcy-config)# im-rule delete-all
Ruijie(cont-plcy-config)# end
```

【检验方法】 ● 使用 show running-config 命令可以查看配置状态。

配置 IM 默认审计

【配置方法】 ● 启用 IM 默认审计。

```
Ruijie# configure terminal
Ruijie(config)# content-policy _AUDIT_DEFAULT
Ruijie(cont-plcy-config)# im-rule audit-default-enable
Ruijie(cont-plcy-config)# end
```

【检验方法】 ● 使用 show running-config 命令可以查看配置状态。

交换 IM 规则的优先级

【配置方法】 ● 交换策略组 policyA 内 IM 访问控制规则 10 和规则 20 的优先级。

```
Ruijie# configure terminal
Ruijie(config)# content-policy policyA
Ruijie(cont-plcy-config)# im-rule priority-swap 10 20
Ruijie(cont-plcy-config)# end
```

【检验方法】 ● 使用 show running-config 命令可以查看配置状态。

常见错误

- 规则 id 重复导致配置失败。
- 未先配置规则的公共部分，直接配置规则的进一步说明导致配置失败。
- 规则引用的对象未存在导致规则不生效。
- 规则优先级未理清导致实际审计结果与预期有差异。

8.5.9 配置 MAIL 规则

配置效果

- 启用 MAIL 默认审计功能。
- 向内容审计策略组中添加 MAIL 规则。
- 交换 MAIL 规则的优先级。

注意事项

- MAIL 规则的生效状态取决于引用的内容对象是否存在、时间对象是否生效、所属的策略组是否关联有效用户。
- 同一个策略组内的规则优先级为后配先生效。

配置方法

配置 MAIL 规则

- 必须配置。

配置 MAIL 默认审计

- 可选配置。若需要开启默认审计功能则可配置。

交换 MAIL 规则的优先级

- 可选配置。若需要交换 MAIL 规则的优先级则可配置。

检验方法

使用 show running-config 命令可以查看配置状态。

相关命令

配置 MAIL 规则的公共部分

【命令格式】 **mail-rule** *rule-id* **time-range** *time-name* [**direction** { **in** | **out** | **double** }] **action** { **permit** | **deny** } [**audit**] [**comment** *comment-string*]

【参数说明】 *rule-id*：规则的 ID 标识，取值范围（1~200）。规则容量为 200。

time-name：代表规则生效时间段的时间对象名。

comment-string：该规则的描述。

【命令模式】 内容审计策略组配置模式

【使用指导】 1：规则的 rule-id 在同一个内容审计策略组中不允许重复，在不同的内容审计策略组中允许重复。

2：一个内容审计策略组中的访问控制规则都有相应的优先级，最后配的那条规则优先级最高。

3：规则所关联的 time-name 可以不存在，此时规则不生效。

4：删除 MAIL 规则可使用命令 **no mail-rule** *rule-id*。

配置 MAIL 规则的进一步描述

【命令格式】 **mail-rule** *rule-id* **relation** { **and** | **or** } [**from** *content-object-name1*] [**to** *content-object-name2*] [**subject** *content-object-name3*] [**body** *content-object-name4*] [**attachment-name** *content-object-name5*] [**mail-size** { **greater** | **greater-equal** | **less** | **less-equal** } *file-size*]

【参数说明】 *rule-id*：规则的 ID 标识，取值范围（1~200）。

content-object-name1：发件人关键字，缺失该项表示不用匹配该项。
content-object-name2：收件人关键字，缺失该项表示不用匹配该项。
content-object-name3：邮件标题关键字，缺失该项表示不用匹配该项。
content-object-name4：邮件内容关键字，缺失该项表示不用匹配该项。
content-object-name5：附件名称关键字，缺失该项表示不用匹配该项。
file-size：文件大小值，为整数，单位为 Kbytes。

【命令模式】 内容审计策略组配置模式

【使用指导】 1：规则配置为阻断时，relation 中实际只有 or 关系才会有效。
2：规则所关联的 content-object-name 可以不存在，此时规则不生效。

配置 MAIL 默认审计

【命令格式】 **mail-rule audit-default-enable**

【参数说明】 -

【命令模式】 内容审计策略组配置模式

【使用指导】 1：默认审计只能在策略组名为_AUDIT_DEFAULT 的默认审计组内进行配置，在其它策略组内配置该命令则不生效。
2：关闭 MAIL 默认审计功能可使用命令 **no mail-rule audit-default-enable**。

删除策略组下所有 MAIL 规则

【命令格式】 **mail-rule delete-all**

【参数说明】 -

【命令模式】 内容审计策略组配置模式

【使用指导】 只能删除当前策略组下的所有 MAIL 规则，不影响其它策略组。

交换 MAIL 规则的优先级

【命令格式】 **mail-rule priority-swap** *rule-id1 rule-id2*

【参数说明】 *rule-id1*：待交换优先级的规则 1 的 ID。
rule-id2：待交换优先级的规则 2 的 ID。

【命令模式】 内容审计策略组配置模式

【使用指导】 交换优先级命令是用于对调两条访问控制规则的优先级，运行该命令后，show running 中可以看到两个规则的排序发生了变化，但 show running 不会出现该命令。

配置举例

配置 MAIL 规则

【配置方法】
- 为内容审计策略组 policyA 添加 MAIL 访问控制规则，允许所有用户发送邮件，对发件人匹配 OBJ-F 关键字，或者主题匹配 OBJ-S 关键字，或者邮件大小小于 20000Kb 的邮件进行审计。

```
Ruijie# configure terminal
Ruijie(config)# content-policy policyA
Ruijie(cont-plcy-config)# mail-rule 1 time-range any action permit audit comment mail-audit-1
Ruijie(cont-plcy-config)# mail-rule 1 relation or from OBJ-F subject OBJ-S mail-size less 20000
```

```
Ruijie(cont-plcy-config)# end
```

- 删除策略组 policyA 中的所有 MAIL 规则。

```
Ruijie# configure terminal
Ruijie(config)# content-policy policyA
Ruijie(cont-plcy-config)# mail-rule delete-all
Ruijie(cont-plcy-config)# end
```

【检验方法】
- 使用 show running-config 命令可以查看配置状态。

配置 MAIL 默认审计

【配置方法】
- 启用 MAIL 默认审计。

```
Ruijie# configure terminal
Ruijie(config)# content-policy _AUDIT_DEFAULT
Ruijie(cont-plcy-config)# mail-rule audit-default-enable
Ruijie(cont-plcy-config)# end
```

【检验方法】
- 使用 show running-config 命令可以查看配置状态。

交换 MAIL 规则的优先级

【配置方法】
- 交换策略组 policyA 内 MAIL 访问控制规则 10 和规则 20 的优先级。

```
Ruijie# configure terminal
Ruijie(config)# content-policy policyA
Ruijie(cont-plcy-config)# mail-rule priority-swap 10 20
Ruijie(cont-plcy-config)# end
```

【检验方法】
- 使用 show running-config 命令可以查看配置状态。

常见错误

- 规则 id 重复导致配置失败。
- 未先配置规则的公共部分，直接配置规则的进一步说明导致配置失败。
- 规则引用的对象未存在导致规则不生效。
- 规则优先级未理清导致实际审计结果与预期有差异。

8.5.10 配置 WEB-BBS 规则

配置效果

- 启用 WEB-BBS 默认审计功能。
- 向内容审计策略组中添加 WEB-BBS 规则。
- 交换 WEB-BBS 规则的优先级。

注意事项

- WEB-BBS 规则的生效状态取决于引用的内容对象是否存在、时间对象是否生效、所属的策略组是否关联有效用户。
- 同一个策略组内的规则优先级为后配先生效。

配置方法

配置 WEB-BBS 规则

- 必须配置。

配置 WEB-BBS 默认审计

- 可选配置。若需要开启默认审计功能则可配置。

交换 WEB-BBS 规则的优先级

- 可选配置。若需要交换 WEB-BBS 规则的优先级则可配置。

检验方法

使用 show running-config 命令可以查看配置状态。

相关命令

配置 WEB-BBS 规则

【命令格式】 **web-bbs-rule** *rule-id* **time-range** *time-name* [**content** *content-object-name*] **action** { **permit** | **deny** } [**audit**] [**comment** *comment-string*]

【参数说明】 *rule-id*：规则的 ID 标识，取值范围（1~200）。规则容量为 200。

time-name：代表规则生效时间段的时间对象名。

content-object-name：规则用到的内容对象名。

comment-string：该规则的描述。

【命令模式】 内容审计策略组配置模式

【使用指导】 1：规则的 rule-id 在同一个内容审计策略组中不允许重复，在不同的内容审计策略组中允许重复。

2：一个内容审计策略组中的访问控制规则都有相应的优先级，最后配的那条规则优先级最高。

3：规则所关联的 time-name、content-object-name 可以不存在，此时规则不生效。

4：删除 WEB-BBS 访问控制规则可使用命令 **no web-bbs-rule** *rule-id*。

配置 WEB-BBS 默认审计

【命令格式】 **web-bbs-rule audit-default-enable**

【参数说明】 -

【命令模式】 内容审计策略组配置模式

【使用指导】 1：默认审计只能在策略组名为_AUDIT_DEFAULT 的默认审计组内进行配置，在其它策略组内配置该命令则不生效。

2：关闭 WEB-BBS 默认审计功能可使用命令 **no web-bbs-rule audit-default-enable**。

删除策略组下所有 WEB-BBS 规则

【命令格式】 **web-bbs-rule delete-all**

【参数说明】 -

【命令模式】 内容审计策略组配置模式

【使用指导】 只能删除当前策略组下的所有 WEB-BBS 规则，不影响其它策略组。

交换 WEB-BBS 规则的优先级

【命令格式】 **web-bbs-rule priority-swap** *rule-id1 rule-id2*

【参数说明】 *rule-id1*：待交换优先级的规则 1 的 ID。

rule-id2：待交换优先级的规则 2 的 ID。

【命令模式】 内容审计策略组配置模式

【使用指导】 交换优先级命令是用于对调两条访问控制规则的优先级，运行该命令后，show running 中可以看到两个规则的排序发生了变化，但 show running 不会出现该命令。

配置举例

配置 WEB-BBS 规则

【配置方法】

- 为内容审计策略组 policyA 添加一个 WEB-BBS 访问审计规则，过滤用户进行 WEB-BBS 内容浏览，并且需要审计该浏览信息。

```
Ruijie# configure terminal
Ruijie(config)# content-policy policyA
Ruijie(cont-plcy-config)# web-bbs-rule 2 time-range any content keyword-group action deny audit
comment DenyInvalidBBS
Ruijie(cont-plcy-config)# end
```

- 删除策略组 policyA 中的所有 WEB-BBS 规则。

```
Ruijie# configure terminal
Ruijie(config)# content-policy policyA
Ruijie(cont-plcy-config)# web-bbs-rule delete-all
Ruijie(cont-plcy-config)# end
```

【检验方法】

- 使用 show running-config 命令可以查看配置状态。

配置 WEB-BBS 默认审计

【配置方法】
- 启用 WEB-BBS 默认审计。

```
Ruijie# configure terminal
Ruijie(config)# content-policy _AUDIT_DEFAULT
Ruijie(cont-plcy-config)# web-bbs-rule audit-default-enable
Ruijie(cont-plcy-config)# end
```

【检验方法】
- 使用 show running-config 命令可以查看配置状态。

交换 WEB-BBS 规则的优先级

【配置方法】
- 交换策略组 policyA 内 WEB-BBS 访问控制规则 10 和规则 20 的优先级。

```
Ruijie# configure terminal
Ruijie(config)# content-policy policyA
Ruijie(cont-plcy-config)# web-bbs-rule priority-swap 10 20
Ruijie(cont-plcy-config)# end
```

【检验方法】
- 使用 show running-config 命令可以查看配置状态。

常见错误

- 规则 id 重复导致配置失败。
- 规则引用的对象未存在导致规则不生效。
- 规则优先级未理清导致实际审计结果与预期有差异。

8.5.11 配置 WEB-MAIL 规则

配置效果

- 启用 WEB-MAIL 默认审计功能。
- 向内容审计策略组中添加 WEB-MAIL 规则。
- 交换 WEB-MAIL 规则的优先级。

注意事项

- WEB-MAIL 规则的生效状态取决于引用的内容对象是否存在、时间对象是否生效、所属的策略组是否关联有效用户。
- 同一个策略组内的规则优先级为后配先生效。

配置方法

配置 WEB-MAIL 规则

- 必须配置。

配置 WEB-MAIL 默认审计

- 可选配置。若需要开启默认审计功能则可配置。

交换 WEB-MAIL 规则的优先级

- 可选配置。若需要交换 WEB-MAIL 规则的优先级则可配置。

检验方法

使用 show running-config 命令可以查看配置状态。

相关命令

配置 WEB-MAIL 规则的公共部分

【命令格式】 **web-mail-rule** *rule-id* **time-range** *time-name* [**direction** { **in** | **out** | **double** }] **action** { **permit** | **deny** } **audit** [**comment** *comment-string*]

【参数说明】 *rule-id*：规则的 ID 标识，取值范围（1~200）。规则容量为 200。

time-name：代表规则生效时间段的时间对象名。

comment-string：该规则的描述。

【命令模式】 内容审计策略组配置模式

【使用指导】 1：规则的 rule-id 在同一个内容审计策略组中不允许重复，在不同的内容审计策略组中允许重复。

2：一个内容审计策略组中的访问控制规则都有相应的优先级，最后配的那条规则优先级最高。

3：规则所关联的 time-name 可以不存在，此时规则不生效。

4：删除 WEB-MAIL 规则可使用命令 **no web-mail-rule** *rule-id*。

配置 WEB-MAIL 规则的进一步描述

【命令格式】 **web-mail-rule** *rule-id* **relation** { **and** | **or** } [**from** *content-object-name1*] [**to** *content-object-name2*] [**subject** *content-object-name3*] [**body** *content-object-name4*] [**attachment-name** *content-object-name5*]

【参数说明】 *rule-id*：规则的 ID 标识，取值范围（1~200）。

content-object-name1：发件人关键字，缺失该项表示不用匹配该项。

content-object-name2：收件人关键字，缺失该项表示不用匹配该项。

content-object-name3：邮件标题关键字，缺失该项表示不用匹配该项。

content-object-name4：邮件内容关键字，缺失该项表示不用匹配该项。

content-object-name5：附件名称关键字，缺失该项表示不用匹配该项。

【命令模式】 内容审计策略组配置模式

【使用指导】 1：规则配置为阻断时，relation 中实际只有 or 关系才会有效。

2：规则所关联的 content-object-name 可以不存在，此时规则不生效。

配置 WEB-MAIL 默认审计

【命令格式】 **web-mail-rule audit-default-enable**

【参数说明】 -

【命令模式】 内容审计策略组配置模式

【使用指导】 1：默认审计只能在策略组名为_AUDIT_DEFAULT 的默认审计组内进行配置，在其它策略组内配置该命令则不生效。

2：关闭 WEB-MAIL 默认审计功能可使用命令 **no web-mail-rule audit-default-enable**。

删除策略组下所有 WEB-MAIL 规则

【命令格式】 **web-mail-rule delete-all**

【参数说明】 -

【命令模式】 内容审计策略组配置模式

【使用指导】 只能删除当前策略组下的所有 WEB-MAIL 规则，不影响其它策略组。

交换 WEB-MAIL 规则的优先级

【命令格式】 **web-mail-rule priority-swap** *rule-id1 rule-id2*

【参数说明】 *rule-id1*：待交换优先级的规则 1 的 ID。

rule-id2：待交换优先级的规则 2 的 ID。

【命令模式】 内容审计策略组配置模式

【使用指导】 交换优先级命令是用于对调两条访问控制规则的优先级，运行该命令后，show running 中可以看到两个规则的排序发生了变化，但 show running 不会出现该命令。

配置举例

配置 WEB-MAIL 规则

【配置方法】

- 为内容审计策略组 policyA 添加 WEB-MAIL 访问控制规则，允许用户发送 WEB 邮件，对发件人匹配 OBJ-F 关键字，或者主题匹配 OBJ-S 关键字。

```
Ruijie# configure terminal
Ruijie(config)# content-policy policyA
Ruijie(cont-plcy-config)# web-mail-rule 1 time-range any action permit audit comment mail-audit-1
Ruijie(cont-plcy-config)# web-mail-rule 1 relation or from OBJ-F subject OBJ-S
Ruijie(cont-plcy-config)# end
```

- 删除策略组 policyA 中的所有 WEB-MAIL 规则。

```
Ruijie# configure terminal
Ruijie(config)# content-policy policyA
Ruijie(cont-plcy-config)# web-mail-rule delete-all
Ruijie(cont-plcy-config)# end
```

【检验方法】

- 使用 show running-config 命令可以查看配置状态。

配置 WEB-MAIL 默认审计

【配置方法】
- 启用 WEB-MAIL 默认审计。

```
Ruijie# configure terminal
Ruijie(config)# content-policy _AUDIT_DEFAULT
Ruijie(cont-plcy-config)# web-mail-rule audit-default-enable
Ruijie(cont-plcy-config)# end
```

【检验方法】
- 使用 show running-config 命令可以查看配置状态。

交换 WEB-MAIL 规则的优先级

【配置方法】
- 交换策略组 policyA 内 WEB-MAIL 访问控制规则 10 和规则 20 的优先级。

```
Ruijie# configure terminal
Ruijie(config)# content-policy policyA
Ruijie(cont-plcy-config)# web-mail-rule priority-swap 10 20
Ruijie(cont-plcy-config)# end
```

【检验方法】
- 使用 show running-config 命令可以查看配置状态。

常见错误

- 规则 id 重复导致配置失败。
- 未先配置规则的公共部分，直接配置规则的进一步说明导致配置失败。
- 规则引用的对象未存在导致规则不生效。
- 规则优先级未理清导致实际审计结果与预期有差异。

8.5.12 配置 WEB-SEARCH 规则

配置效果

- 启用 WEB-SEARCH 默认审计功能。
- 向内容审计策略组中添加 WEB-SEARCH 规则。
- 交换 WEB-SEARCH 规则的优先级。

注意事项

- WEB-SEARCH 规则的生效状态取决于引用的内容对象是否存在、时间对象是否生效、所属的策略组是否关联有效用户。
- 同一个策略组内的规则优先级为后配先生效。

配置方法

配置 WEB-SEARCH 规则

- 必须配置。

配置 WEB-SEARCH 默认审计

- 可选配置。若需要开启默认审计功能则可配置。

交换 WEB-SEARCH 规则的优先级

- 可选配置。若需要交换 WEB-SEARCH 规则的优先级则可配置。

检验方法

使用 show running-config 命令可以查看配置状态。

相关命令

配置 WEB-SEARCH 规则

【命令格式】 **web-search-rule** *rule-id* **time-range** *time-name* [**content** *content-object-name*] **action** { **permit** | **deny** } [**audit**] [**comment** *comment-string*]

【参数说明】 *rule-id*：规则的 ID 标识，取值范围（1~200）。规则容量为 200。

time-name：代表规则生效时间段的时间对象名。

content-object-name：规则用到的内容对象名。

comment-string：该规则的描述。

【命令模式】 内容审计策略组配置模式

【使用指导】 1：规则的 rule-id 在同一个内容审计策略组中不允许重复，在不同的内容审计策略组中允许重复。

2：一个内容审计策略组中的访问控制规则都有相应的优先级，最后配的那条规则优先级最高。

3：规则所关联的 time-name、content-object-name 可以不存在，此时规则不生效。

4：删除 WEB-SEARCH 访问控制规则可使用命令 **no web-search-rule** *rule-id*。

配置 WEB-SEARCH 默认审计

【命令格式】 **web-search-rule audit-default-enable**

【参数说明】 -

【命令模式】 内容审计策略组配置模式

【使用指导】 1：默认审计只能在策略组名为_AUDIT_DEFAULT 的默认审计组内进行配置，在其它策略组内配置该命令则不生效。

2：关闭 WEB-SEARCH 默认审计功能可使用命令 **no web-search-rule audit-default-enable**。

删除策略组下所有 WEB-SEARCH 规则

【命令格式】 **web-search-rule delete-all**

【参数说明】 -

【命令模式】 内容审计策略组配置模式

【使用指导】 只能删除当前策略组下的所有 WEB-SEARCH 规则，不影响其它策略组。

交换 WEB-SEARCH 规则的优先级

【命令格式】 **web-search-rule priority-swap** *rule-id1 rule-id2*

【参数说明】 *rule-id1*：待交换优先级的规则 1 的 ID。

rule-id2：待交换优先级的规则 2 的 ID。

【命令模式】 内容审计策略组配置模式

【使用指导】 交换优先级命令是用于对调两条访问控制规则的优先级，运行该命令后，show running 中可以看到两个规则的排序发生了变化，但 show running 不会出现该命令。

配置举例

配置 WEB-SEARCH 规则

【配置方法】

- 为内容审计策略组 policyA 添加一个 WEB-SEARCH 访问审计规则，对用户搜索包含 keyword-group 内容对象关键字的行为进行过滤，并且需要审计该搜索信息。

```
Ruijie# configure terminal
Ruijie(config)# content-policy policyA
Ruijie(cont-plcy-config)# web-search-rule 2 time-range any content keyword-group action deny audit
comment DenyInvalidSearch
Ruijie(cont-plcy-config)# end
```

- 删除策略组 policyA 中的所有 WEB-SEARCH 规则。

```
Ruijie# configure terminal
Ruijie(config)# content-policy policyA
Ruijie(cont-plcy-config)# web-search-rule delete-all
Ruijie(cont-plcy-config)# end
```

【检验方法】

- 使用 show running-config 命令可以查看配置状态。

配置 WEB-SEARCH 默认审计

【配置方法】

- 启用 WEB-SEARCH 默认审计。

```
Ruijie# configure terminal
Ruijie(config)# content-policy _AUDIT_DEFAULT
Ruijie(cont-plcy-config)# web-search-rule audit-default-enable
Ruijie(cont-plcy-config)# end
```

【检验方法】

- 使用 show running-config 命令可以查看配置状态。

↘ 交换 WEB-SEARCH 规则的优先级

【配置方法】 ● 交换策略组 policyA 内 WEB-SEARCH 访问控制规则 10 和规则 20 的优先级。

```
Ruijie# configure terminal
Ruijie(config)# content-policy policyA
Ruijie(cont-plcy-config)# web-search-rule priority-swap 10 20
Ruijie(cont-plcy-config)# end
```

【检验方法】 ● 使用 show running-config 命令可以查看配置状态。

常见错误

- 规则 id 重复导致配置失败。
- 规则引用的对象未存在导致规则不生效。
- 规则优先级未理清导致实际审计结果与预期有差异。

8.5.13 配置虚拟身份规则

配置效果

- 启用虚拟身份默认审计功能。

注意事项

- -

配置方法

↘ 配置虚拟身份默认审计

- 必须配置。若需要开启默认审计功能则可配置。

检验方法

使用 show running-config 命令可以查看配置状态。

相关命令

↘ 配置 IM 默认审计

【命令格式】 **vid-rule audit-default-enable**

【参数说明】 -

【命令模式】 内容审计策略组配置模式

【使用指导】 1：默认审计只能在策略组名为_AUDIT_DEFAULT 的默认审计组内进行配置，在其它策略组内无该命令。

2：关闭虚拟身份默认审计功能可使用命令 **no vid-rule audit-default-enable**。

配置举例

↘ 配置虚拟身份默认审计

【配置方法】

- 启用 IM 默认审计。

```
Ruijie# configure terminal
Ruijie(config)# content-policy _AUDIT_DEFAULT
Ruijie(cont-plcy-config)# vid-rule audit-default-enable
Ruijie(cont-plcy-config)# end
```

【检验方法】

- 使用 show running-config 命令可以查看配置状态。

常见错误

- -

8.5.14 配置 QQ 聊天内容规则

配置效果

- 启用 QQ 聊天内容默认审计功能。
- 向内容审计策略组中添加 QQ 聊天内容审计规则，即 PLUGIN 规则。
- 交换 PLUGIN 规则的优先级。
- 设置终端下载插件方法

注意事项

- PLUGIN 规则的生效状态取决于引用的内容对象是否存在、时间对象是否生效、所属的策略组是否关联有效用户。
- 同一个策略组内的规则优先级为后配先生效。
- 对同一设备，终端只支持一种下载方法。

配置方法

配置 PLUGIN 规则

- 必须配置。

配置 PLUGIN 默认审计

- 可选配置。若需要开启默认审计功能则可配置。

交换 PLUGIN 规则的优先级

- 可选配置。若需要交换 PLUGIN 规则的优先级则可配置。

终端下载插件方法

- 可选配置。若需要配置内网中终端下载插件的服务器或从设备上下载插件使用的协议、端口则可进行配置

检验方法

使用 show running-config 命令可以查看配置状态。

相关命令

配置 PLUGIN 规则

【命令格式】 **plugin-rule** *rule-id* **time-range** *time-name* [**content** *content-object-name*] **action** { **permit** | **deny** } [**audit**] [**comment** *comment-string*]

【参数说明】 *rule-id*：规则的 ID 标识，取值范围（1~200）。规则容量为 200。

time-name：代表规则生效时间段的时间对象名。

content-object-name：规则用到的内容对象名。

comment-string：该规则的描述。

【命令模式】 内容审计策略组配置模式

【使用指导】 1：规则的 rule-id 在同一个内容审计策略组中不允许重复，在不同的内容审计策略组中允许重复。

2：一个内容审计策略组中的访问控制规则都有相应的优先级，最后配的那条规则优先级最高。

3：规则所关联的 time-name、content-object-name 可以不存在，此时规则不生效。

4：删除 PLUGIN 访问控制规则可使用命令 **no plugin-rule** *rule-id*。

配置 PLUGIN 默认审计

【命令格式】 **plugin-rule audit-default-enable**

【参数说明】 -

【命令模式】 内容审计策略组配置模式

【使用指导】 1：默认审计只能在策略组名为_AUDIT_DEFAULT 的默认审计组内进行配置，在其它策略组内配置该命令则不生效。

2：关闭 PLUGIN 默认审计功能可使用命令 **no plugin-rule audit-default-enable**。

删除策略组下所有 PLUGIN 规则

【命令格式】 **plugin-rule delete-all**

【参数说明】 -

【命令模式】 内容审计策略组配置模式

【使用指导】 只能删除当前策略组下的所有 PLUGIN 规则，不影响其它策略组。

交换 PLUGIN 规则的优先级

【命令格式】 **plugin-rule priority-swap** *rule-id1 rule-id2*

【参数说明】 *rule-id1*：待交换优先级的规则 1 的 ID。

rule-id2：待交换优先级的规则 2 的 ID。

【命令模式】 内容审计策略组配置模式

【使用指导】 交换优先级命令是用于对调两条访问控制规则的优先级，运行该命令后，show running 中可以看到两个规则的排序发生了变化，但 show running 不会出现该命令。

配置终端下载插件使用的协议、端口

【命令格式】 **plugin-config set-download-protol protol** *protolname* **port** *portnum*

【参数说明】 *protolname*：内网终端从设备上下载插件使用的协议(仅支持 http 与 https)

portnum：内网终端从设备上下载插件使用的端口

【命令模式】 全局模式

【使用指导】 运行该命令后，show running 中可以看到内网终端从设备上下载插件使用的协议及端口。

配置终端下载插件的 URL 地址

【命令格式】 **plugin-config set-download-url** *urlstring*

【参数说明】 *urlstring*：内网终端下载插件使用的 url 地址。

【命令模式】 全局模式

【使用指导】 运行该命令后，show running 中可以看到内网终端下载插件的 url 地址。

配置举例

配置 PLUGIN 规则

【配置方法】

- 删除策略组 policyA 中的所有 PLUGIN 规则。

```
Ruijie# configure terminal
Ruijie(config)# content-policy policyA
Ruijie(cont-plcy-config)# plugin-rule delete-all
Ruijie(cont-plcy-config)# end
```

【检验方法】

- 使用 show running-config 命令可以查看配置状态。

配置 PLUGIN 默认审计

【配置方法】

- 启用 PLUGIN 默认审计。

```
Ruijie# configure terminal
Ruijie(config)# content-policy _AUDIT_DEFAULT
Ruijie(cont-plcy-config)# plugin-rule audit-default-enable
```

```
Ruijie(cont-plcy-config)# end
```

【检验方法】 ● 使用 show running-config 命令可以查看配置状态。

交换 PLUGIN 规则的优先级

【配置方法】 ● 交换策略组 policyA 内 PLUGIN 访问控制规则 10 和规则 20 的优先级。

```
Ruijie# configure terminal
Ruijie(config)# content-policy policyA
Ruijie(cont-plcy-config)# plugin-rule priority-swap 10 20
Ruijie(cont-plcy-config)# end
```

【检验方法】 ● 使用 show running-config 命令可以查看配置状态。

配置黑名单

【配置方法】 ● 配置黑名单

```
Ruijie# configure terminal
Ruijie(config)#content-policy _TOP_PRIORITY
Ruijie(cont-plcy-config) plugin-rule 1 time-range any action deny audit comment testcomment
Ruijie(cont-plcy-config)#end
```

【检验方法】 ● 使用 show running-config 命令可以查看配置状态。

配置白名单

【配置方法】 ● 配置白名单

```
Ruijie# configure terminal
Ruijie(config)#content-policy _AUDIT_DEFAULT
Ruijie(cont-plcy-config)#plugin-rule audit-default-enable
Ruijie(cont-plcy-config)#end
Ruijie# configure terminal
Ruijie(config)#content-policy _TOP_PRIORITY
Ruijie(cont-plcy-config) plugin-rule 1 time-range any action permit audit comment testcomment
Ruijie(cont-plcy-config)#end
```

【检验方法】 ● 使用 show running-config 命令可以查看配置状态。

配置插件下载使用的协议与端口

【配置方法】 ● 配置内网终端使用 https 协议从设备上下载插件

```
Ruijie# configure terminal
Ruijie(config)# plugin-config set-download-protol protol https port 4430
Ruijie(cont-plcy-config)#end
```

【检验方法】 ● 使用 show running-config 命令可以查看配置状态。

配置内网终端从内网服务器上下载插件

【配置方法】 ● 配置内网终端从内网服务器上下载插件

```
Ruijie# configure terminal
Ruijie(config)# plugin-config set-downloa-url http://192.168.1.10/download/
Ruijie(cont-plcy-config)#end
```

【检验方法】
- 使用 show running-config 命令可以查看配置状态。

常见错误

- 规则 id 重复导致配置失败。
- 规则引用的对象未存在导致规则不生效。
- 规则优先级未理清导致实际审计结果与预期有差异。

8.5.15 配置外发文件规则

配置效果

- 启用外发文件默认审计功能。
- 向内容审计策略组中添加外发文件规则，即 POSTFILE 规则。
- 交换 POSTFILE 规则的优先级。

注意事项

- POSTFILE 规则的生效状态取决于引用的内容对象是否存在、时间对象是否生效、所属的策略组是否关联有效用户。
- 同一个策略组内的规则优先级为后配先生效。

配置方法

↘ 配置 POSTFILE 规则

- 必须配置。

↘ 配置 POSTFILE 默认审计

- 可选配置。若需要开启默认审计功能则可配置。

↘ 交换 POSTFILE 规则的优先级

- 可选配置。若需要交换 POSTFILE 规则的优先级则可配置。

检验方法

使用 show running-config 命令可以查看配置状态。

相关命令

配置 POSTFILE 规则

【命令格式】 **postfile-rule** *rule-id* **time-range** *time-name* [**content** *content-object-name*] **action** { **permit** | **deny** } [**audit**] [**comment** *comment-string*]

【参数说明】 *rule-id*：规则的 ID 标识，取值范围（1~200）。规则容量为 200。

time-name：代表规则生效时间段的时间对象名。

content-object-name：规则用到的内容对象名。

comment-string：该规则的描述。

【命令模式】 内容审计策略组配置模式

【使用指导】 1：规则的 rule-id 在同一个内容审计策略组中不允许重复，在不同的内容审计策略组中允许重复。

2：一个内容审计策略组中的访问控制规则都有相应的优先级，最后配的那条规则优先级最高。

3：规则所关联的 time-name、content-object-name 可以不存在，此时规则不生效。

4：删除 POSTFILE 访问控制规则可使用命令 **no postfile-rule** *rule-id*。

配置 POSTFILE 默认审计

【命令格式】 **postfile-rule audit-default-enable**

【参数说明】 -

【命令模式】 内容审计策略组配置模式

【使用指导】 1：默认审计只能在策略组名为_AUDIT_DEFAULT 的默认审计组内进行配置，在其它策略组内配置该命令则不生效。

2：关闭 POSTFILE 默认审计功能可使用命令 **no postfile-rule audit-default-enable**。

删除策略组下所有 POSTFILE 规则

【命令格式】 **postfile-rule delete-all**

【参数说明】 -

【命令模式】 内容审计策略组配置模式

【使用指导】 只能删除当前策略组下的所有 POSTFILE 规则，不影响其它策略组。

交换 POSTFILE 规则的优先级

【命令格式】 **postfile-rule priority-swap** *rule-id1 rule-id2*

【参数说明】 *rule-id1*：待交换优先级的规则 1 的 ID。

rule-id2：待交换优先级的规则 2 的 ID。

【命令模式】 内容审计策略组配置模式

【使用指导】 交换优先级命令是用于对调两条访问控制规则的优先级，运行该命令后，show running 中可以看到两个规则的排序发生了变化，但 show running 不会出现该命令。

配置举例

配置 POSTFILE 规则

【配置方法】
- 为内容审计策略组 policyA 添加一个 POSTFILE 审计规则，过滤用户进行外发文件，并且需要审计该行为。

```
Ruijie# configure terminal
Ruijie(config)# content-policy policyA
Ruijie(cont-plcy-config)# postfile-rule 2 time-range any content keyword-group action deny audit
comment TEST
Ruijie(cont-plcy-config)# end
```

- 删除策略组 policyA 中的所有 POSTFILE 规则。

```
Ruijie# configure terminal
Ruijie(config)# content-policy policyA
Ruijie(cont-plcy-config)# postfile-rule delete-all
Ruijie(cont-plcy-config)# end
```

【检验方法】
- 使用 show running-config 命令可以查看配置状态。

配置 POSTFILE 默认审计

【配置方法】
- 启用 POSTFILE 默认审计。

```
Ruijie# configure terminal
Ruijie(config)# content-policy _AUDIT_DEFAULT
Ruijie(cont-plcy-config)# postfile-rule audit-default-enable
Ruijie(cont-plcy-config)# end
```

【检验方法】
- 使用 show running-config 命令可以查看配置状态。

交换 POSTFILE 规则的优先级

【配置方法】
- 交换策略组 policyA 内 POSTFILE 访问控制规则 10 和规则 20 的优先级。

```
Ruijie# configure terminal
Ruijie(config)# content-policy policyA
Ruijie(cont-plcy-config)# postfile-rule priority-swap 10 20
Ruijie(cont-plcy-config)# end
```

【检验方法】
- 使用 show running-config 命令可以查看配置状态。

常见错误

- 规则 id 重复导致配置失败。
- 规则引用的对象未存在导致规则不生效。
- 规则优先级未理清导致实际审计结果与预期有差异。

8.5.16 配置 HTTP POST 规则

配置效果

- 启用 HTTP POST 默认审计功能。
- 向内容审计策略组中添加 HTTP POST 规则，即 POST 规则。
- 交换 POST 规则的优先级。

注意事项

- POST 规则的生效状态取决于引用的内容对象是否存在、时间对象是否生效、所属的策略组是否关联有效用户。
- 同一个策略组内的规则优先级为后配先生效。

配置方法

配置 POST 规则

- 必须配置。

配置 POST 默认审计

- 可选配置。若需要开启默认审计功能则可配置。

交换 POST 规则的优先级

- 可选配置。若需要交换 POST 规则的优先级则可配置。

检验方法

使用 show running-config 命令可以查看配置状态。

相关命令

配置 POST 规则

【命令格式】 **post-rule** *rule-id* **time-range** *time-name* [**content** *content-object-name*] **action** { **permit** | **deny** } [**audit**] [**comment** *comment-string*]

【参数说明】 *rule-id*：规则的 ID 标识，取值范围（1~200）。规则容量为 200。

time-name：代表规则生效时间段的时间对象名。

content-object-name：规则用到的内容对象名。

comment-string：该规则的描述。

【命令模式】 内容审计策略组配置模式

【使用指导】 1：规则的 rule-id 在同一个内容审计策略组中不允许重复，在不同的内容审计策略组中允许重复。

2：一个内容审计策略组中的访问控制规则都有相应的优先级，最后配的那条规则优先级最高。

3：规则所关联的 time-name、content-object-name 可以不存在，此时规则不生效。

4：删除 POST 访问控制规则可使用命令 **no post-rule** *rule-id*。

配置 POST 默认审计

【命令格式】 **post-rule audit-default-enable**

【参数说明】 -

【命令模式】 内容审计策略组配置模式

【使用指导】 1：默认审计只能在策略组名为_AUDIT_DEFAULT 的默认审计组内进行配置，在其它策略组内配置该命令则不生效。

2：关闭 POST 默认审计功能可使用命令 **no post-rule audit-default-enable**。

删除策略组下所有 POST 规则

【命令格式】 **post-rule delete-all**

【参数说明】 -

【命令模式】 内容审计策略组配置模式

【使用指导】 删除当前策略组下的所有 POST 规则，不影响其它策略组。

交换 POST 规则的优先级

【命令格式】 **post-rule priority-swap** *rule-id1 rule-id2*

【参数说明】 *rule-id1*：待交换优先级的规则 1 的 ID。

rule-id2：待交换优先级的规则 2 的 ID。

【命令模式】 内容审计策略组配置模式

【使用指导】 交换优先级命令是用于对调两条访问控制规则的优先级，运行该命令后，show running 中可以看到两个规则的排序发生了变化，但 show running 不会出现该命令。

配置举例

配置 POST 规则

【配置方法】

- 为内容审计策略组 policyA 添加一个 POST 访问审计规则，过滤用户进行 POST 外发信息，并且需要审计该行为。

```
Ruijie# configure terminal
Ruijie(config)# content-policy policyA
Ruijie(cont-plcy-config)# post-rule 2 time-range any content keyword-group action deny audit comment
TEST
Ruijie(cont-plcy-config)# end
```

- 删除策略组 policyA 中的所有 POST 规则。

```
Ruijie# configure terminal
Ruijie(config)# content-policy policyA
Ruijie(cont-plcy-config)# post-rule delete-all
Ruijie(cont-plcy-config)# end
```

【检验方法】

- 使用 show running-config 命令可以查看配置状态。

配置 POST 默认审计

【配置方法】
- 启用 POST 默认审计。

```
Ruijie# configure terminal
Ruijie(config)# content-policy _AUDIT_DEFAULT
Ruijie(cont-plcy-config)# post-rule audit-default-enable
Ruijie(cont-plcy-config)# end
```

【检验方法】
- 使用 show running-config 命令可以查看配置状态。

↘ 交换 POST 规则的优先级

【配置方法】
- 交换策略组 policyA 内 POST 访问控制规则 10 和规则 20 的优先级。

```
Ruijie# configure terminal
Ruijie(config)# content-policy policyA
Ruijie(cont-plcy-config)# post-rule priority-swap 10 20
Ruijie(cont-plcy-config)# end
```

【检验方法】
- 使用 show running-config 命令可以查看配置状态。

常见错误

- 规则 id 重复导致配置失败。
- 规则引用的对象未存在导致规则不生效。
- 规则优先级未理清导致实际审计结果与预期有差异。

8.5.17 配置加密类审计功能开关

配置效果

- 启用加密类审计功能。
- 配置部分用户需要启用加密类审计功能
- 配置部分用户不需要启用加密类审计功能

注意事项

- 加密类审计功能开关只能在默认审计策略下配置，属于全局开关。
- 加密类审计功能不能单独生效，需要配置 WEB-BBS、WEB-MAIL、WEB-SEARCH、虚拟身份、外发文件等各种应用类型的审计策略，协同生效。

配置方法

配置加密类审计功能开关

- 必须配置。

配置部分用户需要启用加密类审计功能

- 可选配置。

配置部分用户不需要启用加密类审计功能

- 可选配置。

检验方法

使用 show running-config 命令可以查看配置状态。

相关命令

配置加密类审计功能开关

【命令格式】 **ssl-audit enable**
【参数说明】
【命令模式】 内容审计默认策略组配置模式
【使用指导】 1：关闭加密类审计功能可使用命令 **no ssl-audit enable**。

配置部分用户需要启用加密类审计功能

【命令格式】 **ssl-audit need-proxy subscriber** *usr_group*
ssl-audit need-proxy auth-subscriber *usr_group_auth*
【参数说明】 *usr_group:*静态用户组
*usr_group_auth:*认证用户组
【命令模式】 全局模式
【使用指导】 可使用 show ssl-audit need-proxy 命令查看配置结果

配置部分用户不需要启用加密类审计功能

【命令格式】 **ssl-audit unneed-proxy subscriber** *usr_group*
ssl-audit unneed-proxy auth-subscriber *usr_group_auth*
【参数说明】 *usr_group:*静态用户组
*usr_group_auth:*认证用户组
【命令模式】 全局模式
【使用指导】 可使用 show ssl-audit unneed-proxy 命令查看配置结果

配置举例

配置加密类审计功能开关

【配置方法】
- 开启加密类审计功能开关。

```
Ruijie# configure terminal
Ruijie(config)# content-policy _AUDIT_DEFAULT
Ruijie(cont-plcy-config)# ssl-audit enable
Ruijie(cont-plcy-config)# end
```

- 关闭加密类审计功能开关。

```
Ruijie# configure terminal
Ruijie(config)# content-policy _AUDIT_DEFAULT
Ruijie(cont-plcy-config)# no ssl-audit enable
Ruijie(cont-plcy-config)# end
```

【检验方法】
- 使用 show running-config 命令可以查看配置状态。

配置部分用户需要启用加密类审计功能

【配置方法】
- 配置部分用户需要启用加密类审计功能

```
Ruijie# configure terminal
Ruijie(config)# ssl-audit need-proxy subscriber usr_group_sub
Ruijie(config)# ssl-audit need-proxy auth-subscriber usr_group_auth
Ruijie(cont-plcy-config)# end
```

- 删除部分用户需要启用加密类审计功能

```
Ruijie# configure terminal
Ruijie(config)# no ssl-audit need-proxy subscriber usr_group_sub
Ruijie(config)# no ssl-audit need-proxy auth-subscriber usr_group_auth
Ruijie(cont-plcy-config)# end
```

【检验方法】
- 使用 show ssl-audit unneed-proxy 命令可以查看配置状态。

配置部分用户不需要启用加密类审计功能

【配置方法】
- 配置部分用户不需要启用加密类审计功能

```
Ruijie# configure terminal
Ruijie(config)# ssl-audit unneed-proxy subscriber usr_group_sub
Ruijie(config)# ssl-audit unneed-proxy auth-subscriber usr_group_auth
Ruijie(cont-plcy-config)# end
```

- 删除部分用户不需要启用加密类审计功能

```
Ruijie# configure terminal
Ruijie(config)# no ssl-audit unneed-proxy subscriber usr_group_sub
Ruijie(config)# no ssl-audit unneed-proxy auth-subscriber usr_group_auth
Ruijie(cont-plcy-config)# end
```

【检验方法】
- 使用 show ssl-audit unneed-proxy 命令可以查看配置状态。

常见错误

- 无

8.5.18 配置阻断信息实时统计

配置效果

- 设置特定 IP 进行统计。

注意事项

- 功能开关属于全局开关。
- 本功能不能单独生效，需要配置 URL、IM、MAIL、WEB-BBS、WEB-MAIL、WEB-SEARCH、虚拟身份、外发文件等各种应用类型的审计策略，协同生效。
- 若设定了 IP，只能统计一个 IP 的阻断信息

配置方法

↘ 设定特定 IP 进行统计

- 可选配置。

检验方法

使用 show running-config 命令可以查看配置状态。

相关命令

↘ 配置特定 IP 进行统计

【命令格式】 content-audit deny-stat ip A.B.C.D
【参数说明】 A.B.C.D IP 地址
【命令模式】 特权模式
【使用指导】 1：删除特定 IP 可使用 **no** content-audit deny-stat ip A.B.C.D

配置举例

↘ 配置特定 IP 进行统计

【配置方法】

- 配置特定 IP 进行统计

```
Ruijie# configure terminal
```

```
Ruijie(config)# content-audit deny-stat ip 192.168.1.2
Ruijie(config)# end
```

- 删除特定 IP

```
Ruijie# configure terminal
Ruijie(config)#no content-audit deny-stat ip 192.168.1.2
Ruijie(config)# end
```

【检验方法】
- 使用 show running-config 命令可以查看配置状态。

常见错误

- 无

8.5.19 配置内容审计信息写本地存储的开关

配置效果

- 缺省情况下，内容审计各业务的审计信息记录在设备的本地存储中；若审计信息有发送到外部 log 服务，可以关闭此开关，审计信息将不再记录到设备本地存储中。

注意事项

- 无

配置方法

↘ 配置内容审计各业务的审计信息是否写本地存储的开关

- 可选配置。

检验方法

使用 show content-audit write-db/show running-config 命令可以查看配置状态。

相关命令

↘ 配置 URL 审计写本地存储的开关

【命令格式】 **content-audit write-db url**
【参数说明】 -
【命令模式】 全局模式
【使用指导】 可以使用命令 **no content-audit write-db url** 关闭 URL 审计写本地存储的开关。

配置 WEB-SEARCH 审计写本地存储的开关

【命令格式】 **content-audit write-db web-search**
【参数说明】 -
【命令模式】 全局模式
【使用指导】 可以使用命令 **no content-audit write-db web-search** 关闭 WEB-SEARCH 审计写本地存储的开关。

配置 WEB-BBS 审计写本地存储的开关

【命令格式】 **content-audit write-db web-bbs**
【参数说明】 -
【命令模式】 全局模式
【使用指导】 可以使用命令 **no content-audit write-db web-bbs** 关闭 WEB-BBS 审计写本地存储的开关。

配置 WEB-MAIL 审计写本地存储的开关

【命令格式】 **content-audit write-db web-mail**
【参数说明】 -
【命令模式】 全局模式
【使用指导】 可以使用命令 **no content-audit write-db web-mail** 关闭 WEB-MAIL 审计写本地存储的开关。

配置 MAIL 审计写本地存储的开关

【命令格式】 **content-audit write-db mail**
【参数说明】 -
【命令模式】 全局模式
【使用指导】 可以使用命令 **no content-audit write-db mail** 关闭 MAIL 审计写本地存储的开关。

配置 IM 审计写本地存储的开关

【命令格式】 **content-audit write-db im**
【参数说明】 -
【命令模式】 全局模式
【使用指导】 可以使用命令 **no content-audit write-db im** 关闭 IM 审计写本地存储的开关。

配置应用控制审计写本地存储的开关

【命令格式】 **content-audit write-db app-control**
【参数说明】 -
【命令模式】 全局模式
【使用指导】 可以使用命令 **no content-audit write-db app-control** 关闭应用控制审计写本地存储的开关。

配置虚拟身份审计写本地存储的开关

【命令格式】 **content-audit write-db vid**
【参数说明】 -
【命令模式】 全局模式
【使用指导】 可以使用命令 **no content-audit write-db vid** 关闭 vid 审计写本地存储的开关。

配置 TELNET 审计写本地存储的开关

【命令格式】 **content-audit write-db telnet**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 可以使用命令 **no content-audit write-db telnet** 关闭 TELNET 审计写本地存储的开关。

配置 FTP 审计写本地存储的开关

【命令格式】 **content-audit write-db ftp**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 可以使用命令 **no content-audit write-db ftp** 关闭 ftp 审计写本地存储的开关。

配置举例

开启内容审计各业务的审计写本地存储开关

【配置方法】

- 进入全局模式，开启各业务审计写本地存储的开关。

```
Ruijie# configure terminal
Ruijie(config)# content-audit write-db url
Ruijie(config)# content-audit write-db im
Ruijie(config)# content-audit write-db app-control
Ruijie(config)# content-audit write-db web-search
Ruijie(config)# content-audit write-db web-bbs
Ruijie(config)# content-audit write-db web-mail
Ruijie(config)# content-audit write-db mail
Ruijie(config)# content-audit write-db vid
Ruijie(config)# content-audit write-db postfile
Ruijie(config)# content-audit write-db plugin
Ruijie(config)# end
```

【检验方法】

- 使用 **show content-audit write-db** 命令可以查看配置状态。

```
Ruijie# show content-audit write-db
url_write_db:           1
im_write_db:            1
app_control_write_db:   1
web_search_write_db:    1
web_bbs_write_db:       1
web_mail_write_db:      1
```

```
mail_write_db:          1
vid_write_db:           1
post_write_db:          1
postfile_write_db:      1
plugin_write_db:        1
telnet_write_db:        1
ftp_write_db:           1
```

常见错误

- 无

8.5.20 配置 HTTP 端口

配置效果

- 当内容审计不依赖于应用识别时，需要通过端口识别 HTTP 报文，缺省下我们认为 tcp 80 和 8080 端口为 HTTP 报文，针对其他特殊 HTTP 报文，可以通过该命令配置 HTTP 端口，以识别 HTTP 报文。

注意事项

- 配置的 HTTP 端口 3 秒内生效。

配置方法

↘ 配置 HTTP 端口

- 可选配置。系统默认将 tcp 80 和 8080 端口的报文识别为 HTTP 报文。若有其他特殊端口的 HTTP 报文，可添加。

检验方法

使用 show content-audit http-port 命令可以查看配置状态。

相关命令

↘ 配置 HTTP 端口

【命令格式】 **content-audit http-port** *port-num*

【参数说明】 *port-num*：端口号，范围 1~65535，其中 80 和 8080 端口为系统内定，不允许手动添加或删除。

【命令模式】 全局模式

【使用指导】 添加 HTTP 端口。使用 **no content-audit http-port** *port-num* 删除。

配置举例

添加一个 HTTP 端口

【配置方法】
- 添加 HTTP 端口 60000。

```
Ruijie# configure terminal
Ruijie(config)# content-audit http-port 60000
Ruijie(url-obj-config)# end
```

【检验方法】
- 使用 show content-audit http-port 命令可以查看配置状态。

```
Ruijie#show content-audit http-port
HTTP port information in user:
80
8080
60000

HTTP port information in kernel:
80
8080
60000
```

删除一个 HTTP 端口

【配置方法】
- 将 60000 从 HTTP 端口中删除。

```
Ruijie# configure terminal
Ruijie(config)# no content-audit http-port 60000
Ruijie(url-obj-config)# end
```

【检验方法】
- 使用 show content-audit http-port 命令可以查看配置状态。

```
Ruijie#show content-audit http-port
HTTP port information in user:
80
8080

HTTP port information in kernel:
80
8080
```

常见错误

- 无。

8.5.21 配置 HTTPS 端口

配置效果

- 当内容审计不依赖于应用识别时，需要通过端口识别 HTTPS 报文，缺省下认为 tcp 443 端口为 HTTPS 报文，针对其他特殊 HTTPS 报文，可以通过该命令配置 HTTPS 端口，以识别 HTTPS 报文。

注意事项

- 配置的 HTTPS 端口 3 秒内生效。

配置方法

↘ 配置 HTTPS 端口

- 可选配置。系统默认将 tcp 443 端口的报文识别为 HTTPS 报文。若有其他特殊端口的 HTTPS 报文，可添加。

检验方法

使用 **show content-audit https-port** 命令可以查看配置状态。

相关命令

↘ 配置 HTTPS 端口

【命令格式】 **content-audit https-port** *port-num*

【参数说明】 *port-num*：端口号，范围 1~65535，其中 443 端口为系统内定，不允许手动添加或删除。

【命令模式】 全局模式

【使用指导】 添加 HTTPS 端口。使用 **no content-audit https-port** *port-num* 删除。

配置举例

↘ 添加一个 HTTPS 端口

【配置方法】

- 添加 HTTPS 端口 4430。

```
Ruijie# configure terminal
Ruijie(config)# content-audit https-port 4430
Ruijie(url-obj-config)# end
```

【检验方法】

- 使用 **show content-audit https-port** 命令可以查看配置状态。

```
Ruijie#show content-audit https-port
```

```
HTTPS port information in user:
443
4430

HTTPS port information in kernel:
443
4430
```

↘ 删除一个 HTTP 端口

【配置方法】

- 将 4430 从 HTTPS 端口中删除。

```
Ruijie# configure terminal
Ruijie(config)# no content-audit https-port 4430
Ruijie(url-obj-config)# end
```

【检验方法】

- 使用 **show content-audit https-port** 命令可以查看配置状态。

```
Ruijie#show content-audit https-port
HTTPS port information in user:
443

HTTPS port information in kernel:
443
```

常见错误

- 无。

8.5.22 配置 HTTPS 审计使能开关

配置效果

- 开启 HTTPS 审计使能开关，配合内容审计各子业务的规则使用，可对 HTTPS 加密的网站进行审计和过滤。
- 目前只支持 HTTPS 域名审计和过滤，需要配合 URL 规则使用。

注意事项

- 必须配合 URL 规则使用，才能对 HTTPS 加密的网站访问进行域名审计和过滤。

配置方法

配置 HTTPS 审计使能开关

- 必须配置。若需对 HTTPS 加密的网站进行审计和过滤，必须开启此开关。

检验方法

使用 **show running-config** 命令可以查看配置状态。

相关命令

配置 HTTPS 审计使能开关

【命令格式】 **https-audit enable**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 开启 HTTPS 审计使能开关。使用 **no https-audit enable** 关闭。

配置举例

开启 HTTPS 审计使能开关

【配置方法】
- 开启 HTTPS 审计使能开关。

```
Ruijie# configure terminal
Ruijie(config)# https-audit enable
Ruijie(url-obj-config)# end
```

- 若要对 HTTPS 域名进行审计和过滤，需要同时配置 URL 规则。如开启 URL 默认审计规则：

```
Ruijie# configure terminal
Ruijie(config)# content-policy _AUDIT_DEFAULT
Ruijie(cont-plcy-config)# url-rule audit-default-enable
Ruijie(cont-plcy-config)# end
```

【检验方法】
- 使用 show running-config 命令可以查看配置状态。

关闭 HTTPS 审计使能开关

【配置方法】
- 关闭 HTTPS 审计使能开关。

```
Ruijie# configure terminal
Ruijie(config)# no https-audit enable
Ruijie(url-obj-config)# end
```

【检验方法】
- 使用 **show running-config** 命令可以查看配置状态。

常见错误

- 无。

8.5.23 配置 TELNET 审计规则

配置效果

- 启用 TELNET 默认审计功能。
- 向内容审计策略组中添加 TELNET 规则。
- 交换 TELNET 规则的优先级。

注意事项

- TELNET 规则的生效状态取决于引用的时间对象是否生效、所属的策略组是否关联有效用户。
- 同一个策略组内的规则优先级为后配先生效。

配置方法

↘ 配置 TELNET 规则

- 必须配置。

↘ 配置 TELNET 默认审计

- 可选配置。若需要开启默认审计功能则可配置。

↘ 交换 TELNET 规则的优先级

- 可选配置。若需要交换 TELNET 规则的优先级则可配置。

检验方法

使用 show running-config 命令可以查看配置状态。

相关命令

↘ 配置 TELNET 规则

【命令格式】 **telnet-rule** *rule-id* **time-range** *time-name* **action** { **permit** | **deny** } [**audit**] [**comment** *comment-string*]

【参数说明】 *rule-id*：规则的 ID 标识，取值范围（1~200）。规则容量为 200。

time-name：代表规则生效时间段的时间对象名。*comment-string*：该规则的描述。

【命令模式】 内容审计策略组配置模式

【使用指导】 1：规则的 rule-id 在同一个内容审计策略组中不允许重复，在不同的内容审计策略组中允许重复。

2：一个内容审计策略组中的访问控制规则都有相应的优先级，最后配的那条规则优先级最高。

3：规则所关联的 time-name 可以不存在，此时规则不生效。

4：删除 TELNET 访问控制规则可使用命令 **no telnet-rule** *rule-id*。

配置 TELNET 默认审计

【命令格式】 **telnet-rule audit-default-enable**

【参数说明】 -

【命令模式】 内容审计策略组配置模式

【使用指导】 1：默认审计只能在策略组名为_AUDIT_DEFAULT 的默认审计组内进行配置，在其它策略组内配置该命令则不生效。

2：关闭 TELNET 默认审计功能可使用命令 **no telnet-rule audit-default-enable**。

删除策略组下所有 TELNET 规则

【命令格式】 **telnet-rule delete-all**

【参数说明】 -

【命令模式】 内容审计策略组配置模式

【使用指导】 只能删除当前策略组下的所有 TELNET 规则，不影响其它策略组。

交换 TELNET 规则的优先级

【命令格式】 **telnet-rule priority-swap** *rule-id1 rule-id2*

【参数说明】 *rule-id1*：待交换优先级的规则 1 的 ID。

rule-id2：待交换优先级的规则 2 的 ID。

【命令模式】 内容审计策略组配置模式

【使用指导】 交换优先级命令是用于对调两条访问控制规则的优先级，运行该命令后，show running 中可以看到两个规则的排序发生了变化，但 show running 不会出现该命令。

配置举例

配置 TELNET 规则

【配置方法】

- 为内容审计策略组 policyA 添加一个 TELNET 审计规则，过滤用户进行外发文件，并且需要审计该行为。

```
Ruijie# configure terminal
Ruijie(config)# content-policy policyA
Ruijie(cont-plcy-config)# telent-rule 2 time-range any action deny audit comment TEST
Ruijie(cont-plcy-config)# end
```

- 删除策略组 policyA 中的所有 TELNET 规则。

```
Ruijie# configure terminal
Ruijie(config)# content-policy policyA
Ruijie(cont-plcy-config)# telnet-rule delete-all
Ruijie(cont-plcy-config)# end
```

【检验方法】 ● 使用 show running-config 命令可以查看配置状态。

配置 TELNET 默认审计

【配置方法】 ● 启用 TELNET 默认审计。

```
Ruijie# configure terminal
Ruijie(config)# content-policy _AUDIT_DEFAULT
Ruijie(cont-plcy-config)# telnet-rule audit-default-enable
Ruijie(cont-plcy-config)# end
```

【检验方法】 ● 使用 show running-config 命令可以查看配置状态。

交换 TELNET 规则的优先级

【配置方法】 ● 交换策略组 policyA 内 TELNET 访问控制规则 10 和规则 20 的优先级。

```
Ruijie# configure terminal
Ruijie(config)# content-policy policyA
Ruijie(cont-plcy-config)# telnet-rule priority-swap 10 20
Ruijie(cont-plcy-config)# end
```

【检验方法】 ● 使用 show running-config 命令可以查看配置状态。

常见错误

- 规则 id 重复导致配置失败。
- 规则引用的对象未存在导致规则不生效。
- 规则优先级未理清导致实际审计结果与预期有差异。

8.5.24 配置 FTP 审计规则

配置效果

- 启用 FTP 默认审计功能。
- 向内容审计策略组中添加 FTP 规则。
- 交换 FTP 规则的优先级。

注意事项

- FTP 规则的生效状态取决于引用的内容对象是否存在、时间对象是否生效、所属的策略组是否关联有效用户。

- 同一个策略组内的规则优先级为后配先生效。

配置方法

配置 FTP 规则

- 必须配置。

配置 FTP 默认审计

- 可选配置。若需要开启默认审计功能则可配置。

交换 FTP 规则的优先级

- 可选配置。若需要交换 FTP 规则的优先级则可配置。

检验方法

使用 show running-config 命令可以查看配置状态。

相关命令

配置 FTP 规则

【命令格式】 **ftp-rule** *rule-id* **time-range** *time-name* [**filename** *content-object-name*] **action** { **permit** | **deny** } [**audit**] [**comment** *comment-string*]

【参数说明】 *rule-id*：规则的 ID 标识，取值范围（1~200）。规则容量为 200。

time-name：代表规则生效时间段的时间对象名。

content-object-name：规则用到的文件名的对象名。

comment-string：该规则的描述。

【命令模式】 内容审计策略组配置模式

【使用指导】 1：规则的 rule-id 在同一个内容审计策略组中不允许重复，在不同的内容审计策略组中允许重复。

2：一个内容审计策略组中的访问控制规则都有相应的优先级，最后配的那条规则优先级最高。

3：规则所关联的 time-name、content-object-name 可以不存在，此时规则不生效。

4：删除 TELNET 访问控制规则可使用命令 **no ftp-rule** *rule-id*。

配置 FTP 默认审计

【命令格式】 **ftp-rule audit-default-enable**

【参数说明】 -

【命令模式】 内容审计策略组配置模式

【使用指导】 1：默认审计只能在策略组名为_AUDIT_DEFAULT 的默认审计组内进行配置，在其它策略组内配置该命令则不生效。

2：关闭 FTP 默认审计功能可使用命令 **no ftp-rule audit-default-enable**。

删除策略组下所有 FTP 规则

【命令格式】 **ftp-rule delete-all**

【参数说明】 -

【命令模式】 内容审计策略组配置模式

【使用指导】 只能删除当前策略组下的所有 FTP 规则，不影响其它策略组。

交换 FTP 规则的优先级

【命令格式】 **ftp-rule priority-swap** *rule-id1 rule-id2*

【参数说明】 *rule-id1*：待交换优先级的规则 1 的 ID。

rule-id2：待交换优先级的规则 2 的 ID。

【命令模式】 内容审计策略组配置模式

【使用指导】 交换优先级命令是用于对调两条访问控制规则的优先级，运行该命令后，show running 中可以看到两个规则的排序发生了变化，但 show running 不会出现该命令。

开关 FTP 规则的上传文件内容审计开关

【命令格式】 **[no] ftp-upload-file-audit enable**

【参数说明】

【命令模式】 内容审计策略组配置模式

【使用指导】 1：默认审计只能在策略组名为_AUDIT_DEFAULT 的默认审计组内进行配置，在其它策略组内配置该命令则不生效。

配置举例

配置 FTP 规则

【配置方法】

- 为内容审计策略组 policyA 添加一个 FTP 审计规则，过滤用户进行外发文件，并且需要审计该行为。

```
Ruijie# configure terminal
Ruijie(config)# content-policy policyA
Ruijie(cont-plcy-config)# ftp-rule 2 time-range any action deny audit comment TEST
Ruijie(cont-plcy-config)# end
```

- 删除策略组 policyA 中的所有 FTP 规则。

```
Ruijie# configure terminal
Ruijie(config)# content-policy policyA
Ruijie(cont-plcy-config)# ftp-rule delete-all
Ruijie(cont-plcy-config)# end
```

【检验方法】

- 使用 show running-config 命令可以查看配置状态。

配置 FTP 默认审计

【配置方法】 ● 启用 FTP 默认审计。

```
Ruijie# configure terminal
Ruijie(config)# content-policy _AUDIT_DEFAULT
Ruijie(cont-plcy-config)# ftp-rule audit-default-enable
Ruijie(cont-plcy-config)# end
```

【检验方法】 ● 使用 show running-config 命令可以查看配置状态。

交换 FTP 规则的优先级

【配置方法】 ● 交换策略组 policyA 内 FTP 访问控制规则 10 和规则 20 的优先级。

```
Ruijie# configure terminal
Ruijie(config)# content-policy policyA
Ruijie(cont-plcy-config)# ftp-rule priority-swap 10 20
Ruijie(cont-plcy-config)# end
```

【检验方法】 ● 使用 show running-config 命令可以查看配置状态。

开关 FTP 规则的上传文件内容审计开关

【配置方法】 ● 开启 FTP 规则的上传文件内容审计总开关

```
Ruijie# configure terminal
Ruijie(config)# content-policy _AUDIT_DEFAULT
Ruijie(cont-plcy-config)# ftp-upload-file-audit enable
Ruijie(cont-plcy-config)# end
```

【检验方法】 ● 使用 show running-config 命令可以查看配置状态。

常见错误

- 规则 id 重复导致配置失败。
- 规则引用的对象未存在导致规则不生效。
- 规则优先级未理清导致实际审计结果与预期有差异。

8.5.25 配置 FILE 过滤规则

配置效果

- 向内容审计策略组中添加 FILE 规则。
- 交换 FILE 规则的优先级。

注意事项

- FILE 规则的生效状态取决于引用的内容对象是否存在、时间对象是否生效、所属的策略组是否关联有效用户。
- 同一个策略组内的规则优先级为后配先生效。

配置方法

配置 FILE 规则

- 必须配置。

交换 FILE 规则的优先级

- 可选配置。若需要交换 FILE 规则的优先级则可配置。

检验方法

使用 show running-config 命令可以查看配置状态。

相关命令

配置 FILE 规则

【命令格式】 **file-rule** *rule-id* **time-range** *time-name* **acti**[1]**on** { **permit** | **deny** } [**audit**] [**comment** *comment-string*]
file-rule *rule-id* **relation** { **and** | **or** } [**file-name** *content-obj-string1*] [**file-type** *content-obj-string2*]

【参数说明】 *rule-id*：规则的 ID 标识，取值范围（1~200）。规则容量为 200。
time-name：代表规则生效时间段的时间对象名。
comment-string：该规则的描述。
content-obj-string1：文件名关键字
content-obj-string2：文件类型关键字

【命令模式】 内容审计策略组配置模式

【使用指导】 1：规则的 rule-id 在同一个内容审计策略组中不允许重复，在不同的内容审计策略组中允许重复。
2：一个内容审计策略组中的访问控制规则都有相应的优先级，最后配的那条规则优先级最高。
3：规则所关联的 time-name、content-obj-string1、content-obj-string2 可以不存在，此时规则不生效。
4：删除 FILE 访问控制规则可使用命令 **no file-rule** *rule-id*。

交换 FILE 规则的优先级

【命令格式】 **file-rule priority-swap** *rule-id1 rule-id2*

【参数说明】 *rule-id1*：待交换优先级的规则 1 的 ID。

rule-id2：待交换优先级的规则 2 的 ID。

【命令模式】 内容审计策略组配置模式

【使用指导】 交换优先级命令是用于对调两条访问控制规则的优先级，运行该命令后，show running 中可以看到两个规则的排序发生了变化，但 show running 不会出现该命令。

配置举例

配置 FILE 规则

【配置方法】

- 为内容审计策略组 policyA 添加一个 FILE 规则，过滤用户进行外发文件，并且需要审计该行为。

```
Ruijie# configure terminal
Ruijie(config)# content-policy policyA
Ruijie(cont-plcy-config)# file-rule 2 time-range any action deny audit comment TEST
Ruijie(cont-plcy-config)# file-rule 2 relation or file-name 文件名关键字
Ruijie(cont-plcy-config)# end
```

交换 FILE 规则的优先级

【配置方法】

- 交换策略组 policyA 内 FILE 控制规则 10 和规则 20 的优先级。

```
Ruijie# configure terminal
Ruijie(config)# content-policy policyA
Ruijie(cont-plcy-config)# file-rule priority-swap 10 20
Ruijie(cont-plcy-config)# end
```

【检验方法】

- 使用 show running-config 命令可以查看配置状态。

删除 FILE 规则

【配置方法】

- 删除策略组 policyA 中的所有 FILE 规则。

```
Ruijie# configure terminal
Ruijie(config)# content-policy policyA
Ruijie(cont-plcy-config)# file-rule delete-all
Ruijie(cont-plcy-config)# end
```

【检验方法】

- 使用 show running-config 命令可以查看配置状态。

常见错误

- 规则 id 重复导致配置失败。
- 规则引用的对象未存在导致规则不生效。
- 规则优先级未理清导致实际审计结果与预期有差异。

8.5.26 配置附件上传 elog 使能开关

配置效果

- 缺省情况下，NPE 模式不支持附件上传 elog，开启附件上传 elog 使能开关，且设备有硬盘的情况下，就可支持附件上传 elog。

注意事项

- 必须在 NPE 模式且有硬盘的情况下开启才有用。

配置方法

↘ 配置附件上传 elog 使能开关

- 可选配置。若 NPE 模式下要发送附件给 elog，开启此开关，必须在有硬盘的情况下才有效。

检验方法

使用 **show running-config** 命令可以查看配置状态。

相关命令

↘ 配置附件上传 elog 使能开关

【命令格式】 **content-attach-to-elog enable**
【参数说明】 -
【命令模式】 全局模式
【使用指导】 开启附件上传 elog 使能开关。使用 **no content-attach-to-elog enable** 关闭。

配置举例

↘ 开启附件上传 elog 使能开关

【配置方法】 ● NPE 模式下开启附件上传 elog 使能开关。

```
Ruijie# configure terminal
Ruijie(config)# content-attach-to-elog enable
Ruijie(url-obj-config)# end
```

【检验方法】 ● 使用 show running-config 命令可以查看配置状态。

↘ 关闭附件上传 elog 使能开关

【配置方法】 ● 关闭附件上传 elog 使能开关。

```
Ruijie# configure terminal
Ruijie(config)# no content-attach-to-elog enable
Ruijie(url-obj-config)# end
```

【检验方法】 ● 使用 **show running-config** 命令可以查看配置状态。

常见错误

- 无。

8.5.27 配置内容审关键字订阅

配置效果

- 缺省情况下，功能不开启。配置后，可定期发送内容审计阻断情况的邮件给关注人。

注意事项

- 无。

配置方法

↘ 配置邮件告警功能开启

- 必须配置，配置后功能方可用。

检验方法

使用 **show content-audit alarm config 可以查看配置状态。**

相关命令

配置审计告警使能开关

【命令格式】 **content-audit alarm enable**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 开启邮件告警功能。使用 **no content-audit alarm enable** 关闭。

配置举例

开启指定审计类型的告警

【配置方法】

- 在全局模式下开启

```
Ruijie# configure terminal
Ruijie(config)# content-audit alarm type all
Ruijie(config)# end
```

【检验方法】

- 使用 **show content-audit alarm config** 命令可以查看配置状态。

关闭某个审计类型的告警

【配置方法】

- 在全局模式下配置。

```
Ruijie# configure terminal
Ruijie(config)# no content-audit alarm type all
Ruijie(config)# end
```

【检验方法】

- 使用 **show content-audit alarmconfig** 命令可以查看配置状态。

设置某个发送邮件的主题和目的邮箱

【配置方法】

- 在全局模式下配置。

```
Ruijie# configure terminal
Ruijie(config)# content-audit alarm mail subject 告警邮件
Ruijie(config)# content-audit alarm mail to xxx@126.com
```

【检验方法】

- 使用 **show content-audit alarmconfig** 命令可以查看配置状态。

设置邮件发送的周期和时间

【配置方法】

- 在全局模式下配置。

```
Ruijie# configure terminal
Ruijie(config)# content-audit alarm mail cycle 5
Ruijie(config)# end
```

【检验方法】

- 使用 **show content-audit alarm config** 命令可以查看配置状态。使用 no content-audit mail cycle 命令取消，恢复默认配置。

常见错误

- 无。

8.5.28 配置内容审计报表

配置效果

- 报表数据后台生成时间，配置后，可根据设置时间后台生成报表数据。
- 控制报表功能开启/关闭
- 自定义报表规则配置

注意事项

- 无。

配置方法

↘ 配置报表数据后台生成时间

- 可选配置，配置后可根据配置的时间定时生成报表数据

↘ 配置报表功能开启

- 可选配置，可打开/关闭报表功能

↘ 配置内容审计自定义报表规则

- 可选配置，可配置统计报表的规则

检验方法

使用 show report-create-time 可以查看配置后台生成时间。

使用 show report-function 查看报表功能开关是否开启

使用 show report-custom-config 查看规则是否正常配置

相关命令

配置举例

配置报表后台数据生成时间

【命令格式】 **report-create-time** *hh:mm:ss*

【参数说明】 *hh:mm:ss:*报表数据生成时间

【命令模式】 全局模式

【使用指导】 使用 **no report-create-time** 关闭。

配置报表功能开启

【命令格式】 **report-function enable**

【参数说明】

【命令模式】 全局模式

【使用指导】 使用 **no report-function enable** 关闭。

配置内容审计自定义报表规则

【命令格式】 **report-custom-config** *rule-id* **set-param report_name** *reportname* **top** *top-nu* **cycle { day | week | month } { usr-ip | usr-name}** *usr_name* **alarm { on | off } { sys-mail | custom-mail** *mail_adds* **}**
report-custom-config *rule-id* **set-app [postfile] [url-cls] [url-host] [web-bbs] [web-search] [vid] [mail] [web-mail] [im]**

【参数说明】

rule-id:自定义报表规则号

reportname:自定义报表规则名称

top-nu:需要统计的 TOP N

cycle:统计周期

usr_name:用户名或用户 IP

alarm:是否需要邮件提醒

mail_adds:自定义提醒邮件接收地址

【命令模式】 全局模式

【使用指导】 使用 **no report-custom-config** *rule-id 删除规则*

配置举例

配置报表后台数据生成时间

【配置方法】

- 在全局模式下开启

```
Ruijie# configure terminal
Ruijie(config)# report-create-time 02:00:00
Ruijie(config)# end
```

【检验方法】

- 使用 **show report-create-time** 命令可以查看配置状态。

配置报表功能打开

【配置方法】 ● 在全局模式下开启

```
Ruijie# configure terminal
Ruijie(config)# report-function enable
Ruijie(config)# end
```

【检验方法】 ● 使用 **show report-function** 命令可以查看配置状态。

配置自定义报表规则

【配置方法】 ● 在全局模式下开启

```
Ruijie# configure terminal
Ruijie(config)# report-custom-config 1 set-param report-name report_usrA top 10 cycle day usr-name usrA alarm on custom-mail 123@126.com
Ruijie(config)# report-custom-config 1 set-app postfile web-search
```

【检验方法】 ● 使用 **show report-custom-config** 命令可以查看配置状态。

常见错误

- 无。

8.6 监视与维护

清除各类信息

作用	命令
清除内容审计的实时统计信息。	**clear content-audit statistics**

查看运行情况

作用	命令
查看内容审计策略组信息。	**show content-policy** [**policy** [*policy-name*] | **stat** [**policy** policy-*name*]]

查看用户和策略的关联信息。	**show content-policy-relate policy-view** [{ **policy** *policy-name* | { **subscriber** { *subs-name1* | **any** } | **auth-subscriber** { *subs-name2* | **any** } | **ip** *A.B.C.D* } }] **show content-policy-relate user-view** { **subscriber** { *subs-name1* | **any** } | **auth-subscriber** { *subs-name2* | **any** } | **ip** *A.B.C.D* } [**detail**]
查看系统 URL 分类信息。	**show url-class system** [**class** { **id** *class-id* | **name** *class-name* }] **show url-class system comment** [**class** { **id** *class-id* | **name** *class-name* }] **show url-class system custom** [**class** { **id** *class-id* | **name** *class-name* }] **show url-class system exact**
查看指定 URL 的分类信息。	**show url-class url** *url-string*
查看用户自定义 URL 分类信息。	**show url-class user-cfg** [*class-name*]
查看 URL 规则信息。	**show url-rule content-policy** *policy-name* [**subscriber** *subs-name*] [**auth-subscriber** *auth-subs-name*]
查询应用控制审计明细信息。	**show app-audit detail** [**export**] { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm:ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**interface** *intf-name* | **bridge** *bridge-num*] [**subscriber** *subs-name1*] [**auth-subscriber** *subs-name2*] [**app-group** *app-group-name*] [**rule-name** *rule-name*] [**ip** *addr*] [**permit | deny**] **order-by** { **time** | **subscriber** | **internal-ip** | **app** } { **asc** | **desc** } [**start-item** *integer1* **end-item** *integer2*]
查询应用控制审计统计信息。	**show app-audit stat** { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm:ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**interface** *intf-name* | **bridge** *bridge-num*] [**subscriber** *subs-name1*] [**auth-subscriber** *subs-name2*] [**ip** *addr*] [**app-group** *app-group-name*] [**rule-name** *rule-name*] [**permit** | **deny**]
查询 IM 审计明细信息。	**show im-audit detail** [**export**] { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm:ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**interface** *intf-name* **| bridge** *bridge-num*] [**subscriber** *subs-name1*] [**auth-subscriber** *subs-name2*] [**direction** { **in** | **out** | **double** }] [**type** { **qq** | **msn** }] [**message** *keyword*] [**account** *account-string*] [**rule-name** *rule-name*] [**ip** *addr*] [**permit | deny**] **order-by** { **time** | **subscriber** | **auth-subscriber | internal-ip | direction** } { **asc** | **desc** } [**start-item** *integer1* **end-item** *integer2*]
查询 IM 审计统计信息。	**show im-audit stat** { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm::ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**interface** *intf-name* **| bridge** *bridge-num*] [**subscriber** *subs-name1*] [**auth-subscriber** *subs-name2*] [**direction** { **in** | **out** | **double** }] [**type** { **qq** | **msn** }] [**message** *keyword*] [**account** *account-string*] [**rule-name** *rule-name*] [**ip** *addr*] [**permit** | **deny**]
查询 MAIL 审计附件信息。	**show mail-audit attachment-info timestamp** *timestamp* **rand-id** *rand-id*

查询 MAIL 审计明细信息。	**show mail-audit detail** [**export**] { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm:ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**interface** *intf-name* **| bridge** *bridge-num*] [**subscriber** *subs-name1*] [**auth-subscriber** *subs-name2*] [**ip** *addr*] [**direction** { **in** | **out** | **double** }] [**from** *keyword1*] [**to** *keyword2*] [**subject** *keyword3*] [**rule-name** *rule-name*] [**permit | deny**] **order-by** { **time** | **subscriber** | **auth-subscriber | internal-ip** | **direction** | **send-mail-addr | mail-size** } { **asc** | **desc** } [**start-item** *integer1* **end-item** *integer2*]
查询 MAIL 审计统计信息。	**show mail-audit stat** { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm:ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**interface** *intf-name* **| bridge** *bridge-num*] [**subscriber** *subs-name1*] [**auth-subscriber** *subs-name2*] [**ip** *addr*] [**direction** { **in** | **out** | **double** }] [**from** *keyword1*] [**to** *keyword2*] [**subject** *keyword3*] [**rule-name** *rule-name*] [**permit | deny**]
查询 URL 审计明细信息。	**show url-audit detail** [**export**] { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm:ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**interface** *intf-name* | **bridge** *bridge-num*] [**subscriber** *subs-name*] [**auth-subscriber** *auth-subs-name*] [**ip** *addr*] [**url-class** *class-name* | **url-object** *obj-name* | **url** *url-string* | **url-host** *host-string1*] [**host** *host-string2*] [**permit | deny**] [**order-by time** | **url-class** | **url** | **host** | **ip**] { **asc** | **desc** } [**start-item** *integer1* **end-item** *integer2*]
查询 URL 审计统计信息。	**show url-audit stat** { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm:ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**interface** *intf-name* | **bridge** *bridge-num*] [**subscriber** *subs-name*] [**auth-subscriber** *auth-subs-name*] [**ip** *addr*] [**url-class** *class-name* | **url-object** *obj-name*] [**host** *host-string*] [**permit | deny**]
查询 URL 审计排名信息。	**show url-audit top** *n* [**export**] { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm:ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**interface** *intf-name* | **bridge** *bridge-num*] [**subscriber** *subs-name*] [**auth-subscriber** *auth-subs-name*] [**url-class** *class-name* | **url-object** *obj-name*] [**host** *host-string*] [**permit | deny**] [**order-by time** | **url-class** | **url** | **url-class** | **host-times**]
查询 WEB-BBS 审计明细信息。	**show web-bbs-audit detail** [**export**] { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm:ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**interface** *intf-name* **| bridge** *bridge-num*] [**subscriber** *subs-name1*] [**auth-subscriber** *subs-name2*] [**ip** *addr*] [**content** *keyword*] [**rule-name** *rule-name*] [**permit | deny**] **order-by** { **time** | **subscriber** | **auth-subscriber | internal-ip | url** } { **asc** | **desc** } [**start-item** *integer1* **end-item** *integer2*]

查询 WEB-BBS 审计统计信息。	**show web-bbs-audit stat** { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm::ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**interface** *intf-name* **| bridge** *bridge-num*] [**subscriber** *subs-name1*] [**auth-subscriber** *subs-name2*] [**ip** *addr*] [**content** *keyword*] [**rule-name** *rule-name*] [**permit** | **deny**]
查询 WEB-MAIL 审计附件信息。	**show web-mail-audit attachment-info timestamp** *timestamp* **rand-id** *rand-id*
查询 WEB-MAIL 审计明细信息。	**show web-mail-audit detail** [**export**] { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm:ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**interface** *intf-name* **| bridge** *bridge-num*] [**subscriber** *subs-name1*] [**auth-subscriber** *subs-name2*] [**ip** *addr*] [**direction** { **in** | **out** | **double** }] [**from** *keyword1*] [**to** *keyword2*] [**subject** *keyword3*] [**rule-name** *rule-name*] [**permit | deny**] **order-by** { **time** | **subscriber** | **auth-subscriber | internal-ip** | **direction** | **send-mail-addr** } { **asc** | **desc** } [**start-item** *integer1* **end-item** *integer2*]
查询 WEB-MAIL 审计统计信息。	**show web-mail-audit stat** { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm:ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**interface** *intf-name* **| bridge** *bridge-num*] [**subscriber** *subs-name1*] [**auth-subscriber** *subs-name2*] [**ip** *addr*] [**direction** { **in** | **out** | **double** }] [**from** *keyword1*] [**to** *keyword2*] [**subject** *keyword3*] [**rule-name** *rule-name*] [**permit | deny**]
查询 WEB-SEARCH 审计明细信息。	**show web-search-audit detail** [**export**] { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm:ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**interface** *intf-name* **| bridge** *bridge-num*] [**subscriber** *subs-name1*] [**auth-subscriber** *subs-name2*] [**ip** *addr*] [**keyword** *keyword*] [**rule-name** *rule-name*] [**permit | deny**] **order-by** { **time** | **subscriber** | **auth-subscriber | internal-ip | url** } { **asc** | **desc** } [**start-item** *integer1* **end-item** *integer2*]
查询 WEB-SEARCH 审计统计信息。	**show web-bbs-audit stat** { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm::ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**interface** *intf-name* **| bridge** *bridge-num*] [**subscriber** *subs-name1*] [**auth-subscriber** *subs-name2*] [**ip** *addr*] [**keyword** *keyword*] [**rule-name** *rule-name*] [**permit** | **deny**]
查询虚拟身份审计统计信息。	**show vid-audit detail** [**export**] { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm:ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**subscriber** *subs-name1*] [**auth-subscriber** *subs-name2*] [**type** { **weibo** | **weixin** }] [**uid** *uid-string*] [**nickname** *nick-string*] [**ip** *addr1*] [**mac** *addr2*] **order-by** { **time** | **subscriber** | **auth-subscriber | internal-ip | uid | mac** } { **asc** | **desc** } [**start-item** *integer1* **end-item** *integer2*]

查询虚拟身份审计统计信息。	**show im-audit stat** { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm:ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**subscriber** *subs-name1*] [**auth-subscriber** *subs-name2*] [**type** { **weibo** | **weixin** }] [**uid** *uid-string*] [**nickname** *nick-string*] [**ip** *addr1*] [**mac** *addr2*]
查询 QQ 聊天内容审计明细信息。	**show plugin-audit detail** [**export**] { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm:ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**interface** *intf-name* **| bridge** *bridge-num*] [**subscriber** *subs-name1*] [**auth-subscriber** *subs-name2*] [**ip** *addr*] [**content** *keyword*] [**rule-name** *rule-name*] [**permit | deny**] **order-by** { **time** | **subscriber** | **auth-subscriber | internal-ip | url** } { **asc** | **desc** } [**start-item** *integer1* **end-item** *integer2*]
查询 QQ 聊天内容审计统计信息。	**show plugin-audit stat** { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm::ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**interface** *intf-name* **| bridge** *bridge-num*] [**subscriber** *subs-name1*] [**auth-subscriber** *subs-name2*] [**ip** *addr*] [**content** *keyword*] [**rule-name** *rule-name*] [**permit** | **deny**]
查询外发文件审计明细信息。	**show postfile-audit detail** [**export**] { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm:ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**interface** *intf-name* **| bridge** *bridge-num*] [**subscriber** *subs-name1*] [**auth-subscriber** *subs-name2*] [**ip** *addr*] [**content** *keyword*] [**rule-name** *rule-name*] [**permit | deny**] **order-by** { **time** | **subscriber** | **auth-subscriber | internal-ip | url** } { **asc** | **desc** } [**start-item** *integer1* **end-item** *integer2*]
查询外发文件审计统计信息。	**show postfile-audit stat** { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm::ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**interface** *intf-name* **| bridge** *bridge-num*] [**subscriber** *subs-name1*] [**auth-subscriber** *subs-name2*] [**ip** *addr*] [**content** *keyword*] [**rule-name** *rule-name*] [**permit** | **deny**]
查询外发文件附件审计信息。	**show postfile-audit relate-id** *relate-id* **timestamp** *timestamp*
查询 HTTP POST 审计明细信息。	**show post-audit detail** [**export**] { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm:ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**interface** *intf-name* **| bridge** *bridge-num*] [**subscriber** *subs-name1*] [**auth-subscriber** *subs-name2*] [**ip** *addr*] [**content** *keyword*] [**rule-name** *rule-name*] [**permit | deny**] **order-by** { **time** | **subscriber** | **auth-subscriber | internal-ip | url** } { **asc** | **desc** } [**start-item** *integer1* **end-item** *integer2*]

查询 HTTP POST 审计统计信息。	**show post-audit stat** { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm::ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**interface** *intf-name* **| bridge** *bridge-num*] [**subscriber** *subs-name1*] [**auth-subscriber** *subs-name2*] [**ip** *addr*] [**content** *keyword*] [**rule-name** *rule-name*] [**permit** | **deny**]
查看内容审计实时统计信息	**show content-audit statistics** { **brief** | **counts** }
查看内容审计信息写本地存储的开关状态	**show content-audit write-db**
查看 HTTP 端口信息	**show content-audit http-port**
查看 HTTPS 端口信息	**show content-audit https-port**
查看阻断审计统计信息	**show content-audit deny-stat** { **brief** | **counts|ip** }
查询 TELNET 审计明细信息。	**show telnet-audit detail** [**export**] { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm:ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**subscriber** *subs-name1*] [**auth-subscriber** *subs-name2*] [**internal-ip** *addr1*] [**service-ip** *addr2*] [**conn** | **disconn**] [**rule-name** *rule-name*] [**permit | deny**] **order-by** { **time** | **subscriber** | **auth-subscriber | internal-ip | service-ip**} { **asc** | **desc** } [**start-item** *integer1* **end-item** *integer2*]
查询 TELNET 审计统计信息。	**show telnet-audit stat** { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm::ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**subscriber** *subs-name1*] [**auth-subscriber** *subs-name2*] [**internal-ip** *addr1*] [**service-ip** *addr2*] [**conn** | **disconn**] [**rule-name** *rule-name*] [**permit** | **deny**]
查询 FTP 审计明细信息。	**show ftp-audit detail** [**export**] { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm:ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**subscriber** *subs-name1*] [**auth-subscriber** *subs-name2*] [**internal-ip** *addr*] [**file-name** *keyword*] [**rule-name** *rule-name*] [**permit | deny**] **order-by** { **time** | **subscriber** | **auth-subscriber | internal-ip | url** } { **asc** | **desc** } [**start-item** *integer1* **end-item** *integer2*]
查询 FTP 审计统计信息。	**show telnet-audit stat** { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm::ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**subscriber** *subs-name1*] [**auth-subscriber** *subs-name2*] [**internal-ip** *addr*] [**file-name** *keyword*] [**rule-name** *rule-name*] [**permit** | **deny**]
查询内容审计自定义报表规则信息	**show report-custom-config {** *rule-id* **}**
查询内容审计自定义报表统计的报表信息	**show report-custom-data** *rule-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
打开应用控制审计审计处理跟踪的调试开关。	**debug app-control audit**
打开应用控制审计配置处理跟踪的调试开关。	**debug app-control config**
打开应用控制审计状态与资源信息显示的调试开关。	**debug app-control info**
打开 URL 审计审计处理跟踪的调试开关。	**debug url-audit audit**
打开 URL 审计配置处理跟踪的调试开关。	**debug url-audit config**
打开 URL 审计状态与资源信息显示的调试开关。	**debug url-audit info**
打开 URL 重定向配置处理跟踪的调试开关。	**debug url-redirect config**
打开 IM 审计审计处理跟踪的调试开关。	**debug im-audit audit**
打开 IM 审计配置处理跟踪的调试开关。	**debug im-audit config**
打开 IM 审计状态与资源信息显示的调试开关。	**debug im-audit info**
打开 MAIL 审计审计处理跟踪的调试开关。	**debug mail-audit audit**
打开 MAIL 审计配置处理跟踪的调试开关。	**debug mail-audit config**
打开 MAIL 审计状态与资源信息显示的调试开关。	**debug mail-audit info**
打开 WEB-BBS 审计审计处理跟踪的调试开关。	**debug web-bbs-audit audit**
打开 WEB-BBS 审计配置处理跟踪的调试开关。	**debug web-bbs-audit config**
打开 WEB-BBS 审计状态与资源信息显示的调试开关。	**debug web-bbs-audit info**
打开 WEB-MAIL 审计审计处理跟踪的调试开关。	**debug web-mail-audit audit**
打开 WEB-MAIL 审计配置处理跟踪的调试开关。	**debug web-mail-audit config**
打开 WEB-MAIL 审计状态与资源信息显示的调试开关。	**debug web-mail-audit info**

打开 WEB-SEARCH 审计审计处理跟踪的调试开关。	**debug web-search-audit audit**
打开 WEB-SEARCH 审计配置处理跟踪的调试开关。	**debug web-search-audit config**
打开 WEB-SEARCH 审计状态与资源信息显示的调试开关。	**debug web-search-audit info**
打开虚拟身份审计审计处理跟踪的调试开关。	**debug vid audit**
打开 QQ 聊天内容审计审计处理跟踪的调试开关。	**debug plugin-audit audit**
打开 QQ 聊天内容审计配置处理跟踪的调试开关。	**debug plugin-audit config**
打开外发信息审计审计处理跟踪的调试开关。	**debug postfile-audit audit**
打开外发信息审计配置处理跟踪的调试开关。	**debug postfile-audit config**
打开 HTTP POST 审计审计处理跟踪的调试开关。	**debug post-audit audit**
打开 HTTP POST 审计配置处理跟踪的调试开关。	**debug post-audit config**
打开 HTTPS 域名审计审计处理跟踪的调试开关。	**debug https-url audit**
打开 HTTPS 域名审计配置处理跟踪的调试开关。	**debug https-url config**
打开 HTTPS 域名审计状态与资源信息显示的调试开关。	**debug https-url info**
打开 TELNET 审计审计处理跟踪的调试开关。	**debug telnet-audit audit**
打开 TELNET 审计配置处理跟踪的调试开关。	**debug telnet-audit config**
打开 FTP 审计审计处理跟踪的调试开关。	**debug ftp-audit audit**
打开 FTP 审计配置处理跟踪的调试开关。	**debug ftp-audit config**

9 LINE-QUALITY

9.1 概述

LINE-QUALITY 是线路质量的拼写。

其主要功能有 3 种：1）监控线路质量，2）根据线路质量进行流量逃生，3）探测线路好坏，对异常线路进行关闭。

一般在具有多条线路的网吧环境使用。

- 线路质量监控，记录线路的质量信息，并进行展示，使得用户能够实时查看线路历史质量情况，为经营配置提供支持。
- 流量逃生，当线路质量不稳定时，将关键应用引流到其他线路，实现更高质量的用户体验，提升网吧竞争力。
- 线路探测，当线路已经断开或者非常不稳定，主动将该线路关闭，使得流量能够从其他线路出去，从而提高体验效果。

下文对 3 个功能分开介绍。

协议规范

- 无

9.2 典型应用

典型应用	场景描述
监控线路质量	设定阀值，以监控各线路质量。
配置线路流量逃生	设定线路质量标准，在异常时进行流量逃生
配置线路探测	设定线路探测方式，在线路异常时关闭线路

9.2.1 监控线路质量

应用场景

本功能能够提供对各个线路的质量数据进行采集，存储，显示。

该功能可以为客户提供最近一段时间的线路质量情况，并对线路异常情况进行告警，为路由策略提供数据支持。数据采集和告警的参数，则可以进行配置。主要有：

1） 采集周期

2） 数据保存时限

3） 采集数据的告警阀值。

系统提供一套默认值，这些值可以进行重新设置。主要有以下几种：

- PING 成功率告警阀值。
- 半连接数百分比告警阀值。
- 新建连接平均延时告警阀值。
- Rnfp 丢包告警阀值（暂未采集该数据）
- 流量过高、过低告警阀值（供流量逃生使用，监控界面不提示告警）

功能部属

该功能应该和 ping 工具，MLLB，DNS-PROXY，流量审计一同部署。

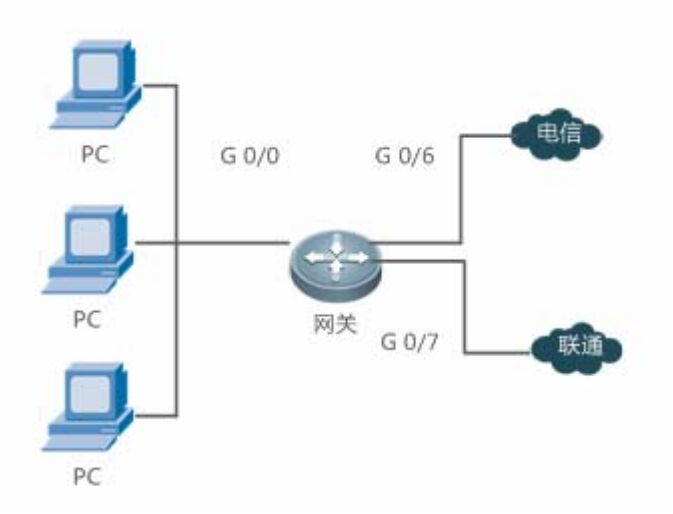
9.2.2 流量逃生

应用场景

本功能根据线路质量监控的几个告警指标，来控制关键应用的选路效果。

如下图，假设电信线路是主线路，联通是副线路，当副线路质量不错的时候，可以跑一些关键应用，比如游戏应用。而当联通线路不好的时候，则将游戏流量引导到电信线路，确保游戏能够继续正常进行。

图 9-1



【注释】 NBR 为出口网关设备。
PC 为内网用户，通过 NBR 上网。
G 0/0 为内网口，G0/6 和 G0/7 为外网口，分别连接电信和联通运营商线路。

功能部属

该功能应该和 ping 工具，MLLB，DNS-PROXY，流量审计，应用路由一同部署。

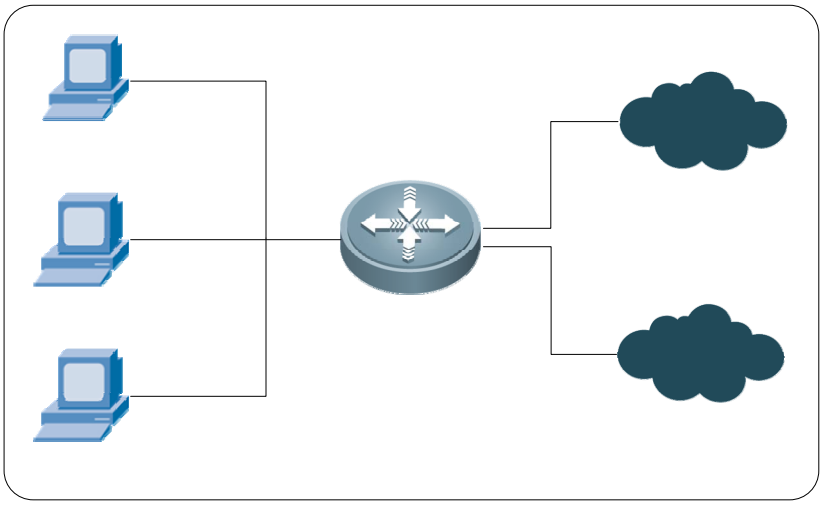
9.2.3 线路探测

应用场景

本功能主动探测线路是否正常，当线路异常时，主动将线路关闭，使得应用流量不再从这条线路出去，提升用户体验。

如下图，假设电信线路是主线路，联通是副线路。电信断网的时候，从该线路出去的应用将无法正常使用，又由于该线路是主线路，基本所有应用都将处于断网状态。此时，可以将 G0/6 接口 DOWN，使得路由能够将流量避开该线路，恢复联网使用，等线路恢复时，再 UP 起来。

图 9-2



【注释】 NBR 为出口网关设备。
PC 为内网用户，通过 NBR 上网。
G 0/0 为内网口，G0/6 和 G0/7 为外网口，分别连接电信和联通运营商线路。

功能部属

该功能应该和 TRACK，RNS 一同部署。

9.3 功能详解

PC G 0/0 G 0/6

基本概念

无。

功能特性

PC NBR G 0/7

功能特性	作用
监控线路质量	设定阀值，以监控各线路质量。
流量逃生策略	设定线路质量标准，在异常时进行流量逃生
线路探测策略	设定线路探测方式，在线路异常时关闭线路

9.3.1 监控线路质量

线路质量监控，主要功能为采集线路质量信息，让客户直观的了解网络状况，并为客户做路由策略调整提高数据支持。

工作原理

该功能主要收集 5 个信息：实时流量，ping 网关成功率，DNS 请求成功率，新建会话未响应比例，新建会话应答时延。各个信息都是由其他模块提供，本模块负责对数据进行收集，记录和展示。

9.3.2 流量逃生功能

流量逃生策略，根据线路监控结果，让指定应用流量能够根据线路质量情况，选择不同的线路走出去，从而达到为该应用提供更好的网络服务的目的。

工作原理

线路质量监控定时采集监控数据，并将数据告警信息通告给流量逃生模块。流量逃生模块根据配置，在到达指定条件时，生效/失效一系列应用路由策略，达到流量逃生的目的。

9.3.3 线路探测功能

线路探测功能，将定时探测线路是否正常。在线路异常时，及时将该线路 DOWN 掉，使得应用能够从正常线路出去，提高体验效果。

工作原理

线路探测功能的探测方法，主要是通过配置 RNS 和 TRACK 来进行的。当 RNS 探测到线路不通了，由 TRACK 通告本模块。本模块则及时对该线路进行协议 DOWN，并继续指导 TRACK+RNS 探测线路情况。当线路恢复时，再将线路协议 UP 起来。

9.4 产品说明



NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1500G、NBR2000G 支持路由流量逃生， NBR800G、NBR950G、NBR1000G-E、 NBR6120-E、 NBR1300G-E、 NBR1700G-E、 NBR2100G-E、 NBR2500D-E、 NBR3000D-E、

NBR3000D-UE、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 不支持路由流量逃生。

NBR108G-P 不支持线路质量功能。

9.5 配置详解

配置项	配置建议 & 相关命令	
配置线路监控策略	⚠ 可选配置。用于调整优化监控方法。	
	line-quanlity enable	启动线路监控功能
	line-quanlity senior-detect on	开启高级查询选项
	line-quanlity refresh *secs*	配置数据采集频率
	line-quanlity data-store *hours*	配置数据存储时限
	line-quanlity effect { ping-range | half-connect | delay-time | rnfp_drop | flow_gate } *min-val max-val*	配置告警阀值
配置流量逃生策略	⚠ 必配配置。	
	line-quanlity track enable	配置源注册过滤
	line-quanlity track set log-only	设置线路检测仅记录检测结果 ,不进行接口的 up/down
	line-quanlity track set flow-gate *percent*	设置线路检测在流量达到阀值时不进行接口 DOWN 操作
	line-quanlity track set interface *interface-name* **source** *ipaddr*	设置监控线路探测的源地址
	line-quanlity track set timeout *msecs*	设置线路检测探测超时时间
	line-quanlity track set { up | down } frequency *f-secs* **delay** *d-secs*	设置线路检测频率和确认时间
	line-quanlity track permit-interface *interface-name*	配置可以探测的接口
	line-quanlity track interface *interface-name* **enable**	开启某条线路的探测功能
	line-quanlity track interface *interface-name* **icmp { enable | ip | url }**	配置线路检测 ICMP 方式。
	line-quanlity track interface *interface-name* **dns { enable | ip }**	配置线路检测 DNS 方式。
	line-quanlity track interface *interface-name* **tcp { enable | ip | url }**	配置线路检测 TCP 方式。
配置线路检测策略	⚠ 必配配置。	

	line-quanlity route *id*	配置一个新的流量逃生策略，并进入策略配置模式
	condition interface *interface-name* **[ping] [dns] [half-connect] [delay] [{flow-low | flow-high}]**	配置流量逃生策略的条件
	route id *id-val* **{ enable | disable }**	配置要作用的应用路由策略 ID
	active	激活流量逃生策略

9.5.1 配置线路监控策略

配置效果

- 调整监控数据采集频率。
- 调整 ping 告警阀值
- 开启高级查询选项。

注意事项

- 调高监控数据采集频率，会使得系统消耗更多的资源用来采集数据，同时也需要花更多的存储空间来存储数据。而调低频率，会使得流量逃生响应相应的变慢。
- 调整 ping 告警阀值，会影响流量逃生的精确度。

配置方法

↘ 调整监控数据采集频率

- 可选配置。
- 若无特殊要求，采用默认配置即可。

【命令格式】 **line-quanlity refresh** *secs*
【参数说明】 secs：采集频率，单位秒
【缺省配置】 300 秒（5 分钟）
【命令模式】 全局配置模式
【使用指导】 一般使用默认值。

↘ 配置 ping 告警阀值

- 可选配置。
- 如无特殊需求，默认配置即可。

【命令格式】 **line-quanlity effect { ping-range | half-connect | delay-time | rnfp_drop | flow_gate }** *min-val max-val*

【参数说明】 *min-val*：普通告警阀值。

max-val：红色告警阀值。

【缺省配置】 50%为普通告警，20%为红色告警

【命令模式】 全局配置模式

【使用指导】 无特殊需求，可不配置。使用 show line-quality config 可查看配置情况。

↘ 开启高级查询选项

- 可选配置。
- 查看线路告警信息时，如果要查看普通告警，则需要开启本开关。

【命令格式】 **line-quanlity senior-detect on**

【参数说明】 **-**

【缺省配置】 关闭高级选项

【命令模式】 全局配置模式

【使用指导】 使用 show line-quality config 可查看配置情况。

检验方法

```
Ruijie#show line-quality config
line-quality enable  : enable
line-quality refresh : 300 s
line-quality storage : 72  h
line-quality senior  : on
line-quality effect  :
  ping_success  : red = 30 %    yellow = 50 %
  half_connect  : red = 50 %    yellow = 30 %
  delay-time    : red = 1000ms  yellow = 500 ms
  flow-gate     : high= 80 %    low    = 1  %
```

配置举例

无。

常见错误

- 无。

9.5.2 配置流量逃生策略

配置效果

- 配置一条流量逃生策略，使得流量能够在线路异常时，回到主线路。

注意事项

- 配置流量逃生，必须确保触发流量逃生后，不会对当前流量分布产生大的影响。比如，不能把大流量应用逃生到小带宽线路，导致小带宽线路爆满卡顿；
- 同时，在跨运营商环境，对 WEB 应用进行逃生要谨慎，因为这可能产生跨运营商访问资源， 导致访问比较慢或者不能访问。

配置方法

配置一条流量逃生策略

- 必选配置。
- 配置完成后，在告警条件达到时，触发应用路由调整，达到流量逃生目的。

【命令格式】 **line-quanlity route** *id*
【参数说明】 *id*：指定策略 ID。
【缺省配置】 无
【命令模式】 全局配置模式
【使用指导】 执行该命令后，进入策略配置模式，初次进入，会创建策略

检验方法

使用 show 命令检查配置是否正常。

【命令格式】 **show line-quality route** [*id*]
【参数说明】 *id*：指定策略 ID。
【配置模式】 特权模式、全局模式、接口模式
【使用指导】 -
【命令展示】

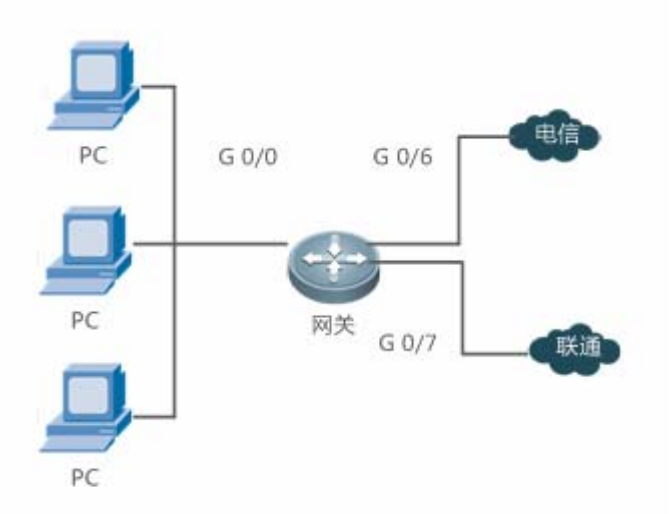
```
Ruijie#show line-quality route 1
line-quality route 1
  active: yes
  condition:
    interface: GigabitEthernet 0/5
    condition: half
  route list:
    enable  app route 1
  state: down
    half connect: up 0, down 32
```

配置举例

↘ 配置一条流量逃生策略。

【网络环境】

图 9-3



【配置方法】

- 假设电信是主线路，联通是副线路，应用路由策略 10 将部分游戏流量甩往联通线路。
- 配置一条流量逃生策略：当联通线路流量超过告警值时，游戏流量往电信线路走。

```
Ruijie#config
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#line-quality route 1
Ruijie(line-quality-route)#condition interface g 0/5 flow-high
Ruijie(line-quality-route)#route id 10 disable
Ruijie(line-quality-route)#active
Ruijie(line-quality-route)#exit
Ruijie(config)#exit
*Nov  3 14:27:40: %SYS-5-CONFIG_I: Configured from console by console
```

【检验方法】

- Show 命令查看配置是否生效

```
Ruijie#show line-quality route 1
line-quality route 1
  active: yes
  condition:
    interface: GigabitEthernet 0/5
    condition: flow-high
  route list:
    disable app route 10
  state: down
    flow_high    : up 0, down 33
```

9.5.3 配置线路检测策略

配置效果

- 配置一条策略，当线路检测到异常时，主动将线路 DOWN；当线路恢复正常时，再 UP 起来。

注意事项

- 当只有一条线路时，没有必要配置本功能。
- 探测目标要预先进行验证是否可达，否则将会误判。
- 最好先开启“只记录日志”选项，观察一段时间，查看是否会误判，再关闭“只记录日志”选项。

配置方法

↘ 开启只记录日志功能

- 可选配置。
- 若无特殊要求，使用默认值即可。

【命令格式】 **line-quanlity track set log-only**
【参数说明】 **-**
【缺省配置】 关闭
【命令模式】 全局配置模式
【使用指导】 -

↘ 设置流量大于阀值时不进行线路 DOWN

- 可选配置。
- 若无特殊要求，使用默认值即可。

【命令格式】 **line-quanlity track set flow-gate** *percent*
【参数说明】 *percent*：流量达到接口带宽的百分比
【缺省配置】 50%
【命令模式】 全局配置模式
【使用指导】 该配置是为了防止接口代码爆满导致的探测丢包，从而影响线路探测的正确判断

设置线路探测的源地址

- 可选配置。
- 若无特殊要求，使用默认值即可。

【命令格式】 **line-quanlity track set interface** *interface-name* **source** *ipaddr*
【参数说明】 *interface-name*：接口名称
ipaddr：源地址
【缺省配置】 无
【命令模式】 全局配置模式
【使用指导】 该配置是为了在特殊模式下（比如：多 wan 口同网段）探测能够正常进行

设置线路探测超时时间

- 可选配置。
- 若无特殊要求，使用默认值即可。

【命令格式】 **line-quanlity track set timeout** *msecs*
【参数说明】 *msesc*：每一次探测的超时时间
【缺省配置】 2000 毫秒
【命令模式】 全局配置模式
【使用指导】 -

设置线路探测频率和确认时间

- 可选配置。
- 若无特殊要求，使用默认值即可。

【命令格式】 **line-quanlity track set { up | down } frequency** *f-secs* **delay** *d-secs*
【参数说明】 *f-sesc*：每一次探测的超时时间
d-secs：探测到一个新状态的等待确认时间
【缺省配置】 探测频率
【命令模式】 全局配置模式
【使用指导】 接口 UP 和 DOWN 时，探测频率和确认事件是不同的。
在接口 UP 时，将以 UP 时的探测频率和确认时间来探测，因此，默认时，最迟 10s（频率）+2s（超时时间）+12s（确认时间）=24s，就能够初步判断接口是否正常；当初步判断接口异常时，则调整探测频率为 3s（接口 DOWN 时的频率），最迟 3s（频率）+2s（超时等待）+12s（确认时间）=17s 时，将接口 down 掉。此时，探测模式才转换为 DOWN 模式，全程最长用时 41s。
在接口 DOWN 时，已 DOWN 时的探测频率和确认事件来探测，默认，最迟 3s（频率）+2s（超时时间）+60s

（确认时间）=65s 时，会将接口 UP 起来。

一般，确认时间要不小于频率+超时的时间，以确保在确认等待期间里，最少又进行了一次探测，减少误判导致的状态频繁变更。

设置线路允许进行探测配置

- 必选配置。

【命令格式】 **line-quanlity track permit-interface** *interface-name*

【参数说明】 *interface-name*：允许配置探测策略的接口名称

【缺省配置】 无

【命令模式】 全局配置模式

【使用指导】 要配置某个接口的探测策略，先要进行探测配置允许。接口必须是 WAN 口。供 web 使用，非强制。

设置线路开启探测配置功能

- 必选配置。

【命令格式】 **line-quanlity track interface** *interface-name* **enable**

【参数说明】 *interface-name*：接口名称

【缺省配置】 无

【命令模式】 全局配置模式

【使用指导】 要配置某个接口的探测策略，先开启这个接口的探测功能。

关闭该接口的探测功能时，将清空该接口已有配置。

设置线路探测协议和目标

- 必选配置。

【命令格式】 **line-quanlity track interface** *interface-name* **icmp { enable |** *ip* **|** *url* **}**

line-quanlity track interface *interface-name* **dns { enable |** *ip* **}**

line-quanlity track interface *interface-name* **tcp { enable |** *ip* **|** *url* **}**

【参数说明】 *interface-name*：接口名称

icmp|dns|tcp：协议名称

enable：协议功能开启

ip：IP 地址

url：url 地址

【缺省配置】 无

【命令模式】 全局配置模式

【使用指导】 配置探测协议和目标时，先配置探测目标 IP 或者 URL，再开启该协议探测。关闭该协议的探测时，配置不清空。

ICMP 的探测目标不配置时，默认使用下一跳地址为目标。

使用 ICMP 探测主流网站时，最好同时配置一个 DNS 和 TCP 探测目标，防止 ICMP 探测的服务器禁 ping，导致接口误判断网。

强制 UP/DOWN 接口的协议状态

- 必选配置。

【命令格式】 **line-quality track interface** *interface-name* **up**

【参数说明】 *interface-name*：接口名称

【缺省配置】 无

【命令模式】 全局配置模式

【使用指导】 当探测功能误判时，可以手动的对接口进行 UP/DOWN 操作

检验方法

- 检查全局配置信息。

【命令格式】 **show line-quality track**

【参数说明】 **-**

【配置模式】 特权模式、全局模式、接口模式

【使用指导】 -

【命令展示】

```
Ruijie#show line-quality track
line quality track           :disable
line quality track log-only  :off
line quality track flow-gate :50%
line quality track timeout   :2000ms
line quality track intf count:1[max:8]
line quality track up        :[freq:10 ; delay:12 ]
line quality track down      :[freq:30 ; delay:0  ]
line quality permit interface:
  [3] GigabitEthernet 0/4
  [4] GigabitEthernet 0/5
  [5] GigabitEthernet 0/6
```

- 检查接口探测信息。

【命令格式】 **show line-quality track interface** [*interface-name*]

【参数说明】 *interface-name*：接口名称

【配置模式】 特权模式、全局模式、接口模式

【使用指导】 -

【命令展示】

```
Ruijie#show line-quality track interface
GigabitEthernet 0/5, index:4, stat:STOP, ctrl:NONE, source 0.0.0.0
  ICMP: enable
    url:
    ip : 1.1.1.1
    track_id : 0; rns_id: 0
    track_msg: NONE; track_stat: NONE
    last time:
  DNS: enable
```

```
  ip : 1.1.1.1
  track_id : 0; rns_id: 0
  track_msg: NONE; track_stat: NONE
  last time:
TCP: enable
  url:
  ip : 0.0.0.0
  track_id : 0; rns_id: 0
  track_msg: NONE; track_stat: NONE
  last time:
```

- 检查接口控制结果。

【命令格式】 **show line-quality track interface line**

【参数说明】 -

【配置模式】 特权模式、全局模式、接口模式

【使用指导】

【命令展示】

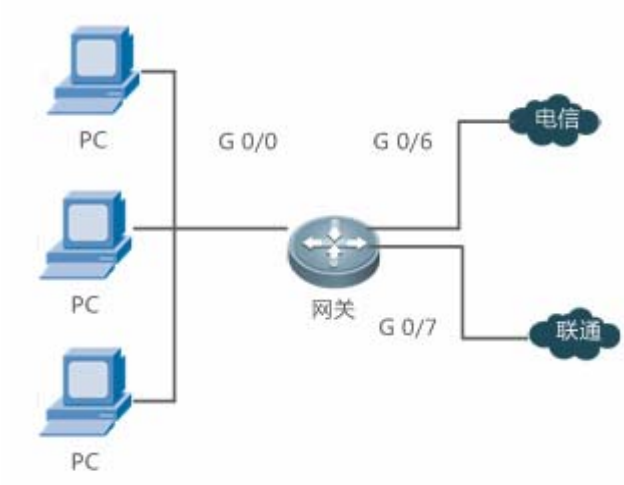
```
Ruijie#show line-quality track interface line
Interface                      Status Protocol Last-ctrl
GigabitEthernet 0/5            UP     UP       --
GigabitEthernet 0/6            UP     UP       --
```

配置举例

配置接口 g 0/6 使用 ICMP 和 DNS 协议进行探测

【网络环境】

图 9-4



【配置方法】

- 开启探测模块功能
- 开启接口 g 0/6 允许探测。
- 开启接口 g 0/6 探测功能。
- 配置接口 g 0/6 ICMP 和 DNS 探测目标
- 开启接口 g 0/6 ICMP 和 DNS 的探测功能

```
Ruijie#show line-quality track interface g 0/6
Ruijie#config
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#line-quality track enable
Ruijie(config)#line-quality track permit-interface g 0/6
Ruijie(config)#line-quality track interface g 0/6 enable
Ruijie(config)#line-quality track interface g 0/6 icmp www.baidu.com
Ruijie(config)#line-quality track interface g 0/6 dns 114.114.114.114
Ruijie(config)#line-quality track interface g 0/6 icmp enable
Ruijie(config)#line-quality track interface g 0/6 dns enable
Ruijie(config)#exit
Ruijie#
```

【检验方法】 查看接口配置的检测信息和状态。

```
Ruijie#show line-quality track interface g 0/6
```

9.6 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
-	-

查看运行情况

作用	命令
查看线路质量信息	**show line-quality { detect | detail-detect } interface** *interface-name* **{{ recent** *hour* **} | { time-interval** *yyyy mm dd hh:mm* **to** *yyyy mm dd hh:mm* **}}**
查看线路探测全局配置信息	**show line-quality track**
查看线路探测线路配置信息	**show line-quality track interface** [*interface-name*]
查看线路探测线路控制信息	**show line-quality track interface line**

查看流量逃生信息	**show line-quality route** [*id*]
查看模块运行日志	**show line-quality log** [**type** *type-num*] [**limit** *count*]

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
打开监控线路质量调试开关。	**debug line-quality detect**
打开流量逃生监控调试开关	**debug line-quality route**
打开线路探测调试开关	**debug line-quality track**

配置指南-应用协议

本分册介绍应用协议相关内容，包括以下章节：

1. 网络通信检测工具
2. DHCP
3. DNS
4. DDNS
5. NTP
6. SNTP
7. DNS Proxy
8. DNS-CACHE
9. FTP-Server
10. FTP Client
11. TIME RANGE

1 网络通信检测工具

1.1 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，以及网路的时延，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

1.2 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。

1.2.1 端对端连通性检查

应用场景

图 1-1 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。

1.2.2 主机路由检查

应用场景

图 1-2 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。

1.3 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。

1.3.1 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

1.3.2 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 ex ceeded）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

1.4 产品说明

NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE 支持 IPV6 PIng 功能；NBR800G、NBR950G、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR108G-P、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1500G、NBR2000G 不支持 IPV6 Ping 功能。

NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE 支持 IPV6 Tracert 功能；NBR800G、NBR950G、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR108G-P 、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1500G、NBR2000G 不支持 IPV6 Tracert。

1.5 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。	
	ping	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。	
	traceroute	运行 Traceroute 功能。

1.5.1 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。
- 如果需要检测 IPv6 地址是否可达，可通过 Ping IPv6 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**] [**interval** millisecond] [**out-interface** interface [**next-hop next-hop]] }**

【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。

next-hop：指定发送数据报文出接口的下一跳 IPv4 地址。

millisecond：指定每个 ping 报文的间隔时间，范围：10~300000（毫秒），缺省间隔时间是 100 毫秒

【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。

Ping IPv6

【命令格式】 **ping** [[**oob**] **ipv6**] [*address* [**via** *mgmt-name*] [**length** *length*] [**ntimes** *times*] [**timeout** *seconds*] [**data** *data*] [**source** *source*] [**detail**] [**interval** millisecond] [**out-interface** interface [**next-hop** *next-hop*]]]

ping [**oob** | **ipv6**] { *address* [**via** *mgmt-name*] [**length** *length*] [**ntimes** *times*] [**timeout** *seconds*] [**data** *data*] [**source** *source*] [**df-bit**] [**validate**] [**detail**] [**interval** millisecond] [**out-interface** interface [**next-hop** *next-hop*]] }

ping [**ipv6**] { *address* [**length** *length*] [**ntimes** *times*] [**timeout** *seconds*] [**data** *data*] [**source** *source*] [**df-bit**] [**validate**] [**detail**] [**interval** millisecond] [**out-interface** interface [**next-hop** *next-hop*]] }

ping [**ipv6**] { *address* [**length** *length*] [**ntimes** *times*] [**timeout** *seconds*] [**data** *data*] [**source** *source*] [**df-bit**] [**validate**] [**detail**] [**interval** millisecond] [**out-interface** interface [**next-hop** *next-hop*]] }

【参数说明】 **oob**：设置使用带外通道。当指定 MGMT 口作为源接口时，必须设置该参数。

address：指定目的 IPv6 地址或域名。

via: 对于支持多 mgmt 口的设备，比如通过 show interface brief 可见多个 mgmt 口，则 ping 的时候建议使用 via mgmt 显式指定具体 mgmt 口做 ping 操作。

mgmt-name : 指定在 oob 模式下报文的出口管理口。

length：指定发送数据包的长度，范围：16~18024，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。

source：指定报文源 IPv6 地址或源接口。其中，环回接口地址（例如::1）不允许作为源地址。

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。

next-hop：指定发送数据报文出接口的下一跳 IPv6 地址。

millisecond：指定每个 ping 报文的间隔时间，范围：10~300000（毫秒），缺省间隔时间是 100 毫秒

【命令模式】 在普通用户模式下，只能运行基本的 **ping ipv6** 功能；在特权用户模式下，还可以运行 **ping ipv6** 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 ipv6** 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 ipv6** 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 ipv6** 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 >
!!!
```

```
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。

运行普通 Ping IPv6 功能

【配置方法】 在特权模式下输入 Ping IPv6 地址 2001::1

常规 ping

```
Ruijie# ping ipv6 2001::1
Sending 5, 100-byte ICMP Echoes to 2001::1, timeout is 2 seconds:
< press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

显示 detail 的 ping

```
Ruijie#ping 2001::1 detail
Sending 5, 100-byte ICMP Echoes to 2001::1, timeout is 2 seconds:
  < press Ctrl+C to break >
Reply from 2001::1: bytes=100 time=1ms
Reply from 2001::1: bytes=100 time=1ms
Reply from 2001::1: bytes=100 time=1ms
Reply from 2001::1: bytes=100 time=1ms
Reply from 2001::1: bytes=100 time=1ms

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 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 IPv6 功能

【配置方法】 在特权模式下输入 Ping IPv6 地址 2001::5，并指定发送数据包的长度、个数、超时的时间等。

常规 ping

```
Ruijie# ping ipv6 2001::5  length 1500 ntimes 100 data ffff source 2001::9 timeout 3
Sending 100, 1500-byte ICMP Echoes to 2000::1, timeout is 3 seconds:
  < press Ctrl+C to break >
!!!
```

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。
- 如果需要跟踪 IPv6 数据包到达目的主机经过哪些网关，可通过配置 Traceroute IPv6 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**] { *adress* [**probe** *number*] [**source** *source*] [**timeout** *seconds*] [**ttl** *minimum maximum*] [**out-interface** interface *[***next-hop** *next-hop]] }*

【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。

next-hop：制定发送数据报文出接口的下一跳 IPv4 地址。

【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。

Traceroute IPv6

【命令格式】 **traceroute** [[**oob**] **ipv6**] { *address* [**via** *mgmt-name*] [**probe** *number*] [**timeout** *seconds*] [**ttl** *minimum maximum*] [**out-interface** interface [**next-hop** *next-hop*]] }

traceroute [[**oob**] **ipv6**] { *address* [**via** *mgmt-name*] [**probe** *number*] [**timeout** *seconds*] [**ttl** *minimum maximum*] [**out-interface** interface [**next-hop** *next-hop*]] }

traceroute [**ipv6**] { *address* [**probe** *number*] [**timeout** *seconds*] [**ttl** *minimum maximum*] [**out-interface** interface [**next-hop** *next-hop*]] }

traceroute [**ipv6**] { *address* [**probe** *number*] [**timeout** *seconds*] [**ttl** *minimum maximum*] [**out-interface** interface [**next-hop** *next-hop*]] }

【参数说明】 **oob**：设置使用带外通道。当指定 MGMT 口作为源接口时，必须设置该参数。

address：指定目的 IPv6 地址或域名。

mgmt-name : 指定在 oob 模式下报文的出口管理口。

number：指定发送的探测的数量，范围：1~255。

seconds：指定超时时间，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。

next-hop：制定发送数据报文出接口的下一跳 IPv6 地址。

【配置模式】 在普通用户模式下，只能运行基本的 **traceroute ipv6** 功能；在特权用户模式下，还可以运行 **traceroute ipv6** 的扩展功能。

【使用指导】 **Traceroute ipv6** 命令主要用于检查网络的连通性，并在网络故障发生时，准确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 IPv6 地址 3002::1。

```
Ruijie#

Ruijie# traceroute ipv6 3004::1

  < press Ctrl+C to break >

Tracing the route to 3004::1

1       3000::1          0 msec  0 msec  0 msec

2       3001::1          4 msec  4 msec 4 msec

3       3002::1          8 msec  8 msec  4 msec
```

从上面的结果可以清楚地看到，从源地址要访问 IP 地址为 3002::1 的主机，网络数据包都经过了哪些网关（1 - 3），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。

↘ 网络畅通的 Traceroute ipv6 举例

【配置方法】 在特权模式下，输入 Traceroute IPv6 地址 3004::1。

```
Ruijie# traceroute ipv6 3004::1

  < press Ctrl+C to break >

Tracing the route to 3004::1

1       3000::1          0 msec  0 msec  0 msec

2       3001::1          4 msec  4 msec 4 msec

3       3002::1          8 msec  8 msec  4 msec

4       3004::1          4 msec  28 msec  12 msec
```

从上面的结果可以清楚地看到，从源地址要访问 IP 地址为 *3004::1* 的主机，网络数据包都经过了哪些网关（1－4），同时给出了到达该网关所花费的时间。

↘ 网络中某些网关不通的 Traceroute IPv6 举例

【配置方法】 在特权模式下，输入 Traceroute IPv6 地址 3004::1。

```
Ruijie# traceroute ipv6 3004::1

  < press Ctrl+C to break >

Tracing the route to 3004::1

1       3000::1          0 msec  0 msec  0 msec

2       3001::1          4 msec  4 msec 4 msec

3       3002::1          8 msec  8 msec  4 msec

4       * * *

5       3004::1          4 msec  28 msec  12 msec
```

从上面的结果可以清楚地看到，从源地址要访问 IP 地址为 *3004::1* 的主机，网络数据包都经过了哪些网关（1－5），并且网关 4 出现了故障。

2 DHCP

2.1 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/Server 工作模式，DHCP 客户端通过发送请求消息向 DHCP 服务器获取 IP 地址，等其他配置信息。当 DHCP 客户端与服务器不在同一个子网上，必须有 DHCP 中继代理（DHCP Relay）来转发 DHCP 请求和应答消息。

协议规范

- RFC2131：Dynamic Host Configuration Protocol
- RFC2132：DHCP Options and BOOTP Vendor Extensions
- RFC3046：DHCP Relay Agent Information Option

2.2 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。
有线场景中 DHCP Relay 典型应用	有线场景中跨网段的用户申请 IP 上网。
指定分配固定地址功能的典型应用	固态绑定终端 MAC 地址、接入位置、主机名信息分配固定地址
授权分配准入功能的典型应用	限制指定终端、接入位置、主机名才允许获取地址

2.2.1 在局域网内提供 DHCP 服务

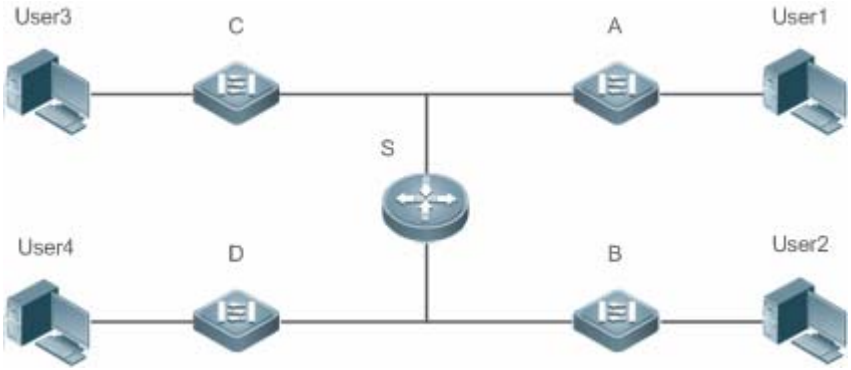
应用场景

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 2-1



【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

功能部属

- 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

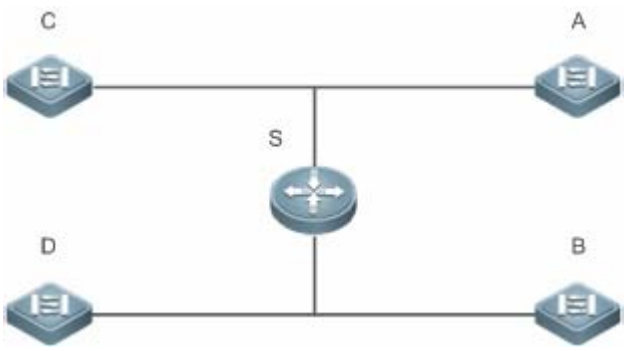
2.2.2 设备启动 DHCP Client 功能

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 2-2



【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

功能部属

- Server(S)上运行 DHCP-Server 服务
- 在 A、B、C、D 在接口上开启 DHCP-Client 功能

2.2.3 有线场景中 DHCP Relay 典型应用

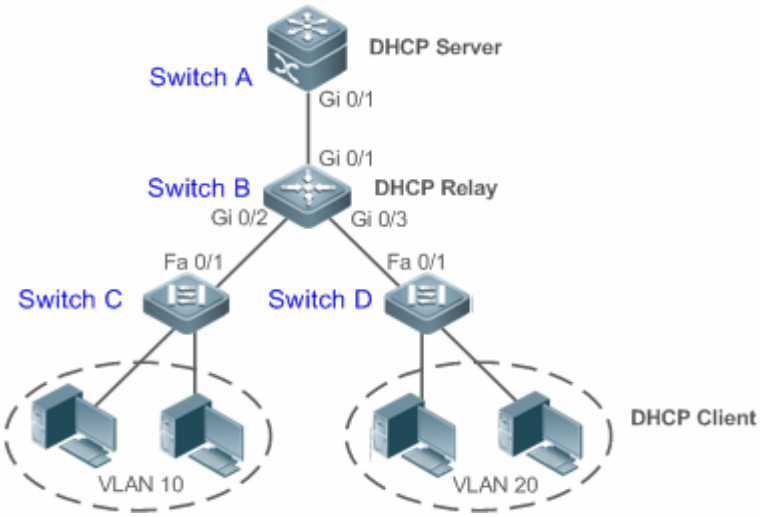
应用场景

如下图所示，Switch C 和 Switch D 作为接入设备，分布着 VLAN 10 和 VLAN 20 的 PC 用户，Switch B 作为网关设备，Switch A 作为核心设备。主要需求如下：

Switch A 可以充当 DHCP Server，为不同 VLAN 用户动态分配不同网段的 IP 地址。

Switch C 和 Switch D 下的接入用户可以跨网段动态获取 IP 地址。。

图 2-3DHCP Relay 组网拓扑图



【注释】 Switch C 与 Switch D 作为接入设备。
Switch B 作为网关设备。
Switch A 作为核心设备。

功能部属

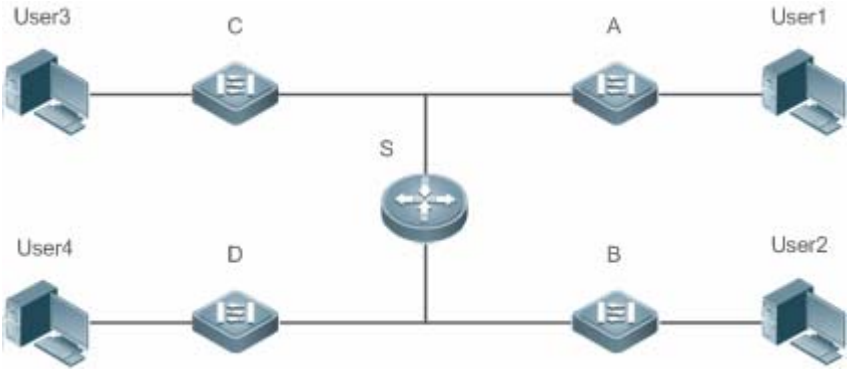
- 配置 Switch B 和 Switch C、D 之间的二层通信。
- 在 Switch B 上，指定 DHCP 服务器地址，并开启 DHCP Relay 功能。

1. 在 Switch A 上，分别为 VLAN 10 和 VLAN 20 的用户创建 DHCP 地址池，开启 DHCP Server 功能。

2.2.4 指定分配固定地址功能的典型应用

应用场景

管理员希望对内外某台服务器分配固定 IP 地址方便进行策略管理。医疗场景中，固定科室的设备希望分配固定的 IP 地址，设备更换也不希望发生变更。中小企业中，也存在根据员工号分配固定 IP 地址从而标识用户的需求。



【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 上开启 DHCP Snooping 功能
- 获取 User1、User2、User3 、User4 的 MAC 地址和主机名称
- 获取 User1、User2、User3 、User4 接入位置处的接入设备地址、端口、vlan
- Server(S)上对指定 MAC 地址、接入位置、主机名称绑定固定的 IP 地址
- User1、User2、User3 、User4 上主动发起 DHCP Client 请求

2.3 功能详解

基本概念

↘ DHCP 服务器

锐捷产品的 DHCP 服务器完全根据 RFC 2131 来实现的，主要功能就是为主机分配和管理 IP 地址。

DHCP 客户端

DHCP 客户端可以让设备自动地从 DHCP 服务器获得 IP 地址以及其它配置参数。

DHCP 中继

当 DHCP 客户端与服务器不在同一个子网上，就必须有 DHCP 中继代理来转发 DHCP 请求和应答消息。

租约

租约是客户机可使用指派的 IP 地址期间 DHCP 服务器指定的时间长度。租用给客户时，租约是活动的。在租约过期之前，客户机一般需要通过服务器更新其地址租约时间。当租约期满或在服务器上删除时，租约是非活动的。租约期限决定租约何时期满以及客户需要用服务器更新它的次数。

排除地址

排除地址是指从 DHCP 服务器中排除指定的一些 IP 地址序列，排除地址作用是为了确保在这些地址都不会是由 DHCP 服务器提供给 DHCP 客户机。

地址池

地址池是指 DHCP 服务器可分配给用户的地址集合，所有分配给用户的地址都从管理员配置的池中取出的。

选项类型

选项类型是 DHCP 服务器在向 DHCP 客户机提供租约服务时指派的配置参数。例如 ,某些公用选项包括默认网关(路由器)、WINS 服务器和 DNS 服务器的 IP 地址。DHCP-Server 还允许配置其它选项。虽然大多数选项都是在 RFC 2132 中预定义的，但若需要的话，可添加自定义选项类型。

功能特性

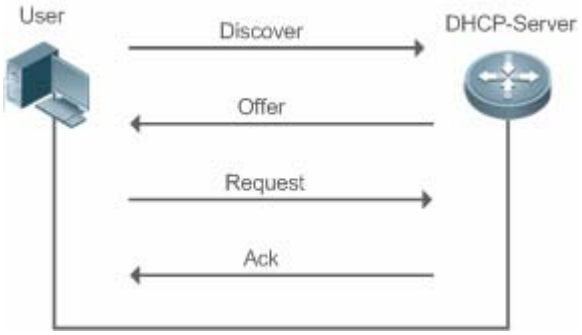
功能特性	作用
DHCP 服务器	设备启用 DHCP Server 功能，可以为主机动态分配 IP 地址和提供主机配置参数。
DHCP 中继代理	设备启用 DHCP Relayr 功能，可以在不同网段之间转发 DHCP 请求和应答消息。
DHCP 客户端	设备启用 DHCP Client 功能，可以自动从 DHCP 服务器获取 IP 地址以及其它配置参数。

2.3.1 DHCP 服务器

工作原理

DHCP 工作的基本流程

图 2-4



DHCP 请求 IP 地址的过程如下：

1. 主机发送 DHCPDISCOVER 广播包在网络上寻找 DHCP 服务器；
2. DHCP 服务器向主机发送 DHCPOFFER 单播/广播(依据主机报文相关属性确定)数据包，包含 IP 地址、MAC 地址、域名信息以及地址租期；
3. 主机发送 DHCPREQUEST 广播包，正式向服务器请求分配已提供的 IP 地址；
4. DHCP 服务器向主机发送 DHCPACK 单播包，确认主机的请求。

DHCP 客户端可以接收到多个 DHCP 服务器的 DHCPOFFER 数据包，然后可能接受任何一个 DHCPOFFER 数据包，但客户端通常只接受收到的第一个 DHCPOFFER 数据包。另外，DHCP 服务器 DHCPOFFER 中指定的地址不一定为最终分配的地址，通常情况下，DHCP 服务器会保留该地址直到客户端发出正式请求。

正式请求 DHCP 服务器分配地址 DHCPREQUEST 采用广播包，是为了让其它所有发送 DHCPOFFER 数据包的 DHCP 服务器也能够接收到该数据包，然后释放已经 OFFER（预分配）给客户端的 IP 地址。

如果发送给 DHCP 客户端的 DHCPOFFER 信息包中包含无效的配置参数，客户端会向服务器发送 DHCPDECLINE 信息包拒绝接受已经分配的配置信息。

在协商过程中，如果 DHCP 客户端没有及时响应 DHCPOFFER 信息包，DHCP 服务器会发送 DHCPNAK 消息给 DHCP 客户端，导致客户端重新发起地址请求过程。

在网络建设中，应用锐捷产品 DHCP 服务器，可以带来以下好处：

- 降低网络接入成本。一般采用静态地址分配的接入费用比较昂贵，应用动态地址分配的接入成本较低。
- 简化配置任务，降低网络建设成本。采用动态地址分配，大大简化了设备配置，对于在没有专业技术人员的地方部署设备，更是降低了部署成本。
- 集中化管理。在对多个子网进行配置管理时，有任何配置参数的变动，只需要修改和更新 DHCP 服务器的配置即可。

地址池

Server 收到来自 Client 请求报文，首先选择出一个合法有效地址池，并在该池中通过 PING 机制确认一个可用的地址，接着下发该池相关配置信息与地址至客户端，同时本地保存该租约信息在，以供该客户续租时检查有效性使用；由此完成整个租约分配流程。

地址池中可以带有各种配置参数，以下列举几个常用的：

- 地址池范围，可以分配给用户的地址范围
- 网关地址，通告用户网关地址，最多可以有八个

- DNS 地址，通告用户 DNS 地址，最多可以有八个
- 租约周期，通告用户地址何时老化，用户何时该请求续租

VRRP 监控功能

在 VRRP (Virtual Router Redundancy Protocol，虚拟路由冗余协议)应用场景下，DHCP 提供配置命令来决定是否监控当前接口的 VRRP 状态。对于配置了 VRRP 地址的接口，当配置监控 VRRP 状态后，DHCP 服务器仅对处于 Master 状态的设备接口上来的 DHCP 客户端请求报文进行处理，处于备份(Backup)状态的接口请求报文将被丢弃。而对于没配置 VRRP 地址的接口，DHCP 服务器不再监控 VRRP 状态，所有 DHCP 请求报文都会得到处理。VRRP 监控命令只能在三层口上配置，默认情况下 VRRP 监控功能关闭，即只有主机处理 DHCP 业务备机不处理。

添加可信 ARP 功能

可信 ARP 用于防止针对网关的 ARP 欺骗。DHCP 提供配置命令来决定分配地址时是否下发可信 ARP。当配置了添加可信 ARP 后，DHCP 服务器在分配地址时，会添加可信 ARP，从而有效防止 ARP 欺骗。

添加伪服务器检测功能

如果网络中私自部署 DHCP 服务器，当客户端申请地址时，会与这台服务器进行交互，导致客户端分配到错误的 IP 地址。这台服务器称为伪服务器。DHCP 提供配置命令来决定是否开启伪服务器检测功能。当配置伪服务器检测功能时，DHCP 会检查接收到的 DHCP 报文中是否携带 Option 54（Server Identifier Option，服务器标识选项）。如果携带该选项，并且选项内容与真实 DHCP 服务器标识不相符，则记录此伪服务器的 IP 地址和接收到报文的端口信息。伪服务器检测只是一种事后检测的安全功能，并不能预防非法 DHCP 服务器给客户端分配地址。

相关配置

全局启动 DHCP-Server 服务

- 缺省情况下，该服务关闭。
- 全局使用 **service dhcp** 开启该服务。
- 必须在全局使用 **service dhcp** 功能，才能进行 DHCP 服务。

配置地址池

- 缺省情况下，无地址池。
- 使用 **ip dhcp pool** 命令可以进入到地址池配置模式，进行地址范围、网关地址、DNS 等信息配置。
- 不配置地址池范围将无地址可分配，无法下发任何地址。

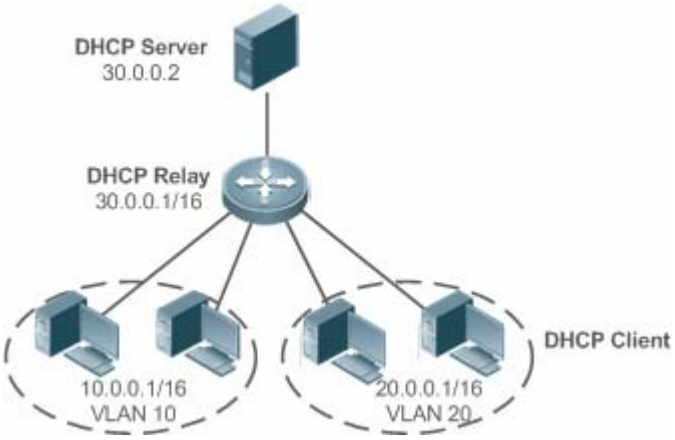
2.3.2 DHCP 中继代理

工作原理

DHCP 请求报文的目的 IP 地址为 255.255.255.255，这种类型报文的转发局限于子网内。为了实现跨网段的动态 IP 地址分配，DHCP 中继就产生了。DHCP 中继将收到的 DHCP 请求报文以单播方式转发给 DHCP 服务器，同时将收到的 DHCP 响应报文

转发给 DHCP 客户端。DHCP 中继相当于一个转发站，负责沟通位于不同网段的 DHCP 客户端和 DHCP 服务器，即转发客户端 DHCP 请求报文、转发服务端 DHCP 应答报文。这样就实现了只要安装一个 DHCP 服务器，就可以实现对多个网段的动态 IP 管理，即 Client—Relay—Server 模式的 DHCP 动态 IP 管理。如图所示：

图 2-5 DHCP Relay 应用场景



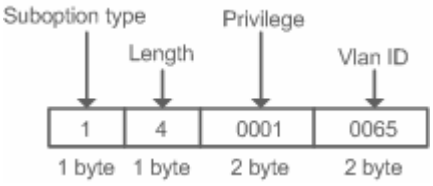
VLAN 10 和 VLAN 20 分别对应 10.0.0.1/16 和 20.0.0.1/16 的网络，而 DHCP 服务器在 30.0.0.1/16 的网络上，30.0.0.2 的 DHCP 服务器要对 10.0.0.1/16 和 20.0.0.1/16 的网络进行动态 IP 管理，只要在作为网关的设备上打开 DHCP 中继功能，并配置 30.0.0.2 为 DHCP 服务器的 IP 地址。

↘ DHCP Relay Agent Information(option 82)

根据 RFC3046 的定义，中继设备进行 DHCP Relay 时，可以通过添加 option 的方式来详细的标明 DHCP 客户端的一些网络信息，从而使服务器可以根据更精确的信息给用户分配不同权限的 IP，根据 RFC3046 的定义，所使用 option 选项的选项号为 82，故也被称作 option 82。锐捷实现的 Relay agent information 目前存在四种应用方案，下面分别对四种应用方案进行说明：

5. Relay agent information option dot1x：此种应用方案需要结合 802.1x认证以及锐捷产品RG-SAM。DHCP中继根据RG-SAM在 802.1x认证过程中下发的IP权限，以及DHCP客户端所属vid，组合构成Circuit ID子选项。选项格式如 图 2-6 所示：

图 2-6 选项格式



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

图 2-7 Agent Circuit ID

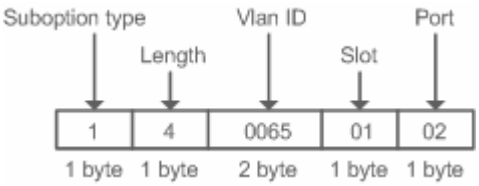
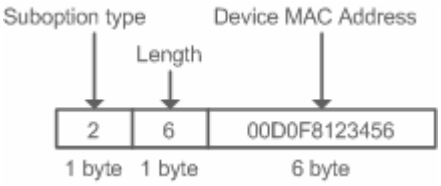


图 2-8 Agent Remote ID



7. Relay agent information option82：此种 option 的应用不需要结合其他协议模块的运行。与之前的 option82 相比较，其选项的填充内容有所改变，且支持自定义的内容填充；默认情况下，DHCP 中继根据接收 DHCP 请求报文的实体端口信息，以及设备自身的物理地址信息和设备名称，组合构成 option82 选项。选项格式如图下图所示：

图 2-14 Option82.1-circuit-id

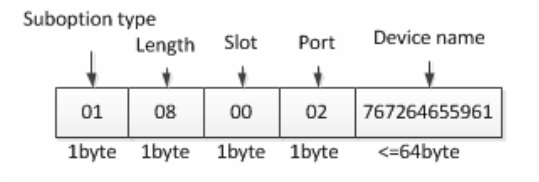
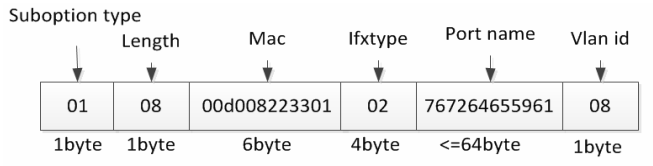


图 2-15 Option82-remote-id



DHCP Relay Check Server-id 功能

在 DHCP 应用环境中，通常会为每一个网络配备多个 DHCP 服务器，从而进行备份，防止因为一台服务器的工作不正常影响网络的正常使用。在 DHCP 获取的四个交互过程中，当 DHCP 客户端在发送 DHCP REQUEST 时已经选定了服务器，此时会在请求的报文中携带一个 server-id 的 option 选项，在某些特定的应用环境中为了减轻网络服务器压力，需要我们 Relay 能够使能此选项 ,只把请求报文发给此选项里的DHCP服务器 ,而不是发送给每一个配置的DHCP 服务器 ,上述就是DHCP Relay check server-id 功能 。

DHCP Relay suppression 功能

在指定接口上配置命令 ip DHCP Relay suppression 后，将屏蔽该接口上收到的 DHCP 请求报文；而对于其他接口上收到的 DHCP 请求报文，则正常转发。

相关配置

启动设备上的 DHCP Relay 功能

- 缺省情况下，设备上的 DHCP Relay 功能关闭。
- 使用 **service dhcp** 命令可以启动设备上的 DHCP Relay 功能。
- 必须在设备上启用 DHCP Relay 功能，DHCP Relay 才能正常工作。

配置 DHCP 服务器的 IP 地址

- 缺省情况下，无 DHCP 服务器的 IP 地址表项。
- 使用 **ip helper-address** 命令可以添加 DHCP 服务器地址表项，DHCP 服务器地址可以全局配置，也可以在三层接口上配置。全局或者每个三层接口上最多可以配置 20 个 DHCP 服务器地址。
- 在接口上收到 DHCP 请求报文时，首先使用接口上的 DHCP 服务器列表；如果接口上面没有配置 DHCP 服务器列表，则使用全局配置的 DHCP 服务器列表。

启动 DHCP option 82 功能

- 缺省情况下，设备上的 DHCP option 82 功能关闭。
- 使用 **ip dhcp relay information option82** 命令可以启动设备上的 DHCP option 82 功能。

启动 DHCP Relay check server-id 功能

- 缺省情况下，设备上的 DHCP Relay check server-id 功能关闭。
- 使用 **ip dhcp relay check server-id** 命令可以启动设备上的 DHCP Relay check server-id 功能。

启动 DHCP Relay suppression 功能

- 缺省情况下，所有接口上 DHCP Relay suppression 功能关闭。
- 使用 **ip dhcp relay suppression** 命令可以启动对应接口上的 DHCP Relay suppression 功能。

2.3.3 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、Rourter Port 等；

2.3.4 指定分配固定地址功能

工作原理

DHCP 请求报文中，OPTION 选项中会携带主机名、终端地址、接入位置信息。管理员针对指定主机名、接入位置、终端 MAC 地址绑定固定 IP 地址后，当终端请求上线时，终端报文信息匹配命中绑定信息后分配固定的 IP 地址给终端。

相关配置

使用 **ip dhcp add-client { solidify-ip ip** *ip-addr* **{ { access-device** *dev-addr* **access-vlan** *vlanid* **access-port** *portid* **| host-name** *hostname* **| mac** *mac-addr* **} binding-type { ip-hostname | ip-hostname-location | ip-mac | ip-mac-hostname | ip-mac-hostname-location | ip-mac-location } } | solidify-location ip** *ip-addr* **access-device** *dev-addr* **access-vlan** *vlanid* **access-port** *portid* **| solidify-mac mac** *mac-addr* **}**命令绑定指定接入位置信息、主机名称信息、终端 MAC 信息分配固定 IP 地址

2.3.5 授权分配准入功能

工作原理

DHCP 报文中会携带终端 MAC 地址信息，终端接入进行 DHCP 请求时，Server 开启授权分配模式后会获取终端 MAC 地址信息检查是否已授权，若已授权正常分配地址，未授权则不分配地址达到限制接入的效果。

相关配置

地址池模式下配置 solidify 命令开启授权分配模式

2.4 产品说明



NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE 支持 DHCP+IPAM 功能；NBR108G-P、NBR800G、NBR950G、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1500G、NBR2000G 不支持 DHCP+IPAM 功能。

2.5 配置详解

↘ 配置 DHCP 服务器

配置项	配置建议 & 相关命令

配置 DHCP 服务器动态分配 IP 地址	必须配置，用于启用 DHCP 服务器实现动态 IP 址分配。	
	service dhcp	启动 DHCP-SERVER 功能
	ip dhcp pool	配置地址池
	network	配置 DHCP 地址池的网络号和掩码
	可选配置，用于设置地址池相关属性。	
	default-router	配置客户端缺省网关
	lease	配置地址租期
	next-server	配置客户端启动的下载服务器地址
	bootfile	配置客户端启动文件
	domain-name	配置客户端的域名
	dns-server	配置域名服务器
	netbios-name-server	配置 NetBIOS WINS 服务器
	netbios-node-type	配置客户端 NetBIOS 节点类型
	lease-threshold	配置地址池告警门限值
	option	配置自定义选项
	pool-status	配置地址池启用或关闭
	update arp	配置从地址池分配地址时添加可信 ARP
	solidify	配置地址池固态属性 ,开启授权分配模式功能

配置 DHCP 中继代理

配置项	配置建议 & 相关命令	
配置 DHCP Relay 基本功能	必须配置。用于建立 DHCP Relay 服务。	
	service dhcp	启动 DHCP Relay 功能
	ip helper-address	配置 DHCP 服务器的 IP 地址
配置 DHCP Relay option 82 功能	可选配置。结合设备自身物理接口信息，给用户分配不同权限 IP。该功能与 **dhcp option dot1x** 不可以同时使用。	
	ip dhcp relay information option82	启用 DHCP option82 功能
配置 DHCP Relay check server-id 功能	可选配置。DHCP Relay 仅将 DHCP 请求报文转发到 option server-id 中指定的服务器。	
	ip dhcp relay check server-id	启用 DHCP Relay check server-di 功能
配置 DHCP Relay suppression 功能	可选配置。屏蔽对应接口地址上 DHCP 请求报文。	
	ip dhcp relay suppression	启用 DHCP Relay suppression 功能

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	
	ip address dhcp	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

配置指定分配固定地址功能

配置项	配置建议 & 相关命令
配置指定分配固定地址功能	可选配置，用于设置绑定接入位置信息、用户主机名信息、终端 MAC 地址信息分配固定地址。同时可用于授权分配模式下的终端单 MAC 授权。
	ip dhcp add-client { solidify-ip ip *ip-addr* **{ { access-device** *dev-addr* **access-vlan** *vlanid* **access-port** *portid* **| host-name** *hostname* **| mac** *mac-addr* **} binding-type { ip-hostname | ip-hostname-location | ip-mac | ip-mac-hostname | ip-mac-hostname-location | ip-mac-location } } | solidify-location ip** *ip-addr* **access-device** *dev-addr* **access-vlan** *vlanid* **access-port** *portid* **| solidify-mac mac** *mac-addr* **}** 绑定指定接入位置信息、用户主机名信息、终端 MAC 地址信息的任意组合进行固定地址分配 授权分配模式下，授权绑定的信息允许分配

2.5.1 配置 DHCP 服务器动态分配 IP 地址

配置效果

向所有 dhcp-client 提供 dhcp 服务，包括地址、网关等信息下发

注意事项

DHCP 服务器和 DHCP 中继共用 **service dhcp** 这条命令 ,但是这两个功能是互斥的 ,两者之间的切换依赖于是否配置了 DHCP 地址池。

配置方法

启动 DHCP-SERVER 功能

- 实现动态分配地址功能，为必选配置。
- 在配置模式下执行 **service dhcp** 命令。

配置地址池

- 创建地址池，为必选配置。
- 在配置模式下执行 **ip dhcp pool** 命令。

配置 DHCP 地址池的网络号和掩码

- 动态分配地址范围，为必选配置。
- 在地址池模式下执行 **network** 命令。

配置客户端缺省网关

- 用于通告客户端网关地址，为可选配置。
- 在地址池模式下执行 **default-router** 命令。

配置地址租期

- 用于通告客户端租约老化周期，默认值为 24h，为可选配置。
- 在地址池模式下执行 **lease** 命令。

配置客户端启动的下载服务器地址

- 用于通告客户端 TFTP 服务器地址，为可选配置。
- 在地址池模式下执行 **next-server** 命令。

配置客户端的域名

- 用于通告客户端的域名，为可选配置。
- 在地址池模式下执行 **domain-name** 命令。

配置域名服务器

- 用于通告客户客户端 dns 地址，为可选配置。
- 在地址池模式下执行 **dns** 命令。

配置 NetBIOS WINS 服务器

- 用于通告 windows 客户端 dns 地址，为可选配置。
- 在地址池模式下执行 **netbios-name-server** 命令。

配置客户端 NetBIOS 节点类型

- 用于通告 windows 客户端节点类型，为可选配置。
- 在地址池模式下执行 **netbios-name-type** 命令。

配置地址池告警门限值

- 用于管理租约数量，达到限制时打印警告，默认为 90%，为可选配置。
- 在地址池模式下执行 **lease-threshold** 命令。

配置自定义选项

- 用于通告客户端相当配置信息，为可选配置。
- 在地址池模式下执行 **option** 命令。

配置地址池启用或关闭

- 用于配置地址池是否可用，默认为开启，为可选配置。

- 在地址池模式下执行 **pool-status** 命令。

配置添加可信 ARP

- 用于配置分配地址时添加可信 ARP，默认为关闭，为可选配置。
- 在地址池模式下执行 **update arp** 命令。

配置地址池授权分配功能

- 用户请求命中开启授权分配模式的地址池网段时，终端需要进行固态绑定授权后才允许继续分配。
- 在地址池模式下执行 **solidify** 命令。

检验方法

利用 DHCP 客户端与 DHCP 服务器进行连接

- 检查客户端是否能取到服务器上配置的相关信息

相关命令

启动 DHCP-SERVER 功能

【命令格式】 **service dhcp**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 启用 DHCP 服务器和 DHCP 中继代理功能，DHCP 服务器和 DHCP 中继共用 **service dhcp** 这条命令，两功能可以同时存在，但是报文是通过 Relay 转发还是直接由 Server 处理，取决于设备上是否配置了合法有效的地址池，如果存在地址池则由 Server 处理，不存在由 Relay 转发。

配置地址池

【命令格式】 **ip dhcp pool** *dhcp-pool*

【参数说明】 *pool-name*：地址池名称

【命令模式】 全局模式

【使用指导】 要给用户下发地址，首先要配置地址池名并进入地址池配置模式

配置 DHCP 地址池的网络号和掩码

【命令格式】 **network** *network-number mask* [*low-ip-address high-ip-address*]

【参数说明】 *network-number:* DHCP 地址池的 IP 地址网络号

mask: DHCP 地址池的 IP 地址网络掩码。如果没有定义掩码，缺省为自然网络掩码

【命令模式】 DHCP 地址池配置模式

【使用指导】 进行动态地址绑定的配置，必须配置新建地址池的子网及其掩码，为 DHCP 服务器提供了一个可分配给客户端的地址空间。DHCP 在分配地址池中的地址，是按顺序进行的，如果该地址已经在 DHCP 绑定表中或者检测到该地址已经在该网段中存在，就检查下一个地址，直到分配一个有效的地址。

锐捷无线产品中新增了可以配置地址池的网段范围，指明可以分配的网段中的起始地址和终止地址，该配置为

可选配置。在不指明起始地址和终止地址的情况下，地址池的可分配的 IP 地址范围为该网段内的所有 IP 地址锐捷产品的 DHCP 动态地址池中 ,地址的分配是以客户端的物理地址和客户端 ID 为索引的 ,这就意味着 DHCP 动态地址池中不可能存在相同客户端的两份租约；如果客户端和服务器之间的网络拓扑存在路径上的冗余[客户端可以通过直连路径，同时也可以通过中继路径到达服务器]，就会导致服务器分配地址出现问题，可能导致地址分配失败；

因此，为了避免上述问题，要求网络管理员在构建网络的时候，通过其它的方式，如调整物理链路或者网络路径，来避免这种客户端到服务器的路径冗余

配置客户端缺省网关

【命令格式】 **default-router** *address* [*address2…address8*]

【参数说明】 *address*：定义客户端默认网关的 IP 地址。要求至少配置一个

ip-address2…ip-address8：（可选）最多可以配置 8 个网关

【命令模式】 DHCP 地址池配置模式

【使用指导】 配置客户端默认网关，这个将作为服务器分配给客户端的默认网关参数。缺省网关的 IP 地址必须与 DHCP 客户端的 IP 地址在同一网络

配置地址租期

【命令格式】 **lease** {*days* [*hours]* [*minutes*] | **infinite**}

【参数说明】 *days*：定义租期的时间，以天为单位

hours: （可选）定义租期的时间，以小时为单位。定义小时数前必须定义天数

minutes: （可选）定义租期的时间，以分钟为单位。定义分钟前必须定义天数和小时数

infinite: 定义没有限制的租期

【命令模式】 DHCP 地址池配置模式

【使用指导】 DHCP 服务器给客户端分配的地址，缺省情况下租期为 1 天。当租期快到时客户端需要请求续租，否则过期后就不能使用该地址

配置客户端启动文件

【命令格式】 **bootfile** *filename*

【参数说明】 *file-name*：定义用于启动的文件名

【命令模式】 DHCP 地址池配置模式

【使用指导】 客户端启动文件是客户端启动时要用到的启动映像文件。启动映像文件通常是 DHCP 客户端需要下载的操作系统

配置客户端的域名

【命令格式】 **domain-name** *domain*

【参数说明】 *domain-name:* 定义 DHCP 客户端的后缀域名字符串

【命令模式】 DHCP 地址池配置模式

【使用指导】 可以指定客户端的域名，这样当客户端通过主机名访问网络资源时，不完整的主机名会自动加上域名后缀形成完整的主机名

配置域名服务器

【命令格式】 **dns-server** { *ip-address* [*ip-address2…ip-address8*] | **use-dhcp-client** *interface-type interface-number* }

【参数说明】 *ip-address:* 定义 DNS 服务器的 IP 地址。要求至少配置一个

ip-address2…ip-address8: （可选）最多可以配置 8 个 DNS 服务器

use-dhcp-client *interface-type interface-number:* 用通过 RGOS 软件的 DHCP 客户端学到的 DNS 服务器，作为 DHCP 客户端的 DNS 服务器

【命令模式】 DHCP 地址池配置模式

【使用指导】 当客户端通过主机名访问网络资源时，需要指定 DNS 服务器进行域名解析。要配置 DHCP 客户端可使用的域名服务器

配置 NetBIOS WINS 服务器

【命令格式】 **netbios-name-server** *address* [*address2…address8*]

【参数说明】 *address:* 定义 WINS 服务器的 IP 地址。要求至少配置一个

ip-address2…ip-address8: （可选）最多可以配置 8 个 WINS 服务器

【命令模式】 DHCP 地址池配置模式

【使用指导】 WINS 是微软 TCP/IP 网络解析 NetNBIOS 名字到 IP 地址的一种域名解析服务。WINS 服务器是一个运行在 Windows NT 下的服务器。当 WINS 服务器启动后，会接收从 WINS 客户端发送的注册请求，WINS 客户端关闭时，会向 WINS 服务器发送名字释放消息，这样 WINS 数据库中与网络上可用的计算机就可以保持一致了

配置客户端 NetBIOS 节点类型

【命令格式】 **netbios-node-type** *type*

【参数说明】 type: 定义 NetBIOS 节点类型，有两种方式

数字定义，范围从 0~FF，十六进制数，但只能取以下值：

- 1，代表 b-node
- 2，代表 p-node
- 4，代表 m-node
- 8，代表 h-node

字符串定义：

- b-node，广播型节点
- p-node，对等型节点
- m-node，混合型节点
- h-node，复合型节点

【命令模式】 DHCP 地址池配置模式

【使用指导】 微软 DHCP 客户端 NetBIOS 节点类型有四种：1）Broadcast，广播型节点，通过广播方式进行 NetBIOS 名字解析；2）Peer-to-peer，对等型节点，通过直接请求 WINS 服务器进行 NetBIOS 名字解析；3）Mixed，混合型节点，先通过广播方式请求名字解析，后通过与 WINS 服务器连接进行名字解析；4）Hybrid，复合型节点，首先直接请求 WINS 服务器进行 NetBIOS 名字解析，如果没有得到应答，就通过广播方式进行 NetBIOS 名字解析。

缺省情况下，微软操作系统的节点类型为广播型或者复合型。如果没有配置 WINS 服务器，就为广播型节点；如果配置了 WINS 服务器，就为复合型节点

配置自定义选项

【命令格式】 **option** *code* { **ascii** *string* | **hex** *string* | **ip** *ip-address* }

【参数说明】 *code:* 定义 DHCP 选项代码

ascii *string:* 定义一个 ASCII 字符串

hex *string:* 定义十六进制字符串

ip *ip-address:* 定义 IP 地址列表

【命令模式】 DHCP 地址池配置模式

【使用指导】 DHCP 提供了一个机制，允许在 TCP/IP 网络中将配置信息传送给主机。DHCP 报文专门有 option 字段，该部分内容为可变化内容，用户可以根据实际情况进行定义，DHCP 客户端必须能够接收携带至少 312 字节 option 信息的 DHCP 报文。另外 DHCP 报文中的固定数据字段也称为一个选项

在 WLAN 无线应用环境中，AP 上的 DHCP 客户端会动态申请获取 AC 的 IP 地址列表，可以通过在 DHCP 服务器上配置自定义选项携带 AC 的 IP 地址列表来实现

配置地址池启用或关闭

【命令格式】 **pool-status** {**enable | disable**}

【参数说明】 **enable***:* 启用地址池

disable*:* 关闭地址池

默认为开启

【命令模式】 DHCP 地址池配置模式

【使用指导】 在锐捷无线产品中新增了可配置 DHCP 地址池是否启用命令，通过配置命令可以启用或关闭对应地址池服务

配置添加可信 ARP

【命令格式】 **update arp**

【参数说明】 -

【命令模式】 DHCP 地址池配置模式

【使用指导】 配置 **update arp** 后，DHCP 从地址池分配地址时添加可信 ARP。可信 ARP 用于防止 ARP 欺骗。

配置授权分配模式

【命令格式】 **Solidify**

【参数说明】 -

【命令模式】 DHCP 地址池配置模式

【使用指导】 DHCP 服务器地址池启用该功能后，终端匹配中该地址池进行分配时，需要进行固态绑定授权才能继续分配。

配置举例

配置地址池

【配置方法】

- 定义了一个地址池 net172
- 地址池网段为 172.16.1.0/24
- 缺省网关为 172.16.1.254
- 地址租期为 1 天
- 排除 172.16.1.2~172.16.1.100 地址

```
Ruijie(config)# ip dhcp excluded-address 172.16.1.2 172.16.1.100
```

```
Ruijie(dhcp-config)# ip dhcp pool net172
Ruijie(dhcp-config)# network 172.16.1.0 255.255.255.0
Ruijie(dhcp-config)# default-router 172.16.1.254
Ruijie(dhcp-config)# lease 1
```

【检验方法】 1.**show run** 查看

```
Ruijie(config)#show run | begin ip dhcp
ip dhcp excluded-address 172.16.1.2 172.16.1.100
ip dhcp pool net172
network 172.16.1.0 255.255.255.0default-router 172.16.1.254
lease 1
```

2.5.2 配置 DHCP 服务器手工地址绑定

配置效果

向某些特定的 dhcp-client 下发特定的 ip 地址及其它配置信息

注意事项

无

配置方法一

↘ 配置地址池名并进入地址池配置模式

- 创建地址池，为必选配置。
- 在配置模式下执行 **ip dhcp pool** 命令。

↘ 配置客户端主机的 IP 地址和网络掩码

- 配置静态 ip 地址及网络掩码，必选配置。
- 在地址池模式下执行 **host** 命令。

↘ 配置客户端的硬件地址

- 配置静态 mac 地址，可选配置。
- 在地址池模式下执行 **hardware** 命令。

↘ 配置客户端的唯一标识

- 配置静态用户 uid，可选配置。
- 在地址池配置下执行 **client-identifier** 命令。

↘ 配置客户端的名字

- 配置静态用户名字，可选配置。
- 在地址池模式下执行 **host-name** 命令。

检验方法

对应的用户上线，判断是否能取到相应地址。

相关命令

↘ 配置地址池

【命令格式】 **ip dhcp pool** *dhcp-pool*
【参数说明】 *pool-name*：地址池名称
【命令模式】 全局模式
【使用指导】 要给用户下发地址，首先要配置地址池名并进入地址池配置模式

↘ 手工地址绑定

【命令格式】 **host** *ip-address* [*netmask*]
client-identifier *unique-identifier*
client-name *name*
【参数说明】 **i***p-address:* 定义 DHCP 客户端主机的 IP 地址
netmask: 定义 DHCP 客户端主机的网络掩码
unique-identifier : 定义客户端硬件地址，如 aabb.bbbb.bb88;定义客户端的标识，如 01aa.bbbb.bbbb.88
name: （可选）用标准的 ASCII 字符定义客户端的名字，名字不要包括域名。如定义 mary 主机名，不可定义成 mary.rg.com
【命令模式】 DHCP 地址池配置模式
【使用指导】 地址绑定是指 IP 地址和客户端 MAC 地址的映射关系。地址绑定有两种：1）手工绑定，就是在 DHCP 服务器数据库中，通过手工定义将 IP 地址和 MAC 地址进行静态映射，手工绑定其实是一个特殊地址池；2）动态绑定，DHCP 服务器接收到 DHCP 请求时，动态地从地址池中分配 IP 地址给客户端，而形成的 IP 地址和 MAC 地址映射。
要定义手工地址绑定，首先需要为每一个手动绑定定义一个主机地址池，然后定义 DHCP 客户端的 IP 地址和硬件地址或客户端标识。硬件地址就是 MAC 地址。客户端标识，微软客户端一般定义客户端标识，而不定义 MAC 地址，客户端标识包含了网络媒介类型和 MAC 地址。关于媒介类型的编码，请参见 RFC 1700 中关于“Address Resolution Protocol Parameters”部分内容。以太网类型为“01”

配置举例

↘ 动态地址池

【配置方法】
- 地址池 vlan1 20.1.1.0 255.255.255.0

- 缺省网关为 20.1.1.1
- 租约时间为 1 天

```
Ruijie(config)# ip dhcp pool vlan1
Ruijie(dhcp-config)# network 20.1.1.0 255.255.255.0
Ruijie(dhcp-config)# default-router 20.1.1.1
Ruijie(dhcp-config)# lease 1 0 0
```

【检验方法】 1. show run 查看

```
Ruijie(config)#show run | begin ip dhcp
ip dhcp pool vlan1
network 20.1.1.0 255.255.255.0
default-router 20.1.1.1
lease 1 0 0
```

↘ 手工绑定配置

【配置方法】

- 主机地址 172.16.1.101，掩码为 255.255.255.0
- 主机名 Billy.rg.com
- 缺省网关为 172.16.1.254
- MAC 地址为 00d0.df34.32a3

```
Ruijie(config)# ip dhcp pool Billy
Ruijie(dhcp-config)# host 172.16.1.101 255.255.255.0
Ruijie(dhcp-config)# client-name Billy
Ruijie(dhcp-config)# hardware-address 00d0.df34.32a3 ethernet
Ruijie(dhcp-config)# default-router 172.16.1.254
```

【检验方法】 1.**show run** 查看

```
Ruijie(config)#show run | begin ip dhcp
ip dhcp pool Billy
host 172.16.1.101 255.255.255.0
client-name Billy
hardware-address 00d0.df34.32a3 ethernet
default-router 172.16.1.254
```

配置方法二

↘ 配置地址池名并进入地址池配置模式

- 创建地址池，为必选配置。
- 在配置模式下执行 **ip dhcp pool** 命令。

↘ 配置静态地址绑定

- 静态地址绑定，必选配置。
- 在地址池模式下执行 **static-bind** 命令。

检验方法

- 对应的用户上线，判断是否能取到相应地址。

相关命令

↘ 配置地址池

【命令格式】 **ip dhcp pool** *dhcp-pool*

【参数说明】 *pool-name*：地址池名称

【命令模式】 全局模式

【使用指导】 要给用户下发地址，首先要配置地址池名并进入地址池配置模式

↘ 手工地址绑定

【命令格式】 **static-bind ip-address** *ip-address* { *mask-len* | *mask-address* } { **hardware-address** *hardware-address* | **client-identifier** *unique-identifier* }

【参数说明】 **i***p-address:* 定义 DHCP 客户端主机的 IP 地址

netmask: 定义 DHCP 客户端主机的网络掩码

hardware-address: 定义客户端硬件地址，如 aabb.bbbb.bb88;

unique-identifier : DHCP 客户端的标识，以点隔开的十六进制表示，有效字符长度必须为偶数位。如：0100.d0f8.2233.b4

【命令模式】 DHCP 地址池配置模式

【使用指导】 地址绑定是指 IP 地址和客户端 MAC 地址或者客户端标识符的映射关系。地址绑定有两种：1）手工绑定，就是在 DHCP 服务器数据库中，通过手工定义将 IP 地址和 MAC 地址进行静态映射，手工绑定其实是一个特殊地址池；2）动态绑定，DHCP 服务器接收到 DHCP 请求时，动态地从地址池中分配 IP 地址给客户端，而形成的 IP 地址和 MAC 地址映射。

可以在地址池下多次使用 static-bind 命令绑定多个静态用户，一个 ip 地址只能绑定一个静态用户，绑定方式只能是 MAC 地址或者客户端标识。

static-bind 命令可以同 network 命令共存。配置时 static-bind 绑定的 IP 地址不一定需要和 network 在同网段，因为静态绑定配置和 network 配置不存在任何互斥关系，只是需要共用地址池下的配置信息。所以如果有配置默认路由时，需要保证存在路由能让静态绑定 IP 和 network 网段的 IP 均能正常联网。例如：通过 static-bind 绑定静态地址 10.1.1.10/24 后，network 配置为 10.1.2.1 255.255.255.0 时，如果网关地址为 10.1.1.1，且网关接口掩码为 16 位时，是可以共用该网关的。如果网关接口的掩码为 24 位时，则需要增加网关地址 10.1.2.1 来满足 network 网段的联网需求。

配置举例

↘ 手工绑定配置

【配置方法】
- 主机地址 172.16.1.101，掩码为 255.255.255.0
- 缺省网关为 172.16.1.254
- MAC 地址为 00d0.df34.32a3

```
Ruijie(config)# ip dhcp pool Billy
Ruijie(dhcp-config)# static-bind ip-address 172.16.1.101 255.255.255.0 hardware-address 00d0.df34.32a3
Ruijie(dhcp-config)# default-router 172.16.1.254
```

【检验方法】 1.**show run** 查看

```
Ruijie(config)#show run | begin ip dhcp
static-bind ip-address 172.16.1.101 255.255.255.0 hardware-address 00d0.df34.32a3
default-router 172.16.1.254
```

2.5.3 配置 DHCP 服务器全局属性

配置效果

开启服务器一些特定的功能，如 ping 机制、强制 nak 等。

注意事项

Nak 命令的配置可能引起网络中其它服务器的功能异常。

配置方法

↘ 配置排除地址

- 配置某些地址或地址段不可用，为可选配置。
- 在配置模式下执行 **ip dhcp excluded-address** 命令

↘ 配置 DHCP 服务器强制回复 NAK

- 针对某些用户的错误地址请求，服务器回复 nak 报文，可选配置。
- 在配置模式下执行 **ip dhcp force-send-nak** 命令。

配置监控 VRRP 状态

- 启动该功能后，主机 server 处理 DHCP 相关报文，备机 server 则不处理 DHCP 相关报文，可选配置。
- 在配置模式下执行 **ip dhcp monitor-vrrp-state** 命令。

配置 Ping 包次数

- 检查地址的可达性，执行 **ping** 操作，默认值为 2，可选配置。
- 在配置模式下执行 **ip dhcp ping packet** 命令。

配置 Ping 包超时时间

- 检查地址的可达性，设置 **ping** 返回时长，默认值为 500ms， 可选配置。
- 在配置模式下执行 **ip dhcp ping timeout** 命令。

配置 DHCP 服务器重新下发可信 ARP

- 用于配置 DHCP 服务器重新下发可信 ARP。只根据从配置有 **update arp** 的地址池上分配出去的地址重新下发可信 ARP。
- 在配置模式下执行 **ip dhcp refresh arp** 命令。

配置伪服务器检测

- 启动该功能后，网络中存在伪服务器，会记录在日志中，可选配置。
- 在配置模式下执行 **ip dhcp server detect** 命令。

检验方法

启动 **dhcp-server** 下发地址过程中可检验。

相关命令

配置排除地址

【命令格式】 **ip dhcp excluded-address** *low-ip-address* [*high-ip-address*]

【参数说明】 *low-ip-address:* 排斥 IP 地址范围的起始 IP 地址

high-ip-address : 排斥地址范围的结束 IP 地址

【命令模式】 全局模式

【使用指导】 如果没有特别配置，DHCP 服务器会试图将在地址池中定义的所有子网地址分配给 DHCP 客户端。因此，如果想保留一些地址不分配，比如已经分配给服务器或者设备了，必须明确定义这些地址是不允许分配给客户端的；配置 DHCP 服务器，一个好的习惯是将所有已明确分配的地址全部不允许 DHCP 分配，这样可以带来两个好处：1）不会发生地址冲突；2）DHCP 分配地址时，减少了检测时间，从而提高 DHCP 分配效率

配置 DHCP 服务器强制回复 NAK

【命令格式】 **ip dhcp force-send-nak**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 在无线应用中，DHCP 客户端的移动性较大，DHCP 客户端会经常性的从一个网络移动到另一个网络中。当 DHCP 服务器在收到客户端的 Request 续租报文时，发现客户端的网段发生更改或者是租约超时会给予回复 NAK，要求客户端重新获取 IP 地址，避免客户端不断发送 Request 报文直至超时后重新获取 IP 地址，延长 IP 地址获取时间。

但是，DHCP 服务器发送 NAK 报文的前提是该 DHCP 客户端在自己的管理范围之内，也就是可以查找到对应的租约记录信息。当 DHCP 客户端从另一个网络环境中移入时，DHCP 服务器将无法在本地查找到对应的租约记录信息，不予回复 NAK，此时 DHCP 客户端需要不断发送 Request 报文直至超时后重新获取 IP 地址，导致 IP 地址获取时间变长。在 DHCP 服务器重启时丢失客户端租约，而客户端要求续租时也会遇到类似情况。在这种情况下，可以通过配置命令强制让 DHCP 服务器在查找不到租约记录时也给予回复 NAK 报文，触发客户端快速获取到 IP 地址，注意：默认情况下该条命令关闭；在开启该命令的时候，在同一广播域内，不允许开启多台 DHCP 服务器

配置 Ping 包次数

【命令格式】 **ip dhcp ping packets** [*number*]

【参数说明】 *Number：*（可选）范围从 0 到 10，0 表示关闭 ping 操作。缺省 ping 两个包

【命令模式】 全局配置模式

【使用指导】 缺省情况，当 DHCP 服务器试图从地址池中分配一个 IP 地址时，会对该地址执行两次 Ping 命令(一次一个数据包)。如果 Ping 没有应答，DHCP 服务器认为该地址为空闲地址，就将该地址分配给 DHCP 客户端；如果 Ping 有应答，DHCP 服务器认为该地址已经在使用，就试图分配另外一个地址给 DHCP 客户端，直到分配成功

配置 Ping 包超时时间

【命令格式】 **ip dhcp ping timeout** *milliseconds*

【参数说明】 *milli-seconds：*DHCP 服务器等待 ping 应答的时间（以毫秒计）。取值范围为 100 到 10000

【命令模式】 全局配置模式

【使用指导】 缺省情况下，DHCP 服务器 Ping 操作如果 500 毫秒没有应答，就认为没有该 IP 地址主机存在。可以通过调整 Ping 包超时时间，改变服务器 Ping 等待应答的时间

配置重新下发可信 ARP

【命令格式】 **ip dhcp refresh arp**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 缺省情况下，如果 DHCP 地址池上配置 **update arp**，DHCP 服务器在分配地址时会下发可信 ARP。如果用户清除掉可信 ARP 后，DHCP 服务器不会主动重新下发可信 ARP。配置该命令后，DHCP 服务器可以根据配置有 **update arp** 的地址池上分配出去的地址重新下发可信 ARP。

配置伪服务器检测

【命令格式】 **ip dhcp server detect**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 缺省情况下，DHCP 服务器是关闭伪服务器检测功能。配置该命令后，DHCP 服务器可以检测网络中存在的

伪服务器。

配置举例

配置 ping 机制

【配置方法】
- 配置 ping 次数为 5
- 配置 ping 超时时长为 800ms

```
Ruijie(config)# ip dhcp ping packet 5
Ruijie(config)# ip dhcp ping timeout 800
```

【检验方法】 1.**show run** 查看

```
Ruijie(config)#show run | begin ip dhcp
ip dhcp ping packet 5
ip dhcp ping timeout 800
```

配置排除地址

【配置方法】
- 排除 192.168.0.0 – 192.168.255.255 的所有地址

```
Ruijie(config)# ip dhcp excluded-address 192.168.0.0 192.168.255.255
```

【检验方法】 1.**show run** 查看

```
Ruijie(config)#show run | begin ip dhcp
ip dhcp excluded-address 192.168.0.0 192.168.255.255
```

2.5.4 配置 DHCP Relay 基本功能

配置效果

- 建立 Client—Relay—Server 模式的 DHCP 动态 IP 管理，解决 DHCP 客户端与 DHCP 服务器不在同一网段时 DHCP 客户端与在其他网段的 DHCP 服务器通讯问题。

注意事项

- DHCP Relay 需要借助网络中现有的单播路由。因此，网络中必须配置 IPv4 单播路由。

配置方法

启动 DHCP Relay 功能

- 必须配置。

- 若无特殊要求，应在设备上启动 DHCP Relay 功能。

配置 DHCP 服务器的 IP 地址

- 必须配置。
- 应在设备上启动 DHCP 服务器的 IP 地址。

检验方法

- 检查用户主机能否通过 DHCP Relay 成功获取到 IP 地址。

相关命令

启动 DHCP Relay 功能

【命令格式】 **service dhcp**
【参数说明】 **-**
【命令模式】 全局模式
【使用指导】 -

配置 DHCP 服务器的 IP 地址

【命令格式】 **ip helper-address { cycle-mode** *A.B.C.D* **}**
【参数说明】 *cycle-mode* ：开启 dhcp 请求报文转发所有 dhcp 服务器
A.B.C.D: Server 的 ip 地址
【命令模式】 全局模式、接口模式
【使用指导】 配置接口必须是三层接口，包括：路由口、L3AP、SVI、loopback 接口。
所有配置接口应 IPv4 单播路由可达。

配置举例

以下配置举例，仅介绍与 DHCP Relay 相关的配置。

有线场景中 DHCP Relay 配置

【网络环境】
图 2-9



【配置方法】
- 用户设备启动通过 DHCP 获取地址的功能。
- 在作为 DHCP Relay Agent 的网络设备中启动 DHCP Relay 功能。
- 配置 DHCP Server。

A 用户设备启动 DHCP 获取地址的功能。

B # 启用 DHCP 中继代理

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

添加一个全局的 DHCP 服务器的地址

```
Ruijie(config)# ip helper-address 172.2.2.1
```

配置与用户设备连接的端口的 IP 地址

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# ip address 192.1.1.1 255.255.255.0
```

配置与 Server 设备连接的端口的 IP 地址

```
Ruijie(config)# interface gigabitEthernet 0/2
Ruijie(config-if-gigabitEthernet 0/2)# ip address 172.2.2.2 255.255.255.0
```

C # 启用 DHCP SERVER 功能

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

添加一个客户端地址池

```
Ruijie(config)# ip dhcp pool relay
Ruijie (dhcp-config)#network 192.1.1.0 255.255.255.0
Ruijie (dhcp-config)#default-router 192.1.1.1
```

配置与 relay 设备连接的端口的 IP 地址

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-gigabitEthernet 0/2)# ip address 172.2.2.1 255.255.255.0
```

【检验方法】 查看用户是否能获取到 IP 地址。

- 检查用户设备是否能获取到 IP 地址。
- 检查 DHCP Relay 配置是否正确。

A 用户设备能获取到 IP 地址

B 登录到 DHCP Relay Agent 设备后在特权模式下用 **show running-config** 命令显示 DHCP Relay 配置

```
Ruijie# show running-config
service dhcp
ip helper-address 172.2.2.1
!
interface GigabitEthernet 0/1
ip address 192.1.1.1 255.255.255.0
!
interface GigabitEthernet 0/2
ip address 172.2.2.2 255.255.255.0
!
```

常见错误

- IPv4 单播路由配置错误。
- 没有启动 DHCP Relay 功能。

- 没有配置 DHCP Relay 与 DHCP Service 之间的路由。
- 没有配置 DHCP 服务器 IP 地址。

2.5.5 配置 DHCP Relay option 82 功能

配置效果

- 中继设备进行 DHCP Relay 时，可以通过添加 option 的方式来详细的标明 DHCP 客户端的一些网络信息，从而使服务器可以根据更精确的信息给用户分配不同权限的 IP。

注意事项

- 必须配置 DHCP Relay 基本功能。

配置方法

↘ 启动 DHCP Relay 基本功能

- 必须配置。
- 若无特殊要求，应在设备上启动 DHCP Relay 基本功能。

↘ 启动 DHCP option82 功能

- 缺省情况下，设备上的 DHCP option 82 功能关闭。
- 使用 **ip dhcp relay information option82 [standard-format | verbose-format]**命令可以启动或关闭设备上的 DHCP option 82 功能。

2.5.6 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
```

2.5.7 配置指定分配固定地址功能

配置效果

对指定接入位置、指定终端、指定终端主机名分配固定的 IP 地址。

注意事项

1.接入位置信息只有我司接入交换机作为终端接入时才能获取。

2.接入位置和主机名可能存在冲突，导致不能惟一标识终端时不能使用绑定位置和主机名分配固定地址。

配置方法

配置指定信息绑定固定 IP 地址

- 在配置模式下执行 **ip dhcp add-client …**命令。

检验方法

show run 查看相关配置是否成功。

相关命令

配置绑定指定信息分配固定地址

【命令格式】 **ip dhcp add-client { solidify-ip ip** *ip-addr* **{ { access-device** *dev-addr* **access-vlan** *vlanid* **access-port** *portid* **| host-name** *hostname* **| mac** *mac-addr* **} binding-type { ip-hostname | ip-hostname-location | ip-mac | ip-mac-hostname | ip-mac-hostname-location | ip-mac-location } } | solidify-location ip** *ip-addr* **access-device** *dev-addr* **access-vlan** *vlanid* **access-port** *portid* **| solidify-mac mac** *mac-addr* **}**

【参数说明】 Binding-type：固定地址绑定类型，包括接入位置、终端主机名、终端 MAC 地址的不同组合绑定分配 IP 地址

Ip-addr：绑定分配的固定 IP 地址

Dev-addr：接入设备的 IP 地址或 mac 地址

Vlanid：终端接入端口所属的 vlanid

Portid：终端接入设备的端口号

hostname：终端的主机名

mac-addr：终端的 mac 地址

【命令模式】 配置模式

【使用指导】 该命令属于 Server 配置；该功能用于分配固定 IP 地址，可以根据指定接入位置信息、指定用户主机名信息、指定终端 MAC 地址信息的之一、之二、之三分配固定的 IP 地址。

其中固态绑定信息同时用于授权分配，当地址池开启固态属性时，命中该地址池分配地址时只有固态绑定的信息匹配的终端才允许分配地址。单 MAC 绑定用户仅用于授权分配有效，非固态地址池下和动态分配 IP 地址功能相同。

配置举例

配置指定终端 MAC 地址分配固定 IP 地址

【配置方法】 **1：配置终端 MAC 地址 0000.dddd.eeee 固定分配 192.168.100.100。**

```
Ruijie(config)# ip dhcp add-client solidify-ip 192.168.100.100 mac 0000.dddd.eeee binding-type ip-mac
```

【检验方法】 通过 **show run** 可见配置成功

```
Ruijie(config)#sh run | in solidify
ip dhcp add-client solidify-ip 192.168.100.100 mac 0000.dddd.eeee binding-type ip-mac
```

2.6 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 DHCP 地址绑定	**clear ip dhcp binding** { *address* | *}
清除 DHCP 地址冲突	**clear ip dhcp conflict** { *address* | *}
清除 DHCP 服务器统计状态	**clear ip dhcp server statistics**
清除 DHCP 中继统计状态	**clear ip dhcp relay statistics**
清除 DHCP 服务器性能统计信息	**clear ip dhcp server rate**
清除 DHCP 伪服务器信息	**clear ip dhcp server detect**
清除 DHCP 待授权表项	**clear ip dhcp auth-agent**
清除 DHCP 动态在线表项	**clear ip dhcp dynamic-binding**
清除 DHCP 在线历史统计信息	**clear ip dhcp record-history**
清除 DHCP 固态绑定分配在线表项	**clear ip dhcp solid-binding**
清除 DHCP 业务告警信息	**clear ip dhcp warn-log**

查看运行情况

作用	命令
显示 DHCP 租约信息	**show dhcp lease**
显示 dhcp 用的套接字	**show ip dhcp socket**
显示已经分配的地址	**show ip dhcp binding**
显示创建的地址池	**show ip dhcp pool**
显示 dhcp-server 统计信息	**show ip dhcp server statistic**
显示 dhcp-relay 统计信息	**show ip dhcp relay statistic**
显示冲突地址	**show ip dhcp conflict**
显示 DHCP 伪伪服务器信息	**show ip dhcp server detect**
显示 server 状态、告警数量信息、认证继承开关	**show dhcp state**
显示所有地址池详细信息	**show dhcp all-pool json**

显示分拣地址池配置信息	**show ip dhcp sort-pool relate-oui json**
显示分拣地址池详细信息	**show ip dhcp sort-pool status**
显示在线 IP 的详细信息	**show ip dhcp online-agent x.x.x.x**
显示用户日志的配置信息	**show ip dhcp agent-log json**
显示待授权用户信息	**show ip dhcp auth-agent json**
显示告警内容详细信息	**show ip dhcp warn-log {address-conflict | address-shift | hist-addr-cflt | hist-addr-shift | hist-pool-exhaust | pool-exhaust | statistic }**
显示安全绑定信息	**show ip dhcp safe-bind**
显示历史在线详细信息	**show ip dhcp record-history json**
显示在线地址信息	**show ip dhcp history [detail]**
显示所有地址池使用状态信息	**show ip dhcp all-pool {stat | order {more-pool | used-number | used-percent}}**

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
DHCPagent 调试开关	**debug ip dhcp server agent**
DHCP 热备调试开关	**debug ip dhcp server ha**
DHCP 地址池调试开关	**debug ip dhcp server pool**
DHCP VRRP 调试开关	**debug ip dhcp server vrrp**
DHCP 打开所有调试开关	**debug ip dhcp server all**
DHCP 报文调试开关	**debug ip dhcp client**
DHCP Relay 事件调试开关。	**debug ip dhcp relay**

3 DNS

3.1 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

3.2 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

3.2.1 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

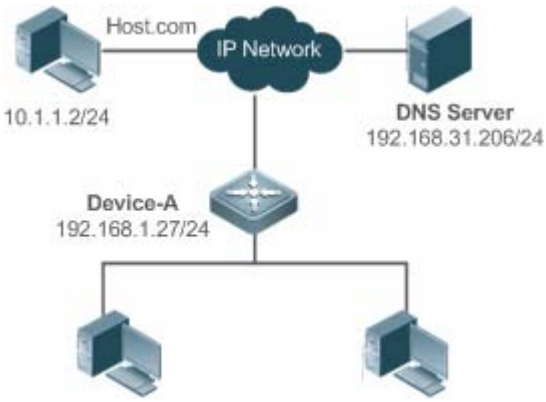
- 在设备上预设置域名和 IP 的对应关系

3.2.2 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 3-1 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

3.3 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

3.3.1 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：

8. 用户应用(Ping、Telnet 等)向系统 DNS 解析器请求域名对应的 IP
9. 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
10. 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
11. 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。

3.4 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	
	ip domain-lookup	开启域名解析功能
	ip host	配置域名对应的 IPv4 地址

3.4.1 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 IP 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        ---
```

3.4.2 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 3-2



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)
```

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
清除动态主机名缓存表。	**clear host** [*host-name*]

查看运行情况

作用	命令
查看 DNS 的相关参数	**show hosts** [*host-name*]

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**

4 DDNS

4.1 概述

DDNS（Dynamic Domain Name Server）是动态域名服务的缩写。

DDNS 是将动态 IP 地址映射到一个固定的域名解析服务上，每次连接网络的时候客户端程序就会通过信息传递把该主机的动态 IP 地址传送给位于服务商主机上的服务器程序，服务器程序负责提供 DNS 服务并实现动态域名解析。

DDNS 服务是将宽带服务提供商（ISP）分配给设备的动态公网 IP 地址与在域名进行绑定。对于使用动态 IP 接入的用户，通过 DDNS 将动态 IP 绑定到固定域名，并将内部服务映射到公网，在互联网上就可以通过固定域名访问用户提供的服务。

目前锐捷网关设备支持花生壳和 3322 提供的动态域名解析，下文仅介绍花生壳和 3322 动态域名解析的相关内容。

4.2 典型应用

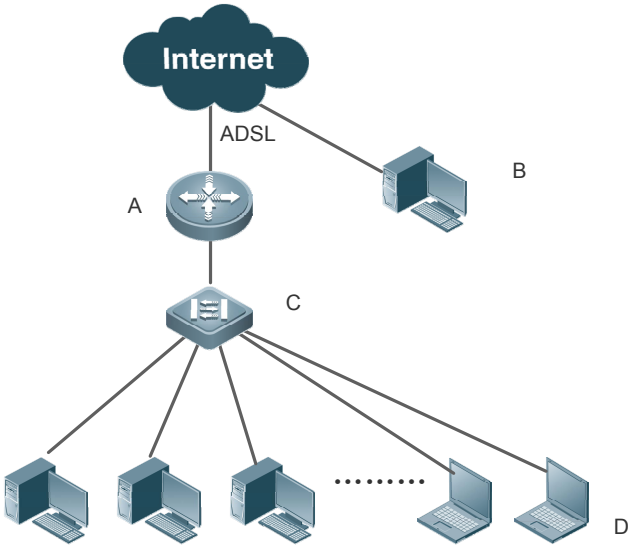
典型应用	场景描述
动态拨号出口网关部署	在动态拨号出口环境部署动态域名解析

4.2.1 动态拨号出口网关部署

应用场景

在一些小型网吧中，网关设备通过拨号上网，网关设备作为动态域名客户端，向动态域名服务器注册域名 IP。

图 4-1



【注释】 A 出口网关设备。
B 动态域名服务器（花生壳或者 3322）
C 为交换机。
D 为接入设备。

功能部属

- 内网通过拨号上线
- 出口网关设备作为动态域名客户端，向动态域名服务器注册域名 IP
- 外网通过动态域名访问出口网关设备

4.3 功能详解

基本概念

无。

功能特性

功能特性	作用
连接动态域名服务器	连接动态域名服务器，验证用户名密码并绑定设备接口，将设备 IP 和域名进行绑定.

4.3.1 连接动态域名服务器

连接动态域名服务器，验证用户名密码，将设备 IP 和域名进行绑定。

工作原理

通过实现动态域名客户端协议，从而使得出口网关设备成为动态域名客户端，为客户提供动态域名服务。

4.4 产品说明

NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR108G-P、NBR800G、NBR950G、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E 支持 3322 域名 DDNS 功能；NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1500G、NBR2000G 不支持 3322 域名 DDNS 功能。

4.5 配置详解

配置项	配置建议 & 相关命令	
配置动态域名账号	必须配置。用于连接动态域名服务器，验证用户名密码并绑定设备接口，将设备 IP 和域名进行绑定。	
	ddns service *service* [**domain** *domain*] **username** *username* **password** *password* **service** *service* [**interface** *interface-name*]	配置动态域名账号并绑定接口

4.5.1 配置动态域名账号

配置效果

- 连接动态域名服务器，验证用户名密码并绑定设备接口，将设备 IP 和域名进行绑定。

注意事项

- 无。

配置方法

配置动态域名

- 必须配置。默认无配置。
- 配置动态域名账号密码后，设备立即向动态域名服务器发起连接，验证账号密码，并绑定设备 IP 和域名。

【命令格式】 **ddns service** *service* [**domain** *domain*] **username** *username* **password** *password* **service** *service* [**interface** *interface-name*]

【参数说明】 *service*：动态域名服务平台(可选 oray 花生壳或者 3322)

domain：3322 域名（动态域名服务平台选择 3322 时需要输入）

username：动态域名账号

password：密码

interface-name：设备外网接口

【缺省配置】 不指定绑定接口

【命令模式】 全局模式

【使用指导】 -

检验方法

检查设备动态域名账号状态。

【命令格式】 **show ddns**

【参数说明】 -

【命令模式】 特权模式、全局模式

【使用指导】 查看动态域名账号状态。

【命令展示】

```
Ruijie#show ddns
------------------[0]------------------
status: Success
code: none
service: oray
username: rujie
password: ruijie
domain: ruijie.imwork.net
interface: Gi0/7
------------------[1]------------------
status: Success
code: good
service: 3322
username: ruijie
password: ruijie
domain: ruijie.f3322.net
interface:
```

关于 show 信息的详细解释请参看对应功能的命令手册。

配置举例

配置动态域名账号

【配置方法】

- 配置花生壳和 3322 账号密码并绑定设备接口

```
Ruijie#configure terminal
Ruijie (config)# ddns service oray username ruijie password ruijie interface GigabitEthernet 0/7
Ruijie (config)# ddns service 3322 domain ruijie.f3322.net username ruijie password ruijie interface GigabitEthernet 0/7
```

【检验方法】

- 使用 show ddns 命令检查账号状态。

```
Ruijie#show ddns
------------------[0]------------------
status: Success
code: none
service: oray
username: rujie
password: ruijie
```

```
domain: ruijie.imwork.net
interface: Gi0/7
------------------[1]-------------------
status: Success
code: good
service: 3322
username: ruijie
password: ruijie
domain: ruijie.f3322.net
interface:
```

常见错误

- 动态域名账号密码错误。
- 设备未正确配置 DNS，无法正确解析出动态域名服务器 IP。
- 动态域名服务器不可达。

4.6 监视与维护

清除各类信息

无

查看运行情况

作用	命令
查看设备动态域名账号状态。	**show ddns**

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
动态域名调试总开关	**debug ddns all**
动态域名处理调试开关	**debug ddns proc**
花生壳账号调试开关	**debug ddns oray**
3322 账号调试开关	**debug ddns pubyun**

5 NTP

5.1 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，提供高精准度的时间校正（LAN 上与标准时间差小于 1 毫秒，WAN 上几十毫秒），且可使用加密确认的方式来防止攻击。

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)

5.2 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。
基于本地时钟参考源同步时间	设备将本地时钟作为 NTP 可靠参考时钟源，作为服务器向其它设备提供时间同步服务。

5.2.1 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 5-1



功能部属

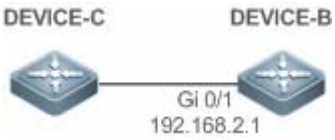
将 DEVICE-B 配置为 NTP 外部时钟参考模式

5.2.2 基于本地时钟参考源同步时间

应用场景

如图所示，DEVICE-B 将本地时钟作为 NTP 参考时钟源，向 DEVICE-C 提供时间同步服务。

图 5-2



功能部属

将 DEVICE-B 配置为 NTP 本地时钟参考模式。

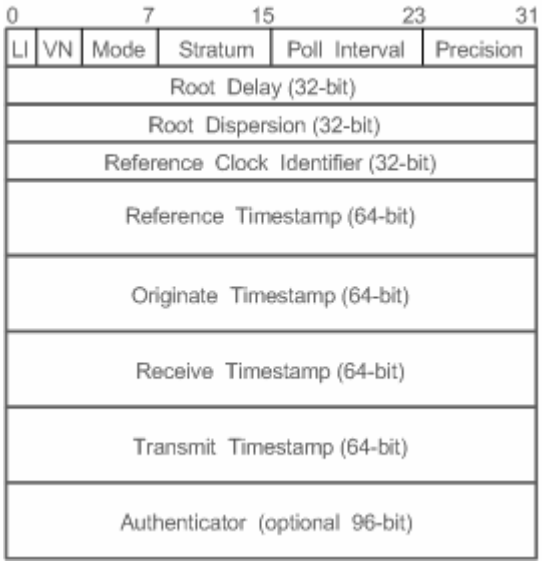
5.3 功能详解

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 5-3 NTP 时间同步报文格式



- Leap Indicator（LI）：2 比特，闰秒标志。

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。

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，相对于祝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
- Autherticator（可选）：验证信息

NTP 服务器

设备将本地时钟作为参考时钟源，为网络中的其它设备提供时间同步服务。

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，以实现高精准度的时间校正。
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。
NTP 访问控制	根据访问控制列表对收到的 NTP 报文进行源过滤。

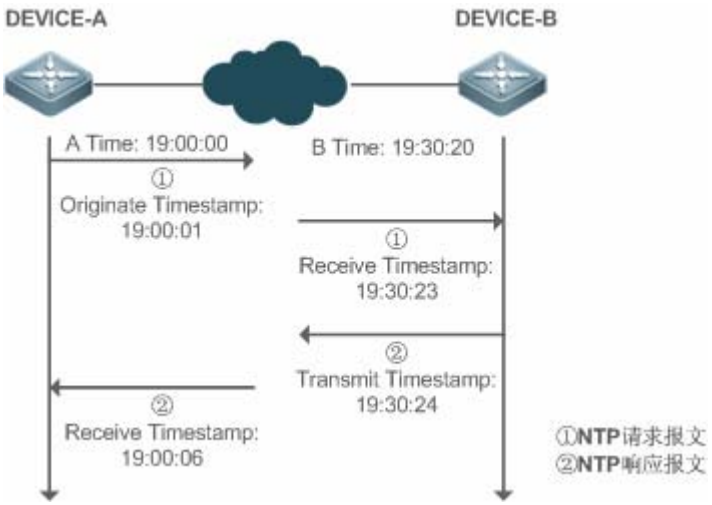
5.3.1 NTP 时间同步

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。

图 5-3 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：

12. 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
13. 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
14. 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
15. 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。

- 本地时钟参考模式

在该模式下，设备默认本地时钟即为可靠时钟源，直接向其它客户提供时间同步服务。

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。

配置 NTP 主时钟

- 缺省情况下，设备处于外部时钟参考模式。
- 通过 **ntp master** 命令可以将设备配置为本地时钟参考模式。

5.3.2 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。

5.3.3 NTP 访问控制

工作原理

通过 ACL 提供了一种最小限度的安全措施

相关配置

↘ 配置 NTP 服务的访问控制权限

- 缺省情况下，没有 NTP 访问控制权限。

- 通过 **ntp access-group** 可配置 NTP 的访问控制权限。

5.4 产品说明



NRB108G-P、NBR800G、NBR950G、NBR1000G-C、NBR1000G-E、NBR6120-E 不支持 NTP； NBR1500G、NBR2000G、NBR2000G-C、NBR3000G-S、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 NTP。

5.5 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。	
	ntp server	配置 NTP 服务器
	ntp update-calendar	自动更新硬件时钟
	可选配置，用于将设备配置为本地时钟参考模式。	
	ntp master	配置 NTP 主时钟
	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
配置 NTP 访问控制	可选配置，用于对收到的 NTP 报文进行源过滤。	
	ntp access-group	设置 NTP 的访问控制权限

5.5.1 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

本地时钟参考模式

- 设备的本地时钟作为 NTP 参考时钟源，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。
- 一旦配置本地时钟参考模式，系统便不会与比其时钟层数数值更高的时钟源进行同步。
- 将本地时钟设置为主时钟（尤其是指定了较低的时钟层数值时）很有可能将真正的有效时钟源覆盖。如果对同一网络中的多个设备都使用了该命令，则可能由于设备之间的时钟差异导致网络的时钟同步不稳定。
- 将本地时钟设置为主时钟前，如果系统从未与外部时钟源同步过，则有可能需要手动校准系统时钟以保证其不会有过大的偏差（关于如何手动校准系统时钟请参考配置指南中的系统时间配置部分）。

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。

配置 NTP 主时钟

- 如果需要将设备切换到本地时钟参考模式，可通过此命令。

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**[**oob**]{ *ip-addr* | *domain* | **ip** *domain* }[**version** *version*][**source** *if-name*][**key** *keyid*][**prefer**]

【参数说明】 oob：参考时钟源是否绑定 MGMT 口

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 Gi gabitEthernet、Loopback、Multilink、Null、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】 **-**

设置本地参考时钟源

【命令格式】 **ntp master**[*stratum*]

【参数说明】 *stratum*：指定本地时钟所处的层数，范围为 1～15；若不指定该参数则默认值为 8。

【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】 -

配置举例

NTP 外部时钟参考模式

【网络环境】

图 5-4



- DEVICE-B：配置为 NTP 外部时钟参考模式
- 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-A 配置本地时钟为 NTP 参考时钟源
- 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-A

```
A#configure terminal
A(config)# ntp master
A(config)#exit
```

DEVICE-B

```
B#configure terminal
B(config)# ntp server 192.168.1.1
B(config)# exit
```

DEVICE-C

```
C#configure terminal
C(config)# ntp server 192.168.2.1
C(config)# exit
```

【检验方法】

- 在 DEVICE-B 上通过 **show ntp status** 查看 NTP 配置信息。
- DEVICE-B 会向 192.168.1.1 发送时间同步报文，从 DEVICE-A 同步时间。
- DEVICE-B 从 DEVICE-A 成功同步时间之后，可以响应 DEVICE-C 的时间同步请求。
- 在 DEVICE-B 和 DEVICE-C 上通过 **show clock** 命令可以查看时间是否成功同步。

NTP 本地时钟参考模式

【网络环境】

图 5-5



- DEVICE-B：本地时钟为 NTP 参考时钟源
- DEVICE-C：从 DEVICE-B 同步时间

【配置方法】

- DEVICE-B 配置本地时钟为 NTP 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 master B(config)# exit
DEVICE-C	C#configure terminal C(config)# ntp server 192.168.2.1 C(config)# exit

【检验方法】
- 在 DEVICE-C 上通过 **show clock** 命令可以查看时间是否成功同步。

5.5.2 配置 NTP 安全认证

配置效果

从可信参考时钟源同步时间

设备作为客户端，只从可信任的外部参考时钟源同步时间到本地时钟

给可信设备提供时间同步服务

设备的本地时钟作为 NTP 参考时钟源，只对可信的设备提供时间同步服务

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** 查看是只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 5-6



- 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

5.5.3 配置 NTP 访问控制

配置效果

NTP 服务的访问控制功能提供了一种最小限度的安全措施（更安全的方法是使用 NTP 身份验证机制）。

注意事项

- 目前系统暂未支持控制查询功能(用于通过网络管理设备对 NTP 服务器进行控制 如设置闰秒标记或监控其工作状态等)。虽然是按照上述顺序进行规则匹配，但涉及到与控制查询相关的请求都无法支持。
- 如果未配置任何访问控制规则，则所有访问都是允许的。但一旦配置了访问控制规则，则仅有规则中所允许的访问才能进行。

相关配置

设置 NTP 的访问控制权限

- 可选配置
- 通过 **ntp access-group** 配置 NTP 访问控制权限及对应的 ACL

检验方法

通过 **show run** 查看 NTP 配置是否正确配置

相关命令

配置 NTP 服务的访问控制权限

【命令格式】 **ntp access-group** { **peer** | **serve** |**serve-only** | **query-only** }*access-list-number* | *access-list-name*

【参数说明】 **peer**：既允许对本地 NTP 服务进行时间请求和控制查询，也允许本地设备与远程系统同步时间（完全访问权限）。

serve：允许对本地 NTP 服务进行时间请求和控制查询，但不允许本地设备与远程系统同步时间。

serve-only：仅允许对本地 NTP 服务进行时间请求。

query-only：仅允许对本地 NTP 服务进行控制查询。

access-list-number：IP 访问控制列表标号；范围为 1～99 和 1300～1999。关于如何创建 IP 访问控制列表请参考《ACL》中的相关描述。

access-list-name：IP 访问控制列表名。关于如何创建 IP 访问控制列表请参考《访问控制列表配置指南》中的相关描述。

【命令模式】 全局模式

【使用指导】 配置 NTP 访问控制权限。

当一个访问请求到达时，NTP 服务按照从最小访问限制到最大访问限制的顺序依次匹配规则，以第一个匹配到的规则为准。匹配顺序为 peer、serve、serve-only、query-only。

配置举例

NTP 访问控制权限配置

【配置方法】 配置只允许 192.168.1.1 的设备对本地设备进行时间同步请求

```
Ruijie(config)# access-list 1 permit 192.168.1.1
Ruijie(config)# ntp access-group serve-only 1
```

5.6 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。

6 SNTP

6.1 概述

SNTP(Simple Network Time Protocol ,简单网络时间协议)是 NTP 的简化版本 ,主要用来同步因特网中的计算机时钟。 SNTP 适用于无需完全使用 NTP 功能的情况。

NTP 算法复杂，对系统要求较高。而 SNTP 在实现时，计算时间用了简单的算法，性能较高。而精确度一般也能达到 1 秒左右，也能基本满足绝大多数场合的需要。由于 SNTP 的报文和 NTP 的报文是完全一致的，所以设备实现的 SNTP Client 能完全兼容 NTP Server。

下文仅介绍 SNTP 的相关内容。

协议规范

- RFC 2030：Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI

6.2 典型应用

典型应用	场景描述
从 NTP 服务器同步时间	设备作为客户端，从 NTP 服务器同步时间

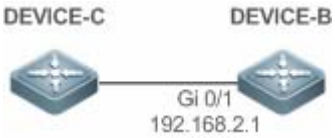
6.2.1 从 NTP 服务器同步时间

应用场景

如图所示，DEVICE-B 将本地时钟作为 NTP 参考时钟源，向 DEVICE-C 提供时间同步服务。

DEVICE-C 作为 SNTP 客户端，从 DEVICE-B 同步时间。

图 6-1



功能部属

- 指定 DEVICE-B 为 DEVICE-C 的 SNTP 服务器。

- DEVICE-C 开启 SNTP 功能

6.3 功能详解

基本概念

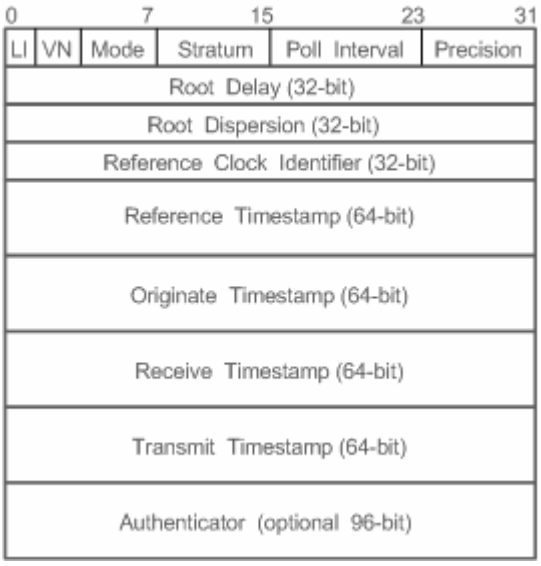
SNTP 报文

SNTPV4 是从 NTP 发展过来的，主要是简化 NTP 的功能。SNTPV4 并没有改变 NTP 规范和原有实现过程。SNTPV4 的消息格式于 RFC1305 中定义的 NTP 格式是一致的，只是一些数据域被初始化为预定的值。

同 RFC1305 定义，SNTP 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错误!**书签自引用无效。**

图 6-2 SNTP 时间同步报文格式



- Leap Indicator（LI）：2 比特，闰秒标志。

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/SNTP 版本号，当前版本号为 3。
- Mode：3 比特，SNTP/NTP 工作模式。

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，相对于祝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
- Autherticator（可选）：验证信息

功能特性

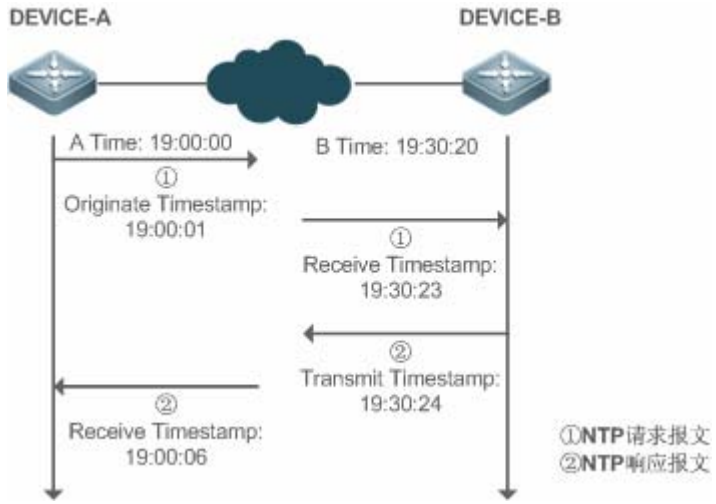
功能特性	作用
SNTP 时间同步	从 SNTP/NTP 服务器同步时间到本地设备。

6.3.1 SNTP 时间同步

工作原理

SNTP 同步时间的方式是与服务器之间交互 SNTP/NTP 报文。客户端每隔一段时间（默认是半小时）向服务器发送时间同步报文。收到服务器响应报文后进行时间同步。

SNTP 时间同步报文格式如图 6-3 SNTP 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 SNTP 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：

16. A 发出 SNTP/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

17. 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

18. 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

19. 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

相关配置

打开 SNTP

- 缺省 SNTP 状态是关闭的。
- 通过 **sntp enable** 命令开启 SNTP 功能

配置 SNTP 服务器

- 缺省情况下，没有配置 SNTP 服务器。
- 通过 **sntp server** 命令指定 SNTP 服务器。

配置 SNTP 同步时钟间隔

- 缺省情况下，SNTP 同步时钟的间隔是 1800s。
- 通过 **sntp interval** 命令指定 SNTP 服务器。

6.4 配置详解

配置项	配置建议&相关命令	
配置 SNTP	必须配置，用于开启 SNTP 功能	
	sntp enable	打开 SNTP
	sntp server	配置 SNTP Server 的地址
	可选配置，用于调整 SNTP 时间同步间隔	
	sntp interval	配置 SNTP 同步时钟的间隔

6.4.1 配置 SNTP

配置效果

SNTP Client 一定的时间间隔定期访问 NTP Server，可以定时校正时钟。

注意事项

通过 SNTP 协议通讯后获取的时间都是格林威治标准时间（GMT），为了准确的获取本地时间，需要设置本地时区来对标准时间进行调正。

配置方法

打开 SNTP

- 必须配置，缺省 SNTP 状态是 Disable。

配置 SNTP Server 的地址

- 必须配置，缺省没有设置 SNTP/NTP 服务器

配置 SNTP 同步时钟的间隔

- 可选配置
- 默认情况下，设备每隔半小时同步一次时间

检验方法

使用 **show sntp** 命令查看 SNTP 相关参数。

相关命令

打开 SNTP

【命令格式】 **sntp enable**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 缺省 SNTP 状态是 Disable。

no sntp enable 全局配置命令来关闭 SNTP。

配置 SNTP Server 的地址

【命令格式】 **sntp server** { *ip- address* | *domain* } [**source** *source-ip-address*]

【参数说明】 *ip-address*：SNTP 服务器的 IP 地址。缺省没有设置任何 SNTP 服务器。

domain: SNTP 服务器的域名。缺省没有设置任何 SNTP 服务器。

source-ip-address : SNTP 指定源 IP 地址。

【命令模式】 全局配置模式

【使用指导】 由于 SNTP 协议和 NTP 完全兼容，所以这个 Server 完全可以配置成 internet 上公用的 NTP Server。

由于 SNTP 的报文和 NTP 的报文是完全一致的，所以 SNTP Client 能完全兼容 NTP Server。网络上存在着较多的 NTP Server，用户可以选择一个网络延迟较少的一个作为设备上的 SNTP Server。

配置 SNTP 同步时钟的间隔

【命令格式】 **sntp interval** *seconds*

【参数说明】 *seconds*：定时同步的间隔，单位为“秒”范围为 60 秒--65535 秒。缺省值为 1800s。

【命令模式】 全局配置模式

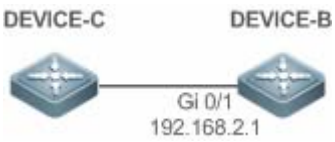
【使用指导】 该命令设置 SNTP Client 需要定时和 NTP/SNTP Server 同步时钟的时间间隔。

这里设置的时间间隔不会立即生效，如果要立即生效，请配置完时间间隔后执行 **sntp enable** 命令。

配置举例

SNTP 时间同步

【网络环境】 图 6-4



- DEVICE-B：网络上的 NTP 服务器
- DEVICE-C：从 DEVICE-B 同步时间

【配置方法】 DEVICE-C 开启 SNTP 功能，NTP 服务器配置为 DEVICE-B

DEVICE-C

```
C#configure terminal
C(config)# sntp server 192.168.2.1
C(config)# sntp enable
C(config)# exit
```

【检验方法】

- 在 DEVICE-C 上通过 **show clock** 命令可以查看时间是否成功同步。
- 在 DEVICE-C 上 **show sntp** 查看 sntp 状态和服务器是否配置成功

6.5 监视与维护

清除各类信息

-

查看运行情况

作用	命令
show sntp	查看 SNTP 的相关参数

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 sntp	打开调试功能。

7 DNS Proxy

7.1 概述

DNS-Proxy 又称正向 DNS 代理，一般部署于用户前端的出口网关设备上，处于 DNS 服务器和用户 PC 中间，代理 DNS 服务器处理用户的 DNS 域名解析请求。

正向DNS代理提供如下功能：

- 多线路负载均衡。
- any dns功能。
- dns 防劫持。

下文仅介绍 DNS Proxy 的相关内容。

协议规范

- RFC1034：DOMAIN NAMES - CONCEPTS AND FACILITIES
- RFC1035：DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION

7.2 典型应用

典型应用	场景描述
多线路负载均衡	当外网部署多个 ISP 出口线路时，可以在出口设备上配置 DNS Proxy，使得出口设备可以根据策略选择 ISP 线路，实现不同线路之间流量均衡。

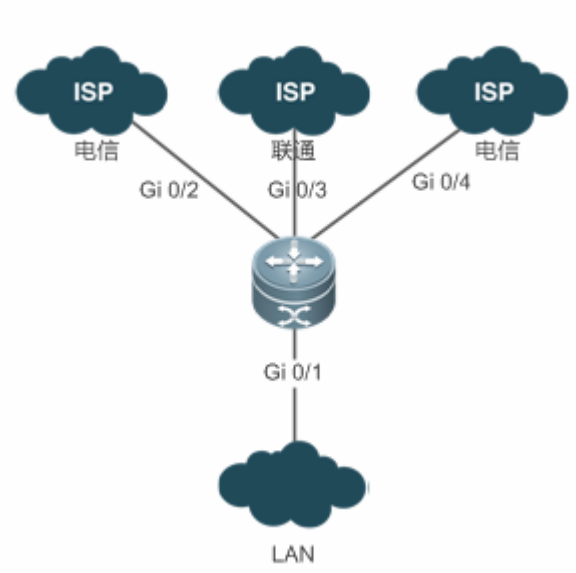
7.2.1 多线路负载均衡

应用场景

如下图所示，外网部署多个 ISP 出口线路：一条电信出口（带宽 1000M）、一条联通出口(带宽为 100M)、一条电信网 PPP 拨号线路(带宽 10M)，分别与出口设备的端口 Gi 0/2、Gi 0/3、Gi 0/4 相连。电信运营商提供了两个 DNS 服务器，首选 DNS 为 218.85.157.99，备选 DNS 为 218.85.152.99。联通运营商提供了两个 DNS 服务器，首选 DNS 地址为 58.22.96.66，备用 DNS 地址为 218.104.128.106。

内网用户通常只会在 PC 端启用一个固定的 DNS 服务器，显然无法发挥多出口的优势，容易出现大部分流量都是同一个 ISP 的，导致一个 ISP 的线路带宽耗尽而别的线路却空闲。如果能根据线路情况智能地在不同 ISP 的 DNS 服务器作出选择，则会大大缓解线路拥塞和闲置问题。

图 7-1 DNS 线路组网拓扑



功能部属

- 在出口设备连接内网的端口 Gi 0/1 上开启 dns-proxy 功能，dns-proxy 才能处理该口收到的 DNS 请求报文。
- 在出口设备连接电信出口的端口 Gi0/2 需要手动配置电信 DNS 服务器 ,连接联通出口的端口 Gi0/3 需要手动配置联通 DNS 服务器。由于端口 Gi 0/4 连接的是电信网 PPP 拨号线路，不需要手动配置 DNS 服务器。

7.3 功能详解

基本概念

↘ DNS 域名解析

要访问互联网上的站点，必须先知道对方的 IP，但是 IP 地址很难记忆。域名系统就是为了方便记忆而专门设计的一套地址转换系统，用户只需要记住域名，DNS 域名解析系统负责将域名解析成 IP 地址，并最终通过 IP 地址访问互联网上的站点。DNS 域名解析系统由 DNS 服务器和客户端组成，DNS 服务器保存着域名和 IP 的对应映射关系，DNS 客户端向服务器发起域名解析查询，服务器响应查询并把域名解析结果返回给客户端。

↘ DNS 代理（DNS Proxy）

DNS代理相当于DNS服务器和客户端中间的代理人，它能替代服务器接受客户端的域名解析查询。DNS代理对DNS客户端可以是可见的或不可见的两种方式，可见方式是DNS客户端设置默认DNS服务器为DNS代理，不可见方式则是DNS代理拦截DNS客户端发往服务端的报文进行处理，客户端觉察不到DNS代理的存在。

功能特性

功能特性	作用
正向 DNS 代理	代理 DNS 服务器处理客户端的域名解析请求，并支持多线路负载均衡、any dns、DNS 防劫持等功能。

7.3.1 正向 DNS 代理

工作原理

当 DNS-Proxy 拦截到转发的 DNS 报文后，根据用户所启用的功能模块，采用适当的策略，决定 DNS 报文应该从哪个外网口转发，然后修改报文的目的 IP 为该出口上配置的 DNS 服务器，并把报文从该出口转发。整个模块对内网用户是透明的，感觉不到 DNS-Proxy 的存在。

正向 DNS 代理提供如下功能：

↘ 多线路负载均衡

为解决网络南北互联互通问题，很多企事业单位、学校等在出口网关部署多线路，使用一些技术手段使用户访问电信的站点时走电信线路，访问联通站点时走联通线路。但由于内网用户通常只使用了一个 DNS 服务器，造成流量多从一个线路上走而另一线路闲置。

DNS-Proxy 可以根据出口的带宽或带宽利用率选择不同 DNS 服务器，使内网访问外网的流量能在不同出口上分担。系统默认采用基于带宽的负载均衡，哪个线路的带宽越大，该线路被选中的概率越大。如果是基于带宽利用率的策略负载均衡则每次选择出口流量/带宽最小的线路。

每个 ISP 线路，运营商都会提供相应的 DNS 服务器，DNS-Proxy 拦截到 DNS 请求报文时，根据策略选择不同线路，把请求报文发往该线路对应的 DNS 服务器，如果目的站点在该 ISP 有对应的 IP 地址，那用户就会从 DNS 应答报文中得到该 IP，于是后续流量都是走该目的 IP 的 ISP 线路，从而达到通过 DNS 实现线路流量分担的效果。存在少部分目的站点在该 ISP 没有对应的 IP 地址，DNS 应答报文分配了其他 ISP 上对应的 IP 地址，后续流量走其他 ISP 线路。

↘ any dns 功能

DNS-Proxy 能判断用户的 DNS 服务器设置是否合理，并自动纠正不合理的设置，保证用户无论设置什么样的 DNS 服务器都能正常上网。这些不合理设置有：跨运营商访问，例如电信用户却采用联通的 DNS 服务器；跨地区访问，例如福州电信用户却采用北京电信的 DNS 服务器。

DNS-Proxy 在收到域名解析请求时检查报文的源 IP 和目的 IP 是否合理，并自动修改目的 IP 为合适的目的 IP。如果是跨运营商访问，则改为同一个运营商；如果是跨地区访问，则改为本地区。

↘ dns 白名单

如果用户某些类型的 DNS 请求不想被正向 DNS 代理给处理，可以把该类型的报文匹配规则加入白名单，则正向 DNS 代理不会对符合规则的报文进行代理拦截。

↘ dns 防劫持

DNS-Proxy 可以防止用户由于收到恶意的 DNS 应答而导致域名被劫持情况。通过网管员预配置 DNS 防劫持黑名单，当转发 DNS 应答报文时，DNS-Proxy 检查报文里域名对应的 IP 是否匹配黑名单中的非法 IP 规则，如果匹配则丢弃该报文。

Proxy 与用户路由联动

在如下应用场景中，电信、移动和教育网出开启正向 DNS 代理，同时配置 PBR 使部分流量强制走教育网；实际使用中 Proxy 优先级高于 PBR，DNS 报文先走 Proxy 后解析出来的域名 IP 很可能与教育网 DNS-Server 解析的不一致，同时由于 PBR 限制使部分用户访问网页流量强制走了教育网 ,访问了其它运营商解析的域名 IP 地址影响了上网性能。Proxy 与用户路由联动后，DNS 报文与流量走两样的用户路由，因而得到有效的域名 IP，从而有效解决了上述存在的问题。

相关配置

配置接口上开启正向 DNS 代理

- 缺省情况下，设备上接口正向 DNS 代理功能关闭。
- 使用 **dns-proxy enable** 命令可以启动或关闭设备上接口正向 DNS 代理功能。
- 必须在设备上接口启用正向 DNS 代理功能，DNS Proxy 才能正常工作。

配置负载均衡策略

- 缺省情况下，设备上负载均衡策略默认是带宽策略。
- 使用 **load-balance** {**load | bandwidth**}命令可以切换为按带宽利用率/带宽策略负载均衡。

配置 dns 白名单

- 缺省情况下，设备上配置 dns 白名单为空。
- 使用 **whitelist** {**source-ip** *start-ip* [*end-ip*] **| name-server** *ip* } [**increase | decrease** *num*]命令可以配置 dns 白名单。

配置 dns 防劫持

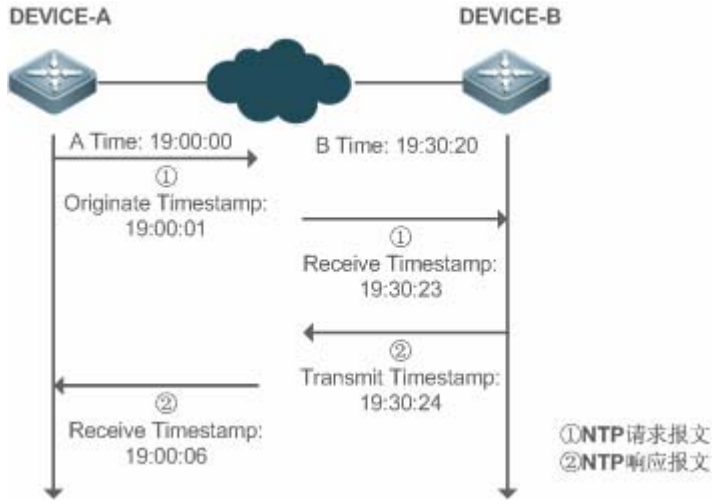
- 缺省情况下，设备上 dns 防劫持的 IP 为空。
- 使用 **blacklist domain-ip** *start-ip* [*end-ip*]命令可以配置 dns 防劫持的 IP。

7.4 配置详解

配置项	配置建议 & 相关命令	
开启正向 DNS 代理功能	必须配置。用于建立 DNS Proxy 服务。	
	dns-proxy enable	使能正向 DNS 代理功能
	ip name-server	配置接口线路的 DNS 服务器
配置负载均衡策略	可选配置。	
	load-balance	切换为按带宽利用率/带宽策略负载均衡

配置 DNS 白名单	可选配置。	
	whitelist	配置 DNS 白名单
配置 DNS 防劫持	可选配置。	
	blacklist domain-ip	配置 DNS 防劫持的 IP。

图 7-2 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：

20. 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
21. 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
22. 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
23. 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。

- 本地时钟参考模式

在该模式下，设备默认本地时钟即为可靠时钟源，直接向其它客户提供时间同步服务。

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。

配置 NTP 主时钟

- 缺省情况下，设备处于外部时钟参考模式。
- 通过 **ntp master** 命令可以将设备配置为本地时钟参考模式。

7.4.1 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。

7.4.2 NTP 访问控制

工作原理

通过 ACL 提供了一种最小限度的安全措施

相关配置

配置 NTP 服务的访问控制权限

- 缺省情况下，没有 NTP 访问控制权限。
- 通过 **ntp access-group** 可配置 NTP 的访问控制权限。

7.5 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。	
	ntp server	配置 NTP 服务器
	ntp update-calendar	自动更新硬件时钟
	可选配置，用于将设备配置为本地时钟参考模式。	
	ntp master	配置 NTP 主时钟
	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

配置 NTP 访问控制	可选配置，用于对收到的 NTP 报文进行源过滤。	
	ntp access-group	设置 NTP 的访问控制权限

7.5.1 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

本地时钟参考模式

- 设备的本地时钟作为 NTP 参考时钟源，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。
- 一旦配置本地时钟参考模式，系统便不会与比其时钟层数数值更高的时钟源进行同步。
- 将本地时钟设置为主时钟（尤其是指定了较低的时钟层数值时）很有可能将真正的有效时钟源覆盖。如果对同一网络中的多个设备都使用了该命令，则可能由于设备之间的时钟差异导致网络的时钟同步不稳定。
- 将本地时钟设置为主时钟前，如果系统从未与外部时钟源同步过，则有可能需要手动校准系统时钟以保证其不会有过大的偏差（关于如何手动校准系统时钟请参考配置指南中的系统时间配置部分）。

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。

配置 NTP 主时钟

- 如果需要将设备切换到本地时钟参考模式，可通过此命令。

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 Gig abitEthernet、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】 -

设置本地参考时钟源

【命令格式】 **ntp master**[*stratum*]

【参数说明】 *stratum*：指定本地时钟所处的层数，范围为 1～15；若不指定该参数则默认值为 8。

【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】 -

配置举例

NTP 外部时钟参考模式

【网络环境】

图 7-3



- DEVICE-B：配置为 NTP 外部时钟参考模式
- 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-A 配置本地时钟为 NTP 参考时钟源
- 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-A

```
A#configure terminal
A(config)# ntp master
A(config)#exit
```

DEVICE-B

```
B#configure terminal
B(config)# ntp server 192.168.1.1
B(config)# exit
```

DEVICE-C

```
C#configure terminal
C(config)# ntp server 192.168.2.1
C(config)# exit
```

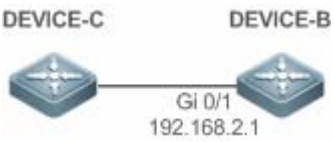
【检验方法】

- 在 DEVICE-B 上通过 **show ntp status** 查看 NTP 配置信息。
- DEVICE-B 会向 192.168.1.1 发送时间同步报文，从 DEVICE-A 同步时间。
- DEVICE-B 从 DEVICE-A 成功同步时间之后，可以响应 DEVICE-C 的时间同步请求。
- 在 DEVICE-B 和 DEVICE-C 上通过 **show clock** 命令可以查看时间是否成功同步。

NTP 本地时钟参考模式

【网络环境】

图 7-4



- DEVICE-B：本地时钟为 NTP 参考时钟源
- DEVICE-C：从 DEVICE-B 同步时间

【配置方法】

- DEVICE-B 配置本地时钟为 NTP 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 master
B(config)# exit
```

DEVICE-C

```
C#configure terminal
C(config)# ntp server 192.168.2.1
C(config)# exit
```

【检验方法】

- 在 DEVICE-C 上通过 **show clock** 命令可以查看时间是否成功同步。

7.5.2 配置 NTP 安全认证

配置效果

↘ 从可信参考时钟源同步时间

设备作为客户端，只从可信任的外部参考时钟源同步时间到本地时钟

↘ 给可信设备提供时间同步服务

设备的本地时钟作为 NTP 参考时钟源，只对可信的设备提供时间同步服务

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** 查看是只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 7-5



- 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

7.5.3 配置 NTP 访问控制

配置效果

NTP 服务的访问控制功能提供了一种最小限度的安全措施（更安全的方法是使用 NTP 身份验证机制）。

注意事项

- 目前系统暂未支持控制查询功能(用于通过网络管理设备对 NTP 服务器进行控制 ,如设置闰秒标记或监控其工作状态等)。虽然是按照上述顺序进行规则匹配，但涉及到与控制查询相关的请求都无法支持。
- 如果未配置任何访问控制规则，则所有访问都是允许的。但一旦配置了访问控制规则，则仅有规则中所允许的访问才能进行。

相关配置

↘ 设置 NTP 的访问控制权限

- 可选配置
- 通过 **ntp access-group** 配置 NTP 访问控制权限及对应的 ACL

检验方法

通过 **show run** 查看 NTP 配置是否正确配置

相关命令

↘ 配置 NTP 服务的访问控制权限

【命令格式】 **ntp access-group** { **peer** | **serve** |**serve-only** | **query-only** }*access-list-number* | *access-list-name*

【参数说明】 **peer**：既允许对本地 NTP 服务进行时间请求和控制查询，也允许本地设备与远程系统同步时间（完全访问权限）。

serve：允许对本地 NTP 服务进行时间请求和控制查询，但不允许本地设备与远程系统同步时间。

serve-only：仅允许对本地 NTP 服务进行时间请求。

query-only：仅允许对本地 NTP 服务进行控制查询。

access-list-number：IP 访问控制列表标号；范围为 1～99 和 1300～1999。关于如何创建 IP 访问控制列表请参考《ACL》中的相关描述。

access-list-name：IP 访问控制列表名。关于如何创建 IP 访问控制列表请参考《访问控制列表配置指南》中的相关描述。

【命令模式】 全局模式

【使用指导】 配置 NTP 访问控制权限。

当一个访问请求到达时，NTP 服务按照从最小访问限制到最大访问限制的顺序依次匹配规则，以第一个匹配到的规则为准。匹配顺序为 peer、serve、serve-only、query-only。

配置举例

NTP 访问控制权限配置

【配置方法】 配置只允许 192.168.1.1 的设备对本地设备进行时间同步请求

```
Ruijie(config)# access-list 1 permit 192.168.1.1
Ruijie(config)# ntp access-group serve-only 1
```

7.6 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。

8 DNS-CACHE

8.1 概述

DNS 缓存功能实现了对域名解析结果进行缓存，当第一次对某个域名进行请求时会对域名解析的结果进行缓存，下次再请求同一个域名的时候，设备会直接返回上次缓存的解析结果，而不用从外网 DNS 服务器上去获取。

协议规范

参见 RFC1034

8.2 典型应用

典型应用	场景描述
网吧出口部署	网吧出口设备部署 DNS 缓存功能

8.2.1 网吧出口部署

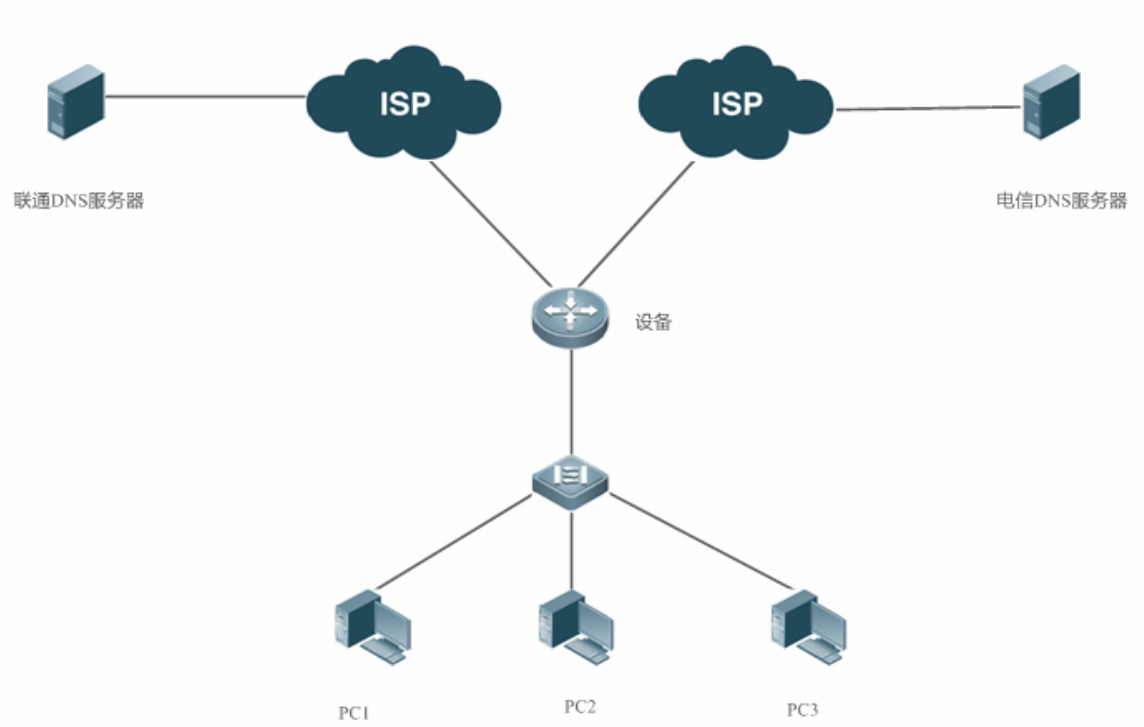
应用场景

DNS 缓存相关场景限制主要有：

1. DNS 服务器部署在内网的场景
2. VPN 场景只支持 PPTP 和 L2TP 客户端

以下为网吧用户典型应用场景：

图 8-1 网吧用户典型的应用场景



【注释】 网吧场景中，DNS 服务器往往都在外网，有大量的网络应用通过出口设备连接互联网，如网页浏览、游戏等等。

功能部属

- 基本 NAT 上网功能：完成基本的 NAT 地址转换，保障用户正常上网。
- 应用识别功能：完成转发流量的应用识别。
- 流量控制功能：和应用识别结合，实现对重点应用流量的保障等功能。
- 流控功能：对网络中的应用流量进行控制。
- DNS 缓存功能：对域名解析进行缓存，缓解由于外网 DNS 服务器不稳定带来的上网体验差等。

8.3 功能详解

基本概念

↘ 域名

一个域名的目的是便于记忆和沟通的一组服务器的地址。真正上网的时候最终要将域名解析成对应的 IP，这就需要进行域名解析，域名解析的结果为一个或多个域名对应的 IP。

↘ 静态缓存

静态缓存为用户自定义的规则，指定某个域名解析为固定 ip。

功能特性

功能特性	作用
DNS 缓存	缓存 DNS 解析结果。

8.3.1 DNS 缓存

DNS 缓存功能实现了对域名解析结果进行缓存，当第一次对某个域名进行请求时会对域名解析的结果进行缓存，下次再请求同一个域名的时候，设备会直接返回上次缓存的解析结果，而不用从外网 DNS 服务器上去获取。。

工作原理

对 DNS 请求报文进行缓存匹配，如果匹配命中则构造 DNS 回应报文，并将 DNS 请求报文吃掉。匹配的条件包括域名、域名服务器 IP，出接口；如果未匹配命中则放行 DNS 请求报文，同时对 DNS 回应报文进行缓存。

相关配置

↘ 开启 DNS 缓存功能

缺省情况下，DNS 缓存功能是开启的。

在全局配置模式中，使用 **dns-cache enable** 命令可以开启 DNS 缓存功能开关。

在全局配置模式中，使用 **no dns-cache enable** 命令可以关闭 DNS 缓存功能开关。

↘ 配置缓存时间

缺省情况下，DNS 结点缓存时间为 300 秒

使用 **dns-cache old-time** *time* 可以调整缓存时间，取值范围为 1~600 秒

要删除相关配置，可以在全局配置模式下执行 **no dns-cache old-time** 命令来执行，删除后恢复默认缓存时间

↘ 配置静态缓存策略

缺省情况下匹配动态缓存

使用 **dns-cache static domain** *domain* **ip** “*ip1 ip2 …*” 命令可以配置静态缓存策略，一条策略最多配置 8 个 ip。

要删除相关配置，可以在配置模式下执行 **no dns-cache static domain** *domain* 命令来执行。

8.4 产品说明

NBR3000G-S 、NBR1500G、NBR2000G、NBR1000G-C、NBR2000G-C 支持 DNS 缓存功能，NBR800G、NBR950G、NBR1000G-E、 NBR108G-P、 NBR1300G-E、 NBR1700G-E、 NBR2100G-E、 NBR2500D-E、 NBR3000D-E、NBR3000D-UE、NBR6205-E、NBR6210-E、NBR6215-E 不支持 DNS 缓存功能。

8.5 配置详解

配置项	配置建议 & 相关命令	
开启关闭流量监控审计功能	必须配置。打开流量审计功能。	
	dns-cache enable	开启 DNS 缓存功能。
配置缓存时间	可选配置。配置结点缓存时间。	
	Dns-cache old-time *time*	配置缓存时间，单位为秒，可配范围 1-600 秒。
配置静态缓存	可选配置。配置用户自定义静态缓存。	
	dns-cache static domain *domain* **ip** *"ip1 ip2 …"*	配置用户自定义静态缓存，最大可配置 100 条，一个域名最多对应 8 个 ip。

8.5.1 开启关闭 DNS 缓存功能

配置效果

- 打开 DNS 缓存功能，能够对 DNS 报文解析结果进行缓存，后面同样的域名请求可以直接从设备返回，不必到外网请求。

注意事项

- DNS 缓存功能开关关闭的情况下，功能失效。
- DNS 缓存时间有限制，保留缓存的结果时间默认 300 秒，最大可配 600 秒。
- DNS 缓存功能开关关闭情况下，缓存信息会删除。

配置方法

- 全局模式下，通过命令开启 DNS 缓存审计。

检验方法

- 通过 **show dns-cache enable** 可查看 DNS 缓存功能是否开启。

相关命令

开启流量监控审计

【命令格式】 **dns-cache enable**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 通过配置本命令启动 DNS 缓存功能。

配置举例

开启流量监控审计

【配置方法】 在出口设备上配置。

```
Ruijie# configure terminal
Ruijie(config)#dns-cache enable
```

【检验方法】

- 查看 DNS 缓存是否开启的状态。

```
Ruijie#show dns-cache enable
dns-cache is on
Ruijie#
```

常见错误

无

8.5.2 配置缓存时间

配置效果

- 配置缓存时间，可以对缓存的保留时间进行配置，默认保存 300 秒，可配范围 1-600 秒。

注意事项

- 可选配置。
- DNS 缓存开关关闭的情况下，功能失效，缓存数据也不会被删除。
- 缺省配置为 300 秒，可配置范围 1-600 秒。

- 删除配置后，缓存时间恢复默认时间

配置方法

- 配置模式下，通过命令配置 DNS 缓存时间。

检验方法

- 检查各个缓存结点保留时间。

相关命令

↘ 配置 DNS 缓存时间

【命令格式】 **dns-cache old-time** *time*

【参数说明】 *time*: 缓存时间，取值范围为 1~600 秒

【命令模式】 全局配置模式

【使用指导】 通过本命令配置可以修改结点缓存时间。

配置举例

↘ 配置缓存时间为 600 秒

【配置方法】 在出口网关设备上配置。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# dns-cache old-time 600
```

【检验方法】

- 查看配置的信息。

```
Ruijie(config)#show run | in dns-cache
dns-cache old-time 600
```

常见错误

无

8.5.3 配置用户自定义静态缓存

配置效果

- 配置用户自定义静态缓存后，指定域名不通过 DNS 服务器直接解析为特定的 IP 地址。

注意事项

- DNS 缓存开关关闭的情况下，功能失效。
- 最大可配置 100 条策略
- 每个域名最多可以指定 8 个 ip

配置方法

- 全局配置模式下，通过命令配置静态缓存。

检验方法

- 检查指定的域名是否未通过 DNS 服务器直接解析为特定的 IP 地址。

相关命令

配置报表预生成时间

【命令格式】 **dns-cache static domain** *domain* **ip** *"ip1 ip2 ..."*

【参数说明】 *domain*：域名，最长长度不超过 64 字节

ip：域名解析出来的 ip

【命令模式】 全局模式

【使用指导】 -

配置举例

配置错误！超链接引用无效。

【配置方法】 在出口设备上配置。

```
Ruijie#config

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

Ruijie(config)#dns-cache static domain www.baidu.com ip "1.2.3.4 5.6.7.8 9.1.3.5"
```

【检验方法】

- 查看静态缓存。

```
Ruijie(config)#show run | in dns-cache
dns-cache static domain www.baidu.com ip 1.2.3.4 5.6.7.8 9.1.3.5
Ruijie(config)#
```

常见错误

无

8.6 监视与维护

清除各类信息

无

查看运行情况

作用	命令
显示 DNS 缓存运行状态信息。	**show dns-cache state**

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
开启 CLI 配置的 debug 信息。	**debug dns-cache cli**

9 FTP-Server

9.1 概述

FTP Server 功能可以将一台设备配置为 FTP 服务器。这样可以通过 FTP 客户端与之连接，通过 FTP 协议往设备上传或下载文件。

用户可以利用 FTP Server 功能方便地获取设备中的文件，如 syslog 日志文件等；也可以通过 FTP 直接往设备的文件系统拷贝文件。

下文仅介绍 FTP 的相关内容。

协议规范

- RFC959：FILE TRANSFER PROTOCOL (FTP)
- RFC3659：Extensions to FTP
- RFC2228: FTP Security Extensions
- RFC1635: How to Use Anonymous FTP

9.2 典型应用

典型应用	场景描述
局域网内提供 FTP 服务	在一个局域网内为同一个用户提供上传与下载服务

9.2.1 局域网内提供 FTP 服务

应用场景

在一个局域网内为同一个用户提供上传与下载服务

以下图为例，仅在局域网内开启 FTP-Server 服务

- G 开启 FTP Server 服务，S 二层透传功能
- User 发起 FTP 上传与下载请求

图 9-1



【注释】 G 为出口网关设备。
S 为接入设备

功能部属

- G 启动 FTP Server
- S 当作二层交换机，起到二层透传的作用

9.3 功能详解

基本概念

FTP 协议

FTP（File Transfer Protocol）是 IETF Network Working Group 所制定的一套标准协议，属于网络协议组的应用层，FTP 基于 TCP 传输控制协议(Transmission Control Protocol)实现文件传输。FTP 使用户能在两个联网的计算机之间传输文件，它是 Internet 传递文件最主要的方法。使用匿名 FTP，用户可以免费获取 Internet 丰富的资源。除此之外，FTP 还提供登录、目录查询、文件操作及其它会话控制等功能。FTP 协议在 TCP/IP 协议族中属于应用层协议，使用 TCP 端口 20 和 21 进行传输。端口 20 用于传输数据，端口 21 用于传输控制消息。FTP 协议基本操作在 RFC959 中进行了描述。

用户授权

FTP Client 要连上 FTP Server，必须要有该 FTP 服务器授权的帐号，只有拥有一个用户标识和一个口令后才能登陆 FTP 服务器，享受 FTP 服务器提供的服务。设计考虑最大支持设定用户个数为 10 个，每个用户最大连接数为 2 个，服务器最大连接数为 10 个。

FTP 文件传输模式

FTP 有两种文件传输模式：

- 文本传输方式：也称为 ASCII 模式，用于传输文本格式的文件（比如后缀名为.txt、.bat 和.cfg 的文件），与 Binary 模式的区别是回车换行的处理，ASCII 模式将回车换行转换为本机的回车字符，比如 Unix 下是\n，Windows 下是\r\n，Mac 下是\r。假定用户正在拷贝的文件包含 ASCII 码文本，如果在远程机器上运行的不是 UNIX，当文件传输时 FTP 通常会自动地调整文件的内容以便于把文件解释成对端计算机存储文本文件的格式。
- 二进制传输模式：也称为 Binary 模式，用于传输程序文件（比如后缀名为.app、.bin 和.btm 的文件），可用来传送可执行文件，压缩文件，和图片文件，不对数据进行任何处理，比文本模式更快，可以传输所有 ASCII 值，保证不出错。

FTP 工作方式

FTP 的两种工作方式：

图 9-2

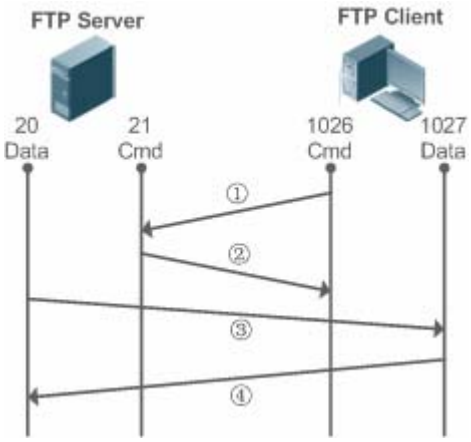
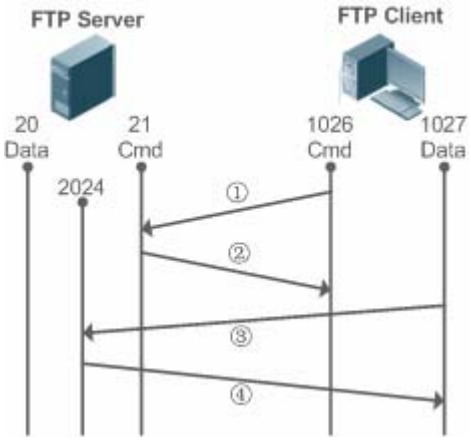


图 9-3



- PORT 模式见**错误！未找到引用源。**：FTP 客户端首先通过端口(1026)和 FTP 服务器的端口(21)建立连接，通过这个通道发送命令，客户端需要接收数据的时候在这个通道上发送 PORT 命令。PORT 命令包含了客户端数据通道端口(1027)来接收数据。在传送数据的时候，服务器端通过自己的端口(20)连接至客户端的端口(1027)建立数据通道，实现数据收发；FTP Server 必须和客户端建立一个新的连接用来传送数据。
- PASV模式见 图 9-3 :在建立控制通道的时候与PORT模式类似，但建立连接后发送的不是Port命令，而是PASV命令。FTP服务器收到PASV命令后，随机打开一个高端端口（2024）并且通知客户端在该端口上传送数据，客户端用端口（1027）连接FTP服务器该端口，之后便可以在通道上进行数据收发，这个时候FTP Server不再需要建立一个新的和客户端之间的连接。

↘ 支持的 FTP 命令

当设备收到 FTP 连接请求时， FTP 服务器将要求客户端提供登录用户名和密码以进行身份认证。
如果客户端通过身份认证，即可执行 FTP 客户端命令进行操作。目前的 FTP 服务器并没有支持所有的 FTP 命令，具体支持的 FTP 客户端命令如下：

ascii	delete	mdelete	mput	quit	send
bin	dir	mdir	nlist	recv	size
bye		mget		rename	system

cd	get	mkdir	passive		type
cdup		mls	put	rmdir	user
close	ls		pwd		

以上 FTP 客户端命令的用法请参考您所使用的 FTP 客户端软件的文档。另外不少 FTP 客户端工具（如 CuteFTP、FlashFXP 等）均提供了图形化的操作界面，使用此类工具可以无需再通过 FTP 命令进行操作。

功能特性

功能特性	作用
开启 FTP Server 服务	为 FTP-Client 提供上传、下载、显示文件、创建文件、删除文件等功能

9.3.1 开启 FTP Server 服务

工作原理

基本工作原理如上一章所述，我司设备需要配置用户名、密码、顶层目录即可为用户提供 FTP 服务。

相关配置

↘ 全局使能 FTP Server

缺省情况下，全局不开启 FTP 服务器

使用 **ftp-server enable** 开启

必须在全局开启 FTP 服务器功能，否则无法使用

↘ 配置用户名密码及顶层目录

缺省情况下，无用户授权及顶层目录

使用 **ftp-server username password**、**ftp-server topdir** 来设置授权与顶层目录

以上三项必须配置无配置无法启动 FTP 服务器功能

9.4 产品说明

NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 FTP Server；NBR108G-P、NBR800G、NBR950G、NBR1500G、NBR2000G、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1000G-E、NBR6120-E、NBR1300G-E 不支持 FTP Server。

9.5 配置详解

配置项	配置建议&相关命令	
配置 FTP Server 基本功能	必须配置，用于启动 FTP 服务器。	
	ftp-server enable	启动 FTP 服务器功能
	ftp-server login timeout	配置 FTP 登陆有效时长
	ftp-server login times	配置 FTP 登陆有效次数
	ftp-server topdir	配置 FTP 服务器顶层目录
	ftp-server username password	设置用户名，密码
	可选配置	
	ftp-server timeout	配置 FTP 会话的空闲时限

9.5.1 配置 FTP Server 基本功能

配置效果

- 建立 FTP Server，向 FTP Client 提供 FTP 服务

注意事项

- 需要配置用户名、密码及顶层访问目录
- 如果需要服务器在有限时间内关闭异常的会话，需要配置会话空闲时限

配置方法

启动 FTP Server 功能

- 必须配置
- 若无特殊要求，应在每台路由器上启动 FTP Server 功能

配置顶层目录

- 必须配置
- 若无特殊要求，应每台路由器上配置顶层目录为根目录

配置登录用户名和密码

- 必须配置
- 注意用户名和密码的长度有限制

配置会话空闲时限

- 可先配置
- 当 FTP 服务器某个用户在线时，如果该用户连接异常中断或用户非正常中断连接，FTP 服务器可能无法知道用户断开而将继续保持连接，导致与服务器的连接被长期占用使服务器无法响应其他用户的登录请求，因此可以配置该选项保证异常发生时在一定时间段内让其它用户可连接上

检验方法

利用 FTP 客户端与服务器进行连接

- 检查客户端是否能连接成功
- 检查客户端相关操作是否正常

相关命令

启动 FTP Server 功能

【命令格式】 **ftp-server enable**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 在正确配置服务器的顶层目录、登录用户名和密码之前客户端仍然无法访问 FTP 服务器，因此建议在首次启动服务之前先参考后面的章节完成服务器顶层目录、登录用户名与密码的配置

配置会话登陆有效次数

【命令格式】 **ftp-server login times** *times*

【参数说明】 *times*：有效次数（范围：1-10）

【命令模式】 全局模式

【使用指导】 会话的有效次数是指在一个 FTP 会话在登陆过程中，用户最多可以进行账号密码认证的次数。默认设置为 3 次，即在累计三次输入错误的用户名或密码时，会话被中止，从而允许其他用户上线。

配置会话登陆有效时长

【命令格式】 **ftp-server login timeout** *timeout*

【参数说明】 *timeout*：登陆有效时间（单位：分钟；范围：1-30）

【命令模式】 全局模式

【使用指导】 登陆有效时间是指用户建立链接后，每次认证用户账号和密码的最长在线时间。在该有效时间内用户若未再次进行用户密码认证将被中止会话，从而保证其他用户能够登陆。

配置服务器顶层目录

【命令格式】 **ftp-server topdir** *directory*

【参数说明】 *directory:* 指定用户访问路径

【命令模式】 全局模式

【使用指导】 如可以指定服务器的顶层目录为“/syslog”目录，则 FTP 客户端登录后将仅能访问设备上“/syslog”目录下的文件和文件夹，客户端由于顶层目录的限制将无法退到“/syslog”目录的上级目录中

配置服务器登录用户名和密码

【命令格式】 **ftp-server username** *username* **password** [*type*] *password*

【参数说明】 *username*：用户名

type：0 或 7，0 代表密码未加密（明文），7 代表密码为加密过的密文

password：密码

【命令模式】 全局模式

【使用指导】 FTP 服务器不支持匿名用户，因此需要配置用户名

用户名最大长度为 64 个字符，中间不允许有空格。用户名可以由英文字母、半角数字和半角符号组成

密码必须为字母或数字，密码前后可以有空格，但将被忽略；密码中间的空格作为密码的一部分。

明文密码的最小长度为 1 个字符、最大长度为 25 个字符；密文密码的最小长度为 4 个字符、最大长度为 52 个字符。

用户名和密码必须一一配对，最多仅能配置 10 个用户。

配置会话空闲时限

【命令格式】 **ftp-Server timeout** *time*

【参数说明】 *time*：空闲时限（单位：分钟；范围：1-3600）

【命令模式】 全局模式

【使用指导】 会话的空闲时间是指在一个 FTP 会话中从上次 FTP 操作完成后到下次 FTP 操作开始之间的时间。服务器在响应完一个 FTP Client 命令操作后(如一个文件全部传输完毕后)重新开始计算会话空闲时间 ;在下一个 FTP Cient 命令操作到来的时停止计算会话空闲时间。 因此会话空闲时限的配置并不会对某些耗时的文件传输操作带来任何影响

查看服务器的状态信息

【命令格式】 **show ftp-server**

【参数说明】 -

【命令模式】 特权模式

【使用指导】 显示 FTP 服务器的相关状态信息

打开服务器的调试信息

【命令格式】 **debug ftp-server pro/err**

【参数说明】 -

【命令模式】 特权模式

【使用指导】 打开 FTP 服务器的过程/错误调试信息输出

配置举例

以下配置举例，仅介绍与 FTP Server 相关的配置。

在 IPv4 网络上建立 FTP Server 服务

【网络环境】
- 能够建立从服务器传输到客户端的 TCP 连接。

【配置方法】
- 开启 FTP Server 服务
- 配置顶层目录/syslog
- 配置用户名为 user、密码为 password
- 配置会话空闲时限为 5 分钟

```
Ruijie(config)#ftp-server username user
Ruijie(config)#ftp-server password password
Ruijie(config)#ftp-server timeout 5
Ruijie(config)#ftp-server topdir /
Ruijie(config)#ftp-server enable
```

【检验方法】 1.**show ftp-server** 查看

```
Ruijie#show ftp-server

    ftp-server information

==================================

enable : Y

topdir : tmp:/

timeout: 10min

username:aaaa          password:(PLAINT)bbbb          connect num[2]

    [0]trans-type:BINARY (ctrl)server IP:192.168.21.100[21]

                               client IP:192.168.21.26[3927]

    [1]trans-type:ASCII (ctrl)server IP:192.168.21.100[21]

                               client IP:192.168.21.26[3929]

username:a1            password:(PLAINT)bbbb          connect num[0]

username:a2            password:(PLAINT)bbbb          connect num[0]

username:a3            password:(PLAINT)bbbb          connect num[0]

username:a4            password:(PLAINT)bbbb          connect num[0]

username:a5            password:(PLAINT)bbbb          connect num[0]

username:a6            password:(PLAINT)bbbb          connect num[0]

username:a7            password:(PLAINT)bbbb          connect num[0]
```

```
username:a8          password:(PLAINT)bbbb          connect num[0]
username:a9          password:(PLAINT)bbbb          connect num[0]
```

常见错误

- 未配置用户名
- 未配置密码
- 未配置顶层目录

9.6 监视与维护

清除各类信息

-

查看运行情况

作用	命令
查看 FTP Server 配置	show ftp-server

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 FTP Server 错误事件的调试开关。	**debug ftp-server err**
打开 FTP Server 消息事件的调试开关。	**debug ftp-server pro**

10 FTP Client

10.1 概述

FTP（File Transfer Protocol，文件传输协议），是 TCP/IP 的一种具体应用，通过在 FTP 客户端和服务器之间建立面向连接的，可靠的 TCP 连接，用户可以访问一个运行有 FTP 服务器程序的远程计算机。

FTP Client 为用户提供在设备上通过 FTP 协议与远程 FTP 服务器进行文件传输的功能。用户通过客户端向服务器发出命令，服务器响应命令并把执行结果返回客户端，通过这种命令交互，用户可以察看服务器目录下的文件，并把文件从远程计算机上拷到本地，或把本地的文件传送到远程计算机去。

FTP 主要是作用是：促进程序/数据文件的共享；鼓励（通过程序）使用远程计算机；使用户不必面对不同主机上不同文件系统的差异；对数据进行高效可靠的传输。适用于远程安全的文件传输。

锐捷 FTP Client 并不像标准 FTP 客户端一样实现交互式命令，其控制连接相关的 open、user、pass 指令由 CLI 输入 copy 命令自动完成，在控制连接建立完成后，则进入文件传输过程，建立数据连接，实现文件的上传或下载。

用于原来的设备支持 TFTP，但是 TFTP 是用于小文件传输，FTP 协议支持大文件传输，在设备上实现文件传输协议 FTP，使设备可以同其它客户机或服务器进行文件传输。

协议规范

- RFC959：FILE TRANSFER PROTOCOL (FTP)

10.2 典型应用

典型应用	场景描述
从本地上传一个文件到远程服务上	本地与远程的的文件需要共享，如需要从本地上传一个文件到远程服务上
从远程服务器中下载一个文件到本地设备	本地与远程的的文件需要共享，如需要从远程服务器中下载一个文件到本地设备。

10.2.1 从本地上传一个文件到远程服务上

应用场景

本地与远程的文件需要共享，如需要从本地上传一个文件到远程服务上。

以下图为例，仅在 Intranet 提供共享资源作用。

图 10-1



功能部属

- 在 Intranet 中只实现通信。
- FTP Client 打开 FTP Client 文件上传功能。
- FTP Server 打开 FTP Server 文件上传功能。

10.2.2 从远程服务器中下载一个文件到本地设备

应用场景

本地与远程的的文件需要共享，如需要从远程服务器中下载一个文件到本地设备。

以下图为例，仅在 Intranet 提供共享资源作用。

图 10-2



功能部属

- 在 Intranet 中只实现通信。
- FTP Client 打开 FTP Client 文件下载功能。
- FTP Server 打开 FTP Server 文件下载功能。

10.3 功能详解

基本概念

↘ FTP 文件上传

从 FTP Client 上把文件上传到 FTP Server 上。

↘ FTP 文件下载

把 FTP Server 上的文件下载到 FTP Client 上。

FTP 连接模式

FTP Client 与 FTP Server 的连接方式，有主动连接和被动连接之分。

FTP 传输模式

FTP Client 与 FTP Server 的之间的传输数据的方式，FTP 的传输有两种方式：文本（ASCII）传输模式和二进制（BINARY）数据传输模式。

FTP 传输指定源接口 IP

FTP Client 可以对与服务端进行通信的客户端源 IP 地址进行绑定。

功能特性

功能特性	作用
FTP 文件上传	从 FTP Client 上把文件上传到 FTP Server 上
FTP 文件下载	将 FTP Server 上的文件下载到 FTP Client 上
FTP 连接模式	FTP Client 与 FTP Server 的连接方式
FTP 传输模式	FTP Client 与 FTP Server 的之间的传输数据的方式
FTP 传输指定源接口 IP	FTP Client 可以对与服务端进行通信的客户端源 IP 地址进行绑定

10.3.1 FTP 文件上传

FTP 具有文件上传的功能。进行 FTP 文件上传文件需要 FTP Client 与 FTP Server 两个设备同时打开，从 FTP Client 上把文件上传到 FTP Server 上。

10.3.2 FTP 文件下载

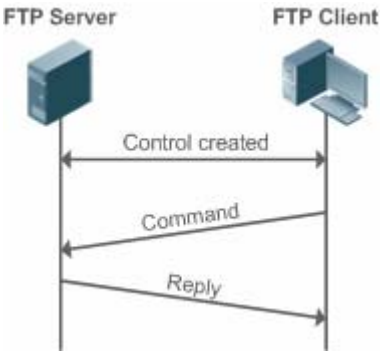
FTP 具有文件下载的功能。进行 FTP 文件下载文件需要 FTP Client 与 FTP Server 两个设备同时打开，把 FTP Server 上的文件下载到 FTP Client 上。

10.3.3 FTP 连接模式

FTP 协议要用到两个 TCP 连接，一个是控制链路（也称命令链路），用来在 FTP 客户端与服务器之间传递命令；另一个是数据链路，用来上传或下载数据。

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

图 10-3 控制连接



2. 控制连接与数据连接：当客户端发出的命令需要上传或下载数据时，这时不仅要建立控制连接还需要建立数据连接。

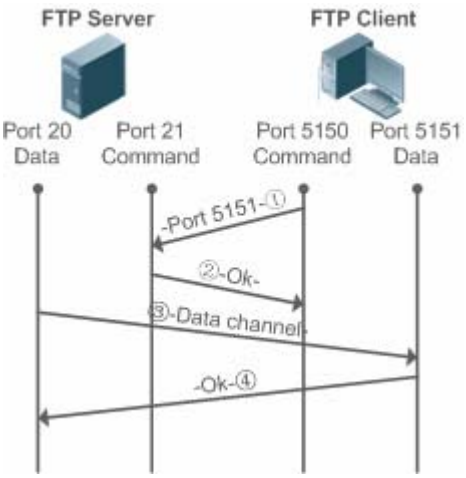
FTP 协议有两种数据连接方式：主动（PORT）方式和被动（PASV）方式。这两种工作模式主要区别在于数据连接建立方式不同，控制连接基本是一样的。

- 主动方式

该模式下 FTP server 在数据连接时是主动去连接 FTP client，所以被称为主动连接，其主要执行如下四个步骤：

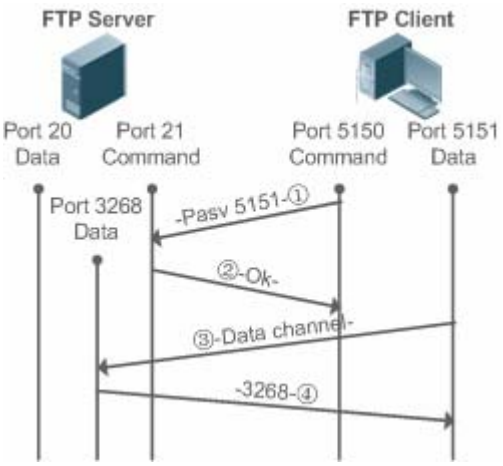
1. 客户端使用图例中的源端口 5150 与 server 端的 21 端口通信，请求建立连接，告诉服务器将用的端口是 5151。
2. server 收到后，发送应答信息，OK(ACK)，client and server 通过控制端口交换控制信令。
3. 服务器打开 20 端口作为数据发送的源端口，向客户端的 5151 端口发送。
4. 客户端应答，传输过程结束。

图 10-4 PORT（主动）模式



- 被动方式

图 10-5 PASV（被动）模式



该模式一般通过 passive 命令进行设置，由于 FTP server 在数据连接时是被动连接 FTP Client，所以称为被动连接，其主要执行如下四个步骤：

2. 被动模式下，客户端初始化控制信令连接，使用图例中 5150 源端口与服务器的 21 端口建立连接，并使用 passive 命令请求进入被动模式。
3. 服务器同意进入 PASV 模式，并随机选择一个大于 1024 的端口号，告知客户端。
4. 客户端接收到此信息后，使用图例中的 5151 端口与刚才服务器提供的 3268 端口进行数据通信，这里 5151 是源端口，3268 是目的端口。
5. 服务器收到信息，回传数据并发送应答 ACK（OK）。

当客户端和服务器建立数据连接后，就可以进行 FTP 最基本的上传和下载功能，并且在客户端可以对服务器进行一些相关文件操作。

用于传输命令和反馈信息的传输的控制连接始终存在，而数据连接只在需要的时候建立；PASV 和 PORT 模式的设置选择权仅在 FTP Client，由 FTP Client 发出命令建立不同的数据连接模式，我司 FTP Client 默认方式为被动模式

10.3.4 FTP 传输模式

FTP 的传输有两种方式：文本（ASCII）传输模式和二进制（BINARY）数据传输模式。我司产品 FTP Client 目前支持 ASCII 和 BINARY 两种传输模式，默认情况下为 BINARY 传输模式。

- 文本模式

ASCII 模式和 BINARY 模式的区别是回车换行的处理，ASCII 模式将回车换行转换为本机的回车字符，比如 Unix 下是\n，Windows 下是\r\n，Mac 下是\r。

- 二进制模式

BINARY 模式可用来传送可执行文件，压缩文件和图片文件，不对数据进行任何处理。以 Unix 传送文本文件到 Windows 为例，使用 BINARY 模式时，不会对 Unix 下的换行符进行从\r 到\r\n 的转换，因此在 windows 上看这个文件是没有换行的，里面是一个个的黑方块。由于不进行回车换行的处理，因此 BINARY 模式比文本模式更快，可以传输所有 ASCII 值，保证不出错。

10.3.5 FTP 传输指定源接口 IP

FTP Client 可以对与服务端进行通信的客户端源 IP 地址进行绑定，这样可以用指定的源 IP 与 FTP Server 进行连接和传输文件。

10.4 产品说明

NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E、NBR1500G、NBR2000G、NBR2000G-C、NBR3000G-S、NBR1000G-E、NBR6120-E、NBR1300G-E 支持 FTP Client；NBR108G-P、 NBR800G、NBR950G、NBR1000G-C 不支持 FTP Client。

10.5 配置详解

配置项	配置建议 & 相关命令	
配置 FTP Client 基本功能	必须配置。配置 FTP CLEINT 功能	
	copy flash	文件上传
	copy ftp	文件下载
配置 FTP Client 可选功能	可选配置。配置 FTP CLEINT 功能的工作模式	
	ftp-client port	设置 FTP 为主动连接模式
	ftp-client ascii	设置 FTP 为文本传输模式
	ftp-client source	配置进行 FTP 连接的客户端源 IP 地址
	ftp-client source-address	配置进行 FTP 连接的客户端源 IP 地址
	default ftp-client	恢复 FTP Client 为缺省配置，数据连接为被动方式，文件传输为二进制模式，清除源 IP 绑定

10.5.1 配置 FTP Client 基本功能

配置效果

- 实现文件上传与下载。

注意事项

- 文件上传与下载的格式。

配置方法

文件上传

- 需要实现文件上传时，为必选配置。
- 在特权模式下的 copy 下的目的地址上配置 FTP 相关的 URL。

文件下载。

- 需要实现文件下载时，为必选配置。
- 在特权模式下的 copy 下的源地址上配置 FTP 相关的 URL。

检验方法

- 在 FTP Server 的目录中看所上传的文件是否存在。
- 在目的地址上查看下载的文件是否存在。

相关命令

文件上传

【命令格式】 **copy flash:**[*local-directory/*]*local-file*

ftp: *//username:password@dest-address*[*/remote-directory*]*/remote-file*

【参数说明】 *local-directory：*指定设备目录，如果未指定，则表示当前工作目录。

*local-file：*表示要操作的本地文件名

username：指定访问 FTP Server 的用户名，最长不超过三十二个字节，不可包含“:”、“/”和空格等字符，不可省略。

*Password：*指定访问 FTP Server 的密码，最长不超过三十二个字节，不可包含“:”、“/”和空格等字符，不可省略。

*dest-address：*指定 FTP Server 的 IP 地址

*remote-directory：*指定 Server 端的目录路径

*remote-file：*指定要操作的 Server 端文件名

如果包含 *local-directory* 字段，则必须保证设备中已创建了该目录，此下载命令不支持目录的自动创建。

【命令模式】 全局模式

【使用指导】 使用该命令从本地设备的 flash 上上传一个文件到 FTP SERVER 上去。

文件下载

【命令格式】 **copy ftp:***//username:password@dest-address*[*/remote-directory*]*/remote-file*

flash:[*local-directory/*]*local-file*

【参数说明】 *username*：指定访问 FTP Server 的用户名，最长不超过三十二个字节，不可包含“:”、“/”和空格等字符，

不可省略。

password：指定访问 FTP Server 的密码，最长不超过三十二个字节，不可包含“:”、“/”和空格等字符，不可省略。

dest-address：指定 FTP Server 的 IP 地址。

remote-directory：指定 Server 端的目录路径。

remote-file：指定要操作的 Server 端文件名。

local-directory：指定设备目录，如果未指定，则表示当前工作目录。

local-file：表示要操作的本地文件名。

如果包含 *local-directory* 字段，则必须保证设备中已创建了该目录，此下载命令不支持目录的自动创建。

【命令模式】 全局模式

【使用指导】 使用该命令从 FTP Server 下载一个文件到本地设备的 flash 上去。

配置举例

以下配置举例，仅介绍与 FTP Client 上传下载相关的配置。

上传文件示例

【配置方法】 将设备 home 目录中的 local-file 文件上传到用户名为 user，密码为 pass，IP 地址为 192.168.23.69 的 FTP Server 的 root 目录下，文件命名为 remote-file。

```
Ruijie# copy flash: home/local-file ftp://user:pass@192.168.23.69/root/remote-file
```

【检验方法】 在 FTP Sserver 上查看 remote-file 是否存在。

下载文件示例

【配置方法】 从用户名为 user ,密码为 pass ,IP 地址为 192.168.23.69 的 FTP Server 的 root 目录下载文件名为 remote-file 的文件到设备上的 home 目录中，存储的文件名为 local-file

```
Ruijie# copy ftp://user:pass@192.168.23.69/root/remote-file flash: home/local-file
```

【检验方法】 在 flash 的 home 目录下查看 remote-file 是否存在。

常见配置错误

- 上传下载输入的格式错误。
- 用户名或密码错误。

10.5.2 配置 FTP Client 可选功能

配置效果

- 根据配置能让 FTP 工作在指定连接、传输模式及指定的 IP 地址下进行文件上传与下载。

注意事项

- FTP Client 在配置时如果需要指定的 vrf-name 进行配置时，首先必须先进行 vrf-name 的相关配置。

配置方法

设置 FTP 为主动连接方式。

- 可选配置。
- 配置 FTP 的连接模式。

设置 FTP 为文本传输模式。

- 可选配置。
- 配置 FTP 的传输模式。

设置进行 FTP 连接的客户端源 IP 地址。

- 可选配置。
- 配置进行 FTP 连接的客户端源 IP 地址。

支持源接口配置命令版本，版本提供全局配置模式的配置命令“**ftp client source**”用来配置源接口和源 IP 地址，废弃原命令，“**ftp client soure-address**”同时该命令隐藏，如果用户执行该命令，将转换成新的配置命令保存。

恢复 FTP Client 为缺省配置。

- 可选配置。
- 恢复 FTP Client 为缺省配置。

检验方法

通过 **show run** 查看

相关命令

配置 FTP 为主动连接模式

【命令格式】 **ftp-client** [**vrf** *vrf-name*] **port**
ftp-client port
【参数说明】 **vrf** *vrf-name*：指定 VRF。
【命令模式】 全局配置模式

【使用指导】 使用该命令可以将连接模式设置为主动方式，主动方式下，服务器主动去连接客户端。默认情况下 FTP 连接为被动（PASV）方式。

配置进行 FTP 连接的客户端源 IP 地址

【命令格式】 **ftp-client** [**vrf** *vrfname*] **source** {*ip-address* | *ipv6-address* | *interface*}
ftp-client [**vrf** *vrfname*] **source** {*ip-address* | *interface*}
ftp-client source {*ip-address* | *ipv6-address* | *interface*}
ftp-client source {*ip-address* | *interface*}
ftp-client [**vrf** *vrfname*] **source-address** {*ip-address* | *ipv6-address* }
ftp-client [**vrf** *vrfname*] **source-address** {*ip-address* }
ftp-client source-address {*ip-address* | *ipv6-address* }
ftp-client source {*ip-address* | *interface*}

【参数说明】 **vrf** *vrf-name*：指定 VRF。
ip-address：本地接口的 IPv4 地址。
ipv6-address：本地接口的 IPv6 地址。
Interface：指定客户端源接口。

【命令模式】 全局配置模式

【使用指导】 该命令替代 **ftp-client** [**vrf** *vrfname*] **source-address** {*ip-address* | *ipv6-address*}命令进行源接口和 IP 的配置，使用 **ftp-client** [**vrf** *vrfname*] **source-address** {*ip-address* | *ipv6-address*}的命令将自动转化为新命令保存。
使用该命令可以绑定客户端不同的接口 IP 地址，使客户端使用此 IP 地址连接服务器。默认情况下客户端不进行本地 IP 绑定，由路由进行选择。

↘ 设置 FTP 为文本传输模式

【命令格式】 **ftp-client** [**vrf** *vrf-name*] **ascii**
ftp-client ascii

【参数说明】 **vrf** *vrf-name*：指定 VRF。

【命令模式】 全局配置模式

【使用指导】 使用该命令可以将文件传输方式设置为文本（ASCII）方式。默认情况下 FTP 传输模式为二进制（BINARY）方式。

↘ 恢复 FTP Client 为缺省配置

【命令格式】 **default ftp-client** [**vrf** *vrf-name*]
default ftp-client

【参数说明】 **vrf** *vrf-name*：指定 VRF。

【命令模式】 全局配置模式

【使用指导】 恢复 FTP Client 为缺省配置，数据连接为被动方式，文件传输为二进制模式，清除源 IP 绑定。

配置举例

以下配置举例，仅介绍与 FTP Client 可选择项相关的配置。

↘ 可选项配置

【配置方法】

- 配置 FTP 连接模式为：port
- 配置传输模式为：ASCI
- 配置源 IP 为 192.168.23.167
- 配置 vrf 123 的连接模式为：port
- 配置 vrf 123 的传输模式为：ASCII

```
Ruijie# configure terminal
Ruijie(config)# ftp-client ascii
Ruijie(config)# ftp-client port
Ruijie(config)# ftp-client source-address 192.168.23.167
Ruijie(config)# ftp-client vrf 123 port
Ruijie(config)# ftp-client vrf 123 ascii
Ruijie(config)# end
```

【检验方法】 在设备上进行 **show run**，能看到以下信息

```
Ruijie# show run
!
ftp-client ascii
ftp-client port
ftp-client vrf 123 ascii
ftp-client source-address 192.168.23.167
!
```

常见配置错误

- 源 IP 不是本地 IP。
- 配置 **ftp-client vrf** 之前，先要配置好 **vrf**。

10.6 监视与维护

清除各类信息

无

查看配置情况

作用	命令
查看 FTP Client 的配置	**show run**

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 FTP Client 调试开关。	**debug ftp-client**

11 TIME RANGE

11.1 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。

11.2 典型应用

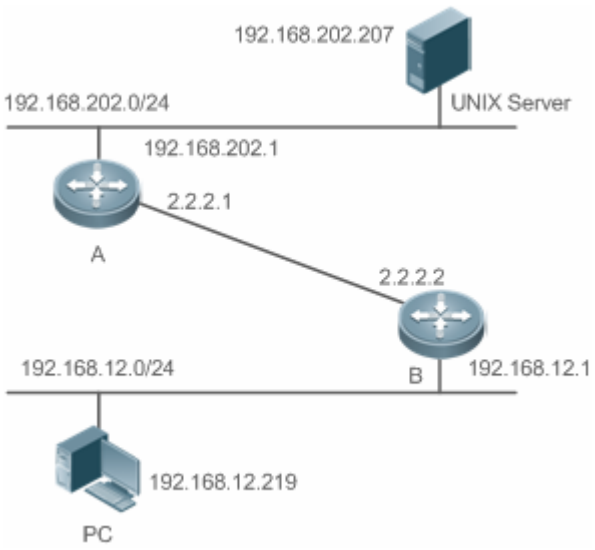
典型应用	场景描述
ACL中的time range应用	应用在 ACL 模块，满足 ACL 基于时间生效的需求。

11.2.1 ACL 中的 time range 应用

应用场景

某单位限制只能在正常上班时间访问远程 UNIX 主机 TELNET 服务：

图 11-1



【注释】 要求通过在设备 B 上配置访问列表，实现以下安全功能：

192.168.12.0/24 网段的主机只能在正常上班时间访问远程 UNIX 主机 TELNET 服务。

功能部属

- 在网络设备 B 上使用 ACL 对来自 192.168.12.0/24 网段的 TELNET 访问进行控制，ACL 应用关联一个 time range，只有在工作时间才允许其访问 Unix 主机。

11.3 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，可以周期性地在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。

11.3.1 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。

11.3.2 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。

11.4 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 *time-range-name*	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 *day-of-the-week time* **to** [*day-of-the-week*] *time*	配置周期时间。

11.4.1 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

【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。

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
```

11.5 监视与维护

查看运行情况

作用	命令
显示 time range。	**show time-range** [*time-range-name*]

配置指南-路由

本分册介绍路由相关内容，包括以下章节：

1. 策略路由
2. ROUTE-DB
3. RIP
4. RIPng
5. OSPFv2
6. OSPFv3
7. 路由管理

1 策略路由

1.1 概述

策略路由（Policy-Based Routing）就是基于策略的路由。将包含策略的路由图应用在接口和设备上，即可实现策略路由。

与静态路由相似，策略路由也是手工配置的路由，不能随网络变化自动更新，仅在本地有效。与静态路由、动态路由相比，策略路由更加灵活。静态路由、动态路由只能依据目的地址转发报文。策略路由可以依据源地址、目的地址、报文长度、入端口等转发报文。

协议规范

无

1.2 典型应用

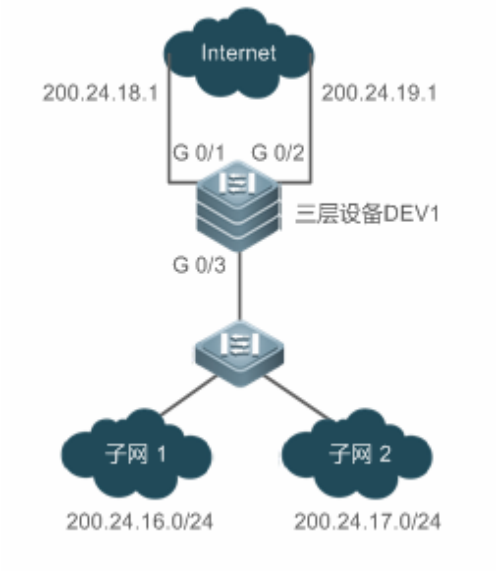
典型应用	场景描述
使用策略路由选择 ISP	为来自不同子网的报文，分别指定优选出接口。

1.2.1 使用策略路由选择ISP

现有用户网络，常常会出现使用到多个 ISP（Internet Server Provider，Internet 服务提供商）资源的情形。由于不同 ISP 申请到的带宽不一，或为了保护某些重点用户的网络资源，需要使用策略路由。通过有选择的控制数据报文的转发，不仅能够充分对利用 ISP 资源，又能满足灵活、多样的应用。

应用场景

图 1-1



某局域网有两个出口连接到因特网，在三层设备 DEV1 上配置策略路由，使这两个出口能够负载分担并互为备份。

具体要求如下：

- 来自子网 1 的数据流，从 GE 0/1 接口发出。
- 来自子网 2 的数据流，从 GE 0/2 接口发出。
- 如果 GE 0/1 链路断开，则将 GE 0/1 上的数据流切换到 GE 0/2 上。反之亦然。

功能部属

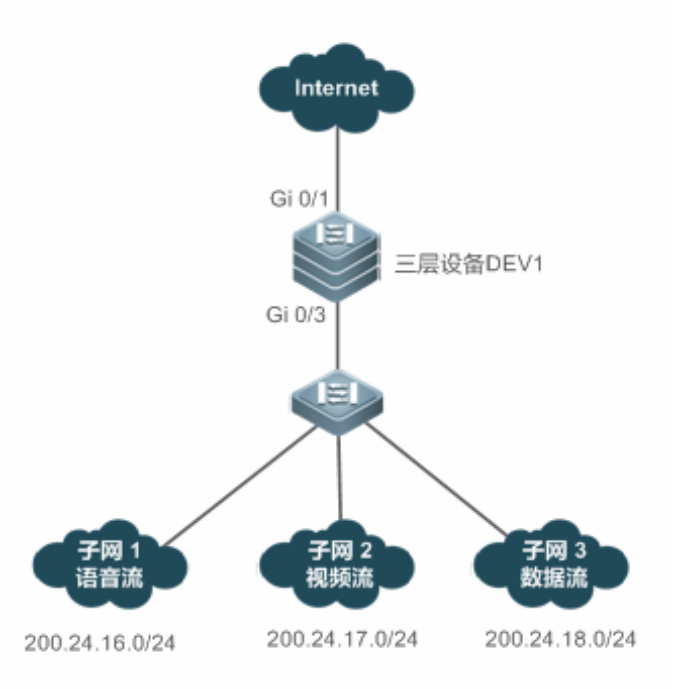
- 在三层设备 DEV1 上，配置两个不同的 ACL：
  ACL1：源地址属于子网 1。
  ACL2：源地址属于子网 2。
- 在三层设备 DEV1 上，在路由图中配置两条策略：
  策略 1：匹配 ACL1 的报文，设置下一跳为 GE0/1、GE0/2。（按配置顺序，GE0/1 优先生效，GE0/2 为备份）
  策略 2：匹配 ACL2 的报文，设置下一跳为 GE0/2、GE0/1。（按配置顺序，GE0/2 优先生效，GE0/1 为备份）
- 在 GE0/3 上配置策略路由（引用路由图），则该接口收到的报文将依照策略转发。

1.2.2 使用策略路由实现流量分类

应用场景

中小企业组网的主要特点是网络结构相对简单，各个分支节点通过运营商专线或者 Internet VPN 方式与中心节点互联，企业组网往往需要实现三网合一（语音、视频、数据），以最大程度的对现有 IP 网络进行利用并节约成本。由于所有的流量都从单一出口流出，所以在网络出口有必要对 QoS 策略进行调整，从而为带宽、时延敏感的应用提供优先通信质量保障。

图 1-2



某局域网有一个出口连接到因特网，在三层设备 DEV1 上配置策略路由，改变来自不同网络报文的 QoS 值。

具体要求如下：

- 来自子网 1 的数据流，表示语音流，DSCP 值设置为 56。
- 来自子网 2 的数据流，表示视频流，DSCP 值设置为 40。
- 来自子网 3 的数据流，表示数据流，DSCP 值设置为 24。

功能部属

- 在三层设备 DEV1 上，配置三个不同的 ACL：
  ACL1：源地址属于子网 1。
  ACL2：源地址属于子网 2。
  ACL3：源地址属于子网 3。
- 在三层设备 DEV1 上，在路由图中配置三条策略：
  策略 1：匹配 ACL1 的报文，设置 DSCP 值为 56。
  策略 2：匹配 ACL2 的报文，设置 DSCP 值为 40。
  策略 3：匹配 ACL3 的报文，设置 DSCP 值为 24。
- 在 GE0/3 上配置策略路由（引用路由图），则该接口收到的报文将依照策略改变 DSCP 值。

1.3 功能详解

功能特性	作用
策略	配置策略路由，需要首先在路由图中配置策略。

策略路由	将包含策略的路由图应用在接口和设备上，即可实现策略路由。

1.3.1 策略

一条策略就是一个 match …, set…语句，表示“如果匹配某些条件，则执行某些处理动作”。

关于策略的详细介绍，请参见“路由图”章节。

策略的执行

在全局模式下，使用 **route-map** *route-map-name* [**permit** | **deny**] [*sequence-number*] 命令在路由图中创建一条策略。

一个路由图中可以包含多条策略。每条策略都有对应的序号，序号越小优先级越高。策略按序号顺序依次执行，一旦满足某条策略的匹配条件，就执行该策略对应的处理动作，并退出路由图。如果不能满足任何一条策略的匹配条件，则不做任何处理。

策略有以下两种工作模式：

- permit：当满足策略的匹配条件时，执行该策略的处理动作，并退出路由图。
- deny：当满足策略的匹配条件时，不执行该策略的处理动作，并退出路由图。

策略的匹配条件

策略的匹配条件包含 0 条、1 条或多条 match 规则。

- 如果包含 0 条 match 规则，则报文不会匹配。
- 如果包含 1 条或多条 match 规则，则必须同时匹配所有 match 规则，才能满足策略的匹配条件。

在路由图模式下，使用 **match** 命令设置 match 规则。一条 **match** 命令对应一条 match 规则。

策略路由支持以下 **match** 命令：

	命令	说明
IPv4 策略路由	**match length**	以 IPv4 报文长度作为匹配条件。 一条策略中只能配置 1 条 **match length** 命令。
	match ip address	以源 IPv4 地址（和目的 IPv4 地址）作为匹配条件。 一条策略中允许配置多条 **match ip address** 命令。
IPv6 策略路由	**match ipv6 address**	以源 IPv6 地址（和目的 IPv6 地址）作为匹配条件。 一条策略中只能配置 1 条 match ipv6 address 命令。

IPv4 策略路由使用 IP 标准或者扩展 ACL 定义报文的源 IP 地址（和目的 IP 地址）范围。

IPv6 策略路由使用 IPv6 扩展 ACL 定义报文的源 IPv6 地址（和目的 IPv6 地址）范围。

策略路由如果引用了 ACL，如果该 ACL 不存在，那么不匹配这条路由子图，从下一条路由子图继续匹配，当所有的路由子图都不匹配时，就走普通路由转发。如果仅配置了 ACL，但未配置 ACE，策略路由转发行为同上述 ACL 不存在的场景。

交换机设备上，如果策略路由的一条路由子图引用了多条 ACL，只匹配第一条存在的 ACL，不会匹配后面的 ACL。

策略的处理动作

策略的处理动作包含 0 条、1 条或多条 set 规则。

- 如果包含 0 条 set 规则，则不做任何处理，直接退出路由图。
- 如果包含 1 条或多条 set 规则，则执行所有处理动作后，退出路由图。

如果 set 规则有优先级关系，则仅优先级最高者生效。

在路由图模式下，使用 **set** 命令设置 set 规则。一条 **set** 命令对应一条 set 规则。

策略路由支持以下 **set** 命令：

	命令	说明
IPv4 策略路由	**set ip tos**	修改 IPv4 报文的 tos 字段。 此命令不能和 **set ip dscp** 同时配置。
	set ip precedence	修改 IPv4 报文的 precedence 字段。 此命令不能和 **set ip dscp** 同时配置。
	set ip dscp	修改 IPv4 报文的 dscp 字段。 此命令不能与 **set ip tos**、**set ip precedence** 同时配置。
IPv6 策略路由	**set ipv6 precedence**	修改 IPv6 报文的 precedence 字段。 IPv6 策略路由不支持 set ipv6 tos 和 set ipv6 dscp。
	set ipv6 next-hop	配置 IPv6 报文转发的下一跳。 匹配 match 规则的 IPv6 报文将优先转发到 **set ipv6 next-hop** 所指定的下一跳，而不管该 IPv6 报文在路由表中的实际选路结果和策略路由指定的下一跳是否一致。 下一跳必须是直连的，否则此命令无效。
	set ipv6 default next-hop	配置 IPv6 报文转发的缺省下一跳。 匹配 match 规则的 IPv6 报文 ,如果该报文在路由表中选路失败或者选到缺省路由，那么该报文将转发到该命令指定的下一跳。 下一跳必须是直连的，否则此命令无效。

优先级顺序：**set ip next-hop > set interface >** 普通路由 **> set ip default next-hop > set default interface >** 缺省路由。以上 set 命令允许同时配置，但只有优先级最高的生效。

1.3.2 策略路由

策略路由

将包含策略的路由图应用在接口或设备上，即可实现策略路由。

- 将路由图应用在接口上，则接口收到的报文遵循策略进行路由。
  此类策略路由常用来控制设备收到的用户数据报文。它只对转发的报文起作用，对本地始发的报文不起作用。
- 将路由图应用在设备上，则本地始发的报文遵循策略进行路由。
  此类策略路由常用来控制设备之间交互的协议报文（比如本地发出的 ping 报文）。它只对本地始发的报文起作用，对转发的报文不起作用。

缺省情况下，设备上不存在策略路由，报文转发参照路由表执行。

交换机产品，支持应用策略路由的接口包括：三层以太网口、SVI 口以及三层 AP 口。

冗余备份或负载均衡

可以在一条策略中设置多个下一跳。多个下一跳之间可以是冗余备份，也可以是负载均衡。缺省为冗余备份。

冗余备份或负载均衡仅对 **set ip next-hop**、**set ip default next-hop**、set ipv6 next-hop、set ipv6 default next-hop 命令设置的下一跳生效，仅在同一 set 规则的多个下一跳之间生效。

- 冗余备份
  按配置顺序，第一个可达的下一跳生效。当前生效的下一跳（R1）发生故障后，流量会自动切换到下一个可达的下一跳（R2）。当 R1 恢复可达时，流量会自动切回 R1。
  新添加的下一跳排序在最后。假设多个下一跳的原有顺序为 R1/R2/R3，删除 R1 后再添加 R1，顺序变为 R2/R3/R1。
  如果所有的下一跳都不可达，则丢弃报文。
- 负载均衡
  多个可达的下一跳同时生效 ,支持 WCMP(Weighted Cost Multiple Path ,加权多路径)和 ECMP(Equal Cost Multiple Path，等价多路径)。某一个可达的下一跳失效后，流量在其它可达的下一跳上负载均衡。

与 Track 联动

策略路由与 Track 联动，对 **set ip next-hop** 命令设置的下一跳生效。

在 **set ip next-hop** 命令中携带参数 **verify-availability**、**track** *track-obj-number*，可以将策略路由与 Track 会话建立联动，监控下一跳的可达性。

策略路由与 Track 联动，有助于增强策略路由对网络环境变化的感知能力。当 Track 发现当前用于转发到下一跳不可达时，会立即通知策略路由将流量切换到下一个可达的下一跳（冗余备份）或者其余所有可达的下一跳（负载均衡）。

仅 IPv4 策略路由支持与 Track 联动。

策略路由与 Track 联动的配置与相关命令，请参见“RNS”章节。

1.4 产品说明



NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE 支持 PBR v6；NBR800G、NBR950G、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR108G-P、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1500G、NBR2000G 不支持 PBR v6。

1.5 配置详解

配置项	配置建议 & 相关命令	
配置策略路由基本功能	⚠ 必须配置。用于应用策略路由对报文进行转发。	
	ip policy route-map	对接口收到的 IPv4 报文应用策略路由。
	ipv6 policy route-map	对接口收到的 IPv6 报文应用策略路由。

1.5.1 配置策略路由基本功能

配置效果

通过制定灵活的策略，对用户数据流进行个性化的路由管理。

通过制定灵活的策略，对协议交互和网络拓扑进行个性化的管理。

注意事项

- 配置策略路由时必须引用路由图。因此，必须在设备上配置路由图。
- 如果配置路由图时引用了 ACL，则必须在设备上配置 ACL。

配置方法

↘ 对接口收到的 IPv4 报文应用策略路由

- 如果需要对流经设备的 IPv4 用户数据流进行个性化的路由管理，则应执行此配置。
- 在用户数据流的入接口上配置。
- 使用 **ip policy route-map** 命令将路由图应用在接口上，则接口收到的 IPv4 报文执行策略路由。

【命令格式】 **ip policy route-map** *route-map-name*
【参数说明】 *route-map-name*：路由图的名称
【缺省配置】 设备上不存在策略路由，报文转发参照路由表执行
【命令模式】 接口模式

【使用指导】 一个接口上只能配置 1 条 **ip policy route-map** 命令。如果在同一个接口上多次配置 **ip policy route-map** 命令，仅最后一次配置生效。

如果此策略路由中引用的路由图实际不存在，则此策略路由不生效。

对接口收到的 IPv6 报文应用策略路由

- 如果需要对流经设备的 IPv6 用户数据流进行个性化的路由管理，则应执行此配置。
- 在用户数据流的入接口上配置。
- 使用 **ipv6 policy route-map** 命令将路由图应用在接口上，则接口收到的 IPv6 报文执行策略路由。

【命令格式】 **ipv6 policy route-map** *route-map-name*

【参数说明】 *route-map-name*：路由图的名称

【缺省配置】 设备上不存在策略路由，报文转发参照路由表执行

【命令模式】 接口模式

【使用指导】 一个接口上只能配置 1 条 **ipv6 policy route-map** 命令。如果在同一个接口上多次配置 **ipv6 policy route-map** 命令，仅最后一次配置生效。

如果此策略路由中引用的路由图实际不存在，则此策略路由不生效。

对本地始发的 IPv4 报文应用策略路由

- 如果需要对 IPv4 协议交互和 IPv4 网络拓扑进行个性化的管理，则应执行此配置。
- 使用 **ip local policy route-map** 命令将路由图应用在设备上，则本地始发的 IPv4 报文执行策略路由。

【命令格式】 **ip local policy route-map** *route-map-name*

【参数说明】 *route-map-name*：路由图的名称

【缺省配置】 设备上不存在策略路由，报文转发参照路由表执行

【命令模式】 全局模式

【使用指导】 一个设备上只能配置 1 条 **ip local policy route-map** 命令。

如果此策略路由中引用的路由图实际不存在，则此策略路由不生效。

对本地始发的 Ipv6 报文应用策略路由

- 如果需要对 Ipv6 协议交互和 Ipv6 网络拓扑进行个性化的管理，则应执行此配置。
- 使用 **ipv6 local policy route-map** 命令将路由图应用在设备上，则本地始发的 IPv6 报文执行策略路由。

【命令格式】 **ipv6 local policy route-map** *route-map-name*

【参数说明】 *route-map-name*：路由图的名称

【缺省配置】 设备上不存在策略路由，报文转发参照路由表执行

【命令模式】 全局模式

【使用指导】 一个设备上只能配置 1 条 **ipv6 local policy route-map** 命令。

如果此策略路由中引用的路由图实际不存在，则此策略路由不生效。

检验方法

- 查看策略路由的配置信息。
- 查看策略路由引用的路由图的配置信息。
- 如果配置路由图时引用了 ACL，则应查看 ACL 的配置信息。

查看 IPv4 策略路由的配置信息

【命令格式】 **show ip policy** [*route-map-name*]

【参数说明】 *route-map-name*：路由图的名称

【命令模式】 特权模式、全局模式、接口模式

【使用指导】 从输出信息中观察有哪些接口上配置了 IPv4 策略路由，引用的路由图叫什么名字。

```
Ruijie# show ip policy
Banlance mode: redundance
Interface               Route map
local                   RM_for_PBR_1
GigabitEthernet 0/1     RM_for_PBR_2
```

Local 表示对本地始发的 IPv4 报文应用策略路由。

查看 IPv6 策略路由的配置信息

【命令格式】 **show ipv6 policy** [*route-map-name*]

【参数说明】 *route-map-name*：路由图的名称

【命令模式】 特权模式、全局模式、接口模式

【使用指导】 从输出信息中观察有哪些接口上配置了 IPv6 策略路由，引用的路由图叫什么名字。

```
Ruijie#show ipv6 policy
Banlance mode: redundance
Interface           Route map
local               RM_for_PBR_1
VLAN 1              RM_for_PBR_2
```

Local 表示对本地始发的 IPv6 报文应用策略路由。

查看路由图的配置信息

【命令格式】 **show route-map** [*route-map-name*]

【参数说明】 *route-map-name*：路由图的名称

【命令模式】 特权模式、全局模式、接口模式

【使用指导】 设备上可能存在多份路由图。关注策略路由中引用的路由图，查看其策略设置。

```
Ruijie# show route-map
route-map RM_FOR_PBR, permit, sequence 10
  Match clauses:
```

```
    ip address acl1
  Set clauses:
    ip next-hop 200.24.18.1
route-map RM_FOR_PBR, permit, sequence 20
  Match clauses:
    ip address acl2
  Set clauses:
    ip next-hop 200.24.19.1
```

查看 ACL 的配置信息

【命令格式】 **show access-lists** [*acl-id* | *acl-name*]

【参数说明】 *acl-id*：ACL 的编号

acl-name：ACL 的名称

【命令模式】 特权模式、全局模式、接口模式

【使用指导】 设备上可能存在多个 ACL。关注路由图中引用的那个 ACL，查看其配置信息。

```
Ruijie# show access-lists 1
ip access-list standard 1
 10 permit 200.24.16.0 0.0.0.255
ip access-list standard 2
 10 permit 200.24.17.0 0.0.0.255
```

查看 IPv4 策略路由的路由信息

【命令格式】 **show ip pbr route** [**interface** *if-name* | **local**]

【参数说明】 *if-name*：接口名称

local：本地

【命令模式】 特权模式、全局模式、接口模式

【使用指导】 指定接口或设备本地，查看 IPv4 策略路由的路由信息。

```
Ruijie# show ip pbr route
PBR IPv4 Route Summay : 1
Interface        : GigabitEthernet 0/1
  Sequence       : 10
  Min Length     : None
  Max Length     : None
  VRF ID         : 0
  Route Flags    :
   Route Type    : PBR
   Direct        : Permit
   Priority      : High
   Tos_Dscp      : None
   Precedence    : None
  Tos_Dscp       : 0
```

```
Precedence      : 0
Mode            : redundance
Nexthop Count   : 1
 Nexthop[0]     : 192.168.8.100
 Weight[0]      : 1
 Ifindex[0]     : 2
```

网关产品不支持 VRF，配置举例仅作为配置参考，实际请以具体设备配置为准。

查看 IPv6 策略路由的路由信息

【命令格式】 **show ipv6 pbr route** [**interface** *if-name* | **local**]

【参数说明】 *if-name*：接口名称

local：本地

【命令模式】 特权模式、全局模式、接口模式

【使用指导】 指定接口或设备本地，查看 IPv6 策略路由的路由信息。

```
Ruijie# show ipv6 pbr route
PBR IPv6 Route Summary : 1
Interface         : GigabitEthernet 0/1
  Sequence        : 10
  ACL[0]          : 2900
  ACL_CLS[0]      : 5
  Min Length      : None
  Max Length      : None
  VRF ID          : 0
  Route Flags     :
   Route Type     : PBR
   Direct         : Permit
   Priority       : High
   Tos_Dscp       : None
   Precedence     : None
  Tos_Dscp        : 0
  Precedence      : 0
  Mode            : redundance
  Nexthop Count   : 1
   Nexthop[0]     : 10::2
   Weight[0]      : 1
   Ifindex[0]     : 2
```

查看 IPv4 策略路由引用的路由图

【命令格式】 **show ip pbr route-map** *rmap-name*

【参数说明】 *rmap-name*：路由图名称

【命令模式】 特权模式、全局模式、接口模式

【使用指导】 指定路由图，查看 IPv4 策略路由引用的路由图。

```
Ruijie# show ip pbr route-map rm
PBR VRF: GLOBAL, ID: 0
 Forward Mode: redundance
 Forwarding: On

Route-map rm
  Route-map index: Sequence 10, permit
    Match rule:
      ACL ID :   2900, CLS: 1, Name: acl1
    Set rule:
      IPv4 nexthop: 192.168.8.100, (VRF name: , ID: 0), Weight: 0
        PBR state info ifx: 2, Connected: True, Track state: Up
```

网关产品不支持 VRF, Global，配置举例仅作为配置参考，实际请以具体设备配置为准。

查看 IPv6 策略路由引用的路由图

【命令格式】 **show ipv6 pbr route-map** *rmap-name*

【参数说明】 *rmap-name*：路由图名称

【命令模式】 特权模式、全局模式、接口模式

【使用指导】 指定路由图，查看 IPv6 策略路由引用的路由图。

```
Ruijie# show ipv6 pbr route-map rm6
PBR VRF: GLOBAL, ID: 0
 Forward Mode: redundance
 Forwarding: On

Route-map rm6
  Route-map index: Sequence 10, permit
    Match rule:
      ACL ID :   2901, CLS: 5, Name: acl6
    Set rule:
      IPv6 nexthop: 10::2, (VRF name: , ID: 0), Weight: 0
        PBR state info ifx: 2, Connected: True, Track state: Up
```

查看 IPv4 策略路由转发的报文个数统计值

【命令格式】 **show ip pbr statistics** [**interface** *if-name* | **local**]

【参数说明】 *if-name*：接口名称

local：本地

【命令模式】 特权模式、全局模式、接口模式

【使用指导】

```
Ruijie# show ip pbr statistics
IPv4 Policy-based route statistic
gigabitEthernet 0/1
  statistics : 10
```

查看 IPv6 策略路由转发的报文个数统计值

【命令格式】 **show ipv6 pbr statistics** [**interface** *if-name* | **local**]

【参数说明】 *if-name*：接口名称

local：本地

【命令模式】 特权模式、全局模式、接口模式

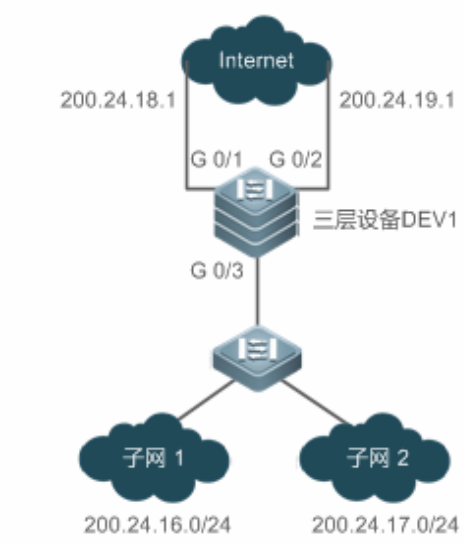
【使用指导】

```
Ruijie# show ipv6 pbr statistics
IPv6 Policy-based route statistic
gigabitEthernet 0/1
  statistics : 20
```

IPv4 策略路由与 Track 联动

【网络环境】

图 1-3



三层设备 DEV1 通过 GE0/3 连接子网 1 和子网 2。子网 1 的网段为 200.24.16.0/24，子网 2 的网段为 200.24.17.0/24。

三层设备 DEV1 通过 GE0/1 和 GE0/2 连接因特网，其下一跳为 200.24.18.1、200.24.19.1。

【配置要求】

- DEV1 设备能够快速探知出口链路故障，并快速切换备份链路。

【配置方法】 在配置 IPv4 策略路由，根据报文源地址选择出口链路配置下，增加或修改如下配置（红色字段）：

- 设置两个 Track 对象，分别跟踪两个出口下一跳的可达性。
- 配置策略时，设置下一跳与 Track 对象联动。

DEV1

```
DEV1(config)# ip access-list extended 101
```

```
DEV1(config-ip-acl)# permit ip 200.24.16.0 0.0.0.255 any
DEV1(config-ip-acl)# exit
DEV1(config)# ip access-list extended 102
DEV1(config-ip-acl)# permit ip 200.24.17.0 0.0.0.255 any
DEV1(config-ip-acl)# exit
DEV1(config)#ip rns 1
DEV1(config-ip-rns)#icmp-echo 200.24.18.1
DEV1(config)#ip rns schedule 1 start-time now life forever
DEV1(config)#track 1 rns 1
DEV1(config)#ip rns 2
DEV1(config-ip-rns)#icmp-echo 200.24.19.1
DEV1(config)#ip rns schedule 2 start-time now life forever
DEV1(config)#track 2 rns 2
DEV1(config)# route-map RM_FOR_PBR 10
DEV1(config-route-map)# match ip address 101
DEV1(config-route-map)# set ip next-hop verify-availability 200.24.18.1 track 1
DEV1(config-route-map)# set ip next-hop verify-availability 200.24.19.1 track 2
DEV1(config-route-map)# exit
DEV1(config)# route-map RM_FOR_PBR 20
DEV1(config-route-map)# match ip address 102
DEV1(config-route-map)# set ip next-hop verify-availability 200.24.19.1 track 2
DEV1(config-route-map)# set ip next-hop verify-availability 200.24.18.1 track 1
DEV1(config-route-map)# exit
DEV1(config)# interface GigabitEthernet 0/3
DEV1(config-if-GigabitEthernet 0/3)# ip policy route-map RM_FOR_PBR
DEV1(config-if-GigabitEthernet 0/3)# exit
DEV1(config)# ip policy redundance
```

【检验方法】

- 查看 Track 的跟踪对象是否 UP。

DEV1

```
DEV1#show track
Track 1
  Reliable Network Service 1
  The state is Up
    1 change, current state last: 120 secs
  Delay up 30 secs, down 50 secs
Track 2
  Reliable Network Service 2
  The state is Up
    1 change, current state last: 130 secs
  Delay up 30 secs, down 50 secs
```

常见错误

- 配置策略路由时引用了路由图，但此路由图实际并不存在。
- 配置路由图时引用了 ACL，但此 ACL 实际并不存在。

1.5.2 设置冗余备份或负载均衡

配置效果

- 使多个下一跳互为备份，可以增强网络的可靠性。
- 在多个下一跳之间负载均衡，可以扩展网络带宽。

注意事项

- 必须配置策略路由基本功能。
- 冗余备份和负载均衡仅对如下 **set** 命令设置的下一跳生效，且仅在使用相同的 **set** 命令设置的多个下一跳之间生效。

命令	说明
set ip next-hop	配置 IPv4 报文的下一跳。此命令携带参数 *weight*，用来设定 WCMP 的权重，缺省值 1。
set ip default next-hop	配置 IPv4 报文的缺省下一跳。此命令携带参数 *weight*，用来设定 WCMP 的权重。缺省值 1。
set ipv6 next-hop	配置 IPv6 报文的下一跳。此命令携带参数 *weight*，用来设定 WCMP 的权重，缺省值 1。
set ipv6 default next-hop	配置 IPv6 报文的缺省下一跳。此命令携带参数 *weight*，用来设定 WCMP 的权重，缺省值 1。

WCMP 最多可以设置 8 个下一跳，ECMP 最多可以设置 32 个下一跳。

配置方法

设置 IPv4 策略路由在多个下一跳之间冗余备份或负载均衡

- 如果需要在多个下一跳之间进行负载均衡，则需要执行此配置。
- 如果当前配置为负载均衡，需要恢复成冗余备份，则也需要执行此配置。
- 此项配置对设备上配置的所有策略路由生效。

【命令格式】 **ip policy** { **redundance** | **load-balance** }

【参数说明】 redundance：冗余备份

load-balance：负载均衡

【缺省配置】 冗余备份

【命令模式】 全局模式

【使用指导】 选择冗余备份，则按配置顺序，只有第一个下一跳生效。

选择负载均衡，则所有下一跳同时生效，且按权重分担流量。

设置 IPv6 策略路由在多个下一跳之间冗余备份或负载均衡

- 如果需要在多个下一跳之间进行负载均衡，则需要执行此配置。
- 如果当前配置为负载均衡，需要恢复成冗余备份，则也需要执行此配置。
- 此项配置对设备上配置的所有策略路由生效。

【命令格式】 **ipv6 policy** { **redundance** | **load-balance** }
【参数说明】 redundance：冗余备份
load-balance：负载均衡
【缺省配置】 冗余备份
【命令模式】 全局模式
【使用指导】 选择冗余备份，则按配置顺序，只有第一个下一跳生效。
选择负载均衡，则所有下一跳同时生效，且按权重分担流量。

检验方法

- 查看多个下一跳之间是冗余备份还是负载均衡。

查看 IPv4 策略路由多个下一跳之间是冗余备份或负载均衡

【命令格式】 **show ip policy** [*route-map-name*]
【参数说明】 *route-map-name*：指定路由图。
【配置模式】 特权模式、全局模式、接口模式
【使用指导】 如下示例，关注红色字段。

```
ruijie# show ip policy
Banlance mode: redundance
Interface               Route map
local                   test
GigabitEthernet 0/3     test
```

查看 IPv6 策略路由多个下一跳之间是冗余备份或负载均衡

【命令格式】 **show ipv6 policy** [*route-map-name*]
【参数说明】 *route-map-name*：指定路由图。
【配置模式】 特权模式、全局模式、接口模式
【使用指导】 如下示例，关注红色字段。

```
ruijie#show ipv6 policy
Banlance mode: redundance
Interface               Route map
VLAN 1                  RM_for_Vlan_1
VLAN 2                  RM_for_Vlan_2
```

配置举例

↘ 配置 IPv4 策略路由，多个下一跳之间冗余备份

参考上文举例: 配置 IPv4 策略路由，根据报文源地址选择出口链路

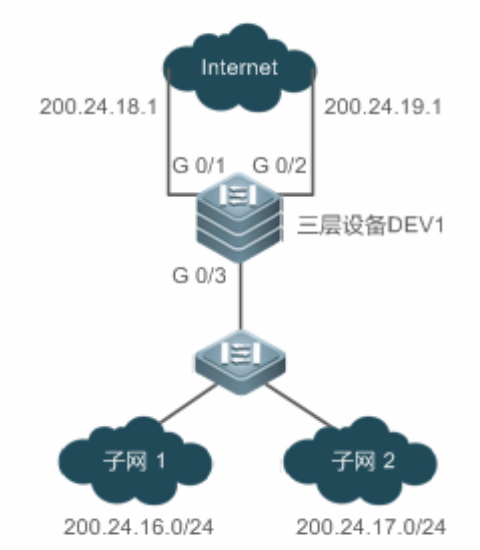
↘ 配置 IPv6 策略路由，多个下一跳之间冗余备份

参考上文举例：配置 IPv6 策略路由，根据报文源地址选择出口链路

↘ 配置 IPv4 策略路由，多个下一跳之间负载均衡

【网络环境】

图 1-4



三层设备 DEV1 通过 GE0/3 连接子网 1 和子网 2。子网 1 的网段为 200.24.16.0/24，子网 2 的网段为 200.24.17.0/24。

三层设备 DEV1 通过 GE0/1 和 GE0/2 连接因特网，其下一跳为 200.24.18.1、200.24.19.1。

【配置要求】 该局域网有两个出口连接到因特网，要求：GE0/1 口与 GE0/2 口各分担一半的流量。

【配置方法】

- 配置策略路由基本功能。指定多个下一跳。
- 设置负载均衡模式。

```
DEV1(config)# route-map RM_LOAD_PBR 10
DEV1(config-route-map)# set ip next-hop 200.24.18.1
DEV1(config-route-map)# set ip next-hop 200.24.19.1
DEV1(config-route-map)# exit
DEV1(config)# interface GigabitEthernet 0/3
DEV1(config-if-GigabitEthernet 0/3)# ip policy route-map RM_LOAD_PBR
DEV1(config-if-GigabitEthernet 0/3)# exit
DEV1(config)# ip policy load-balance
```

【检验方法】
- 查看 IPv4 策略路由的配置信息
- 查看路由图的配置信息

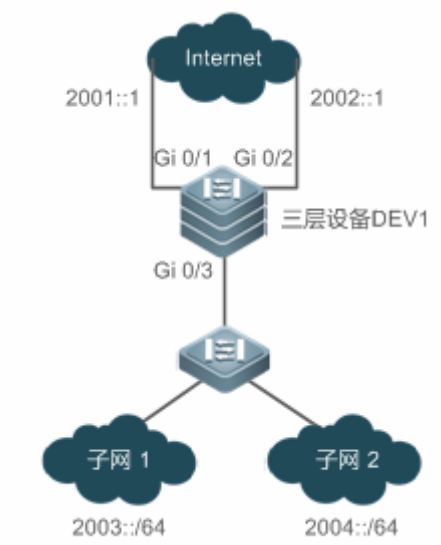
```
DEV1# show ip policy
Balance mode: load-balance
Interface                    Route map
GigabitEthernet 0/3          RM_LOAD_PBR
DEV1# show route-map
route-map PBR-VRF-Selection, permit, sequence 10
Match clauses:
Set clauses:
ip next-hop 200.24.18.1 8
ip next-hop 200.24.19.1 8
```

网关产品不支持 VRF，配置举例仅作为配置参考，实际请以具体设备配置为准。

配置 IPv6 策略路由，多个下一跳之间负载均衡

【网络环境】

图 1-5



DEV1 通过 GE0/3 连接子网 1 和子网 2。子网 1 的网段为 2003::/64，子网 2 的网段为 2004::/64。
DEV1 通过 GE0/1 和 GE0/2 连接因特网，其下一跳为 2001::1/64、2002::1/64。

【配置要求】 该局域网有两个出口连接到因特网，要求：GE0/1 口与 GE0/2 口各分担一半的流量。

【配置方法】
- 配置策略路由基本功能。指定多个下一跳。
- 设置负载均衡模式。

```
DEV1(config)# route-map RM_LOAD_PBR 20
DEV1(config-route-map)# set ipv6 next-hop 2001::1
DEV1(config-route-map)# set ipv6 next-hop 2002::1
DEV1(config-route-map)# exit
```

```
DEV1(config)# interface GigabitEthernet 0/3
DEV1(config-if-GigabitEthernet 0/3)# ipv6 policy route-map RM_LOAD_PBR
DEV1(config-if-GigabitEthernet 0/3)# exit
DEV1(config)# ipv6 policy load-balance
```

【检验方法】

- 查看 IPv6 策略路由的配置信息
- 查看路由图的配置信息

```
DEV1# show ipv6 policy
Balance mode: load-balance
Interface                      Route map
GigabitEthernet 0/3            RM_LOAD_PBR
DEV1# show route-map
route-map PBR-VRF-Selection, permit, sequence 10
  Match clauses:
  Set clauses:
    ipv6 next-hop 2001::1
    ipv6 next-hop 2002::1
```

常见配置错误

无

1.6 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 IPv4 策略路由转发的报文数统计值	**clear ip pbr statistics** [**interface** *if-name* | **local**]
清除 IPv6 策略路由转发的报文数统计值	**clear ipv6 pbr statistics** [**interface** *if-name* | **local**]

查看运行情况

作用	命令
查看 IPv4 策略路由的配置信息。	**show ip policy**
查看 IPv6 策略路由的配置信息。	**show ipv6 policy**
查看路由图的配置信息。	**show route-map** [*name*]
查看 ACL 的配置信息。	**show access-list**

查看 IPv4 策略路由的路由信息。	**show ip pbr route** [**interface** *if-name* | **local**]
查看 IPv6 策略路由的路由信息。	**show ipv6 pbr route** [**interface** *if-name* | **local**]
查看 IPv4 策略路由引用的路由图。	**show ip pbr route-map** *rmap-name*
查看 IPv6 策略路由引用的路由图。	**show ipv6 pbr route-map** *rmap-name*
查看 IPv4 策略路由的统计信息。	**show ip pbr statistics** [**interface** *if-name* | **local**]
查看 IPv6 策略路由的统计信息。	**show ipv6 pbr statistics** [**interface** *if-name* | **local**]

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
打开策略路由的错误调试开关	**debug pbr error**
打开策略路由的事件相关调试开关	**debug pbr events**
打开策略路由支持多业务卡相关调试开关	**debug pbr ms**
打开策略路由的消息通讯调试开关	**debug pbr msg**
打开策略路由与 NSM 交互的调试开关	**debug pbr nsm**
打开策略路由的报文转发相关的调试开关	**debug pbr packet**
打开策略路由的 GR 调试开关	**debug pbr restart**

2 ROUTE-DB

2.1 概述

地址库（ROUTE-DB）是指在多运营商线路环境中，根据用户访问的外网地址来匹配地址库，找出最合适的线路类型转发报文，降低用户跨运营商访问的几率，提高用户访问网络的速度。

协议规范

- 无

2.2 典型应用

典型应用	场景描述
多运营商线路场景	网络出口设备通过多线路接入到不同的运营商网络。

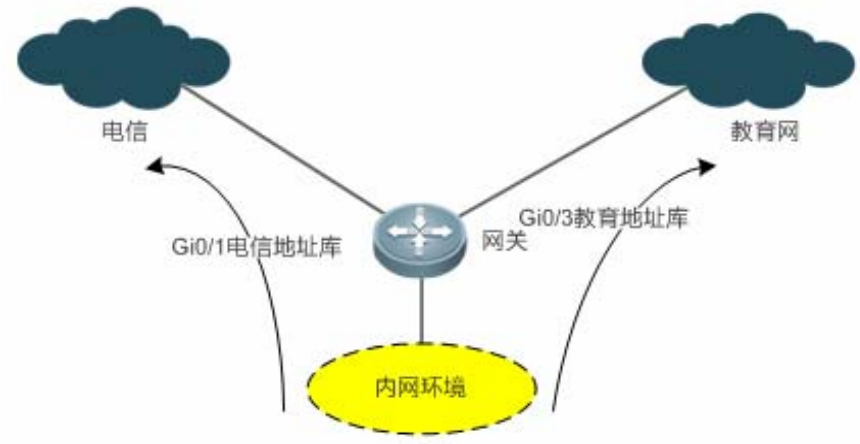
2.2.1 多运营商线路场景

应用场景

在网络出口环境中，有 2 条出口线路，分别为中国电信，教育网。

- 访问电信资源的数据流，走电信线路。
- 访问教育网资源的数据流，走教育网线路。

图 2-1



功能部属

- 为不同的线路配置不同的运营商。

2.3 功能详解

基本概念

↘ ISP

ISP(Internet Service Provider) 互联网服务提供商，即向广大用户综合提供互联网接入业务、信息业务、和增值业务的电信运营商。

当用户跨运营商访问某个网络资源的时候，往往会出现速度异常缓慢，甚至无法访问的情况。

功能特性

功能特性	作用
地址库选路	根据用户访问的外网地址来匹配地址库，找出最合适的线路类型来转发报文。
地址库升级	升级地址库版本。
自定义地址库	创建并添加自定义地址库
地址库查询	查询地址库信息

2.3.1 地址库选路

在多运营商线路场景，降低用户跨运营商访问的几率，提高用户访问网络的速度。

工作原理

当用户跨运营商访问某个网络资源时，会出现访问速度异常缓慢，甚至无法访问的情况，这就让许多网络场所都采用了多线路接入，多线路接入就需要网络出口设备能够根据用户访问外网的 IP 来自动选择线路类型进行转发。地址库就是在这种情况下，匹配外网 IP，根据不同外网 IP 确定该数据流需要使用的线路类型。从而保证用户不会出现跨运营商访问的情况出现，提高用户体验。

由于各运营商的网段划分是固定的，将这些网段划分信息记录在加密的地址库文件中。当设备运行时，通过获取这些信息修改路由表，从而达到控制用户数据流选路的目的。

相关配置

↘ 配置接口的地址库。

缺省情况下，所有接口是没有配置对应的地址库的。

使用 **route-auto-choose** 命令配置接口的地址库功能。

2.3.2 地址库升级

当地址库信息发生变更的时候，就需要更新地址库。

工作原理

当运营商的地址信息发生改变的时候，就需要更新地址库里面的信息，重新生成新版本的地址库，升级到设备上。

相关配置

↘ 升级地址库信息

使用 **route-auto-choose update** 命令来升级地址库信息。

2.3.3 自定义地址库

用户可以根据需要添加自定义的地址库信息。

工作原理

无

相关操作

↘ 添加用户自定义的地址库。

使用 **route-auto-choose user-defined name** 命令来添加用户自定义地址库的信息。

2.3.4 地址库查询

当管理员需要掌握当前地址库文件中有多少运营商类型，或者确定某个 IP 属于哪个运营商时，就需要对地址库进行查询。

工作原理

通过命令查询地址库文件中支持的运营商类型：若为老版本地址库，则查询返回默认的四大运营商信息；若含有其他二级运营商类型，则返回所有的运营商信息。地址库中每个 IP 对应一个运营商，查询地址库文件信息即可。

相关操作

使用 **show route-db-info db-type** 命令可以查询当前地址库文件中的运营商类型；

使用 **show route-db-info** *ip-address* 命令可以查询 *ip-address* 所属的运营商。

2.4 配置详解

配置项	配置建议 & 相关命令	
配置地址库	⚠ 必须配置。	
	route-auto-choose	配置地址库类型
地址库升级	⚠ 可选配置。	
	route-auto-choose update	更新地址库
自定义地址库	⚠ 可选配置。	
	route-auto-choose user-defined name	添加自定义地址库信息

2.4.1 配置地址库

配置效果

- 配置地址库类型，是符合地址库的流量走到该线路。

注意事项

- 以前运营商的环境相对简单，所以考虑一般一个出口只有一个运营商属性。现在越来越多的二级运营商出现，一个二级运营商可能同属于多个一级运营商，造成负载均衡无法通过地址库来辅助，多出口负载均衡效果不佳。鉴于此，需要在一个接口上可以配置多个运营商，即一个接口不再局限于只能设置一种线路类型，可以把 gigabitEthernet 0/1 同时配置为电信和联通线路类型。
- 不同的接口可以设置同一种线路类型，例如，gigabitEthernet 0/1 和 gigabitEthernet 0/2 可同时属于电信线路。

配置方法

↘ 配置地址库类型

- 必须配置。

检验方法

将某个接口配置为电信。

- 访问对应的电信资源，看是否选路正确。
- 使用 traceroute 验证选路是否准确。

相关命令

配置地址库类型

【命令格式】 [**no**] **route-auto-choose** { **cnc** | **cnii** | **cernet** | **cmcc** | *word* } *interface next-hop* [**tag** *num*] [*distance*]

【参数说明】 **cnc**：联通地址库。

cnii：电信地址库。

cernet：教育网地址库。

cmcc：移动地址库。

word：用于配置除以上 4 个运营商的其他类型。

interface：地址库对应的路由出接口。

next-hop：地址库对应的路由下一跳 ip。

tag *num*：地址库对应的路由的 tag。

distance：地址库路由的 metric 值。

【命令模式】 全局配置模式

【使用指导】 -

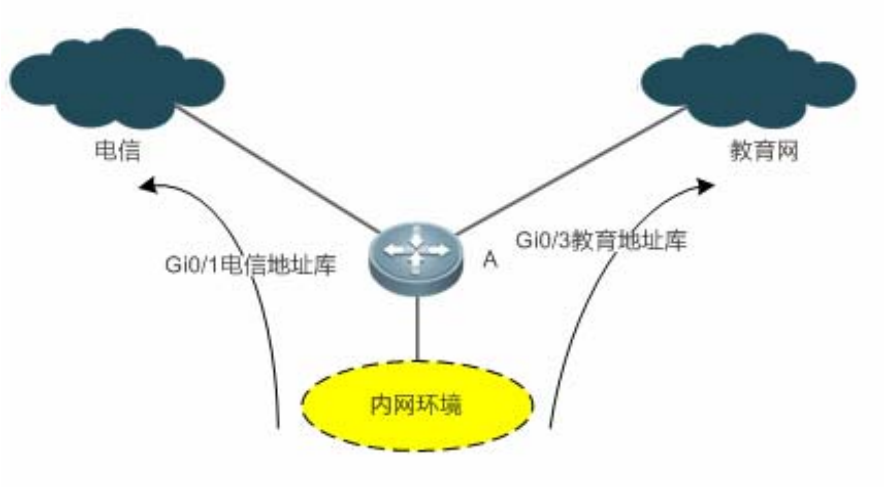
配置举例

以下配置举例，仅介绍与地址库相关的配置。

在 gigabitEthernet 0/1 口应用电信地址库，在 gigabitEthernet 0/3 口应用教育网地址库。

【网络环境】

图 2-2



【配置方法】 ● 在 gigabitEthernet 0/1 口上应用电信地址库，gigabitEthernet 0/3 口上应用教育网地址库。

A

```
A# configure terminal
```

```
A(config)# route-auto-choose cnii gigabitEthernet 0/1 202.100.12.5
A(config)# route-auto-choose cernet gigabitEthernet 0/3 201.1.1.1
```

【检验方法】 内网访问电信资源，看数据流是否选路正确。

- 通过 show 命令可以查看是否配置成功。

A

```
A# show run | i route-auto-choose
route-auto-choose cnii gigabitEthernet 0/1 202.100.12.5
route-auto-choose cernet gigabitEthernet 0/3 201.1.1.1
```

常见错误

- 配置的时候没有配置对应的路由出接口。
- 配置了地址库接口 down 掉，走该地址库的流量不会在走默认路由，而是直接丢掉。

2.4.2 地址库升级

配置效果

- 将新的版本更新到正在运行的系统中。

注意事项

无

配置方法

- 将新的特征库版本上传到设备上。
- 使用命令 route-auto-choose update 进行更新。

检验方法

查看地址库版本。

相关命令

↘ 配置升级地址库

【命令格式】 **route-auto-choose update**

【参数说明】 **update**：更新。

【命令模式】 全局配置模式
【使用指导】 -

配置举例

↘ 升级地址库。

【配置方法】
- 升级地址库。

```
Ruijie# configure terminal
Ruijie(config)# route-auto-choose update
Ruijie(config)# end
```

【检验方法】 无提示异常，即成功。

常见配置错误

- 无。

2.4.3 自定义地址库

配置效果

- 添加新的用户自定义地址库信息。

注意事项

无

配置方法

- 使用命令 route-auto-choose user-defined name 添加用户自定义地址库信息。

检验方法

使用 show route-db-info user-defined 命令查看自定义地址库信息。

相关命令

↘ 配置添加自定义地址库信息

【命令格式】 **route-auto-choose user-defined name** *string* **[** *ip_address ip_mask* **]**

【参数说明】 *string*：用户自定义库名称。

ip_address：用户自定义地址库 IP

ip_mask：用户自定义地址库掩码

【命令模式】 全局配置模式

【使用指导】 -

配置举例

↘ 升级地址库。

【配置方法】

- 添加用户自定义地址库信息

```
Ruijie# configure terminal
Ruijie(config)# route-auto-choose user-defined name test1 1.2.3.0 255.255.255.0
Ruijie(config)# end
```

【检验方法】

- 使用 show route-db-info user-defined 命令，可以查看添加的自定义地址库信息。

```
Ruijie#show route-db-info user-defined
test1:
  1.2.3.0 255.255.255.0
```

常见配置错误

- 无。

2.5 监视与维护

清除各类信息

无

查看运行情况

无

查看调试信息

无

3 RIP

3.1 概述

RIP（Routing Information Protocol，路由信息协议）是一种单播路由协议，应用于 IPv4 网络。运行 RIP 的路由器之间通过交换路由信息，获得到达远程网络的路由。

RIP 属于 IGP (Interior Gateway Protocol，内部网关协议)，只能在 AS 内运行，适用于规模较小的网络（不大于 16 跳）。

协议规范

- RFC1058：定义了 RIPv1
- RFC2453：定义了 RIPv2

3.2 典型应用

典型应用	场景描述
RIP 基本应用	在一个小型网络中，通过 RIP 自动维护路由信息。

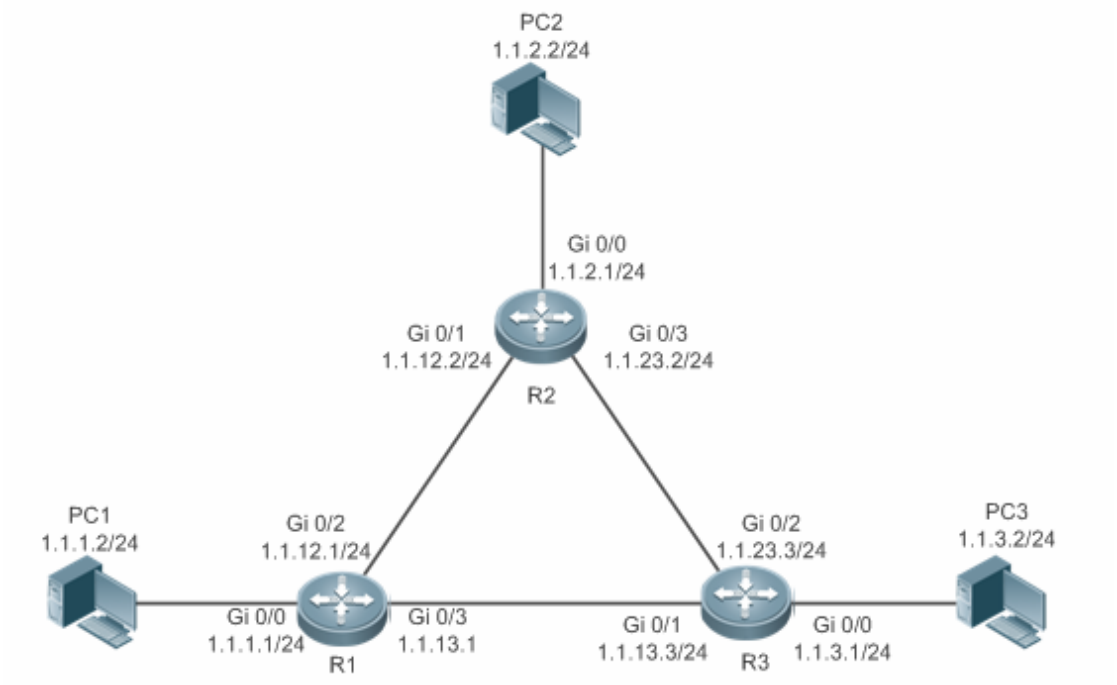
3.2.1 RIP基本应用

应用场景

在组网结构比较简单的网络中，可以通过配置 RIP 实现网络互通，相比 OSPF 等 IGP 协议 RIP 的配置更为简单，相比静态路由 RIP 能够动态适应网络结构变化，更容易维护。

以下图为例，为了使得 PC1，PC2，PC3 互通，可以在 R1，R2，R3 上配置 RIP 路由。

图 3-1



功能部属

- 在三台 PC 上配置 IP 和网关；
- 在三台路由设备上配置 IP 和掩码
- 在三台路由设备上配置 RIP 协议

3.3 功能详解

基本概念

IGP、EGP

内部网关协议（Interior Gateway Protocol，简称 IGP）：在一个自治系统内部运行。比如：RIP。

外部网关协议（Exterior Gateway Protocol，简称 EGP）：运行于不同自治系统之间。

有类路由协议、无类路由协议

从支持有类路由还是无类路由的角度来分类：

有类路由协议（Classful Routing Protocol）：支持有类路由。比如：RIPv1。

无类路由协议（Classless Routing Protocol）：支持无类路由。比如：RIPv2。

功能特性

功能特性	说明
RIPv1 与 RIPv2	RIP 有两个版本：RIPv1 和 RIPv2。
交换路由信息	通过在设备间交换路由信息，RIP 可以自动获得远程网络的路由，并保持实时更新。
路由算法	RIP 是一种基于距离矢量（Distance-Vector）算法的协议，运用矢量叠加的方法来计算路由信息。
避免路由环路	RIP 使用“水平分割”和“毒性逆转”等功能来避免路由环路。
安全措施	RIP 使用“认证”、“源地址校验”等功能来保障协议安全。
可靠性措施	RIP 使用“与 BFD 联动”、“快速重路由”、“GR”等功能来增强协议可靠性。
多实例	RIP 支持多实例，支持 VPN 应用。

3.3.1 RIPv1 与RIPv2

RIP 有两个版本：RIPv1、RIPv2。

工作原理

RIPv1

RIPv1 以广播方式发送 RIPv1 报文，广播地址 255.255.255.255，UDP 端口号 520。RIPv1 不能识别子网掩码，仅支持有类别路由。

RIPv2

RIPv2 以组播方式发送 RIPv2 报文，组播地址 224.0.0.9，UDP 端口号 520。RIPv2 能够识别子网掩码，支持无类别路由、路由汇聚、超网路由。RIPv2 支持认证，提供明文认证和 MD5 认证两种方式。

相关配置

启动 RIP 进程

缺省情况下，未启动 RIP 进程。

使用 **router rip** 命令，启动 RIP 进程。

必须在设备上启动 RIP 进程，否则与 RIP 相关的任何功能都无法生效。

在接口上运行 RIP

缺省情况下，接口上未运行 RIP。

使用 **network** 命令，定义一个地址范围，则在此地址范围内的接口上运行 RIP。

在接口上运行 RIP 后，接口上才能交互 RIP 报文，RIP 才能学到其直连网段的路由。

定义 RIP 版本

缺省情况下，接口接收 RIPv1 和 RIPv2 报文，发送 RIPv1 报文。

使用 **version** 命令，定义所有接口上接收和发送的 RIP 报文的版本号。

使用 **ip rip send version** 命令，在接口上定义发送的 RIP 报文的版本号。

使用 **ip rip receive version** 命令，在接口上定义接收的 RIP 报文的版本号。

⚠ 如果相邻路由器上运行的 RIP 版本不一致，运行 RIPv1 的路由器会学习到错误的路由。

限制接口上的报文交互

缺省情况下，运行 RIP 的接口允许接收、发送 RIP 报文。

使用 **no ip rip receive enable** 命令，禁止接口接收 RIP 报文。

使用 **no ip rip send enable** 命令，禁止接口发送 RIP 报文。

使用 **passive-interface** 命令，禁止接口以广播或组播的方式发送 RIP 报文。

发送 RIP 报文的其他方式

缺省情况下，以广播方式发送 RIPv1 报文，以组播方式发送 RIPv2 报文。

使用 **ip rip v2-broadcast** 命令，在接口上以广播方式发送 RIPv2 报文。

使用 **neighbor** 命令，以单播方式向指定的邻居路由器发送 RIP 报文。

3.3.2 交换路由信息

与静态路由相比，动态路由协议的一大优点：通过在设备间交换路由信息，设备可以自动获得远程网络的路由，并保持实时更新。

工作原理

初始化

路由器启动 RIP 后，会向相邻路由器发送请求报文（Request message），请求全部路由信息（即路由表）。邻居收到请求报文后，回送包含本地路由表的响应报文（Response message）。路由器收到响应报文后，更新本地路由表，同时向相邻路由器发送更新报文（Update message），通告路由更新信息。相邻路由器收到更新报文后，更新本地路由表，并向其它相邻路由器发送更新报文。在一连串的更新通告后，各路由器都能获得并保持最新的路由信息。

定时更新

缺省情况下，RIP 启用定时更新。相邻路由器之间每隔 30 秒（update timer）进行完全的路由信息交换（即将整个路由表发送给邻居）。1 份更新报文只能包含 25 条路由，发送整个路由表可能需要大量更新报文。通过设置更新报文间的发送延时，可以避免路由信息丢失。

ℹ 对于每条非本地路由，如果 180 秒内（invalid timer）得不到刷新，则 metric 值改为 16（不可达）；如果随后的 120 秒内（flush timer）得不到刷新，则从路由表中删除。

触发更新

启用触发更新后，定时更新自动关闭。当路由信息发生改变时，立即向邻居发送与改变有关的路由（而非完整的路由表），并采用确认+重发机制来保障邻居成功接收。与定时更新相比，触发更新有助于减少泛洪，加速路由收敛。

能够触发更新的事件包括：路由设备启动、接口状态改变、路由信息发生改变（比如 metric 值）、接收到请求报文。

路由汇聚

RIP 向邻居发送路由信息时，会将属于同一个有类网络的子网路由汇聚成一条路由，发送给邻居。比如：将 80.1.1.0/24（metric=2）和 80.1.2.0/24（metric=3）汇聚成 80.0.0.0/8（metric=2），汇聚后的路由选用最优的 metric 值。

仅 RIPv2 支持路由汇聚。聚合路由可以缩减路由表，提高交换路由信息的效率。

超网路由

当路由的掩码长度小于其自然掩码长度时，这条路由称为超网路由。比如：80.0.0.0/6。根据 IP 地址分类，80.0.0.0 属于 A 类网络，其自然掩码长度为 8，所以 80.0.0.0/6 是超网路由。

仅 RIPv2 支持超网路由。

缺省路由

在路由表中，目的网络为 0.0.0.0/0 的路由为缺省路由。

可以从邻居学到缺省路由，也可以向邻居发送缺省路由。

路由重分布

对于 RIP 来说，其他类型的路由（比如直连路由、静态路由、其他路由协议的路由）为外部路由。

可以将设备上的外部路由（不包括缺省路由）重分布到 RIP 中，通告给邻居。

路由过滤

可以通过设置过滤规则，限制相邻设备间交换的路由信息。只有被过滤规则允许的路由信息，才能被发送或接收。

相关配置

更新报文间的发送延时

缺省情况下，连续发送无延时。

使用 **output-delay** 命令，设置更新报文间的发送延时。

RIP 时钟

缺省情况下，update timer 为 30 秒，invalid timer 为 180 秒，flush 为 120 秒。

使用 **timers basic** 命令，修改 RIP 时钟的超时时间。

增加超时时间，有助于减少路由振荡。缩短超时时间，有助于加快路由收敛。

相邻设备上的 RIP 时钟值必须一致。若没有特殊要求，不建议修改 RIP 时钟。

触发更新

缺省情况下，启用定时更新。

使用 **ip rip triggered** 命令，在接口上启动触发更新，定时更新关闭。

使用 **ip rip triggered retransmit-timer** 命令，修改更新报文的重发间隔，缺省值 5 秒。

使用 **ip rip triggered retransmit-count** 命令，修改更新报文的最大重发次数，缺省值 36 次。

路由汇聚

缺省情况下，如果允许接口发送 RIPv2 报文，则自动进行路由汇聚。

使用 **no auto-summary** 命令，关闭自动汇聚。

使用 **ip rip summary-address** 命令，在接口上配置路由汇聚。

超网路由

缺省情况下，如果允许接口发送 RIPv2 报文，则允许发送超网路由。

使用 **no ip rip send supernet-routes** 命令，禁止发送超网路由。

缺省路由

使用 **ip rip default-information** 命令，在接口上向邻居通告缺省路由。

使用 **default-information originate** 命令，从所有接口向邻居通告缺省路由。

↘ 路由重分布

使用 **redistribute** 命令，将外部路由（不包括缺省路由）重分布到 RIP，通告给邻居。

↘ 路由过滤

使用 **distribute-list out** 命令，设置过滤规则，限制设备发出的路由信息。

使用 **distribute-list in** 命令，设置过滤规则，限制设备接收的路由信息。

3.3.3 路由算法

RIP 是一种基于距离矢量（Distance-Vector）算法的协议，运用矢量叠加的方法来计算路由信息。

工作原理

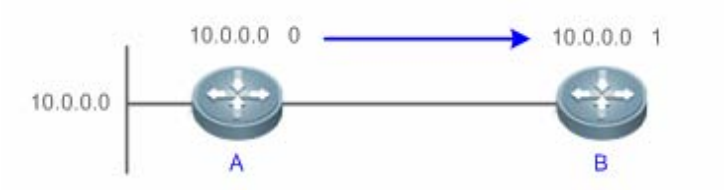
↘ 距离矢量算法

RIP 是一种基于距离矢量算法的协议。“距离矢量”就是将一条路由信息看作一个由目的网络和距离（metric）组成的矢量。路由器从邻居处获得一条路由信息，并在这条路由信息上叠加从自己到这个邻居的距离矢量，从而形成自己的路由信息。

RIP 使用跳数（Hop Count）来衡量到达目的网络的距离（metric）。缺省情况下，路由器到与它直接相连网络的跳数为 0，通过一个路由器可达的网络的跳数为 1，其余依此类推。也就是说，metric 等于从本网络到达目的网络间的路由器数量。为限制收敛时间，RIP 规定 metric 取 0～15 之间的整数，大于或等于 16 表示目的网络或主机不可达。由于这个限制，使得 RIP 不可能在大型网络中得到应用。

如下图所示，A 连接网络 10.0.0.0。B 从 A 处获得路由信息（10.0.0.0，0），则在此基础上叠加 metric1，得到自己的路由信息（10.0.0.0，1），下一跳指向 A。

图 3-2

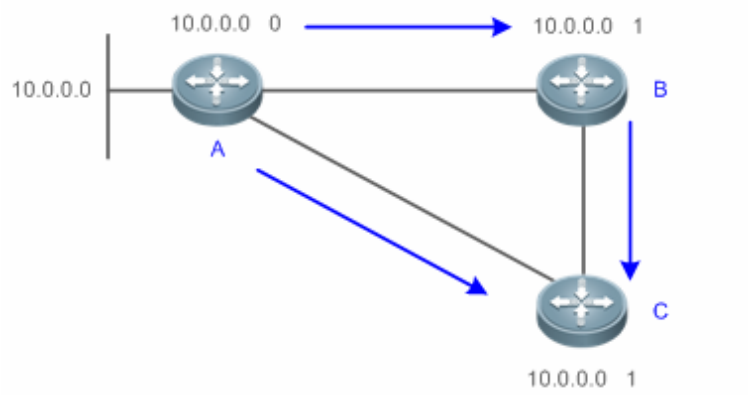


↘ 选择最优路由

RIP 选择最优路由的原则：如果路由器获得了多条到达同一目的网络的路由信息，优先选用 metric 值较小的路由信息。

如下图所示，A 连接网络 10.0.0.0。C 从 A 处获得路由信息（10.0.0.0，0），从 B 处获得路由信息（10.0.0.0，1），则 C 会选用来自 A 的路由信息，并在此基础上叠加 metric1，得到自己的路由信息（10.0.0.0，1），下一跳指向 A。

图 3-3



当路由器上存在多种来源的路由时，优先选用 distance 值较小的路由。

路由来源	缺省 distance 值
直连网络	0
静态路由	1
OSPF 路由	110
RIP 路由	120
不可达路由	255

相关配置

修改 distance 值

缺省情况下，RIP 路由的 distance 值为 120。

使用 **distance** 命令，可以修改 RIP 路由的 distance 值。

修改 metric 值

对于设备主动发现的 RIP 路由，缺省 metric 值等于从本地到目的网络的跳数。对于人为配置的 RIP 路由（缺省路由、重分布路由），缺省 metric 值为 1。

使用 **offset-list in** 命令，可以增加收到的 RIP 路由的 metric 值。

使用 **offset-list out** 命令，可以增加发出的 RIP 路由的 metric 值。

使用 **default-metric** 命令，可以修改重分布路由的缺省 metric 值。

使用 **redistribute** 命令，可以在重分布路由时修改其 metric 值。

使用 **default-information originate** 命令，可以在引入缺省路由时修改其 metric 值。

使用 **ip rip default-information** 命令，可以在创建缺省路由时修改其 metric 值。

3.3.4 避免路由环路

RIP 使用“水平分割”、“毒性逆转”等功能来避免路由环路。

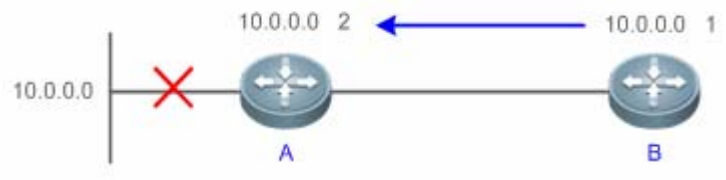
工作原理

路由环路

由于距离矢量算法的固有缺陷，RIP 会发生路由环路。

如下图所示，A 连接网络 10.0.0.0，每隔 30 秒发送一次 Update 报文。因此 B 每 30 秒会收到从 A 发送来的到 10.0.0.0 的路由。如果 A 到 10.0.0.0 的连接中断，到 10.0.0.0 的路由就会从 A 的路由表中消失，下次 A 发出的 Update 报文将不再包含此路由。因为 B 没有收到关于 10.0.0.0 的 Update 报文，在 180 秒内认为到 10.0.0.0 的路由有效，并使用 Update 报文将此路由发送给 A。因为 A 上不存在到 10.0.0.0 的路由，因此将从 B 学到的路由加入路由表。于是，B 认为通过 A 能够到达网络 10.0.0.0，A 认为通过 B 能够到达网络 10.0.0.0，形成路由环路。

图 3-4



水平分割（Split Horizon）

水平分割可以防止路由环路。在接口上启动水平分割功能后，从该接口接收到的路由，不会再从该接口发送出去。

如下图所示，在 A 与 B 相连的接口上启动水平分割后，B 不会再把到 10.0.0.0 路由发回给 A，180 秒后 B 会知道 10.0.0.0 不可达。

图 3-5



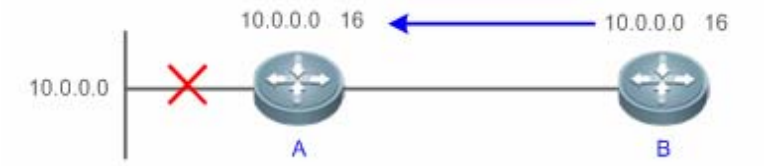
↘ 毒性逆转（Poison Reverse）

毒性逆转也可以防止路由环路。相比水平分割，毒性逆转更加可靠，但会带来更多的协议报文，加重网络拥塞。

在接口上启动毒性逆转后，从该接口接收到的路由，会再从该接口发送出去，且度量值被改为 16（即不可达）。

如下图所示，B 从 A 学习到路由 10.0.0.0 之后，就将该路由的度量设置为 16 定时发回 A。当该路由失效后，B 向 A 通告度量为 16 的 10.0.0.0 将加快该路由信息的清除。

图 3-6



相关配置

↘ 水平分割

缺省情况下，启动水平分割。

使用 **no ip rip split-horizon** 命令，关闭水平分割。

↘ 毒性逆转

缺省情况下，关闭毒性逆转。

使用 **ip rip split-horizon poisoned-reverse** 命令，启动毒性逆转（水平分割自动关闭）。

3.3.5 安全措施

RIP 使用“认证”、“源地址校验”等功能来保障协议安全。

工作原理

↘ 认证

RIPv1 不支持认证，RIPv2 支持认证。

在接口上启动认证功能后，如果认证失败，则相邻设备间无法交换路由信息。认证功能用来阻止非法设备接入 RIP 路由域。

两种认证方式：明文认证和 MD5 认证。

↘ 源地址校验

当运行 RIP 的设备收到更新报文时，会校验报文的源 IP 地址是否与入接口 IP 地址在同一网段。如果不在同一网段，则丢弃该报文。源地址校验功能用来保障 RIP 只在相邻的路由设备间交换路由信息。

- 如果是无编号 IP 地址接口，则不进行源地址校验（不可配置）。
- 如果启动了触发更新，则自动启用源地址校验（不可配置）。
- 如果关闭了水平分割，则自动启用源地址校验（不可配置）。

相关配置

认证

缺省情况下，认证功能关闭。

使用 **ip rip authentication mode text** 命令，在接口上启动明文认证。

使用 **ip rip authentication mode md5** 命令，在接口上启动 MD5 认证。

使用 **ip rip authentication text-password** 命令，在接口上设置明文认证的字符串。

使用 **ip rip authentication key-chain** 命令，在接口上引用 KEY 作为认证的密钥。

源地址校验

缺省情况下，启用源地址校验功能。

使用 **no validate-update-source** 命令，关闭源地址校验功能。

3.3.6 可靠性措施

RIP 使用“与 BFD 联动”、“快速重路由”、“GR”等功能来增强协议可靠性。

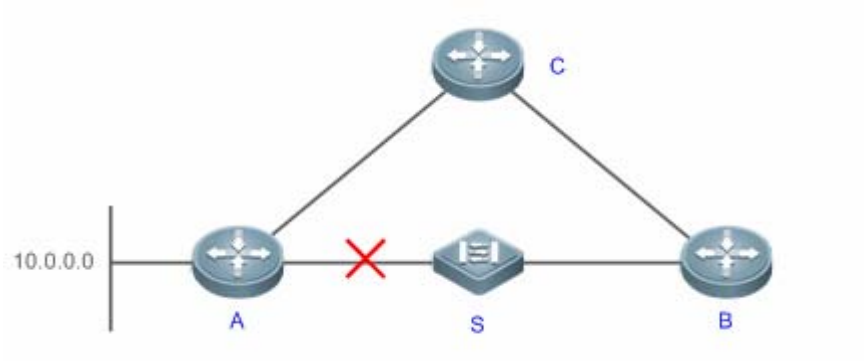
工作原理

与 BFD 联动、快速重路由

当网络中发生链路故障（或设备故障）时，经过此路由传输的报文将会丢失，直到路由重新收敛。

如下图所示，A 与 S 之间的链路通信发生故障后，B 可能需要等待 180 秒才能发现路由（目的网络 10.0.0.0，下一跳 A）失效。而后 B 可能还需要等待 30 秒才能获得来自 C 的路由信息，重新获得路由（目的网络 10.0.0.0，下一跳 C）。流量中断 210 秒。

图 3-7



快速发现路由失效，或者快速切换备份路由，都有助于缩短流量中断时间。

- 在 A、B 之间建立 BFD 会话，并与 RIP 联动。BFD 可以快速检测相邻路由器之间的连通状态。一旦发生链路故障，RIP 在 1 秒内就能发现路由失效。
- 使用“快速重路由”功能，预先在 B 上配置一条备份路由（目的网络 10.0.0.0，下一跳 C），一旦 RIP 发现路由失效，将立即启用备份路由。

GR

GR（Graceful Restart，优雅重启）功能，是为了实现在协议的重新启动过程中数据转发不间断。设备启用 GR 功能后，在 RIP 协议重启过程中，会维持重启前的转发表，并向邻居发送请求报文重新学习路由。在 GR 周期内，RIP 会完成路由的重新收敛。在 GR 周期结束后，RIP 会更新转发表项，并将路由表向邻居进行通告。

相关配置

GR

缺省情况下，未启动 GR 功能。

使用 **graceful-restart** 命令，启动 GR 功能。

3.4 配置详解

配置项	配置建议 & 相关命令	
配置 RIP 基本功能	⚠ 必须配置。用于构建 RIP 路由域。	
	router rip	启动 RIP 路由进程，进入路由进程模式。
	network	在指定地址范围的接口上运行 RIP。
	version	定义 RIP 版本号。
	ip rip split-horizon	在接口上启动水平分割、毒性反转。
	passive-interface	配置被动接口。
控制 RIP 报文交互	⚠ 可选配置。若希望改变 RIP 协议的报文发送、接收的默认机制，需要配置。	
	neighbor	以单播方式向指定的邻居发送 RIP 报文。
	ip rip v2-broadcast	在接口上以广播方式发送 RIPv2 报文。
	ip rip receive enable	允许接口接收 RIP 报文。
	ip rip send enable	允许接口发送 RIP 报文。
	ip rip send version	定义接口发送 RIP 报文的版本号。
	ip rip receive version	定义接口接收 RIP 报文的版本号。
启动触发更新	⚠ 可选配置。	
	ip rip triggered	在接口上启动触发更新。
启动源地址校验	⚠ 可选配置。	
	validate-update-source	启动源地址校验。
启动认证	⚠ 可选配置。仅 RIPv2 支持认证。	
	ip rip authentication mode	在接口上启动认证，设置认证模式。
	ip rip authentication text-password	在接口上配置明文认证的字符串。
	ip rip authentication key-chain	在接口上配置认证密钥串。
启动路由汇聚	⚠ 可选配置。仅 RIPv2 支持路由汇聚。	
	auto-summary	允许 RIP 路由自动汇聚。
	ip rip summary-address	在接口上配置路由汇聚。
启动超网路由	⚠ 可选配置。仅 RIPv2 支持超网路由。	
	ip rip send supernet-routes	在接口上允许通告 RIP 超网路由。
通告缺省路由/外部路由	⚠ 可选配置。	
	ip rip default-information	在接口上向邻居通告缺省路由。
	default-information originate	向邻居通告缺省路由。
	redistribute	路由重分布，向邻居通告外部路由。
设置路由过滤规则	⚠ 可选配置。	
	distribute-list in	对收到的 RIP 路由信息进行过滤。

	distribute-list out	对发出的 RIP 路由信息进行过滤。
修改路由选择参数	⚠ 可选配置。	
	distance	修改 RIP 路由的管理距离。
	offset-list	增加接收或发送的 RIP 路由的 metric。
	default-metric	配置重分布到 RIP 中的外部路由的缺省 metric。
修改时钟	⚠ 可选配置。	
	timers basic	修改 RIP 路由更新、失效、清除的时间。
	output-delay	设置 RIP 路由更新报文的发送延时。
启动 GR	⚠ 可选配置。	
	graceful-restart	启动 GR restarter 能力。

3.4.1 配置RIP基本功能

配置效果

- 在网络中建立一个 RIP 路由域。
- 域内的路由器通过 RIP 获得远端网络的路由。

注意事项

- 必须配置 IPv4 地址。
- 必须启动 IPv4 单播路由。

配置方法

↘ **启动 RIP 路由进程**

- 必须配置。
- 若无特殊要求，应在 RIP 路由域内的每台路由器上配置。

↘ **关联本地网络**

- 必须配置。
- 若无特殊要求，应在 RIP 路由域内的每台路由器上配置。
- 若无特殊要求，RIP 关联的本地网络应覆盖所有三层接口所在网段。

↘ **定义 RIP 版本**

- 如果需要使用 RIPv2 版本的功能（比如：可变长子网掩码、认证。），则必须启动 RIPv2 版本。
- 若无特殊要求，应在每台路由器上定义相同的 RIP 版本。

↘ **启动水平分割、毒性逆转**

- 缺省启动水平分割，关闭毒性逆转。
- 若无特殊要求，应在每个连接广播类型网络（比如：以太网）的接口上启动水平分割。（缺省即可）。
- 若无特殊要求，应在每个连接在点到点类型网络（比如：PPP、HDLC）的接口上启动水平分割。（缺省即可）。
- 建议在连接非广播多路访问类型网络（比如：FR、X.25）的接口上关闭水平分割和毒性逆转，否则可能导致部分设备学不到全部的路由信息。
- 如果连接非广播网络的接口上配置了次 IP 地址，建议关闭水平分割和毒性逆转。

↘ **设置被动接口**

- 如果要在某个 RIP 接口抑制更新报文，则需要设置被动接口。
- 使用被动接口设置 RIP 路由域的边界。被动接口所在网段属于 RIP 路由域，但被动接口上不能发送 RIP 报文。
- RIP 路由域内的需要交互 RIP 路由的接口（比如：路由器互联接口）不能设置为被动接口。

检验方法

- 检查路由器上的路由表，确认通过 RIP 获得远端网络的路由。

相关命令

启动 RIP 路由进程

【命令格式】 **router rip**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 本命令用来创建 RIP 路由进程，并进入路由进程模式。

关联本地网络

【命令格式】 **network** *network-number* [*wildcard*]

【参数说明】 *network-number*：网络号。

wildcard：IP 地址比较比特位，0 表示精确匹配，1 表不做比较。

【命令模式】 路由进程模式

【使用指导】 只有被 **network** 覆盖的接口才能运行 RIP，才能被 RIP 学到直连路由，才能交互 RIP 报文。

配置 **network** 0.0.0.0 255.255.255.255，即可覆盖所有接口。

如果未配置 *wildcard* 参数，默认按照有类地址范围来处理，使落在该有类地址范围内的接口地址参与 RIP 运行。

定义 RIP 版本

【命令格式】 **version** { **1** | **2** }

【参数说明】 **1**：RIPv1。

2：RIPv2。

【命令模式】 全局模式

【使用指导】 此命令对整机生效，定义所有接口上发送和接收的 RIP 报文的版本号。

启动水平分割

【命令格式】 **ip rip split-horizon** [**poisoned-reverse**]

【参数说明】 **poisoned-reverse**：毒性逆转

【命令模式】 接口模式

【使用指导】 启动毒性逆转后，水平分割自动关闭。

配置被动接口

【命令格式】 **passive-interface** { **default** | *interface-type interface-num* }

【参数说明】 **default**：所有接口。

interface-type interface-num：指定接口。

【命令模式】 路由进程模式

【使用指导】 先配置 **passive-interface default**，将所有接口设置为被动接口。

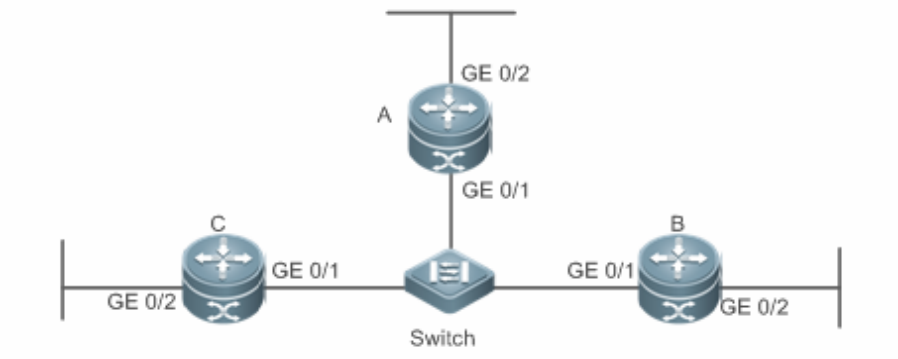
再配置 **no passive-interface** *interface-type interface-num* 取消与域内路由器互联的接口。

配置举例

建立 RIP 路由域

【网络环境】

图 3-8



【注释】 接口 IP 地址：

A： GE0/1 110.11.2.1/24 G E0/2 155.10.1.1/24

B： GE0/1 110.11.2.2/24 GE0/2 196.38.165.1/24

C： GE0/1 110.11.2.3/24 GE0/2 117.102.0.1/16

【配置方法】

- 所有路由器配置接口 IP 地址。
- 所有路由器配置 RIP 基本功能。

A

```
A# configure terminal
A(config)# interface GigabitEthernet 0/1
A(config-if-GigabitEthernet 0/1)# ip address 110.11.2.1 255.255.255.0
A(config-if-GigabitEthernet 0/1)# exit
A(config)# interface GigabitEthernet 0/2
A(config-if-GigabitEthernet 0/2)# ip address 155.10.1.1 255.255.255.0
A(config)# router rip
A(config-router)# version 2
A(config-router)# network 0.0.0.0 255.255.255.255
A(config-router)# passive-interface default
A(config-router)# no passive-interface GigabitEthernet 0/1
```

B

```
B# configure terminal
B(config)# interface GigabitEthernet 0/1
B(config-if-GigabitEthernet 0/1)# ip address 110.11.2.2 255.255.255.0
B(config-if-GigabitEthernet 0/1)# exit
B(config)# interface GigabitEthernet 0/2
B(config-if-GigabitEthernet 0/2)# ip address 196.38.165.1 255.255.255.0
B(config-if-GigabitEthernet 0/2)# exit
B(config)# router rip
B(config-router)# version 2
B(config-router)# network 0.0.0.0 255.255.255.255
B(config-router)# passive-interface default
B(config-router)# no passive-interface GigabitEthernet 0/1
```

C

```
C# configure terminal
C(config)# interface GigabitEthernet 0/1
C(config-if-GigabitEthernet 0/1)# ip address 110.11.2.3 255.255.255.0
C(config-if-GigabitEthernet 0/1)# exit
C(config)# interface GigabitEthernet 0/2
C(config-if-GigabitEthernet 0/2)# ip address 117.102.0.1 255.255.0.0
C(config-if-GigabitEthernet 0/2)# exit
C(config)# router rip
C(config-router)# version 2
C(config-router)#no auto-summary
C(config-router)# network 0.0.0.0 255.255.255.255
C(config-router)# passive-interface default
C(config-router)# no passive-interface GigabitEthernet 0/1
```

【检验方法】 检查 A、B、C 上的 IP 路由表，应看到 RIP 学到了远端网络的路由（蓝色字段）。

A

```
A# show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    110.11.2.0/24 is directly connected, GigabitEthernet 0/1
C    110.11.2.1/32 is local host.
R    117.0.0.0/8 [120/1] via 110.11.2.2, 00:00:47, GigabitEthernet 0/1
C    155.10.1.0/24 is directly connected, GigabitEthernet 0/2
C    155.10.1.1/32 is local host.
C    192.168.217.0/24 is directly connected, VLAN 1
C    192.168.217.233/32 is local host.
R    196.38.165.0/24 [120/1] via 110.11.2.3, 00:19:18, GigabitEthernet 0/1
```

B

```
B# show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default
```

```
Gateway of last resort is no set
C    110.11.2.0/24 is directly connected, GigabitEthernet 0/1
C    110.11.2.2/32 is local host.
R    155.10.0.0/16 [120/1] via 110.11.2.1, 00:15:21, GigabitEthernet 0/1
C    196.38.165.0/24 is directly connected, GigabitEthernet 0/2
C    196.38.165.1/32 is local host.
R    117.0.0.0/8 [120/1] via 110.11.2.2, 00:00:47, GigabitEthernet 0/1
```

C

```
C# show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    110.11.2.0/24 is directly connected, GigabitEthernet 0/1
C    110.11.2.3/32 is local host.
C    117.102.0.0/16 is directly connected, GigabitEthernet 0/2
C    117.102.0.1/32 is local host.
R    155.10.0.0/16 [120/1] via 110.11.2.1, 00:20:55, GigabitEthernet 0/1
R    196.38.165.0/24 [120/1] via 110.11.2.3, 00:19:18, GigabitEthernet 0/1
```

网关产品不支持 BGP,ISIS，配置举例仅作为配置参考，实际请以具体设备配置为准。

常见错误

- 接口上未配置 IPv4 地址。
- 某台设备上没有定义 RIP 版本，或 RIP 版本号与其他路由器不一致。
- **network** 命令配置的地址范围未覆盖某接口。
- **network** 命令参数“IP 地址比较比特位”配置错误。0 表示精确匹配，1 表不做比较。
- 设备互联接口被设置为被动接口。

3.4.2 控制RIP报文交互

配置效果

通过配置，改变 RIP 协议的默认运行机制，人为控制 RIP 报文的交互方式。

包括：

- 允许或禁止某个接口以单播方式向指定的邻居发送 RIP 报文。
- 允许或禁止某个接口以广播而非多播的方式发送 RIP version 2 报文。

- 允许或禁止在某个接口上接收 RIP 报文。
- 允许或禁止在某个接口上发送 RIP 报文。
- 允许或禁止在某个接口上接收特定版本的 RIP 报文。
- 允许或禁止在某个接口上发送特定版本的 RIP 报文。

注意事项

- 必须配置 RIP 基本功能。
- 邻居设备的连接接口上，配置的发送和接收版本需要保持一致。

配置方法

↘ 以单播方式向指定的邻居发送 RIP 路由更新

- 如果不希望接口所连接的设备均能收到路由信息更新，而只希望其中部分设备收到路由信息，则必须配置该功能。
- RIPv1 缺省使用 IP 广播地址（255.255.255.255）通告路由信息，RIPv2 缺省使用组播地址（224.0.0.9）通告路由信息。如果不希望广播网或非广播多路访问网上的全部设备，均可接收到路由信息，可以配置相应接口设置为被动接口，然后只定义某些邻居可以接收到路由信息。该命令不会影响 RIP 信息报文的接收。在接口上以广播方式发送 RIPv2 报文
- 若无特殊要求，应在以单播方式更新路由信息的路由设备上启用该功能。

↘ 在接口上以广播方式发送 RIPv2 报文

- 如果邻居设备不支持以组播方式接收 RIPv2 报文，则必须配置该功能。
- 若无特殊要求，应在每台路由器上，以广播方式发送 RIPv2 报文的接口上配置该功能。

↘ 在接口上允许接收 RIP 报文

- 该功能缺省启用，如果希望某接口不接收 RIP 报文，则应关闭该功能。
- 若无特殊要求，应在每台路由器上，不允许接收 RIP 报文的接口上配置该功能。

↘ 在接口上允许发送 RIP 报文。

- 该功能缺省启用，如果希望某接口不发送 RIP 报文，则应关闭该功能。
- 若无特殊要求，应在每台路由器上，不允许发送 RIP 报文的接口上配置该功能。

↘ 在接口上允许发送指定版本的 RIP 报文

- 如果某接口上允许发送的 RIP 报文版本需要设置为与全局不同，则必须配置该功能。
- 若无特殊要求，应在每台路由器上，需要设置允许发送的 RIP 报文版本的接口上配置该功能。

↘ 在接口上允许接收指定版本的 RIP 报文

- 如果某接口上允许接收的 RIP 报文版本需要设置为与全局不同，则必须配置该功能。
- 若无特殊要求，应在每台路由器上，需要设置允许接收的 RIP 报文版本的接口上配置该功能。

检验方法

打开调试开关 **debug ip rip packet**，查看报文是否发送以及报文的类型。

相关命令

↘ 以单播方式向指定的邻居发送 RIP 路由更新

【命令格式】 **neighbor** *ip-address*

【参数说明】 *ip-address*：邻居的 IP 地址。应该是本地设备直连网络地址。

【命令模式】 路由进程模式

【使用指导】 一般可以先用路由进程配置命令 **passive-interface** 将相应接口设置为被动接口，然后只定义某些邻居可以接收到路由信息。该命令不会影响 RIP 信息报文的接收。设置了 passive 属性的接口，重启后也不会发送请求报

文。

在接口上以广播方式发送 RIPv2 报文

【命令格式】 **ip rip v2-broadcast**

【参数说明】 **-**

【命令模式】 接口模式

【使用指导】 缺省行为取决于 **version** 命令的配置。该命令的配置结果，可以覆盖用 **vesion** 命令的缺省配置。该命令只影响本接口发送 RIP 报文的行为，可以允许该接口同时发送 RIPv1 和 RIPv2 的数据包。此命令配置时不带参数则接收行为取决于 version 的配置。

在接口上允许接收 RIP 报文

【命令格式】 **ip rip receive enable**

【参数说明】 **-**

【命令模式】 接口模式

【使用指导】 如果要禁止某接口接收 RIP 数据包，在该接口的接口模式下使用该命令的 **no** 形式配置。命令仅作用于配置了此命令的接口。可使用该命令的 **default** 形式恢复接口接收 RIP 数据包。

在接口上允许发送 RIP 报文。

【命令格式】 **ip rip send enable**

【参数说明】 **-**

【命令模式】 接口模式

【使用指导】 如果要禁止某接口发送 RIP 数据包，在该接口的接口模式下使用该命令的 **no** 形式配置。命令仅作用于配置了此命令的接口。可使用该命令的 **default** 形式恢复接口发送 RIP 数据包。

在接口上允许发送指定版本的 RIP 报文

【命令格式】 **ip rip send version** [**1**] [**2**]

【参数说明】 **1**：只发送 RIPv1 的数据包。

2：只发送 RIPv2 的数据包。

【命令模式】 接口模式

【使用指导】 缺省行为取决于 **version** 命令的配置。该命令的配置结果，可以覆盖用 **vesion** 命令的缺省配置。该命令只影响本接口发送 RIP 报文的行为，可以允许该接口同时发送 RIPv1 和 RIPv2 的数据包。此命令配置时不带参数则接收行为取决于 version 的配置。

在接口上允许接收指定版本的 RIP 报文

【命令格式】 **ip rip receive version** [**1**] [**2**]

【参数说明】 **1**：只接收 RIPv1 的数据包。

2：只接收 RIPv2 的数据包。

【命令模式】 接口模式

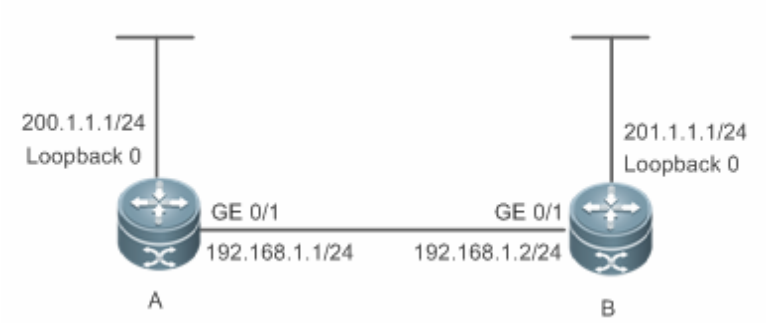
【使用指导】 缺省行为取决于 **version** 命令的配置。该命令的配置结果，可以覆盖用 **vesion** 命令的缺省配置。该命令只影响本接口接收 RIP 报文的行为，可以允许该接口同时接收 RIPv1 和 RIPv2 的数据包。此命令配置时不带参数则接收行为取决于 version 的配置。

配置举例

在接口上禁止发送 RIP 报文

【网络环境】

图 3-9



【配置方法】

- 所有路由器配置接口 IP 地址。略
- 所有路由器配置 RIP 基本功能。略
- 路由器 A 配置禁止 RIP 报文发送。

A

```
A# configure terminal
A(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# no ip rip send enable
```

【检验方法】 路由器 A 打开 **debug ip rip packet send**，报文无法发送。

A

```
A# debug ip rip packet recv
*Nov  4 08:19:31: %RIP-7-DEBUG:  [RIP] Prepare to send BROADCAST response...
*Nov  4 08:19:31: %RIP-7-DEBUG:  [RIP] Building update entries on GigabitEthernet 0/1
*Nov  4 08:19:31: %RIP-7-DEBUG:        117.0.0.0/8 via 0.0.0.0 metric 1 tag 0
*Nov  4 08:19:31: %RIP-7-DEBUG:  [RIP] Interface GigabitEthernet 0/1 is disabled to send RIP packet!
```

常见错误

邻居配置的 RIP 协议版本不一致，无法兼容。

3.4.3 启动触发更新

配置效果

- 开启 RIP 的触发扩展功能，RIP 协议不再定时发送路由更新。

注意事项

- 必须配置 RIP 基本功能。
- 建议同时启用带毒性逆转的水平分割功能，否则可能会出现无效路由信息残留等现象。
- 必须保证连接在同一链路上的每台路由设备都启动了触发更新，否则无法正确交互路由信息。

配置方法

↘ 启动触发更新

- 如果广域网接口为按需链路，则必须启用触发更新功能
- 允许在以下两种情况下启用该功能：A.接口仅存在一个邻居；B.存在多个邻居但是以单播方式交互。
- 建议在广域网接口上（运行 PPP、帧中继、X.25 等链路层协议）启动触发更新，以满足按需链路的要求。
- 如果接口启用了该功能，则无论是否启用源地址校验功能（**validate-update-source**），均执行源地址校验。

- 若若无特殊要求，应在每台路由器上的按需链路上启用触发更新功能。

检验方法

当启用了 RIP 触发扩展功能 ,RIP 协议不再定时发送路由更新 ,只在以下事件发生的时候 RIP 才会向广域网接口发送路由更新：

- 当接收到路由请求报文。
- RIP 路由信息发生变化。
- 当接口状态变化。
- 当路由设备启动。

相关命令

↘ 启动触发更新

【命令格式】 **ip rip triggered** { **retransmit-timer** *timer* | **retransmit-count** *count* }

【参数说明】 **retransmit-timer** *timer*：配置重传 Update Request、Update Response 报文的时间间隔，缺省为 5 秒，取值范围：1-3600

retransmit-count *count*：配置 Update Request、Update Response 报文的最大重传次数，缺省为 36 次，取值范围：1-3600。

【命令模式】 接口模式

【使用指导】 配置 **ip rip triggered** 可以直接启用 RIP 触发扩展功能

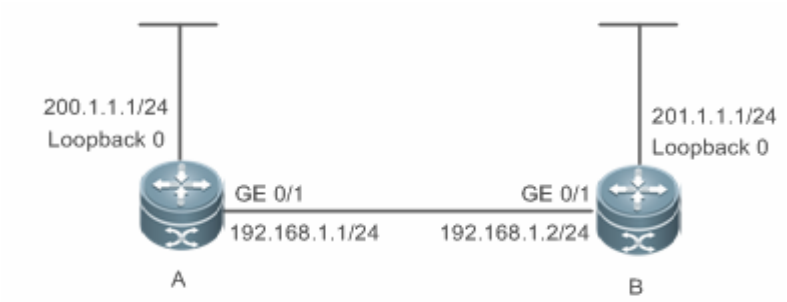
触发扩展功能取消了 RIP 定时更新，因此需要采用确认和重发机制来保证更新报文在广域网上的成功发送和接收。可以使用 **retransmit-timer** 和 **retransmit-count** 指定请求和更新报文的重传间隔和最大重传次数。

配置举例

↘ 启动触发更新

【网络环境】

图 3-10



【配置方法】

- 所有路由器配置接口 IP 地址。略
- 所有路由器配置 RIP 基本功能。略
- 路由器 A 启用 RIP 触发扩展功能，并指定 Update Request、Update Response 报文的重传间隔为 10s，最大重传次数为 18。

A

```
A# configure terminal
A(config)# interface GigabitEthernet 0/1
A(config-if-GigabitEthernet 0/1)# encapsulation ppp
A(config-if-GigabitEthernet 0/1)# ip rip triggered
A(config-if-GigabitEthernet 0/1)# ip rip triggered retransmit-timer 10
```

```
A(config-if-GigabitEthernet 0/1)# ip rip triggered retransmit-count 18
A(config-if-GigabitEthernet 0/1)# ip rip split-horizon poisoned-reverse
A(config)# router rip
A(config-router)# network 192.168.1.0
A(config-router)# network 200.1.1.0
```

B

```
B# configure terminal
B(config)# interface GigabitEthernet 0/1
B(config-if-GigabitEthernet 0/1)# encapsulation ppp
B(config-if-GigabitEthernet 0/1)# ip rip triggered
B(config-if-GigabitEthernet 0/1)# ip rip split-horizon poisoned-reverse
B(config)# router rip
B(config-router)# network 192.168.1.0
B(config-router)# network 201.1.1.0
```

【检验方法】 路由器 A、B 检查 RIP 的数据库，对应的路由属性是永久的。

A

```
A# sho ip rip database
201.1.1.0/24    auto-summary
201.1.1.0/24
    [1] via 192.168.12.2 GigabitEthernet 0/1  06:25    permanent
```

B

```
B# sho ip rip database
200.1.1.0/24    auto-summary
200.1.1.0/24
    [1] via 192.168.12.1 GigabitEthernet 0/1  06:25    permanent
```

常见错误

- 链路两端的 RIP 配置一致，但确启用了该功能。
- 未在同链路所有路由器上启用该功能

3.4.4 启动源地址校验

配置效果

- 对接收到的 RIP 路由更新报文的源地址，进行有效性验证。

注意事项

- 必须配置 RIP 基本功能。

配置方法

↘ 启动源地址校验

- 该功能缺省启用，如果不需要进行源地址校验，则必须配置关闭该功能。
- 在接口上关闭水平分割，将引起 RIP 路由进程执行更新报文源地址验证，不管是否执行了路由进程配置命令 **validate-update-source**。

- 对于 ip unnumbered 接口，RIP 路由进程将不执行更新报文源地址验证，不管是否执行了路由进程配置命令 **validate-update-source**。
- 若无特殊要求，应在不需要进行源地址校验的每台路由器上关闭该功能。

检验方法

只接收来自同一个 IP 子网邻居的路由更新。

相关命令

【命令格式】 **validate-update-source**

【参数说明】 -

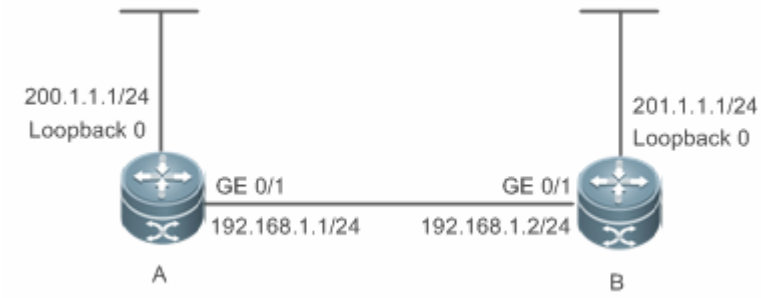
【命令模式】 路由进程模式

【使用指导】 缺省启用更新报文源地址验证。开启后可以对 RIP 路由更新报文的源地址，进行有效性验证。验证的目的是为了保证 RIP 路由进程，只接收来自同一个 IP 子网邻居的路由更新。

配置举例

【网络环境】

图 3-11



【配置方法】

- 所有路由器配置接口 IP 地址。略
- 所有路由器配置 RIP 基本功能。略。
- 所有路由器关闭更新报文源地址验证。

A

```
A# configure terminal
A(config)# router rip
A(config-router)# no validate-update-source
```

B

```
B# configure terminal
B(config)# router rip
B(config-router)# no validate-update-source
```

【检验方法】

- 检查路由器 A 的路由表，已加载 201.1.1.0/24 表项。
- 检查路由器 B 的路由表，已加载 200.1.1.0/24 表项。

A

```
A# show ip route rip
R    201.1.1.0/24 [120/1] via 192.168.2.2, 00:06:11, GigabitEthernet 0/1
```

B

```
A# show ip route rip
R    200.1.1.0/24 [120/1] via 192.168.1.1, 00:06:11, GigabitEthernet 0/1
```

常见错误

-

3.4.5 启动认证

配置效果

- 防止学到非认证、无效路由，避免通告有效路由到非认证设备，保证路由系统的稳定性和抗入侵性。

注意事项

- 必须配置 RIP 基本功能。
- RIPv1 不支持 RIP 数据包认证，只有 RIPv2 支持。

配置方法

启用并指定 RIP 认证所使用的密钥串

- 如果需要启动认证，则必须执行次配置。
- 如果密钥串在接口配置中指定了，请使用 key chain 全局配置命令进行该密钥串的定义，否则将可能导致 RIP 数据包认证失败。
- 若无特殊要求，应在每台需要启动认证的路由器上执行该配置。

定义 RIP 认证模式

- 如果需要启动认证，则必须执行次配置。
- 当配置 RIP 认证时，所有需要直接交换 RIP 路由信息的设备，所配置的 RIP 认证模式必须一致，否则 RIP 数据包交换将失败。
- 如果采用明文认证，但未配置明文认证字符串，或者未配置关联密钥串，此时并不会有认证行为发生。同样，如果采用 MD5 认证，但未配置关联密钥串，也不会有认证行为发生。
- 若无特殊要求，应在每台需要启动认证的路由器上执行该配置。

启用并设置 RIP 明文认证字符串

- 如果需要启动认证，则必须执行次配置。
- 如果要启用 RIP 明文认证功能，可以直接使用本命令配置明文认证字符串，也可以通过关联密钥串获取明文认证字符串，后者优先级高于前者。
- 若无特殊要求，应在每台需要启动认证的路由器上执行该配置。

检验方法

- RIP 明文认证方式只提供有限的安全，因为报文中传送的密码是可直观显示的。
- RIP MD5 加密认证方式则可以提供较高的安全性，因为报文中传送的密码是经过 MD5 算法加密的。
- 配置正确的认证，路由可以正确学习。
- 配置错误的认证，路由无法学习。

相关命令

启动源地址校验

【命令格式】 **ip rip authentication key-chain** *name-of-keychain*

【参数说明】 *name-of-keychain* 密钥串名字，指定 RIP 认证所使用的密钥串。

【命令模式】 接口模式

【使用指导】 所指定的密钥串需要使用 key chain 全局配置命令进行该密钥串的定义。

定义 RIP 认证模式

【命令格式】 **ip rip authentication mode** { **text** | **md5** }

【参数说明】 **text** RIP 认证模式为明文认证。

md5 RIP 认证模式为 MD5 认证。

【命令模式】 接口模式

【使用指导】 所有需要直接交换 RIP 路由信息的设备，所配置的 RIP 认证模式必须一致。

启用并设置 RIP 明文认证字符串

【命令格式】 **ip rip authentication text-password** [**0** | **7**] *password-string*

【参数说明】 **0** 指定密钥以明文显示

7 指定密钥以密文显示

password-string 明文认证的字符串，长度 1 ~ 16 字节。

【命令模式】 接口模式

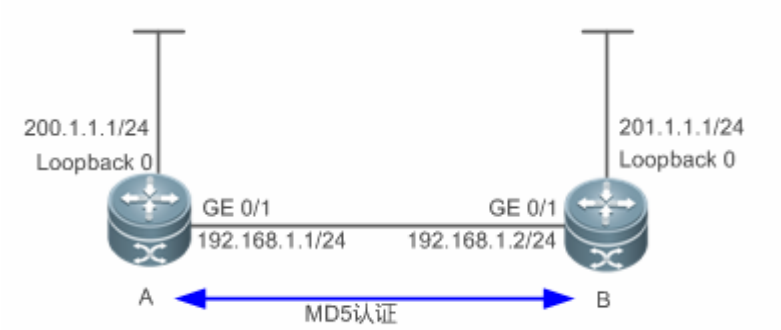
【使用指导】 该命令仅在明文认证模式下生效。

配置举例

配置 RIP 基本功能并且启用 MD5 认证

【配置方法】

图 3-12



【配置方法】

- 所有路由器配置接口 IP 地址。略
- 所有路由器配置 RIP 基本功能。略。
- 所有路由器配置认证类型和 MD5 认证密钥。

A

```
A# configure terminal
A(config)# key chain hello
A(config-keychain)# key 1
A(config-keychain-key)# key-string world
A(config-keychain-key)# exit
A(config-keychain)# exit
A(config)# interface GigabitEthernet 0/1
A(config-if-GigabitEthernet 0/1)# ip rip authentication mode md5
A(config-if-GigabitEthernet 0/1)# ip rip authentication key-chain hello
```

B

```
B# configure terminal
B(config)# key chain hello
B(config-keychain)# key 1
B(config-keychain-key)# key-string world
B(config-keychain-key)# exit
B(config-keychain)# exit
B(config)# interface GigabitEthernet 0/1
B(config-if-GigabitEthernet 0/1)# ip rip authentication mode md5
B(config-if-GigabitEthernet 0/1)# ip rip authentication key-chain hello
```

【检验方法】

- 检查路由器 A 的路由表，已加载 201.1.1.0/24 表项。
- 检查路由器 B 的路由表，已加载 200.1.1.0/24 表项。

A

```
A# show ip route rip
R    201.1.1.0/24 [120/1] via 192.168.1.2, 00:06:11, GigabitEthernet 0/1
```

B

```
A# show ip route rip
R    200.1.1.0/24 [120/1] via 192.168.1.1, 00:06:11, GigabitEthernet 0/1
```

常见错误

- 需要交互 RIP 信息的路由器配置的密码不一致
- 需要交互 RIP 信息的路由器配置的认证方式不同

3.4.6 启动路由汇聚

配置效果

缩小了路由表的规模，提高路由效率，并在一定程度上规避了路由震荡的影响，提高了网络的伸缩性和有效性。

如果有汇总路由存在，在路由表中将看不到包含在汇总路由内的子路由，这样可以大大缩小路由表的规模。

通告汇总路由会比通告单独的每条路由将更有效率，主要有以下因素：1）当查找 RIP 数据库时，汇总路由会得到优先处理；2）当查找 RIP 数据库时，任何子路由将被忽略，减少了处理时间。

注意事项

- 必须配置 RIP 基本功能
- 超网路由范围比有类网络更大，路由自动汇总功能对超网路由无效。
- RIPv1 总是进行自动汇总，如果需要通告明细路由，请设置协议版本为 RIPv2。

配置方法

↘ 启用路由自动汇总

- 该功能缺省启用。
- 如果希望学到具体的子网路由，而不只是汇总后的网络路由，则需要关闭路由自动汇总功能。
- 只有 RIPv2 允许关闭路由自动汇总功能，RIPv1 总是应用路由自动汇总。

↘ 配置 RIP 接口级汇聚

- 如果需要进行有类子网的汇聚，则必须配置该功能。

- 命令 ip rip summary-address 用来在某个指定接口下汇聚一个地址或子网。RIP 自动汇聚到有类网络边界。只有接口汇聚能配置每个有类子网。
- 该命令所配置的汇总范围不能是超类网络，即配置的掩码长度不能小于网络的自然掩码长度。
- 若无特殊要求，应在需要进行有类子网汇聚的路由器上配置该功能。

检验方法

查看对端路由表路由是否有汇聚

相关命令

启用路由汇总总功能

【命令格式】 **auto-summary**

【参数说明】 -

【命令模式】 路由进程模式

【使用指导】 RIPv1 和 RIPv2 中此命令默认开启。

只有配置 RIPv2 时才可以关闭，RIPv1 总是应用。

配置 RIP 接口级汇聚

【命令格式】 **ip rip summary-address** *ip-address ip-network-mask*

【参数说明】 *ip-address* 要被汇聚的 IP 地址

ip-network-mask 为指定 IP 地址进行路由汇聚的子网掩码

【命令模式】 接口模式

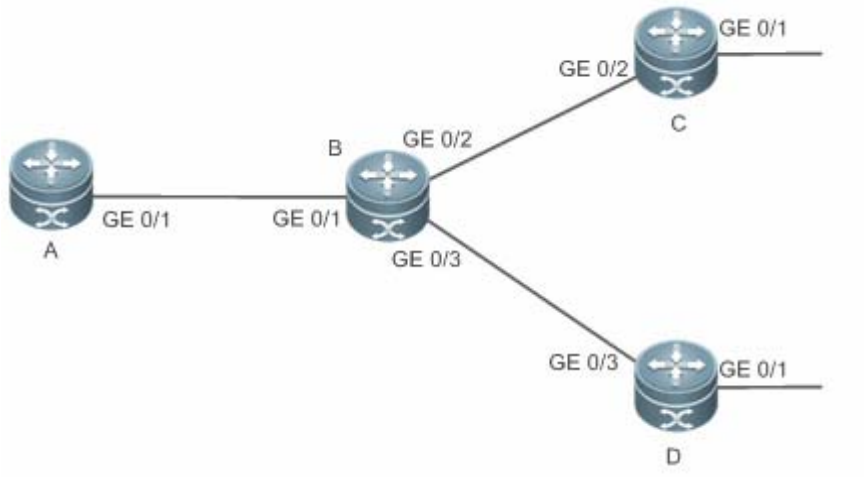
【使用指导】 该用来在某个指定接口下汇聚一个地址或子网

配置举例

配置路由汇聚功能

【网络环境】

图 3-13



【注释】 接口 IP 地址：

A： GE0/1 192.168.1.1

B： GE0/1 192.168.1.2 GE0/2 172.16.2.1 GE0/3 172.16.3.1

C： GE0/2 172.16.2.2 GE0/3 172.16.4.2

D： GE0/2 172.16.3.2 GE0/3 172.16.5.2

【配置方法】
- 所有路由器配置接口 IP 地址。略。
- 所有路由器配置 RIP 基本功能。略。
- 路由器 B 上配置路由汇聚。

```
B# configure terminal
B(config)# interface GigabitEthernet 0/1
B(config-if-GigabitEthernet 0/1)# ip rip summary-address 172.16.0.0 255.255.0.0
B(config)# router rip
B(config-router)# version 2
B(config-router)# no auto-summary
```

【检验方法】 检查路由器 A 路由表，生成 172.16.0.0/16 表项。

```
A# show ip route rip
R 172.16.0.0/16 [120/2] via 192.168.1.2, 00:01:04, GigabitEthernet 0/1
```

常见错误

- 未配置 RIP 基本功能，或配置失败。

3.4.7 启动超网路由

配置效果

- 允许 RIP 在指定接口上发送 RIP 超网路由。

注意事项

- 必须配置 RIP 基本功能。

配置方法

↘ 启用超网络路由

- 当 RIPv1 路由设备监听 RIPv2 路由响应报文时，如果监听到超网路由信息，由于 RIPv1 会将报文中路由信息的子网掩码忽略，从而学习到错误的路由。所以，这种情况下，需要在 RIPv2 路由设备使用该命令的 no 形式禁止在相应接口通告超网路由。命令仅作用于配置了此命令的接口。
- 该命令仅在接口发送 RIPv2 报文时有效，用于控制超网路由的发送。

检验方法

在邻居设备上观察是否学习到超网路由。

相关命令

【命令格式】 **ip rip send supernet-routes**
【参数说明】 -
【命令模式】 接口模式
【使用指导】 缺省允许接口发送 RIP 超网路由

配置举例

关闭超网络路由

【网络环境】

图 3-14



【配置方法】

- 所有路由器配置接口 IP 地址。略
- 所有路由器配置 RIP 基本功能。略。
- 在 B 设备 GigabitEthernet 0/1 接口禁止发送 RIP 的超网路由。

```
B# configure terminal
B(config)# ip route 207.0.0.0 255.0.0.0 Null 0
B(config)# ip route 208.1.1.0 255.255.255.0 Null 0
B(config)# router rip
B(config-router)# redistribute static
B(config)# interface GigabitEthernet 0/1
B(config-if-GigabitEthernet 0/1)# no ip rip send supernet-routes
```

【检验方法】 检查路由器 A 的路由表，只能学习到非超网路由 208.1.1.0/24，不能学习到超网路由 207.0.0.0/8

```
A#show ip route rip
R    208.1.1.0/24 [120/1] via 192.168.1.2, 00:06:11, GigabitEthernet 0/1
```

常见错误

-

3.4.8 通告缺省路由/外部路由

配置效果

- 在 RIP 路由域内引入其他 AS 的单播路由，为 RIP 路由域内的用户提供到其他 AS 的单播路由服务。
- 往 RIP 路由域内注入一条通往其他 AS 的默认路由，为 RIP 路由域内的用户提供到其他 AS 的单播路由服务。

注意事项

- 必须配置 RIP 基本功能。
- 路由重分布，不能将其他协议的缺省路由引入到 RIP 中。

配置方法

向邻居通告缺省路由

如果需要向邻居通告缺省路由，则必须启用此功能。

缺省没有指定产生缺省路由；产生的缺省路由的 metric 值缺省为 1。

如果 RIP 进程能够通过本命令生成缺省路由，那么 RIP 将不再学习邻居通告的缺省路由。

若无特殊要求，应在需要通告缺省路由的路由器上配置该功能。

↘ 在接口上向邻居通告缺省路由

如果需要在指定接口向邻居通告缺省路由，则必须启用此功能。

默认没有缺省路由配置。metric 默认为 1。

在某接口配置了该命令后，就会产生一条缺省路由，并从该接口通告此路由。

若无特殊要求，应在需要通告缺省路由的路由器上配置该功能。

↘ 路由重分布，向邻居通告外部路由

如果需要重分布其它协议的路由，则必须启用此功能。

缺省情况下，

- 若配置重分布 OSPF，则重分布该实例的所有子类型的路由；
- 其他情况下，重分布该类型的所有路由；
- 重分布后的路由的 metric 缺省为 1；
- 缺省不关联 route-map。

路由重分布时，将一个路由协议的量度转换成另一种路由协议的量度是没有必要的，因为不同路由协议所采用的量度计算方法是完全不同的。RIP 量度计算是基于跳数，OSPF 是基于带宽，因此它们计算出来的量度是没有可比性的。但是路由重分布时，又必须要设置一个象征性的量度，否则路由重分布将失败。

若无特殊要求，应在需要重分布路由的路由器上配置该功能。

检验方法

- 在邻居设备上观察 RIP 路由表中是否存在缺省路由。
- 在本机和邻居设备上观察 RIP 路由表中是否存在外部路由（到其他 AS 的路由）。

相关命令

↘ 向邻居通告缺省路由

【命令格式】 **default-information originate** [**always**] [**metric** *metric-value*] [**route-map** *map-name*]

【参数说明】 **always** 该关键字使 RIP 无条件产生缺省路由，不管本地是否存在缺省路由。

metric *metric-value* 缺省路由初始的量度值，*metric-value* 取值范围：1-15。

route-map *map-name* 关联的 route-map 的名字，缺省没有关联 route-map

【命令模式】 路由进程模式

【使用指导】 如果路由设备的路由表中存在缺省路由，RIP 默认不会向外通告缺省路由，需要使用 **default-information originate** 路由进程配置命令进行配置，才能向邻居通告缺省路由。

如果选择 **always** 参数，RIP 路由进程不管是否存在缺省路由，都会向邻居通告一条缺省路由，但该缺省路由并不会在本地路由表中显示。要确认是否产生缺省路由，可以用 **show ip rip database** 观察 RIP 路由信息数据库。

如果要对 RIP 通告缺省路由进行更多的控制，可以使用 **route-map** 参数，如：使用 **set metric** 规则对缺省路由的度量值进行设置。

可以使用 **metric** 参数对通告缺省路由的度量值进行设置，但优先级低于 **route-map** 的 **set metric** 规则；如果没有配置 **metric** 参数，则缺省路由使用 RIP 配置的默认度量值。

对于 **ip default-network** 生成的缺省路由，仍然需要使用 **default-information originate** 命令才能够被引入到 RIP。

↘ 在接口上向邻居通告缺省路由

【命令格式】 **ip rip default-information** { **only** | **originate** } [**metric** *metric-value*]

【参数说明】 **only** 通告缺省路由，不通告其它路由

originate 通告缺省路由，也通告其它路由

metric *metric-value* 缺省路由的量度值，取值范围：1-15

【命令模式】 接口模式

【使用指导】 如果同时配置了接口下的 **ip rip default-information** 和 RIP 进程的 **default-information originate**，则只通告接口配置的缺省路由。

只要有一个接口配置了 **ip rip default-information**，RIP 就不再学习邻居通告的缺省路由。

↘ 路由重分布，向邻居通告外部路由

【命令格式】 **redistribute** {**connected** |**ospf** *process-id* | **static** } [**match** { **internal | external** [**1 | 2**] **| nssa-external** [**1 | 2**] }] [**metric** *metric-value*] [**route-map** *route-map-name*]

【参数说明】 **connected**：从直连路由重分布

ospf *process-id*：从 ospf 重分布，*process-id* 为 ospf 进程号，取值范围 1-65535

static：从静态路由重分布

match：针对重分布 OSPF 路由，用于过滤特定路由进行重分布

metric *metric-value*：设置重分布的路由的 metric，取值范围 1-16

route-map *route-map-name*：设置重分布过滤规则

【命令模式】 路由进程模式

【使用指导】 配置重分布 ospf 路由时，不带 match 参数时，默认允许重分布所有子类型的 ospf 路由； 而后的第一次配置 match 参数作为初始的 match 参数， 重分布时只允许匹配的子类型的路由进行重分布；使用 no 命令恢复 match 参数为默认值。

redistribute 命令的 no 形式配置的规则如下：

1．如果 no 命令指定某些参数，则将这些参数恢复缺省配置；

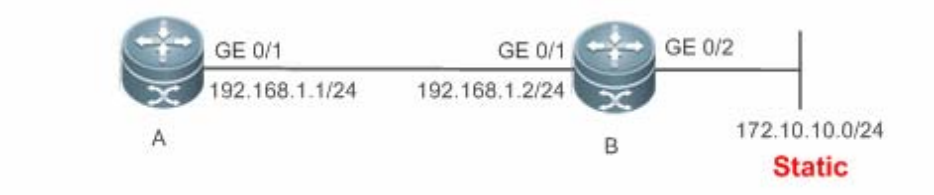
2．如果 no 命令不指定任何参数，则将整个命令删除。

配置举例

↘ 路由重分布，向邻居通告外部路由

【网络环境】

图 3-15



【配置方法】

- 所有路由器配置接口 IP 地址。略。
- 所有路由器配置 RIP 基本功能。略。
- 路由器 B 配置重分布静态路由。

B

```
B# configure terminal
B(config)# router rip
B(config-router)# redistribute static
```

【检验方法】 路由器 A 上检查路由表：加载了 172.10.10.0/24 表项。

```
A# show ip route rip
R    172.10.10.0/24 [120/1] via 192.168.1.2, 00:06:11, GigabitEthernet 0/1
```

常见错误

-

3.4.9 设置路由过滤规则

配置效果

- 被过滤掉的路由不能被加载到路由表或被传播给邻居，从而阻止网络内的用户访问指定的目的网络。

注意事项

- 必须配置 RIP 基本功能。
- 对于发出的过滤规则，必须先配置重分布路由，针对重分布路由实现过滤。

配置方法

对收到的 RIP 路由信息进行过滤

- 如果需要对接收的路由信息进行过滤，则必须配置该功能。
- 为了拒绝接收某些指定路由，可以通过配置路由分布控制列表，对所有接收到的路由更新报文进行处理。如果没指定接口，就对所有的接口接收的路由更新报文进行处理。
- 若无特殊要求，应在需要过滤的路由器上配置该功能。

对发出的 RIP 路由信息进行过滤

- 如果需要对发送的重分布路由信息进行过滤，则必须配置该功能。
- 如果该命令不跟任何可选参数，路由更新通告控制对所有接口起作用；如果跟接口选项，路由更新通告控制只对指定接口起作用；如果跟其它路由进程参数，则路由更新通告控制只对指定路由进程起作用。
- 若无特殊要求，应在需要过滤的路由器上配置该功能。

检验方法

- 通过 **show ip route rip** 确认被过滤的路由没有加载到路由表

相关命令

对收到的 RIP 路由信息进行过滤

【命令格式】 **distribute-list** { [*access-list-number* | *name*] | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*] } **in** [*interface-type interface-number*]

【参数说明】 *access-list-number* | *name*：指定访问列表。只有访问列表允许的路由，才可以被接收。

prefix *prefix-list-name*：使用前缀列表来过滤路由。

gateway *prefix-list-name*：使用前缀列表来过滤路由的源。

interface-type interface-number：该分布列表，只应用在指定接口。

【命令模式】 路由进程模式

【使用指导】 -

对发出的 RIP 路由信息进行过滤

【命令格式】 **distribute-list** { [*access-list-number* | *name*] | **prefix** *prefix-list-name* } **out** [*interface* | [**connected | ospf** *process-id* **|rip | static**]]

【参数说明】 *access-list-number* | *name*：指定访问列表。只有访问列表允许的路由，才可以被发送。

prefix *prefix-list-name*：使用前缀列表来过滤路由。

Interface：路由更新通告控制只应用在指定接口。

connected：路由更新通告控制只应用在从直连引入的路由。

ospf *process-id*：路由更新通告控制只应用在从 ospf 引入的路由，*process-id* 指定具体某个 ospf 实例。

rip：路由更新通告控制只应用在 rip 路由。

static：路由更新通告控制只应用在从静态引入的路由。

【命令模式】 路由进程模式

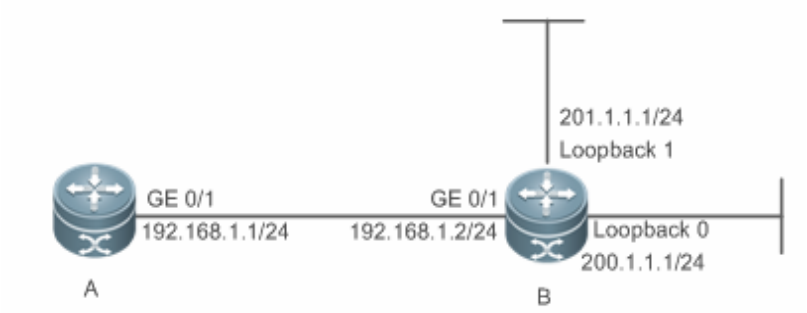
【使用指导】 -

配置举例

对收到的 RIP 路由信息进行过滤

【网络环境】

图 3-16



【配置方法】

- 所有路由器配置接口 IP 地址。略。
- 所有路由器配置 RIP 基本功能。略。
- RIP 对从 GigabitEthernet 0/1 端口接收的路由进行控制处理，只允许接收 200.1.1.0 的路由。

A

```
A# configure terminal
A(config)# router rip
A(config-router)# distribute-list 10 in GigabitEthernet 0/1
A(config-router)# no auto-summary
A(config)# access-list 10 permit 200.1.1.0 0.0.0.255
```

【检验方法】 检查路由器 A 的路由表，只有 200.1.1.0/24 表项。

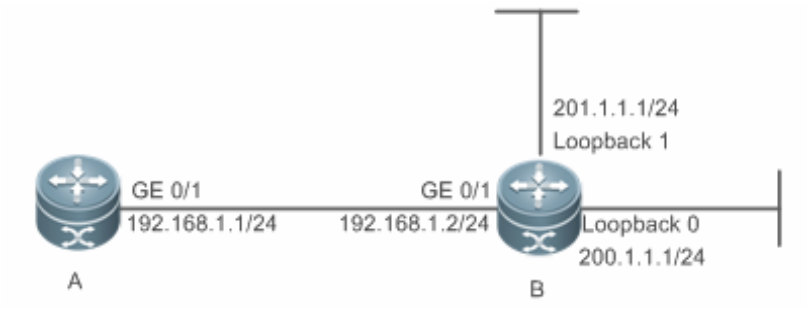
A

```
A# show ip route rip
R    200.1.1.0/24 [120/1] via 192.168.1.2, 00:06:11, GigabitEthernet 0/1
```

对发出的 RIP 路由信息进行过滤

【网络环境】

图 3-17



【配置方法】

- 所有路由器配置接口 IP 地址。略。
- 所有路由器配置 RIP 基本功能。略。
- RIP 路由进程只对外通告 200.1.1.0/24 路由。

B

```
B# configure terminal
B(config)# router rip
B(config-router)# redistribute connected
B(config-router)# distribute-list 10 out
B(config-router)# version 2
B(config)# access-list 10 permit 200.1.1.0 0.0.0.255
```

【检验方法】 查看 A 路由表，只有 200.1.1.0 网段的路由。

A

```
A# show ip route rip
R    200.1.1.0/24 [120/1] via 192.168.1.2, 00:06:11, GigabitEthernet 0/1
```

常见配置错误

- 列表的过滤规则错误，导致过滤失败

3.4.10 修改路由选择参数

配置效果

- 改变 RIP 路由，使流量经过或避开某些节点。
- 改变路由器选择各类路由的顺序，使 RIP 路由的优先级提高或降低。

注意事项

- 必须配置 RIP 基本功能。

配置方法

↘ 修改 RIP 路由的管理距离

- 可选配置。
- 在同时运行多种单播路由协议的路由器上，若希望改变 RIP 路由的优先级，必须配置。

↘ 增加接受或发送的 RIP 路由的 metric

- 可选配置。

- 若无特殊要求，应在需要调整路由 metric 的路由器上配置该功能。

配置重分布到 RIP 中的路由的缺省 metric

- 可选配置。
- 若无特殊要求，应在引入域外路由的 AS 边界路由器上配置。

检验方法

使用 show ip rip 查看当前所配置的 distance 值。可以使用 show ip rip data 查看重分发进来的路由的度量，确定配置是否生效。

相关命令

修改 RIP 路由的管理距离

【命令格式】 **distance** *distance* [*ip-address wildcard*]

【参数说明】 *distance*：设置 RIP 路由管理距离，1-255 之间的整数

ip-address：路由来源 IP 地址前缀

wildcard：定义 IP 地址比较比特位，0 表示精确匹配，1 表不做比较。

【命令模式】 路由进程模式

【使用指导】 使用该命令设置 RIP 路由的管理距离。

增加接受或发送的 RIP 路由的 metric

【命令格式】 **offset-list** { *access-list-number* | *name* } { **in** | **out** } *offset* [*interface-type interface-number*]

【参数说明】 *access-list-number* | *name*：指定访问列表

In：应用 acl 对接收的路由的 metric 进行修改

out：应用 acl 对发送的路由的 metric 进行修改

offset：修改的 metric 的变动值，取值范围：0-16

interface-type：应用 acl 到指定接口

interface-number：指定接口编号

【命令模式】 路由进程模式

【使用指导】 增加接收或发送的 RIP 路由的 metric 值，若指定接口则针对对应接口，若未指定则全局成立。

配置重分布到 RIP 中的路由的缺省 metric

【命令格式】 **default-metric** *metric-value*

【参数说明】 *metric-value：*缺省的量度值，有效值为 1 到 16。如果 *metric-value* 值大于等于 16，RGOS 将认为该路由不可达。

【命令模式】 路由进程模式

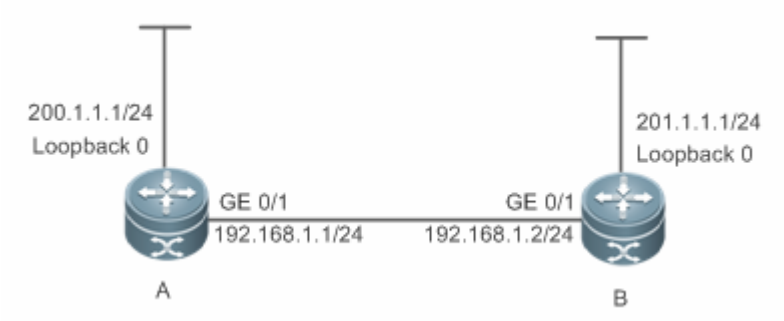
【使用指导】 该命令需要与路由协议配置命令 **redistribute** 配合使用。

配置举例

增加接受或发送的 RIP 路由的 metric

【网络环境】

图 3-18



【配置方法】

- 所有路由器配置接口 IP 地址。略。
- 所有路由器配置 RIP 基本功能。略。
- 在 acl 7 指定的范围内的 RIP 路由才会对 metric 增加 7。
- 对学习的在 acl 8 指定的范围内的 RIP 路由才会对 metric 增加 7。

A

```
A# configure terminal
A(config)# access-list 7 permit host 200.1.1.0
A(config)# access-list 8 permit host 201.1.1.0
A(config)# router rip
A(config-router)# offset-list 7 out 7
A(config-router)# offset-list 8 in 7
```

【检验方法】 检查路由器 A、B 的路由表，RIP 路由的 metric 为 8。

A

```
A# show ip route rip
R    201.1.1.0/24 [120/8] via 192.168.1.2, 00:06:11, GigabitEthernet 0/1
```

B

```
B# show ip route rip
R    200.1.1.0/24 [120/8] via 192.168.1.1, 00:06:11, GigabitEthernet 0/1
```

常见错误

-

3.4.11 修改时钟

配置效果

- 改变控制协议运行的定时器，加快或延缓协议状态的改变，加快或延缓事件的发生。

注意事项

- 必须配置 RIP 基本功能。
- 改变协议控制参数，有可能导致协议运行失败。不建议执行此项配置。

配置方法

↘ 修改 RIP 路由更新、失效、清除的时间

如果需要调整 RIP 时钟，则必须配置该功能。

通过调整时钟，可能会加快路由协议的收敛时间以及故障恢复时间。连接在同一网络上的设备，RIP 时钟值一定要一致。一般不建议对 RIP 时钟进行调整，除非有明确的需求。

在低速链路上将时钟设得很短，将会带来一定风险，因为大量的更新报文会消耗带宽。一般只有在以太网或者 2Mbps 以上的线路，可以将时钟设置得短一点，这样可以缩短网络路由的收敛时间。

若无特殊要求，应在需要修改 RIP 时钟的路由器上配置该功能。

↘ 设置 RIP 路由更新报文的发送延时

如果需要调整 RIP 更新报文的发送延时，则必须配置该功能。

使用 output-delay 命令增加高速设备的报文间的发送延时，使低速设备能够接收处理全部更新报文。

若无特殊要求，应在需要调整发送延时的路由器上配置该功能。

检验方法

可以用 **show ip rip** 命令进行查看当前的 RIP 时钟参数设置。

相关命令

↘ 修改 RIP 路由更新、失效、清除的时间

【命令格式】 **timers basic** *update invalid flush*

【参数说明】 *update*：路由更新时间，以秒计。update 定义了设备发送路由更新报文的周期，每接收到更新报文，invalid 和 flush 时钟就复位。缺省每隔 30 秒发送一次路由更新报文。

invalid：路由无效时间，以秒计，从最近一次有效更新报文开始计时。invalid 定义了路由表中路由因没有更新而变为无效的时间。路由无效时间至少应该为路由更新时间的三倍，如果在路由无效时间内没有接收到任何更新报文，相应的路由将变为无效，进入 invalid 状态；invalid 时间内接收到路由更新报文，时钟会复位。Invalid 缺省时间为 180 秒。

flush：路由清除时间，以秒计，从 RIP 路由进入 invalid 状态开始计时。flush 时间到期，处于 invalid 状态路由将被清除出路由表。Flush 缺省时间为 120 秒。

【命令模式】 路由进程模式

【使用指导】 缺省情况下，更新时间为 30 秒，无效时间为 180 秒，清除时间为 120 秒。

↘ 设置 RIP 路由更新报文的发送延时

【命令格式】 **output-delay** *delay*

【参数说明】 *delay：*设置报文间发送延时，单位为毫秒，范围是<8-50>。

【命令模式】 接口模式

【使用指导】 正常情况下，RIP 更新报文大小为 512 字节，可以包含 25 条路由，如果更新的路由条目大于 25，就会通过多个路由更新报文发送，正常情况下是尽可能快的发送。

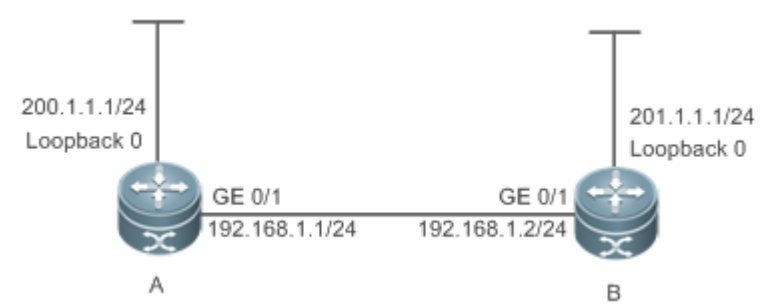
但是，当高速设备向低速设备发送大量更新报文时，低速设备可能来不急处理全部的更新报文，造成路由信息丢失。此时，需要使用 **output-delay** 命令增加高速设备的报文间的发送延时，使低速设备能够接收处理全部更新报文。

配置举例

↘ 设置 RIP 路由更新报文的发送延时

【网络环境】

图 3-19



【配置方法】

- 所有路由器配置接口 IP 地址。略。
- 所有路由器配置 RIP 基本功能。略。
- 路由器 A 配置更新报文的延时时间。

A

```
A# configure terminal
A(config)# router rip
A(config-router)# output-delay 30
```

【检验方法】 抓包检查路由器 A 的更新报文发送时间，与原来相比延时了 30 毫秒。

常见错误

连接在同一网络上的设备，RIP 时钟值设置不一致。

3.4.12 启动GR

配置效果

- 分布式路由器从主板切换到备板过程中，用户数据流量始终保持转发不断流
- RIP 协议进程重新启动期间，用户数据流量始终保持转发不断流

注意事项

- 必须配置 RIP 基本功能。
- 需要保证 GR 重启周期至少为 2 个 RIP 路由更新周期。
- 在 RIP 优雅重启运行过程中，请保持网络环境的稳定。

配置方法

↘ 启动 GR restarter 能力

如果需要 RIP 进行优雅重启以保证在热备切换过程中的数据转发，则必须启用该功能

优雅重启功能基于 RIP 实例配置，不同的 RIP 实例可以根据情况配置不同的参数。

优雅重启周期为执行 RIP 重启到 RIP 完成优雅重启的最长时间，在这段时间内转发表维持为重启前的转发表，并执行 RIP 路由恢复工作，使 RIP 恢复到协议重启前的状态。当重启周期到期后，RIP 将退出 GR 状态，执行普通的 RIP 操作。

若无特殊要求，应在每台需要优雅重启的路由器上启用该功能

检验方法

- 使用 show ip rip 可以查看 GR 是否开启和所配置的时间

- 执行热备切换，数据转发保持不中断。

相关命令

启动 GR restarter 能力

【命令格式】 **graceful-restart** [**grace-period** *grace-period*]

【参数说明】 **graceful-restart**：启用优雅重启(Graceful Restart，GR)功能.

grace-period：显式配置 *grace-period*

grace-period：用户设置的 GR 重启周期。取值范围 1-1800 秒。

缺省值为更新时间的 2 倍和 60s 两者中的较小者。

【命令模式】 路由进程模式

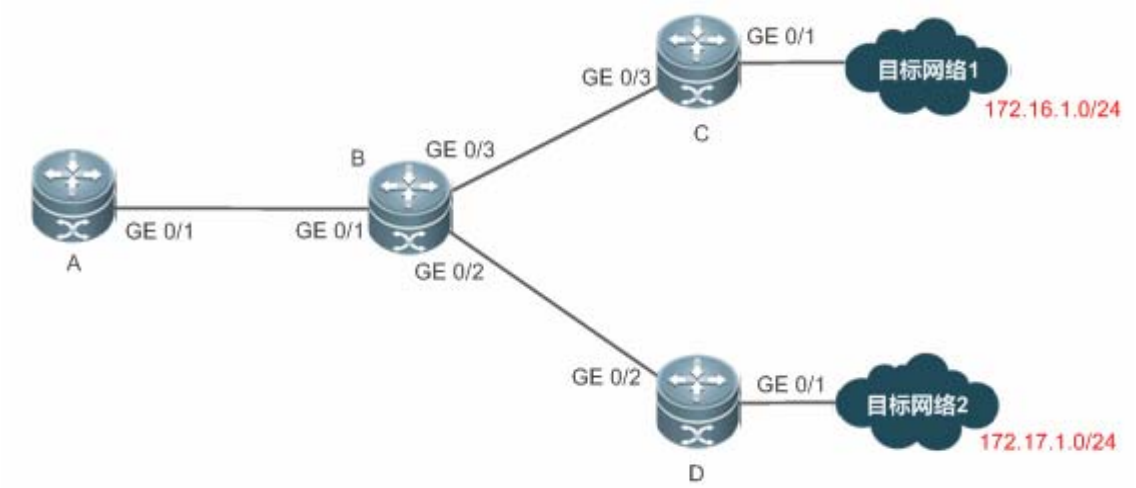
【使用指导】 **graceful-restart grace-period** 允许用户显式修改重启周期。注意，要能够保证在 RIP 路由无效时间之内完成 GR 重启，并经过一次 RIP 路由更新周期。如果该值设置不当，可能无法保证优雅重启过程中数据转发的不间断，典型的情况如：如重启周期大于邻居的路由无效时间，在路由无效时间到期时还没有完成 GR，没有重新向邻居通告路由，邻居的路由在无效时间到期后就停止转发，导致网络的数据转发中断。所以除非有明确的需求，否则不建议调整优雅重启周期。如果需要调整，请结合 **timers basic** 命令的配置，确定重启周期的值大于路由更新时间，且小于路由无效时间。

配置举例

启动 GR restarter 能力

【网络环境】

图 3-20



【注释】 接口 IP 地址：

A：GE 0/1 192.168.1.1

B：GE 0/1 192.168.1.1 GE 0/2 192.168.2.1 GE 0/3 192.168.3.1

C：GE 0/1 192.168.4.2 GE 0/3 192.168.3.2

D：GE 0/1 192.168.5.2 GE 0/2 192.168.2.2

【配置方法】

- 所有路由器配置接口 IP 地址。略。
- 所有路由器配置 RIP 基本功能。略。
- 路由器 B 开启 GR 功能。

```
B# configure terminal
B(config)# router rip
B(config-router)# graceful-restart grace-period 90
```

【检验方法】
- 路由器 B 执行热备切换，期间在路由器 A 上查看到目标网络 1 和目标网络 2 的路由表保持不变。
- 路由器 B 执行热备切换，期间在路由器 A 上 ping 目标网络 1 不间断。

常见错误

-

3.5 监视与维护

查看运行情况

作用	命令
查看 RIP 进程的基本信息	**show ip rip**
查看 RIP 路由表	**show ip rip database** [*network-number network-mask*] [**count**]
查看 RIP 重分布的外部路由信息	**show ip rip external** [**connected** | **ospf** *process-id* | **static**]
查看 RIP 接口信息	**show ip rip interface** [*interface-type interface-number*]
查看 RIP 邻居信息	**show ip rip peer** [*ip-address*]

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 RIP 进程运行过程中发生的事件	**debug ip rip event**
查看与 NSM 进程的交互信息	**debug ip rip nsm**
查看 RIP 的收发包信息	**debug ip rip packet** [**interface** *interface-type interface-number* | **recv** | **send**]
查看 RIP 的 GR 过程中的信息	**debug ip rip restart**
查看 RIP 进程路由变化信息	**debug ip rip route**

4 RIPng

4.1 概述

RIPng（RIP next generation，下一代 RIP）是一种单播路由协议，应用于 IPv6 网络。运行 RIPng 的路由器之间通过交换路由信息，获得到达远程网络的路由。

RIPng 属于 IGP (Interior Gateway Protocol，内部网关协议)，只能在 AS 内运行，适用于规模较小的网络（不大于 16 跳）。

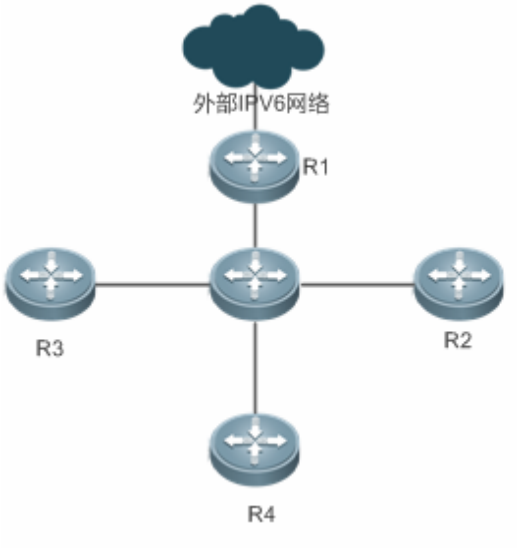
协议规范

- RFC2080：定义了 RIPng

4.2 典型应用

RIPng 一般用于一些小型的网络当中，如小公司的办公网络等。

如下图，该公司组建了一个 IPV6 网络，该网络中所有的路由器都能运行 IPV6 的协议。虽然该网络比较小，但如果纯由人工来维护，也需要一定的工作量。这时候就可以通过配置 RIPng，来自适应该小型网络拓扑的变化，减少工作量。



4.3 功能详解

基本概念

IGP、EGP

内部网关协议（Interior Gateway Protocol，简称 IGP）：在一个自治系统内部运行。比如：RIPng。

外部网关协议（Exterior Gateway Protocol，简称 EGP）：运行于不同自治系统之间。比如：BGP。

功能特性

功能特性	说明

RIPng 与 RIP	RIPng 是 RIPv2 在 IPv6 上的扩展，两者在功能和配置上非常相似。
交换路由信息	通过在设备间交换路由信息，RIPng 可以自动获得远程网络的路由，并保持实时更新。
路由算法	RIPng 是一种基于距离矢量（Distance-Vector）算法的协议，运用矢量叠加的方法来计算路由信息。
避免路由环路	RIPng 使用“水平分割”和“毒性逆转”等功能来避免路由环路。

4.3.1 RIPng与RIP

RIP 应用于 IPv4 网络，包括 RIPv2、RIPv2 两个版本。

RIPng 是 RIPv2 在 IPv6 上的扩展，两者在功能和配置上非常相似。

工作原理

RIPv2

RIPv2 以组播方式发送 RIPv2 报文，组播地址 224.0.0.9，UDP 端口号 520。RIPv2 能够识别子网掩码。

RIPng

RIPng 以组播方式发送 RIPng 报文，组播地址 FF02::9，源地址 FE80::/10，UDP 端口号 521。RIPng 报文能够识别子网掩码。

本章详细介绍了 RIPng 的功能和配置。关于 RIPv2 的详细内容，请参见“RIP”。

相关配置

启动 RIPng 进程

缺省情况下，未启动 RIPng 进程。

使用 **ipv6 router rip** 命令，启动 RIPng 进程。

必须在设备上启动 RIPng 进程，否则与 RIPng 相关的任何功能都无法生效。

在接口上运行 RIPng

缺省情况下，接口上未运行 RIPng。

使用 **ipv6 rip enable** 命令，在接口上运行 RIPng。

在接口上运行 RIPng 后，接口上才能交互 RIPng 报文，RIPng 才能学到其直连网段的路由。

限制接口上的报文交互

缺省情况下，运行 RIPng 的接口允许接收、发送 RIPng 报文。

使用 **passive-interface** 命令，禁止接口发送 RIPng 报文。

4.3.2 交换路由信息

与静态路由相比，动态路由协议的一大优点：通过在设备间交换路由信息，设备可以自动获得远程网络的路由，并保持实时更新。

工作原理

初始化

路由器启动 RIPng 后，会向相邻路由器发送请求报文（Request message），请求全部路由信息（即路由表）。邻居收到请求报文后，回送包含本地路由表的响应报文（Response message）。路由器收到响应报文后，更新本地路由表，同时向相邻路由器发送更新报文（Update message），通告路由更新信息。相邻路由器收到更新报文后，更新本地路由表，并向其它相邻路由器发送更新报文。在一连串的更新通告后，各路由器都能获得并保持最新的路由信息。

定时更新

缺省情况下，RIPng 启用定时更新。相邻路由器之间每隔 30 秒（update timer）进行完全的路由信息交换（即将整个路由表发送给邻居）。

对于每条非本地路由，如果 180 秒内（invalid timer）得不到刷新，则 metric 值改为 16（不可达）；如果随后的 120 秒内（flush timer）得不到刷新，则从路由表中删除。

缺省路由

在路由表中，目的网络为::/0 的路由为缺省路由。

可以从邻居学到缺省路由，也可以向邻居发送缺省路由。

路由重分布

对于 RIPng 来说，其他类型的路由（比如直连路由、静态路由、其他路由协议的路由）为外部路由。

可以将设备上的外部路由（不包括缺省路由）重分布到 RIPng 中，通告给邻居。

路由过滤

可以通过设置过滤规则，限制相邻设备间交换的路由信息。只有被过滤规则允许的路由信息，才能被发送或接收。

相关配置

RIPng 时钟

缺省情况下，update timer 为 30 秒，invalid timer 为 180 秒，flush 为 120 秒。

使用 **timers basic** 命令，修改 RIPng 时钟的超时时间。

增加超时时间，有助于减少路由振荡。缩短超时时间，有助于加快路由收敛。

相邻设备上的 RIPng 时钟值必须一致。若没有特殊要求，不建议修改 RIPng 时钟。

缺省路由

使用 **ipv6 rip default-information** 命令，在接口上向邻居通告缺省路由。

路由重分布

使用 **redistribute** 命令，将外部路由（不包括缺省路由）重分布到 RIPng，通告给邻居。

路由过滤

使用 **distribute-list out** 命令，设置过滤规则，限制设备发出的路由信息。

使用 **distribute-list in** 命令，设置过滤规则，限制设备接收的路由信息。

4.3.3 路由算法

RIPng 是一种基于距离矢量（Distance-Vector）算法的协议，运用矢量叠加的方法来计算路由信息。

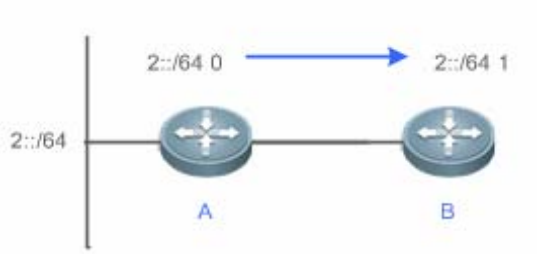
工作原理

距离矢量算法

RIPng 是一种基于距离矢量算法的协议。“距离矢量”就是将一条路由信息看作一个由目的网络和距离（metric）组成的矢量。路由器从邻居处获得一条路由信息，并在这条路由信息上叠加从自己到这个邻居的距离矢量，从而形成自己的路由信息。

RIPng 使用跳数（Hop Count）来衡量到达目的网络的距离（metric）。缺省情况下，路由器到与它直接相连网络的跳数为 0，通过一个路由器可达的网络的跳数为 1，其余依此类推。也就是说，metric 等于从本网络到达目的网络间的路由器数量。为限制收敛时间，RIPng 规定 metric 取 0～15 之间的整数，大于或等于 16 表示目的网络或主机不可达。由于这个限制，使得 RIPng 不可能在大型网络中得到应用。

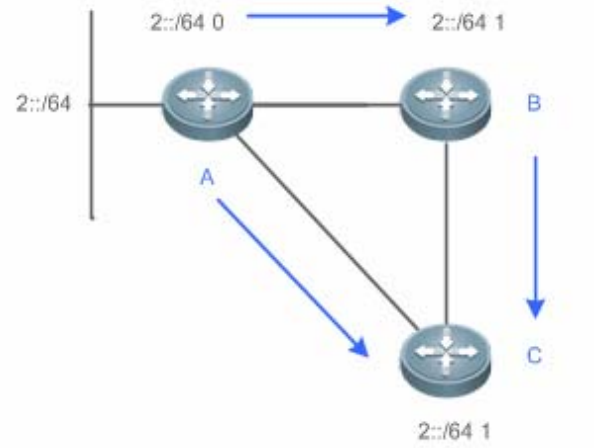
如下图所示，A 连接网络 2::/64。B 从 A 处获得路由信息（2::/64，0），则在此基础上叠加 metric1，得到自己的路由信息（2::/64，1），下一跳指向 A。



选择最优路由

RIPng 选择最优路由的原则：如果路由器获得了多条到达同一目的网络的路由信息，优先选用 metric 值较小的路由信息。

如下图所示，A 连接网络 2::/64。C 从 A 处获得路由信息（2::/64，0），从 B 处获得路由信息（2::/64，1），则 C 会选用来自 A 的路由信息，并在此基础上叠加 metric1，得到自己的路由信息（2::/64，1），下一跳指向 A。



当路由器上存在多种来源的路由时，优先选用 distance 值较小的路由。

路由来源	缺省 distance 值
直连网络	0
静态路由	1
OSPF 路由	110
ISIS 路由	115
RIPng 路由	120
不可达路由	255

相关配置

修改 distance 值

缺省情况下，RIPng 路由的 distance 值为 120。

使用 **distance** 命令，修改 RIPng 路由的 distance 值。

修改 metric 值

对于设备主动发现的 RIPng 路由，缺省 metric 值等于从本地到目的网络的跳数，接口上的 metric 叠加值为 1。

对于人为配置的 RIPng 路由（缺省路由、重分布路由），缺省 metric 值为 1。

使用 **ipv6 rip metric-offset** 命令，修改接口上的 metric 叠加值。

使用 **default-metric** 命令，修改外部路由（路由重分布）的缺省 metric 值。

使用 **redistribute** 命令，在通告外部路由（路由重分布）时修改其 metric 值。
使用 **ipv6 rip default-information** 命令，在通告缺省路由时修改其 metric 值。

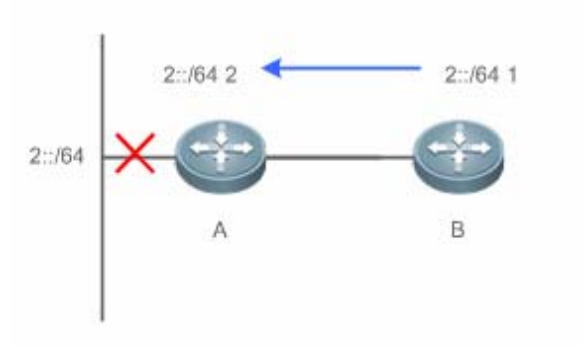
4.3.4 避免路由环路

RIPng 使用“水平分割”、“毒性逆转”等功能来避免路由环路。

工作原理

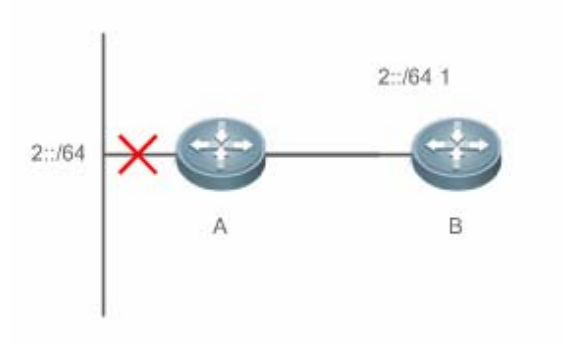
↘ 路由环路

由于距离矢量算法的固有缺陷，RIPng 会发生路由环路。
如下图所示，A 连接网络 2::/64，每隔 30 秒发送一次 Update 报文。因此 B 每 30 秒会收到从 A 发送来的到 2::/64 的路由。如果 A 到 2::/64 的连接中断，到 2::/64 的路由就会从 A 的路由表中消失，下次 A 发出的 Update 报文将不再包含此路由。因为 B 没有收到关于 2::/64 的 Update 报文，在 180 秒内认为到 2::/64 的路由有效，并使用 Update 报文将此路由发送给 A。因为 A 上不存在到 2::/64 的路由，因此将从 B 学到的路由加入路由表。于是，B 认为通过 A 能够到达网络 2::/64，A 认为通过 B 能够到达网络 2::/64，形成路由环路。



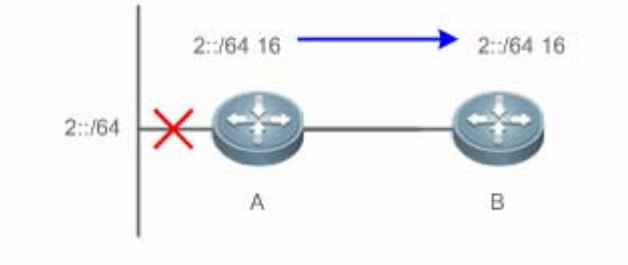
↘ 水平分割（Split Horizon）

水平分割可以防止路由环路。启动水平分割功能后，从该接口接收到的路由，不会再从该接口发送出去。
如下图所示，在 B 上启动水平分割后，B 不会再把到 2::/64 路由发回给 A，180 秒后 B 会知道 2::/64 不可达。



↘ 毒性逆转（Poison Reverse）

毒性逆转也可以防止路由环路。相比水平分割，毒性逆转更加可靠，但会带来更多的协议报文，加重网络拥塞。
在接口上启动毒性逆转后，从该接口接收到的路由，会再从该接口发送出去，且度量值被改为 16（即不可达）。
如下图所示，在 A 上启动毒性逆转后，如果 A 发现到 2::/64 的连接中断，不会将到 2::/64 的路由删除，而是将其跳数改为 16，通过 Update 报文发布出去。当 B 收到 Update 报文时会知道 2::/64 不可达。



相关配置

↘ 水平分割

缺省情况下，启动水平分割。

使用 **no split-horizon** 命令，关闭水平分割。

↘ 毒性逆转

缺省情况下，关闭毒性逆转。

使用 **split-horizon poisoned-reverse** 命令，启动毒性逆转（水平分割自动关闭）。

4.4 产品说明

NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE 支持 RIPNG 功能 ;NBR800G、NBR950G、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR108G-P、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1500G、NBR2000G 不支持 RIPNG 功能。

4.5 配置详解

配置项	& 相关命令	
配置 RIPng 基本功能	⚠ 必须配置。用于构建 RIPng 路由域。	
	ipv6 router rip	启动 RIPng 路由进程，进入路由进程模式。
	ipv6 rip enable	在接口上运行 RIPng。
	split-horizon	启动水平分割、毒性反转。
	passive-interface	配置被动接口。
通告缺省路由/外部路由	⚠ 可选配置。	
	ipv6 rip default-information	在接口上向邻居通告缺省路由。
	redistribute	路由重分布，向邻居通告外部路由。
设置路由过滤规则	⚠ 可选配置。	
	distribute-list in	对收到的 RIPng 路由信息进行过滤。
	distribute-list out	对发出的 RIPng 路由信息进行过滤。
修改路由选择参数	⚠ 可选配置。	
	distance	修改 RIPng 路由的管理距离。
	ipv6 rip metric-offset	在接口上修改 metric 叠加值。

	default-metric	配置路由重分布的缺省 metric。
修改时钟	可选配置。	
	timers	修改 RIPng 路由更新、失效、清除的时间。
启动认证功能	可选配置。	
	authentication	在进程上启动认证
	encryption	在进程上启动加密认证
	ipv6 rip authentication	在接口上启动认证
	ipv6 rip encryption	在接口上启动加密认证

4.5.1 配置RIPng基本功能

配置效果

- 在网络中建立一个 RIPng 路由域。
- 域内的路由器通过 RIPng 获得远端网络的路由。

注意事项

- 必须配置 IPv6 地址。
- 必须启动 IPv6 单播路由。

配置方法

启动 RIPng 路由进程

- 必须配置。
- 若无特殊要求，应在 RIPng 路由域内的每台路由器上配置。

在接口上运行 RIPng

- 必须配置。
- 若无特殊要求，应在 RIPng 路由域内的每个路由器互联接口上配置。

启动水平分割、毒性逆转

- 缺省启动水平分割，关闭毒性逆转。
- 若无特殊要求，应在每个连接广播类型网络（比如：以太网）的接口上启动水平分割。（缺省即可）。
- 若无特殊要求，应在每个连接在点到点类型网络（比如：PPP、HDLC）的接口上启动水平分割。（缺省即可）。
- 建议在连接非广播多路访问类型网络（比如：FR、X.25）的接口上关闭水平分割和毒性逆转，否则可能导致部分设备学不到全部的路由信息。
- 如果连接非广播网络的接口上配置了次 IP 地址，建议关闭水平分割和毒性逆转。

设置被动接口

- 建议配置。
- 使用被动接口设置 RIPng 路由域的边界。被动接口所在网段属于 RIPng 路由域，但被动接口上不能发送 RIPng 报文。
- RIPng 路由域内的需要交互 RIPng 路由的接口（比如：路由器互联接口）不能设置为被动接口。

检验方法

- 检查路由器上的路由表，确认通过 RIPng 获得远端网络的路由。

相关命令

启动 RIPng 路由进程

【命令格式】 **ipv6 router rip**

【参数说明】 **-**

【命令模式】 全局模式

【使用指导】 本命令用来创建 RIPng 路由进程，并进入路由进程模式。

在接口上运行 RIPng

【命令格式】 **ipv6 rip enable**

【参数说明】 **-**

【命令模式】 接口模式

【使用指导】 与 RIPv2 不同。RIPv2 是在路由进程模式下配置 **network** 命令，定义一个 IP 地址范围，则在 IP 地址属于此范围的接口上自动运行 RIP。

启动水平分割

【命令格式】 **split-horizon** [**poisoned-reverse**]

【参数说明】 **poisoned-reverse**：带毒性逆转功能

【命令模式】 路由进程模式

【使用指导】 使用 **show ipv6 rip** 命令检查是否启用了水平分割。

与 RIPv2 不同。RIPv2 是在接口模式下配置。

配置被动接口

【命令格式】 **passive-interface** { **default** | *interface-type interface-num* }

【参数说明】 **default**：所有接口。

interface-type interface-num：指定接口。

【命令模式】 路由进程模式

【使用指导】 先配置 **passive-interface default**，将所有接口设置为被动接口。

再配置 **no passive-interface** *interface-type interface-num* 取消与域内路由器互联的接口。

查看 IP 路由表

【命令格式】 **show ipv6 route**

【参数说明】 **-**

【命令模式】 特权模式、全局模式

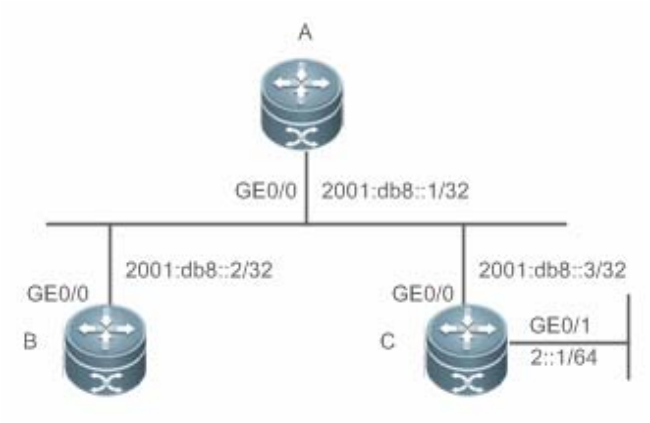
【使用指导】 查看是否存在由 RIPng 学到的远端网络的路由信息。

配置举例

建立 RIPng 路由域

【网络环境】

图 4-1



【配置方法】

- 所有的路由器配置 IPv6 地址。
- 所有的路由器使能 RIPng。

A

```
A# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
A(config)# ipv6 router rip
A(config-router)# exit
A(config)# interface GigabitEthernet 0/0
A(config-if-GigabitEthernet 0/0)# ipv6 address 2001:db8::1/32
A(config-if-GigabitEthernet 0/0)# ipv6 rip enable
```

B

```
B# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
B(config)# ipv6 router rip
B(config-router)# exit
B(config)# interface GigabitEthernet 0/0
B(config-if-GigabitEthernet 0/0)# ipv6 address 2001:db8::2/32
B(config-if-GigabitEthernet 0/0)# ipv6 rip enable
```

C

```
C# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
C(config)# ipv6 router rip
C(config-router)# exit
C(config)# interface GigabitEthernet 0/0
C(config-if-GigabitEthernet 0/0)#
C(config-if-GigabitEthernet 0/0)# ipv6 address 2001:db8::3/32
C(config-if-GigabitEthernet 0/0)# ipv6 rip enable
C(config)# interface GigabitEthernet 0/1
C(config-if-GigabitEthernet 0/1)# ipv6 address 2::1/64
C(config-if-GigabitEthernet 0/1)# ipv6 rip enable
```

【检验方法】 检查路由器 A、B、C 的路由表，应看到 RIPng 学到了远端网络的路由。

A

```
A# show ipv6 route

IPv6 routing table name - Default - 6 entries
Codes:  C - Connected, L - Local, S - Static
        R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - Inter area

R       2::/64 [120/2] via FE80::2D0:F8FF:FEFB:D521, GigabitEthernet 0/0
C       2001:DB8::/32 via GigabitEthernet 0/0, directly connected
L       2001:DB8::1/128 via GigabitEthernet 0/0, local host
C       FE80::/10 via ::1, Null0
C       FE80::/64 via GigabitEthernet 0/0, directly connected
L       FE80::2D0:F8FF:FEFB:E7CE/128 via GigabitEthernet 0/0, local host
```

B

```
B# show ipv6 route

IPv6 routing table name - Default - 6 entries
Codes:  C - Connected, L - Local, S - Static
        R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - Inter area

R       2::/64 [120/2] via FE80::2D0:F8FF:FEFB:D521, GigabitEthernet 0/0
C       2001:DB8::/32 via GigabitEthernet 0/0, directly connected
L       2001:DB8::2/128 via GigabitEthernet 0/0, local host
C       FE80::/64 via GigabitEthernet 0/0, directly connected
L       FE80::2D0:F8FF:FEFB:C9BA/128 via GigabitEthernet 0/0, local host
```

C

```
Ruijie# show ipv6 route

IPv6 routing table name - Default - 9 entries
Codes:  C - Connected, L - Local, S - Static
        R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - Inter area
```

```
C       2::/64 via GigabitEthernet 0/1, directly connected
L       2::2/128 via GigabitEthernet 0/1, local host
C       2001:DB8::/32 via GigabitEthernet 0/0, directly connected
L       2001:DB8::3/128 via GigabitEthernet 0/0, local host
C       FE80::/10 via ::1, Null0
C       FE80::/64 via GigabitEthernet 0/0, directly connected
L       FE80::2D0:F8FF:FEFB:D521/128 via GigabitEthernet 0/0, local host
C       FE80::/64 via GigabitEthernet 0/1, directly connected
L       FE80::2D0:F8FF:FEFB:D521/128 via GigabitEthernet 0/1, local host
```

常见错误

- 接口上未配置 IPv6 地址。
- 设备互联接口被设置为被动接口。

4.5.2 通告缺省路由/外部路由

配置效果

- 在 RIPng 路由域内引入其他 AS 的单播路由，为 RIP 路由域内的用户提供到其他 AS 的单播路由服务。
- 往 RIPng 路由域内注入一条通往其他 AS 的默认路由，为 RIPng 路由域内的用户提供到其他 AS 的单播路由服务。

注意事项

- 必须配置 RIPng 基本功能。

配置方法

配置重分发外部路由

- 可选配置。
- 若在 AS 边界路由器上需要引入 RIPng 域外路由时，需要配置。

配置生成缺省路由

- 可选配置。
- 若在 AS 边界路由器上需要引入默认路由，使得 RIPng 域内访问其他 AS 域默认通过该边界路由器，则需要配置。

检验方法

- 在非 AS 边界路由器上通过 **show ipv6 route rip** 检查域外路由、缺省路由已经加载

相关命令

在接口上向邻居通告缺省路由

【命令格式】 **ipv6 rip default-information** { **only**|**originate** } [**metric** *metric-value*]

【参数说明】 **only**: 通告 ipv6 默认路由，不通告其它路由

originate: 通告 ipv6 默认路由，也通告其它路由

metric *metric-value*: 默认路由的度量值，取值范围：1-15。默认为 1。

【命令模式】 接口模式

【使用指导】 在接口上配置了该命令后，将从该接口往外通告一条 IPv6 缺省路由，但该路由本身不添加到设备的路由转发表和 RIPng 的路由数据库。

为避免形成路由环路，一旦有接口配置了该命令，RIPng 将拒绝接收邻居通告的缺省路由更新。

↘ 路由重分布，向邻居通告外部路由

【命令格式】 **redistribute** { **bgp | connected | isis** [*area-tag*] **| ospf** *process-id* **| static** } [**metric** *metric-value* | **route-map** *route-map-name*]

【参数说明】 **bgp**：从 BGP 重分布

Connected：从直连路由重分布

isis [*area-tag*]：从 ISIS 重分布，*area-tag* 表示 ISIS 进程号

ospf *process-id*：从 OSPF 重分布，*process-id* 表示 OSPF 进程号，取值范围 1-65535

static：从静态路由重分布

metric *metric-value*：设置被重分布到 RIPng 域的路径的度量值

route-map *route-map-name*：设置重分布路径过滤

【命令模式】 路由进程模式

【使用指导】 路由重分布时，将一个路由协议的度量转换成另一种路由协议的度量是没有必要的，因为不同路由协议所采用的度量计算方法是完全不同的。RIP 度量计算是基于跳数，OSPF 是基于带宽，因此它们计算出来的度量是没有可比性的。

配置举例

【网络环境】



【配置方法】

- 所有路由器配置接口 IPv6 地址。略。
- 所有路由器配置 RIPNG 基本功能。略。
- 在路由器 B 上重分发静态路由。
- 在路由器 A 的接口 GE0/1 配置通告缺省路由。

A

```
A# configure terminal
A(config)# interface GigabitEthernet 0/1
A(config-if-GigabitEthernet 0/1)# ipv6 rip default-information originate
```

B

```
B# configure terminal
B(config)# ipv6 router rip
B(config-router)# redistribute static
```

【检验方法】

- 检查路由器 A，B 路由表，路由器 A 能学习到 3001:10:10::/64，路由器 B 学习到默认路由::/0。

A

```
A# show ipv6 route rip

IPv6 routing table name - Default - 17 entries
Codes:  C - Connected, L - Local, S - Static
        R - RIP, O - OSPF, B - BGP, I - IS-IS
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - Inter area
R      3001:10:10::/64 [120/2] via FE80::2D0:F8FF:FE22:334A, GigabitEthernet 0/1
```

B

```
B# show ipv6 route rip

IPv6 routing table name - Default - 17 entries
Codes:  C - Connected, L - Local, S - Static
        R - RIP, O - OSPF, B - BGP, I - IS-IS
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - Inter area
R      ::/0 [120/2] via FE80::21A:A9FF:FE41:5B06, GigabitEthernet 0/1
```

常见错误

-

4.5.3 设置路由过滤规则

配置效果

- 被过滤掉的路由不能被加载到路由表或被传播给邻居，从而阻止网络内的用户访问指定的目的网络。

注意事项

- 必须配置 RIPng 基本功能。

配置方法

↘ 对收到的 RIP 路由信息进行过滤

- 为了拒绝接收某些指定路由，可以通过配置路由分布控制列表，对所有接收到的路由更新报文进行处理。如果没指定接口，就对所有的接口接收的路由更新报文进行处理。

↘ 对发出的 RIP 路由信息进行过滤

- 如果该命令不跟任何可选参数，路由更新通告控制对所有接口起作用；如果跟接口选项，路由更新通告控制只对指定接口起作用；如果跟其它路由进程参数，则路由更新通告控制只对指定路由进程起作用。

检验方法

- 通过 **show ipv6 route rip** 检查被过滤的路由没有加载到路由表。

相关命令

【命令格式】 **distribute-list prefix-list** *prefix-list-name* { **in** | **out** } [*interface-type interface-name*]

【参数说明】 **prefix-list** *prefix-list-name:* **prefix-list** 的名字，使用前缀列表来过滤路由。

in | **out:** 指定该分布列表是对接收或发送更新路由使用过滤

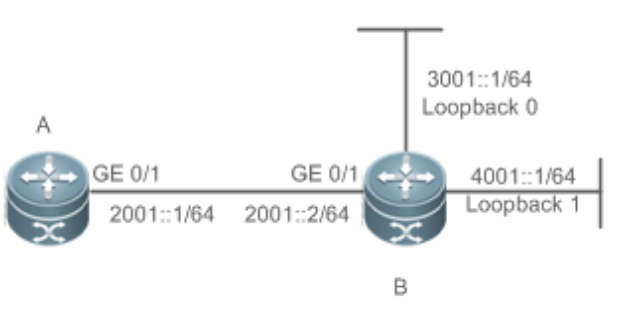
interface-type interface-name: 该分布列表只应用在指定接口

【命令模式】 路由进程模式

【使用指导】 --

配置举例

【网络环境】



【配置方法】

- 所有路由器配置接口 IPv6 地址。略。
- 所有路由器配置 RIPNG 基本功能。略。
- 路由器 A 配置路由过滤。

A

```
A# configure terminal
A(config)# ipv6 prefix-list hello permit 4001::/64
A(config)# ipv6 router rip
A(config-router)# distribute-list prefix-list hello in
```

【检验方法】

- 检查路由器 A 只能学习到 4001::/64 的路由。

A

```
A# show ipv6 route rip
IPv6 routing table name - Default - 17 entries
Codes:  C - Connected, L - Local, S - Static
        R - RIP, O - OSPF, B - BGP, I - IS-IS
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - Inter area
R      4001::/64 [120/2] via FE80::2D0:F8FF:FE22:334A, GigabitEthernet 0/1
```

常见配置错误

-

4.5.4 修改路由选择参数

配置效果

- 改变 RIPng 路由，使流量经过或避开某些节点。
- 改变路由器选择各类路由的顺序，使 RIPng 路由的优先级提高或降低。

注意事项

- 必须配置 RIPng 基本功能。

配置方法

↘ **修改 RIPng 路由的管理距离**

- 可选配置。
- 在同时运行多种单播路由协议的路由器上，若希望改变 RIPng 路由的优先级，必须配置。

↘ **在接口上修改 metric 叠加值**

- 可选配置。
- 若无特殊要求，应在需要调整路由 metric 的路由器上配置该功能。

↘ **配置重分布到 RIPng 中的路由的缺省 metric**

- 可选配置。
- 若无特殊要求，应在引入域外路由的 AS 边界路由器上配置。

检验方法

- 使用 **show ipv6 rip** 查看 RIPng 路由的管理距离。
- 使用 **show ipv6 rip data** 查看重分发进来的域外路由的度量。

相关命令

↘ **修改 RIPng 路由的管理距离**

【命令格式】 **distance** *distance*

【参数说明】 *distance*：设置 RIPng 路由管理距离，允许设置<1-254>之间的整数

【命令模式】 路由进程模式

【使用指导】 为 RIPng 路由设置管理距离，用此命令。

↘ **在接口上修改 metric 叠加值**

【命令格式】 **ipv6 rip metric-offset** *value*

【参数说明】 *value*: 接口度量值，取值范围：1-16

【命令模式】 路由进程模式

【使用指导】 在路由加入路由表前，路由的 metric 要加上接口上设置的度量值。所以可以通过设置接口的度量值影响路由的使用。

↘ **配置重分布到 RIPng 中的路由的缺省 metric**

【命令格式】 **default-metric** *metric*

【参数说明】 *metric*：缺省的度量值，有效值为 1 到 16。如果 metric 值大于等于 16，RGOS 将认为该路由不可达。

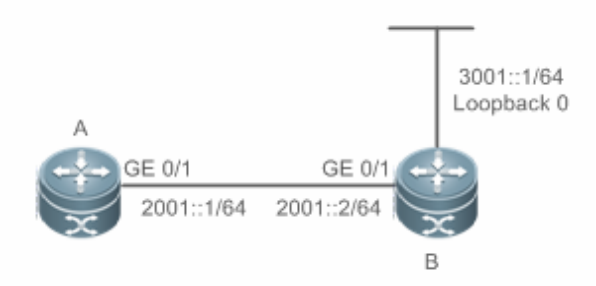
【命令模式】 全局模式

【使用指导】 如果重分布一个路由协议进程时，没有明确定义度量值，RIPng 将使用 **default-metric** 定义的度量值；如果有明确定义度量值，该值将覆盖 **default-metric** 定义的度量值。不配置该命令则 **default-metric** 值缺省为 1。

配置举例

↘ 修改 RIPng 路由的管理距离

【网络环境】



【配置方法】

- 所有路由器配置接口 IPv6 地址。略。
- 所有路由器配置 RIPNG 基本功能。略。
- 路由器 A 配置 RIPNG 路由管理距离为 160。

```
A# configure terminal
A(config)# ipv6 router rip
A(config-router)# distance 160
```

【检验方法】

- 检查路由器 A 的 RIPng 路由的管理距离为 160。

```
A# show ipv6 route rip | in 3001::/64
R      3001::/64 [160/2] via FE80::2D0:F8FF:FE22:334A, GigabitEthernet 0/1
```

常见错误

-

4.5.5 修改时钟

配置效果

- 改变控制协议运行的定时器，加快或延缓协议状态的改变，加快或延缓事件的发生。

注意事项

- 必须配置 RIPng 基本功能。
- 改变协议控制参数，有可能导致协议运行失败。不建议执行此项配置。

配置方法

↘ 修改 RIP 路由更新、失效、清除的时间

- 必须配置。
- 若无特殊要求，应在需要修改 RIPng 时钟的路由器上配置。

检验方法

- 通过 **show ipv6 rip** 查看时钟参数。

相关命令

【命令格式】 **timers** *update invalid flush*

【参数说明】 *Update*：路由更新时间，以秒计。update 定义了设备发送路由更新报文的周期，每接收到更新报文，invalid 和 flush 时钟就复位。缺省每隔 30 秒发送一次路由更新报文。

Invalid：路由无效时间，以秒计，从最近一次有效更新报文开始计时。invalid 定义了路由表中路由因没有更新而变为无效的时间。路由无效时间至少应该为路由更新时间的三倍，如果在路由无效时间内没有接收到任何更新报文，相应的路由将变为无效，进入 invalid 状态；invalid 时间内接收到路由更新报文，时钟会复位。Invalid 缺省时间为 180 秒。

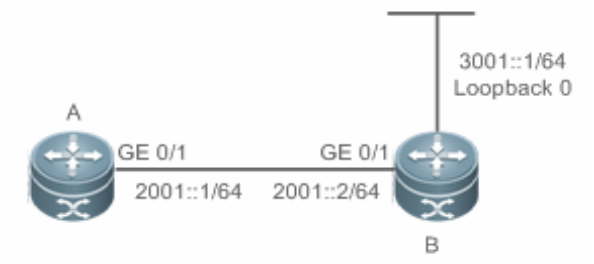
Flush：路由清除时间，以秒计，从 RIPng 路由进入 invalid 状态开始计时。flush 时间到期，处于 invalid 状态路由将被清除出路由表。flush 缺省时间为 120 秒。

【命令模式】 路由进程模式

【使用指导】 缺省情况下，更新时间为 30 秒，无效时间为 180 秒，清除时间为 120 秒。

配置举例

【网络环境】



【配置方法】

- 所有路由器配置接口 IPv6 地址。略。
- 所有路由器配置 RIPNG 基本功能。略。
- 路由器 A 配置路由更新、失效、清除时间。

B

```
B# configure terminal
B(config)# ipv6 router rip
B(config-router)# timers 10 30 90
```

【检验方法】

- 路由器 B 检查 RIPng 对应的定时器。

B

```
B# show ipv6 rip
Routing Protocol is "RIPng"
  Sending updates every 10 seconds with +/-50%, next due in 12 seconds
  Timeout after 30 seconds, garbage collect after 90 seconds
  Outgoing update filter list for all interface is: not set
  Incoming update filter list for all interface is: not set
  Default redistribution metric is 1
  Default distance is 120
  Redistribution:
      Redistributing protocol connected
  Default version control:  send version 1, receive version 1
  Interface                 Send   Recv
      GigabitEthernet 0/1   1      1
  Routing Information Sources:
      Gateway: fe80::2d0:f8ff:fe22:334a  Distance: 120
      Last Update: 00:00:02   Bad Packets: 0   Bad Routes: 0
```

常见错误

- 连接在同一网络上的设备，RIPng 时钟值设置的不一致，导致路由学习异常。

4.6 监视与维持

查看运行情况

作用	命令
查看 RIPng 进程	**show ipv6 rip**
查看 RIPng 路由表	**show ipv6 rip database**

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 RIPng 调试开关	**debug ipv6 rip** [interface *interface-type interface-num* | nsm | restart | event [ipsec]]

5 OSPFv2

5.1 概述

OSPF（Open Shortest Path First，开放式最短路径优先协议）是一种内部网关协议（Interior Gateway Protocol，简称 IGP），应用在 AS（Autonomous System，自治系统）内部，使路由器获得远端网络的路由。

OSPF 具备如下特点：

- 适用范围广：适用于更大规模的网络（最大可支持几百台路由器）。
- 快速收敛：一旦网络拓扑发生变化，路由器之间能够快速通告信息，更新路由。
- 无自环：路由器之间仅同步链路状态信息，每台路由器独立计算路由，不会生成自环。
- 区域划分：将一个大的路由域划分为多个较小的区域，可以节省系统资源和网络带宽，使路由稳定可靠。
- 路由分类：将路由分为多种类型区别对待，支持灵活的控制策略。
- 等价路由：支持等价路由。
- 支持认证：支持报文认证，保障协议交互过程的安全。
- 组播发送：支持以组播地址发送协议报文，可以避免干扰无关者、节省系统资源。

本章使用“路由器”指代支持路由功能的网络设备。这些网络设备可以是三层交换机、路由器、防火墙等。

若无特殊说明，下文以“OSPF”来指代“OSPFVersion 2”。

协议规范

RFC2328	This memo documents version 2 of the OSPFprotocol. OSPF is a link-state routing protocol.
RFC 2370	This memo defines enh ancements to the OSPFprotocol to support a ne w class of lin k-stateadvertisements (LSA) called Opaque LSAs.Opaque LSAs provide a generalized mechanismto allow for the future extensibility of OSPF.
RFC3137	This memo describes a backward-compatibletechnique that may be used by OSPF (OpenShortest Path First) implementations to advertiseunavailability to forward transit traffic or to lowerthe preference level for the paths through such arouter.
RFC3623	This memo documents an enhancement to theOSPF routing protocol, whereby an OSPF routercan stay on the forwarding path even as its OSPFsoftware is restarted.
RFC3630	This document describes extensions to the OSPFprotocol version 2 to support intra-area TrafficEngineering (TE), using Opaque Link StateAdvertisements.
RFC3682	The use of a packet's Time to Live (T TL) (IPv4)or Hop Limit (IPv6) to protect a protocol st ackfrom CPU-utilization based attacks has beenproposed in many settings.

RFC3906	This document describes h ow conventional hop-by-hop link-state routing protocols i nteract withnew Traffic Engineering capabilities to createInterior Gateway Protocol (IGP) shortcuts.
RFC4576	This document specifies the nece ssary procedure,using one of the options bits in the LSA (Link StateAdvertisements) to in dicate that an LSA hasalready been forwarded by a PE and should beignored by any other PEs that see it.
RFC4577	This document extends that specification byallowing the routing protocol on the PE/CEinterface to be the Open Shortest Path First(OSPF) protocol.
RFC4750	This memo defines a portio n of the ManagementInforma tion Base (MIB) for use with networkmanagement protocols in TCP/IP-based internets.In particular, it defines objects for managingversion 2 of the Open Shortest Path First RoutingProtocol. Version 2 of the OSPF protocol isspecific to the IPv4 address family.

5.2 典型应用

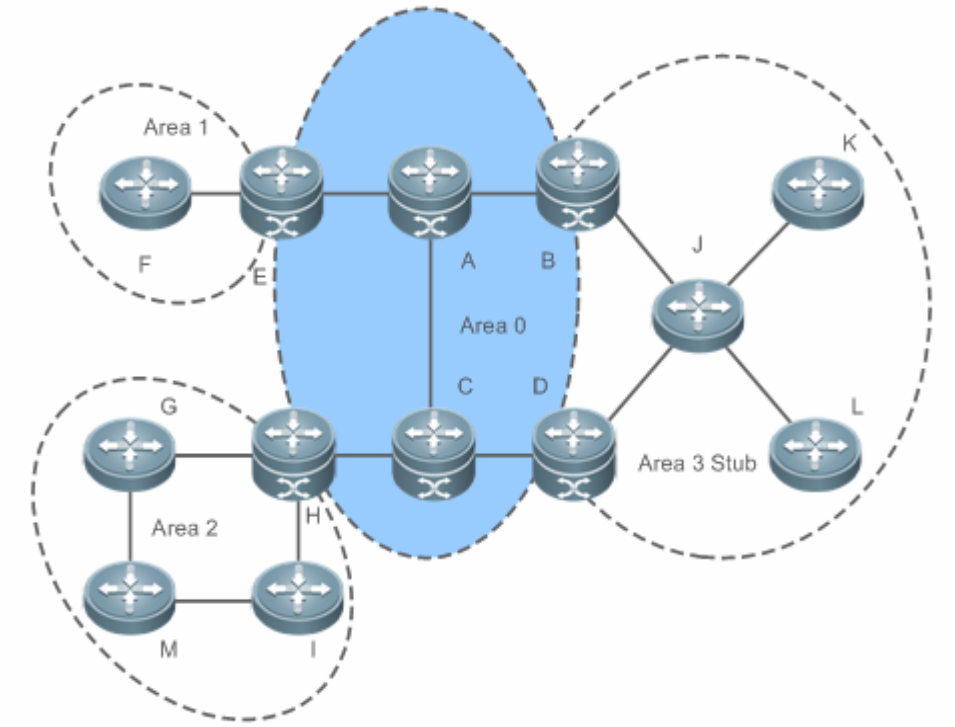
典型应用	场景描述
域内互联	在 AS 内部运行 OSPF，划分多个区域。

5.2.1 域内互联

应用场景

在 AS 内部运行 OSPF，如果路由设备超过 40 台，建议划分多个区域。通常，骨干区域应该采用性能可靠且处理速度较快的高端设备，非骨干区域可以采用性能相对较低的中低端设备。所有非骨干区域都必须与骨干区域相连。建议将位于末梢的非骨干区域设置为 Stub 区域。以图 1-1 为例，将该网络划分成 4 个区域，不同区域间的通信都经过骨干区域（即区域 0）。

图 4-1 OSPF 区域划分



【注释】 A、B、C、D、E、H 处于骨干区域，是骨干路由器。
区域 3 配置成 Stub 区域。

功能部属

- AS 内部，所有路由器运行 OSPF 协议，实现单播路由。

5.3 功能详解

基本概念

路由域

一个 AS 中的所有路由器必须相互连接，运行相同的路由协议。因此，AS 也被称为路由域（Routing Domain）。

运行 OSPF 的 AS 也被称为 OSPF 路由域，简称 OSPF 域。

OSPF 进程

OSPF 支持多实例（Instance），每个实例对应一个 OSPF 进程（Process）。

一台路由器上可以启用一个 OSPF 进程，也可以启用多个 OSPF 进程。每个 OSPF 进程独立执行 OSPF 协议，相互隔离。

Process ID 只有本地意义，不影响相邻接口上的 OSPF 报文交互。

RouterID

OSPF 域内，使用 Router ID 唯一标识一台路由器。任意两台路由器的 Router ID 不能相同。

如果路由器上存在多个 OSPF 进程，则每个 OSPF 进程使用一个 Router ID。任意两个 OSPF 进程的 Router ID 不能相同。

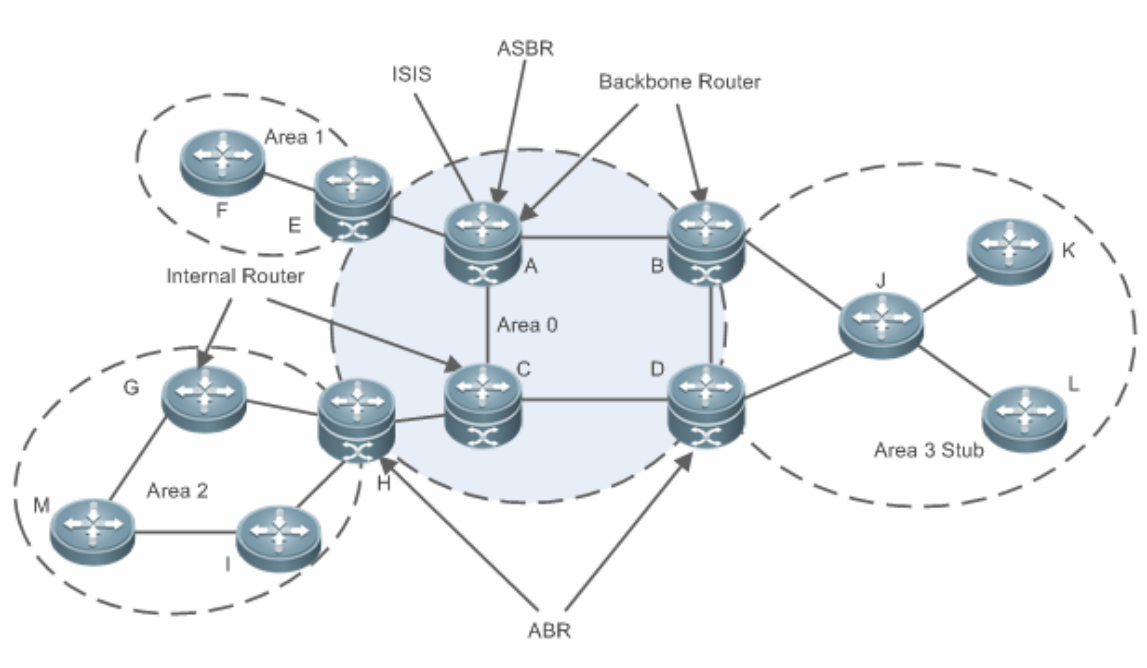
区域

OSPF 支持多区域（Area）。将一个 OSPF 域划分为多个区域，有助于缓解大规模网络的计算压力。

区域是从逻辑上将路由器划分为不同的组，每个组用区域号（Area ID）来标识。区域的边界是路由器，一台路由器可以只属于一个区域，也可以属于多个区域。一个网段（链路）只能属于一个区域，或者说每个运行 OSPF 的接口必须指明属于哪一个区域。

区域 0 为骨干区域（Backbone Area），其他区域为常规区域（NormalArea）。常规区域必须与骨干区域直接相连。

图 5-2 OSPF 区域划分



OSPF 路由器

在 OSPF 中定义了几种路由器类型，并为每种类型的路由器赋予不同的职责。

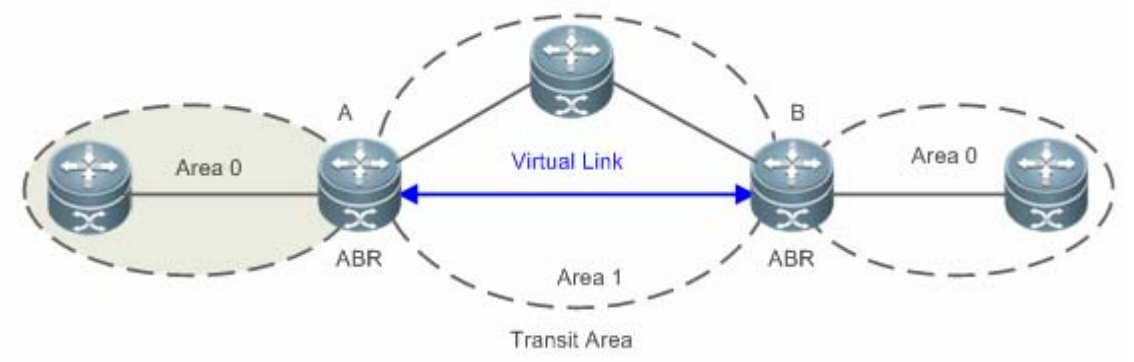
- 区域内路由器（Internal Router）
  该类路由器的所有接口都属于同一个 OSPF 区域。如上图中的 A、C、F、G、I、M、J、K、L。
- 区域边界路由器（Area Border Router，简称 ABR）
  该类路由器用来连接骨干区域和常规区域。ABR 同时属于两个以上的区域，其中一个必须是骨干区域。如上图中的 B、D、E、H。
- 骨干路由器（Backbone Router）
  该类路由器至少有一个接口属于骨干区域。所有的 ABR 和 Area0 的区域内路由器都是骨干路由器。如上图中的 A、B、C、D、E、H。

- 自治系统边界路由器（AS Boundary Router，简称 ASBR）
  该类路由器用来与其他 AS 交换路由信息。ASBR 并不一定位于 AS 的边界，它可能是区域内路由器，也可能是 ABR。如上图中的 A。

虚链路

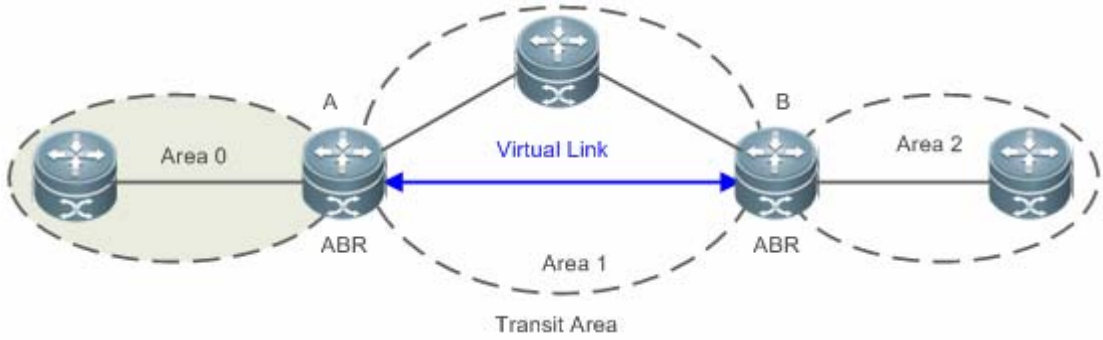
OSPF 支持虚链路（Virtual link）。虚链路是一条逻辑链路，属于骨干区域，用于解决在物理网络上骨干区域不连续或骨干区域与常规区域不能直接相连的问题。虚链路只能穿越一个常规区域，该区域被称为“传输区域”（Transit Area）。虚链路两端的路由器均为 ABR。

图 5-3 在物理网络上，骨干区域不连续



如上图所示：在 A、B 之间建立虚链路，将 Area0 连接起来；Area1 是传输区域；A、B 是 Area1 的 ABR。

图 5-4 在物理网络上，骨干区域与常规区域不能直接相连



如上图所示：在 A、B 之间建立虚链路，将 Area0 延伸到 B，则 Area0 与 Area2 在 B 上直接相连；Area1 是传输区域；A 是 Area1 的 ABR；B 是 Area1、Area2 的 ABR。

LSA

OSPF 以 LSA（Link State Advertisement，链路状态通告）的形式来描述路由信息。

LSA 类型	说明
Router-LSA（Type1）	由每个路由器始发，描述了路由器的链路状态和代价，在始发路由器所在区域内传播。
Network-LSA（Type2）	由 NBMA 类型网络上的 DR 始发，描述本网段的链路状态，在 DR 所在区域内传播。
Network-summary-LSA（Type3）	由 ABR 始发，描述到其它区域的路由，通告给非 Totally STUB、NSSA 区域。
ASBR-summary-LSA（Type4）	由 ABR 始发，描述到 ASBR 的路由，通告给除 ASBR 所在区域的其他区域。

AS-external-LSA（Type5）	由 ASBR 始发，描述到 AS 外部的路由，通告到所有区域（除了 STUB、NSSA 区域）。
NSSA LSA（Type7）	由 ASBR 始发，描述到 AS 外部的路由，仅在 NSSA 区域内传播。
Opaque LSA （Type9/Type10/Type11）	Opaque LSA 提供用于 OSPF 的扩展的通用机制。其中： ● Type9 LSA 仅在接口所在网段范围内传播。用于支持 GR 的 Grace LSA 就是 Type9 LSA 的一种。 ● Type10 LSA 在区域内传播。用于支持 TE 的 LSA 就是 Type10 LSA 的一种。 ● Type11 LSA 在自治域内传播，目前还没有实际应用的例子。

STUB 区域、NSSA 区域、Totally STUB 区域、Totally NSSA 区域，是常规区域的几种特殊形态，有助于减轻路由器负担，增强 OSPF 路由稳定性。

OSPF 报文

OSPF 使用以下几种类型的协议报文。这些 OSPF 报文被封装在 IP 报文中，以组播或单播方式发送。

报文类型	说明
Hello	周期性发送，用来发现 OSPF 邻居，维持邻接关系。
DD（Database Description）	描述本地 LSDB（Link-State Database，链路状态数据库）的摘要信息，用于在 OSPF 邻居之间进行数据库同步。
LSR（Link State Request）	用于向对方请求所需的 LSA。只有在 OSPF 邻居双方成功交换 DD 报文后，才会向对方发出 LSR 报文。
LSU（Link State Update）	用于向对方发送其所需要的 LSA。
LSAck（Link State Acknowledgment）	用来对收到的 LSA 进行确认。

功能特性

功能特性	作用
链路状态路由协议	在路由器上运行 OSPF，即可获得到达网络各个位置的路由。
OSPF 路由管理	通过人为配置，合理规划或优化 OSPF 路由，实现管理的目的。
增强安全性、可靠性	认证、与 BFD 联动等功能使 OSPF 更安全、更稳定可靠。
支持网管功能	MIB、SYSLOG 等功能使 OSPF 更易于管理。

5.3.1 链路状态路由协议

OSPF 属于链路状态路由协议（Link-StateRouting Protocols），工作过程概述：

- 邻居发现→双向通信
  在相连的路由器之间建立 OSPF 邻居关系，并保持双向通信。
- 数据库同步→完全邻接
  路由器使用 LSA 发布自己的全部链路状态。邻居之间交换 LSA，同步 LSDB，达到完全邻接状态。
- 计算 SPT →形成路由表
  路由器依据 LSDB 计算出到达每个目标网络的最短路径，形成 OSPF 路由表。

工作原理

邻居发现→双向通信

路由器从所有启动 OSPF 的接口上（或虚链路）发出 Hello 报文。如果两台路由器之间能够交互 Hello 报文，并且能够成功协商 Hello 报文中携带的参数，则它们就成为了邻居（Neighbor）。当互为邻居的路由器在彼此的 Hello 报文中找到自己的 Router ID 时，双向通信就建立了。

Hello 报文中包含（但不限于）如下信息：

- 始发路由器的 Router ID
- 始发路由器接口（或虚链路）的 Area ID
- 始发路由器接口（或虚链路）的网络掩码
- 始发路由器接口（或虚链路）的认证信息
- 始发路由器接口（或虚链路）的 Hello 时间间隔
- 始发路由器接口（或虚链路）的邻居死亡时间
- 始发路由器接口的优先级（用于 DR/BDR 竞选）
- DR（Designated Router，指定路由器），BDR（Backup Designated Router，备份指定路由器）的 IP 地址
- 始发路由器的邻居的 Router ID

数据库同步→完全邻接

邻居路由器之间建立双向通信后，使用 DD、LSR、LSU、LSAck 报文交换 LSA，建立邻接关系。简要过程如下：

- 路由器产生 LSA，用来描述该设备上的全部链路状态。
- 邻居之间交换 LSA。当路由器接收到邻居发送的 LSA 时，将拷贝一份到本地 LSDB，然后再传播给其它邻居。
- 当路由器及其邻居都获得了相同的 LSDB 时，达到完全邻接状态。

如果没有链路代价、网络增删变化，OSPF 将会十分安静。如果发生变化，则通告变化的链路状态，快速同步 LSDB。

计算最短路径→形成路由表

路由器上获得完整的 LSDB 后，将运行 Dijkstra 算法生成一棵从本地到每个目标网络的最短路径树（Shortest Path Tree，简称 SPT）。SPT 中记录了：目标网络、下一跳地址、代价。OSPF 依据 SPT 形成路由表。

如果发生链路代价、网络增删变化，则会引起 LSDB 的更新。设备将再次运行 Dijkstra 算法，生成新的 SPT，并更新路由表。

Dijkstra 算法用来在一个有权重的有向图中，找到从一个顶点到其他顶点的最短路径。

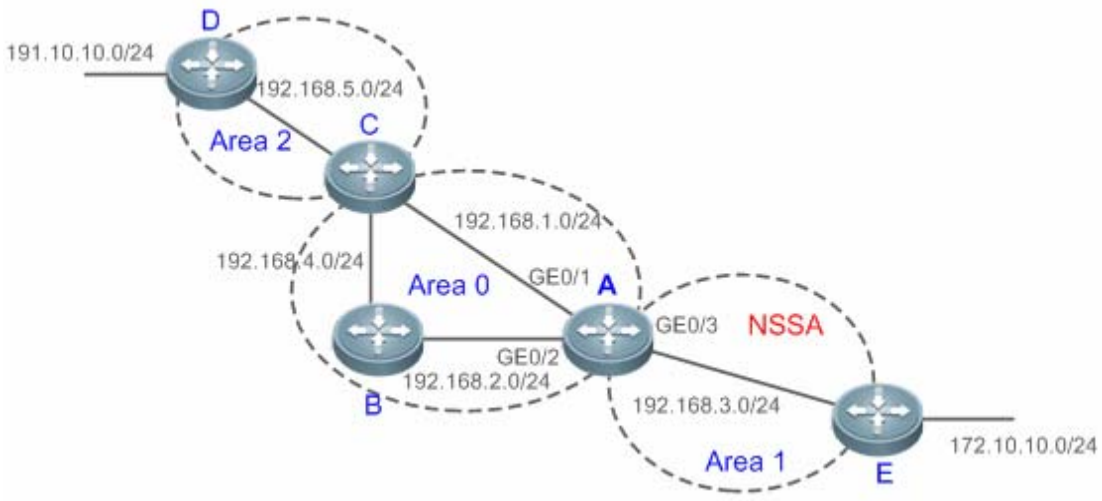
OSPF 网络类型

路由器不一定需要与它的每一个邻居交换 LSA、建立邻接关系。为提高效率，OSPF 将各种链路层协议的网络归类为 5 种类型，以不同的方式交换 LSA、建立邻接关系。

- 广播（Broadcast）
  自动发现邻居，选举 DR、BDR。
  DR（或 BDR）与其他所有路由器交换 LSA、建立邻接关系。DR、BDR 之外的路由器之间不交换 LSA、不建立邻接关系。
  Ethernet、FDDI 默认属于此类型。
- 非广播（Non-broadcast multiple access，简称 NBMA）
  手工配置邻居，选举 DR、BDR。
  DR（或 BDR）与其他所有路由器交换 LSA、建立邻接关系。DR、BDR 之外的路由器之间不交换 LSA、不建立邻接关系。
  X.25、帧中继、ATM 默认属于此类型。
- 点到点（point-to-point，简称 P2P）
  自动发现邻居，不选举 DR/BDR。
  链路两端路由器之间交换 LSA、建立邻接关系。
  PPP、HDLC、LAPB 默认属于此类型。
- 点到多点（Point-to-Multipoint，简称 P2MP）
  自动发现邻居，不选举 DR/BDR。
  任意两台路由器之间都要交换 LSA、建立邻接关系。
  没有任何链路层协议的网络默认为此类型。
- 点到多点非广播
  手动配置邻居，不选举 DR/BDR。
  任意两台路由器之间都要交换 LSA、建立邻接关系。
  没有任何链路层协议的网络默认为此类型。

OSPF 路由类型

图 5-5



在 A 上查看路由表中的 OSPF 路由（如下红色字体）。

```
A#show ip route
```

```
Codes:  C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
O N2 172.10.10.0/24 [110/20] via 192.168.3.2, 00:01:00, GigabitEthernet 0/3
O E2 191.10.10.0/24 [110/20] via 192.168.1.2, 01:11:26, GigabitEthernet 0/1
C    192.168.1.0/24 is directly connected, GigabitEthernet 0/1
C    192.168.1.1/32 is local host.
C    192.168.2.0/24 is directly connected, GigabitEthernet 0/2
C    192.168.2.1/32 is local host.
C    192.168.3.0/24 is directly connected, GigabitEthernet 0/3
C    192.168.3.1/32 is local host.
O    192.168.4.0/24 [110/2] via 192.168.2.2, 00:00:02, GigabitEthernet 0/2
O IA 192.168.5.0/24 [110/3] via 192.168.1.2, 00:01:02, GigabitEthernet 0/1
```

网关产品不支持 BGP,ISIS，配置举例仅作为配置参考，实际请以具体设备配置为准。

每条 OSPF 路由前都带有一个标识，用来说明此路由的类型。OSPF 路由共有 6 种类型。

- O：区域内路由
  此类路由描述了如何到达本区域内的目标网络。路由代价=本地到目标网络的代价。
- IA：区域间路由
  此类路由描述了如何到达其他区域的目标网络。路由代价=本地到目标网络的代价。
- E1：第一类外部路由
  此类路由描述了如何到达 AS 以外的目标网络。路由代价=本地到 ASBR 的代价+ASBR 到目标网络的代价。Stub、NSSA 区域内的路由器上不存在此类路由。
- E2：第二类外部路由
  此类路由描述了如何到达 AS 以外的目标网络。路由代价=ASBR 到目标网络的代价。Stub、NSSA 区域内的路由器上不存在此类路由。
- N1：NSSA 区域的第一类外部路由
  此类路由仅描述了如何经 NSSA 区域的 ASBR 到达 AS 以外的目标网络。路由代价=本地到 ASBR 的代价+ASBR 到目标网络的代价。仅 NSSA 区域的路由器上存在此类路由。
- N2：NSSA 区域的第二类外部路由
  此类路由描述了如何经 NSSA 区域的 ASBR 到达 AS 以外的目标网络。路由代价=ASBR 到目标网络的代价。仅 NSSA 区域的路由器上存在此类路由。

E2、N2 这两类路由的可信度比较低，OSPF 认为从 ASBR 到自治系统之外的代价远远大于在自治系统之内到达 ASBR 的代价。所以，计算路由代价时只考虑 ASBR 到自治系统之外的代价。

相关配置

启动 OSPF

缺省情况下，未启动 OSPF。

使用 **router ospf** 1 命令，在路由器上创建一个 OSPF 进程。

使用 **network area** 命令，在接口上启动 OSPF，指定 Area ID。

使用 **area virtual-link** 命令，在路由器上创建一个虚链接。可将虚链接视为一个逻辑接口。

Router ID

缺省情况下 ,OSPF 进程选举所有 Loopback 接口中 IP 地址最大的作为 Router ID。如果没有配置了 IP 地址的 Loopback 接口，则选取所有物理接口中 IP 地址最大的作为路由设备标识。

也可以使用 **router-id** 命令，人为指定 Router ID。

协议控制参数

使用 **ip ospf hello-interval** 命令，修改接口上的 Hello 消息发送间隔，缺省值是 10 秒（NBMA 类型 30 秒）。

使用 **ip ospf dead-interval** 命令，修改接口上的邻居死亡时间，缺省值是 Hello 报文发送间隔的四倍。

使用 **neighbor** 命令的 **poll-interval** 参数，修改 NBMA 类型接口上的邻居轮询间隔，缺省值是 120 秒。

使用 **ip ospf transmit-delay** 命令，修改接口上的 LSU 报文传输延时，缺省值是 1 秒。

使用 **ip ospf retransmit-interval** 命令，修改接口上的 LSU 报文重传间隔，缺省值是 5 秒。

使用 **areavirtual-link** 命令的 **hello-interval** 参数，修改虚链路上的 Hello 消息发送间隔，缺省值是 10 秒。

使用 **areavirtual-link** 命令的 **dead-interval** 参数，修改虚链路上的邻居死亡时间，缺省值是 Hello 报文发送间隔的四倍。

使用 **areavirtual-link** 命令的 **transmit-delay** 参数，修改虚链路上的 LSU 报文传输延时，缺省值是 1 秒。

使用 areavirtual-link 命令的 retransmit-interval 参数，修改虚链路上的 LSU 报文重传间隔，缺省值是 5 秒。

使用 **timers throttle lsa all** 命令，修改生成 LSA 的指数退避算法参数，缺省值是 0 毫秒，5000 毫秒，5000 毫秒。

使用 **timerspacinglsa-group** 命令，修改 LSA 分组刷新的时间，缺省值是 30 秒。

使用 **timers pacing lsa-transmit** 命令，修改（LSA 分组刷新的）LS-UPD 报文发送间隔和个数，缺省值是 40 毫秒、1 个。

使用 **timers lsa arrival** 命令，修改接收相同 LSA 的延时，缺省值是 1000 毫秒。

使用 **timers throttlespf** 命令，修改计算 SPT 的延时，两次计算的最小间隔、最大间隔。缺省值是 1000 毫秒、5000 毫秒、10000 毫秒。

OSPF 网络类型

缺省情况下，Ethernet、FDDI 为广播类型；X.25、帧中继、ATM 为 NBMA 类型；PPP、HDLC、LAPB 为 P2P 类型。

使用 **ip ospf network** 命令，手工指定接口的网络类型。

使用 **neighbor** 命令，手工指定邻居。NBMA、点到多点非广播类型必须手工指定邻居。

使用 **ip ospf priority** 命令，调整接口的优先级（用于 DR/BDR 竞选）。广播、NBMA 类型需要竞选 DR/BDR。优先级最大者获胜，优先级为 0 者弃权。缺省值为 1。

5.3.2 OSPF路由管理

通过人为配置，可以合理规划或优化 OSPF 路由，实现管理的目的。

工作原理

（Totally）Stub、NSSA 区域

（Totally）Stub、NSSA 区域有助于减轻协议交互负担、减小路由表的规模。

- 将适当的区域设置为（Totally）Stub、NSSA 区域，则可以免除大量的 LSAType 5、3 在区域内传播。

区域	LSAType1、2	LSAType 3	LSAType 4	LSAType 5	LSAType 7
非（Totally）Stub、NSSA 区域	允许	允许	允许	允许	不允许
Stub 区域	允许	允许，包括一条缺省路由	不允许	不允许	不允许
Totally Stub 区域	允许	只允许一条缺省路由	不允许	不允许	不允许
NSSA 区域	允许	允许，包括一条缺省路由	允许	不允许	允许
Totally NSSA 区域	允许	只允许一条缺省路由	允许	不允许	允许

ABR 使用 LSAType 3 向（Totally）Stub、NSSA 区域发布一条缺省路由。

ABR 将（Totally）NSSA 区域内的 LSAType 7 转换成 LSAType 5，发布到骨干区域。

- 将适当的区域设置为（Totally）Stub、NSSA 区域，则区域内路由器的路由表中可以免除大量 E1、E2、IA 类型的路由。

区域	区域内路由器的路由表中存在哪些路由
非（Totally）Stub、NSSA 区域	O：到本区域某目标网段的路由 IA：到其他区域某目标网段的路由 E1 或 E2：（经过 AS 内任意 ASBR）到 AS 外部某目标网段的路由、缺省路由
Stub 区域	O：到本区域某目标网段的路由 IA：到其他区域某目标网段的路由、缺省路由
Totally Stub 区域	O：到本区域某目标网段的路由 IA：缺省路由
NSSA 区域	O：到本区域某目标网段的路由 IA：到其他区域某目标网段的路由、缺省路由 N1 或 N2：（经过本区域内的 ASBR）到 AS 外部某目标网段的路由、缺省路由
Totally NSSA 区域	O：到本区域某目标网段的路由 IA：缺省路由 N1 或 N2：（经过本区域内的 ASBR）到 AS 外部某目标网段的路由、缺省路由

路由重分布

路由重分布是指：将设备上存在的“其他路由协议的路由、其他 OSPF 进程的路由、静态路由、直连路由”引入 OSPF 进程，以 LSA Type 5、7 的方式发送给邻居。路由重分布不能引入缺省路由。

路由重分布常用于 AS 间互联。通过在 ASBR 上配置路由重分布，可以将 AS 外部的路由信息传播到 AS 内部，也可以将 AS 内部的路由信息传播到 AS 外部。

引入缺省路由

通过在 ASBR 上配置命令，可以将一条缺省路由引入 OSPF 进程，以 LSA Type 5、7 的方式发送给邻居。

“引入缺省路由”常用于 AS 间互联，以一条缺省路由代替所有 AS 外部的路由信息。

路由汇聚

路由汇聚是指将具有相同前缀的路由信息汇聚为一条路由，并将汇聚后的路由（替代大量琐碎路由）发布给邻居。路由汇聚有助于减轻协议交互负担、减小路由表的规模。

缺省情况下，对于区域间的路由信息，ABR 以网段为单位发布 LSA Type 3；对于重分布进来的路由信息，ASBR 逐条发布 LSA Type 5、7。如果其中存在一些连续的网段，则建议配置路由汇聚。

配置路由汇聚时，汇聚范围有可能超出实际路由的网络范围。如果数据发往汇聚范围内不存在的网络，将有可能发生路由环路或加重路由器的处理负担。为阻止这种情况的发生，ABR 或 ASBR 会自动添加一条 discard 路由到路由表。该路由不会被传播。

路由过滤

OSPF 允许在学习、交互、使用路由信息的过程中进行过滤，以达到安全可控的目的。

通过配置命令，可以在以下几处进行路由过滤：

- 针对接口。禁止接口发出路由信息（任意 LSA）、或禁止接口与邻居交互路由信息（任意 LSA）。
- 针对区域间发布的路由信息。只有满足过滤条件的路由信息才能被发布到另一区域（LSA Type 3）。
- 针对 AS 外部的路由信息。只有满足过滤条件的路由信息才能被重分布到 OSPF 进程（LSA Type 5、7）。
- 针对路由器收到的 LSA。OSPF 路由表中，只有由满足过滤条件的 LSA 计算出的路由，才能执行报文转发。

路由代价

如果网络中存在冗余链路或设备，则从本地到目的网络之间可能存在多条路径。OSPF 选择其中总代价最小的路径形成 OSPF 路由。一条路径的总代价等于沿途链路上的代价之和。通过修改沿途链路上的代价，使一条路径的总代价最小，即可使 OSPF 选择此路径形成路由。

通过配置命令，可以修改如下链路代价：

- 从接口到直连网段的代价、从接口到邻居的代价
- 从 ABR 到区间汇聚网段的代价、从 ABR 到缺省网段的代价
- 从 ASBR 到外部网段的代价、从 ASBR 到缺省网段的代价

cost、metric 都表示代价，没有实质上的差别。

OSPF 管理距离

管理距离（administrative distance，缩写为 AD）用于评价路由的可信度，取值范围 0～255（整数）。AD 值越小，则表示此路由更值得信任。到达同一目的地存在多条路由时，路由器优先选择 AD 值较小的路由。AD 值较大者，成为浮动路由（作为最优路由的备份）。

缺省情况下，每种来源的路由对应一个 AD 值。AD 值为本地概念，修改 AD 值只会影响当前路由器上的路由选择。

路由来源	直连网络	静态路由	OSPF 路由	RIP 路由	不可达路由
缺省 AD	0	1	110	120	255

相关配置

Stub、NSSA 区域

缺省情况下，没有 Stub、NSSA 区域。

使用 **area stub** 命令，将指定区域设置为 Stub 区域。

使用 **area nssa** 命令，将指定区域设置为 NSSA 区域。

骨干区域不能设置为 Stub（或 NSSA）区域。

传输区域（虚链路穿过的区域）不能设置为 Stub（或 NSSA）区域。

包含 ASBR 的区域不能设置为 Stub 区域。

路由重分布、引入缺省路由

缺省情况下，不进行路由重分布，不引入缺省路由。

使用 **redistribute** 命令，配置路由重分布。

使用 default-information originate 命令，引入缺省路由。

配置路由重分布、引入缺省路由后，路由器自动成为 ASBR。

路由汇聚

缺省情况下，不进行路由汇聚。如果配置路由汇聚，会自动添加 discard 路由。

使用 **arearange** 命令，在 ABR 上汇聚区域间发布的路由（LSA Type 3）。

使用 **summary-address** 命令，在 ASBR 上汇聚重分布路由（LSA Type 5、7）。

使用 **discard-route** 命令，向路由表中添加一条 discard 路由。

路由过滤

缺省情况下，不进行路由过滤。

使用 **passive-interface** 命令，设置被动接口。被动接口上不能交互路由信息（任意 LSA）。

使用 ip ospfdatabase-filter all out 命令，禁止接口发出路由信息（任意 LSA）。

使用 **area filter-list** 命令，在 ABR 上过滤区域间发布的路由信息。只有满足条件的路由信息才能被发布到另一区域（LSA Type 3）。

使用 **redistribute** 命令的 **route-map** 参数，或使用 **distribute-list out** 命令，在 ASBR 上过滤 AS 外部的路由信息。只有满足过滤条件的路由信息才能被重分布到 OSPF 进程（LSA Type 5、7）。

使用 **distribute-list in** 命令，过滤路由器收到的 LSA。OSPF 路由表中，只有由满足过滤条件的 LSA 计算出的路由才能执行报文转发。

路由代价

- 从接口到直连网段的代价（即接口上的 cost 值）
  缺省值为自动代价。自动代价 = 参考带宽/接口带宽。
  使用 **auto-cost reference-bandwidth** 命令，设置自动代价的参考带宽，缺省值为 100Mbps。
  使用 **ip ospf cost** 命令，人为设置接口上的 cost 值。此项配置优先级高于自动代价。
- 从接口到指定邻居的代价（即从本地到指定邻居的 cost 值）
  缺省值为自动代价。
  使用 **neighbor** 命令中的 **cost** 参数，修改接口到指定邻居的代价。此项配置优先级高于接口上的 cost 值。
  只有 P2MP 类型的接口允许此项配置。
- 从 ABR 到区间汇聚网段的代价（区域间路由汇聚的 cost 值）
  如果兼容 RFC1583，缺省值为被汇总的链路代价的最小值，否则为被汇总的链路代价的最大值。
  使用 **compatible rfc1583** 命令，设置 OSPF 选路规则兼容 RFC1583。缺省兼容 RFC1583。
  使用 **area range** 命令的 **cost** 参数，修改区域间路由汇聚的 cost 值。
- 从 ABR 到缺省网段的代价（ABR 自动向 Stub、NSSA 区域发布的缺省路由的 cost 值）
  缺省值为 1。
  使用 **area default-cost** 命令，修改 ABR 自动向 Stub、NSSA 区域发布的缺省路由的 cost 值。
- 从 ASBR 到外部网段的代价（外部路由的 metric 值）
  缺省情况下，重分布其它路由的 metric 为 20，路由类型 Type2 External。
  使用 **default-metric** 命令，修改外部路由的 metric 值的缺省值。
  使用 **redistribute** 命令中的 **metric**、**metric-type**、**route-map** 参数，修改外部路由的 metric 值、路由类型。
- 从 ASBR 到缺省网段的代价（人为引入的缺省路由的 metric 值）
  缺省情况下，metric 为 1，路由类型 Type2 External。
  使用 **default-information originate** 命令的 **metric**、**metric-type**、**route-map** 参数，修改人为引入的缺省路由的 metric 值、路由类型。
  使用 **area nssa** 命令的 **default-information-originate** 参数的 **metric**、**metric-type** 参数，修改 NSSA 区域内人为引入的缺省路由的 metric 值、路由类型。
- 此外，使用 **max-metric router-lsa** 命令，可以将路由器上发布的所有链路代价均为最大值。则途径此路由器的任何路径，总代价都会变得很大，几乎不可能成为最短路径。

OSPF 管理距离

缺省情况下，OSPF 管理距离为 110。

使用 **distance** 命令，设置 OSPF 路由的管理距离值。

5.3.3 增强安全性、可靠性

认证、与 BFD 联动等功能使 OSPF 更安全、更稳定可靠。

工作原理

认证

认证是为了阻止非法接入网络的路由器和伪造 OSPF 报文的主机参与 OSPF 协议过程。在 OSPF 接口（或虚链路两端）对收到的 OSPF 报文进行认证。如果认证失败，则丢弃报文，邻接关系将不能被建立。

启动认证功能后，可以避免学到非认证、无效路由，避免通告有效路由到非认证设备。在广播类型网络中，认证还可以避免非认证设备成为指定设备的可能性，保证了路由系统的稳定性和抗入侵性。

MTU 校验

OSPF 在收到 DD 时会校验邻居的接口的 MTU 和自己接口的 MTU 是否相同，如果收到的 DD 报文中指示的接口的 MTU 大于接收接口的 MTU，则邻接关系将不能被建立。关闭 MTU 的校验，可以避免此问题。

源地址校验

通常情况下，OSPF 收到报文的源地址和接收接口会在同一个网段。不过在点到点链路上，链路两端的地址是独立设置的，可以不要求在同一个网段，在这种场景下，由于点到点链路协商过程中会告知对端的地址信息，因此 OSPF 会检查报文的源地址是否就是协商时对端通告的地址，若不是则认为报文非法并丢弃该报文。特别的，对于 unnumbered 接口，OSPF 始终不进行地址校验。

但在某些应用场景中，可能会出现源地址不如上面所述，导致 OSPF 校验失败，比如点到点链路上，协商的对端地址无法获取。在这种场景中，需要关闭源地址校验功能，以保证 OSPF 邻居能正常建立。

双向维持

OSPF 路由器之间通过周期性发送 Hello 报文来维持邻接关系。在较大的网络中，可能会出现大量的报文收发，占用较高的 CPU 和内存资源，造成部分部分报文的延迟或丢弃。如果 Hello 报文的处理超出了死亡间隔，将导致邻接关系断开。

如果启用双向维持功能，则除了 Hello 报文外，DD、LSU、LSR、LSAck 报文也能用来维持邻居之间的双向通信，从而使邻接关系更加稳定。

并发邻居交互限制

当路由器同时与多个邻居交换数据时，其性能会受到影响。限制 OSPF 进程可并发交互（发起或接受）的邻居最大数目，使路由器可以分批与邻居进行交互，有助于保障数据转发或其他关键业务。

OVERFLOW

OSPF 要求同一个区域中的路由器保存相同的 LSDB。随着网络上路由数量不断增加，一些路由器由于系统资源有限，不能承载如此多的路由信息，有可能导致路由器系统资源耗尽而失效的故障。

OVERFLOW 是通过限制 LSDB 中外部路由的数量，达到控制 LSDB 的规模的目的。

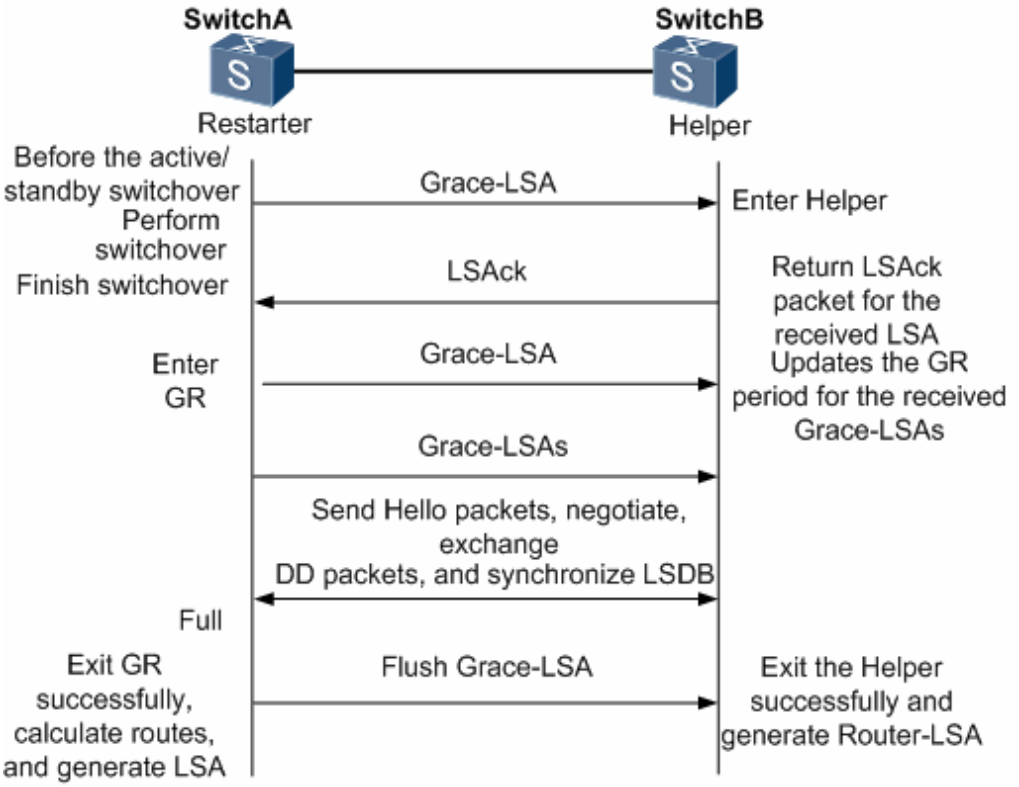
当路由器上的外部路由数量达到上限时，进入 Overflow 状态：删除 LSDB 中自己产生的外部路由、不产生新的外部路由、丢弃新收到的外部路由。Overflow 状态超时后（5 秒），如果外部路由数量低于上限，则恢复正常状态。

GR

路由器普遍采用了控制和转发分离的技术。在网络拓扑保持稳定的情况下，启用 GR（Graceful Restart，优雅重启）功能的路由器在控制层面的重启过程中转发层面能够继续指导数据的转发，同时控制层面邻居关系的重建以及路由计算等动作不会影响转发层面的功能，从而避免了路由震荡引发的业务中断，提高了整网的可靠性。

目前，GR 功能只在主备切换和系统升级过程中使用。

图 5-6 正常的 OSPF GR 过程



- GR 过程需要 Restarter 和 Helper 的协作。Restarter 是发生 GR 的路由器。Helper 是 Restarter 的邻居。
- Restarter 在开始和退出 GR 时向邻居发送 Grace-LSA，通知邻居进入和退出 Helper 状态。
- Restarter 与 Helper 邻居关系达到 Full 状态，则 GR 可成功退出。

5.3.4 支持网管功能

MIB、SYSLOG 等功能使 OSPF 更易于管理。

工作原理

MIB

MIB（管理信息库）是设备端维护的设备状态信息集。管理程序可以对 MIB 节点进行查阅和设置。

路由器上可以同时启动多个 OSPF 进程，但 OSPF MIB 只能与一个 OSPF 进程绑定。

Trap

告警是系统检测到故障而产生的通知，告警中携带对应的故障信息。

启动 Trap 功能，则路由器可以主动将告警信息发送到网管设备。

SYSLOG

日志记录了用户对路由器的操作（比如命令配置）以及特定事件（比如网络连接失效）等信息。

允许日志记录邻接状态变化，则网络管理员可以通过查看日志了解 OSPF 邻居之间建立和维持邻接关系的全过程。

相关配置

MIB

缺省情况下，MIB 绑定在进程号最小的 OSPF 进程上。

使用 **enable mib-binding** 命令，将 MIB 绑定在当前 OSFP 进程上。

Trap

缺省情况下，所有 TRAP 开关关闭，且不允许设备发送 OSPFTrap。

使用 **enable traps** 命令，在 OSFP 进程下打开指定的 Trap 开关。

使用 **snmp-server enable traps ospf** 命令，允许设备发送 OSPF Trap。

SYSLOG

缺省情况下，允许日志记录邻接状态变化。

使用 **log-adj-changes** 命令，允许日志记录邻接状态变化。

5.4 配置详解

配置项	配置建议&相关命令

配置 OSPF 基本功能	⚠ 必须配置。用于构建 OSPF 路由域。	
	router ospf	创建 OSPF 进程。
	router-id	设置 Router ID。
	network area	在接口上启动 OSPF，指定 Area ID。
	area virtual-link	创建虚链路。
设置网络类型	⚠ 可选配置。如果物理网络为 X.25、帧中继、ATM，则必须配置此项。	
	ip ospf network	定义网络类型。
	neighbor	指定邻居。
	ip ospf priority	配置 DR 优先级。
配置路由重分布、缺省路由	⚠ 可选配置。如果 OSPF 路由域连接外网，则建议配置此项。	
	redistribute	路由重分布。
	default-information originate	引入缺省路由。
设置 Stub、NSSA 区域	⚠ 可选配置。有助于减少路由信息的交互，缩小路由表规模，增强路由稳定性。	
	area stub	设置 Stub 区域。
	area nssa	设置 NSSA 区域。
配置路由汇聚	⚠ 可选配置。有助于减少路由信息的交互，缩小路由表规模，增强路由稳定性。	
	area range	汇聚区域间发布的路由信息。
	summary-address	汇聚重分布引入的路由信息。
	discard-route	向路由表中添加一条 discard 路由。
配置路由过滤	⚠ 可选配置。人为控制路由信息交互过程、筛选可用的 OSPF 路由。	
	passive-interface	设置被动接口。
	ip ospf database-filter all out	禁止接口发出 LSA。
	area filter-list	对区域间发布的路由信息进行过滤。
	distribute-list out	对重分布引入的路由进行过滤。
	distribute-list in	对收到的 LSA 计算出的路由进行过滤。
修改路由代价、管理距离	⚠ 可选配置。人为控制 OSPF 计算的最短路径、是否优先选择 OSPF 路由。	
	auto-cost reference-bandwidth	修改自动代价的参考带宽。
	ip ospf cost	修改接口出方向的 cost 值。
	area default-cost	修改 Stub/NSSA 区域缺省路由的 cost 值。
	default-metric	修改重分布路由的缺省 metric 值。
	max-metric router-lsa	设置最大度量值。
	commpatible rfc1583	设置选路规则兼容 RFC1583。
	distance	修改 OSPF 管理距离。
启动认证功能	⚠ 可选配置。阻止非法接入网络的路由器和伪造 OSPF 报文的主机参与 OSPF 协议。	

	area authentication	在区域上启动认证、设置认证方式
	ip ospf authentication	在接口上启动认证、设置认证方式
	ip ospf authentication-key	在接口上设置文本认证的密码
	ip ospf message-digest-key md5	在接口上设置 MD5 认证的密码
启动溢出功能	⚠ 可选配置。避免由于过度消耗内存导致 OSPF 进程停止运行的问题。	
	overflow memory-lack	允许内存不足时进入 OVERFLOW 状态。
	overflow database	允许 LSA 数量超限后进入 OVERFLOW 状态。
	overflow database external	允许 external LSA 数量超限后进入 OVERFLOW 状态。
修改并发邻居数量限制	⚠ 可选配置。避免由于过度消耗 CPU 导致设备性能下降的问题。	
	max-concurrent-dd	修改当前 OSPF 进程上并发邻居数量限制。
	router ospf max-concurrent-dd	修改所有 OSPF 进程上并发邻居总数限制。
关闭源地址校验	⚠ 可选配置。避免由于无法获取对端地址导致无法建立邻接关系的问题。	
	ip ospf source-check-ignore	在接口上关闭源地址校验功能。
关闭 MTU 校验	⚠ 可选配置。避免由于邻居接口 MTU 不一致导致无法建立邻接关系的问题。	
	ip ospf mtu-ignore	在接口上关闭 MTU 校验功能。
启动双向维持	⚠ 可选配置。避免由于 Hello 报文延迟或丢失导致邻接关系断开的问题。	
	two-way-maintain	启动双向维持功能。
启动 GR 功能	⚠ 可选配置。在 OSPF 进程重启或主备切换过程中，维持 OSPF 路由转发，避免流量中断。	
	graceful-restart	配置 Restarter 功能。
	graceful-restart helper	配置 Helper 功能。
启动 Fast Hello	⚠ 可选配置。在链路故障时，快速发现邻居死亡，避免流量中断。	
	ip ospf dead-intervalminimal hello-multiplier	在接口上启动 Fast Hello 功能。
配置网管功能	⚠ 可选配置。使用户可以通过 SNMP 网管软件来管理 OSPF。	
	enable mib-binding	在 OSFP 进程下绑定 MIB。
	enable traps	在 OSFP 进程下打开指定的 Trap 开关。
	snmp-server enable traps ospf	允许设备发送 OSPF Trap。
	log-adj-changes	允许日志记录邻接状态变化。
修改协议控制参数	⚠ 可选配置。除非必要，不建议修改协议控制参数。	
	ip ospf hello-interval	修改 hello 报文发送间隔。
	ip ospf dead-interval	修改邻居死亡时间。
	timers throttle lsa all	修改生成 LSA 的指数退避算法参数。
	timers throttle route inter-area	修改区间路由计算的延时时间。
	timers throttle route ase	修改外部路由计算的延时时间。

	timers pacing lsa-group	修改分组刷新 LSA 的分组时间。
	timers pacing lsa-transmit	修改分组刷新 LSA 的发送间隔。
	ip ospf transmit-delay	修改 LSU 报文传输延时。
	ip ospf retransmit-interval	修改 LSU 报文重传间隔。
	timers lsa arrival	修改接收相同 LSA 的延时。
	timers throttle spf	修改计算 SPT 的计时器。

5.4.1 配置OSPF基本功能

配置效果

- 在网络中建立一个 OSPF 路由域，为网络内用户提供 IPv4 单播路由服务。

注意事项

- 需要确保 IP 单播路由功能启用，即 **ip routing** 开关未被关闭，才能够启用 OSPF。
- 强烈建议手工配置 Router ID。
- 配置 **ip ospf disable all** 后，即使接口属于该 network，也不再接收和发送任何 OSPF 报文，也不参与 OSPF 的计算。

配置方法

创建 OSPF 进程

- 必须配置。
- 每台路由器都需要配置。

设置 Router ID

- 可选配置，但强烈建议手工配置 Router ID。
- 不配置 Router ID 时，OSPF 会选择接口 IP 地址，若没有接口配置 IP 地址或者配置的 IP 地址已经被其他 OSPF 实例使用，则必须手工配置 Router ID。

在接口上启动 OSPF，指定 Area ID

- 必须配置。
- 每台路由器都需要配置。

检验方法

- 通过 **show ip route ospf** 命令查看 OSPF 路由表项加载正确。

- 通过 **ping** 命令查看 IPv4 单播业务正确。

相关命令

创建 OSPF 进程

【命令格式】 **router ospf** *process-id* [**vrf** *vrf-name*]

【参数说明】 *process-id*：OSPF 进程号。未配置进程号时，表示配置进程 1。

vrf-name：指定 OSPF 进程所属的 VRF。

【命令模式】 全局配置模式。

【使用指导】 不同 OSPF 进程间相互独立，可以近似认为是两个独立运行的路由协议。

设置 Router ID

【命令格式】 **router-id** *router-id*

【参数说明】 *router-id*：要设置的路由设备的 ID，以 IP 地址形式表示。

【命令模式】 OSPF 路由进程配置模式。

【使用指导】 不同 OSPF 进程间相互独立，可以近似认为是两个独立运行的路由协议。

每个 OSPF 进程使用不同的 Router ID。

在接口上启动 OSPF，指定 Area ID

【命令格式】 **network** *ip-address wildcard* **area** *area-id*

【参数说明】 *ip-address*：接口对应的 IP 地址。

wildcard：定义 IP 地址比较比特位，0 表示精确匹配，1 表示不做比较。

area-id：OSPF 区域标识。一个 OSPF 区域总是关联一个地址范围，为了便于管理，也可以用一个子网作为 OSPF 区域标识。

【命令模式】 OSPF 路由进程配置模式。

【使用指导】 *ip-address* 和 *wildcard* 两个参数的定义，允许用一条命令就可以将多个接口关联到一个 OSPF 区域。要在一个接口上运行 OSPF，必须将该接口的主 IP 地址包括在 **network area** 定义的 IP 地址范围内。如果 **network area** 定义的 IP 地址范围只包括接口的次 IP 地址，该接口将不会运行 OSPF。当接口地址同时与多个 OSPF 进程 network 命令定义的 IP 地址范围相匹配时，按照最优匹配方式，确定接口参与的 OSPF 进程。

设置虚链路

【命令格式】 **area** *area-id* **virtual-link** *router-id* [**authentication** [**message-digest** | **null**]] [**dead-interval** { *seconds* | **minimal hello-multiplier** *multiplier* }] [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [[**authentication-key** [**0** | **7**] *key*] | [**message-digest-key** *key-id* **md5** [**0** | **7**] *key*]]

【参数说明】 *area-id*：OSPF 过渡区域号。区域号可以是一个十进制整数值，也可以是一个 IP 地址。

router-id ：虚拟链路邻居的路由设备标识。。

dead-interval *seconds*：定义宣告邻居丢失时间，以秒为单位，取值范围：0-2147483647。该参数必须与邻居保持一致。

minimal：启用 Fast Hello 功能，将死亡时间设置为 1s。

hello-multiplier：Fast Hello 功能中，死亡间隔与 Hello 间隔的乘数。

multiplier：Fast Hello 功能中，每秒钟发送的 Hello 报文的次数。取值范围：3-20。

hello-interval *seconds*：OSPF 往虚拟链路发送 Hello 报文的时间间隔，以秒为单位，取值范围：1-65535。该参数必须与邻居保持一致。

retransmit-interval *seconds*：OSPF 链路状态描述（LSA）重传时间，以秒为单位，取值范围：0-65535。

transmit-delay *seconds*：OSPF 发送链路状态描述（LSA）的时延，以秒为单位，取值范围：0-65535。

authentication-key [**0** | **7**] *key*：定义 OSPF 明文认证的密钥。

message-digest-key *key-id* **md5** [**0** | **7**] key：定义 OSPF MD5 认证的密钥标识符和密钥。

authentication：设置认证类型，使用明文认证。

message-digest：设置认证类型为 MD5 认证。

null：设置为不认证。

【命令模式】 OSPF 路由进程配置模式。

【使用指导】 在 OSPF 路由域中，所有的区域都必须与骨干域连接，如果骨干域断接，就需要配置虚拟链接将骨干域接续起来，否则网络通讯将出现问题。虚拟链接需要在两个区域边界路由设备（ABR）之间创建，两个 ABR 共同所属的区域成为过渡区域。残域（Stub Area）和 NSSA 是不能作为过渡区域的。虚拟链接也可以用于接续其它非骨干区域。

router-id 为 OSPF 邻居路由设备标识符，如果不确定 router-id 的值，请用 **show ip ospf neighbor** 命令进行确认。可以通过配置 Loopback 地址做路由标识符。

area virtual-link 命令只定义虚拟链路的认证密钥，要启用虚拟链路所连接区域的 OSPF 报文认证，用路由进程配置命令 **area authentication**。

OSPF 支持 Fast Hello 功能：

启用 OSPF Fast Hell o 功能将加速 OSPF 发现邻居，并快速检测邻居失效。通过指定 **minimal** 和 **hello-multiplier** 关键字和 *multiplier* 参数，启用 OSPF Fast Hell o 功能。**minimal** 关键字将死亡时间设置为 1s，**hello-multiplier** 值指定每秒钟发送的 Hello 报文的次数，这样 Hello 报文的发送间隔就降到 1s 以内了。

当某个虚链路配置了 Fast Hello 功能，从该虚链路通告的 Hello 报文的 Hello 间隔字段设置为 0，从该虚链路接收的 Hello 报文的 Hello 间隔字段被忽略。

无论是否启用 Fast Hello 功能，虚链路两端的设备死亡间隔始终要保持一致，**hello-multiplier** 值不必设置为一致，只要保证在死亡间隔内能够接收到至少 1 个 Hello 报文即可。

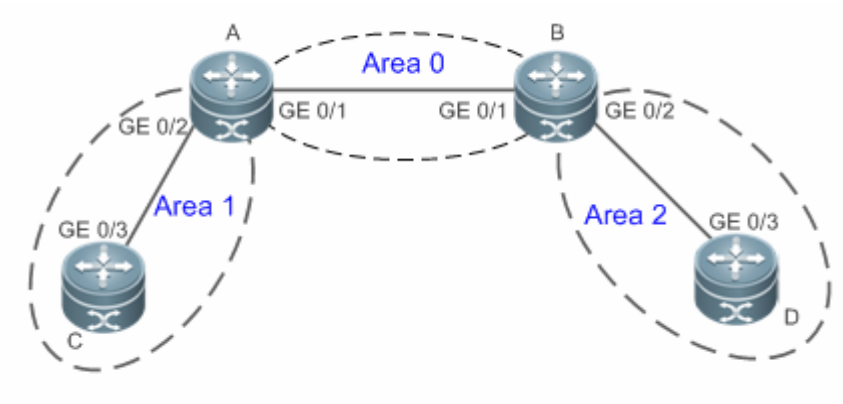
使用 **show ip ospf virtual-links** 命令监控虚链路配置的死亡间隔和 Fast Hello 间隔。

为 Fast Hello 功能引入的 **dead-interval minimal hello-multiplier** 参数和 **hello-interval** 参数不允许同时配置。

配置举例

【网络环境】

图 4-7



【注释】 接口 IP 地址：

A： GE 0/1 192.168.1.1 GE 0/2 192.168.2.1

B： GE 0/1 192.168.1.2 GE 0/2 192.168.3.1

C： GE 0/3 192.168.2.2

D： GE 0/3 192.168.3.2

【配置方法】

- 在所有路由器上配置接口 IP 地址。
- 在所有路由器上启动 IPv4 单播路由功能（该功能默认已开启）。
- 在所有路由器上配置 OSPF 实例、Router ID
- 在所有路由器上配置接口使能 OSPF

A

```
A# configure terminal
A(config)# interface GigabitEthernet 0/1
A(config-if-GigabitEthernet 0/1)# ip address 192.168.1.1 255.255.255.0
A(config-if-GigabitEthernet 0/1)# exit
A(config)# interface GigabitEthernet 0/2
A(config-if-GigabitEthernet 0/2)# ip address 192.168.2.1 255.255.255.0
A(config-if-GigabitEthernet 0/2)# exit
A(config)# router ospf 1
A(config-router)# router-id 192.168.1.1
A(config-router)# network 192.168.1.0 0.0.0.255 area 0
A(config-router)# network 192.168.2.0 0.0.0.255 area 1
```

B

```
B# configure terminal
B(config)# interface GigabitEthernet 0/1
B(config-if-GigabitEthernet 0/1)# ip address 192.168.1.2 255.255.255.0
B(config-if-GigabitEthernet 0/1)# exit
B(config)# interface GigabitEthernet 0/2
```

```
B(config-if-GigabitEthernet 0/2)# ip address 192.168.3.1 255.255.255.0
B(config-if-GigabitEthernet 0/2)# exit
B(config)# router ospf 1
B(config-router)# router-id 192.168.1.2
B(config-router)# network 192.168.1.0 0.0.0.255 area 0
B(config-router)# network 192.168.3.0 0.0.0.255 area 2
```

C

```
C# configure terminal
C(config)# interface GigabitEthernet 0/3
C(config-if-GigabitEthernet 0/3)# ip address 192.168.2.2 255.255.255.0
C(config-if-GigabitEthernet 0/3)# exit
C(config)# router ospf 1
C(config-router)# router-id 192.168.2.2
C(config-router)# network 192.168.2.0 0.0.0.255 area 1
```

D

```
D# configure terminal
D(config)# interface GigabitEthernet 0/3
D(config-if-GigabitEthernet 0/3)# ip address 192.168.3.2 255.255.255.0
D(config-if-GigabitEthernet 0/3)# exit
D(config)# router ospf 1
D(config-router)# router-id 192.168.3.2
D(config-router)# network 192.168.3.0 0.0.0.255 area 2
```

【检验方法】

- 所有路由器上检查 OSPF 邻居正确。
- 所有路由器上检查路由表加载正确。
- D 上 ping 192.168.2.2 正确。

A

```
A# show ip ospf neighbor
OSPF process 1, 2 Neighbors, 2 is Full:
Neighbor ID   Pri   State      Dead Time   Address       Interface
192.168.1.2   1     Full/DR    00:00:40    192.168.1.2   GigabitEthernet 0/1
192.168.2.2   1     Full/BDR   00:00:34    192.168.2.2   GigabitEthernet 0/2

A# show ip route ospf
O IA 192.168.3.0/24 [110/2] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1
```

B

```
B# show ip ospf neighbor
OSPF process 1, 2 Neighbors, 2 is Full:
Neighbor ID   Pri   State      Dead Time   Address       Interface
192.168.1.1   1     Full/BDR   00:00:32    192.168.1.1   GigabitEthernet 0/1
192.168.3.2   1     Full/BDR   00:00:30    192.168.3.2   GigabitEthernet 0/2

B# show ip route ospf
O IA 192.168.2.0/24 [110/2] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1
```

C

```
C# show ip ospf neighbor
OSPF process 1, 1 Neighbors, 1 is Full:
Neighbor ID   Pri   State      Dead Time   Address       Interface
192.168.1.1   1     Full/BDR   00:00:32    192.168.2.1   GigabitEthernet 0/3

C# show ip route ospf
O IA 192.168.1.0/24 [110/2] via 192.168.2.1, 00:19:05, GigabitEthernet 0/3
O IA 192.168.3.0/24 [110/3] via 192.168.2.1, 00:19:05, GigabitEthernet 0/3
```

D

```
D# show ip ospf neighbor
OSPF process 1, 1 Neighbors, 1 is Full:
Neighbor ID   Pri   State      Dead Time   Address       Interface
192.168.1.2   1     Full/BDR   00:00:30    192.168.3.1   GigabitEthernet 0/3

D# show ip route ospf
O IA 192.168.1.0/24 [110/2] via 192.168.3.1, 00:19:05, GigabitEthernet 0/3
O IA 192.168.2.0/24 [110/3] via 192.168.3.1, 00:19:05, GigabitEthernet 0/3

D# ping 192.168.2.2
Sending 5, 100-byte ICMP Echoes to 192.168.2.2, timeout is 2 seconds：
< press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms.
```

常见错误

- IP 单播路由功能被关闭，OSPF 协议无法启用。
- **network** 命令配置的网段范围未包含接口 IP 地址。
- 相连接口使能的区域号不一致。
- 多台路由器上配置了相同的 Router ID，导致 Router ID 冲突。
- 多台路由器上配置了相同的接口 IP 地址，导致 OSPF 网络运行错误。

5.4.2 设置网络类型

配置效果

- 物理网络为 X.25、帧中继、ATM 时，也可以运行 OSPF 协议，提供 IPv4 单播路由服务。

注意事项

- 必须配置 OSPF 基本功能
- 广播网络以组播方式发送 OSPF 报文，自动发现邻居，需要选举 DR 和 BDR。
- P2P 网络以组播方式发送 OSPF 报文，自动发现邻居。
- NBMA 网络以单播方式发送 OSPF 报文，必须手动指定邻居，需要选举 DR 和 BDR。
- P2MP 网络（不携带 **non-broadcast** 参数）以组播方式发送 OSPF 报文，自动发现邻居。
- P2MP 网络（携带 **non-broadcast** 参数）以单播方式发送 OSPF 报文，必须手动指定邻居。

配置方法

↘ 配置接口网络类型

- 可选配置。
- 链路两端路由器都需要配置。

↘ 配置邻居

- 可选配置。若接口的网络类型配置为 NBMA 或者 P2MP（携带 **non-broadcast** 参数），则必须配置。
- 在 NBMA 或者 P2MP（携带 **non-broadcast** 参数）网络两端路由器上配置。

↘ 配置接口优先级

- 可选配置。若需要指定路由器做为 DR 或者禁止路由器做为 DR，需要配置。

- 在被指定为 DR 或者被禁止做为 DR 的路由器上配置。

检验方法

- 通过 show ip ospf interface 查看接口的网络类型正确。

相关命令

配置接口网络类型

【命令格式】 **ip ospf network** { **broadcast** | **non-broadcast** | **point-to-multipoint** [**non-broadcast**] | **point-to-point** }

【参数说明】

broadcast：将接口设定为广播类型。

non-broadcast：将接口设定为 NBMA 类型。

point-to-multipoint [**non-broadcast**]：将接口设定为 P2MP 类型，如果接口不具备广播能力，需携带 non-broadcast 参数。

point-to-point：将接口设定为 P2P 类型。

【命令模式】 接口配置模式

【使用指导】 广播类型要求接口具有广播能力。

P2P 类型要求接口 1 对 1 互联。

NBMA 类型要求全网状连接，所有互联的路由设备必须能够直接通讯。

P2MP 类型无要求。

配置邻居

【命令格式】 **neighbor** *ip-address* [**poll-interval** *seconds*] [**priority** *priority*] [**cost** *cost*]

【参数说明】

ip-address：邻居接口的 IP 地址。。

poll-interval*seconds*：邻居轮询时间间隔，以秒为单位，取值范围：0-2147483647。只有 NBMA 类型支持该参数。

priority*priority*：邻居的优先权值，取值范围：0-255。只有 NBMA 类型支持该参数。

cost*cost*：到每个邻居所要的费用，无缺省值，取值范围：0-65535。只有 P2MP 类型支持该选项。

【命令模式】 OSPF 路由进程配置模式

【使用指导】 必须为 NBMA 类型接口和 P2MP 类型非广播接口指定邻居。邻居的 IP 地址，必须为该邻居接口的主 IP 地址。

在 NBMA 网络上如果邻居路由设备变为不活跃，即在路由设备死亡时间内还没有收到 Hello 报文，OSPF 还会往该邻居发送 Hello 报文，发送 Hello 报文的时间间隔称为轮询间隔。当 OSPF 第一次开始运行时，只向优先权值不为 0 的邻居发送 Hello 报文，这样优先权值设为 0 的邻居就不会参与 DR/BDR 的竞选。等 DR/BDR 产生以后，DR/BDR 会向所有的邻居发送 Hello 报文建立邻居关系。

在 P2MP 非广播网络上，因为不具备广播能力所以无法动态的发现邻居，因此必须使用该命令手工为其配置邻居。此外 P2MP 类型的网络可以通过 cost 选项指定到达每个邻居的花费。

配置接口优先级

【命令格式】 **ip ospf priority** *priority*

【参数说明】 *priority*：设置接口的 OSPF 优先权值，取值范围：0-255。

【命令模式】 接口配置模式

【使用指导】 OSPF 接口的优先权值包含在 hello 报文中。当 OSPF 广播类型网络发生 DR/BDR（指定路由设备 / 备份指定路由设备）竞选时，高优先权值的路由设备，将成为 DR 或 BDR。如果优先权值一样，路由设备标识符高的路由设备将成为 DR 或 BDR。优先权值为 0 的路由设备，不参与 DR/BDR 竞选。

该命令只对 OSPF 广播类型和 NBMA 类型有效。

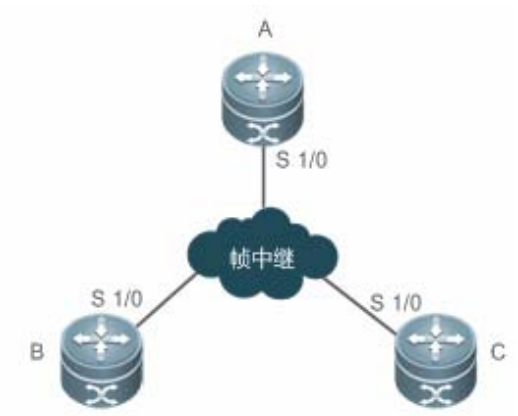
配置举例

以下配置举例，需要基于 OSPF 基本功能进行配置，OSPF 基本功能请参见 1.4.1.配置 OSPF 基本功能的介绍。

配置接口网络类型为 P2MP。

【网络环境】

图 4-8



【注释】 接口 IP 地址：

A： S1/0 192.168.1.2

B： S1/0 192.168.1.3

C： S1/0 192.168.1.4

【配置方法】

- 所有路由器配置接口 IP 地址。略。
- 所有路由器配置 OSPF 基本功能。略。
- 所有路由器上配置接口的网络类型为 P2MP。

A

```
A# configure terminal
A(config)# interface Serial 1/0
A(config-Serial1/0)# encapsulation frame-relay
A(config-Serial1/0)# ip ospf network point-to-multipoint
```

B

```
B# configure terminal
B(config)# interface Serial 1/0
B(config-Serial1/0)# encapsulation frame-relay
B(config-Serial1/0)# ip ospf network point-to-multipoint
```

C

```
C# configure terminal
C(config)# interface Serial 1/0
C(config-Serial1/0)# encapsulation frame-relay
C(config-Serial1/0)# ip ospf network point-to-multipoint
```

【检验方法】 查看接口的网络类型为 P2MP。

```
A# show ip ospf interface Serial 1/0
Serial 1/0 is up, line protocol is up
  Internet Address 192.168.1.2/24, Ifindex 2, Area 0.0.0.1, MTU 1500
  Matching network config: 192.168.1.0/24
  Process ID 1, Router ID 192.168.1.2, Network Type POINTOMULTIPOINT, Cost: 1
  Transmit Delay is 1 sec, State Point-To-Point
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:02
  Neighbor Count is 1, Adjacent neighbor count is 0
  Crypt Sequence Number is 4787
  Hello received 465 sent 466, DD received 8 sent 8
  LS-Req received 2 sent 2, LS-Upd received 8 sent 21
  LS-Ack received 14 sent 7, Discarded 3
```

常见配置错误

- 两端接口配置的网络类型不一致，导致路由学习不正常。
- 网络类型配置为 NBMA，P2MP（携带 **non-broadcast** 参数），但没有指定邻居。

5.4.3 配置路由重分布、缺省路由

配置效果

- 在 OSPF 域内引入其他 AS 域的单播路由，为 OSPF 域内的用户提供到其他 AS 域的单播路由服务。
- 往 OSPF 域内注入一条通往其他 AS 域的默认路由，为 OSPF 域内的用户提供到其他 AS 域的单播路由服务。

注意事项

- 必须配置 OSPF 基本功能

配置方法

配置重分发外部路由

- 可选配置。若在 AS 边界路由器上需要引入 OSPF 域外路由时，需要配置
- 在 AS 边界路由器上配置。

配置生成缺省路由

- 可选配置。若在 AS 边界路由器上需要引入默认路由，使得 OSPF 域内访问其他 AS 域默认通过该边界路由器，则需要配置。
- 在 AS 边界路由器上配置。

检验方法

- OSPF 域内路由器通过 **show ip route** 查看加载了其他 AS 域的单播路由。
- OSPF 域内路由器通过 **show ip route** 查看加载了到达 ASBR 的默认路由。
- 通过 **ping** 命令查看通往其他 AS 域的 IPv4 单播业务正确。

相关命令

配置重分发路由

【命令格式】 **redistribute** { **connected** | **ospf***process-id* | **rip** | **static** }[**match** { **internal** | **external** [**1** | **2**] | **nssa-external** [**1 | 2**] }] [**metric** *metric-value*] [**metric-type** { **1** | **2** }] [**route-map** *route-map-name*] [**subnets**] [**tag***tag-value*]

【参数说明】 **connected**：从直连路由重分布

ospf *process-id*：从 ospf 重分布，通过 *process-id* 指定具体某个 ospf 实例，取值范围：1-65535

rip：从 rip 重分布

static：从静态路由重分布

match：只针对配置重分布 OSPF 路由时使用，用于过滤特定路由进行重分布，默认状态允许所有的 OSPF 路由进行重分布。

metric *metric-value*：设置 OSPF external LSA 的 metric，通过 metric-value 指定 metric 大小，取值范围：0-16777214。

metric-type { 1 | 2 }：设置外部路由类型为 E-1 或 E-2。

route-map *route-map-name*：设置重分布过滤规则。

subnets：可重分布非标准类网络。

tag *tag-value*：设置重分布到 OSPF 内路由的 tag 值，取值范围：0-4294967295。

【配置模式】 OSPF 路由进程配置模式

【使用指导】 配置完该命令后，该路由设备将变为 ASBR，将相应路由信息导入 OSPF 域内，并以 type-5 LSA 广播到域内其他 OSPF 路由设备。

配置重分布 ospf 路由时，不带 match 参数时，默认允许重分布所有子类型的 ospf 路由；而后的第一次配置 match 参数作为初始的 match 参数，重分布时只允许匹配的子类型的路由进行重分布，使用 no 命令恢复 match 参数为默认值。参看举例说明。

配置重分布时，配置 route-map 过滤时，route-map 中的 match 规则是针对重分布的原始参数进行匹配；对于重分布 OSPF，只有重分布的路由满足配置的 match 的规则，才再进行 route-map 的判断。

所关联的 route-map 的 set metric 取值范围应当为<0-16777214>，如果超出该范围，将无法引入路由。

redistribute 命令的 no 形式配置的规则如下：

1．如果 no 命令指定某些参数，则将这些参数恢复缺省配置；

2．如果 no 命令不指定任何参数，则将整个命令删除。

配置导入缺省路由

【命令格式】 **default-information originate** [**always**] [**metric** *metric*] [**metric-type** *type*] [**route-map***map-name*]

【参数说明】 **always**：该关键字使得 OSPF 无条件产生缺省路由，不管本地是否存在缺省路由。

metric *metric*：缺省路由初始的量度值，取值范围：0-16777214。

metric-type*type*：缺省路由的类型。OSPF 外部路由有两种类型：类型 1，不同路由设备上看到的量度值不一样；类型 2，所有路由设备看到的量度值都一样。类型 1 的外部路由比类型 2 可信。

route-map *map-name*：关联的 route-map 的名字，缺省没有关联 route-map。

【配置模式】 OSPF 路由进程配置模式

【使用指导】 当执行 **redistribute** 或者 **default-information** 命令时，OSPF 路由设备会自动变为 ASBR（自治域边界路由设备）。但是 ASBR 不会自动产生缺省路由，并通告给 OSPF 路由域中的所有路由设备。ASBR 产生缺省路由，必须用 **default-information originate** 路由进程配置命令进行配置。

如果选择 always 参数，OSPF 路由进程不管是否存在缺省路由，都会向邻居通告一条外部缺省路由。但是本地路由设备不会显示该缺省路由，要确认是否产生缺省路由，可以用 **show ip ospf database** 观察 OSPF 链路状态数据库，链路标识为 0.0.0.0 的外部链路描述了缺省路由。OSPF 的邻居通过执行 **show ip route** 命令，是可以看到缺省路由的。

外部缺省路由的路由量度值，只能由 **default-information originate** 命令进行定义，不能通过命令 **default-metric** 设置。

OSPF 有两种外部路由，类型 1 外部路由的路由量度会改变，而类型 2 外部路由的路由量度是固定不变。到一个目标网络存在两条并行路径，同样的路由量度，类型 1 会比类型 2 优先级高，所以 **show ip route** 只显示类型 1 那条路由。

Stub 区域中的路由设备是不可以产生外部缺省路由的。

所关联的 route-map 的 set metric 取值范围为 0-16777214，如果超出该范围，将无法引入路由。

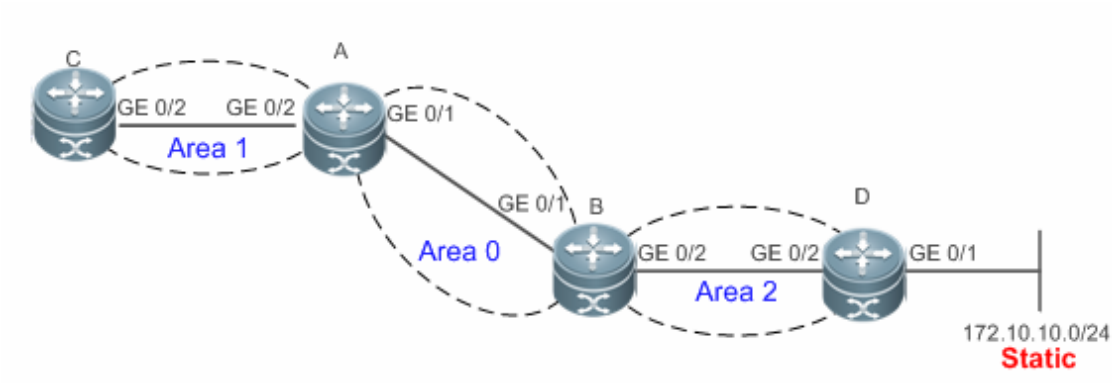
配置举例

以下配置举例，需要基于 OSPF 基本功能进行配置，OSPF 基本功能请参见 1.4.1.配置 OSPF 基本功能的介绍。

配置重分发静态路由

【网络环境】

图 4-9



【注释】 接口 IP 地址：

A：GE 0/1 192.168.1.1 GE 0/2 192.168.2.1

B：GE 0/1 192.168.1.2 GE 0/2 192.168.3.1

C：GE 0/2 192.168.2.2

D：GE 0/1 192.168.6.2 GE 0/2 192.168.3.2

【配置方法】

- 所有路由器配置接口 IP 地址。略。
- 所有路由器配置 OSPF 基本功能。略。
- 路由器 D 上配置引入外部静态路由。

D

```
D# configure terminal
D(config)# ip route 172.10.10.0 255.255.255.0 192.168.6.3
D(config)# router ospf 1
D(config-router)# redistribute static subnets
```

【检验方法】

- 路由器 D 上使用 **show ip ospf database external brief** 查看有外部路由对应的 LSA 生成。
- 路由器 C 上使用 **show ip route ospf** 查看已经加载引入的外部静态路由。

D

```
D# show ip ospf database external brief

            OSPF Router with ID (192.168.22.30) (Process ID 1)

                AS External Link States


Link ID         ADV Router      Age  Seq#       CkSum    Route                Tag
172.10.10.0     192.168.22.30   11   0x80000001 0xa4bb   E2 172.10.10.0/24    0
```

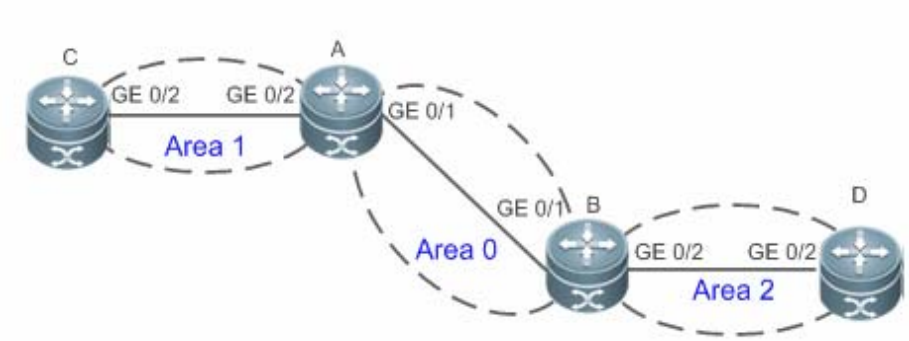
C

```
C# show ip route ospf

O E2 172.10.10.0/24 [110/20] via 192.168.2.1, 00:18:03, GigabitEthernet 0/2
```

配置缺省路由

【网络环境】

图 4-10



【注释】 接口 IP 地址：

A：GE 0/1 192.168.1.1 GE 0/2 192.168.2.1

B：GE 0/1 192.168.1.2 GE 0/2 192.168.3.1

C：GE 0/2 192.168.2.2

D：GE 0/2 192.168.3.2

【配置方法】

- 所有路由器配置接口 IP 地址。略。
- 所有路由器配置 OSPF 基本功能。略。
- 路由器 D 上配置缺省路由。

D

```
D# configure terminal

D(config)# router ospf 1

D(config-router)# default-information originate always
```

【检验方法】

- 在路由器 D 上使用 **show ip ospf database external brief** 查看有缺省路由对应的 LSA。
- 在路由器 C 上使用 **show ip route ospf** 查看有 ospf 缺省路由。

D

```
D# show ip ospf database external brief

            OSPF Router with ID (192.168.22.30) (Process ID 1)

                AS External Link States


Link ID         ADV Router      Age  Seq#       CkSum    Route                Tag
0.0.0.0         192.168.22.30   565  0x80000002 0xa190   E2 0.0.0.0/0         1
```

C

```
C# show ip route ospf

O E2 0.0.0.0/0 [110/20] via 192.168.2.1, 00:18:03, GigabitEthernet 0/2
```

常见配置错误

- **redistribute** 命令的 **subnets** 参数未配置，导致子网路由未被引入。
- 多台设备配置了 default-information originate always，造成路由环路。
- 在 Stub 区域配置路由重分布，无法引入路由。

5.4.4 设置Stub、NSSA区域

配置效果

- 将末梢区域设置为 Stub 区域，有助于减少路由信息的交互，缩小路由表规模，增强路由稳定性。

注意事项

- 必须配置 OSPF 基本功能
- 骨干区域、传输区域不能设置为 Stub 区域、NSSA 区域。
- Stub 区域内路由器不能引入外部路由，NSSA 区域内路由器可以引入外部路由。

配置方法

↘ 配置 Stub 区域

- 可选配置。若希望减小区域内路由器的路由表规模，需要配置。
- 必须在该区域内的所有路由器上配置该区域为 Stub 区域。

↘ 配置 Nssa 区域

- 可选配置。若希望减小区域内路由器的路由表规模，又希望本区域可以引入 OSPF 域外路由，需要配置。

- 必须在该区域内的所有路由器上配置该区域为 NSSA 区域。

检验方法

检验 Stub 区域

- 在 Stub 区域内部的路由器上，通过 **show ip route** 查看路由器没有加载外部明细路由。

检验 Nssa 区域

- 在 NSSA 区域内部的路由器上，通过 **show ip ospf database** 查看引入的外部路由生成了 7 类 LSA。
- 在骨干区域内部的路由器上，通过 **show ip route** 查看路由器加载了从 NSSA 区域引入的外部路由。

相关命令

配置 Stub 区域

【命令格式】 **area** *area-id* **stub** [**no-summary**]

【参数说明】 *area-id* *：* Stub 区域的区域号。

no-summary：阻止 ABR 往残域发送网络摘要链路通告，此时残域可称为全残域。只有 ABR 才需要配置该参数。

【配置模式】 OSPF 路由进程配置模式

【使用指导】 OSPF 残域内所有的路由设备都必须执行 area stub 命令。ABR 只向残域发送三种链路状态描述(LSA)：1）类型 1，路由设备 LSA；2）类型 2，网络 LSA；3）类型 3，网络摘要 LSA。从路由表角度看，残域中的路由设备只能学习到 OSPF 路由域内部的路由，包括由 ABR 产生的内部缺省路由。残域的路由设备不能学习到 OSPF 路由域外部的路由。

如果需要配置全残域，只需在 ABR 上执行 area stub 命令时，选择 no-summary 关键字。全残域的路由设备只能学到本区域内的路由，以及 ABR 产生的内部缺省路由。

将一个 OSPF 区域设置为残域有两条命令 area stub 和 area default-cost。所有连接到残域的路由设备上，都必须配置 area stub 命令，但 area default-cost 命令只需要在 Stub 区域的 ABR 上配置。area default-cost 命令定义了内部缺省路由的初始花费（即量度）。

配置 Nssa 区域

【命令格式】 **area** *area-id* **nssa** [**no-redistribution**] [**default-information-originate** [**metric** *value*] [**metric-type** *type*]] [**no-summary**] [**translator** [**stability-interval** *seconds* | **always**]]

【参数说明】 *area-id* *：* NSSA 区域的区域号。

no-redistribution：当该路由设备是一个 NSSA ABR 时，如果用户只想用重分布命令将路由信息导入普通区间而不让它进入 NSSA 区间时，可以选上该选项。

default-information-originate：产生缺省的类型 7 的 LSA 进入 NSSA 区间，该选项只在 NSSA ABR 或者 ASBR 上有效。

metric*value* *：*设置产生的缺省 LSA 的度量值。metric 取值范围 0-16777214，缺省值 1。

metric-type*type* *：*设置产生的缺省 LSA 的路由类型。type 取值 1 或 2。1 表示 N-1；2 表示 N-2。缺省值 2。

no-summary：阻止 NSSA 的边界路由设备(ABR)发送 summary LSAs（Type-3 LSA）。

translator：配置 NSSA 的边界路由设备(ABR)转换者。

stability-interval*seconds*：配置 NSSA 的边界路由设备(ABR)由转换者变为非转换者后保持的稳定间隔。单位：秒。缺省值为 40。取值范围：0- 2147483647。

always：配置当前 NSSA 的边界路由设备(ABR)总是作为转换者角色。缺省为备选转换者。

【配置模式】 OSPF 路由进程配置模式

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

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

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

另外 **area default-cost** 用在连接在该 NSSA 区域的 ABR/ASBR 上。该命令配置 ABR/ASBR 发送到 NSSA 区域的缺省路由的花费值。缺省情况下，发送到 NSSA 缺省路由的花费值为 1。

如果一个 NSSA 区域有两个（或者两个以上）ABR，缺省情况下，选举路由设备标识最大的 ABR 设备作为 Type-7 转 Type-5 的转换者；如果希望当前设备总是作为 Type-7 转 Type-5 的转换者 ABR，使用 translator always 参数。

如果当前设备的转换者角色被其它 ABR 取代，在 stability-interval 时间内将继续保持转换能力，如果在这段时间内没有重新成为转换者，stability-interval 到期后由 Type-7 转换为 Type-5 的 LSA 将从自治域中被清除。

为防止路由环路，由 Type-7 汇聚生成的 Type-5 LSA 将在当前设备失去转换者角色后立即被清除，而无需等待 stability-interval 到期。

同一 NSSA 区域中，建议仅在一台 ABR 配置 translator always 参数。

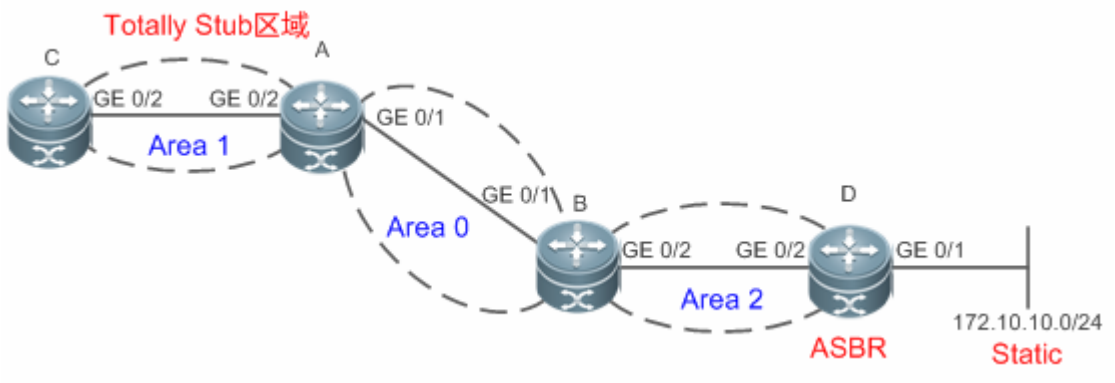
配置举例

以下配置举例，需要基于 OSPF 基本功能进行配置，OSPF 基本功能请参见“配置 OSPF 基本功能”的介绍。

配置 Stub 区域

【网络环境】

图 4-11



【注释】 接口 IP 地址：

A：GE 0/1 192.168.1.1 GE 0/2 192.168.2.1

B：GE 0/1 192.168.1.2 GE 0/2 192.168.3.1

C：GE 0/2 192.168.2.2

D：GE 0/1 192.168.6.2 GE 0/2 192.168.3.2

【配置方法】

- 所有路由器配置接口 IP 地址。略。
- 所有路由器配置 OSPF 基本功能。略。
- 路由器 D 上配置引入外部静态路由。
- 路由器 A、C 上区域 1 配置成 Stub 类型。

D

```
D# configure terminal
D(config)# router ospf 1
D(config-router)# redistribute static subnets
```

A

```
A# configure terminal
A(config)# router ospf 1
A(config-router)# area 1 stub no-summary
```

C

```
C# configure terminal
C(config)# router ospf 1
C(config-router)# area 1 stub
```

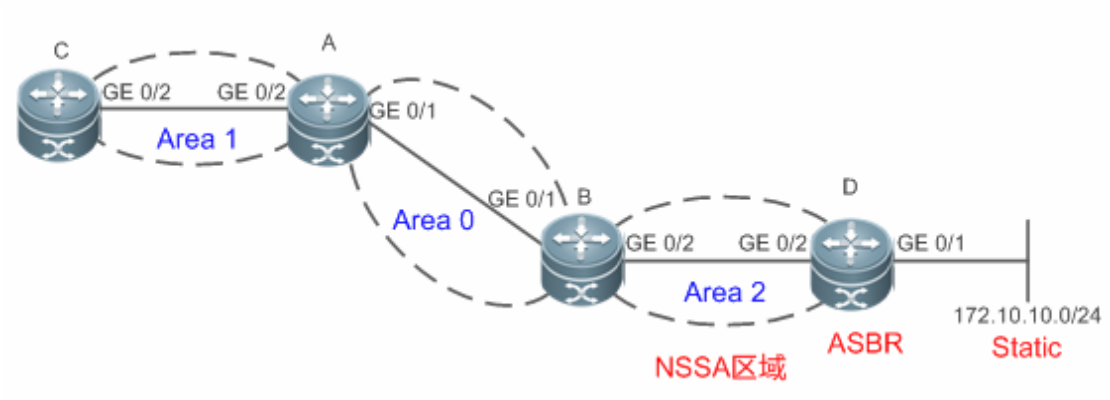
【检验方法】 在路由器 C 上使用 **show ip route ospf** 查看路由表，只有一条默认区间路由，没有 D 引入的外部静态路由

```
C# show ip route ospf
O*IA 0.0.0.0/0 [110/2] via 192.168.2.1, 00:30:53, GigabitEthernet 0/2
```

配置 NSSA 区域。

【网络环境】

图 4-12



【注释】 接口 IP 地址：

A：GE 0/1 192.168.1.1 GE 0/2 192.168.2.1

B：GE 0/1 192.168.1.2 GE 0/2 192.168.3.1

C：GE 0/2 192.168.2.2

D：GE 0/1 192.168.6.2 GE 0/2 192.168.3.2

【配置方法】

- 所有路由器配置接口 IP 地址。略。
- 所有路由器配置 OSPF 基本功能。略。
- 路由器 D 上配置引入外部静态路由。
- 路由器 B、D 上区域 2 配置成 NSSA。

B

```
B# configure terminal
B(config)# router ospf 1
B(config-router)# area 2 nssa
```

D

```
D# configure terminal
D(config)# ip route 172.10.10.0 255.255.255.0 192.168.6.2
D(config)# router ospf 1
D(config-router)# redistribute static subnets
D(config-router)# area 2 nssa
```

【检验方法】

- 路由器 D 上查看生成 172.10.10.0/24 的 7 类 LSA
- 路由器 B 上查看 172.10.10.0/24 同时存在 5 类和 7 类 LSA
- 路由器 B 上查看生成了 172.10.10.0/24 的 N2 类型的路由。

D

```
D# show ip ospf database nssa-external
            OSPF Router with ID (192.168.6.2) (Process ID 1)
                NSSA-external Link States (Area 0.0.0.1 [NSSA])
  LS age: 61
```

```
  Options: 0x8 (-|-|-|-|N/P|-|-|-)
  LS Type: AS-NSSA-LSA
  Link State ID: 172.10.10.0 (External Network Number For NSSA)
  Advertising Router: 192.168.6.2
  LS Seq Number: 80000001
  Checksum: 0xc8f8
  Length: 36
  Network Mask: /24
        Metric Type: 2 (Larger than any link state path)
        TOS: 0
        Metric: 20
        NSSA: Forward Address: 192.168.6.2
        External Route Tag: 0
```

B

```
B# show ip ospf database nssa-external
            OSPF Router with ID (192.168.3.1) (Process ID 1)
                NSSA-external Link States (Area 0.0.0.1 [NSSA])
  LS age: 314
  Options: 0x8 (-|-|-|-|N/P|-|-|-)
  LS Type: AS-NSSA-LSA
  Link State ID: 172.10.10.0 (External Network Number For NSSA)
  Advertising Router: 192.168.6.2
  LS Seq Number: 80000001
  Checksum: 0xc8f8
  Length: 36
  Network Mask: /24
        Metric Type: 2 (Larger than any link state path)
        TOS: 0
        Metric: 20
        NSSA: Forward Address: 192.168.6.2
        External Route Tag: 0
B# show ip ospf database external
```

```
          OSPF Router with ID (192.168.3.1) (Process ID 1)

              AS External Link States

 LS age: 875

 Options: 0x2 (-|-|-|-|-|-|E|-)

 LS Type: AS-external-LSA

 Link State ID: 172.10.10.0 (External Network Number)

 Advertising Router: 192.168.3.1

 LS Seq Number: 80000001

 Checksum: 0xd0d3

 Length: 36

 Network Mask: /24

       Metric Type: 2 (Larger than any link state path)

       TOS: 0

       Metric: 20

       Forward Address: 192.168.6.2

       External Route Tag: 0


B# show ip route ospf

O N2  172.10.10.0/24 [110/20] via 192.168.3.2, 00:06:53, GigabitEthernet 0/2
```

常见配置错误

- 同一区域中的设备，区域类型配置不一致
- 在 Stub 区域中配置路由重分布，将无法加入外部路由

5.4.5 配置路由汇聚

配置效果

- 明细路由汇聚，减少路由信息的交互，缩小路由表规模，增强路由稳定性。
- 屏蔽或者过滤路由。

注意事项

- 必须配置 OSPF 基本功能
- 汇总路由的地址范围有可能超出路由表中实际的网络范围，如果数据发往汇总范围内不存在的网络，将有可能发生路由环路或加重路由设备的处理负担。为阻止这种情况的发生，需要向路由表中添加一条 discard 路由屏蔽或者过滤路由。

配置方法

配置区间路由汇聚

- 可选配置。对 OSPF 区域的路由进行汇聚时，需要配置。
- 若无特殊要求，应在被汇聚路由所在区域的 ABR 上配置。

配置外部路由汇聚

- 可选配置。对域外的路由进行汇聚时，需要配置。
- 若无特殊要求，应在引入被汇聚路由的 ASBR 上配置。

检验方法

通过 **show ip route ospf** 查看明细路由不存在，只有汇聚后的路由。

相关命令

配置区间路由汇聚

【命令格式】 **area** *area-id* **range** *ip-address net-mask* [**advertise** | **not-advertise**] [**cost** *cost*]

【参数说明】 *area-id*：指定要注入汇聚路由的 OSPF 区域号。区域号可以是一个十进制整数值，也可以是一个 IP 地址。

ip-address net-mask：定义汇聚路由的网段。

advertise | **not-advertise**：定义是否要公布该汇聚路由。

cost *cost*：设置汇聚路由的度量值，取值范围：0-16777215。

【命令模式】 OSPF 路由进程配置模式

【使用指导】 该命令只能在 ABR 上执行有效，用来将一个区域的多个路由合并或汇聚成一条路由，然后通告到其它区域去。路由信息的合并行为只发生在区域边界，区域内部路由设备上看到的都是具体的路由信息，但其它区域的设备只能看到一条汇聚路由。并且可以通过设置 advertise 和 not-advertise 选项来决定是否公布这个汇聚范围，起到屏蔽和过滤的作用，缺省是向外公布。可以通过 cost 选项来设置汇聚路由的度量值。

可以定义多个区域路由汇聚命令，这样整个 OSPF 路由域的路由将得到简化，特别是网络规模大时，会提高网络转发性能。

当配置了多条汇总，并且项目直接有包含关系的时候，路由是根据最长匹配原则确定被汇总的 area range 的。

配置外部路由汇聚

【命令格式】 **summary-address** *ip-address net-mask* [**not-advertise** | **tag** *value*]

【参数说明】 *ip-address*：汇聚路由的 IP 地址。

net-mask：汇聚路由的网络掩码。

not-advertise：不公告汇聚的路由，若未配置则为公告。

tag*value*：设置汇聚路由的 tag 值，取值范围：0-4294967295。

【命令模式】 OSPF 路由进程配置模式

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

area range 汇聚的是 OSPF 区域之间路由，而 **summary-address** 汇聚的是 OSPF 路由域的外部路由。

summary-address 命令配置在 NSSA 的 ABR 转换者上时，对重分布的路由及 LSA 从 7 类转 5 类的路由进行汇聚，而配置在 ASBR（非 NSSA 的 ABR 转换者）时，只对重分布的路由进行汇聚。

配置 Discard Route

【命令格式】 **discard-route** { **internal** | **external** }

【参数说明】 **internal**：允许添加区间路由汇聚命令 area range 生成的 discard 路由。

external：允许添加外部路由汇聚命令 summary-address 生成的 discard 路由。

【命令模式】 OSPF 路由进程配置模式

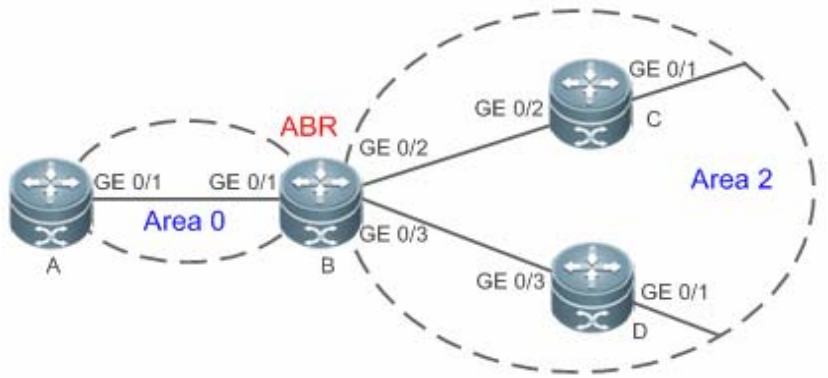
【使用指导】 在路由汇聚时，汇聚后的范围有可能超出路由表中实际的网络范围，如果数据发往汇聚范围内不存在的网络，将有可能发生路由环路或加重路由设备的处理负担。为阻止这种情况的发生，需要在 ABR 或 ASBR 添加一条 discard 路由到路由表。该路由自动生成，并且不会被传播。

配置举例

以下配置举例，需要基于 OSPF 基本功能进行配置，OSPF 基本功能请参见前文。

【配置方法】

图 4-13



【注释】 接口 IP 地址：

A： GE0/1 192.168.1.1

B： GE0/1 192.168.1.2 GE0/2 172.16.2.1 GE0/3 172.16.3.1

C： GE0/2 172.16.2.2 GE0/1 172.16.4.2

D： GE0/2 172.16.3.2 GE0/1 172.16.5.2

【配置方法】

- 所有路由器配置接口 IP 地址。略。
- 所有路由器配置 OSPF 基本功能。略。
- 路由器 B 上配置将区域 2 路由汇聚。

B

```
B# configure terminal
B(config)# router ospf 1
B(config-router)# area 2 range 172.16.0.0 255.255.0.0
```

【检验方法】 路由器 A 查看路由表，生成 172.16.0.0/16 表项。

A

```
A# show ip route ospf
O IA 172.16.0.0/16 [110/2] via 192.168.1.2, 00:01:04, GigabitEthernet 0/1
```

常见配置错误

- 在非 ABR 设备上配置 **area range**，无法进行区间路由汇聚。

5.4.6 配置路由过滤

配置效果

- 被过滤掉的路由不能被加载到路由表或被传播给邻居，网络内用户将无法访问指定的目的网络。

注意事项

- 必须配置 OSPF 基本功能.
- 通过 **distribute-list in** 过滤只影响本地路由转发，不影响 LSA 计算路由。因此，如果确定需要在 ABR 上配置过滤，则由于 LSA 仍然可以计算出路由，仍会生产 Type-3 LSA 往其他区域通告，这将导致黑洞路由存在。这时可以在 ABR 上使用 **area filter-list** 或 **area range** 带 not-advertise 选项来避免产生黑洞路由。

配置方法

↘ 配置区间路由过滤

- 可选配置。若限制用户访问 OSPF 某个区域的网络，建议配置。
- 若无特殊要求，应在被过滤路由所在区域的 ABR 上配置。

↘ 配置重分布路由过滤

- 可选配置。ASBR 引入外部路由时，如果需要对引入的外部路由进行过滤，必须配置。
- 若无特殊要求，应在引入被过滤外部路由的 ASBR 上配置。

↘ 配置对学习的路由过滤

- 可选配置。若需要限制用户访问指定的目的网络，必须配置。
- 若无特殊要求，应在需要过滤的路由器上配置该功能。

检验方法

- 通过 **show ip route** 查看路由器没有加载被过滤的路由。
- 通过 **ping** 命令确认指定的目的网络无法访问。

相关命令

配置被动接口

【命令格式】 **passive-interface** { **default** | *interface-type interface-number* | *interface-type interface-numberip-address*}

【参数说明】 *interface-type interface-number*：要配置为被动接口的接口。

default：该选项表示将所有接口设置为被动接口。

interface-type interface-numberip-address：指定接口下的地址为被动地址。

【命令模式】 OSPF 路由进程配置模式

【使用指导】 为了防止网络中的其他路由设备动态的学习到本路由设备的路由信息 ,可以将本路由设备的指定网络接口设为被动接口或者指定网络接口下的 IP 地址为被动地址。

配置 lsa 更新报文过滤功能

【命令格式】 **ip ospf database-filter all out**

【参数说明】 -

【命令模式】 接口配置模式

【使用指导】 要阻止在某个接口上发送 LSA 的更新报文时，可以在该接口上打开该功能，打开该功能后，本设备将不向邻居通告 LSA 更新报文，但仍然同邻居建立邻接关系并接收邻居发来的 LSA 信息。

配置区间路由过滤

【命令格式】 **area** *area-id* **filter-list** {**access***acl-name*| **prefix** *prefix-name*} {**in** | **out**}

【参数说明】 *area-id*：区域号。

access *acl-name*：关联 ACL。

prefix *prefix-name*：关联 prefix list。

in | **out**：设置该条件应用于进入|发出该区的路由。

【命令模式】 OSPF 路由进程配置模式

【使用指导】 该命令只能在 ABR（区域边界路由设备）上进行配置。

当需要在该 ABR 上配置不同区域之间路由学习的过滤条件时，使用本命令。

配置重分布路由过滤

【命令格式】 **distribute-list** { [*access-list-number* | *name*] | **prefix** *prefix-list-name* } **out** [**connected** | **ospf** *process-id* | **rip** | **static**]

【参数说明】 *access-list-number* | *name*：使用 acl 过滤规则。

prefix *prefix-list-name*：使用 prefix-list 过滤规则。**connected | ospf** *process-id* | **rip** | **static**：待过滤路由的来源。

【命令模式】 OSPF 路由进程配置模式

【使用指导】 **distribute-list out** 与 **redistribute route-map** 命令类似，对从其他协议重分布到 OSPF 中的路由进行过滤，但它本身不执行路由重分布，一般与 **redistribute** 命令配合使用。ACL 过滤规则和 prefix-list 过滤规则不能在该配置中共存，即若对某一来源的路由使用 ACL 过滤规则，则不能再配置 prefix-list 进行过滤。

配置对学习的路由过滤

【命令格式】 **distribute-list** { [*access-list-number* | *name*] | **prefix***prefix-list-name* [**gateway** *prefix-list-name*] | **route-map** *route-map-name* } **in** [*interface-typeinterface-number*]

【参数说明】 *access-list-number* | *name*：使用 acl 过滤规则。

gateway*prefix-list-name*：使用 gateway 过滤规则。

prefix*prefix-list-name*：使用 prefix-list 过滤规则。

route-map *route-map-name*：使用 route-map 过滤规则。

interface-type interface-number：配置只针对某个接口进行 LSA 路由过滤。

【命令模式】 OSPF 路由进程配置模式

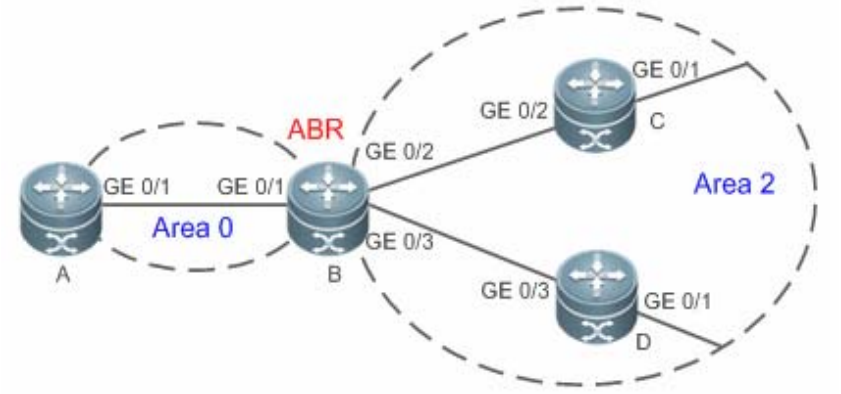
【使用指导】 对收到的 LSA 计算出的路由进行过滤，满足过滤条件的路由才能用于转发。它并不会影响链路状态数据库，对邻居的路由表也不会产生任何影响。ACL 过滤规则、prefix-list 过滤规则和 route-map 过滤规则不能在该配置中共存，即若对指定接口使用 ACL 过滤规则，则不能再对该接口配置 prefix-list 进行过滤或 route-map 过滤规则。

配置举例

以下配置举例，需要基于 OSPF 基本功能进行配置，OSPF 基本功能请参见 1.4.1.配置 OSPF 基本功能的介绍。

【网络环境】

图 4-13



【注释】 接口 IP 地址：

A： GE0/1 192.168.1.1

B： GE0/1 192.168.1.2 GE0/2 172.16.2.1 GE0/3 172.16.3.1

C： GE0/2 172.16.2.2 GE0/3 172.16.4.2

D： GE0/2 172.16.3.2 GE0/3 172.16.5.2

【配置方法】
- 所有路由器配置接口 IP 地址。略。
- 所有路由器配置 OSPF 基本功能。略。
- 路由器 A 配置路由过滤。

A

```
A# configure terminal
A(config)# access-list 3 permit host 172.16.5.0
A(config)# router ospf 1
A(config-router)# distribute-list 3 in GigabitEthernet 0/1
```

【检验方法】
- 路由器 A 检查路由表，只有加载 172.16.5.0/24 表项。

A

```
A# show ip route ospf
O   172.16.5.0/24 [110/2] via 192.168.1.2, 10:39:40, GigabitEthernet 0/1
```

常见配置错误

- 通过 **distribute-list in** 过滤只影响本地路由转发，不影响 LSA 计算路由。因此，如果确定需要在 ABR 上配置过滤，则由于 LSA 仍然可以计算出路由，仍会生产 Type-3 LSA 往其他区域通告，这将导致黑洞路由存在。

5.4.7 修改路由代价、管理距离

配置效果

- 改变 OSPF 路由，使流量经过或避开某些节点。
- 改变路由器选择各类路由的顺序，使 OSPF 路由的优先级提高或降低。

注意事项

- 必须配置 OSPF 基本功能
- 如果用命令 **ip ospf cost** 设置了接口的 cost，则将覆盖自动代价算出的 cost。

配置方法

↘ 配置参考带宽

- 可选配置。
- 路由器连接不同带宽的线路，若希望优先选择带宽大的线路，建议配置。

↘ 配置接口 cost 值

- 可选配置。
- 路由器连接多条线路，若希望手动指定优先的线路，建议配置。

配置重分布缺省度量

- 可选配置。
- 在 ASBR 上引入域外路由时，若需要指定域外路由的代价，必须配置。

配置最大度量值

- 可选配置。。
- 路由器重启过程中以及重启刚完成的一段时间内，路由器可能还不稳定，用户的数据流量转发不希望经过该路由器，此时建议配置。

配置管理距离

- 可选配置。
- 在同时运行多种单播路由协议的路由器上，若希望改变 OSPF 路由的优先级，必须配置。

检验方法

- 通过 **show ip ospf interface** 查看接口的代价正确
- 通过 **show ip route** 查看 ASBR 引入的外部路由的代价正确
- 重启路由器，在指定的一段时间内，数据流量转发不经过重启的路由器

相关命令

配置参考带宽

【命令格式】 **auto-cost reference-bandwidth** *ref-bw*

【参数说明】 *ref-bw*：参考带宽值。以 Mbps 为单位， 范围: 1-4294967。

【命令模式】 OSPF 路由进程配置模式

【使用指导】 缺省情况下，OSPF 接口 cost 值等于自动代价参考值/接口带宽。

使用 auto-cost 命令自动代价参考值。缺省值 100Mbps。

使用 bandwidth 命令设置接口带宽。

几种典型线路的 OSPF 接口 cost 缺省值为：

64K 串行线路，cost 为 1562；

E1 线路，cost 为 48；

10M 以太网，cost 为 10；

100M 以太网，cost 为 1。

如果用命令 ip ospf cost 设置了接口的 cost，则将覆盖自动代价算出的 cost。

配置接口 cost 值

【命令格式】 **ip ospf cost** *cost*

【参数说明】 *cost*：OSPF 接口的花费值，取值范围：0-65535。

【命令模式】 接口配置模式

【使用指导】 缺省情况下，OSPF 接口 cost 值等于自动代价参考值/接口带宽。

使用 auto-cost 命令自动代价参考值。缺省值 100Mbps。

使用 bandwidth 命令设置接口带宽。

几种典型线路的 OSPF 接口 cost 缺省值为：

64K 串行线路，cost 为 1562；

E1 线路，cost 为 48；

10M 以太网，cost 为 10；

100M 以太网，cost 为 1。

如果用命令 ip ospf cost 设置了接口的 cost，则将覆盖自动代价算出的 cost

配置 Stub/NSSA 区域缺省路由的 cost 值

【命令格式】 **area** *area-id* **default-cost***cost*

【参数说明】 *area-id*：Stub 区域或 NSSA 的区域号。

cost：注入 Stub 区域或者 NSSA 的缺省汇聚路由的花费值，取值范围：0-16777215。

【命令模式】 OSPF 路由进程配置模式

【使用指导】 该命令只有在 Stub 区域的 ABR 或 NSSA 区域的 ABR/ASBR 上配置才能生效。

Stub 区域的 ABR 或 NSSA 区域的 ABR/ASBR 设备允许在 Stub 或者 NSSA 区域中通告一个表示缺省路由的 LSA，用户可以通过 **area default-cost** 命令修改通告的 LSA 的花费值。

配置重分布缺省度量

【命令格式】 **default-metric** *metric*

【参数说明】 *metric*：定义 OSPF 重分布路由的缺省量度值，取值范围：1-16777214。

【命令模式】 OSPF 路由进程配置模式

【使用指导】 **default-metric** 命令必须与 **redistribute** 路由进程配置命令配合使用，可以修改所有重分布路由的初始化量度值。

default-metric 命令的设置，对以 **default-information originate** 方式注入 OSPF 路由域的外部路由不起作用。

配置最大度量值

【命令格式】 **max-metric router-lsa** [**external-lsa** [*max-metric-value*]] [**include-stub**] [**on-startup**[*seconds*]] [**summary-lsa** [*max-metric-value*]]

【参数说明】 **router-lsa**：配置 Router LSA 中的非 stub links 的度量为最大值（0xFFFF）。

external-lsa：配置路由设备使用最大度量值取代外部 LSA（包括 Type-5 和 Type-7）的度量值。

max-metric-value：LSA 的最大度量值。缺省值为 16711680。取值范围：1-16777215。

include-stub：配置路由设备通告 Router LSA 中的 stub links 为最大度量值。

on-startup：配置路由设备在启动时通告最大度量。

seconds：通告最大度量的指定时间间隔。缺省值为 600s。取值范围：5-86400。

summary-lsa：配置路由设备使用最大度量值取代汇总 LSA（包括 Type-3 和 Type-4）的度量值。

【命令模式】 OSPF 路由进程配置模式

【使用指导】 使能命令 **max-metric router-lsa** 后，路由设备生成的 Router LSA 中的非 stub links 的度量将被设置为最大值（0xFFFF）。在用户取消该配置，或者定时器到期后，恢复链路的正常度量。

缺省情况下，当使能该命令，stub links 仍将通告普通度量值，即出接口代价值，如果配置了 **include-stub** 参数，stub links 将通告为最大度量值；

作为 ABR 设备，如果不希望传输区间流量则使用 **summary-lsa** 参数设置汇总 LSA 为最大度量值；

作为 ASBR 设备，如果不希望传输外部流量则使用 **external-lsa** 参数设置外部 LSA 为最大度量值。

max-metric router-lsa 命令通常在以下场景使用：

重启设备。当设备重启，IGP 协议通常更快收敛，其它设备试图通过新启动的设备转发流量。如果当前设备仍然在构建 BGP 路由表，部分 BGP 路由还没有被学习到，发往这些网络的报文将被丢弃。这种情况可以使用 **on-startup** 参数设置一定的延时，启动后等待定时器到期后再开始作为传输节点。

将设备加入网络但不用于传输流量。将设备加入网络，如果存在备选路径，则当前设备不用于传输流量；如果不存在备选路径，则当前设备仍然用于传输流量。

将设备优雅的从网络中移除。通过使能该命令，当前设备通告所有最大度量值，这样就能够在设备关闭前，使网络中的其它设备选择备份路径传输流量。

在旧版本 OSPF 实现（RFC 1247 或更早的版本）中，LSA 中最大度量（0xFFFF）的 links 不参与 SPF 计算，即没有流量发往生成这些 LSAs 的路由设备。

配置兼容 RFC1583

【命令格式】 **commpatible rfc1583**

【参数说明】 -

【命令模式】 OSPF 路由进程配置模式

【使用指导】 当存在多条到达 ASBR 或外部路由转发地址的路径时，RFC1583 与 RFC2328 定义了不同的选路规则。配置兼容 RFC1583 时，优先选择骨干区域的区域内路径或区域间路径；不兼容 RFC1583 时，优先选择非骨干区域的区域内路径。

配置管理距离

【命令格式】 **distance** { *distance* | **ospf** { [**intra-area** *distance*] [**inter-area** *distance*] [**external** *distance*] } }

【参数说明】 *distance*：设置路由管理距离，取值范围：1-255。

intra-area *distance*：设置区内路由管理距离，取值范围：1-255。

inter-area *distance*：设置区间路由管理距离，取值范围：1-255。

external *distance*：设置外部路由管理距离，取值范围：1-255。

【命令模式】 OSPF 路由进程配置模式

【使用指导】 若要指定 OSPF 不同类型路由对应不同管理距离时，用此命令。

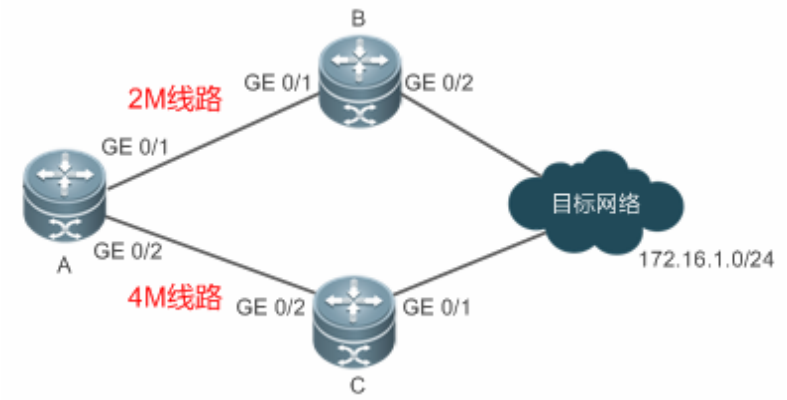
配置举例

以下配置举例，需要基于 OSPF 基本功能进行配置，OSPF 基本功能请参见前文。

配置接口 cost 值

【网络环境】

图 4-14



【注释】 接口 IP 地址：

A：GE0/1 192.168.1.1 GE0/2 192.168.2.1

B：GE0/1 192.168.1.2 GE0/2 192.168.3.2

C：GE0/1 192.168.4.2 GE0/2 192.168.2.2

【配置方法】

- 所有路由器配置接口 IP 地址。略。
- 所有路由器配置 OSPF 基本功能。略。
- 路由器 A 配置接口代价。

A

```
A# configure terminal
A(config)# interface GigabitEthernet 0/1
A(config-if-GigabitEthernet 0/1)# ip ospf cost 10
A(config)# interface GigabitEthernet 0/2
A(config-if-GigabitEthernet 0/2)# ip ospf cost 20
```

【检验方法】 路由器 A 检查路由表，172.16.1.0/24 的最优路径下一跳是路由器 B。

A

```
A# show ip route ospf
O E2 172.16.1.0/0 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1
```

常见配置错误

- ip ospf cost 配置为 0，路由计算可能会出错，比如计算出路由环路；

5.4.8 启动认证功能

配置效果

- 所有接入 OSPF 网络的路由器都必须经过认证，保证 OSPF 协议的稳定性和抗入侵性。

注意事项

- 必须配置 OSPF 基本功能
- 在区域上配置认证，则在属于此区域的所有接口上生效。
- 区域和接口同时配置认证，接口配置优先生效。

配置方法

配置区域认证类型

- 可选配置。如果要求同一区域内所有接口启用相同的认证类型，建议配置。
- 若路由器接入需要认证的网络，需要配置。

配置接口认证类型

- 可选配置。如果要求同一区域内不同接口启用不同的认证类型，必须配置。
- 若路由器接入需要认证的网络，需要配置。

配置接口明文认证密钥

- 可选配置。
- 若路由器接入需要明文认证的网络，需要配置。

配置接口 md5 认证密钥

- 可选配置。MD5 认证安全性较高，建议用户使用 MD5 认证。明文认证与 MD5 认证必须配置一个。
- 若路由器接入需要 MD5 认证的网络，需要配置。

检验方法

- 路由器配置不同的认证密钥，通过 **show ip ospf neighbor** 查看 OSPF 邻居为空
- 路由器配置相同的认证密钥后，通过 **show ip ospf neighbor** 查看 OSPF 邻居正确

相关命令

配置区域认证类型

【命令格式】 **area** *area-id* **authentication** [**message-digest**]

【参数说明】 *area-id*：指定要启用 OSPF 认证的区域号。区域号可以是一个十进制整数值，也可以是一个 IP 地址。

message-digest：采用 MD5（message digest 5）认证模式。

【配置模式】 OSPF 路由配置模式

【使用指导】 RGOS 软件可以支持三种认证类型：

1）类型 0，不要求认证，当没有用该命令启用 OSPF 认证，OSPF 数据包中的认证类型为 0；

2）类型 1，为明文认证模式，配置该命令时，没有使用 message-digest 选项；

3）类型 2，为 MD5 认证模式，配置该命令时，使用 message-digest 选项。

一个 OSPF 区域中所有的路由设备，必须采用同一种认证类型。如果启用了认证，还必须在有连接邻居的接口配置认证口令。接口配置命令 **ip ospf authentication-key** 可以配置明文认证口令；接口配置命令 **ip ospf message-digest-key** 可以配置 MD5 认证口令。

配置接口认证类型

【命令格式】 **ip ospfauthentication** [**message-digest** | **null**]

【参数说明】 **message-digest**：该选项表示在该接口上进行 MD5 加密认证。

null：该选项表示不进行认证。

【配置模式】 接口配置模式

【使用指导】 如果命令后面不跟任何选项表示进行明文认证. 注意在配置认证方式时使用 **no** 选项将认证方式恢复缺省值时，实际是否认证是由该接口所在区间上设置的认证方式决定的，如果将认证方式设置为 **null**，则强制设置为不认证，当接口上的认证方式和接口所在的区域的认证方式都设置时，优先采用接口上的认证方式。

配置接口明文认证密钥

【命令格式】 **ip ospf authentication-key** [**0** | **7**] *key*

【参数说明】 **0**：指定密钥以明文显示。

7：指定密钥以密文显示。

key：密钥，最多可以由 8 个字符组成。

【配置模式】 接口配置模式

【使用指导】 **ip ospf authentication-key** 命令配置的密钥，将被插入所有 OSPF 报头。因此密钥不一致，两台直接连接的设备是不能建立 OSPF 邻居关系，当然也不能进行路由信息的交换。

不同接口的密钥可以配置不一样，但所有连接在同一物理网段上的路由设备，必须配置一样的密钥。

一个 OSPF 区域是否启用认证，用路由进程配置命令 area authentication 进行配置。

在接口上也可以单独启用认证，使用接口模式下的配置命令 ip ospf authentication 进行配置，当区域认证和接口认证都配置时优先取接口的认证类型。

配置接口 md5 认证密钥

【命令格式】 **ip ospf message-digest-key** *key-id* **md5** [**0** | **7**] *key*

【参数说明】 *key-id*：密钥标识符，从 1 到 255。

0：指定密钥以明文显示。

7：指定密钥以密文显示。

Key：密钥，最多可以由 16 个字符组成。

【配置模式】 接口配置模式

【使用指导】 **ip ospf message-digest-key** 命令配置的密钥，将被插入所有 OSPF 报头。因此密钥不一致，两台直接连接的设备是不能建立 OSPF 邻居关系的，当然也不能进行路由信息的交换。

不同接口的密钥可以配置不一样，但所有连接在同一物理网段上的路由设备，必须配置一样的密钥。邻居路由设备相同的密钥标识对应的密钥必须一样。

一个 OSPF 区域是否启用认证，使用路由进程配置命令 **area authentication** 进行配置。在接口上也可以单

独启用认证，使用接口模式下的配置命令 **ip ospf authentication** 进行配置，当区域认证和接口认证都配置时优先取接口的认证类型。

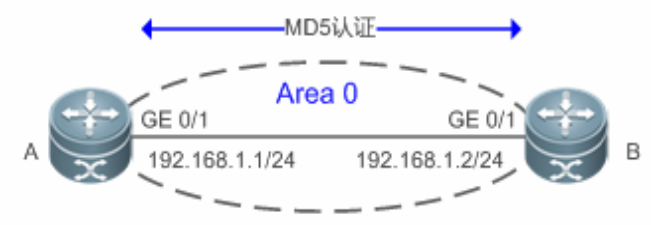
RGOS 软件支持平滑地进行 MD5 认证密钥修改，修改应该遵循一个先加后删除的原则。当增加一个路由设备的 OSPF MD5 认证密钥时，该路由设备会认为其它路由设备还没有用新的密钥，因此会分别用不同的密钥发送多份 OSPF 报文，直到确认邻居已经配置了新的密钥。等所有路由设备配置了新的密钥后，就可以删除旧的密钥了。

配置举例

以下配置举例，需要基于 OSPF 基本功能进行配置，OSPF 基本功能请参见 1.4.1.配置 OSPF 基本功能的介绍。

【网络环境】

图 4-15



【配置方法】

- 所有路由器配置接口 IP 地址。略。
- 所有路由器配置 OSPF 基本功能。略。
- 所有路由器配置认证类型和 MD5 认证密钥。

A

```
A# configure terminal
A(config)# router ospf 1
A(config-router)# area 0 authentication message-digest
A(config-router)# exit
A(config)# interface GigabitEthernet 0/1
A(config-if-GigabitEthernet 0/1)# ip ospf message-digest-key 1 md5 hello
```

B

```
B# configure terminal
B(config)# router ospf 1
B(config-router)# area 0 authentication message-digest
B(config-router)# exit
B(config)# interface GigabitEthernet 0/3
B(config-if-GigabitEthernet 0/3)# ip ospf message-digest-key 1 md5 hello
```

【检验方法】 路由器 A、B 上查看 OSPF 邻居状态正确。

A

```
A# show ip ospf neighbor
OSPF process 1, 1 Neighbors, 1 is Full:
Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.1.2     1     Full/DR         00:00:32    192.168.1.2     GigabitEthernet 0/1
```

B

```
A# show ip ospf neighbor
OSPF process 1, 1 Neighbors, 1 is Full:
Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.1.1     1     Full/DR         00:00:32    192.168.1.1     GigabitEthernet 0/1
```

常见配置错误

- 配置的认证方式不一致。
- 配置的认证密钥不一致。

5.4.9 启动溢出功能

配置效果

- 内存不足时路由器不再加载新的路由。
- 数据库达到上限后路由器不再加载新的路由。

注意事项

- 必须配置 OSPF 基本功能
- 进入 OVERFLOW 状态后，可以通过使用 **clear ip ospf process** 命令，或者关闭再重新启动 OSPF 协议的方式退出 OVERFLOW 状态。

配置方法

↘ 配置内存 OVERFLOW

- 可选配置。
- 若域内有大量路由，可能导致路由器内存不足，建议配置。

↘ 配置数据库 OVERFLOW

- 可选配置。

- 若域内有大量路由，可能导致路由器内存不足，建议配置。

配置外部 lsa 数据库 OVERFLOW

- 可选配置。
- 若 ASBR 引入了大量外部路由，可能导致路由器内存不足，建议配置

检验方法

- 内存不足后，网络增加新的路由，通过 show ip route 查看新的路由没有加载
- 数据库达到上限后，网络增加新的外部路由，通过 show ip route 查看新的路由没有加载

相关命令

配置内存 OVERFLOW

【命令格式】 **overflow memory-lack**

【参数说明】 -

【配置模式】 OSPF 路由配置模式

【使用指导】 OSPF 进入 OVERFLOW 状态主要是丢弃新学到外部路由，该行为能够有效保证内存不再增长。

开启该功能，在 OSPF 进入 OVERFLOW 状态丢弃新学到的外部路由，可能会引起整网出现路由环路的现象。为了减少出现这种现象的产生，OSPF 会生成一条指向 NULL 口的缺省路由，从而降低这种现象产生的概率，该路由在 OVERFLOW 状态下将一直存在。

用户可以使用 clear ip ospf process 命令重新复位 OSPF 运行，清除 OSPF OVERFLOW 状态。使用 no 选项不允许 OSPF 在内存不足时进入 OVERFLOW 状态，这可能会造成内存资源继续消耗，在内存进一步消耗到一定程度，OSPF 实例将停止运行，并删除所有学到的路由。

配置数据库 OVERFLOW

【命令格式】 **overflow database** *number* [**hard | soft**]

【参数说明】 *number*：LSA 最大数目，取值范围*<1-4294967294>*。

hard：LSA 超过该数目时，关闭该 OSPF 实例。

soft：LSA 超过该数目时，发出警告。

【配置模式】 OSPF 路由配置模式

【使用指导】 若超过指定数目需要关闭 OSPF 时，用 hard 参数，若不需关闭 OSPF，只需警告时，用 soft 参数。

配置外部 lsa 数据库 OVERFLOW

【命令格式】 **overflow database external** *max-dbsize wait-time*

【参数说明】 *max-dbsize*：external lsa 的最大数目（同一 AS 内所有路由设备该值需相同），取值范围：0-2147483647。

wait-time：路由设备从 overflow 状态尝试回复普通状态所需等待的时间，取值范围：0-2147483647。

【配置模式】 OSPF 路由配置模式

【使用指导】 当设备的 external-LSA 数目超过配置的 *max-dbsize* 时，会进入溢出状态，该状态下，不再加载 external-LSA，并将清除本地生成的 external-LSA。当经过 *wait-time* 时间后，设备恢复正常状态，并重新加载 external-LSA。

在使用该功能时必须保证 OSPF 主干区域和普通区域的所有设备配置相同的 *max-dbsize* 值 ,否则可能引起如下现象：

整网的链路状态数据库无法达成一致，邻居无法达到 Full 状态；

错误的路由，包括环路的情况；

频繁的 AS-External-LSA 重传；

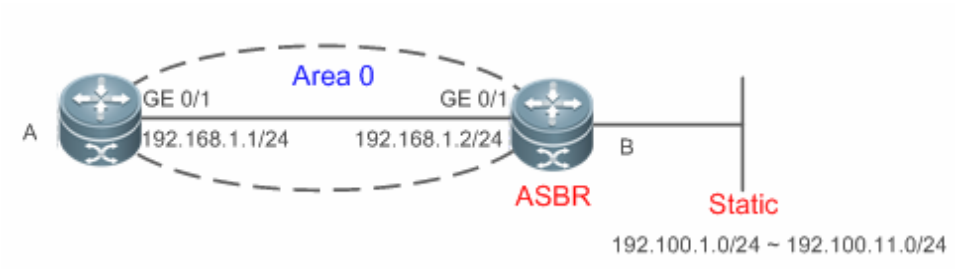
配置举例

以下配置举例，需要基于 OSPF 基本功能进行配置，OSPF 基本功能请参见前文。

配置外部 LSA 数据库 OVERFLOW

【网络环境】

图 4-16



【配置方法】

- 所有路由器配置接口 IP 地址。略。
- 所有路由器配置 OSPF 基本功能。略。
- 路由器 B 配置重分发引入外部静态路由。
- 路由器 A 配置外部 LSA 最大值。

B

```
B# configure terminal
B(config)# router ospf 1
B(config-router)# redistribute static subnets
```

A

```
A# configure terminal
A(config)# router ospf 1
A(config-router)# overflow database external 10 3
```

【检验方法】 路由器 B 配置 11 条静态路由（192.100.1.0/24 ~ 192.100.11.0/24），路由器 A 上查看只加载了 10 条。

A

```
A# show ip route ospf
O E2 192.100.1.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1
O E2 192.100.2.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1
O E2 192.100.3.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1
O E2 192.100.4.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1
O E2 192.100.5.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1
O E2 192.100.6.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1
O E2 192.100.7.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1
O E2 192.100.8.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1
O E2 192.100.9.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1
O E2 192.100.10.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1
```

常见配置错误

- 路由器配置的数据库上限数量不一致，导致 OSPF 邻居状态异常。

5.4.10 修改并发邻居数量限制

配置效果

- 控制 OSPF 邻居的并发建立，缓解设备压力

注意事项

- 必须配置 OSPF 基本功能

配置方法

↘ 配置进程并发邻居数

- 可选配置。若路由器连接了大量其他路由器，且希望 OSPF 邻居建立加快，建议配置。
- 在核心路由器上配置。

检验方法

- 通过 **show ip ospf neighbor** 查看正在并发建立的邻居个数

相关命令

配置当前进程并发邻居数

【命令格式】 **max-concurrent-dd** *number*

【参数说明】 *number*:指定并发交互的邻居最大数目，范围 1-65535。

【配置模式】 OSPF 路由配置模式

【使用指导】 当路由设备与多个邻居同时交换数据，其性能受到影响时，配置该命令，可限制每个 OSPF 实例允许同时并发交互（发起或接受）的邻居最大数目。

配置所有进程并发邻居数

【命令格式】 **router ospf max-concurrent-dd** *number*

【参数说明】 *number*:指定并发交互的邻居最大数目，范围 1-65535

【配置模式】 全局配置模式

【使用指导】 当路由设备与多个邻居同时交换数据，其性能受到影响时，配置该命令，可限制所有 OSPF 实例允许同时并发交互（发起或接受）的邻居最大数目。

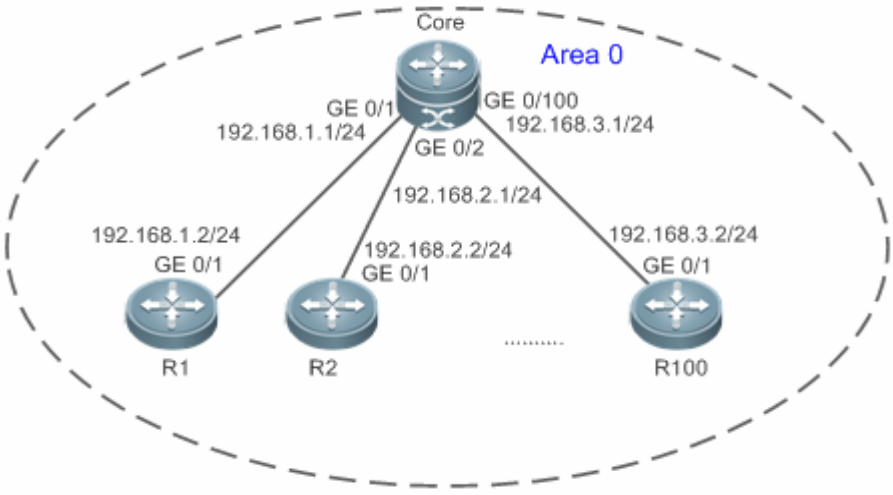
配置举例

以下配置举例，需要基于 OSPF 基本功能进行配置，OSPF 基本功能请参见前文。

配置进程并发邻居数

【网络环境】

图 4-17



【配置方法】

- 所有路由器配置接口 IP 地址。略。
- 所有路由器配置 OSPF 基本功能。略。
- 核心路由器 Core 配置最大邻居并发数为 4。

Core

```
Core# configure terminal

Core(config)# router ospf max-concurrent-dd 4
```

【检验方法】 路由器 Core 上查看邻居状态，同时在建立的邻居最多 8 个。

常见配置错误

-

5.4.11 关闭源地址校验

配置效果

- 相邻路由器的接口 IP 地址不同网段，也能提供单播路由服务

注意事项

- 必须配置 OSPF 基本功能
- 广播网络和 NBMA 网络不能关闭源地址校验

配置方法

↘ 配置关闭源地址校验

- 可选配置。若希望两端接口 IP 地址不同网段也能建立邻接关系，必须配置。
- 在两端接口 IP 地址不同网段的路由器上配置。

检验方法

- 不同网段邻居能建立。

相关命令

↘ 配置关闭源地址校验

【命令格式】 **ip ospf source-check-ignore**

【参数说明】 **-**

【命令模式】 接口配置模式

【使用指导】 通常情况下，OSPF 收到报文的源地址和接收接口会在同一个网段。不过在点对点链路上，链路两端的地址是独立设置的，可以不要求在同一个网段，在这种场景下，由于点对点链路协商过程中会告知对端的地址信息，因此 OSPF 会检查报文的源地址是否就是协商时对端通告的地址，若不是则认为报文非法并丢弃该报文。特别的，对于 unnumbered 接口，OSPF 始终不进行地址校验。但在某些应用场景中，可能会出现源地址不如

上面所述，导致 OSPF 校验失败，比如点对点链路上，协商的对端地址无法获取。在这种场景中，需要关闭源地址校验功能，以保证 OSPF 邻居能正常建立。

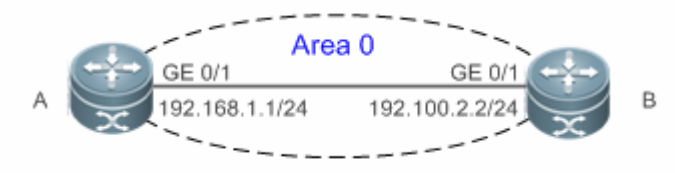
配置举例

以下配置举例，需要基于 OSPF 基本功能进行配置，OSPF 基本功能请参见前文。

配置关闭源地址校验

【网络环境】

图 4-18



【配置方法】

- 所有路由器配置接口 IP 地址。略。
- 所有路由器配置 OSPF 基本功能。略。
- 所有路由器接口配置网络类型配置为 P2P。
- 所有路由器配置关闭源地址校验。

A

```
A# configure terminal
A(config)# interface GigabitEthernet 0/1
A(config-if-GigabitEthernet 0/1)# ip ospf network point-to-point
A(config-if-GigabitEthernet 0/1)# ip ospf source-check-ignore
```

B

```
B# configure terminal
B(config)# interface GigabitEthernet 0/1
B(config-if-GigabitEthernet 0/1)# ip ospf network point-to-point
B(config-if-GigabitEthernet 0/1)# ip ospf source-check-ignore
```

【检验方法】 路由器 A 上查看 OSPF 邻居正确。

A

```
A# show ip ospf neighbor
OSPF process 1, 1 Neighbors, 1 is Full:
Neighbor ID     Pri   State           Dead Time   Address         Interface
192.100.2.2       1   Full/-          00:00:34    192.100.2.2     GigabitEthernet 0/1
```

常见配置错误

-

5.4.12 关闭MTU校验

配置效果

- 相邻路由器的接口 MTU 不同，也能提供单播路由服务

注意事项

- 须配置 OSPF 基本功能

配置方法

↘ 配置关闭 MTU 校验

- 可选配置。默认已关闭 MTU 校验，建议保持默认配置。
- 在两端接口 MTU 不同的路由器上配置。

检验方法

MTU 不一致的邻居也能建立。

相关命令

↘ 配置关闭 mtu 校验

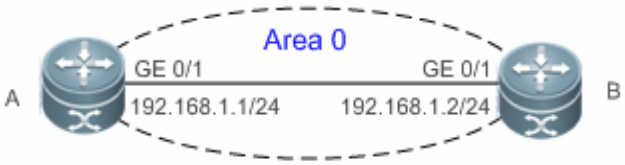
【命令格式】 **ip ospf mtu-ignore**
【参数说明】 **-**
【命令模式】 接口配置模式
【使用指导】 OSPF 在收到数据库描述报文时会校验邻居的接口的 MTU 和自己接口的 MTU 是否相同，如果收到的数据库描述报文中指示的接口的 MTU 大于接收接口的 MTU，那么邻接关系将不能被建立，此时可以通过关闭 MTU 的校验来解决。

配置举例

以下配置举例，需要基于 OSPF 基本功能进行配置，OSPF 基本功能请参见前文。

【网络环境】

图 4-19



【配置方法】

- 所有路由器配置接口 IP 地址。略。
- 所有路由器配置 OSPF 基本功能。略。
- 配置两边接口 MTU 不一致。
- 所有路由器配置关闭 MTU 校验（该功能默认已经开启）。

A

```
A# configure terminal
A(config)# interface GigabitEthernet 0/1
A(config-if-GigabitEthernet 0/1)# ip mtu 1400
A(config-if-GigabitEthernet 0/1)# ip ospf mtu-ignore
```

B

```
B# configure terminal
B(config)# interface GigabitEthernet 0/1
A(config-if-GigabitEthernet 0/1)# ip mtu 1600
B(config-if-GigabitEthernet 0/1)# ip ospf mtu-ignore
```

【检验方法】

- 路由器 A 上查看 OSPF 邻居正确。

A

```
A# show ip ospf neighbor
OSPF process 1, 1 Neighbors, 1 is Full:
Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.1.2       1   Full/DR         00:00:34    192.168.1.2     GigabitEthernet 0/1
```

常见配置错误

-

5.4.13 启动双向维持

配置效果

- 非 hello 报文也能维持邻居状态

注意事项

- 必须配置 OSPF 基本功能

配置方法

配置双向维持

- 可选配置。该功能默认已开启，建议保持默认配置。
- 所有路由器上配置。

检验方法

非 hello 报文也能维持邻居。

相关命令

配置双向维持

【命令格式】 **two-way-maintain**

【参数说明】 -

【命令模式】 OSPF 路由配置模式

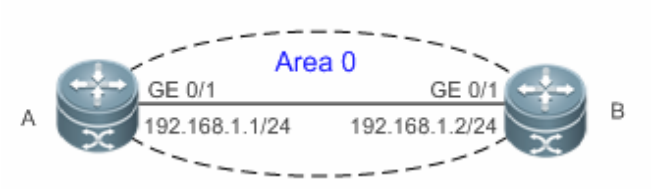
【使用指导】 在较大的网络中，可能会出现大量的报文收发，占用较高的 CPU 和内存资源，造成部分部分报文的延迟或丢弃，如果 Hello 报文的处理超出了死亡间隔，将导致对应的邻接超时断开。这时启用双向维持功能，如果网络中存在大量的报文，除了 Hello 报文外，来自某个邻居的 DD、LSU、LSR、LSAck 报文也能够用于维持该邻居的双向关系，避免由于 Hello 报文的延迟或丢弃而导致邻居的失效。

配置举例

以下配置举例，需要基于 OSPF 基本功能进行配置，OSPF 基本功能请参见前文。

【网络环境】

图 4-20



【配置方法】

- 所有路由器配置接口 IP 地址。略。
- 所有路由器配置 OSPF 基本功能。略。
- 路由器 A 配置启动双向维持（该功能默认已经启动）。

A

```
A# configure terminal
A(config)# router ospf 1
A(config-router)# two-way-maintain
```

【检验方法】 建邻居过程中，路由器 A 检查邻居到期时间，并没有等路由器 B 发送 Hello 报文后才更新。

A

```
A# show ip ospf neighbor

OSPF process 1, 1 Neighbors, 1 is Full:

Neighbor ID     Pri   State           Dead Time   Address         Interface

192.168.1.2     1     Full/BDR        00:00:40    192.168.1.2     GigabitEthernet 0/1
```

常见配置错误

-

5.4.14 启动GR功能

配置效果

- 分布式路由器从主板切换到备板过程中，用户数据流量始终保持转发不断流
- OSPF 协议进程重新启动期间，用户数据流量始终保持转发不断流

注意事项

- 必须配置 OSPF 基本功能
- 邻居路由器必须支持 GR helper。
- GR 时间不能小于邻居路由器的邻居维持时间。

配置方法

↘ 配置 OSPF GR 功能

- 可选配置。该功能默认已开启，建议保持开启状态。
- 在所有路由器上配置。

↘ 配置 OSPF GR helper 功能

- 可选配置。该功能默认已开启，建议保持开启状态。
- 在所有路由器上配置。

检验方法

- 分布式路由器热备切换到备板，在此期间数据流量始终保持转发不断流。
- OSPF 协议进程重启，在此期间数据流量始终保持转发不断流。

相关命令

配置 OSPF 功能

【命令格式】 **graceful-restart** [**grace-period** *grace-period* | **inconsistent-lsa-checking**]

【参数说明】 **grace-period** *grace-period*：配置 GR 重启周期，重启周期为从 OSPF 失效到 OSPF 重新启动并完成优雅重启的最长时间。*grace-period* 取值范围 1-1800 秒，缺省值为 120s。

inconsistent-lsa-checking：拓扑变化检测。检测到拓扑改变，提前退出 GR 完成收敛。开启 GR 后，默认开启检测。

【配置模式】 OSPF 路由配置模式

【使用指导】 优雅重启功能基于 OSPF 实例配置，不同的实例可以根据情况配置不同的参数。该命令用于配置设备的 GR Restarter 能力。重启周期为 GR 从开始到结束的最长时间，在这段时间内执行链路状态重建工作，使 OSPF 恢复到原有状态。当重启周期到期后，OSPF 将退出 GR 状态，执行普通的 OSPF 操作。

graceful-restart 设置 GR 的重启周期为 120 秒，**graceful-restart grace-period** 允许用户显式修改重启周期。GR 成功执行，保证转发不间断的前提是拓扑保持稳定。若拓扑发生改变，OSPF 将尽快收敛，不再等待 GR 的继续执行，避免长时间的转发黑洞。

关闭拓扑检测：对于热备过程中的拓扑变化不能及时收敛，有可能造成长时间的转发黑洞;

使能拓扑检测：有可能转发间断，但间断时间远小于关闭拓扑检测；

对于拓扑检测，大部分情况下不建议关闭。在特殊场景下，热备后拓扑会变化，但可保证不会出现长时间的转发黑洞，此时可关闭拓扑检测，最大程度减少热备过程中转发间断的时间。

在 Fast Hello 功能下，不支持启用优雅重启功能。

配置 OSPF GR helper 功能

【命令格式】 **graceful-restart helper** { **disable | strict-lsa-checking | internal-lsa-checking** }

【参数说明】 **disable**：禁止设备作为辅助设备辅助其他设备执行优雅重启。

strict-lsa-checking：GR Helper 期间通过检查 types 1-5，7 的 LSA 的变化判断网络是否发生变化，如果网络发生变化，将退出 GR Helper。

internal-lsa-checking：GR Helper 期间通过检查 types 1-3 的 LSA 的变化判断网络是否发生变化，如果网络发生变化，将退出 GR Helper。

【配置模式】 OSPF 路由配置模式

【使用指导】 该命令用于配置设备的 GR Help 能力，当邻居设备实施优雅重启时，将发送 Grace-LSA 通告其所有的邻居设备，如果本设备使能 GR Help 能力，在收到 Grace-LSA 时，会成为 GR Helper，辅助邻居完成优雅重启。disable 选项表示禁止对任何执行优雅重启的设备进行 GR 辅助。

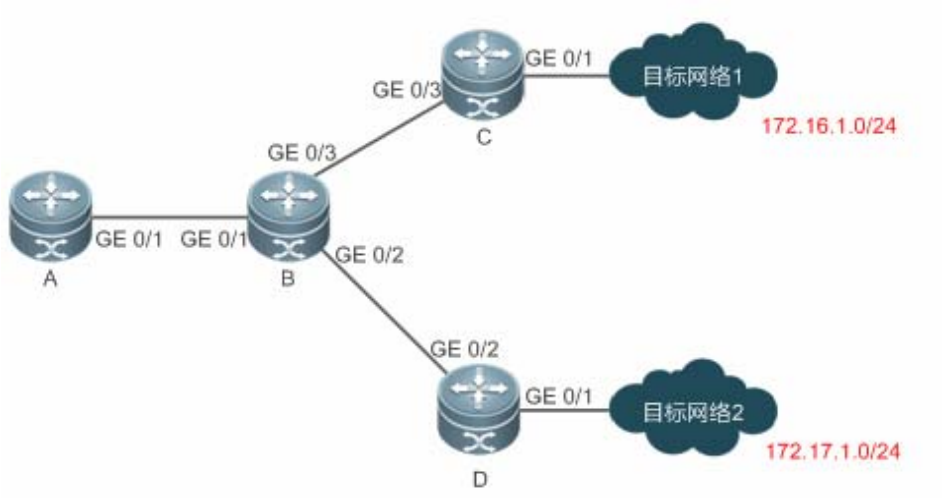
设备成为 GR Helper 后，默认情况下不对网络变化进行检测，如果网络发生变化，也将等到 GR 完成之后才会重新进行收敛。如果用户希望在 GR 过程中，对于变化的网络能够快速探测，可以通过配置 strict-lsa-checking 或者 internal-lsa-checking 选项启动检测，其中前者对任何表示网络信息的 LSA(types 1-5，7)进行检测，后者对表示 AS 域内路由的 LSA(types 1-3)进行检测。在网络规模较大的情况下，不建议用户启动 LSA 检测选项，因为局部网络的变化会触动 GR 结束，从而导致整网的收敛降低。

配置举例

以下配置举例，需要基于 OSPF 基本功能进行配置，OSPF 基本功能请参见前文。

【网路环境】

图 4-21



【注释】 接口 IP 地址：

A：GE 0/1 192.168.1.1

B：GE 0/1 192.168.1.1 GE 0/2 192.168.2.1 GE 0/3 192.168.3.1

C：GE 0/1 192.168.4.2 GE 0/3 192.168.3.2

D：GE 0/1 192.168.5.2 GE 0/2 192.168.2.2

【配置方法】

- 所有路由器配置接口 IP 地址。略。
- 所有路由器配置 OSPF 基本功能。略。
- 路由器 A、C、D 开启 GR Helper 功能（该功能默认已经开启）。
- 路由器 B 开启 GR 功能。

B

```
B# configure terminal
B(config)# router ospf 1
B(config-router)# graceful-restart
```

【检验方法】

- 路由器 B 执行热备切换，期间在路由器 A 上查看到目标网络 1 和目标网络 2 的路由表保持不变。
- 路由器 B 执行热备切换，期间在路由器 A 上 ping 目标网络 1 不间断。

常见配置错误

- 配置的 GR 时间小于邻居路由器的邻居维持时间，导致 GR 过程中转发中断。

5.4.15 配置网管功能

配置效果

- 通过网管软件管理 OSPF 协议的参数及监控协议运行状态。

注意事项

- 必须配置 OSPF 基本功能
- 要开启 OSPF 的 MIB 功能，必须开启 SNMP-Server 的 MIB 功能。
- 要开启 OSPF 的 Trap 功能，必须开启 SNMP-Server 的 Trap 功能。
- 要输出 OSPF 的日记信息，必须开启设备的日记开关。

配置方法

配置 MIB 绑定

- 可选配置。若希望通过网管软件管理指定的 OSPF 实例的参数，需要配置。
- 所有路由器上配置。

配置使能 Trap

- 可选配置。若希望通过网管软件监控协议的运行状态，需要配置。
- 所有路由器上配置。

配置日记输出

- 可选配置。该功能默认已开启，建议保持默认配置，若希望减少日记输出，可关闭该功能。
- 所有路由器上配置。

检验方法

- 通过网管软件可管理协议的参数。
- 通过网管软件可监控协议的运行状态。

相关命令

配置 MIB 绑定

【命令格式】 **enable mib-binding**

【参数说明】 -

【命令模式】 OSPF 路由进程配置模式

【使用指导】 由于 OSPFv2 MIB 没有 OSPFv2 进程信息，所以用户通过 SNMP 操作 OSPFv2 进程，只能操作唯一的进程。
缺省情况下，OSPFv2 MIB 绑定在进程号最小的 OSPFv2 进程上，用户的操作都对该进程生效。
如果用户希望能够通过 SNMP 操作指定的 OSPFv2 进程，可以通过本命令将 MIB 绑定到该进程上。

配置使能 Trap

【命令格式】 **enable traps [error [IfAuthFailure | IfConfigError | IfRxBadPacket | VirtIfAuthFailure | VirtIfConfigError | VirtIfRxBadPacket] | lsa [LsdbApproachOverflow | LsdbOverflow | MaxAgeLsa | OriginateLsa] | retransmit [IfTxRetransmit | VirtIfTxRetransmit] | state-change [IfStateChange | NbrRestartHelperStatusChange | NbrStateChange | NssaTranslatorStatusChange | RestartStatusChange | VirtIfStateChange | VirtNbrRestartHelperStatusChange | VirtNbrStateChange]]**

【参数说明】 **IfAuthFailure**：接口认证错误。

IfConfigError：接口参数配置错误。

IfRxBadPacket：接口接收到错误报文。

IfRxBadPacket：接口接收到错误报文。

VirtIfAuthFailure：虚拟接口认证错误。

VirtIfConfigError：虚拟接口参数配置错误。

VirtIfRxBadPacket：虚拟接口接收到错误报文。

LsdbApproachOverflow：外部 LSA 的数量达到了上限值的 90%。

LsdbOverflow：外部 LSA 的数量达到了上限值。

MaxAgeLsa：LSA 达到老化时间。

OriginateLsa：产生新的 LSA。

IfTxRetransmit：接口上发生报文重传。

VirtIfTxRetransmit：虚接口上发生报文重传。

IfStateChange：接口状态变化。

NbrRestartHelperStatusChange:邻居 GR 过程状态变化。

NbrStateChange：邻居状态变化。

NssaTranslatorStatusChange：NSSA 转换者状态变化。

RestartStatusChange：本机 GR 状态变化。

VirtIfStateChange：虚拟接口状态变化。

VirtNbrRestartHelperStatusChange：虚拟邻居 GR 过程状态变化。

VirtNbrStateChange：虚拟邻居状态变化。

【命令模式】 OSPF 路由进程配置模式

【使用指导】 本命令对应功能受 **snmp-server** 命令的限制，必须先打开配置开关 **snmp-server enable traps ospf**，再配置 enable traps 以后，对应的 ospf trap 才能够正确发送。

本命令不受进程绑定 MIB 的限制，允许不同进程同时打开 TRAP 开关。

配置日记输出

【命令格式】 **log-adj-changes [detail]**

【参数说明】 **detail**：记录全部状态变化信息。

【命令模式】 OSPF 路由进程配置模式

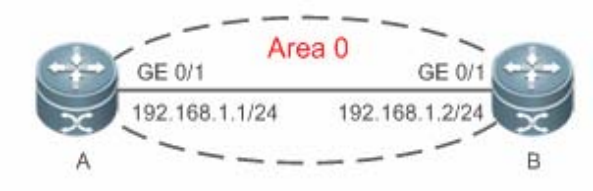
【使用指导】 -

配置举例

以下配置举例，需要基于 OSPF 基本功能进行配置，OSPF 基本功能请参见前文。

【网络环境】

图 4-22



【配置方法】

- 所有路由器配置接口 IP 地址。略。
- 所有路由器配置 OSPF 基本功能。略。
- 路由器 A 配置 MIB 绑定。
- 路由器 A 配置 Trap 使能。

A

```
A# configure terminal
A(config)# snmp-server host 192.168.2.2 traps version 2c public
A(config)# snmp-server community public rw
A(config)# snmp-server enable traps
A(config)# router ospf 10
A(config-router)# enable mib-binding
A(config-router)# enable traps
```

【检验方法】 通过 MIB 工具读取、设置 OSPF 的参数信息，并查看 OSPF 协议运行状态。

常见配置错误

SNMP-Server 配置错误：没有开启 MIB、Trap 功能等。

5.4.16 修改协议控制参数

配置效果

修改协议运行参数，改变协议运行状态。

注意事项

- 必须配置 OSPF 基本功能
- 邻居维持时间不得小于 Hello 间隔时间

配置方法

配置 hello 时间

- 可选配置，不建议修改默认配置。
- 在链路两端的路由器上配置。

配置 dead 时间

- 可选配置，不建议修改默认配置。若用户希望链路失效时加快协议收敛，可调整该配置。
- 在链路两端的路由器上配置。

配置 lsu 重传间隔

- 可选配置。若用户环境有大量路由并且网络拥塞严重，建议调整该配置。

配置 lsa 生成时间

- 可选配置，不建议修改默认配置。

配置 lsa 分组刷新时间

- 可选配置，不建议修改默认配置。若用户环境有大量路由，可调整该配置。
- 在 ASBR 或者 ABR 上配置。

配置 lsa 重复接收延迟

- 可选配置，不建议修改默认配置。

配置 SPF 计算时间

- 可选配置。若网络环境频繁震荡，可调整该配置。

配置区间路由计算延时时间

- 可选配置。不建议修改默认配置。
- 在所有路由器上配置。

配置外部路由计算延时时间

- 可选配置。不建议修改默认配置。
- 在所有路由器上配置。

检验方法

通过 **show ip ospf**、**show ip ospf neighbor** 查看协议运行参数及状态

相关命令

配置 hello 时间

【命令格式】 **ip ospf hello-interval** *seconds*

【参数说明】 *seconds*：设置 OSPF 发送 hello 报文的时间间隔，以秒为单位，取值范围 1-65535。

【命令模式】 接口配置模式

【使用指导】 hello 报文时间间隔包含在 hello 报文中。该时间越短，OSPF 检测到拓扑变化的时间也将越快，但是将增加网络流量。同一网段上的所有路由设备的 hello 报文时间间隔必须一致。如果还想手工修改判断邻居死亡时间，必须保证 hello 报文时间间隔不能大于邻居死亡时间。

配置 dead 时间

【命令格式】 **ip ospf dead-interval** *seconds*

【参数说明】 *seconds*：定义判断邻居死亡的时间，以秒为单位，取值范围：0-2147483647。

【命令模式】 接口配置模式

【使用指导】 OSPF 的死亡时间包含在 Hello 报文内。如果 OSPF 在死亡时间内，没有收到邻居发送的 Hello 报文，就宣告邻居无效并从邻居表中删除该邻居记录。死亡时间缺省为 hello 报文时间间隔的 4 倍，如果修改了 hello 时间间隔，会自动修改死亡时间。

用该命令可以手工修改 OSPF 判断邻居死亡时间，但是必须十分谨慎。有两点必须注意：

第一点：死亡时间间隔，不能小于 hello 报文时间间隔；

第二点：同一网段上的所有路由设备的死亡时间间隔必须一致。

配置 lsu 发送延迟

【命令格式】 **ip ospf transmit-delay***seconds*

【参数说明】 *seconds*：定义 OSPF 接口传输 LSU 报文的延时，以秒为单位，取值范围：1-65535。

【命令模式】 接口配置模式

【使用指导】 在传输 LSU 报文之前，该报文中所有 LSAs（链路状态描述）的 Age 字段将增加，增加量根据该接口配置命令 **ip ospf transmit-delay** 的定义。设置该参数必须考虑到该接口的发送和线路传播时延，对于低速线路，接口的传输延时应该设置得大些。虚拟链路的 LSU 报文传输延时，用 **area virtual-link** 命令跟随 transmit-delay 关键字进行定义。

对 Age 达到 3600 的 LSA，将进行重传或请求重传，如果没有得到及时刷新，超时的 LSA 将从链路状态数据库中清除。

配置 lsu 重传间隔

【命令格式】 **ip ospf retransmit-interval***seconds*

【参数说明】 *seconds*：LSU 重传时间间隔，以秒为单位，取值范围：1-65535。该时间必须大于两个邻居之间的数据包往返传输延时。

【命令模式】 接口配置模式

【使用指导】 当路由设备发送完一个 LSU 报文 ,该 LSU 报文还保留在发送缓冲队列中 ,如果在 **ip ospf retransmit-interval** 命令定义的时间内，没有得到邻居的确认，将重新发送 LSU。

为了避免不必要的重传，在串行线路或虚拟链路上，可以将重传时间设置得大一点。虚拟链路的 LSU 报文重传时间间隔用 area virtual-link 命令跟随 retransmit-interval 关键字进行定义。

配置 lsa 生成时间

【命令格式】 **timers throttle lsa all** *delay-time hold-time max-wait-time*

【参数说明】 *delay-time*：LSA 生成的最小延迟时间，数据库中的第一份 LSA 总是立即生成的。取值范围：0-600000，单位：毫秒。

hold-time：配置首次与第 2 次刷新 LSA 时，最短的时间间隔。取值范围：1-600000，单位：毫秒。

max-wait-time：连续刷新 LSA 时，两次刷新 LSA 的时间间隔最大值。同时，这个时间间隔也是判断 LSA 是否连续刷新的值。取值范围：1-600000，单位：毫秒。

【命令模式】 OSPF 路由进程配置模式

【使用指导】 对链路变化时收敛性要求较高时，delay-time 可以配置为较小值。若希望减少 CPU 消耗，可以把几个值适当调高。

配置命令时，hold-time 不允许小于 delay-time，max-wait-time 也不允许小于 hold-time。

设置 lsa 分组刷新时间

【命令格式】 **timers pacinglsa-group** *seconds*

【参数说明】 *seconds*：LSA 组步调更新的步调时间，取值范围: 10-1800，单位：秒。

【命令模式】 OSPF 路由进程配置模式

【使用指导】 每个 LSA 都有自己的生存时间(LSA age)，当生存时间达到 1800 秒时，需要进行重刷新以防止正常的 LSA 通告达到最大生存时间而被清除掉。如果对每个 LSA 都独立进行 LSA 的更新和老化计算，将消耗大量的 CPU 资源。为了有效利用 CPU 资源，将设备内 LSA 分组进行刷新操作。这里称一个分组刷新操作的时间间隔为组步调间隔，分组刷新操作即将一个组步调间隔内需要刷新的 LSA 编成一组统一刷新。

在 LSA 数量一定的情况下，步调时间间隔越大，定时器期满后处理的 LSA 数量越多。为了保持 CPU 的稳定，建议每次期满处理的 LSA 数量不宜太多，所以如果 LSA 数量较大，建议降低步调间隔。比如，数据库中有 10000 条 LSA，可以降低步调时间间隔，如果只有 40～100 条，则可以调整到 10~20 分钟。

配置 lsa 分组刷新间隔

【命令格式】 **timers pacing lsa-transmit** *transmit-time transmit-count*

【参数说明】 *transmit-time*：配置 LSA 分组发送时间间隔。取值范围：10-1000，单位：毫秒。

transmit-count：配置每组 LS-UPD 报文的个数。取值范围：1-200，单位：个。

【命令模式】 OSPF 路由进程配置模式

【使用指导】 环境中 LSA 数量很多，设备本身负荷太大时，配置适当的 **transimit-time** 和 **transimit-count** 可以抑制网络中洪泛的 LS-UPD 报文数量。

CPU 负荷不高，网络带宽负荷不大时，减小 **transimit-time** 增加 **transimit-count** 可以加快环境的收敛。

配置 lsa 重复接收延迟

【命令格式】 **timers lsa arrival** *arrival-time*

【参数说明】 *arrival-time*：配置接收相同 LSA 时延时。取值范围：0-600000，单位：毫秒。

【命令模式】 OSPF 路由进程配置模式

【使用指导】 配置指定时间之内接收到相同 LSA 时，不做处理。

配置区间路由计算延时时间

【命令格式】 **timers throttle route inter-area** *ia-delay*

【参数说明】 *ia-delay*：定义区间路由计算的延时时间，以毫秒为单位，取值范围：0-600000。

【命令模式】 OSPF 路由进程配置模式

【使用指导】 对网络收敛时间有严格要求时，不能更改该时间。

配置外部路由计算延时时间

【命令格式】 **timers throttle route ase** *ase-delay*

【参数说明】 *ase-delay*：定义外部路由计算的延时时间，以毫秒为单位，取值范围：0-600000。

【命令模式】 OSPF 路由进程配置模式

【使用指导】 对网络收敛时间有严格要求时，不能更改该时间。

配置 SPF 计算时间

【命令格式】 **timers throttle spf** *spf-delay spf-holdtime spf-max-waittime*

【参数说明】 *spf-delay*：定义 SPF 计算的等待时间，以毫秒为单位，取值范围：1-600000。OSPF 路由进程接收到拓扑变化，触发的 SPF 计算至少要在 spf-delay 时间间隔后执行。

spf-holdtime：定义两次 SPF 运算之间的最小时间间隔，以毫秒为单位，取值范围：1-600000。

spf-max-waittime：定义两次 SPF 运算之间的最大时间间隔，以毫秒为单位，取值范围：1-600000。

number：聚合路由的度量值。

【命令模式】 OSPF 路由进程配置模式

【使用指导】 *spf-delay* 表示从拓扑发生变化到 SPF 开始计算，至少需要延迟的时间。第一次触发 SPF 计算到第二次触发 SPF 计算的最小时间间隔为 *spf-holdtime*，此后，连续触发 SPF 计算的时间间隔至少为上一次时间间隔的两倍，当时间间隔达到 *spf-max-waittime* 之后，将不再增加。如果两次 SPF 计算的时间间隔已经超过了要求的最小值，那么 SPF 计算时间间隔将重新从 *spf-holdtime* 开始计算。

spf-delay 和 *spf-holdtime* 可以设置小些以加快拓扑的收敛 ;*spf-max-waittime* 可以设置大些以减少 SPF 计算，可以根据实际网络拓扑稳定性采取灵活设置。

与 **timers spf** 命令相比，该命令能够进行更灵活的设置，既可以加快 SPF 计算收敛速度，又可以在拓扑连续变化时更好的减少 SPF 计算的系统资源消耗，所以推荐使用 **timers throttle spf** 命令进行配置。

1. spf-holdtime 的值不能小于 spf-delay，否则 spf-holdtime 的值将被自动设置为与 spf-delay 相等；
2. spf-max-waittime 的值不能小于 spf-holdtime ,否则 spf-max-waittime 的值将被自动设置为与 spf-holdtime 相等；
3. timers throttle spf 配置与 timers spf 配置会互相覆盖；
4. 当 timers spf 与 timers throttle spf 都未配置时，缺省值参见 timers throttle spf 配置的缺省值。

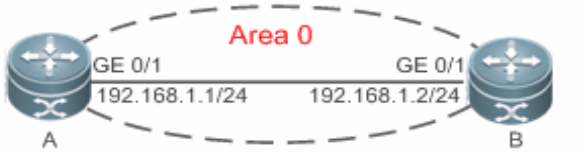
配置举例

以下配置举例，需要基于 OSPF 基本功能进行配置，OSPF 基本功能请参见前文。

配置 hello 时间和 dead 时间

【网络环境】

图 4-23



【配置方法】
- 所有路由器配置接口 IP 地址。略。
- 所有路由器配置 OSPF 基本功能。略。
- 所有路由器配置 Hello 时间和 Dead 时间。

A

```
A# configure terminal
A(config)# interface GigabitEthernet 0/1
A(config-if-GigabitEthernet 0/1)# ip ospf hello-interval 15
A(config-if-GigabitEthernet 0/1)# ip ospf dead-interval 50
```

B

```
B# configure terminal
B(config)# interface GigabitEthernet 0/1
B(config-if-GigabitEthernet 0/1)# ip ospf hello-interval 15
A(config-if-GigabitEthernet 0/1)# ip ospf dead-interval 50
```

【检验方法】 路由器 A 查看接口参数：Hello 时间为 10S，Dead 时间为 50S。

A

```
A# show ip ospf interface
GigabitEthernet 0/1 is up, line protocol is up
  Internet Address 192.168.1.1/24, Ifindex 2, Area 0.0.0.0, MTU 1500
  Matching network config: 192.168.1.0/24
  Process ID 1, Router ID 192.168.1.2, Network Type POINTOMULTIPOINT, Cost: 1
  Transmit Delay is 1 sec, State Point-To-Point
  Timer intervals configured, Hello 15, Dead 50, Wait 40, Retransmit 5
    Hello due in 00:00:02
  Neighbor Count is 1, Adjacent neighbor count is 0
  Crypt Sequence Number is 4787
  Hello received 465 sent 466, DD received 8 sent 8
  LS-Req received 2 sent 2, LS-Upd received 8 sent 21
  LS-Ack received 14 sent 7, Discarded 3
```

常见配置错误

- 配置的邻居维持时间小于 Hello 时间间隔。

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
清除并重启 OSPF 进程。	**clear ip ospf** [*process-id*] **process**

查看运行情况

作用	命令
查看 OSPF 进程的配置信息。	**show ip ospf** [*process-id*]
查看 OSPF 内部路由表（到 ABR、ASBR 的路由）。	**show ip ospf** [*process-id*] **border-routers**
查看 OSPF 链路状态数据库。	**show ip ospf** [*process-id area-id*] **database** [{ **asbr-summary** | **external** | **network** | **nssa-external** | **opaque-area** | **opaque-as** | **opaque-link** | **router** | **summary** }] [{ **adv-router** *ip-address* | **self-originate** } | *link-state-id* | **brief**] [**database-summary** | **max-age** | **detail**]
查看运行 OSPF 的接口。	**show ip ospf** [*process-id*] **interface** [*interface-type interface-number* | **brief**]
查看 OSPF 的邻居表。	**show ip ospf** [*process-id*] **neighbor** [**detail**] [*interface-typeinterface-number*] [*neighbor-id*]
查看 OSPF 路由表。	**show ip ospf** [*process-id*] **route**[**count**]
查看 OSPF 区域的 SPT 计算次数。	**show ip ospf** [*process-id*] **spf**
查看 OSPF 重分布路由的汇聚路由。	**show ip ospf**[*process-id*] **summary-address**
查看 OSPF 的虚链路	**show ip ospf** [*process-id*] **virtual-links** [*ip-address*]

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 OSPF 事件的调试开关。	**debug ip ospf events** [**abr** | **asbr** | **lsa** | **nssa** | **os** | **restart** | **router** | **slink** | **vlink**]
打开 OSPF 接口的调试开关。	**debug ip ospf ifsm** [**events** | **status** | **timers**]
打开 OSPF 邻居的调试开关。	**debug ip ospf nfsm** [**events** | **status** | **timers**]
打开 OSPF NSM 的调试开关。	**debug ip ospf nsm** [**interface** | **redistribute** | **route**]
打开 OSPF LSA 的调试开关。	**debug ip ospf lsa** [**flooding** | **generate** | **install** | **maxage** | **refresh**]
打开 OSPF 报文的调试开关。	**debug ip ospf packet** [**dd** | **detail** | **hello** | **ls-ack** | **ls-request** | **ls-update** | **recv** | **send**]
打开 OSPF 路由的调试开关。	**debug ip ospf route** [**ase** | **ia** | **install** | **spf** | **time**]

6 OSPFv3

6.1 概述

OSPF（Open Shortest Path First，开放式最短路径优先协议）是一种内部网关协议（Interior Gateway Protocol，简称 IGP），应用在 AS（Autonomous System，自治系统）内部，使路由器获得远端网络的路由。

OSPF Version 2 应用于 IPv4，OSPF Version 3 应用于 IPv6，协议运行机制和大部分配置都相同。

OSPF 具备如下特点：

- 适用范围广：适用于更大规模的网络（最大可支持几百台路由器）。
- 快速收敛：一旦网络拓扑发生变化，路由器之间能够快速通告信息，更新路由。
- 无自环：路由器之间仅同步链路状态信息，每台路由器独立计算路由，不会生成自环。
- 区域划分：将一个大的路由域划分为多个较小的区域，可以节省系统资源和网络带宽，使路由稳定可靠。
- 路由分类：将路由分为多种类型区别对待，支持灵活的控制策略。
- 等价路由：支持等价路由。
- 支持认证：支持报文认证，保障协议交互过程的安全。
- 组播发送：支持以组播地址发送协议报文，可以避免干扰无关者、节省系统资源。

本章使用“路由器”指代支持路由功能的网络设备。这些网络设备可以是三层交换机、路由器、防火墙等。

若无特殊说明，下文以 OSPF 来指代“OSPFVersion 3”。

协议规范

RFC2740	This document describes the modifications to OSPF to support version 6 of the Internet Protocol (IPv6).
draft-ietf-ospf-ospfv3-graceful-restart	This document describes the OSPFv3 graceful restart. The OSPFv3 graceful restart is identical to OSPFv2 except for the differences described in this document. These differences include the format of the grace Link State Advertisements (LSA) and other considerations.
draft-ietf-ospf-ospfv3-mib-11	This memo defines a portion of the Management Information Base (MIB) for use with network management protocols in IPv6-based internets. In particular, it defines objects for managing the Open Shortest Path First Routing Protocol for IPv6.

6.2 典型应用

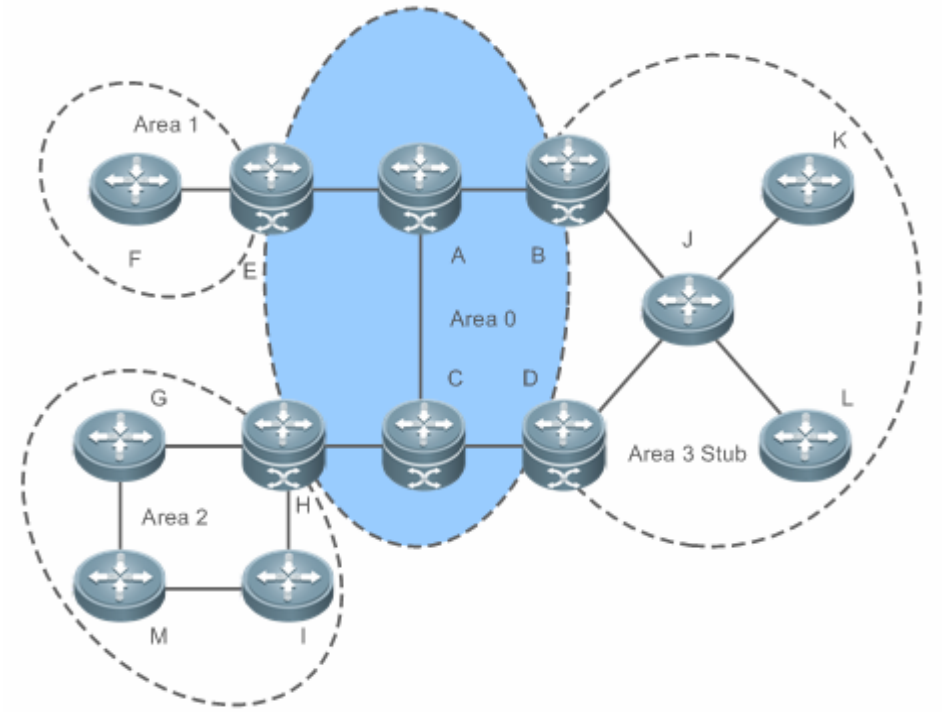
典型应用	场景描述
域内互联	在 AS 内部运行 OSPF，划分多个区域。
域间互联	多个 AS 互联，在 AS 内部运行 OSPF，在 AS 之间运行 BGP。

6.2.1 域内互联

应用场景

在 AS 内部运行 OSPF，如果路由设备超过 40 台，建议划分多个区域。通常，骨干区域应该采用性能可靠且处理速度较快的高端设备，非骨干区域可以采用性能相对较低的中低端设备。所有非骨干区域都必须与骨干区域相连。建议将位于末梢的非骨干区域设置为 Stub 区域。以图 1-1 为例，将该网络划分成 4 个区域，不同区域间的通信都经过骨干区域（即区域 0）。

图 6-1 OSPF 区域划分



【注释】 A、B、C、D、E、H 处于骨干区域，是骨干路由器。
区域 3 配置成 Stub 区域。

功能部属

- AS 内部，所有路由器运行 OSPF 协议，实现单播路由。

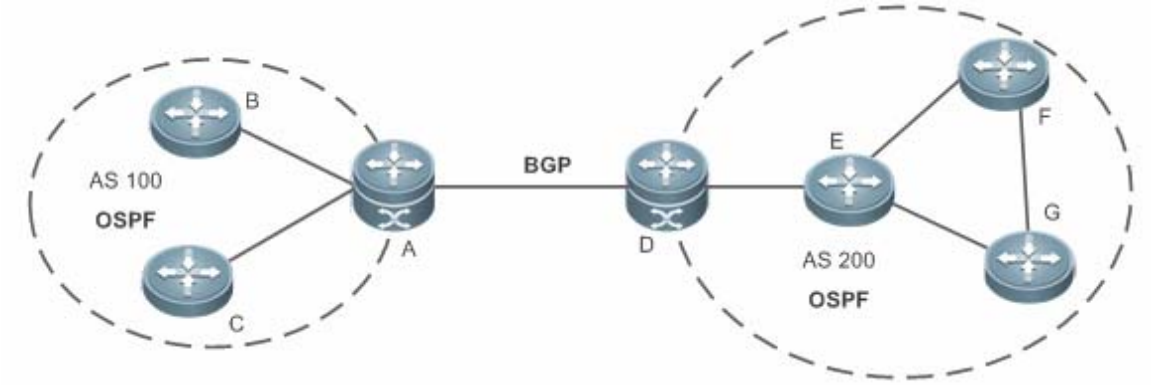
6.2.2 域间互联

应用场景

多个 AS 互联，在 AS 内部运行 OSPF，在 AS 之间运行 BGP。通常，OSPF 与 BGP 应该相互学习路由信息。

以图 1-2 为例，AS 100 和 AS 200 内部都是通过 OSPF 协议来实现单播路由，在两个 AS 之间通过 BGP 协议来实现单播路由。

图 6-2 OSPF 与 BGP 互联



【注释】 A、D 同时运行 OSPF 协议和 BGP 协议

功能部属

- AS 100 和 AS 200 内部运行 OSPF 协议，实现单播路由。
- 两个 AS 之间运行 BGP 协议，实现单播路由。

6.3 功能详解

基本概念

路由域

一个 AS 中的所有路由器必须相互连接，运行相同的路由协议。因此，AS 也被称为路由域（Routing Domain）。

运行 OSPF 的 AS 也被称为 OSPF 路由域，简称 OSPF 域。

OSPF 进程

OSPF 支持多实例（Instance），每个实例对应一个 OSPF 进程（Process）。

一台路由器上可以启用一个 OSPF 进程，也可以启用多个 OSPF 进程。每个 OSPF 进程独立执行 OSPF 协议，相互隔离。

OSPF 报文头中包含 Instance ID 字段，单个链路上可以运行多个 OSPF 实例。但 Process ID 只有本地意义。

RouterID

OSPF 域内，使用 Router ID 唯一标识一台路由器。任意两台路由器的 Router ID 不能相同。

如果路由器上存在多个 OSPF 进程，则每个 OSPF 进程使用一个 Router ID。任意两个 OSPF 进程的 Router ID 不能相同。

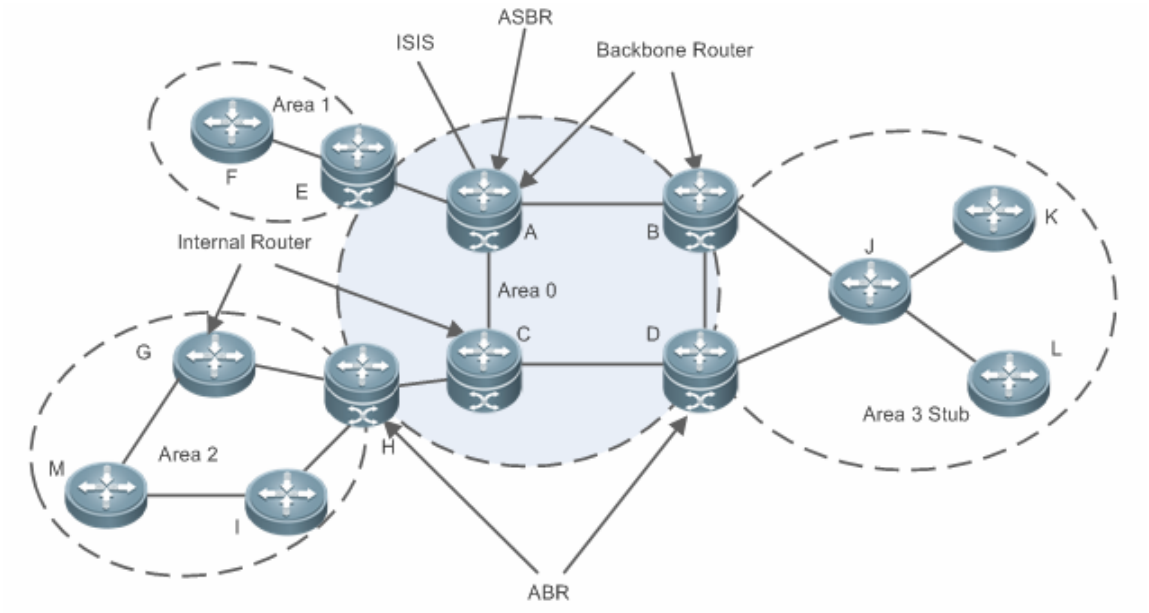
区域

OSPF 支持多区域（Area）。将一个 OSPF 域划分为多个区域，有助于缓解大规模网络的计算压力。

区域是从逻辑上将路由器划分为不同的组，每个组用区域号（Area ID）来标识。区域的边界是路由器，一台路由器可以只属于一个区域，也可以属于多个区域。一个网段（链路）只能属于一个区域，或者说每个运行 OSPF 的接口必须指明属于哪一个区域。

区域 0 为骨干区域（Backbone Area），其他区域为常规区域（NormalArea）。常规区域必须与骨干区域直接相连。

图 6-3OSPF 区域划分



OSPF 路由器

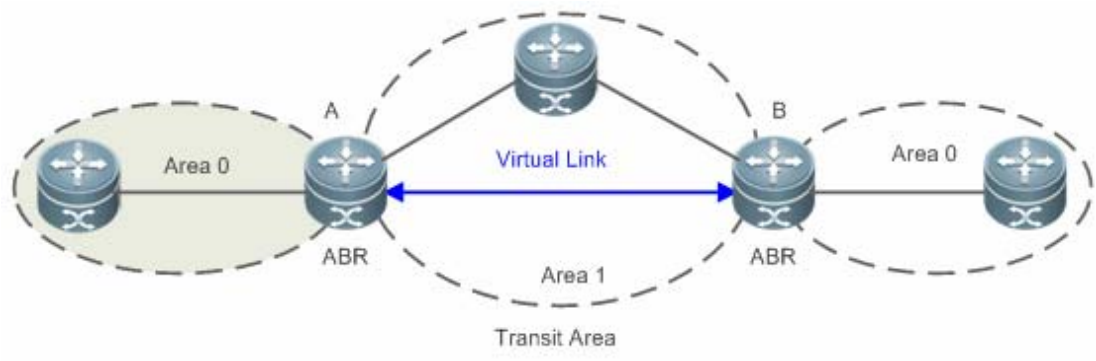
在 OSPF 中定义了几种路由器类型，并为每种类型的路由器赋予不同的职责。

- 区域内路由器（Internal Router）
  该类路由器的所有接口都属于同一个 OSPF 区域。如上图中的 A、C、F、G、I、M、J、K、L。
- 区域边界路由器（Area Border Router，简称 ABR）
  该类路由器用来连接骨干区域和常规区域。ABR 同时属于两个以上的区域，其中一个必须是骨干区域。如上图中的 B、D、E、H。
- 骨干路由器（Backbone Router）
  该类路由器至少有一个接口属于骨干区域。所有的 ABR 和 Area0 的区域内路由器都是骨干路由器。如上图中的 A、B、C、D、E、H。
- 自治系统边界路由器（AS Boundary Router，简称 ASBR）
  该类路由器用来与其他 AS 交换路由信息。ASBR 并不一定位于 AS 的边界，它可能是区域内路由器，也可能是 ABR。如上图中的 A。

虚链路

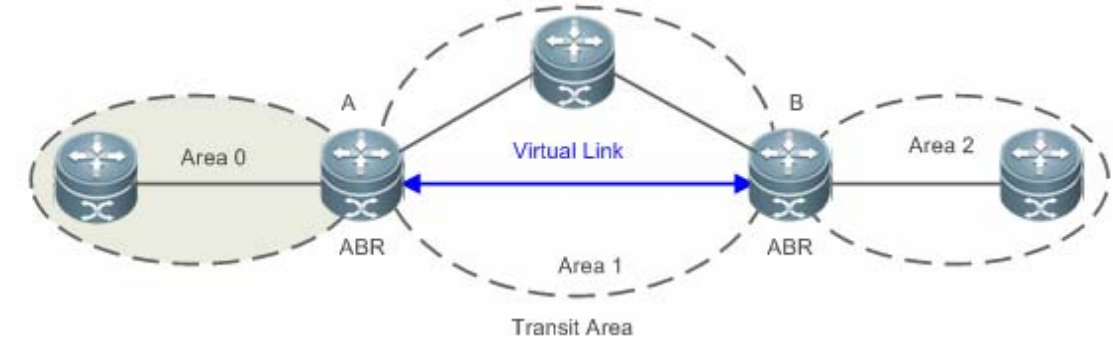
OSPF 支持虚链路（Virtual link）。虚链路是一条逻辑链路，属于骨干区域，用于解决在物理网络上骨干区域不连续或骨干区域与常规区域不能直接相连的问题。虚链路只能穿越一个常规区域，该区域被称为“传输区域”（Transit Area）。虚链路两端的路由器均为 ABR。

图 6-4 在物理网络上，骨干区域不连续



如上图所示：在 A、B 之间建立虚链路，将 Area0 连接起来；Area1 是传输区域；A、B 是 Area1 的 ABR。

图 6-5 在物理网络上，骨干区域与常规区域不能直接相连



如上图所示：在 A、B 之间建立虚链路，将 Area0 延伸到 B，则 Area0 与 Area2 在 B 上直接相连；Area1 是传输区域；A 是 Area1 的 ABR；B 是 Area1、Area2 的 ABR。

LSA

OSPF 以 LSA（Link State Advertisement，链路状态通告）的形式来描述路由信息。

LSA 类型	说明
Router-LSA（Type1）	由每个路由器始发，描述了路由器的链路状态和代价，在始发路由器所属区域内传播。
Network-LSA（Type2）	由 DR 始发，描述本链路的链路状态，在 DR 所属区域内传播。
Inter-Area-Prefix-LSA（Type3）	由 ABR 始发，描述到其它区域的路由，通告给非 Totally STUB、NSSA 区域。
Inter-Area-Router-LSA（Type4）	由 ABR 始发，描述到 ASBR 的路由，通告给除 ASBR 所在区域的其他区域。
AS-external-LSA（Type5）	由 ASBR 始发，描述到 AS 外部的路由，通告到所有区域（除了 STUB、NSSA 区域）。
NSSA LSA（Type7）	由 ASBR 始发，描述到 AS 外部的路由，仅在 NSSA 区域内传播。
Link-LSA（Type8）	由每个路由器始发，描述每个链路的 link-local 地址、IPv6 前缀地址，并提供将会在 Network-LSA 中设置的链路选项，仅在此链路内传播。
Intra-Area-Prefix-LSA（Type9）	每个路由器及 DR 都会产生一个或多个此类 LSA，在所属的区域内传播。 ● 路由器产生的此类 LSA，描述与 Route-LSA 相关联的 IPv6 前缀地址。 ● DR 产生的此类 LSA，描述与 Network-LSA 相关联的 IPv6 前缀地址。

（Totally）STUB、NSSA 区域，是常规区域的特殊形态，有助于减轻路由器负担，增强 OSPF 路由稳定性。

OSPF 报文

OSPF 使用以下几种类型的协议报文。这些 OSPF 报文被封装在 IP 报文中，以组播或单播方式发送。

报文类型	说明
Hello	周期性发送，用来发现 OSPF 邻居，维持邻接关系。

DD（Database Description）	描述本地 LSDB（Link-State Database，链路状态数据库）的摘要信息，用于在 OSPF 邻居之间进行数据库同步。
LSR（Link State Request）	用于向对方请求所需的 LSA。只有在 OSPF 邻居双方成功交换 DD 报文后，才会向对方发出 LSR 报文。
LSU（Link State Update）	用于向对方发送其所需要的 LSA。
LSAck（Link State Acknowledgment）	用来对收到的 LSA 进行确认。

功能特性

功能特性	作用
链路状态路由协议	在路由器上运行 OSPF，即可获得到达网络各个位置的路由。
OSPF 路由管理	通过人为配置，合理规划或优化 OSPF 路由，实现管理的目的。
增强安全性、可靠性	认证、与 BFD 联动等功能使 OSPF 更安全、更稳定可靠。
支持网管功能	MIB、SYSLOG 等功能使 OSPF 更易于管理。

6.3.1 链路状态路由协议

OSPF 属于链路状态路由协议（Link-StateRouting Protocols），工作过程概述：

- 邻居发现→双向通信
  在相连的路由器之间建立 OSPF 邻居关系，并保持双向通信。
- 数据库同步→完全邻接
  路由器使用 LSA 发布自己的全部链路状态。邻居之间交换 LSA，同步 LSDB，达到完全邻接状态。
- 计算 SPT →形成路由表
  路由器依据 LSDB 计算出到达每个目标网络的最短路径，形成 OSPF 路由表。

工作原理

↘ 邻居发现→双向通信

路由器从所有启动 OSPF 的接口上（或虚链路）发出 Hello 报文。如果两台路由器之间能够交互 Hello 报文，并且能够成功协商 Hello 报文中携带的参数，则它们就成为了邻居（Neighbor）。当互为邻居的路由器在彼此的 Hello 报文中找到自己的 Router ID 时，双向通信就建立了。

Hello 报文中包含（但不限于）如下信息：

- 始发路由器的 Router ID
- 始发路由器接口（或虚链路）的 Area ID
- 始发路由器接口（或虚链路）的 Instance ID
- 始发路由器接口（或虚链路）的 Interface ID
- 始发路由器接口的优先级（用于 DR/BDR 竞选）
- 始发路由器接口（或虚链路）的 Hello 时间间隔
- 始发路由器接口（或虚链路）的邻居死亡时间
- DR（Designated Router，指定路由器），BDR（Backup Designated Router，备份指定路由器）的 Router ID
- 始发路由器的邻居的 Router ID

↘ 数据库同步→完全邻接

邻居路由器之间建立双向通信后，使用 DD、LSR、LSU、LSAck 报文交换 LSA，建立邻接关系。简要过程如下：

- 路由器产生 LSA，用来描述该设备上的全部链路状态。

- 邻居之间交换 LSA。当路由器接收到邻居发送的 LSA 时，将拷贝一份到本地 LSDB，然后再传播给其它邻居。
- 当路由器及其邻居都获得了相同的 LSDB 时，达到完全邻接状态。

如果没有链路代价、网络增删变化，OSPF 将会十分安静。如果发生变化，则通告变化的链路状态，快速同步 LSDB。

计算最短路径→形成路由表

路由器上获得完整的 LSDB 后，将运行 Dijkstra 算法生成一棵从本地到每个目标网络的最短路径树（Shortest Path Tree，简称 SPT）。SPT 中记录了：目标网络、下一跳地址、代价。OSPF 依据 SPT 形成路由表。

如果发生链路代价、网络增删变化，则会引起 LSDB 的更新。设备将再次运行 Dijkstra 算法，生成新的 SPT，并更新路由表。

Dijkstra 算法用来在一个有权重的有向图中，找到从一个顶点到其他顶点的最短路径。

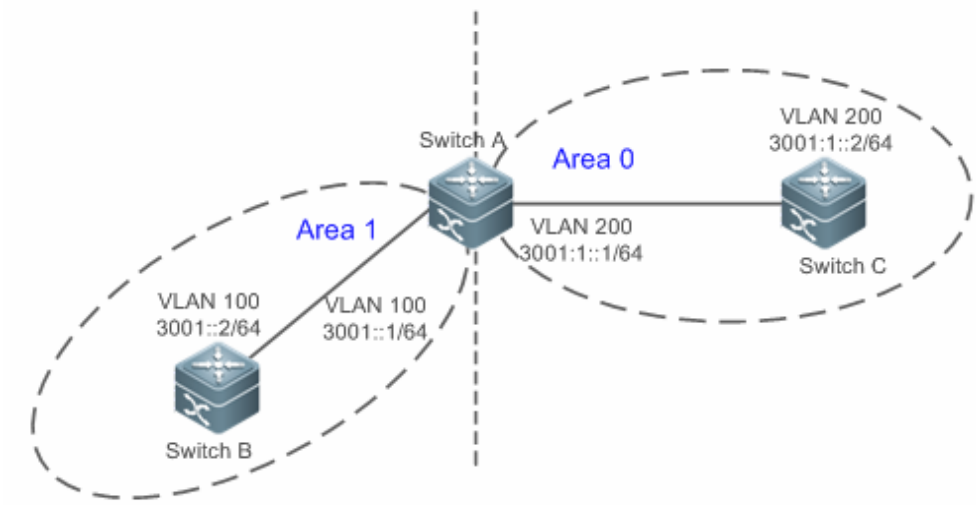
OSPF 网络类型

路由器不一定需要与它的每一个邻居交换 LSA、建立邻接关系。为提高效率，OSPF 将各种链路层协议的网络归类为 5 种类型，以不同的方式交换 LSA、建立邻接关系。

- 广播（Broadcast）
  自动发现邻居，选举 DR、BDR。
  DR（或 BDR）与其他所有路由器交换 LSA、建立邻接关系。DR、BDR 之外的路由器之间不交换 LSA、不建立邻接关系。
  Ethernet、FDDI 默认属于此类型。
- 非广播（Non-broadcast multiple access，简称 NBMA）
  手工配置邻居，选举 DR、BDR。
  DR（或 BDR）与其他所有路由器交换 LSA、建立邻接关系。DR、BDR 之外的路由器之间不交换 LSA、不建立邻接关系。
  X.25、帧中继、ATM 默认属于此类型。
- 点到点（point-to-point，简称 P2P）
  自动发现邻居，不选举 DR/BDR。
  链路两端路由器之间交换 LSA、建立邻接关系。
  PPP、HDLC、LAPB 默认属于此类型。
- 点到多点（Point-to-Multipoint，简称 P2MP）
  自动发现邻居，不选举 DR/BDR。
  任意两台路由器之间都要交换 LSA、建立邻接关系。
  没有任何链路层协议的网络默认为此类型。
- 点到多点非广播
  手动配置邻居，不选举 DR/BDR。
  任意两台路由器之间都要交换 LSA、建立邻接关系。
  没有任何链路层协议的网络默认为此类型。

OSPF 路由类型

图 6-6



在 C 上查看路由表中的 OSPF 路由（如下红色字体）。

```
C#show ipv6 route ospf
IPv6 routing table name is Default(0) global scope - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra area, OI - OSPF inter area,  OE1 - OSPF external type 1, OE2 - OSPF external type 2
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       [*] - NOT in hardware forwarding table

L      ::1/128  via Loopback, local host
OI     3001::/64  [110/2] via FE80::21A:A9FF:FE15:4CB9, VLAN 200
C      3001:1::/64  via VLAN 200, directly connected
L      3001:1::2/128  via VLAN 200, local host
L      FE80::/10  via ::1, Null0
C      FE80::/64  via VLAN 200, directly connected
L      FE80::21A:A9FF:FE01:FB1F/128  via VLAN 200, local host
```

每条 OSPF 路由前都带有一个标识，用来说明此路由的类型。OSPF 路由共有 6 种类型。

- O：区域内路由
  此类路由描述了如何到达本区域内的目标网络。路由代价=本地到目标网络的代价。
- OI：区域间路由
  此类路由描述了如何到达其他区域的目标网络。路由代价=本地到目标网络的代价。
- OE1：第一类外部路由
  此类路由描述了如何到达 AS 以外的目标网络。路由代价=本地到 ASBR 的代价+ASBR 到目标网络的代价。Stub、NSSA 区域内的路由器上不存在此类路由。
- OE2：第二类外部路由
  此类路由描述了如何到达 AS 以外的目标网络。路由代价=ASBR 到目标网络的代价。Stub、NSSA 区域内的路由器上不存在此类路由。

- ON1：NSSA 区域的第一类外部路由
  此类路由仅描述了如何经 NSSA 区域的 ASBR 到达 AS 以外的目标网络。路由代价=本地到 ASBR 的代价+ASBR 到目标网络的代价。仅 NSSA 区域的路由器上存在此类路由。
- ON2：NSSA 区域的第二类外部路由
  此类路由描述了如何经 NSSA 区域的 ASBR 到达 AS 以外的目标网络。路由代价=ASBR 到目标网络的代价。仅 NSSA 区域的路由器上存在此类路由。

OE2、ON2 这两类路由的可信度比较低，OSPF 认为从 ASBR 到自治系统之外的代价远远大于在自治系统之内到达 ASBR 的代价。所以，计算路由代价时只考虑 ASBR 到自治系统之外的代价。

相关配置

启动 OSPF

缺省情况下，未启动 OSPF。

使用 **ipv6 router ospf** 1 命令，在路由器上创建一个 OSPF 进程。

使用 **ipv6 ospfarea** 命令，在接口上启动 OSPF，指定 Area ID。

使用 **area virtual-link** 命令，在路由器上创建一个虚链接。可将虚链接视为一个逻辑接口。

Router ID

缺省情况下，OSPF 进程选举所有 Loopback 接口中 IPv4 地址最大的作为 Router ID。如果没有配置了 IPv4 地址的 Loopback 接口，则选取所有物理接口中 IPv4 地址最大的作为路由设备标识。

也可以使用 **router-id** 命令，人为指定 Router ID。

协议控制参数

使用 **ipv6 ospf hello-interval** 命令，修改接口上的 Hello 消息发送间隔，缺省值是 10 秒（NBMA 类型 30 秒）。

使用 **ipv6 ospf dead-interval** 命令，修改接口上的邻居死亡时间，缺省值是 Hello 报文发送间隔的四倍。

使用 **ipv6 ospf neighbor** 命令的 **poll-interval** 参数，修改 NBMA 类型接口上的邻居轮询间隔，缺省值是 120 秒。

使用 **ipv6 ospf transmit-delay** 命令，修改接口上的 LSU 报文传输延时，缺省值是 1 秒。

使用 **ipv6 ospf retransmit-interval** 命令，修改接口上的 LSU 报文重传间隔，缺省值是 5 秒。

使用 **area virtual-link** 命令的 **hello-interval** 参数，修改虚链路上的 Hello 消息发送间隔，缺省值是 10 秒。

使用 **area virtual-link** 命令的 **dead-interval** 参数，修改虚链路上的邻居死亡时间，缺省值是 Hello 报文发送间隔的四倍。

使用 **area virtual-link** 命令的 **transmit-delay** 参数，修改虚链路上的 LSU 报文传输延时，缺省值是 1 秒。

使用 **area virtual-link** 命令的 **retransmit-interval** 参数，修改虚链路上的 LSU 报文重传间隔，缺省值是 5 秒。

使用 **timers throttle lsa all** 命令，修改生成 LSA 的指数退避算法参数，缺省值是 0 毫秒，5000 毫秒，5000 毫秒。

使用 **timers pacing lsa-group** 命令，修改 LSA 分组刷新的时间，缺省值是 30 秒。

使用 **timers pacing lsa-transmit** 命令，修改（LSA 分组刷新的）LS-UPD 报文发送间隔和个数，缺省值是 40 毫秒、1 个。

使用 **timers lsa arrival** 命令，修改接收相同 LSA 的延时，缺省值是 1000 毫秒。

使用 **timers throttle spf** 命令，修改计算 SPT 的延时，两次计算的最小间隔、最大间隔。缺省值是 1000 毫秒、5000 毫秒、10000 毫秒。

OSPF 网络类型

缺省情况下，Ethernet、FDDI 为广播类型；X.25、帧中继、ATM 为 NBMA 类型；PPP、HDLC、LAPB 为 P2P 类型。

使用 **ipv6 ospf network** 命令，手工指定接口的网络类型。

使用 **ipv6 ospf neighbor** 命令，手工指定邻居。NBMA、点到多点非广播类型必须手工指定邻居。

使用 **ipv6 ospf priority** 命令，调整接口的优先级（用于 DR/BDR 竞选）。广播、NBMA 类型需要竞选 DR/BDR。优先级最大者获胜，优先级为 0 者弃权。缺省值为 1。

6.3.2 OSPF路由管理

通过人为配置，可以合理规划或优化 OSPF 路由，实现管理的目的。

工作原理

（Totally）Stub、NSSA 区域

（Totally）Stub、NSSA 区域有助于减轻协议交互负担、减小路由表的规模。

- 将适当的区域设置为（Totally）Stub、NSSA 区域，则可以免除大量的 LSAType 5、3 在区域内传播。

区域	LSA Type 1、2	LSA Type 3	LSA Type 4	LSA Type 5	LSA Type 7
非（Totally）Stub、NSSA 区域	允许	允许	允许	允许	不允许
Stub 区域	允许	允许，包括一条缺省路由	不允许	不允许	不允许
Totally Stub 区域	允许	只允许一条缺省路由	不允许	不允许	不允许
NSSA 区域	允许	允许，包括一条缺省路由	允许	不允许	允许
Totally NSSA 区域	允许	只允许一条缺省路由	允许	不允许	允许

ABR 使用 LSA Type 3 向（Totally）Stub、NSSA 区域发布一条缺省路由。

ABR 将（Totally）NSSA 区域内的 LSA Type 7 转换成 LSA Type 5，发布到骨干区域。

- 将适当的区域设置为（Totally）Stub、NSSA 区域，则区域内路由器的路由表中可以免除大量 OE1、OE2、OI 类型的路由。

区域	区域内路由器的路由表中存在哪些路由
非（Totally）Stub、NSSA 区域	O：到本区域某目标网段的路由 OI：到其他区域某目标网段的路由 OE1 或 OE2：（经过 AS 内任意 ASBR）到 AS 外部某目标网段的路由、缺省路由
Stub 区域	O：到本区域某目标网段的路由 OI：到其他区域某目标网段的路由、缺省路由
Totally Stub 区域	O：到本区域某目标网段的路由 OI：缺省路由
NSSA 区域	O：到本区域某目标网段的路由 OI：到其他区域某目标网段的路由、缺省路由 ON1 或 ON2：（经过本区域内的 ASBR）到 AS 外部某目标网段的路由、缺省路由
Totally NSSA 区域	O：到本区域某目标网段的路由 OI：缺省路由 ON1 或 ON2：（经过本区域内的 ASBR）到 AS 外部某目标网段的路由、缺省路由

路由重分布

路由重分布是指：将设备上存在的“其他路由协议的路由、其他 OSPF 进程的路由、静态路由、直连路由”引入 OSPF 进程，以 LSA Type 5、7 的方式发送给邻居。路由重分布不能引入缺省路由。

路由重分布常用于 AS 间互联。通过在 ASBR 上配置路由重分布，可以将 AS 外部的路由信息传播到 AS 内部，也可以将 AS 内部的路由信息传播到 AS 外部。

引入缺省路由

通过在 ASBR 上配置命令，可以将一条缺省路由引入 OSPF 进程，以 LSA Type 5、7 的方式发送给邻居。

“引入缺省路由”常用于 AS 间互联，以一条缺省路由代替所有 AS 外部的路由信息。

路由汇聚

路由汇聚是指将具有相同前缀的路由信息汇聚为一条路由，并将汇聚后的路由（替代大量琐碎路由）发布给邻居。路由汇聚有助于减轻协议交互负担、减小路由表的规模。

缺省情况下，对于区域间的路由信息，ABR 以网段为单位发布 LSA Type 3；对于重分布进来的路由信息，ASBR 逐条发布 LSA Type 5、7。如果其中存在一些连续的网段，则建议配置路由汇聚。

路由过滤

OSPF 允许在学习、交互、使用路由信息的过程中进行过滤，以达到安全可控的目的。

通过配置命令，可以在以下几处进行路由过滤：

- 针对接口。禁止接口发出路由信息（任意 LSA）、或禁止接口与邻居交互路由信息（任意 LSA）。
- 针对 AS 外部的路由信息。只有满足过滤条件的路由信息才能被重分布到 OSPF 进程（LSA Type 5、7）。
- 针对路由器收到的 LSA。OSPF 路由表中，只有由满足过滤条件的 LSA 计算出的路由，才能执行报文转发。

路由代价

如果网络中存在冗余链路或设备，则从本地到目的网络之间可能存在多条路径。OSPF 选择其中总代价最小的路径形成 OSPF 路由。一条路径的总代价等于沿途链路上的代价之和。通过修改沿途链路上的代价，使一条路径的总代价最小，即可使 OSPF 选择此路径形成路由。

通过配置命令，可以修改如下链路代价：

- 从接口到直连网段的代价、从接口到邻居的代价
- 从 ABR 到缺省网段的代价
- 从 ASBR 到外部网段的代价、从 ASBR 到缺省网段的代价

cost、metric 都表示代价，没有实质上的差别。

OSPF 管理距离

管理距离（administrative distance，缩写为 AD）用于评价路由的可信度，取值范围 0～255（整数）。AD 值越小，则表示此路由更值得信任。到达同一目的地存在多条路由时，路由器优先选择 AD 值较小的路由。AD 值较大者，成为浮动路由（作为最优路由的备份）。

缺省情况下，每种来源的路由对应一个 AD 值。AD 值为本地概念，修改 AD 值只会影响当前路由器上的路由选择。

路由来源	直连网络	静态路由	EBGP 路由	OSPF 路由	ISIS 路由	RIP 路由	IBGP 路由	不可达路由
缺省 AD	0	1	20	110	115	120	200	255

相关配置

Stub、NSSA 区域

Stub 区域

缺省情况下，没有 Stub、NSSA 区域。

缺省情况下，没有 Stub 区域。

使用 **area stub** 命令，将指定区域设置为 Stub 区域。

使用 **area nssa** 命令，将指定区域设置为 NSSA 区域。

骨干区域不能设置为 Stub（或 NSSA）区域。

传输区域（虚链路穿过的区域）不能设置为 Stub（或 NSSA）区域。

骨干区域不能设置为 Stub 区域。

传输区域（虚链路穿过的区域）不能设置为 Stub 区域。

包含 ASBR 的区域不能设置为 Stub 区域。

路由重分布、引入缺省路由

缺省情况下，不进行路由重分布，不引入缺省路由。

使用 **redistribute** 命令，配置路由重分布。

使用 **default-information originate** 命令，引入缺省路由。

配置路由重分布、引入缺省路由后，路由器自动成为 ASBR。

↘ 路由汇聚

缺省情况下，不进行路由汇聚。如果配置路由汇聚，会自动添加 discard 路由。

使用 **arearange** 命令，在 ABR 上汇聚区域间发布的路由（LSA Type 3）。

使用 **summary-prefix** 命令，在 ASBR 上汇聚重分布路由（LSA Type 5）。

↘ 路由过滤

缺省情况下，不进行路由过滤。

使用 **passive-interface** 命令，设置被动接口。被动接口上不能交互路由信息（任意 LSA）。

使用 **redistribute** 命令的 **route-map** 参数，或使用 **distribute-list out** 命令，在 ASBR 上过滤 AS 外部的路由信息。只有满足过滤条件的路由信息才能被重分布到 OSPF 进程（LSA Type 5）。

使用 **distribute-listin** 命令，过滤路由器收到的 LSA。OSPF 路由表中，只有由满足过滤条件的 LSA 计算出的路由才能执行报文转发。

↘ 路由代价

- 从接口到直连网段的代价（即接口上的 cost 值）

  缺省值为自动代价。自动代价 = 参考带宽/接口带宽。

  使用 **auto-cost reference-bandwidth** 命令，设置自动代价的参考带宽，缺省值为 100Mbps。

  使用 **ipv6 ospf cost** 命令，人为设置接口上的 cost 值。此项配置优先级高于自动代价。

- 从接口到指定邻居的代价（即从本地到指定邻居的 cost 值）

  缺省值为自动代价。

  使用 **ipv6 ospf neighbor** 命令中的 **cost** 参数，修改接口到指定邻居的代价。此项配置优先级高于接口上的 cost 值。只有 P2MP 类型的接口允许此项配置。

- 从 ABR 到缺省网段的代价（ABR 自动向 Stub、NSSA 区域发布的缺省路由的 cost 值）

  缺省值为 1。

  使用 **area default-cost** 命令，修改 ABR 自动向 Stub 区域发布的缺省路由的 cost 值。

- 从 ASBR 到外部网段的代价（外部路由的 metric 值）

  缺省情况下，重分布 BGP 路由的 metric 为 1，重分布其它路由的 metric 为 20，路由类型 Type2 External。

  使用 **default-metric** 命令，修改外部路由的 metric 值的缺省值。

  使用 **redistribute** 命令中的 **metric**、**metric-type**、**route-map** 参数，修改外部路由的 metric 值、路由类型。

- 从 ASBR 到缺省网段的代价（人为引入的缺省路由的 metric 值）

  缺省情况下，metric 为 1，路由类型 Type2 External。

  使用 **default-information originate** 命令的 **metric**、**metric-type**、**route-map** 参数，修改人为引入的缺省路由的 metric 值、路由类型。

  使用 **area nssa** 命令的 **default-information-originate** 参数的 **metric**、**metric-type** 参数，修改 NSSA 区域内人为引入的缺省路由的 metric 值、路由类型。

↘ OSPF 管理距离

缺省情况下，OSPF 管理距离为 110。

使用 **distance** 命令，设置 OSPF 路由的管理距离值。

6.3.3 增强安全性、可靠性

认证、与 BFD 联动等功能使 OSPF 更安全、更稳定可靠。

工作原理

↘ 认证

OSPFv3 利用 IPv6 提供的认证机制，即 IP 认证头部（AH）和 IP 封装安全负载（ESP），来阻止非法接入网络的路由器和伪造 OSPF 报文的主机参与 OSPF 路由交换。在 OSPF 接口（或虚链路两端）上对收到的 OSPF 报文进行认证。如果认证失败，则丢弃报文，邻接关系将不能被建立。

↘ 启动认证功能后，可以避免学到非认证、无效路由，避免将有效路由通告到非认证设备。在广播类型网络中，认证还可以避免非认证设备成为指定设备的可能性，保证了路由系统的稳定性和抗入侵性。MTU 校验

OSPF 在收到 DD 时会校验邻居的接口的 MTU 和自己接口的 MTU 是否相同，如果收到的 DD 报文中指示的接口的 MTU 大于接收接口的 MTU，则邻接关系将不能被建立。关闭 MTU 的校验，可以避免此问题。

↘ 双向维持

OSPF 路由器之间通过周期性发送 Hello 报文来维持邻接关系。在较大的网络中 ,可能会出现大量的报文收发 ,占用较高的 CPU 和内存资源，造成部分部分报文的延迟或丢弃。如果 Hello 报文的处理超出了死亡间隔，将导致邻接关系断开。

如果启用双向维持功能，则除了 Hello 报文外，DD、LSU、LSR、LSAck 报文也能用来维持邻居之间的双向通信，从而使邻接关系更加稳定。

↘ 并发邻居数量限制

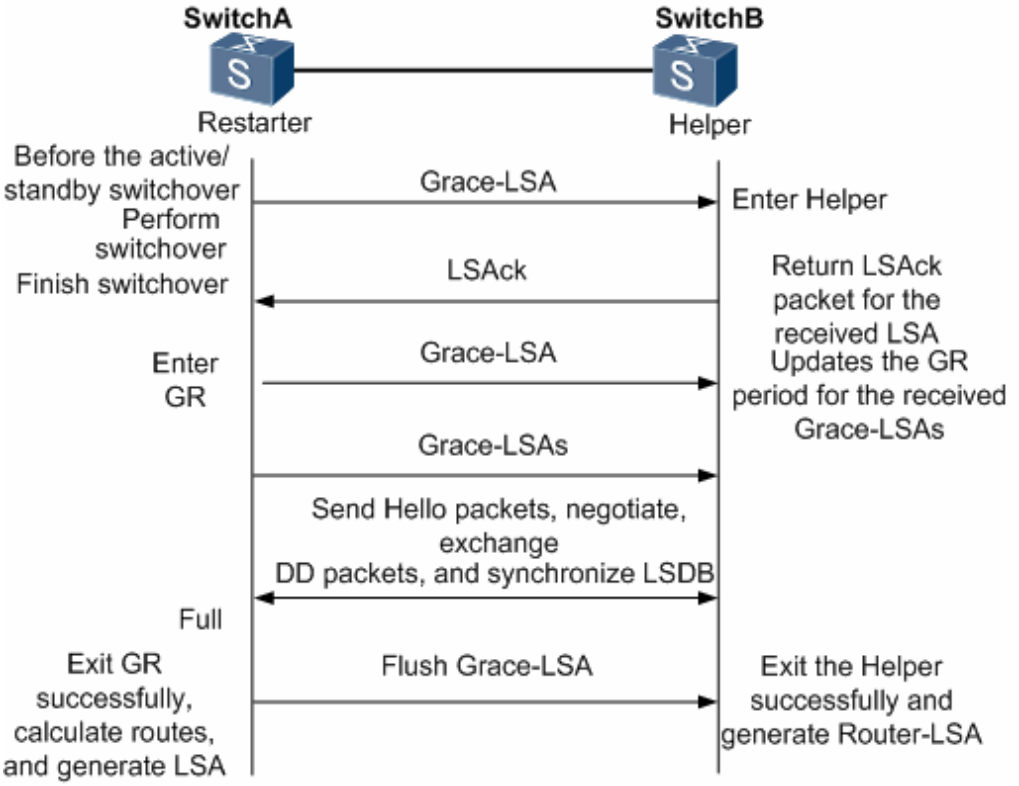
当路由器同时与多个邻居交换数据时，其性能会受到影响。限制 OSPF 进程可并发交互（发起或接受）的邻居最大数目，使路由器可以分批与邻居进行交互，有助于保障数据转发或其他关键业务。

↘ GR

路由器普遍采用了控制和转发分离的技术。在网络拓扑保持稳定的情况下，启用 GR（Graceful Restart，优雅重启）功能的路由器在控制层面的重启过程中转发层面能够继续指导数据的转发，同时控制层面邻居关系的重建以及路由计算等动作不会影响转发层面的功能，从而避免了路由震荡引发的业务中断，提高了整网的可靠性。

目前，GR 功能只在主备切换和系统升级过程中使用。

图 6-7 正常的 OSPF GR 过程



- GR 过程需要 Restarter 和 Helper 的协作。Restarter 是发生 GR 的路由器。Helper 是 Restarter 的邻居。
- Restarter 在开始和退出 GR 时向邻居发送 Grace-LSA，通知邻居进入和退出 Helper 状态。
- Restarter 与 Helper 邻居关系达到 Full 状态，则 GR 可成功退出。

Fast Hello、与 BFD 联动

Fast Hello

当发生链路故障后，OSPF 需要一段时间（约 40 秒）才能感知邻居死亡。而后再将此信息传播出去、并重新计算 SPT。这期间会发生流量中断。

- 启动 Fast Hello 功能（即将邻居死亡时间设置为 1 秒）后，一旦发生链路故障后，OSPF 可以在 1 秒内感知到邻居死亡。从而大大加快路由收敛，避免流量中断。
- BFD（Bidirectional Forwarding Detection，双向转发检测）用于检测设备之间的连通性，最短能够在 150 毫秒内发现链路故障。将 OSPF 与 BFD 联动后，一旦发生链路故障，OSPF 最短可以在 150 毫秒内感知到邻居死亡。从而大大加快路由收敛，避免流量中断。

相关配置

OSPF 报文认证

缺省情况下，关闭认证功能。

- 使用 **area authentication** 命令，在整个区域上启动认证功能，在该区域内所有接口上生效。如果在区域 0 上启动认证功能，则也对虚链路生效。
- 使用 **area encryption** 命令，在整个区域上启动加密认证功能，在该区域内所有接口上生效。如果在区域 0 上启动加密认证功能，则也对虚链路生效。

- 使用 **ipv6 ospf authentication** 命令，在接口上启动认证功能，优先级高于区域上的配置。
- 使用 **ipv6 ospf encryption** 命令，在接口上启动加密认证功能，优先级高于区域上的配置。
- 使用 **area virtual-link** 命令的 **authentication** 参数，在虚链路两端启动认证功能，优先级高于区域上的配置。
- 使用 **area virtual-link** 命令的 **encryption** 参数，在虚链路两端启动加密认证功能，优先级高于区域上的配置。

MTU 校验

缺省情况下，关闭 MTU 校验。

使用 **ipv6 ospf mtu-ignore** 命令，在接口上关闭 MTU 校验。

双向维持

缺省情况下，启动双向维持功能。

使用 **two-way-maintain** 命令，启动双向维持功能。

并发邻居数量限制

使用 **max-concurrent-dd** 命令，修改当前 OSPF 进程并发交互的邻居数量限制。缺省值 5。

使用 **ipv6 router ospf max-concurrent-dd** 命令，修改路由器上所有 OSPF 进程并发交互的邻居总数限制。缺省值 10。

GR

缺省情况下，关闭 Restarter 功能，启动 Helper 功能。

使用 **graceful-restart** 命令，配置 Restarter 功能。

使用 **graceful-restart helper** 命令，配置 Helper 功能。

Fast Hello

缺省情况下，接口上的邻居死亡时间为 40 秒。

使用 **ipv6 ospf dead-intervalminimal hello-multiplier** 命令，在接口上启动 Fast Hello 功能（邻居死亡时间为 1 秒）。

OSPF 与 BFD 联动

缺省情况下，OSPF 不与 BFD 联动。

使用 **bfd interval min_rx multiplier** 命令，设置 BFD 参数。

使用 **bfd all-interfaces** 命令，所有接口启用 OSPF 与 BFD 联动。

使用 **ipv6 ospf bfd** 命令，当前接口启动 OSPF 与 BFD 联动。

6.3.4 支持网管功能

MIB、SYSLOG 等功能使 OSPF 更易于管理。

工作原理

MIB

MIB（管理信息库）是设备端维护的设备状态信息集。管理程序可以对 MIB 节点进行查阅和设置。

路由器上可以同时启动多个 OSPF 进程，但 OSPF MIB 只能与一个 OSPF 进程绑定。

Trap

告警是系统检测到故障而产生的通知，告警中携带对应的故障信息。

启动 Trap 功能，则路由器可以主动将告警信息发送到网管设备。

Syslog

日志记录了用户对路由器的操作（比如命令配置）以及特定事件（比如网络连接失效）等信息。

允许日志记录邻接状态变化，则网络管理员可以通过查看日志了解 OSPF 邻居之间建立和维持邻接关系的全过程。

相关配置

MIB

缺省情况下，MIB 绑定在进程号最小的 OSPF 进程上。

使用 **enable mib-binding** 命令，将 MIB 绑定在当前 OSFP 进程上。

Trap

缺省情况下，所有 TRAP 开关关闭，且不允许设备发送 OSPFTrap。

使用 **snmp-server enable traps ospf** 命令，允许设备发送 OSPF Trap。

使用 **enable traps** 命令，在 OSFP 进程下打开指定的 Trap 开关。

Syslog

缺省情况下，允许日志记录邻接状态变化。

使用 **log-adj-changes** 命令，允许日志记录邻接状态变化。

6.4 产品说明

NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE 支持OSPFV3功能，NBR800G、NBR950G、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR108G-P、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1500G、NBR2000G 不支持 OSPFV3 功能。

6.5 配置详解

配置项	配置建议&相关命令	
配置 OSPF 基本功能	必须配置。用于构建 OSPF 路由域。	
	ipv6 router ospf	创建 OSPF 进程。
	router-id	设置 Router ID。
	ipv6 ospf area	在接口上启动 OSPF 进程，指定 Area ID。
	area virtual-link	创建虚链路。
设置网络类型	可选配置。如果物理网络为 X.25、帧中继、ATM，则必须配置此项。	
	ipv6 ospf network	定义网络类型。
	ipv6 ospf neighbor	指定邻居。
	ipv6 ospf priority	配置 DR 优先级。
配置路由重分布、缺省路由	可选配置。如果 OSPF 路由域连接外网，则建议配置此项。	
	redistribute	路由重分布。
	default-information originate	引入缺省路由。
设置 Stub、NSSA 区域	可选配置。有助于减少路由信息的交互，缩小路由表规模，增强路由稳定性。	
	area stub	设置 Stub 区域。
	area nssa	设置 NSSA 区域。
配置路由汇聚	可选配置。有助于减少路由信息的交互，缩小路由表规模，增强路由稳定性。	
	area range	汇聚区域间发布的路由信息。
	summary-prefix	汇聚重分布引入的路由信息。
配置路由过滤	可选配置。人为控制路由信息交互过程、筛选可用的 OSPF 路由。	
	passive-interface	设置被动接口。
	distribute-list out	对重分布引入的路由进行过滤。

	distribute-list in	对收到的 LSA 进行过滤。
修改路由代价、管理距离	⚠ 可选配置。人为控制 OSPF 计算的最短路径、是否优先选择 OSPF 路由。	
	auto-cost reference-bandwidth	修改自动代价的参考带宽。
	ipv6 ospf cost	修改接口出方向的 cost 值。
	area default-cost	修改 Stub/NSSA 区域缺省路由的 cost 值。
	default-metric	修改重分布路由的缺省 metric 值。
	distance	修改 OSPF 管理距离。
启动认证功能	⚠ 可选配置。阻止非法接入网络的路由器和伪造 OSPF 报文的主机参与 OSPF 协议。	
	area authentication	在区域上启动认证、设置认证方式。
	area encryption	在区域上启动加密认证、设置认证方式。
	ipv6 ospf authentication	在接口上启动认证、设置认证方式。
	ipv6 ospf encryption	在接口上启动加密认证、设置认证方式。
修改并发邻居数量限制	⚠ 可选配置。避免由于过度消耗 CPU 导致设备性能下降的问题。	
	max-concurrent-dd	修改当前 OSPF 进程上的并发邻居数量限制。
	ipv6 router ospf max-concurrent-dd	修改所有 OSPF 进程上的并发邻居总数限制。
关闭 MTU 校验	⚠ 可选配置。避免由于邻居接口 MTU 不一致导致无法建立邻接关系的问题。	
	ipv6 ospf mtu-ignore	在接口上关闭 MTU 校验功能。
启动双向维持	⚠ 可选配置。避免由于 Hello 报文延迟或丢失导致邻接关系断开的问题。	
	two-way-maintain	启动双向维持功能。
启动 GR 功能	⚠ 可选配置。在 OSPF 进程重启或主备切换过程中，维持 OSPF 路由转发，避免流量中断。	
	graceful-restart	启动 Restarter 功能。
	graceful-restart helper	启动 Helper 功能。
启动 Fast Hello	⚠ 可选配置。在链路故障时，快速发现邻居死亡，避免流量中断。	
	ipv6 ospf dead-intervalminimal hello-multiplier	在接口上启动 Fast Hello 功能。
配置网管功能	⚠ 可选配置。使用户可以通过 SNMP 网管软件来管理 OSPF。	
	enable mib-binding	OSFP 进程绑定 MIB。
	enable traps	打开 OSFP 进程的 Trap 开关。
	log-adj-changes	允许日志记录邻接状态变化。
修改协议控制参数	⚠ 可选配置。除非必要，不建议修改协议控制参数。	
	ipv6 ospf hello-interval	修改接口上的 hello 报文发送间隔。
	ipv6 ospf dead-interval	修改接口上的邻居死亡时间。
	ipv6 ospf transmit-delay	修改接口上的 LSU 报文传输延时。
	ipv6 ospf retransmit-interval	修改接口上的 LSU 报文重传间隔。
	timers throttle lsa all	修改生成 LSA 的指数退避算法参数。
	timerspacinglsa-group	修改分组刷新 LSA 的分组时间。
	timers pacing lsa-transmit	修改分组刷新 LSA 的发送间隔。
	timers lsa arrival	修改接收相同 LSA 的延时。
	timers throttlespf	修改计算 SPT 的计时器。
	timers throttle route inter-area	修订区间路由计算的延时间隔。

	timers throttle route ase	修订外部路由计算的延时间隔。

6.5.1 配置OSPF基本功能

配置效果

- 在网络中建立一个 OSPF 路由域，为网络内用户提供 IPv6 单播路由服务。

注意事项

- 需要确保 IPv6 路由功能启用，即 ipv6 routing 开关未被关闭，才能够启用 OSPF。
- 接口必须使能 IPv6。
- 强烈建议进行手工配置 Router ID。

配置方法

创建 OSPF 进程

- 必须配置。
- 每台路由器都需要配置。

设置实例 ID

- 可选配置，但强烈建议手工配置 Router ID
- 不配置 Router ID 时，OSPF 会选择接口 IP 地址，若没有接口配置 IP 地址或者配置的 IP 地址已经被其他 OSPF 实例使用，那么需要手工配置 Router ID。

在接口上启动 OSPF，指定 Area ID

- 必须配置。
- 每台路由器都需要配置。

检验方法

- 通过 **show ipv6 route ospf** 命令查看 OSPF 路由表项加载正确。
- 通过 **ping** 命令查看 IPv6 单播业务正确。

相关命令

创建 OSPF 进程

【命令格式】 **ipv6 router ospf***process-id* [**vrf***vrf-name*]

【参数说明】 *process-id*：OSPFv3 进程号。未配置进程号时，表示开启进程 1。

vrf-name：指定 OSPFv3 进程所属的 VRF。

【命令模式】 全局配置模式。

【使用指导】 打开 OSPFv3 进程后，将进入路由进程配置模式。

设置 Router ID

【命令格式】 **router-id***router-id*

【参数说明】 *router-id*：设备的标识，使用 IPv4 地址格式表示。

【命令模式】 OSPF 路由进程配置模式。

【使用指导】 每台运行 OSPFv3 进程的设备都必须使用一个 Router ID 来标识。可以配置任何一个 IPv4 地址作为该路由设

备的路由设备标识，但是必须保证自治系统中每台路由设备的路由设备标识唯一，如果同一台设备运行多个 OSPFv3 进程，也必须保证每个进程的路由设备标识唯一。

注意路由设备标识改变后，协议内部会做大量处理，所以不主张随意改变路由设备标识，修改路由设备标识时会提示是否确定要修改。建议在启动 OSPFv3 进程后，先指定好 Router ID，在配置 OSPFv3 进程其他参数。

在接口上启动 OSPF，指定 Area ID

【命令格式】 **ipv6 ospf***process-id* **area***area-id* [**instance***instance-id*]

【参数说明】 *process-id*：OSPFv3 进程号，范围 1-65535。

area*area-id*：接口所参与的 OSPFv3 区域，其可以指定为一个整数或者一个 IPv4 前缀。

instance*instance-id*：对接口特定 OSPFv3 实体进行配置，范围 0-255。

【命令模式】 接口配置模式。

【使用指导】 可以在接口配置模式下，先使用本命令启动接口参与 OSPFv3，再通过 **ipv6 router ospf** 配置 OSPFv3 进程，配置完 OSPFv3 进程后，接口将自动参与相应的进程。

使用 **no ipv6 ospfarea** 命令指定接口将不再参与 OSPFv3 路由进程。

使用 **no ipv6 router ospf** 命令所有接口都不再参与 OSPFv3 路由进程。

只有 *instance-id* 相同的设备之间才能正常建立邻接关系。

配置本命令后，接口上所有的前缀信息都将参与 OSPFv3 运行。

配置虚链路

【命令格式】 **area** *area-id***virtual-link***router-id* [**hello-interval** *seconds*] [**dead-interval***seconds*] [**retransmit-interval***seconds*] [**transmit-delay***seconds*] [**instance***instance-id*] [**authenticationipsec spi***spi*[**md5|sha1**] [**0|7**] *key*] [**encryption ipsec spi***spi* **esp** [**null**|[**des | 3des**] [**0** | **7**]*des-key*][**md5|sha1**] [**0|7**] *key*]

【参数说明】 *area-id*：虚拟连接所在区域的区域号，其可以指定为一个整数或者一个 IPv4 前缀。

router-id：虚拟连接的邻居的标识(router-ID)。

dead-interval*seconds*：虚拟连接本地接口上认为邻居失效的时间，范围 1-65535 秒。

hello-interval *seconds*：虚拟连接本地接口上发送 hello 报文的间隔，范围 1-65535 秒。

retransmit-interval *seconds*：虚拟连接本地接口上发送 LSA 的重传间隔，范围 1-65535 秒。

transmit-delay *seconds*：虚拟连接本地接口上发送 LSA 的延迟时间，取值范围：1-65535。

instance*instance-id*：指定虚链接对应的 instance，不同的 instance 无法正确建立虚链接，范围 0-255。*spi*：安全参数索引，范围是 256-4294967295。

md5：指定 md5 认证模式。

sha1：指定 sha1 认证模式。

0：指定密钥以明文显示。

7：指定密钥以密文显示。

key：认证密钥。

null：不采用加密。

des：指定 des 加密模式。

3des：指定 3des 加密模式。

des-key：加密密钥。

【命令模式】 OSPF 路由进程配置模式。

【使用指导】 在 OSPFv3 自治域中，所有区域都必须与主干区域连接，以保证能够正确学习到整个 OSPFv3 自治域的路由

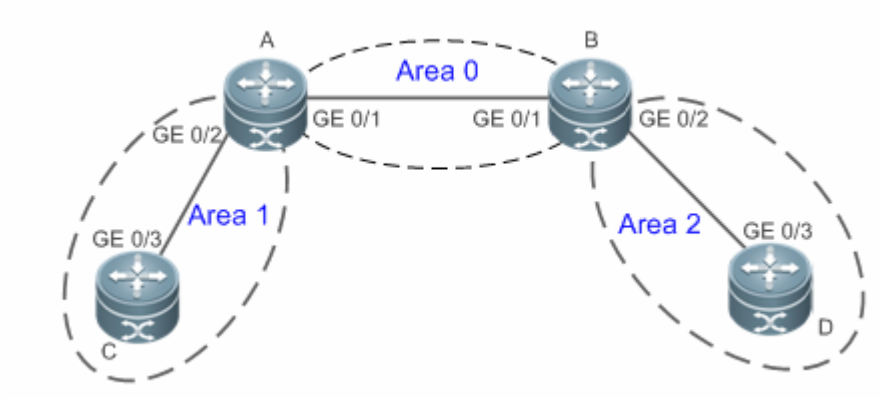
信息。如果一个区域无法直接与主干区域连接，可以使用虚拟连接使该区域同主干区域相连。

虚拟连接所在的区域不允许是 stub 或者 NSSA 区域。

虚拟连接邻居两端上配置的参数中，**hello-interval**、**dead-interval** 和 **instance** 都必须一致，否则虚拟邻居之间无法正确建立邻居关系。

配置举例

【网络环境】



【注释】 接口 IP 地址：

A： GE 0/1 2001:1::1/64 G E 0/2 2001:2::1/64

B： GE 0/1 2001:1::2/64 G E 0/2 2001:3::1/64

C： GE 0/3 2001:2::2/64

D： GE 0/3 2001:3::2/64

【配置方法】

- 在所有路由器上配置接口 IP 地址。
- 在所有路由器上启动 IPv4 单播路由功能（该功能默认已开启）。
- 在所有路由器上配置 OSPF 实例、Router ID
- 在所有路由器上配置接口使能 OSPF

A

```
A#configure terminal
A(config)#interface GigabitEthernet 0/1
A(config-if-GigabitEthernet 0/1)#ipv6 enable
A(config-if-GigabitEthernet 0/1)#ipv6 address 2001:1::1/64
A(config-if-GigabitEthernet 0/1)#ipv6 ospf 1 area 0
A(config-if-GigabitEthernet 0/1)#exit
A(config)#interface GigabitEthernet 0/2
A(config-if-GigabitEthernet 0/2)#ipv6 enable
A(config-if-GigabitEthernet 0/2)#ipv6 address 2001:2::1/64
A(config-if-GigabitEthernet 0/2)#ipv6 ospf 1 area 1
A(config-if-GigabitEthernet 0/2)#exit
A(config)#ipv6 router ospf 1
A(config-router)#router-id1.1.1.1
```

B

```
B#configure terminal
B(config)#interface GigabitEthernet 0/1
B(config-if-GigabitEthernet 0/1)#ipv6 enable
```

```
B(config-if-GigabitEthernet 0/1)#ipv6 address 2001:1::2/64
B(config-if-GigabitEthernet 0/1)#ipv6 ospf 1 area 0
B(config-if-GigabitEthernet 0/1)#exit
B(config)#interface GigabitEthernet 0/2
B(config-if-GigabitEthernet 0/2)#ipv6 enable
B(config-if-GigabitEthernet 0/2)#ipv6 address 2001:3::1/64
B(config-if-GigabitEthernet 0/2)#ipv6 ospf 1 area 2
B(config-if-GigabitEthernet 0/2)#exit
B(config)#ipv6 router ospf 1
B(config-router)#router-id2.2.2.2
```

C

```
C#configure terminal
C(config)#interface GigabitEthernet 0/3
C(config-if-GigabitEthernet 0/3)#ipv6 enable
C(config-if-GigabitEthernet 0/3)#ipv6 address 2001:2::2/64
C(config-if-GigabitEthernet 0/3)#ipv6 ospf 1 area 1
C(config-if-GigabitEthernet 0/3)#exit
C(config)#ipv6 router ospf 1
C(config-router)#router-id3.3.3.3
```

D

```
D#configure terminal
D(config)#interface GigabitEthernet 0/3
D(config-if-GigabitEthernet 0/3)#ipv6 enable
D(config-if-GigabitEthernet 0/3)#ipv6 address 2001:4::2/64
D(config-if-GigabitEthernet 0/3)#ipv6 ospf 1 area 2
D(config-if-GigabitEthernet 0/3)#exit
D(config)#ipv6 router ospf 1
D(config-router)#router-id4.4.4.4
```

【检验方法】

- 所有路由器上检查 OSPF 邻居正确。
- 所有路由器上检查路由表加载正确。
- 路由器 D 上 ping 2001:2::2/64 正确。

A

```
A#show ipv6 ospf neighbor
OSPFv3 Process (1), 1 Neighbors, 1 is Full:
Neighbor ID     Pri   State           Dead Time   Instance ID   Interface
2.2.2.2           1   Full/BDR        00:00:30    0             GigabitEthernet 0/1
3.3.3.3           1   Full/BDR        00:00:35    0             GigabitEthernet 0/2

A#show ipv6 route ospf

IPv6 routing table name - Default - 0 entries
Codes:  C - Connected, L - Local, S - Static
        R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
        E1 - OSPF external type 1, E2 - OSPF external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - Inter area

O  IA  2001:3::/64 [110/20] via FE80::2D0:F8FF:FE22:4524, GigabitEthernet 0/1
```

B

```
B# show ipv6 ospf neighbor
OSPFv3 Process (1), 1 Neighbors, 1 is Full:
Neighbor ID     Pri   State           Dead Time   Instance ID   Interface
1.1.1.1           1   Full/DR         00:00:30    0             GigabitEthernet 0/1
4.4.4.4           1   Full/BDR        00:00:35    0             GigabitEthernet 0/2

B#show ipv6 route ospf

IPv6 routing table name - Default - 0 entries
Codes:  C - Connected, L - Local, S - Static
        R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - Inter area

O  IA  2001:2::/64 [110/20] via FE80::2D0:F8FF:FE22:4536, GigabitEthernet 0/1
```

C

```
C# show ipv6 ospf neighbor
OSPFv3 Process (1), 1 Neighbors, 1 is Full:
Neighbor ID     Pri   State           Dead Time   Instance ID   Interface
1.1.1.1           1   Full/DR         00:00:30    0             GigabitEthernet 0/3

C#show ipv6 route ospf

IPv6 routing table name - Default - 0 entries
Codes:  C - Connected, L - Local, S - Static
        R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - Inter area

O  IA  2001:1::/64 [110/2] via FE80::2D0:F8FF:FE22:4537, GigabitEthernet 0/3
O  IA  2001:3::/64 [110/3] via FE80::2D0:F8FF:FE22:4537, GigabitEthernet 0/3
```

D

```
D# show ipv6 ospf neighbor
OSPFv3 Process (1), 1 Neighbors, 1 is Full:
```

```
Neighbor ID     Pri   State           Dead Time   Instance ID   Interface
2.2.2.2           1   Full/DR         00:00:30    0             GigabitEthernet 0/3

D#show ipv6 route ospf

IPv6 routing table name - Default - 0 entries
Codes:  C - Connected, L - Local, S - Static
        R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - Inter area

O  IA  2001:1::/64 [110/2] via FE80::2D0:F8FF:FE22:4547, GigabitEthernet 0/3
O  IA  2001:2::/64 [110/3] via FE80::2D0:F8FF:FE22:4547, GigabitEthernet 0/3
D#
D#ping 2001:2::2
Sending 5, 100-byte ICMP Echoes to 2001:2::2, timeout is 2 seconds:
< press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/9/14 ms.
```

常见错误

- 接口没有使能 IPv6。
- IPv6 单播路由功能被关闭，OSPF 协议无法启用。
- 相连接口使能的区域号不一致。
- 多台路由器上配置了相同的 Router ID，导致 Router ID 冲突。

6.5.2 设置网络类型

配置效果

- 物理网络为 X.25、帧中继、ATM 时，也可以运行 OSPF 协议，提供 IPv6 单播路由服务。

注意事项

- 必须配置 OSPF 基本功能
- 广播网络以组播方式发送 OSPF 报文，自动发现邻居，需要选举 DR 和 BDR。
- P2P 网络以组播方式发送 OSPF 报文，自动发现邻居。
- NBMA 网络以单播方式发送 OSPF 报文，必须手动指定邻居，需要选举 DR 和 BDR。
- P2MP 网络（不携带 **non-broadcast** 参数）以组播方式发送 OSPF 报文，自动发现邻居。
- P2MP 网络（携带 **non-broadcast** 参数）以单播方式发送 OSPF 报文，必须手动指定邻居。

配置方法

配置接口网络类型

- 可选配置。
- 链路俩端路由器都需要配置。

配置邻居

- 可选配置。若接口的网络类型配置为 NBMA 或者 P2MP（携带 **non-broadcast** 参数），则必须配置
- 在 NBMA 或者 P2MP（携带 **non-broadcast** 参数）网络两端路由器上配置。

配置接口优先级

- 可选配置。若需要指定路由器做为 DR 或者禁止路由器做为 DR，需要配置。
- 在被指定为 DR 或者被禁止做为 DR 的路由器上配置。

检验方法

- 通过 **show ipv6 ospf interface** 查看接口的网络类型正确。

相关命令

配置接口网络类型

【命令格式】 **ipv6 ospf network** {**broadcast** | **non-broadcast** |**point-to-point** | **point-to-multipoint**[**non-broadcast**]}[**instance***instance-id*]

【参数说明】 **broadcast**：设置广播网络类型。

non-broadcast：设置非广播网络类型。

point-to-multipoint：设置点对多点网络类型。

point-to-multipoint non-broadcast：设置点对多点非广播网络类型。

point-to-point：设置点对点网络类型。

instance*instance-id*：对接口特定 OSPFv3 实体进行配置，范围 0-255。

【命令模式】 接口配置模式

【使用指导】 可以根据实际应用的链路类型和拓扑关系，设定接口的网络类型。

配置邻居

【命令格式】 **ipv6 ospf neighbor** *ipv6-address*{ [**cost***cost*] | [**poll-interval***seconds* | **priority***value*] }[**instance***instance-id*]

【参数说明】 *ip-address*：邻居接口的链路地址。。

cost*cost*：设置点到多点网络到每个邻居所要的费用，缺省未定义，使用接口上配置的 cost，范围 1-65535。点到多点网络类型(point-to-multipoint)才支持该选项。

poll-interval *seconds*：邻居轮询时间间隔，以秒为单位，范围 1-2147483647。非广播网络类型(NBMA)才支持该选项。

priority *value*：设置非广播网络邻居的优先权值，范围 0-255。非广播网络类型(NBMA)才支持该选项。

instance*instance-id*：对接口特定 OSPFv3 实体进行配置，范围 0-255。

【命令模式】 接口配置模式

【使用指导】 用户可以根据实际网络类型，设置邻居相应参数。

配置接口优先级

【命令格式】 **ipv6 ospf priority** *number-value*[**instance***instance-id*]

【参数说明】 *number-value*：接口的优先级。范围 0-255。

instance*instance-id*：对接口特定 OSPFv3 实体进行配置，范围 0-255。

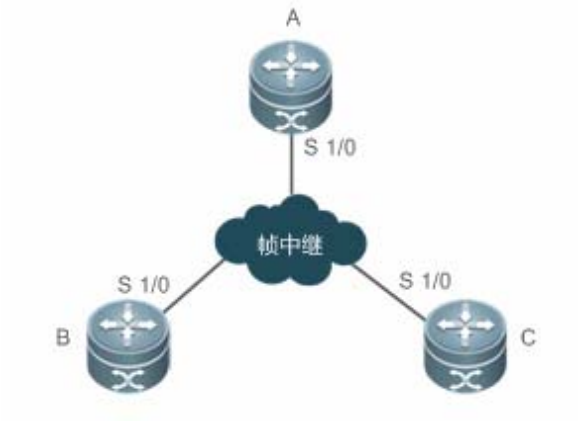
【命令模式】 接口配置模式

【使用指导】 当广播网络类型中，需要选举 DR/BDR(指定路由设备/备份指定路由设备)。在进行 DR/BDR 选举时，优先级值高的设备将优先成为 DR 或 BDR，如果优先级值相同，Router-ID 值高的设备，将优先成为 DR 或 BDR。优先级值为 0 的设备，将不参与 DR/BDR 的选举。

配置举例

配置接口网络类型

【网络环境】



【配置方法】

- 所有路由器接口使能 IPv6。略。
- 所有路由器配置 OSPF 基本功能。略。
- 所有路由器上配置接口的网络类型为 P2MP。

A

```
A#configure terminal
A(config)# interface Serial1/0
A(config-Serial1/0)# encapsulation frame-relay
A(config-Serial1/0)# ipv6 ospf network point-to-multipoint
```

B

```
B#configure terminal
B(config)# interface Serial1/0
B(config-Serial1/0)# encapsulation frame-relay
B(config-Serial1/0)# ipv6 ospf network point-to-multipoint
```

C

```
C#configure terminal
C(config)# interface Serial1/0
C(config-Serial1/0)# encapsulation frame-relay
C(config-Serial1/0)# ipv6 ospf network point-to-multipoint
```

【检验方法】

- 查看接口的网络类型为 P2MP。

A

```
A#show ipv6 ospf interface Serial1/0
Serial1/0 is up, line protocol is up
  Interface ID 2
  IPv6 Prefixes
    fe80::2d0:f8ff:fe22:3346/64 (Link-Local Address)
  OSPFv3 Process (1), Area 0.0.0.1, Instance ID 0
    Router ID 192.168.22.30,Network Type POINTOMULTIPOINT, Cost: 1
    Transmit Delay is 1 sec, State Point-To-Point, Priority 1
    Timer interval configured, Hello 30, Dead 120, Wait 40, Retransmit 10
      Hello due in 00:00:06
    Neighbor Count is 1, Adjacent neighbor count is 1
  Hello received 40 sent 40, DD received 17 sent 9
  LS-Req received 1 sent 3, LS-Upd received 6 sent 5
  LS-Ack received 3 sent 4, Discarded 1
```

常见配置错误

- 两端接口配置的网络类型不一致，导致路由学习不正常。
- 网络类型配置为 NBMA，P2MP（携带 **non-broadcast** 参数），但没有指定邻居。

6.5.3 配置路由重分布、缺省路由

配置效果

- 在 OSPF 域内引入其他 AS 域的单播路由，为 OSPF 域内的用户提供到其他 AS 域的单播路由服务。
- 往 OSPF 域内注入一条通往其他 AS 域的默认路由，为 OSPF 域内的用户提供到其他 AS 域的单播路由服务。

注意事项

- 必须配置 OSPF 基本功能

配置方法

配置重分发外部路由

- 可选配置。若在 AS 边界路由器上需要引入 OSPF 域外路由时，需要配置
- 在 AS 边界路由器上配置。

配置生成缺省路由

- 可选配置。若在 AS 边界路由器上需要引入默认路由，使得 OSPF 域内访问其他 AS 域默认通过该边界路由器，则需要配置。
- 在 AS 边界路由器上配置。

检验方法

- OSPF 域内路由器通过 **show ipv6 route ospf** 查看加载了其他 AS 域的单播路由。
- OSPF 域内路由器通过 **show ipv6 route ospf** 查看加载了到达 ASBR 的默认路由。
- 通过 **ping** 命令查看通往其他 AS 域的 IPv6 单播业务正确。

相关命令

配置重分发路由

【命令格式】 **redistribute** {**bgp** | **connected** | **isis**[*area-tag*] | **ospf***process-id* | **rip** | **static**}[{**level-1** | **level-1-2** | **level-2**} | **match** {**internal | external** [**1|2**] **nssa-external** [**1|2**]} | **metric** *metric-value*|**metric-type** {**1**|**2**} | **route-map** *route-map-name* |**tag***tag-value*]

【参数说明】 **bgp**：从 bgp 重分布

connected：从直连路由重分布

isis [*area-tag*]：从 isis 重分布，通过 *area-tag* 指定具体某个 isis 实例

ospf*process-id*：从 ospf 重分布，通过 *process-id* 指定具体某个 ospf 实例，取值范围：1-65535

rip：从 rip 重分布

static：从静态路由重分布

level-1 | **level-1-2** | **level-2**：只针对配置重分布 IS-IS 路由时使用，用于指定特定 level 的路由进行重分布，默认状态只允许 level-2 的 IS-IS 路由进行重分布。

match：只针对配置重分布 OSPF 路由时使用，用于过滤特定路由进行重分布，默认状态允许所有的 OSPF 路由进行重分布。

metric*metric-value*：设置 OSPF external LSA 的 metric，通过 metric-value 指定 metric 大小，取值范围：0-16777214。

metric-type {**1**|**2**}：设置外部路由类型为 E-1 或 E-2。

route-map*route-map-name*：设置重分布过滤规则。

tag*tag-value*：设置重分布到 OSPF 内路由的 tag 值，取值范围：0-4294967295。

【配置模式】 OSPF 路由进程配置模式

【使用指导】 当设备支持了多个路由协议时，各协议之间的互相合作是一个非常重要的内容。设备在同一时间要能运行多个路由协议，它必须能将一个协议的信息重新分配到另一个协议。这对所有路由协议都是适用的。

重分发 ISIS 协议路由时，允许后面配置 level-1、level-2 或 level-1-2 参数，表示重分发 ISIS 路由中对应 level 的路由，默认情况为重分发 level-2 类型的 ISIS 路由。

重分发 OSPFv3 协议路由时，允许后面配置 *match* 参数，表示重分发 OSPFv3 路由中，对应子类型的路由，默认情况为重分发所有类型的 OSPFv3 路由。

对于重分发 ISIS 时的 *level* 以及 OSPFv3 的 *match* 参数，只有路由子类型正确的，才进行 route-map 的匹配。

对于重分发 OSPFv3 的 match 参数，只有路由子类型正确的，才进行 route-map 的匹配。

配置重分发时 route-map 规则中的 *match* 参数是针对路由的原始信息进行匹配的，重分发配置中的 tag，*metric* 与 *metric-type* 参数优先级低于 *route-map* 中对应该参数 *set* 规则的优先级。

所关联的 route-map 的 set metric 取值范围应当为<0-16777214>，如果超出该范围，将无法引入路由。

redistribute 命令的 no 形式配置的规则如下：

1．如果 no 命令指定某些参数，则将这些参数恢复缺省配置；

2．如果 no 命令不指定任何参数，则将整个命令删除。

例如：已知配置了 redistribute isis 112 level-2，通过命令 no redistribute isis 112 level-2 修改配置，则该命令仅将 level-2 参数恢复缺省值。而 level-2 本身又是参数缺省值，所以，执行上述 no 命令后，配置仍保存为 redistribute isis 112 level-2。如果要将整个命令删除需配置 no redistribute isis 112。

配置导入缺省路由

【命令格式】 **default-information originate** [**always**] [**metric** *metric*] [**metric-type** *type*] [**route-map***map*]

【参数说明】 **always：**该关键字使得 OSPF 无条件产生缺省路由，不管本地是否存在缺省路由。

metric *metric：*缺省路由初始的量度值，取值范围：0-16777214，默认情况下，缺省路由度量值为 1。

metric-type*type：*缺省路由的类型。OSPF 外部路由有两种类型：类型 1，不同路由设备上看到的量度值不一样；类型 2，所有路由设备看到的量度值都一样。类型 1 的外部路由比类型 2 可信。

route-map *map-name：*关联的 route-map 的名字，缺省没有关联 route-map。

【配置模式】 OSPF 路由进程配置模式

【使用指导】 当执行 **redistribute** 或者 **default-information** 命令时，OSPFv3 路由设备会自动变为 ASBR（自治域边界路由设备）。

但是 **redistribute** 无法产生缺省路由，并通告给 OSPFv3 路由域中的所有路由设备。ASBR 产生缺省路由，必须用 **default-information originate** 路由进程配置命令进行配置。

如果选择 always 参数，不管核心路由表是否存在缺省路由，OSPFv3 进程都会向邻居通告一条外部缺省路由。但是本地路由设备不会显示该缺省路由，要确认是否产生缺省路由，可以用 **show ipv6 ospf database** 观察 OSPFv3 链路状态数据库。OSPFv3 的邻居通过执行 **show ipv6 route ospf** 命令，是可以看到缺省路由的。

外部缺省路由的路由度量值，只能由 **default-information originate** 命令进行定义，不能通过命令 **default-metric** 设置。

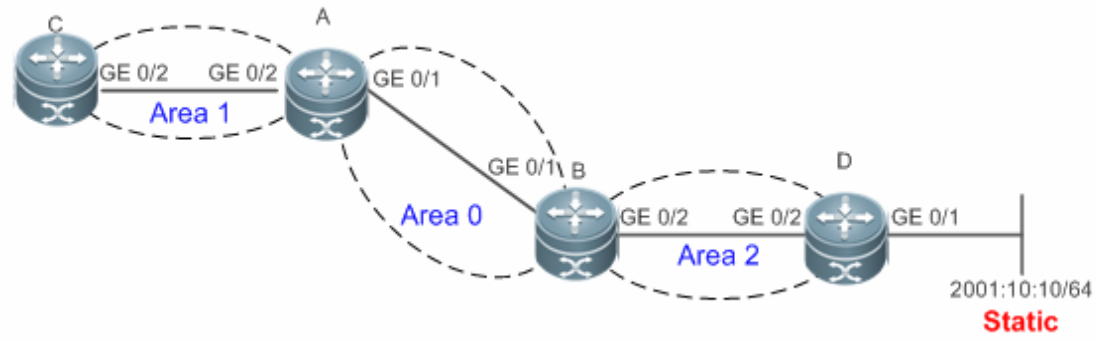
OSPFv3 有两种外部路由，类型 1 外部路由的路由度量会改变，而类型 2 外部路由的路由度量是固定不变。到一个目标网络存在两条并行路径，同样的路由度量，类型 1 会比类型 2 优先级高，所以 **show ipv6 route ospf** 只显示类型 1 那条路由。

stub 区域中的路由设备是不可以产生外部缺省路由的。

配置举例

配置重分发路由

【网络环境】



【配置方法】

- 所有路由器配置接口使能 IPv6。略。
- 所有路由器配置 OSPF 基本功能。略。
- 路由器 D 上配置引入外部静态路由。

D

```
D#configure terminal
D(config)#ipv6 router ospf 1
D(config-router)# redistribute static
```

【检验方法】

- 路由器 D 上使用 show ipv6 ospf database external 查看有外部路由对应的 LSA 生成。
- 路由器 C 上使用 `show ipv6 route ospf` 查看已经加载引入的外部静态路由。

D

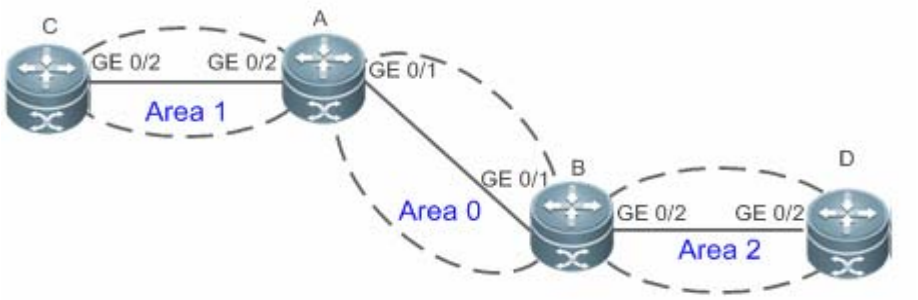
```
D#show ipv6 ospf database external
            OSPFv3 Router with ID (4.4.4.4) (Process 1)
                AS-external-LSA
  LS age: 7
  LS Type: AS-External-LSA
  Link State ID: 0.0.0.6
  Advertising Router: 4.4.4.4
  LS Seq Number: 0x80000001
  Checksum: 0x9C1F
  Length: 36
    Metric Type: 2 (Larger than any link state path)
    Metric: 20
    Prefix: 2001:10:10::/64
    Prefix Options: 0 (-|-|-|-)
```

C

```
C#show ipv6 route ospf

IPv6 routing table name - Default - 0 entries
Codes:  C - Connected, L - Local, S - Static
        R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - Inter area

O   E2   2001:10:10::/64 [110/20] via FE80::2D0:F8FF:FE22:4547, GigabitEthernet 0/2
```

↘ 配置缺省路由。

【网络环境】



【配置方法】

- 所有路由器配置接口使能 IPv6。略。
- 所有路由器配置 OSPF 基本功能。略。
- 路由器 D 上配置缺省路由。

D

```
D#configure terminal
D(config)#ipv6 router ospf 1
D(config-router)#default-information originate always
```

【检验方法】
- 在路由器 D 上使用 show ipv6 ospf database external 查看有缺省路由对应的 LSA。
- 在路由器 C 上使用 show ipv6 route ospf 查看有 ospf 缺省路由。

D

```
D#show ipv6 ospf database external
            OSPFv3 Router with ID (4.4.4.4) (Process 1)
                AS-external-LSA
LS age: 3
  LS Type: AS-External-LSA
  Link State ID: 0.0.0.7
  Advertising Router: 4.4.4.4
  LS Seq Number: 0x80000001
  Checksum: 0x1839
  Length: 32
    Metric Type: 2 (Larger than any link state path)
    Metric: 1
    Prefix: ::/0
    Prefix Options: 0 (-|-|-|-)
    External Route Tag: 1
```

C

```
C#show ipv6route ospf

IPv6 routing table name - Default - 0 entries
Codes:  C - Connected, L - Local, S - Static
        R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - Inter area

O  E2::/0 [110/20] via FE80::2D0:F8FF:FE22:4547, GigabitEthernet 0/2
```

常见配置错误

- 多台设备配置了 **default-information originate always**，造成路由环路。
- 在 Stub 区域配置路由重分布，无法引入路由

6.5.4 设置Stub

配置效果

- 将末梢区域设置为 Stub 区域，有助于减少路由信息的交互，缩小路由表规模，增强路由稳定性。

注意事项

- 必须配置 OSPF 基本功能
- 骨干区域、传输区域不能设置为 Stub 区域、NSSA 区域。

- Stub 区域内路由器不能引入外部路由，NSSA 区域内路由器可以引入外部路由。
- 骨干区域、传输区域不能设置为 Stub 区域。
- Stub 区域内路由器不能引入外部路由。

配置方法

配置 Stub 区域

- 可选配置。若希望减小区域内路由器的路由表规模，需要配置。
- 同一个区域内所有路由器上配置。

配置 Nssa 区域

- 可选配置。若希望减小区域内路由器的路由表规模，又希望本区域可以引入 OSPF 域外路由，需要配置。
- 必须在该区域内的所有路由器上配置该区域为 NSSA 区域。

检验方法

检验 Stub 区域

- 在 Stub 区域内部的路由器上，通过 **show ipv6 route ospf** 查看路由器没有加载外部明细路由。

检验 Nssa 区域

- 在 NSSA 区域内部的路由器上，通过 **show ipv6 ospf database** 查看引入的外部路由生成了 7 类 LSA。
- 在骨干区域内部的路由器上，通过 **show ipv6 route** 查看路由器加载了从 NSSA 区域引入的外部路由。

相关命令

配置 Stub 区域

【命令格式】 **area***area-id***stub** [**no-summary**]

【参数说明】 *area-id :* Stub 区域的区域号。其可以指定为一个整数或者一个 IPv4 前缀。

no-summary :该选项只在 stub 区域的 ABR 上有效，表示该 ABR 只将一条表示缺省路由的类型 3 的 LSA 公告到 stub 区域内，而不再公告类型 3 的其他 LSA。

【配置模式】 OSPF 路由进程配置模式

【使用指导】 如果一个区域处于整个网络的末梢部分，可以将该区域设计为 stub 区域，stub 区域内所有的路由设备都必须执行 **area stub** 命令。如果区域设计为 stub 区域，其将学习不到 AS 外部路由信息(type 5 LSAs)，而在实际应用中，外部路由信息在链路状态数据库中又占有很大比重，所以 stub 区域内部设备将只学习到很少的路由信息，从而降低了运行 OSPFv3 协议所需要占用的系统资源。

在 stub 区域的 ABR 上缺省生成一条表示缺省路由的类型 3 的 LSA 公告到 stub 区域内，这样，stub 区域内部的设备就可以到达 AS 外部。

如果需要配置 totally stub（完全 stub）区域，只需在 ABR 上执行 **area stub** 命令时，选择 **no-summary** 关键字。

配置 Nssa 区域

【命令格式】 **area** *area-id* **nssa** [**no-redistribution**] [**default-information-originate** [**metric** *value*] [**metric-type** *type*]] [**no-summary**] [**translator** [**stability-interval** *seconds* | **always**]]

[translate type7 suppress-fa]

【参数说明】 *area-id*：NSSA 区域的区域号。

no-redistribution：当该路由设备是一个 NSSA ABR 时，如果用户只想用重分布命令将路由信息导入普通区间而不让它进入 NSSA 区间时，可以选上该选项。

default-information-originate：产生缺省的类型 7 的 LSA 进入 NSSA 区间，该选项只在 NSSA ABR 或者 ASBR 上有效。

metric*value*：设置产生的缺省 LSA 的度量值。metric 取值范围 0-16777214，缺省值 1。

metric-type*type*：设置产生的缺省 LSA 的路由类型。type 取值 1 或 2。1 表示 N-1；2 表示 N-2。缺省值 2。

no-summary：阻止 NSSA 的边界路由设备(ABR)发送 summary LSAs（Type-3 LSA）。

translator：配置 NSSA 的边界路由设备(ABR)转换者。

stability-interval*seconds*：配置 NSSA 的边界路由设备(ABR)由转换者变为非转换者后保持的稳定间隔。单位：秒。缺省值为 40。取值范围：0- 2147483647。

always：配置当前 NSSA 的边界路由设备(ABR)总是作为转换者角色。缺省为备选转换者。

translate type7 suppress-fa:配置 7 类 LSA 转换成 5 类 LSA 的时候，5 类 LSA 不携带转发地址(FA)。

【配置模式】 OSPF 路由进程配置模式

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

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

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

另外 **area default-cost** 用在连接在该 NSSA 区域的 ABR/ASBR 上。该命令配置 ABR/ASBR 发送到 NSSA 区域的缺省路由的花费值。缺省情况下，发送到 NSSA 缺省路由的花费值为 1。

如果一个 NSSA 区域有两个（或者两个以上）ABR，缺省情况下，选举路由设备标识最大的 ABR 设备作为 Type-7 转 Type-5 的转换者；如果希望当前设备总是作为 Type-7 转 Type-5 的转换者 ABR，使用 translator always 参数。

如果当前设备的转换者角色被其它 ABR 取代，在 stability-interval 时间内将继续保持转换能力，如果在这段时间内没有重新成为转换者，stability-interval 到期后由 Type-7 转换为 Type-5 的 LSA 将从自治域中被清除。

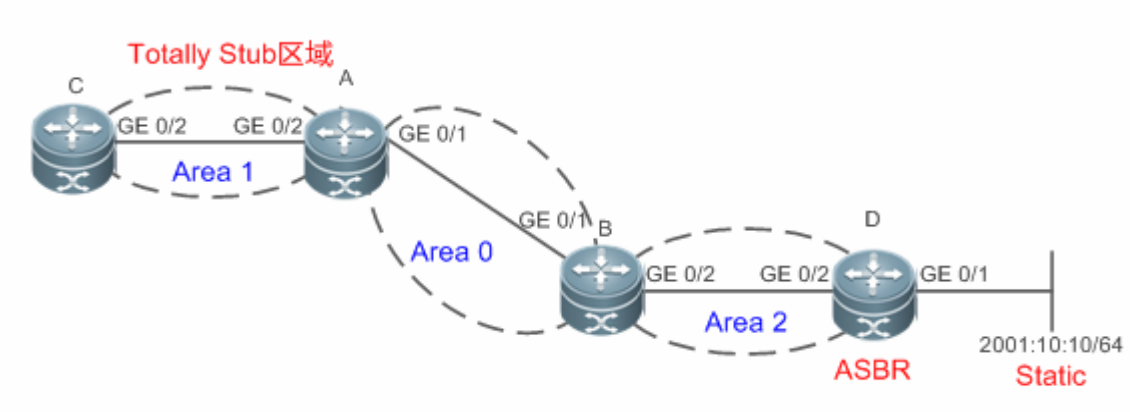
为防止路由环路，由 Type-7 汇聚生成的 Type-5 LSA 将在当前设备失去转换者角色后立即被清除，而无需等待 stability-interval 到期。

同一 NSSA 区域中，建议仅在一台 ABR 配置 translator always 参数。

配置举例

配置 Stub 区域。

【网络环境】



【配置方法】

- 所有路由器配置接口使能 IPv6。略。
- 所有路由器配置 OSPF 基本功能。略。
- 路由器 D 上配置引入外部静态路由。
- 路由器 A、C 上区域 1 配置成 Stub 类型。

D

```
D#configure terminal
D(config)#ipv6 router ospf 1
D(config-router)#redistribute static
```

A

```
A# configure terminal
A(config)#ipv6 router ospf 1
A(config-router)#area 1 stub no-summary
```

C

```
C#configure terminal
C(config)#ipv6 router ospf 1
C(config-router)#area 1 stub
```

【检验方法】

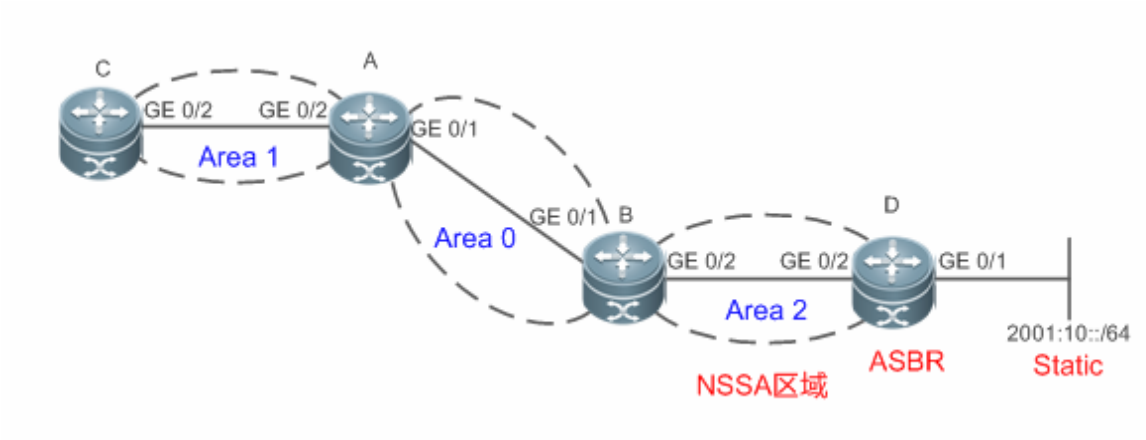
- 在路由器 C 上使用 **show ipv6 route ospf** 查看路由表，只有一条默认区间路由，没有 D 引入的外部静态路由

C

```
C#show ipv6 route ospf

IPv6 routing table name - Default - 0 entries
Codes:  C - Connected, L - Local, S - Static
        R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - Inter area

O  IA::/0 [110/3] via FE80::2D0:F8FF:FE22:4547, GigabitEthernet 0/2
```

↘ 配置 Nssa 区域。

【网络环境】



【配置方法】

- 所有路由器配置接口使能 IPv6。略。
- 所有路由器配置 OSPF 基本功能。略。
- 路由器 D 上配置引入外部静态路由。
- 路由器 B、D 上区域 1 配置成 Nssa 类型。

D

```
D#configure terminal
D(config)#ipv6 router ospf 1
D(config-router)#area 1 nssa
D(config-router)#redistribute static
```

B

```
B#configure terminal
B(config)#ipv6 router ospf 1
B(config-router)#area 1 nssa
```

【检验方法】

- 在路由器 D 上使用 **show ipv6 ospf database** 查看数据库，有生成 7 类 LSA
- 在路由器 A 上使用 **show ipv6 route ospf** 查看路由表，有 D 引入的外部静态路由

D

```
D#show ipv6 ospf database nssa-external
            OSPFv3 Router with ID (1.1.1.1) (Process 1)
                NSSA-external-LSA (Area 0.0.0.1)
  LS age: 1196
  LS Type: NSSA-external-LSA
  Link State ID: 0.0.0.3
  Advertising Router: 1.1.1.1
  LS Seq Number: 0x80000004
  Checksum: 0x1F25
  Length: 52
     Metric Type: 2 (Larger than any link state path)
     Metric: 20
Prefix: 2001:10::/64
Prefix Options: 8 (P|-|-|-)
Forwarding Address: 4000::1
```

A

```
A#show ipv6 route ospf

IPv6 routing table name - Default - 0 entries
Codes:  C - Connected, L - Local, S - Static
        R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - Inter area

O  N2  2001:10::/64 [110/20] via FE80::2D0:F8FF:FE22:4547, GigabitEthernet 0/1
```

常见配置错误

- 同一区域中的设备，区域类型配置不一致
- 在 Stub 区域中配置路由重分布，将无法加入外部路由

6.5.5 配置路由汇聚

配置效果

- 明细路由汇聚，减少路由信息的交互，缩小路由表规模，增强路由稳定性。
- 屏蔽或者过滤路由。

注意事项

- 必须配置 OSPF 基本功能

- 汇总路由的地址范围有可能超出路由表中实际的网络范围，如果数据发往汇总范围内不存在的网络，将有可能发生路由环路或加重路由设备的处理负担。为阻止这种情况的发生，需要向路由表中添加一条 discard 路由屏蔽或者过滤路由。

配置方法

配置区间路由汇聚

- 可选配置。对 OSPF 区域的路由进行汇聚时，需要配置。
- 若无特殊要求，应在被汇聚路由所在区域的 ABR 上配置。

配置外部路由汇聚

- 可选配置。对域外的路由进行汇聚时，需要配置。
- 若无特殊要求，应在引入被汇聚路由的 ASBR 上配置。

检验方法

- 通过 **show ipv6 route ospf** 查看明细路由不存在，只有汇聚后的路由。

相关命令

配置区间路由汇聚

【命令格式】 **area** *area-id* **range** *ipv6-prefix* /*prefix-length* [**advertise | not-advertise**]

【参数说明】 *area-id*：指定要注入汇聚路由的 OSPF 区域号。其可以指定为一个整数或者一个 IPv4 前缀。

ipv6-prefix/*prefix-length*：汇聚的地址范围。

advertise | **not-advertise**：定义是否要公布该汇聚路由。

【命令模式】 OSPF 路由进程配置模式

【使用指导】 该命令只在 ABR 上有效，用来将一个区域内的多条路由汇聚成一条路由，通告到其他区域中。路由信息的合并行为只发生在区域边界，区域内部路由设备上看到的都是具体的路由信息，但其它区域的设备只能看到一条汇聚路由。并且可以通过设置 advertise 和 not-advertise 选项来决定是否公布这个汇聚范围，起到屏蔽和过滤的作用，缺省是向外公布。可以通过 cost 选项来设置汇聚路由的度量值。

可以定义多个区域路由汇聚命令，这样整个 OSPF 路由域的路由将得到简化，特别是网络规模大时，会提高网络转发性能。

当配置了多条汇总，并且项目直接有包含关系的时候，路由是根据最长匹配原则确定被汇总的 area range 的。

配置外部路由汇聚

【命令格式】 **summary-prefix** *ipv6-prefix* /*prefix-length* [**not-advertise** | **tag** *number*]

【参数说明】 *ipv6-prefix*/*prefix-length*：汇聚的地址范围。

not-advertise：不公告汇聚的路由，若未配置则为公告。

tag*number* *：*设置重分布到 OSPFv3 内路由的 tag 值，取值范围：0-4294967295。

【命令模式】 OSPF 路由进程配置模式

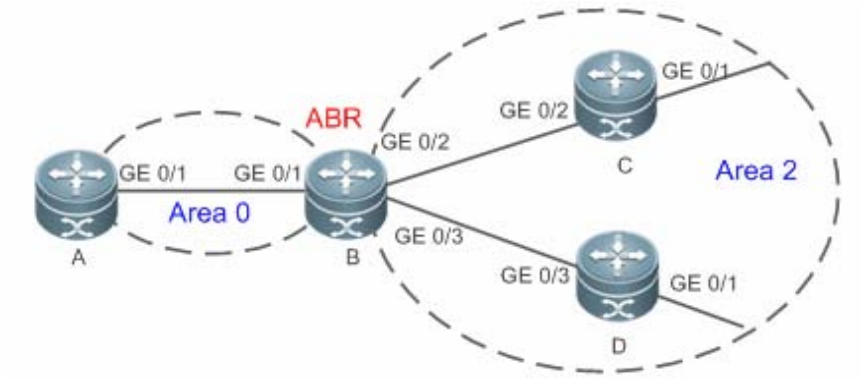
【使用指导】 当路由从其它路由进程重新分布，注入 OSPFv3 路由进程时，每条路由均分别单独以一个外部链路状态的方式通告给 OSPFv3 路由设备。如果注入的路由是一个连续的地址空间，自治域边界路由设备可以只通告一个汇聚路由，从而大大减小路由表的规模。

与 **area range** 命令不同，arearange 汇聚的是 OSPFv3 区域之间路由，而 **summary-prefix** 汇聚的是 OSPFv3 路由域的外部路由。

summary-prefix 命令配置在 NSSA 的 ABR 转换者上时，对重分布的路由及 LSA 从 7 类转 5 类的路由进行汇聚，而配置在 ASBR（非 NSSA 的 ABR 转换者）时，只对重分布的路由进行汇聚。

配置举例

【配置方法】



【注释】 接口 IPv6 地址：

B： GE0/2 2001:16:2::1/64 GE0/3 2001:16:3::1/64

C： GE0/2 2001:16:2::2/64 GE0/1 2001:16:4::2/64

D： GE0/3 2001:16:3::2/64 GE0/1 2001:16:5::1/64

【配置方法】

- 所有路由器配置接口使能 IPv6。略。
- 所有路由器配置 OSPF 基本功能。略。
- 路由器 B 上配置将区域 2 路由汇聚。

B

```
B#configure terminal
B(config)#ipv6 router ospf 1
B(config-router)#area 2 range 2001:16::/64
```

【检验方法】 路由器 A 查看路由表，生成 2001:16::/64 表项，无其他明细路由。

A

```
A#show ipv6 route ospf

IPv6 routing table name - Default - 0 entries
Codes:  C - Connected, L - Local, S - Static
        R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - Inter area

O  IA  2001:16::/64 [110/2] via FE80::2D0:F8FF:FE22:4547, GigabitEthernet 0/1
```

常见配置错误

- 在非 ABR 设备上配置 **area range**，无法进行区间路由汇聚。

6.5.6 配置路由过滤

配置效果

- 被过滤掉的路由不能被加载到路由表或被传播给邻居，网络内用户将无法访问指定的目的网络。

注意事项

- 必须配置 OSPF 基本功能
- 通过 **distribute-listin** 过滤只影响本地路由转发，不影响 LSA 计算路由。因此，如果确定需要在 ABR 上配置过滤，则由于 LSA 仍然可以计算出路由，仍会生产 Type-3 LSA 往其他区域通告，这将导致黑洞路由存在。这时可以在 ABR 上使用 **area filter-list** 或 **area range** 带 not-advertise 选项来避免产生黑洞路由

配置方法

配置区间路由过滤

- 可选配置。若限制用户访问 OSPF 某个区域的网络，建议配置。
- 若无特殊要求，应在被过滤路由所在区域的 ABR 上配置。

配置重分布路由过滤

- 可选配置。ASBR 引入外部路由时，如果需要对引入的外部路由进行过滤，必须配置。
- 若无特殊要求，应在引入被过滤外部路由的 ASBR 上配置。

配置对学习的路由过滤

- 可选配置。若需要限制用户访问指定的目的网络，必须配置。
- 若无特殊要求，应在需要过滤的路由器上配置该功能。

检验方法

- 通过 **show ipv6 route ospf** 查看路由器没有加载被过滤的路由。
- 通过 **ping** 命令确认指定的目的网络无法访问。

相关命令

配置被动接口

【命令格式】 **passive-interface** {**default** | *interface-typeinterface-number* }

【参数说明】 *interface-type interface-number*：要配置为被动接口的接口。

default：该选项表示将所有接口设置为被动接口。

【命令模式】 OSPF 路由进程配置模式

【使用指导】 当一个接口被设置为消极接口，将不再接收和发送 hello 报文。

该命令只对参与 OSPFv3 运行的接口生效，且对虚链路不生效。

配置重分布路由过滤

【命令格式】 **distribute-list**{*name* | **prefix-list** *prefix-list-name*}**out** [**bgp** | **connected** | **isis**[*area-tag*]| **ospf** *process-id*| **rip** | **static**]

【参数说明】 *name*：使用 acl 过滤规则。

prefix *prefix-list-name*：使用 prefix-list 过滤规则。

bgp | connected | isis[*area-tag*] | **ospf** process-id| **rip** | **static**：待过滤路由的来源。

【命令模式】 OSPF 路由进程配置模式

【使用指导】 **distribute-list out** 与 **redistribute route-map** 命令类似 对从其他协议重分布到 OSPFv3 中的路由进行过滤，但它本身不执行路由重分布，一般与 **redistribute** 命令配合使用。ACL 过滤规则和 prefix-list 过滤规则不能在该配置中共存，即若对某一来源的路由使用 ACL 过滤规则，则不能再配置 prefix-list 进行过滤。

配置对学习的路由过滤

【命令格式】 **distribute-list**{*name* | **prefix-list** *prefix-list-name*}**in** [*interface-typeinterface-number*]

【参数说明】 *name*：使用 acl 过滤规则。

prefix*prefix-list-name*：使用 prefix-list 过滤规则。

interface-type interface-number：配置只针对某个接口进行 LSA 路由过滤。

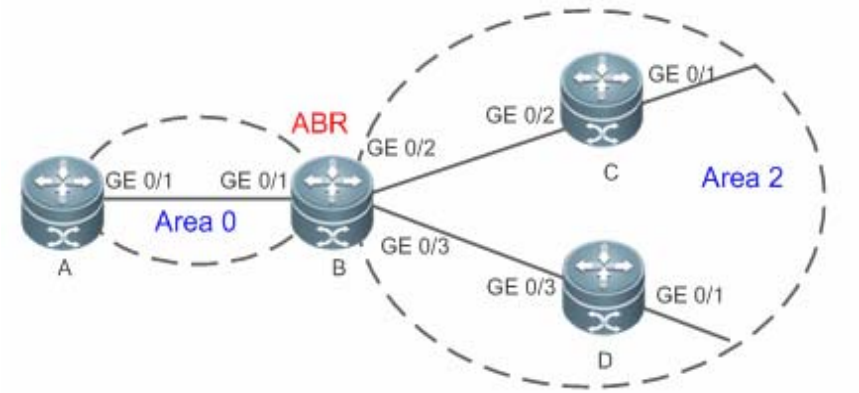
【命令模式】 OSPF 路由进程配置模式

【使用指导】 对收到的 LSA 计算出的路由进行过滤，满足过滤条件的路由才能用于转发。它并不会影响链路状态数据库，对邻居的路由表也不会产生任何影响。ACL 过滤规则和 prefix-list 过滤规则不能在该配置中共存，即若对指定接口使用 ACL 过滤规则，则不能再对该接口配置 prefix-list 进行过滤。

该过滤只影响本地路由转发，不影响 LSA 计算路由。因此，如果确定需要在 ABR 上配置过滤，则由于 LSA 仍然可以计算出路由，仍会生产区域间前缀 LSA 往其他区域通告，这将导致黑洞路由存在。这时可以在 ABR 上使用 **area range** 带 **not-advertise** 选项来避免产生黑洞路由。

配置举例

【网络环境】



【注释】 接口 IPv6 地址：

B： GE0/2 2001:16:2::1/64 GE0/3 2001:16:3::1/64

C： GE0/2 2001:16:2::2/64 GE0/1 2001:16:4::2/64

D： GE0/3 2001:16:3::2/64 GE0/1 2001:16:5::1/64

【配置方法】

- 所有路由器配置接口使能 IPv6。略。
- 所有路由器配置 OSPF 基本功能。略。
- 路由器 A 配置路由过滤。

A

```
A#configure terminal
A(config)#ipv6 access-list test
A (config-ipv6-acl)#permit ipv6 2001:16:5::/64 any
A(config)#ipv6 router ospf 1
A(config-router)#distribute-list test in GigabitEthernet0/1
```

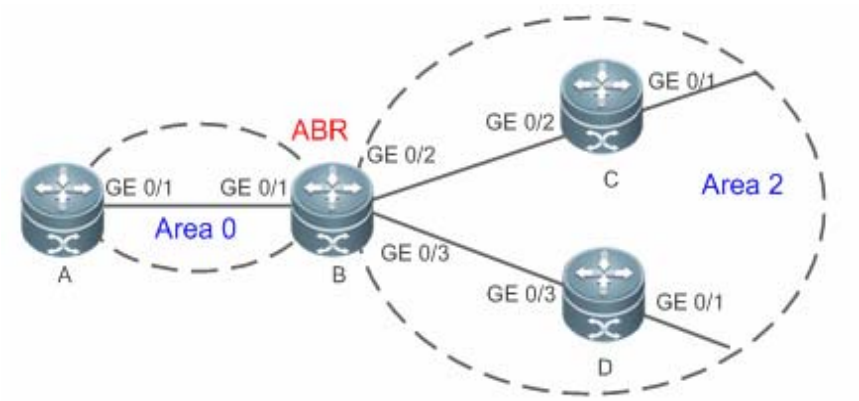
【检验方法】

- 路由器 A 检查路由表，只有加载 2001:16:5::/64 表项。

A

```
A#show ipv6 route ospf

IPv6 routing table name - Default - 0 entries
Codes:  C - Connected, L - Local, S - Static
```

【网络环境】



【注释】 接口 IPv6 地址：

B： GE0/2 2001:16:2::1/64 GE0/3 2001:16:3::1/64

C： GE0/2 2001:16:2::2/64 GE0/1 2001:16:4::2/64

D： GE0/3 2001:16:3::2/64 GE0/1 2001:16:5::1/64

【配置方法】

- 所有路由器配置接口使能 IPv6。略。
- 所有路由器配置 OSPF 基本功能。略。
- 路由器 A 配置路由过滤。

A

```
A#configure terminal
A(config)#ipv6 access-list test
A (config-ipv6-acl)#permit ipv6 2001:16:5::/64 any
A(config)#ipv6 router ospf 1
A(config-router)#distribute-list test in GigabitEthernet0/1
```

【检验方法】

- 路由器 A 检查路由表，只有加载 2001:16:5::/64 表项。

```
       R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area

O   IA  2001:16:5::/64 [110/2] via FE80::2D0:F8FF:FE22:4547, GigabitEthernet 0/1
```

常见配置错误

- 通过 **distribute-listin** 过滤只影响本地路由转发，不影响 LSA 计算路由。因此，如果确定需要在 ABR 上配置过滤，则由于 LSA 仍然可以计算出路由，仍会生产 Type-3 LSA 往其他区域通告，这将导致黑洞路由存在。

6.5.7 修改路由代价、管理距离

配置效果

- 改变 OSPF 路由，使流量经过或避开某些节点。
- 改变路由器选择各类路由的顺序，使 OSPF 路由的优先级提高或降低。

注意事项

- 必须配置 OSPF 基本功能
- 如果用命令 **ipv6 ospf cost** 设置了接口的 cost，则将覆盖自动代价算出的 cost

配置方法

配置参考带宽

- 可选配置。
- 路由器连接不同带宽的线路，若希望优先选择带宽大的线路，建议配置。

配置接口 cost 值

- 可选配置。
- 路由器连接多条线路，若希望手动指定优先的线路，建议配置。

配置重分布缺省度量

- 可选配置。
- 在 ASBR 上引入域外路由时，若需要指定域外路由的代价，必须配置。

配置最大度量值

- 可选配置。
- 路由器重启过程中以及重启刚完成的一段时间内，路由器可能还不稳定，用户的数据流量转发不希望经过该路由器，此时建议配置。

配置管理距离

- 可选配置。
- 在同时运行多种单播路由协议的路由器上，若希望改变 OSPF 路由的优先级，必须配置。

检验方法

- 通过 **show ipv6 ospf interface** 查看接口的代价正确
- 通过 **show ipv6 route ospf** 查看 ASBR 引入的外部路由的代价正确
- 重启路由器，在指定的一段时间内，数据流量转发不经过重启的路由器

相关命令

配置参考带宽

【命令格式】 **auto-cost reference-bandwidth** *ref-bw*

【参数说明】 *ref-bw*：参考带宽值。以 Mbps 为单位，范围: 1-4294967。

【命令模式】 OSPF 路由进程配置模式

【使用指导】 用户可以通过在接口配置模式下执行命令 **ipv6 ospf cost** 为指定接口设置代价，其优先级高于根据带宽参考值计算出来的度量。

配置接口 cost 值

【命令格式】 **ipv6 ospf cost** *cost*[**instance***instance-id*]

【参数说明】 *cost*：OSPF 接口的花费值，取值范围：0-65535。

instance*instance-id*：对接口特定 OSPFv3 实体进行配置，范围 0-255。

【命令模式】 接口配置模式

【使用指导】 缺省情况下，OSPFv3 接口花费值为 100Mbps/Bandwidth，其中 Bandwidth 为接口的带宽，通过接口配置命

令 bandwidth 进行设置。

几种典型线路的 OSPF 接口 cost 缺省值为：

64K 串行线路，cost 为 1562；

E1 线路，cost 为 48；

10M 以太网，cost 为 10；

100M 以太网，cost 为 1。

如果用命令 ipv6 ospf cost 设置了接口的 cost，则将覆盖自动代价算出的 cost

配置 Stub/NSSA 区域缺省路由的 cost 值

【命令格式】 **area***area-id* **default-cost***cost*

【参数说明】 *area-id*：Stub 区域或 NSSA 的区域号。

cost：注入 Stub 区域或者 NSSA 的缺省汇聚路由的花费值，取值范围：0-16777215。

【命令模式】 OSPF 路由进程配置模式

【使用指导】 该命令只有在 Stub 区域的 ABR 或 NSSA 区域的 ABR/ASBR 上配置才能生效。

配置重分布缺省度量

【命令格式】 **default-metric** *metric*

【参数说明】 *metric*：定义 OSPF 重分布路由的缺省量度值，取值范围：1-16777214。

【命令模式】 OSPF 路由进程配置模式

【使用指导】 **default-metric** 命令必须与 **redistribute** 路由进程配置命令配合使用，可以修改所有重分布路由的初始化量度值。对以 **default-information originate** 方式注入 OSPF 路由域的外部路由不起作用。

重分发的直连路由，重分发直连路由将始终使用 20 作为缺省度量值。

配置管理距离

【命令格式】 **distance** { *distance* | **ospf** { [**intra-area** *distance*] [**inter-area** *distance*] [**external** *distance*] } }

【参数说明】 *distance*：设置路由管理距离，取值范围：1-255。

intra-area*distance*：设置区内路由管理距离，取值范围：1-255。

inter-area *distance*：设置区间路由管理距离，取值范围：1-255。

external *distance*：设置外部路由管理距离，取值范围：1-255。

【命令模式】 OSPF 路由进程配置模式

【使用指导】 若要指定 OSPF 不同类型路由对应不同管理距离时，用此命令。

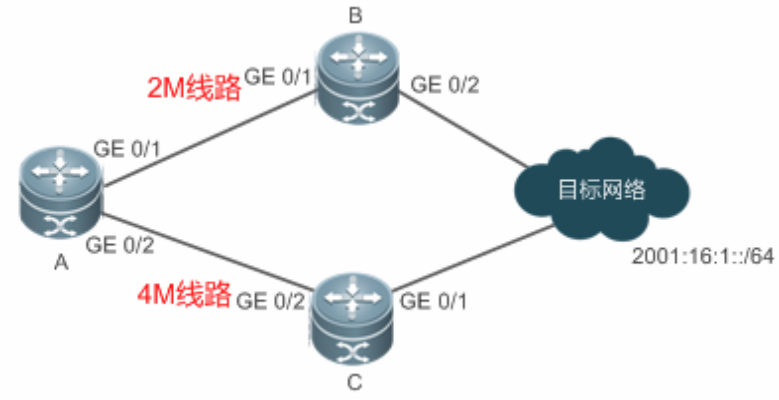
路由管理距离提供给不同路由协议进行路由优先级比较，管理距离越小，路由优先级越高。

不同的 OSPFv3 进程生成的路由要进行优先级比较，必须通过管理距离进行比较。

管理距离设置为 255，表示路由表项不可信，将不参与报文转发。

配置举例

【网络环境】



【配置方法】

- 所有路由器配置接口使能 IPv6。略。
- 所有路由器配置 OSPF 基本功能。略。
- 路由器 A 配置接口代价。

A

```
A#configure terminal
A(config)#interface GigabitEthernet 0/1
A(config-if-GigabitEthernet 0/1)#ipv6 ospf cost 10
A(config)#interface GigabitEthernet 0/2
A(config-if-GigabitEthernet 0/2)#ipv6 ospf cost 20
```

【检验方法】

- 路由器 A 检查路由表，2001:16:1::/64 的最优路径下一跳是路由器 B。

A

```
A#show ipv6 route ospf

IPv6 routing table name - Default - 0 entries
Codes:  C - Connected, L - Local, S - Static
        R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - Inter area

O  E2  2001:16:1::/64 [110/2] via FE80::2D0:F8FF:FE22:4547, GigabitEthernet 0/1
```

常见配置错误

- Ipv6 ospf cost 配置为 0，路由计算可能会出错，比如计算出路由环路；

6.5.8 启动认证功能

配置效果

- 所有接入 OSPF 网络的路由器都必须经过认证，保证 OSPF 协议的稳定性和抗入侵性。

注意事项

- 必须配置 OSPF 基本功能

- 在区域上配置认证，则在属于此区域的所有接口上生效。
- 区域和接口同时配置认证，接口配置优先生效。

配置方法

配置认证

- 可选配置。
- 若路由器接入需要认证的网络，需要配置。

配置加密

- 可选配置。
- 若路由器接入需要加密的网络，需要配置。

配置虚链路认证

- 可选配置。
- 若路由器接入需要认证的网络，需要配置。

配置虚链路加密

- 可选配置。
- 若路由器接入需要加密的网络，需要配置。

检验方法

- 路由器配置不同的认证密钥，通过 **show ipv6 ospf neighbor** 查看 OSPF 邻居为空
- 路由器配置相同的认证密钥后，通过 **show ipv6 ospf neighbor** 查看 OSPF 邻居正确

相关命令

配置区域认证

【命令格式】 **area***area-id***authenticationipsec spi***spi*[**md5|sha1**] [**0 | 7**] *key*

【参数说明】 *area-id*：区域号。其可以指定为一个整数或者一个 IPv4 前缀。

spi：安全参数索引，范围 256-4294967295。

md5：采用 MD5（message digest 5）认证模式。

sha1：采用 SHA1（Secure Hash Algorithm 1）认证模式。

0：指定密钥以明文显示。

7：指定密钥以密文显示。

key：认证密钥

【配置模式】 OSPF 路由配置模式

【使用指导】 RGOS 软件可以支持三种认证类型：

1）不要求认证，没有配置的时候；

2）为 MD5 认证模式；

3）为 SHA1 认证模式。

OSPFv3 配置区域认证，则对该区域内的所有接口生效（虚链路除外），但是接口配置认证优先。

配置区域加密认证

【命令格式】 **area***area-id***encryption ipsec spi***spi* **esp**[**null**|[**des** | **3des**][**0 | 7**] *des-key*][**md5|sha1**] [**0|7**] *key*

【参数说明】 *area-id*：区域号。其可以指定为一个整数或者一个 IPv4 前缀。

spi：安全参数索引，范围 256-4294967295。

null:不采用加密。

des:采用 DES(Data Encryption Standard，数据加密标准)加密模式。

3des:采用 3DES(三重 DES)加密模式。

des-key：加密密钥。

md5：采用 MD5（message digest 5）认证模式。

sha1：采用 SHA1（Secure Hash Algorithm 1）认证模式。

0：指定密钥以明文显示。

7：指定密钥以密文显示。

key：认证密钥

【配置模式】 OSPF 路由配置模式

【使用指导】 RGOS 软件可以支持。

两种加密类型：

1）DES 加密模式；

2）3DES 加密模式。

两种认证类型：

1）MD5 认证模式；

2）SHA1 认证模式。

OSPFv3 配置区域加密认证，则对该区域内的所有接口生效（虚链路除外），但是接口配置加密认证优先。

↘ 配置接口认证

【命令格式】 **ipv6 ospfauthentication**[**null | ipsec spi***spi*[**md5|sha1**] [**0|7**]*key*][**instance***instance-id*]

【参数说明】 *area-id*：区域号。其可以指定为一个整数或者一个 IPv4 前缀。

spi：安全参数索引，范围 256-4294967295。

md5：采用 MD5（message digest 5）认证模式。

sha1：采用 SHA1（Secure Hash Algorithm 1）认证模式。

0：指定密钥以明文显示。

7：指定密钥以密文显示。

*key：*认证密钥

instance *instance-id：*对接口特定 OSPFv3 实体进行配置，范围 0-255。

【配置模式】 OSPF 路由配置模式

【使用指导】 RGOS 软件可以支持三种认证类型：

1）不要求认证，没有配置的时候；

2）为 MD5 认证模式；

3）为 SHA1 认证模式。

OSPFv3 配置接口认证，互联的接口配置的认证参数必须一致。。

↘ 配置接口加密认证

【命令格式】 **ipv6 ospfencryption ipsec spi***spi* **esp**[**null**|[**des** | **3des**][**0** | **7**] *des-key*][**md5|sha1**] [**0|7**] *key*[**instance***instance-id*]

【参数说明】 *spi*：安全参数索引，范围 256-4294967295。

null:不采用加密。

des:采用 DES(Data Encryption Standard，数据加密标准)加密模式。

3des:采用 3DES(三重 DES)加密模式。

des-key：加密密钥。

md5：采用 MD5（message digest 5）认证模式。

sha1：采用 SHA1（Secure Hash Algorithm 1）认证模式。

0：指定密钥以明文显示。

7：指定密钥以密文显示。

key：认证密钥。

instance *instance-id*：对接口特定 OSPFv3 实体进行配置，范围 0-255。

【配置模式】 OSPF 路由配置模式

【使用指导】 RGOS 软件可以支持。

两种加密类型：

1）DES 加密模式；

2）3DES 加密模式。

两种认证类型：

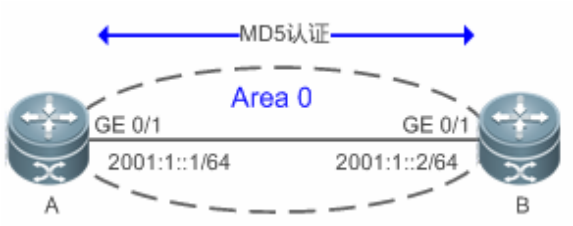
1）MD5 认证模式；

2）SHA1 认证模式。

OSPFv3 配置接口加密认证，互联的接口配置的加密认证参数必须一致。

配置举例

【网络环境】



【配置方法】

- 所有路由器配置接口使能 IPv6。略。
- 所有路由器配置 OSPF 基本功能。略。
- 所有路由器接口配置 MD5 认证。

A

```
A#configure terminal
A(config)#interface GigabitEthernet 0/1
A(config-if-GigabitEthernet 0/1)#ipv6 ospf authentication ipsec spi 256 md5
0123456789012345678901234567891 2
```

B

```
B# configure terminal
B(config)#interface GigabitEthernet 0/3
B(config-if-GigabitEthernet 0/3)#ipv6 ospf authentication ipsec spi 256 md5
0123456789012345678901234567891 2
```

【检验方法】

- 路由器 A、B 上查看 OSPF 邻居状态正确。

A

```
A# show ipv6 ospf neighbor
OSPFv3 Process (1), 1 Neighbors, 1 is Full:
Neighbor ID     Pri   State           Dead Time   Instance ID   Interface
2.2.2.2           1   Full/DR         00:00:38    0             GigabitEthernet 0/1
```

B

```
B# show ipv6 ospf neighbor
OSPFv3 Process (1), 1 Neighbors, 1 is Full:
Neighbor ID     Pri   State           Dead Time   Instance ID   Interface
1.1.1.1           1   Full/BDR        00:00:38    0             GigabitEthernet 0/1
```

常见配置错误

- 配置的认证方式不一致。
- 配置的认证密钥不一致

6.5.9 修改并发邻居数量限制

配置效果

- 控制 OSPF 邻居的并发建立，缓解设备压力

注意事项

- 必须配置 OSPF 基本功能

配置方法

↘ 配置进程并发邻居数

- 可选配置。若路由器连接了大量其他路由器，且希望 OSPF 邻居建立加快，建议配置。
- 在核心路由器上配置。

检验方法

- 通过 **show ipv6 ospf neighbor** 查看正在并发建立的邻居个数

相关命令

↘ 配置当前进程并发邻居数

【命令格式】 **max-concurrent-dd***number*

【参数说明】 *number*:指定并发交互的邻居最大数目，范围 1-65535。

【配置模式】 OSPF 路由配置模式

【使用指导】 当路由设备与多个邻居同时交换数据，其性能受到影响时，配置该命令，可限制每个 OSPF 实例允许同时并发交互（发起或接受）的邻居最大数目。

↘ 配置所有进程并发邻居数

【命令格式】 **Ipv6 router ospf max-concurrent-dd***number*

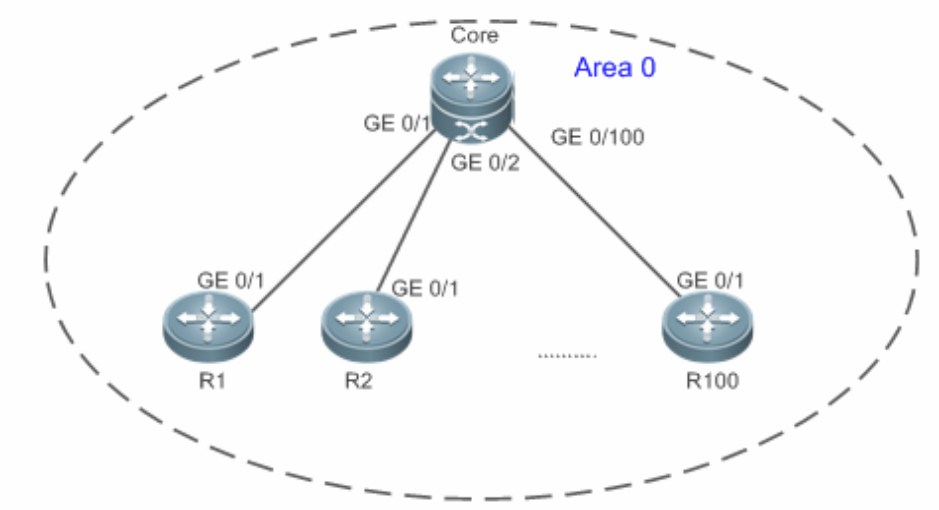
【参数说明】 *number*:指定并发交互的邻居最大数目，范围 1-65535

【配置模式】 全局配置模式

【使用指导】 当路由设备与多个邻居同时交换数据，其性能受到影响时，配置该命令，可限制所有 OSPF 实例允许同时并发交互（发起或接受）的邻居最大数目。

配置举例

【网络环境】



【配置方法】
- 所有路由器配置接口使能 IPv6。略。
- 所有路由器配置 OSPF 基本功能。略。
- 核心路由器 Core 配置最大邻居并发数为 4。

Core

```
Core# configure terminal
Core(config)# ipv6 router ospf max-concurrent-dd 4
```

【检验方法】
- 路由器 Core 上查看邻居状态，同时在建立的邻居最多 8 个。

常见配置错误

-

6.5.10 关闭MTU校验

配置效果

- 相邻路由器的接口 MTU 不同，也能提供单播路由服务。

注意事项

- 必须配置 OSPF 基本功能

配置方法

↘ 配置关闭 MTU 校验

- 可选配置。默认已关闭 MTU 校验，建议保持默认配置。
- 在俩端接口 MTU 不同的路由器上配置。

检验方法

- MTU 不一致的邻居也能建立。

相关命令

↘ 配置关闭 mtu 校验

【命令格式】 **Ipv6 ospf mtu-ignore**

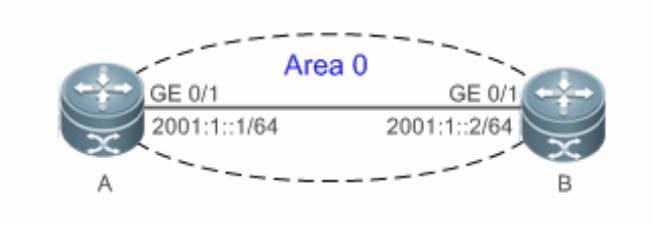
【参数说明】 -

【命令模式】 接口配置模式

【使用指导】 OSPF 在收到数据库描述报文时会校验邻居的接口的 MTU 和自己接口的 MTU 是否相同，如果收到的数据库描述报文中指示的接口的 MTU 大于接收接口的 MTU，那么邻接关系将不能被建立，此时可以通过关闭 MTU 的校验来解决。

配置举例

【网络环境】



【配置方法】

- 所有路由器配置接口使能 IPv6。略。
- 所有路由器配置 OSPF 基本功能。略。
- 配置俩边接口 MTU 不一致。
- 所有路由器配置关闭 MTU 校验（该功能默认已经开启）。

A

```
A# configure terminal
A(config)# interface GigabitEthernet 0/1
A(config-if-GigabitEthernet 0/1)# ipv6 mtu 1400
A(config-if-GigabitEthernet 0/1)#ipv6 ospf mtu-ignore
```

B

```
B# configure terminal
B(config)# interface GigabitEthernet 0/1
A(config-if-GigabitEthernet 0/1)# ipv6 mtu 1600
B(config-if-GigabitEthernet 0/1)# ipv6 ospf mtu-ignore
```

【检验方法】

- 路由器 A 上查看 OSPF 邻居正确。

A

```
A# show ipv6 ospf neighbor
OSPFv3 Process (1), 1 Neighbors, 1 is Full:
Neighbor ID     Pri   State           Dead Time   Instance ID   Interface
2.2.2.2           1   Full/DR         00:00:38    0             GigabitEthernet 0/1
```

常见配置错误

-

6.5.11 启动双向维持

配置效果

- 非 hello 报文也能维持邻居状态

注意事项

- 必须配置 OSPF 基本功能

配置方法

配置双向维持

- 可选配置。该功能默认已开启，建议保持默认配置
- 所有路由器上配置。

检验方法

- 非 hello 报文也能维持邻居。

相关命令

配置双向维持

【命令格式】 **two-way-maintain**

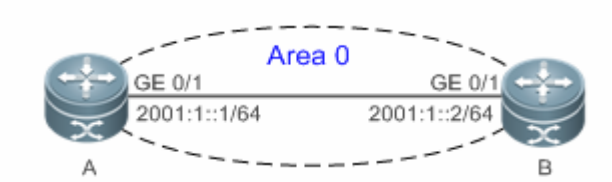
【参数说明】 -

【命令模式】 OSPF 路由配置模式

【使用指导】 在较大的网络中，可能会出现大量的报文收发，占用较高的 CPU 和内存资源，造成部分部分报文的延迟或丢弃，如果 Hello 报文的处理超出了死亡间隔，将导致对应的邻接超时断开。这时启用双向维持功能，如果网络中存在大量的报文，除了 Hello 报文外，来自某个邻居的 DD、LSU、LSR、LSAck 报文也能够用于维持该邻居的双向关系，避免由于 Hello 报文的延迟或丢弃而导致邻居的失效。

配置举例

【网络环境】



【配置方法】
- 所有路由器配置接口使能 IPv6。略。
- 所有路由器配置 OSPF 基本功能。略。
- 路由器 A 配置启动双向维持（该功能默认已经启动）。

A

```
A# configure terminal
A(config)# ipv6 routerospf 1
A(config-router)#two-way-maintain
```

【检验方法】
- 建邻居过程中，路由器 A 检查邻居到期时间，并没有等路由器 B 发送 Hello 报文后才更新。

A

```
A# show ipv6 ospfneighbor
OSPFv3 Process (1), 1 Neighbors, 1 is Full:
Neighbor ID     Pri   State           Dead Time   Instance ID   Interface
2.2.2.2           1   Full/DR         00:00:38    0             GigabitEthernet 0/1
```

常见配置错误

-

6.5.12 启动GR功能

配置效果

- 分布式路由器从主板切换到备板过程中，用户数据流量始终保持转发不断流
- OSPF 协议进程重新启动期间，用户数据流量始终保持转发不断流

注意事项

- 必须配置 OSPF 基本功能
- 邻居路由器必须支持 GR helper。
- GR 时间不能小于邻居路由器的邻居维持时间。

配置方法

↘ 配置 OSPF GR 功能

- 可选配置。该功能默认已开启，建议保持开启状态。
- 在进行热备切换或者进程重启的路由器上配置。

↘ 配置 OSPF GR helper 功能

- 可选配置。该功能默认已开启，建议保持开启状态。
- 若邻居设备进行热备切换或者进程重启，本机需要配置。

检验方法

- 分布式路由器热备切换到备板，在此期间数据流量始终保持转发不断流。
- OSPF 协议进程重启，在此期间数据流量始终保持转发不断流。

相关命令

↘ 配置 OSPF 功能

【命令格式】 **graceful-restart** [**grace-period***grace-period*|**inconsistent-lsa-checking**]

【参数说明】 **grace-period** *grace-period*：配置 GR 重启周期，重启周期为从 OSPF 失效到 OSPF 重新启动并完成优雅重启的最长时间。*grace-period* 取值范围 1-1800 秒，缺省值为 120s。

inconsistent-lsa-checking：拓扑变化检测。检测到拓扑改变，提前退出 GR 完成收敛。开启 GR 后，默认开启检测。

【配置模式】 OSPF 路由配置模式

【使用指导】 优雅重启功能基于 OSPF 实例配置，不同的实例可以根据情况配置不同的参数。该命令用于配置设备的 GR Restarter 能力。重启周期为 GR 从开始到结束的最长时间，在这段时间内执行链路状态重建工作，使 OSPF 恢复到原有状态。当重启周期到期后，OSPF 将退出 GR 状态，执行普通的 OSPF 操作。

graceful-restart 设置 GR 的重启周期为 120 秒 ,**graceful-restart grace-period** 允许用户显式修改重启周期。GR 成功执行，保证转发不间断的前提是拓扑保持稳定。若拓扑发生改变，OSPF 将尽快收敛，不再等待 GR 的继续执行，避免长时间的转发黑洞。

１）关闭拓扑检测：对于热备过程中的拓扑变化不能及时收敛，有可能造成长时间的转发黑洞;

２）使能拓扑检测：有可能转发间断，但间断时间远小于关闭拓扑检测；

对于拓扑检测，大部分情况下不建议关闭。在特殊场景下，热备后拓扑会变化，但可保证不会出现长时间的转

发黑洞，此时可关闭拓扑检测，最大程度减少热备过程中转发间断的时间。

在 Fast Hello 功能下，不支持启用优雅重启功能。

配置 OSPF GR helper 功能

【命令格式】 **graceful-restart helper** { **disable |strict-lsa-checking | internal-lsa-checking**}

【参数说明】 **disable**：禁止设备作为辅助设备辅助其他设备执行优雅重启。

strict-lsa-checking：GR Helper 期间通过检查 types 1-5，7 的 LSA 的变化判断网络是否发生变化，如果网络发生变化，将退出 GR Helper。

internal-lsa-checking : GR Helper 期间通过检查 types 1-3 的 LSA 的变化判断网络是否发生变化，如果网络发生变化，将退出 GR Helper。

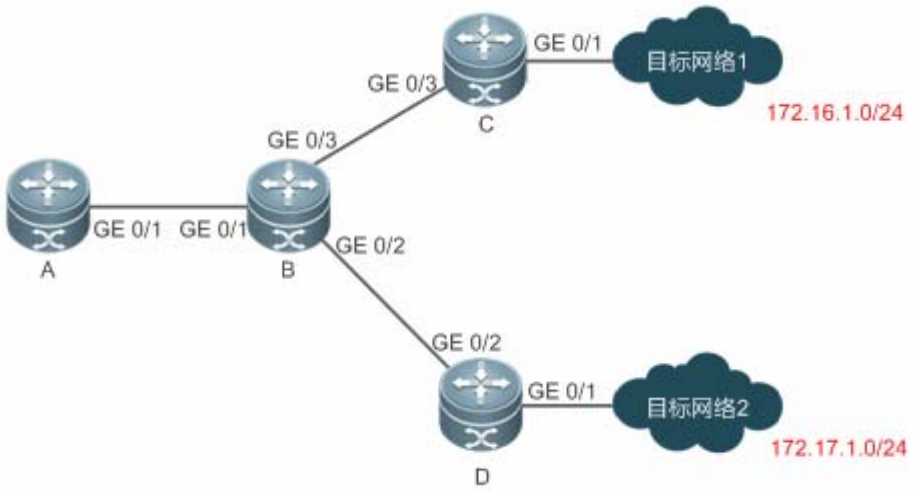
【配置模式】 OSPF 路由配置模式

【使用指导】 该命令用于配置设备的 GR Help 能力，当邻居设备实施优雅重启时，将发送 Grace-LSA 通告其所有的邻居设备 如果本设备使能 GR Help 能力 ,在收到 Grace-LSA 时 ,会成为 GR Helper ,辅助邻居完成优雅重启。**disable** 选项表示禁止对任何执行优雅重启的设备进行 GR 辅助。

设备成为 GR Helper 后，默认情况下不对网络变化进行检测，如果网络发生变化，也将等到 GR 完成之后才会重新进行收敛。如果用户希望在 GR 过程中，对于变化的网络能够快速探测，可以通过配置 **strict-lsa-checking** 或者 **internal-lsa-checking** 选项启动检测，其中前者对任何表示网络信息的 LSA(types 1-5，7)进行检测，后者对表示 AS 域内路由的 LSA(types 1-3)进行检测。在网络规模较大的情况下，不建议用户启动 LSA 检测选项，因为局部网络的变化会触动 GR 结束，从而导致整网的收敛降低。

配置举例

【网路环境】



【配置方法】

- 所有路由器配置接口使能 IPv6。略。
- 所有路由器配置 OSPF 基本功能。略。
- 路由器 A、C、D 开启 GR Helper 功能（该功能默认已经开启）。
- 路由器 B 开启 GR 功能。

B

```
B# configure terminal
B(config)# ipv6 router ospf1
B(config-router)# graceful-restart
```

【检验方法】

- 路由器 B 执行热备切换，期间在路由器 A 上查看到目标网络 1 和目标网络 2 的路由表保持不变。
- 路由器 B 执行热备切换，期间在路由器 A 上 ping 目标网络 1 不间断。

常见配置错误

- 配置的 GR 时间小于邻居路由器的邻居维持时间，导致 GR 过程中转发中断。

6.5.13 配置网管功能

配置效果

- 通过网管软件管理 OSPF 协议的参数及监控协议运行状态。

注意事项

- 必须配置 OSPF 基本功能
- 要开启 ospf 的 mib 功能，必须开启 snmp-server 的 mib 功能。
- 要开启 ospf 的 trap 功能，必须开启 snmp-server 的 trap 功能。
- 要输出 ospf 的日记信息，必须开启设备的日记开关。

配置方法

配置 MIB 绑定

- 可选配置。若希望通过网管软件管理指定的 OSPF 实例的参数，需要配置。
- 所有路由器上配置。

配置使能 Trap

- 可选配置。若希望通过网管软件监控协议的运行状态，需要配置。
- 所有路由器上配置。

配置日记输出

- 可选配置。该功能默认已开启，建议保持默认配置，若希望减少日记输出，可关闭该功能。
- 所有路由器上配置。

检验方法

- 通过网管软件可管理协议的参数。
- 通过网管软件可监控协议的运行状态。

相关命令

配置 MIB 绑定

【命令格式】 **enable mib-binding**

【参数说明】 -

【命令模式】 OSPF 路由进程配置模式

【使用指导】 由于 OSPFv2 MIB 没有 OSPFv3 进程信息，所以用户通过 SNMP 操作 OSPFv3 进程，只能操作唯一的进程。
缺省情况下，OSPFv3 MIB 绑定在进程号最小的 OSPFv3 进程上，用户的操作都对该进程生效。
如果用户希望能够通过 SNMP 操作指定的 OSPFv3 进程，可以通过本命令将 MIB 绑定到该进程上。

配置使能 Trap

【命令格式】 **enable traps[error [IfConfigError| IfRxBadPacket | VirtIfConfigError | VirtIfRxBadPacket] | state-change[IfStateChange | NbrStateChange | NssaTranslatorStatusChange | VirtIfStateChange |**

VirtNbrStateChange | RestartStatusChange | NbrRestartHelperStatusChange | VirtNbrRestartHelperStatusChange]]

【参数说明】 **IfConfigError**：接口参数配置错误。

IfRxBadPacket：接口接收到错误报文。

VirtIfConfigError：虚拟接口参数配置错误。

VirtIfRxBadPacket：虚拟接口接收到错误报文。

IfStateChange：接口状态变化。

NbrStateChange：邻居状态变化。

NssaTranslatorStatusChange：NSSA 转换者状态变化。

VirtIfStateChange：虚拟接口状态变化。

VirtNbrStateChange：虚拟邻居状态变化。

RestartStatusChange：本机 GR 状态变化。

NbrRestartHelperStatusChange：邻居 GR 过程状态变化。

VirtNbrRestartHelperStatusChange：虚拟邻居 GR 过程状态变化。

【命令模式】 OSPF 路由进程配置模式

【使用指导】 本命令对应功能受 **snmp-server** 命令的限制，必须先打开配置开关 **snmp-server enable traps ospf**，再配置 enable traps 以后，对应的 ospf trap 才能够正确发送。

本命令不受进程绑定 MIB 的限制，允许不同进程同时打开 TRAP 开关。

配置日记输出

【命令格式】 **log-adj-changes**[**detail**]

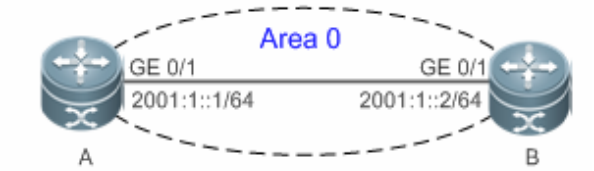
【参数说明】 **detail**：记录全部状态变化信息。

【命令模式】 OSPF 路由进程配置模式

【使用指导】 -

配置举例

【网络环境】



【配置方法】

- 所有路由器配置接口使能 IPv6。略。
- 所有路由器配置 OSPF 基本功能。略。
- 路由器 A 配置 MIB 绑定。
- 路由器 A 配置 Trap 使能。

A	A# configure ter minal A(config)#snmp-server host 192.168.2.2 traps version 2c public A(config)#snmp-server community public rw A(config)#snmp-server enable traps A(config)# A(config)# ipv6 routerospf 10 A(config-router)# enable mib-binding A(config-router)# enable traps

【检验方法】
- 通过 MIB 工具读取、设置 OSPF 的参数信息，并查看 OSPF 协议运行状态。

常见配置错误

-

6.5.14 修改协议控制参数

配置效果

- 修改协议运行参数，改变协议运行状态。

注意事项

- 必须配置 OSPF 基本功能
- 邻居维持时间不得小于 Hello 间隔时间

配置方法

↘ **配置 hello 时间**
- 可选配置，不建议修改默认配置。
- 在链路俩端的路由器上配置。

↘ **配置 dead 时间**
- 可选配置，不建议修改默认配置。若用户希望链路失效时加快协议收敛，可调整该配置。
- 在链路俩端的路由器上配置。

↘ **配置 lsu 重传间隔**
- 可选配置。若用户环境有大量路由并且网络拥塞严重，建议调整该配置。

↘ **配置 lsa 生成时间**
- 可选配置，不建议修改默认配置。

↘ **配置 lsa 分组刷新时间**
- 可选配置，不建议修改默认配置。若用户环境有大量路由，可调整该配置。
- 在 ASBR 或者 ABR 上配置。

↘ **配置 lsa 重复接收延迟**
- 可选配置，不建议修改默认配置。

↘ **配置 SPF 计算时间**
- 可选配置。若网络环境频繁震荡，可调整该配置。

配置区间路由计算延时时间

- 可选配置。不建议修改默认配置。
- 在所有路由器上配置。

配置区间路由计算延时时间

- 可选配置。不建议修改默认配置。
- 在所有路由器上配置。

检验方法

- 通过 **show ipv6 ospf**、**show ipv6 ospf neighbor** 查看协议运行参数及状态

相关命令

配置 hello 时间

【命令格式】 **ipv6ospf hello-interval***seconds*

【参数说明】 *seconds*：设置 OSPF 发送 hello 报文的时间间隔，以秒为单位，取值范围 1-65535。

【命令模式】 接口配置模式

【使用指导】 hello 报文时间间隔包含在 hello 报文中。该时间越短，OSPF 检测到拓扑变化的时间也将越快，但是将增加网络流量。同一网段上的所有路由设备的 hello 报文时间间隔必须一致。如果还想手工修改判断邻居死亡时间，必须保证 hello 报文时间间隔不能大于邻居死亡时间。

配置 dead 时间

【命令格式】 **ipv6ospf dead-interval** *seconds*

【参数说明】 *seconds*：定义判断邻居死亡的时间，以秒为单位，取值范围：1-65535。

【命令模式】 接口配置模式

【使用指导】 OSPF 的死亡时间包含在 Hello 报文内。如果 OSPF 在死亡时间内，没有收到邻居发送的 Hello 报文，就宣告邻居无效并从邻居表中删除该邻居记录。死亡时间缺省为 hello 报文时间间隔的 4 倍，如果修改了 hello 时间间隔，会自动修改死亡时间。

用该命令可以手工修改 OSPF 判断邻居死亡时间，但是必须十分谨慎。有两点必须注意：

第一点：死亡时间间隔，不能小于 hello 报文时间间隔；

第二点：同一网段上的所有路由设备的死亡时间间隔必须一致。

配置 lsu 发送延迟

【命令格式】 **ipv6ospf transmit-delay***seconds*

【参数说明】 *seconds*：定义 OSPF 接口传输 LSU 报文的延时，以秒为单位，取值范围：1-65535。

【命令模式】 接口配置模式

【使用指导】 在传输 LSU 报文之前，该报文中所有 LSAs（链路状态描述）的 Age 字段将增加，增加量根据该接口配置命令 **ip ospf transmit-delay** 的定义。设置该参数必须考虑到该接口的发送和线路传播时延，对于低速线路，接口的传输延时应该设置得大些。虚拟链路的 LSU 报文传输延时，用 **area virtual-link** 命令跟随 transmit-delay 关键字进行定义。

对 Age 达到 3600 的 LSA，将进行重传或请求重传，如果没有得到及时刷新，超时的 LSA 将从链路状态数据库中清除。

配置 lsu 重传间隔

【命令格式】 **ipv6ospf retransmit-interval***seconds*

【参数说明】 *seconds*：LSU 重传时间间隔，以秒为单位，取值范围：1-65535。该时间必须大于两个邻居之间的数据包往

返传输延时。

【命令模式】 接口配置模式

【使用指导】 当路由设备发送完一个 LSU 报文 ,该 LSU 报文还保留在发送缓冲队列中 ,如果在 **ip ospf retransmit-interval** 命令定义的时间内，没有得到邻居的确认，将重新发送 LSU。

为了避免不必要的重传，在串行线路或虚拟链路上，可以将重传时间设置得大一点。虚拟链路的 LSU 报文重传时间间隔用 area virtual-link 命令跟随 retransmit-interval 关键字进行定义。

配置 lsa 生成时间

【命令格式】 **timers throttle lsa all** *delay-time hold-time max-wait-time*

【参数说明】 *delay-time*：LSA 生成的最小延迟时间，数据库中的第一份 LSA 总是立即生成的。取值范围：0-600000，单位：毫秒。

hold-time：配置首次与第 2 次刷新 LSA 时，最短的时间间隔。取值范围：1-600000，单位：毫秒。

max-wait-time：连续刷新 LSA 时，两次刷新 LSA 的时间间隔最大值。同时，这个时间间隔也是判断 LSA 是否连续刷新的值。取值范围：1-600000，单位：毫秒。

【命令模式】 OSPF 路由进程配置模式

【使用指导】 对链路变化时收敛性要求较高时，delay-time 可以配置为较小值。若希望减少 CPU 消耗，可以把几个值适当调高。

配置命令时，hold-time 不允许小于 delay-time，max-wait-time 也不允许小于 hold-time。

设置 lsa 分组刷新时间

【命令格式】 **timers pacinglsa-group** *seconds*

【参数说明】 *seconds*：LSA 组步调更新的步调时间，取值范围: 10-1800，单位：秒。

【命令模式】 OSPF 路由进程配置模式

【使用指导】 每个 LSA 都有自己的生存时间(LSA age)，当生存时间达到 1800 秒时，需要进行重刷新以防止正常的 LSA 通告达到最大生存时间而被清除掉。如果对每个 LSA 都独立进行 LSA 的更新和老化计算，将消耗大量的 CPU 资源。为了有效利用 CPU 资源，将设备内 LSA 分组进行刷新操作。这里称一个分组刷新操作的时间间隔为组步调间隔，分组刷新操作即将一个组步调间隔内需要刷新的 LSA 编成一组统一刷新。

在 LSA 数量一定的情况下，步调时间间隔越大，定时器期满后处理的 LSA 数量越多。为了保持 CPU 的稳定，建议每次期满处理的 LSA 数量不宜太多，所以如果 LSA 数量较大，建议降低步调间隔。比如，数据库中有 10000 条 LSA，可以降低步调时间间隔，如果只有 40～100 条，则可以调整到 10~20 分钟。

配置 lsa 分组刷新间隔

【命令格式】 **timers pacing lsa-transmit** *transmit-time transmit-count*

【参数说明】 *transmit-time*：配置 LSA 分组发送时间间隔。取值范围：10-1000，单位：毫秒。

transmit-count：配置每组 LS-UPD 报文的个数。取值范围：1-200，单位：个。

【命令模式】 OSPF 路由进程配置模式

【使用指导】 环境中 LSA 数量很多，设备本身负荷太大时，配置适当的 **transimit-time** 和 **transimit-count** 可以抑制网络中洪泛的 LS-UPD 报文数量。

CPU 负荷不高，网络带宽负荷不大时，减小 **transimit-time** 增加 **transimit-count** 可以加快环境的收敛。

配置 lsa 重复接收延迟

【命令格式】 **timers lsa arrival***arrival-time*

【参数说明】 *arrival-time*：配置接收相同 LSA 时延时。取值范围：0-600000，单位：毫秒。

【命令模式】 OSPF 路由进程配置模式

【使用指导】 配置指定时间之内接收到相同 LSA 时，不做处理。

配置 SPF 计算时间

【命令格式】 **timers throttle spf** *spf-delay spf-holdtime spf-max-waittime*

【参数说明】 *spf-delay*：定义 SPF 计算的等待时间，以毫秒为单位，取值范围：1-600000。OSPF 路由进程接收到拓扑变化，触发的 SPF 计算至少要在 spf-delay 时间间隔后执行。

spf-holdtime：定义两次 SPF 运算之间的最小时间间隔，以毫秒为单位，取值范围：1-600000。

spf-max-waittime：定义两次 SPF 运算之间的最大时间间隔，以毫秒为单位，取值范围：1-600000。

number：聚合路由的度量值。

【命令模式】 OSPF 路由进程配置模式

【使用指导】 *spf-delay* 表示从拓扑发生变化到 SPF 开始计算，至少需要延迟的时间。第一次触发 SPF 计算到第二次触发 SPF 计算的最小时间间隔为 *spf-holdtime*，此后，连续触发 SPF 计算的时间间隔至少为上一次时间间隔的两倍，当时间间隔达到 *spf-max-waittime* 之后，将不再增加。如果两次 SPF 计算的时间间隔已经超过了要求的最小值，那么 SPF 计算时间间隔将重新从 *spf-holdtime* 开始计算。

spf-delay 和 *spf-holdtime* 可以设置小些以加快拓扑的收敛 ;*spf-max-waittime* 可以设置大些以减少 SPF 计算，可以根据实际网络拓扑稳定性采取灵活设置。

与 **timers spf** 命令相比，该命令能够进行更灵活的设置，既可以加快 SPF 计算收敛速度，又可以在拓扑连续变化时更好的减少 SPF 计算的系统资源消耗，所以推荐使用 **timers throttle spf** 命令进行配置。

1． spf-holdtime 的值不能小于 spf-delay，否则 spf-holdtime 的值将被自动设置为与 spf-delay 相等；

2． spf-max-waittime 的值不能小于 spf-holdtime ,否则 spf-max-waittime 的值将被自动设置为与 spf-holdtime 相等；

3． timers throttle spf 配置与 timers spf 配置会互相覆盖；

4． 当 timers spf 与 timers throttle spf 都未配置时，缺省值参见 timers throttle spf 配置的缺省值。

配置区间、外部路由计算延时时间

【命令格式】 **timers throttle route**{**inter-area***ia-delay*|**ase***ase-delay*}

【参数说明】 **inter-area***ia-delay*：定义区间路由计算的等待时间，以毫秒为单位，取值范围：0-600000。

ase*ase-delay*：定义外部路由计算的等待时间，以毫秒为单位，取值范围：0-600000。

【命令模式】 OSPF 路由进程配置模式

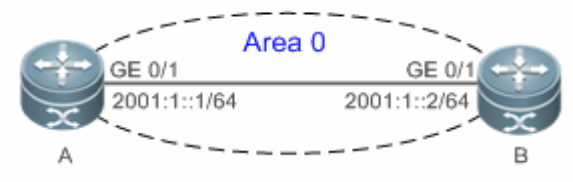
【使用指导】 如果对网络收敛时间有严格要求，使用默认值即可。

而对于存在大量区间、外部路由的网络，且网络不稳定时，可调整相应的延时时间，优化路由计算，减轻设备负担。

配置举例

配置 hello 时间和 dead 时间

【网络环境】



【配置方法】

- 所有路由器配置接口使能 IPv6。略。
- 所有路由器配置 OSPF 基本功能。略。
- 所有路由器配置 Hello 时间和 Dead 时间。

A

```
A# configure terminal
A(config)# interface GigabitEthernet 0/1
A(config-if-GigabitEthernet 0/1)# ipv6 ospf hello-interval 15
A(config-if-GigabitEthernet 0/1)# ipv6 ospf dead-interval 50
```

B

```
B# configure terminal
B(config)# interface GigabitEthernet 0/1
B(config-if-GigabitEthernet 0/1)# ipv6 ospf hello-interval 15
A(config-if-GigabitEthernet 0/1)# ipv6 ospf dead-interval 50
```

【检验方法】

- 路由器 A、B 检查接口参数：Hello 时间为 10S，Dead 时间为 50S。
- 路由器 A、B 检查 OSPF 邻居正确。

A

```
A# show ipv6 ospf interface
GigabitEthernet 0/1 is up, line protocol is up
  Interface ID 2
  IPv6 Prefixes
    fe80::2d0:f8ff:fe22:3346/64 (Link-Local Address)
  OSPFv3 Process (1), Area 0.0.0.0, Instance ID 0
    Router ID 1.1.1.1,Network Type BROADCAST, Cost: 1
    Transmit Delay is 1 sec, State DR, Priority 1
    Timer interval configured, Hello 15, Dead 50, Wait 40, Retransmit 10
      Hello due in 00:00:06
    Neighbor Count is 1, Adjacent neighbor count is 1
  Hello received 40 sent 40, DD received 17 sent 9
  LS-Req received 1 sent 3, LS-Upd received 6 sent 5
  LS-Ack received 3 sent 4, Discarded 1

A# show ipv6 ospf neighbor
OSPFv3 Process (1), 1 Neighbors, 1 is Full:
Neighbor ID     Pri   State           Dead Time   Instance ID   Interface
2.2.2.2           1   Full/BDR        00:00:30    0             GigabitEthernet 0/1
```

B

```
B# show ipv6 ospf interface
GigabitEthernet 0/1 is up, line protocol is up
  Interface ID 2
  IPv6 Prefixes
    fe80::2d0:f8ff:fe22:3446/64 (Link-Local Address)
  OSPFv3 Process (1), Area 0.0.0.0, Instance ID 0
    Router ID 2.2.2.2,Network Type BROADCAST, Cost: 1
    Transmit Delay is 1 sec, State BDR, Priority 1
    Timer interval configured, Hello 15, Dead 50, Wait 40, Retransmit 10
      Hello due in 00:00:06
    Neighbor Count is 1, Adjacent neighbor count is 1
  Hello received 40 sent 40, DD received 17 sent 9
  LS-Req received 1 sent 3, LS-Upd received 6 sent 5
  LS-Ack received 3 sent 4, Discarded 1

B# show ipv6 ospf neighbor
OSPFv3 Process (1), 1 Neighbors, 1 is Full:
Neighbor ID     Pri   State           Dead Time   Instance ID   Interface
1.1.1.1           1   Full/DR         00:00:38    0             GigabitEthernet 0/1
```

常见配置错误

- 配置的邻居维持时间小于 Hello 时间间隔。

6.6 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
清除并重启 OSPF 进程。	**clear ipv6 ospf** [*process-id*]**process**

查看运行情况

作用	命令
查看 OSPF 进程的配置信息。	**show ipv6 ospf** [*process-id*]
查看 OSPF 链路状态数据库。	**show ipv6 ospf**[*process- id*] **database**[*lsa-type* [**adv-router***router-id*]]
查看运行 OSPF 的接口。	**show ipv6 ospf** [*process-id*] **interface** [*interface-type interface-number* | **brief**]
查看 OSPF 的邻居表。	**show ipv6 ospf**[*process- id*] **neighbor**[*interface-type interface-number*[**detail**]| *neighbor-id* |**detail**]
查看 OSPF 路由表。	**show ipv6 ospf** [*process-id*] **route**[**count**]
查看 OSPF 重分布路由的汇聚路由。	**showipv6ospf**[*process-id*]**summary-prefix**
查看 OSPF 网络拓扑信息。	**show ipv6 ospf**[*process- id*] **topology** [**area***area-id*]

查看 OSPF 的虚链路	**show ipv6 ospf** [*process-id*] **virtual-links**

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 OSPF 事件的调试开关。	**debug ipv6 ospf events** [**abr**|**asbr**|**os**|**nssa**|**router**| **vlink**]
打开 OSPF 接口的调试开关。	**debug ipv6 ospf ifsm** [**events**|**status**|**timers**]
打开 OSPF 邻居的调试开关。	**debug ipv6 ospf nfsm** [**events** | **status** | **timers**]
打开 OSPF NSM 的调试开关。	**debug ipv6 ospf nsm** [**interface** | **redistribute** | **route**]
打开 OSPF LSA 的调试开关。	**debug ipv6 ospf lsa** [**flooding** | **generate** | **install** | **maxage** | **refresh**]
打开 OSPF 报文的调试开关。	**debug ipv6 ospf packet** [**dd**|**detail**|**hello**|**ls-ack**|**ls-request**|**ls-update**|**recv**|**send**]
打开 OSPF 路由的调试开关。	**debug ipv6 ospf route** [**ase** | **ia** | **install** | **spf** | **time**]

7 路由管理

7.1 概述

路由管理负责管理路由表，整合各种路由协议下发的路由，进行优选，并下发给转发表。路由表中保存了各种路由协议发现的路由，根据来源不同，通常分为以下三类：

- 直连路由：链路层协议发现的路由，也称为接口路由。
- 静态路由：网络管理员手工配置的。静态路由配置方便，对系统要求低，适用于拓扑结构简单并且稳定的小型网络。其缺点是每当网络拓扑结构发生变化，都需要手工重新配置，不能自动适应。
- 动态路由：动态路由协议发现的路由。

下文仅介绍路由表管理和静态路由的相关内容。

协议规范

- 无

7.2 典型应用

典型应用	场景描述
静态路由基本功能	手工方式配置路由
静态浮动路由	多路径情况下，配置备份路由
静态负载分担路由	多路径情况下，配置负载分担

7.2.1 静态路由基本功能

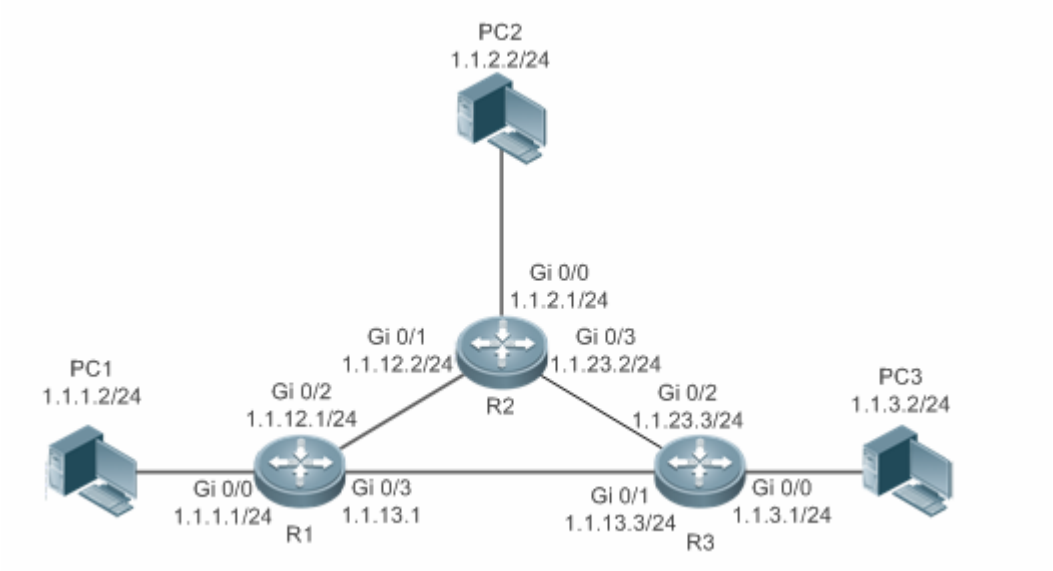
应用场景

在组网结构比较简单的网络中，只需配置静态路由就可以实现网络互通。恰当地设置和使用静态路由可以改善网络的性能，并可为重要的网络应用保证带宽。

以下图为例，为了使得 PC1，PC2，PC3 互通，可以在 R1，R2，R3 上配置静态路由。

- 在 R1 上配置到达 PC2 网段的路由走 R2，配置到达 PC3 网段的路由走 R3
- 在 R2 上配置到达 PC1 网段的路由走 R1，配置到达 PC3 网段的路由走 R3
- 在 R3 上配置到达 PC1 网段的路由走 R1，配置到达 PC2 网段的路由走 R2

图 7-1



功能部属

- 配置各接口的地址和掩码。
- 在 R1，R2，R3 上配置静态路由。

7.2.2 静态浮动路由

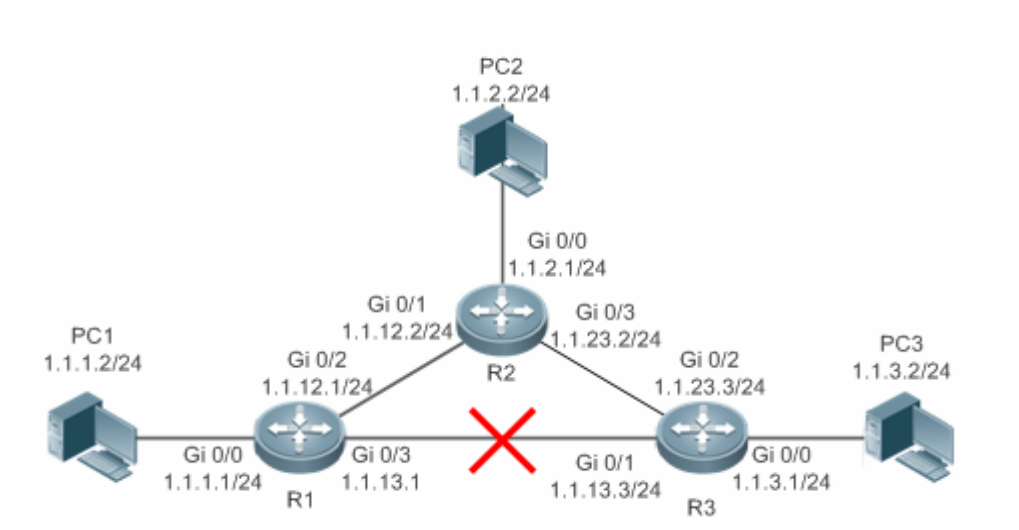
应用场景

在没有配置动态路由协议的情况下，为了避免网络线路故障导致的通信中断，可以配置静态浮动路由，实现路由的动态切换。

以下图为例，为避免 R1 与 R3 间线路故障导致的通信中断，可以在 R1 和 R3 上配置静态浮动路由。正常情况下，报文走管理距离（distance）小的路径，当该路由的链路出现故障 down 掉时，路由自动切换到管理距离大的路径。

- R1 上配置 2 条到达 PC3 网段的路由，一条走 R3（默认 distance=1），另一条走 R2（distance=2）。
- R3 上配置 2 条到达 PC1 网段的路由，一条走 R1（默认 distance=1），另一条走 R2（distance=2）。。

图 7-2



功能部属

- 配置各接口的地址和掩码。
- 在 R1，R2，R3 上配置静态路由。

7.2.3 静态负载分担路由

应用场景

在存在多条路径到达同一个目的的情况下，可以配置负载分担路由。与浮动路由不同的是，多条路由的管理距离（distance）相同。报文根据均衡转发策略在多条路由间分流。

以下图为例，在 R1，R3 上配置负载分担路由，使得到达 PC3 和 PC1 网段的报文，在 R2，R4 两条路径间均衡。

- 在 R1 上配置 2 条到达 PC3 网段的路由，一条走 R2，一条走 R4
- 在 R3 上配置 2 条到达 PC1 网段的路由，一条走 R2，一条走 R4

图 7-3



【注释】 缺省根据源 IP 地址进行负载均衡。

交换机上配置命令 aggregateport load-balance 可以修改 ECMP 路由的均衡模式。

路由器上配置命令 ip ref load-sharing original 指定 v4 路由的负载均衡策略

功能部属

- 配置各接口的地址和掩码。
- 在 R1，R2，R3，R4 上配置静态路由。
- 在 R1，R3 上配置负载分担策略。

7.3 功能详解

功能特性	作用
路由计算	在设备上产生可效的路由。
路由优选	在设备选择最优路由，以供报文转发。
缺省路由	使所有报文得以转发，且有助于缩小路由表规模。
路由可靠性	快速发现路由失效，并快速恢复通信。

7.3.1 路由计算

路由功能

路由功能分 IPv4 路由功能和 IPv6 路由功能。若关闭了路由功能，则设备相当于一台主机，不具备路由转发功能。

动态路由

动态路由协议以邻居间交换路由的方式学习远方的路由、并保持动态更新。如果邻居失效，则下一跳为此邻居的路由随之失效。

静态路由

在组网结构比较简单的网络中，只需配置静态路由就可以实现网络互通。恰当地设置和使用静态路由可以改善网络的性能，并可为重要的网络应用保证带宽。

静态路由根据本地接口的状态计算路由的活动性。当静态路由的出口处于三层 up 状态（链路状态为 up，且配置有 IP 地址）时，该路由为活动的，可以指导转发。

7.3.2 路由优选

管理距离

当多个路由协议产生了到达同一个目的地址的路由时，根据管理距离判断这些路由的优先级。管理距离越小，优先级越高。

等价路由

到达同一个目的地址，下一跳不同，管理距离相同的多条路由，则形成等价路由。报文根据均衡转发策略在多条路由间分流，从而实现负载分担。

具体设备上，对等价路由中包括的路由条目数是有限制的，超出限制的路由不会参与转发。

浮动路由

到达同一目的地址，下一跳不同，管理距离不同的多条路由，形成浮动路由。管理距离小的优先被选择参与转发，若管理距离小的路由失效，则管理距离大的路由替代管理距离小的路由参与转发，从而达到避免网络线路故障导致的通信中断。

7.3.3 缺省路由

在转发路由表中，目的网段 0.0.0.0 掩码 0.0.0.0 的路由，就是缺省路由。无法被其他路由转发的报文，可以被缺省路由转发出去。缺省路由可以静态配置，也可以由动态路由协议生成。

缺省网关

二层交换机通过配置 **ip default gateway** 命令来生成缺省路由。

静态缺省路由

三层交换机通过配置网段 0.0.0.0 掩码 0.0.0.0 的静态路由来生成缺省路由。

缺省网络

配置缺省网络的目的是为了产生缺省路由，当在设备上使用 **ip default-network** 指定一个网络（必须为 A 类，B 类，C 类的有类网络）时，这个网络如果在路由表中存在，则路由设备会将该网络作为缺省网络，该网络的下一跳成为缺省网关。因为 **ip**

default-network 是有类的，如果使用该命令标记一个主类网络的某个子网，路由设备会自动生成一条主类网络的静态路由而不会产生任何缺省路由。

7.3.4 路由可靠性

当网络中的一台设备发生故障时，会使某些路由不可达，从而造成流量中断。如果能够对路由下一跳的可达性进行实时检测，就可以在故障发生时立即重新计算路由，或者切换到备份路由。

与 Track 联动

Track 对象是一个抽象的概念，一个 Track 对象可以跟踪一个 IP 地址是否可达，也可以跟踪一个接口是否 up。将动态路由协议或静态路由与 Track 联动，可以使动态路由协议或静态路由快速感知下一跳不可达，从而快速反应。

7.4 产品说明

NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE 支持 IPV6 等价路由功能；NBR800G、NBR950G、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR108G-P、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1500G、NBR2000G 不支持 IPV6 等价路由。

7.5 配置详解

配置项	配置建议&相关命令	
配置静态路由	⚠ 必须配置。用于配置静态路由条目。	
	ip route	配置静态 IPv4 路由
	ipv6 route	配置静态 IPv6 路由
配置缺省路由	⚠ 可选配置。用于配置缺省网关。	
	ip default gateway	二层设备配置 IPv4 缺省网关
	ipv6 default gateway	二层设备配置 IPv6 缺省网关
	ip route 0.0.0.0 0.0.0.0 *gateway*	三层设备配置 IPv4 缺省网关
	ipv6 route ::/0 *ipv6-gateway*	三层设备配置 IPv6 缺省网关
	ip default network	三层设备配置 IPv4 缺省网络
配置路由限制	⚠ 可选配置。用于限制等价路由的条数，静态路由的条数和限制路由。	
	maximum-paths	配置等价路由条数限制
	ip static route-limit	配置静态 IPv4 路由限制
	ipv6 static route-limit	配置静态 IPv6 路由限制
	no ip routing	配置禁止 IPv4 路由

	no ipv6 unicast-routing	配置禁止 IPv6 路由

7.5.1 配置静态路由

配置效果

- 路由表中生成一条静态路由。使用静态路由，转发去远端网络的报文。

注意事项

- 二层交换机不能配置。
- 三层交换机若配置了 **no ip routing**，则不能配置 IPv4 静态路由，之前已经存在的 IPv4 静态路由也会被删除。在未重启的情况下，重新配置 **ip routing**，可以恢复被清空的 IPv4 静态路由。重启过后，则无法恢复这些 IPv4 静态路由。
- 三层交换机若配置了 **no ipv6 unicast- routing** ,则不能配置 IPv6 静态路由 ,之前已经存在的 IPv6 静态路由也会被删除。在未重启的情况下 ,重新配置 **ipv6 unicast- routing** ,可以恢复被清空的 IPv6 静态路由。重启过后 ,则无法恢复这些 IPv6 静态路由。
- 如需配置静态路由与 Track 联动，必须先通过 **track** 命令 track 对象。

配置方法

↘ 配置 IPv4 静态路由

在支持 IPv4 的路由器上，配置如下命令。

【命令格式】 **ip route***networknet-mask* {*ip-address* | *interface* [*ip-address*]} [*distance*] [**tag** *tag*] [**permanent** | **track** *object-number*] [**weight** *number*] [**description***description-text*] [**disabled** | **enabled**]

【参数说明】

network	目标网络的网络地址
net-mask	目标网络的掩码
ip-address	（可选）静态路由的下一跳地址。ip-address 和 interface 至少要指定一个，或者两者都指定。当未指定 ip-address 时，表示配置静态直连路由。
interface	（可选）静态路由的下一跳出口。ip-address 和 interface 至少要指定一个，或者两者都指定。当未指定 interface 时，表示配置静态递归路由，出口由下一跳在路由表中选路获得。
distance	（可选）静态路由的管理距离，缺省为 1。
tag	（可选）静态路由的 Tag 值，缺省为 0。
permanent	（可选）永久路由标识，缺省为非永久路由。
track *object-number*	（可选）与 Track 联动，object-number 指定 Track 对象 id，缺省不与 Track 联动
weight *number*	（可选）静态路由的权重值，缺省为 1。
description*descri*	（可选）静态路由描述信息，缺省无描述信息，*description-text* 为 1～60 个字符的字符

ption-text	串。
disabled/enabled	（可选）静态路由的使能标识，缺省为 enabled。

【缺省配置】 没配置静态路由

【命令模式】 全局模式

【使用指导】 此命令的最简配置：**ip route** *networknet-maskip-address*

配置静态路由与 Track 联动时，若 Track 对象检测出 down 状态，则该静态路由不活动，不参与路由转发。

配置 IPv6 静态路由

在支持 IPv6 的路由器上，配置如下命令。

【命令格式】 **ipv6 route** [**vrf***vrf-name*] *ipv6-prefix*/*prefix-length* { *ipv6-address* [**nexthop-vrf** {*vrf-name1*| **default**}] | *interface* [*ipv6-address* [**nexthop-vrf** {*vrf-name1*| **default**}]] } [*distance*] [**weight***number*] [**description***description-text*]

ipv6 route*ipv6-prefix*/*prefix-length* { *ipv6-address* | *interface* [*ipv6-address*] } [*distance*] [**weight***number*] [**description***description-text*]

【参数说明】

vrf*vrf-name*	（可选）路由所属 VRF，必须是已经配置 IPv6 地址族的多协议 VRF。缺省为全局 VRF。
ipv6-prefix	IPv6 前缀，必须遵循 RFC4291 的地址表示形式。
prefix-length	IPv6 前缀的长度，注意前面必须加上'/'
Ipv6-address	（可选）静态路由的下一跳地址。ipv6-address 和 interface 至少要指定一个，或者两者都指定。当未指定 ipv6-address 时，表示配置静态直连路由。
interface	（可选）静态路由的下一跳出口。ipv6-address 和 interface 至少要指定一个，或者两者都指定。当未指定 interface 时，表示配置静态递归路由，出口由下一跳在路由表中选路获得。
nexthop-vrf *vrf-name1*	（可选）下一跳所属 VRF，必须是已经配置 IPv6 地址族的多协议 VRF。缺省下一跳所属的 VRF 与 vrf name 指定的 VRF 相同。**nexthop-vrf default** 表示下一跳所属的 VRF 为全局 VRF。
distance	（可选）静态路由的管理距离，缺省为 1。
weight *number*	（可选）静态路由的权重值，在配置等价路径时指明该路径的权重。配置范围：1-8，一条路由的所有等价路径的权重之和不能超过该条路由所能配置的最大等价路径条目数，同一条路由的等价路径之间的权重比指明了这些路径之间的流量比率关系。缺省为 1。
description*description-text*	（可选）静态路由描述信息，缺省无描述信息，*description-text* 为 1～60 个字符的字符串。

【缺省配置】 没配置静态路由

【命令模式】 全局模式

【使用指导】 此命令的最简配置：**ipv6 route***ipv6-prefix*/*prefix-length**ipv6-address*

检验方法

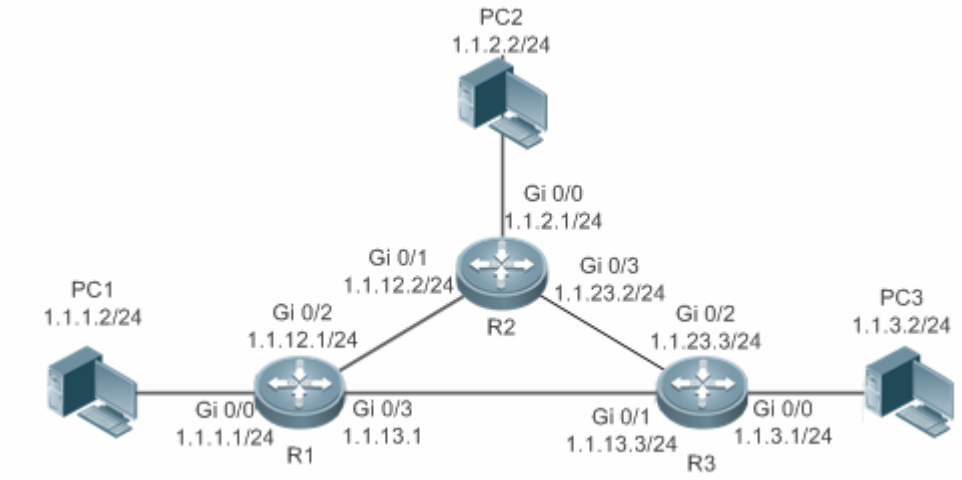
- 使用 **show ip route** 命令查看 IPv4 路由表，检查之前配置的 IPv4 静态路由是否生效。
- 使用 **show ipv6 route** 命令查看 IPv6 路由表，检查之前配置的 IPv6 静态路由是否生效。

配置举例

↘ 在 IPv4 网络上，配置静态路由使网络联通

【网络环境】

图 7-4



【配置方法】

- 在设备各接口上配置地址

R1

```
R1#configure terminal
R1(config)#interface gigabitEthernet 0/0
R1(config-if-GigabitEthernet 0/0)# ip address 1.1.1.1 255.255.255.0
R1(config-if-GigabitEthernet 0/0)# exit
R1(config)#interface gigabitEthernet 0/2
R1(config-if-GigabitEthernet 0/2)# ip address 1.1.12.1 255.255.255.0
R1(config-if-GigabitEthernet 0/0)# exit
R1(config)#interface gigabitEthernet 0/3
R1(config-if-GigabitEthernet 0/3)# ip address 1.1.13.1 255.255.255.0
```

R2

```
R2#configure terminal
R2(config)#interface gigabitEthernet 0/0
R2(config-if-GigabitEthernet 0/0)# ip address 1.1.2.1 255.255.255.0
R2(config-if-GigabitEthernet 0/0)# exit
R2(config)#interface gigabitEthernet 0/1
R2(config-if-GigabitEthernet 0/1)# ip address 1.1.12.2 255.255.255.0
R2(config-if-GigabitEthernet 0/0)# exit
R2(config)#interface gigabitEthernet 0/3
```

```
R2(config-if-GigabitEthernet 0/3)# ip address 1.1.23.2 255.255.255.0
```

R3

```
R3#configure terminal
R3(config)#interface gigabitEthernet 0/0
R3(config-if-GigabitEthernet 0/0)# ip address 1.1.3.1 255.255.255.0
R3(config-if-GigabitEthernet 0/0)# exit
R3(config)#interface gigabitEthernet 0/1
R3(config-if-GigabitEthernet 0/1)# ip address 1.1.13.3 255.255.255.0
R3(config-if-GigabitEthernet 0/0)# exit
R3(config)#interface gigabitEthernet 0/2
R3(config-if-GigabitEthernet 0/2)# ip address 1.1.23.3 255.255.255.0
```

- 在设备上配置静态路由

R1

```
R1#configure terminal
R1(config)#ip route 1.1.2.0 255.255.255.0 GigabitEthernet 0/2 1.1.12.2
R1(config)# ip route 1.1.3.0 255.255.255.0 GigabitEthernet 0/3 1.1.13.3
```

R2

```
R2#configure terminal
R2(config)#ip route 1.1.1.0 255.255.255.0 GigabitEthernet 0/1 1.1.12.1
R2(config)# ip route 1.1.3.0 255.255.255.0 GigabitEthernet 0/3 1.1.23.3
```

R3

```
R3#configure terminal
R3(config)#ip route 1.1.2.0 255.255.255.0 GigabitEthernet 0/2 1.1.23.2
R3(config)# ip route 1.1.1.0 255.255.255.0 GigabitEthernet 0/1 1.1.13.1
```

【检验方法】

- 显示路由表

R1

```
R1# show ip route
Codes:  C - Connected, L - Local, S - Static
        R - RIP, O - OSPF, B - BGP, I - IS-IS
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - Inter area, * - candidate default

Gateway of last resort is no set
C     1.1.1.0/24 is directly connected, GigabitEthernet 0/0
C     1.1.1.1/32 is local host.
S     1.1.2.0/24 [1/0] via 1.1.12.2, GigabitEthernet 0/2
S     1.1.3.0/24 [1/0] via 1.1.13.3, GigabitEthernet 0/2
C     1.1.12.0/24 is directly connected, GigabitEthernet 0/2
C     1.1.12.1/32 is local host.
C     1.1.13.0/24 is directly connected, GigabitEthernet 0/3
C     1.1.13.1/32 is local host.
```

R2

```
R2# show ip route
Codes:  C - Connected, L - Local, S - Static
```

```
        R - RIP, O - OSPF, B - BGP, I - IS-IS
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - Inter area, * - candidate default

Gateway of last resort is no set
S     1.1.1.0/24 [1/0] via 1.1.12.1, GigabitEthernet 0/0
C     1.1.2.0/24 is directly connected, GigabitEthernet 0/0
C     1.1.2.1/32 is local host.
S     1.1.3.0/24 [1/0] via 1.1.23.3, GigabitEthernet 0/3
C     1.1.12.0/24 is directly connected, GigabitEthernet 0/1
C     1.1.12.2/32 is local host.
C     1.1.23.0/24 is directly connected, GigabitEthernet 0/3
C     1.1.23.2/32 is local host.
```

R3

```
R3# show ip route
Codes:  C - Connected, L - Local, S - Static
        R - RIP, O - OSPF, B - BGP, I - IS-IS
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - Inter area, * - candidate default

Gateway of last resort is no set
S     1.1.1.0/24 [1/0] via 1.1.13.1, GigabitEthernet 0/2
S     1.1.2.0/24 [1/0] via 1.1.23.2, GigabitEthernet 0/2
C     1.1.3.0/24 is directly connected, GigabitEthernet 0/0
C     1.1.3.1/32 is local host.
C     1.1.13.0/24 is directly connected, GigabitEthernet 0/1
C     1.1.13.3/32 is local host.
C     1.1.23.0/24 is directly connected, GigabitEthernet 0/2
C     1.1.23.3/32 is local host.
```

网关产品不支持 isis,bgp，配置举例仅作为配置参考，实际请以具体设备配置为准。

配置 IPv4 静态路由与 Track 联动

【网络环境】

图 7-5



【配置方法】
- 在 R1、R2 上配置静态路由，指定出接口/下一跳为互联接口。
- 在 R1、R2 上配置静态路由与 TRACK 联动，检测静态路由下一跳的连通性。
-

R1

```
R1#configure terminal
R1(config)#interface gigabitEthernet 0/1
R1(config-if-GigabitEthernet 0/1)# ip address 1.1.12.1 255.255.255.0
R1(config-if-GigabitEthernet 0/1)# exit
R1(config)#track 2 interface gigabitEthernet 0/1 line-protocol
R1(config)# ip route 1.1.2.0 255.0.0.0 gigabitEthernet 0/1 1.1.12.2 track 2
```

R2

```
R2#configure terminal
R1(config)#interface gigabitEthernet 0/1
R1(config-if-GigabitEthernet 0/1)# ip address 1.1.12.2 255.255.255.0
R1(config-if-GigabitEthernet 0/1)# exit
R1(config)#track 2 interface gigabitEthernet 0/1 line-protocol
R1(config)# ip route 1.1.1.0 255.0.0.0 gigabitEthernet 0/1 1.1.12.1 track 2
```

【检验方法】
- 查看 TRACK 状态
- 查看与 TRACK 联动的静态路由

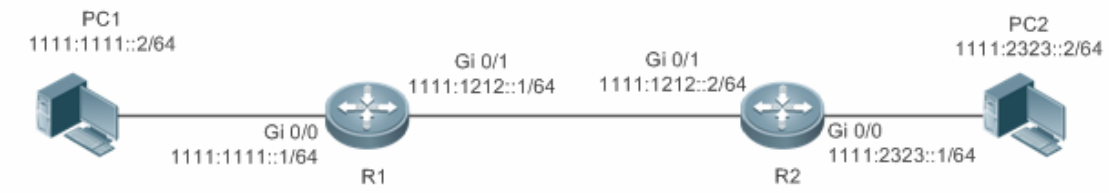
```
R1# show track 2
Track 2
Interface gigabitEthernet 0/1
  The state is Up, delayed Down (5 secs remaining)
    1 change, current state last: 300 secs
  Delay up 0 secs, down 0 secs

R1#show ip route track-table
ip route 1.1.2.0 255.0.0.0 GigabitEthernet 0/1 1.1.12.2 track 2 up
```

-

在 IPv6 网络上，配置静态路由使网络联通

【网络环境】

图 7-6



【配置方法】
- 在设备各接口上配置地址

R1

```
R1#configure terminal
R1(config)#interface gigabitEthernet 0/0
```

```
R1(config-if-GigabitEthernet 0/0)# ipv6 address 1111:1111::1/64
R1(config-if-GigabitEthernet 0/0)# exit
R1(config)#interface gigabitEthernet 0/1
R1(config-if-GigabitEthernet 0/1)# ipv6 address 1111:1212::1/64
```

R2

```
R2#configure terminal
R2(config)#interface gigabitEthernet 0/0
R2(config-if-GigabitEthernet 0/0)#ipv6 address 1111:2323::1/64
R2(config-if-GigabitEthernet 0/0)# exit
R2(config)#interface gigabitEthernet 0/1
R2(config-if-GigabitEthernet 0/1)# ipv6 address 1111:1212::2/64
```

- 在设备上配置静态路由

R1

```
R1#configure terminal
R1(config)#ipv6 route 1111:2323::0/64 gigabitEthernet 0/1
```

R2

```
R2#configure terminal
R2(config)#ipv6 route 1111:1111::0/64 gigabitEthernet 0/1
```

【检验方法】

- 显示路由表

R1

```
R1# show ipv6 route

IPv6 routing table name - Default - 10 entries
Codes:  C - Connected, L - Local, S - Static
        R - RIP, O - OSPF, B - BGP, I - IS-IS
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - Inter area

C       1111:1111::/64 via GigabitEthernet 0/0, directly connected
L       1111:1111::1/128 via GigabitEthernet 0/0, local host
C       1111:1212::/64 via GigabitEthernet 0/1, directly connected
L       1111:1212::1/128 via GigabitEthernet 0/1, local host
S       1111:2323::/64 [1/0] via GigabitEthernet 0/1, directly connected
C       FE80::/10 via ::1, Null0
C       FE80::/64 via GigabitEthernet 0/0, directly connected
L       FE80::2D0:F8FF:FEFB:C092/128 via GigabitEthernet 0/0, local host
C       FE80::/64 via GigabitEthernet 0/1, directly connected
L       FE80::2D0:F8FF:FEFB:C092/128 via GigabitEthernet 0/1, local host
```

R2

```
R2# show ipv6 route
```

```
IPv6 routing table name - Default - 10 entries
Codes:  C - Connected, L - Local, S - Static
        R - RIP, O - OSPF, B - BGP, I - IS-IS
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - Inter area

C       1111:2323::/64 via GigabitEthernet 0/0, directly connected
L       1111:2323::1/128 via GigabitEthernet 0/0, local host
C       1111:1212::/64 via GigabitEthernet 0/1, directly connected
L       1111:1212::1/128 via GigabitEthernet 0/1, local host
S       1111:1111::/64 [1/0] via GigabitEthernet 0/1, directly connected
C       FE80::/10 via ::1, Null0
C       FE80::/64 via GigabitEthernet 0/0, directly connected
L       FE80::2D0:F8FF:FEFB:C092/128 via GigabitEthernet 0/0, local host
C       FE80::/64 via GigabitEthernet 0/1, directly connected
L       FE80::2D0:F8FF:FEFB:C092/128 via GigabitEthernet 0/1, local host
```

常见错误

- 接口链路没有 up
- 接口没有配置地址
- 配置静态路由与 Track 联动，但未配置 Track 对象。

7.5.2 静态配置缺省路由

配置效果

- 路由表中生成一条缺省路由。不能被其他路由转发的报文，使用缺省路由转发。

注意事项

- 二层交换机可以通过 **ip default gateway** 和 **ipv6 default gateway** 命令配置网关。
- 三层交换机可以通过 **ip route** 0.0.0.0 0.0.0.0 *gateway* 和 **ipv6 route** ::/0 *ipv6-gateway* 命令配置网关。
- 三层交换机若配置了 **no ip routing** 或 **no ipv6 unicast- routing** 则可通过 **ip default gateway** 和 **ipv6 default gateway** 命令配置网关。

配置方法

二层交换机配置 IPv4 网关

【命令格式】 **ip default-gateway***gateway*

【参数说明】 *gateway* | IPv4 网关地址

【缺省配置】 无静态缺省路由

【命令模式】 全局模式

【使用指导】 -

二层交换机配置 IPv6 网关

【命令格式】 **ipv6 default-gateway***gateway*

【参数说明】 *gateway* | IPv6 网关地址

【缺省配置】 无静态缺省路由

【命令模式】 全局模式

【使用指导】 -

三层交换机配置 IPv4 缺省网关

【命令格式】 **ip route0.0.0.00.0.0.0**{*ip-address* | *interface* [*ip-address*]} [*distance*] [**tag** *tag*] [**permanent**] [**weight** *number*] [**description***description-text*] [**disabled** | **enabled**]

【参数说明】

0.0.0.0	目标网络的网络地址
0.0.0.0	目标网络的掩码
ip-address	（可选）静态路由的下一跳地址。ip-address 和 interface 至少要指定一个，或者两者都指定。当未指定 ip-address 时，表示配置静态直连路由。
interface	（可选）静态路由的下一跳出口。ip-address 和 interface 至少要指定一个，或者两者都指定。当未指定 interface 时，表示配置静态递归路由，出口由下一跳在路由表中选路获得。
distance	（可选）静态路由的管理距离，缺省为 1。
tag	（可选）静态路由的 Tag 值，缺省为 0。
permanent	（可选）永久路由标识，缺省为非永久路由。
weight *number*	（可选）静态路由的权重值，缺省为 1。
description*description-text*	（可选）静态路由描述信息，缺省无描述信息，*description-text* 为 1～60 个字符的字符串。
disabled /enabled	（可选）静态路由的使能标识，缺省为 enabled。

【缺省配置】 无静态缺省路由

【命令模式】 全局模式

【使用指导】 此命令的最简配置：**ip route0.0.0.0 0.0.0.0***ip-address*

三层交换机配置 IPv6 缺省网关

【命令格式】 **ipv6 route** [**vrf***vrf-name*] **::/0** { *ipv6-address* [**nexthop-vrf** {*vrf-name1*| **default**}] | *interface* [*ipv6-address*[**nexthop-vrf** {*vrf-name1*| **default**}]] } [*distance*] [**weight***number*] [**description***description-text*]

ipv6 route::/0 { *ipv6-address* | *interface* [*ipv6-address*] } [*distance*] [**weight***number*] [**description***description-text*]

【参数说明】

vrf*vrf-name*	（可选）路由所属 VRF ,必须是已经配置 IPv6 地址族的多协议 VRF。缺省为全局 VRF。
::	IPv6 前缀，必须遵循 RFC4291 的地址表示形式。
0	IPv6 前缀的长度，注意前面必须加上'/'
Ipv6-address	（可选）静态路由的下一跳地址。ipv6-address 和 interface 至少要指定一个，或者两者都指定。当未指定 ipv6-address 时，表示配置静态直连路由。
interface	（可选）静态路由的下一跳出口。ipv6-address 和 interface 至少要指定一个，或者两者都指定。当未指定 interface 时，表示配置静态递归路由，出口由下一跳在路由表中选路获得。
nexthop-vrf *vrf-name1*	（可选）下一跳所属 VRF，必须是已经配置 IPv6 地址族的多协议 VRF。缺省下一跳所属的 VRF 与 vrf name 指定的 VRF 相同。**nexthop-vrf default** 表示下一跳所属的 VRF 为全局 VRF。
distance	（可选）静态路由的管理距离，缺省为 1。
weight *number*	（可选）静态路由的权重值，在配置等价路径时指明该路径的权重。配置范围：1-8，一条路由的所有等价路径的权重之和不能超过该条路由所能配置的最大等价路径条目数，同一条路由的等价路径之间的权重比指明了这些路径之间的流量比率关系。缺省为 1。
description*description-text*	（可选）静态路由描述信息，缺省无描述信息，*description-text* 为 1～60 个字符的字符串。

【缺省配置】 无静态缺省路由

【命令模式】 全局模式

【使用指导】 此命令的最简配置：**ipv6 route** ::/0 *ipv6-gateway*

三层交换机配置 IPv4 缺省网络

【命令格式】 **ip default-network** *network*

【参数说明】 *network* | 网络地址（必须为 A 类，B 类，C 类的有类网络）

【缺省配置】 无缺省网络

【命令模式】 全局模式

【使用指导】 如果 **ip default-network** 指定的网络在路由表中存在，则生成一条缺省路由，以到达该网络的下一跳为缺省网关。否则不产生缺省路由。

检验方法

- 在二层交换机（及关闭了路由功能的三层交换机）上，使用 **show ip redirects** 和 **show ipv6 redirects** 查看默认网关。
- 在（未关闭路由功能的）三层交换机上，使用 **show ip route、show ipv6route** 命令查看缺省路由。

配置举例

↘ 三层交换机，配置 IPv4 缺省路由，使网络连通

【网络环境】

图 7-6



【配置方法】

- 在三层设备上配置 IP 地址

R1

```
R1#configure terminal
R1(config)#interface gigabitEthernet 0/0
R1(config-if-GigabitEthernet 0/0)# ip address 1.1.1.1 255.255.255.0
R1(config-if-GigabitEthernet 0/0)# exit
R1(config)#interface gigabitEthernet 0/1
R1(config-if-GigabitEthernet 0/1)# ip address 1.1.12.1 255.255.255.0
R1(config-if-GigabitEthernet 0/0)# exit
```

R2

```
R2#configure terminal
R2(config)#interface gigabitEthernet 0/0
R2(config-if-GigabitEthernet 0/0)# ip address 1.1.2.1 255.255.255.0
R2(config-if-GigabitEthernet 0/0)# exit
R2(config)#interface gigabitEthernet 0/1
R2(config-if-GigabitEthernet 0/1)# ip address 1.1.12.2 255.255.255.0
R2(config-if-GigabitEthernet 0/0)# exit
```

R1

- 在三层设备 R1 上配置缺省网关

```
R1#configure terminal
R1(config)#ip route 0.0.0.0 0.0.0.0  GigabitEthernet 0/1 1.1.12.2
```

```
R2#configure terminal
R2(config)#ip route 0.0.0.0 0.0.0.0  GigabitEthernet 0/1 1.1.12.1
```

R2

【检验方法】 ● 显示路由表

R1

```
R1# show ip route
Codes:  C - Connected, L - Local, S - Static
        R - RIP, O - OSPF, B - BGP, I - IS-IS
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - Inter area, * - candidate default

Gateway of last resort is 1.1.12.2
S*    0.0.0.0/0 [1/0] via 1.1.12.2, GigabitEthernet 0/1
C     1.1.1.0/24 is directly connected, GigabitEthernet 0/0
C     1.1.1.1/32 is local host.
C     1.1.12.0/24 is directly connected, GigabitEthernet 0/1
C     1.1.12.1/32 is local host.
```

网关产品不支持 BGP,ISIS，配置举例仅作为配置参考，实际请以具体设备配置为准。

7.5.3 配置路由限制

配置效果

- 限制等价路由的条数，静态路由的条数或限制路由转发

注意事项

二层交换机不能配置

配置方法

↘ 配置等价路由的条数

【命令格式】 **maximum-paths***number*

【参数说明】 *number* | 等价路由条数，范围 1-64，实际支持范围与具体设备型号相关。

【缺省配置】 实际缺省值与具体设备型号相关。

【命令模式】 全局模式

【使用指导】 通过该命令限制等价路由中下一跳的数目。配置等价路由条数后，在负载均衡模式下，负载均衡的分路数不会超过配置的等价路由数。

↘ 配置静态 IPv4 路由限制

【命令格式】 **ip static route-limit***number*

【参数说明】 *number* | 路由上限，范围 1-10000，缺省值 1024

【缺省配置】 允许配置的静态路由条数最大值为 IP 路由 1024 条

【命令模式】 全局模式

【使用指导】 使用此命令配置 IPV4 静态路由最大条数。超过了最大条数值后，IPV4 静态路由配置不成功。

配置静态 IPv6 路由限制

【命令格式】 **ipv6 static route-limit***number*

【参数说明】 *number* | 路由上限，范围 1-10000，缺省值 1000

【缺省配置】 允许配置的静态路由条数最大值为 IPv6 路由 1000 条

【命令模式】 全局模式

【使用指导】 使用此命令配置 IPV6 静态路由最大条数。超过了最大条数值后，IPV6 静态路由配置不成功。

配置禁止 IPv4 路由转发

【命令格式】 **no ip routing**

【参数说明】 -

【缺省配置】 IP 路由功能开启

【命令模式】 全局模式

【使用指导】 使用此命令关闭 IPv4 路由。当设备只作为桥接设备，或者只作为 VOIP 网关设备时，可以不需要 RGOS 软件的 IPv4 路由转发功能。这时可以关闭 RGOS 的 IPv4 路由功能。

配置禁止 IPv6 路由

【命令格式】 **no ipv6 unicast-routing**

【参数说明】 -

【缺省配置】 IPv6 路由功能开启

【命令模式】 全局模式

【使用指导】 使用此命令关闭 IPv6 路由。当设备只作为桥接设备，或者只作为 VOIP 网关设备时，可以不需要 RGOS 软件的 IPv6 路由转发功能。这时可以关闭 RGOS 的 IPv6 路由功能。

7.6 监视与维护

查看运行情况

作用	命令
查看 IPv4 路由表。	**show ip route**

查看 IPv6 路由表。	show ipv6 route

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 v4 路由管理的调试开关	**debug nsm kernel ucast- v4**
打开缺省网络管理的调试开关	**debug nsm kernel default-network**
打开路由管理内部事件调试开关	**debug nsm events**
打开路由管理与路由协议消息发送开关	**debug nsm packet send**
打开路由管理与路由协议消息接收开关	**debug nsm packet recv**

配置指南-安全

本分册介绍安全相关内容，包括以下章节：

1. ACL
2. RPL
3. REF-RNFP
4. SSH
5. DHCP Snooping
6. ARP Check
7. IP Source Guard
8. SEC-VPDN
9. IPSEC
10. IKE
11. AAA
12. RADIUS
13. TACACS+
14. Web 认证
15. 全局 IP+MAC 绑定
16. IPoE
17. IP-GROUP
18. APP-AUTH
19. Webservice

20. ANTI-PAP
21. 广告推送
22. Local-Account
23. 防火墙

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。

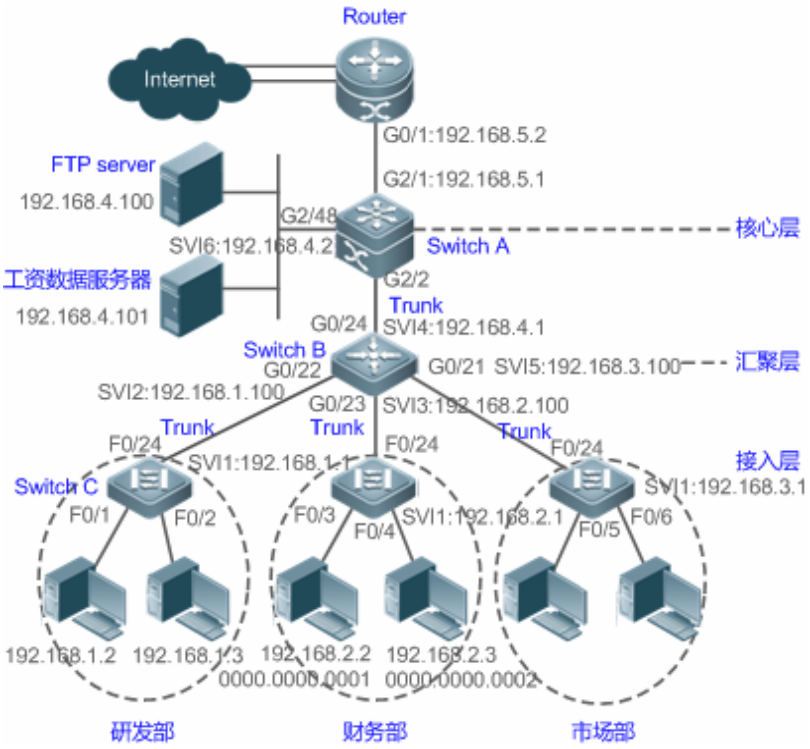
1.2.1 企业内网络访问控制应用

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。

功能部属

- 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。

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。

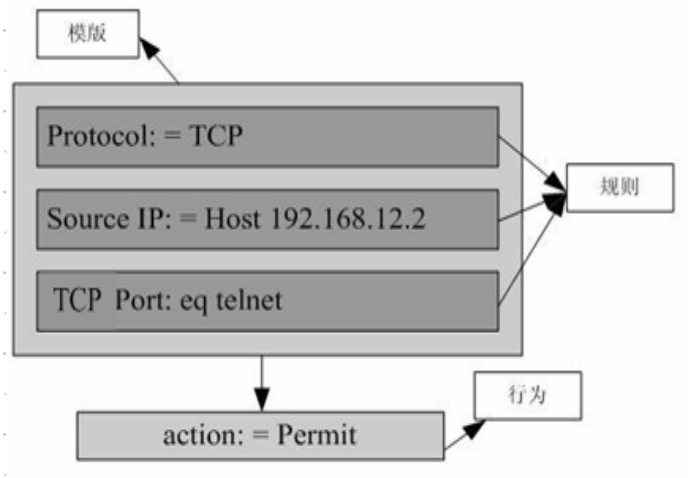
过滤域指的是，在生成一条 ACE 时，根据报文中的哪些字段用以对报文进行识别、分类。过滤域模板就是这些字段组合的定义。比如，在生成某一条 ACE 时希望根据报文的目的 IP 字段对报文进行识别、分类，而在生成另一条 ACE 时，希望根据的是报文的源 IP 地址字段和 UDP 的源端口字段，这样，这两条 ACE 就使用了不同的过滤域模板。

规则(Rules)，指的是 ACE 过滤域模板对应的值。 比如有一条 ACE 内容如下：

```
permit tcp host 192.168.12.2 any eq telnet
```

在这条 ACE 中，过滤域模板为以下字段的集合：源 IP 地址字段、IP 协议字段、目的 TCP 端口字段。对应的值(Rules)分别为：源 IP 地址 = Host 192.168.12.2；IP 协议 = TCP；TCP 目的端口 = Telnet。

图 1-2 对 ACE：permit tcp host 192.168.12.2 any eq telnet 的分析



过滤域模板可以是三层字段(Layer 3 Field)和四层字段(Layer 4 Field)字段的集合，也可以是多个二层字段(Layer 2 Field)的集合，但标准与扩展的 ACL 的过滤域模板不能是二层和三层、二层和四层、二层和三层、四层字段的集合。要使用二层、三层、四层字段集合，可以应用 Expert 扩展访问控制列表（Expert ACLs）。

OUT 方向 ACL 关联 SVI 的注意事项：支持 IP 标准，IP 扩展，MAC 扩展。

对 ACL 中匹配目的 IP 和目的 MAC 有一些限制，如果在 MAC 扩展中匹配目的 MAC，将这样的 ACL 应用到 SVI 的 OUT 方向时，表项会被设置，但无法生效。如果想要在 IP 扩展中匹配目的 IP，而目的 IP 不在所关联的 SVI 的子网 IP 范围内时，该配置的 ACL 将无法生效。比如 VLAN 1 的地址为 192.168.64.1 255.255.255.0，创建一条 IP 扩展的 ACL， ace 为 deny udp any 192.168.65.1 0.0.0.255 eq 255，将该 ACL 应用到 VLAN 1 的出口，将无法生效，因为目的 IP 不在 VLAN 1 子网 IP 范围内，如果 ace 为 deny udp any 192.168.64.1 0.0.0.255 eq 255 将可以生效，因为目的 IP 符合规定。

应用 ACL 时，如果 ACL（包括 IP 访问列表）中的 ACE 匹配了非 L2 字段，比如 SIP，DIP 时，对于带标签的 MPLS 报文匹配是无效的。

ACL logging

为了让用户更好的掌握 ACL 在设备中的运行状态，在添加规则时可以根据需要决定是否指定报文匹配日志输出选项，如果指定了该选项，则在规则匹配到报文时会输出匹配日志信息。ACL logging 信息是基于 ACE 来打印 log 信息的，也即设备周期性的打印命中报文的 ACE 信息，以及该 ACE 命中的报文数量。如下：

```
*Sep  9 16:23:06: %ACL-6-MATCH: ACL 100 ACE 10 permit icmp any any, match 78 packets.
```

为合理控制 log 输出的数量和频率，ACL logging 支持配置 log 输出间隔的配置，并且支持分别配置 IPv4 ACL 和 IPv6 ACL 的 log 输出间隔。

- 带 ACL logging 选项的 ACE 使用更多的硬件资源，如果配置的所有 ACE 都带有 ACL logging 选项，则会导致设备的 ACE 容量减半。
- 默认 ACL logging 的 log 输出间隔是 0，也即不输出 log。在为 ACE 指定了报文匹配日志输出选项后，若要输出相应的 log，需要配置 ACL logging 的输出间隔。
- 对于带 ACL logging 选项的 ACE，如果指定的时间间隔内没有匹配到任何报文，则不会输出与该 ACE 有关的报文匹配日志；如果指定的时间间隔内有匹配到报文，则时间间隔到期后，会输出与该 ACE 有关的报文匹配日志。其中的报文命中数目为该时间间隔内该 ACE 匹配到的报文总数，即为该 ACE 上一次输出 log 到本次输出 log 之间命中的报文数。
- 仅在交换机设备上支持 ACL logging 功能。

ACL 报文匹配计数

由于网络管理的需要，有时用户可能会想知道某条 ACE 有没有匹配到报文，匹配了多少个。因此，ACL 提供了基于 ACE 的报文匹配计数，用户可以基于 ACL 开启和关闭该 ACL 下的所有的 ACE 的报文匹配计数功能，支持的 ACL 类型包括：IP 访问列表、MAC 访问列表、Expert 访问列表和 IPv6 访问列表。此外，用户可通过 ACL 的统计清除命令将 ACL 规则的报文匹配计数器清 0，以便重新统计。

- 开启 ACL 的报文匹配计数功能需要更多的硬件表项，极端情况下会使设备可以配置的 ACE 容量减半。
- 仅在交换机设备上支持 ACL 报文匹配计数功能。

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。
IPv6 访问列表	可以根据 IPv6 报文头部的三层或四层信息对进出设备的 IPv6 报文进行控制
报文匹配日志	可以根据需要每隔一段时间输出 ACL 的报文匹配日志信息，根据信息可以了解到指定规则的报文匹配情况

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：

- 不管是命名的标准 IP 访问列表，还是数值索引的标准 IP 访问列表，都可以在标准 IP 访问列表模式下使用[*sn*] { **permit** | **deny** } {**host** *source* | **any** | *source source-wildcard* } [**time-range** *time-range-name*] [**log**]命令为访问列表配置一条匹配规则。
- 数值索引的标准 IP 访问列表，除了可以在标准 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** } {**host** *source* | **any** | *source source-wildcard* } [**time-range** *tm-rng-name*][**log**]命令为标准 IP 访问列表配置一条匹配规则。

对于扩展 IP 访问列表，可以通过以下方式配置匹配规则：

应用 IP 访问列表

缺省情况下，设备上的所有接口都没有应用 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。

在接口模式下使用 **ip access-group** { *acl-id* **|** *acl-name* } { **in** | **out** }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 报文匹配日志

报文匹配日志主要用于监控访问列表规则的运行状态，为日常网络维护以及网络优化提供必要的信息。

工作原理

为了让用户更好的掌握 ACL 在设备中的运行状态，在添加规则时可以根据需要决定是否指定报文匹配日志输出选项，如果指定了该选项，则在规则匹配到报文时会输出匹配日志信息。ACL logging 信息是基于 ACE 来打印 log 信息的，也即设备周期性的打印命中报文的 ACE 信息，以及该 ACE 命中的报文数量。如下：

```
*Sep  9 16:23:06: %ACL-6-MATCH: ACL 100 ACE 10 permit icmp any any, match 78 packets.
```

为合理控制 log 输出的数量和频率，ACL logging 支持配置 log 输出间隔的配置。

带 log 选项的访问列表规则会使用更多的硬件资源，如果配置的所有规则都带有 log 选项，则会导致设备的硬件策略容量减半。

默认报文匹配日志输出间隔是 0，即不输出上层。在配置访问列表规则时指定了 log 选项后，还需要配置输出间隔，否则不会输出匹配日志。

对于带 log 选项的规则，如果指定的时间间隔内没有匹配到任何报文，则不会输出与该规则有关的报文匹配日志；如果指定的时间间隔内有匹配到报文，则时间间隔到期后，会输出与该规则有关的报文匹配日志。其中的报文命中数目为该时间间隔内该规则匹配到的报文总数，即为该规则上一次输出日志到本次输出日志之间命中的报文数。

相关配置

配置访问列表

在配置带 log 选项的访问列表规则之前，必须先配置访问列表，访问列表的配置说明请参考相关的章节。

配置访问列表规则

访问列表规则的配置方法请参考 IP 以及 IPv6 访问列表的相关章节说明。注意要配置 log 选项。

配置报文匹配日志输出间隔

在配置模式下使用{ **Ip | ipv6** } **access-list log-update inerval** *time* 命令配置报文匹配日志输出间隔。

应用访问列表

访问列表规则的应用方法请参考 IP 以及 IPv6 访问列表的相关章节说明。

1.3.3 报文匹配计数

除了报文匹配日志外，报文匹配计数为日常的网络维护和网络优化提供了另一种选择。

工作原理

出于网络管理的需要，用户可能会想知道某条访问列表规则有没有匹配到报文，匹配了多少个。因此，ACL 提供了基于规则的报文匹配计数功能，用户可以基于 ACL 开启和关闭该 ACL 下的所有规则的报文匹配计数功能，当有报文匹配到了这条规则，对应的匹配计数就相应地增长。用户可通过 ACL 的统计清除命令将该 ACL 下所有规则的报文匹配计数器清 0，以便重新统计。

开启 ACL 的报文匹配计数功能需要更多的硬件表项，极端情况下会使设备可以配置的硬件策略容量减半。

支持在 IP 访问列表、上开启报文匹配计数功能。

仅在交换机设备上支持 ACL 报文匹配计数功能。

相关配置

配置访问列表

在配置带 log 选项的访问列表规则之前，必须先配置访问列表，访问列表的配置说明请参考相关的章节。

配置访问列表规则

访问列表规则的配置方法请参考访问列表的相关章节说明。注意要配置 log 选项。

开启报文匹配计数

如果用户想在 IP 访问列表、上开始报文匹配计数功能，请在配置模式下使用{ **Ip**} **access-list counter** { *acl-id* | *acl-name* }命令来开启；

应用访问列表

访问列表规则的应用方法请参考 IP 访问列表、的相关章节说明。

清除报文匹配计数

在特权模式下使用 **clear counters access-list** [*acl-id* | *acl-name*]命令来清除。

1.4 产品说明

NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE 支持 IPV6 ACL 功能；NBR800G、NBR950G、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR108G-P、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1500G、NBR2000G 不支持 IPV6 ACL 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。	
	ip access-list standard	配置 IP 标准访问列表
	ip access-list extended	配置 IP 标准访问列表

	permit host any time-range log	配置 permit 类型的 IP 标准访问列表规则
	deny host any time-range log	配置 deny 类型的 IP 标准访问列表规则
	permit host any host any precedence time-range log	配置 permit 类型的 IP 扩展访问列表规则
	deny host any host any precedence time-range log	配置 deny 类型的 IP 扩展访问列表规则
	ip access-group in out	应用 IP 标准或 IP 扩展访问列表
配置 IPv6 访问列表	⚠ 可选配置。用于匹配过滤 IPv6 报文	
	ipv6 access-list	配置 IPv6 访问列表
	permit host any host any range dscp flow-label fragment time-range log	配置 permit 类型的 IPv6 访问列表规则
	deny host any host any range dscp flow-label fragment time-range log	配置 deny 类型的 IPv6 访问列表规则
	ipv6 traffic-filter in out	应用 IPv6 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。	
	list-remark	在访问列表模式下为访问列表配置注释信息
	access-list list-remark	在全局模式为访问列表配置注释信息。
	remark	在访问列表模式下为规则配置注释信息

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】 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** } {**host** *source* | **any** | *source source-wildcard* } [**time-range** *time-range-name*] [**log**]

【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；

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

log：该选项若被配置，表示本规则如果匹配到了报文需要定时输出匹配日志，有关匹配日志更详细描述请参考本手册的 ACL logging 一节。

【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*] [**log**]

【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

log：该选项若被配置，表示本规则如果匹配到了报文需要定时输出匹配日志，有关匹配日志更详细描述请参考本手册的 ACL logging 一节。

【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：

【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。

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；

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；

host *destination*：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；

precedence *precedence*：该选项若被配置，表示要匹配 IP 报文头部中的优先级域。

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

log：该选项若被配置，表示本规则如果匹配到了报文需要定时输出匹配日志，有关匹配日志更详细描述请参考本手册的 ACL logging 一节。

【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。

【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。

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；

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；

host *destination*：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；

precedence *precedence*：该选项若被配置，表示要匹配 IP 报文头部中的优先级域。

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

log：该选项若被配置，表示本规则如果匹配到了报文需要定时输出匹配日志，有关匹配日志更详细描述请参考本手册的 ACL logging 一节。

【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** | **out** }

【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。

out：该选项若被配置，表示这个访问列表对从该接口发出的 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。

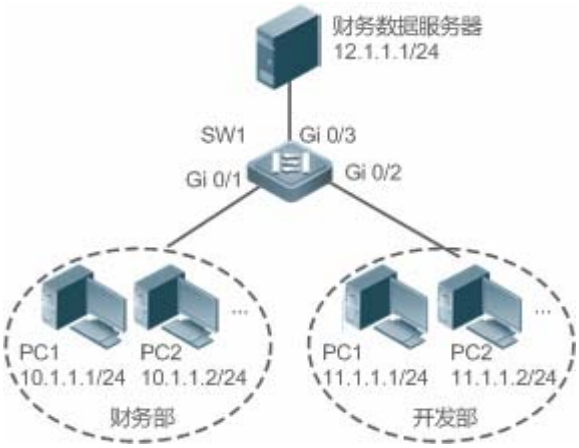
配置举例

以下配置举例，仅介绍与 ACL 相关的配置。

通过 IP 访问列表，禁止财务部以外的部门访问财务数据服务器

【网络环境】

图 1-3



【配置方法】

- 配置 IP 访问列表
- 在 IP 访问列表中添加访问规则
- 将 IP 访问列表应用在连接财务数据服务器接口的出方向上

SW1

```
sw1(config)#ip access-list standard 1
sw1(config-std-nacl)#permit 10.1.1.0 0.0.0.255
sw1(config-std-nacl)#deny 11.1.1.1 0.0.0.255
sw1(config-std-nacl)#exit
sw1(config)#int gigabitEthernet 0/3
sw1(config-if-GigabitEthernet 0/3)#ip access-group 1 out
```

【检验方法】
- 从开发部的某台 PC 机上 ping 财务数据服务器，确认 ping 不通。
- 从财务部的某台 PC 机上 ping 财务数据服务器，确认 ping 得通

SW1

```
sw1(config)#show access-lists

ip access-list standard 1
 10 permit 10.1.1.0 0.0.0.255
 20 deny 11.1.1.0 0.0.0.255

sw1(config)#show access-group
ip access-group 1 out
Applied On interface GigabitEthernet 0/3
```

1.5.2 配置基于时间区的规则

配置效果

如果想让访问列表的某些规则在指定的时间生效，或在指定的时间内失效，比如让 ACL 在一个星期的某些时间段内生效等。可以配置基于时间区的访问列表规则 .

注意事项

无

配置方法

配置访问列表

- 必须配置。要实现基于时间区生效的规则，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。

配置带时间区的访问列表规则

- 必须配置。配置时需要带上对应的时间区选项，时间区的配置请参考时间区相关的配置手册。

应用访问列表

- 必须配置。要使得访问列表规则在指定的时间区内生效，就必须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

在生效时间区内，可以通过 ping 或构造符合规则报文的方式来进行检验规则是否生效来检验；在失效时间区内，可以通过 ping 或构造符合规则报文的方式来进行检验规则是否不生效来检验。

相关命令

配置访问列表

访问列表的配置命令请参考 IP 以及 IPv6 访问列表的相关章节说明。

配置带时间区的访问列表规则

访问列表规则的配置命令请参考 IP 以及 IPv6 访问列表的相关章节说明。

应用访问列表

访问列表规则的应用命令请参考 IP 以及 IPv6 访问列表的相关章节说明。

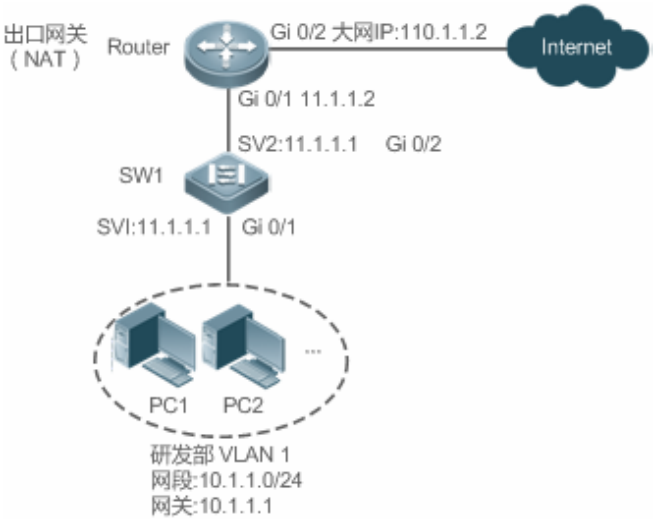
配置举例

以下配置举例，仅介绍与 ACL 相关的配置。

配置基于时间区的访问列表规则，只允许研发部门在每天的 12:00 到 13:30 访问 internet

【网络环境】

图 1-4



【配置方法】

- 配置名称为 access-internet 的时间区，并添加每天 12:00 到 13:30 的时间段表项。
- 配置 IP 访问列表 ip_std_internet_acl。
- 在访问列表中添加允许源 IP 网段为 10.1.1.0/24 的地址规则，关联的时间区为 access-internet。
- 在访问列表中添加禁止源 IP 网段为 10.1.1.0/24 的地址规则。表明时间区之外都不允许访问 internet
- 在访问列表中添加允许所有的地址规则
- 将访问列表应用在设备与出口网关相连接口的出方向上。

SW1

```
Ruijie(config)# time-range access-internet
```

```
Ruijie(config-time-range)# periodic daily 12:00 to 13:30
Ruijie(config-time-range)# exit
sw1(config)# ip access-list standard ip_std_internet_acl
sw1(config-std-nacl)# permit 10.1.1.0 0.0.0.255 time-range access-internet
sw1(config-std-nacl)# deny 10.1.1.0 0.0.0.255
sw1(config-std-nacl)# permit any
sw1(config-std-nacl)# exit
sw1(config)#int gigabitEthernet 0/2
sw1(config-if-GigabitEthernet 0/2)# ip access-group ip_std_internet_acl out
```

【检验方法】

- 在时间区生效期内（12:00 至 13:30），从研发部分内的某台 PC 机访问百度主页，确认可以访问。
- 在时间区失效期（12:00 至 13:30 这个时段外），从研发部分内的某台 PC 机访问百度主页，确认不能访问。

SW1

```
sw1#show time-range

time-range entry: access-internet (inactive)
  periodic Daily 12:00 to 13:30

sw1#show access-lists

ip access-list standard ip_std_internet_acl
 10 permit 10.1.1.0 0.0.0.255 time-range access-internet (inactive)
 20 deny 10.1.1.0 0.0.0.255
 30 permit any

sw1#show access-group
ip access-group ip_std_internet_acl out
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 以及 IPv6 访问列表的相关章节说明。

配置访问列表注释信息

有以下两种方式为访问列表配置注释信息：

【命令格式】 **list-remark** *comment*

【参数说明】 *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】 访问列表模式

【使用指导】 通过该命令为指定的访问列表配置注释信息

【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 以及 IPv6 访问列表的相关章节说明。

配置访问列表规则注释信息

有以下两种方式为访问列表规则配置注释信息：

【命令格式】 **remark** *comment*

【参数说明】 *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】 访问列表模式

【使用指导】 通过该命令为指定的访问列表规则配置注释信息

【命令格式】 **access-list** *acl-id* **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

作用	命令
清除访问列表报文匹配计数	**clear counters access-list** [*acl-id* | *acl-name*]
清除访问列表 deny 报文匹配计数	**clear access-list counters [***acl-id* |*acl-name* **]**

查看运行情况

作用	命令
查看基本访问列表	**show access-lists** [*acl-id* | *acl-ame*] [**summary**]
显示接口上应用的访问列表配置信息。	**show access-group** [**interface** *interface-name*]
显示接口上应用的 IP 访问列表配置信息。	**show ip access-group** [**interface** *interface-name*]
显示接口上应用的 IPv6 访问列表配置信息。	**show ipv6 traffic-filter** [**interface***interface-name*]

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**

2 RPL

2.1 概述

RPL（Reverse Path Limit，反向路径限制）保证报文能够从哪个线路来还从哪个线路回，避免报文被不允许半连接的防火墙等设备过滤。

路由器在建立流表时，可根据首个数据包所流入的端口进行缓存，对同一个数据流中回应的数据包优先匹配流表，并直接从入端口转发回应数据包（不查找路由表或策略路由表）。

锐捷网关产品 RPL 模块支持数据流反向路径限制功能，维护数据流访问安全。

RPL 适用于出口网络维护源进源出的网络访问环境。

协议规范

无

2.2 典型应用

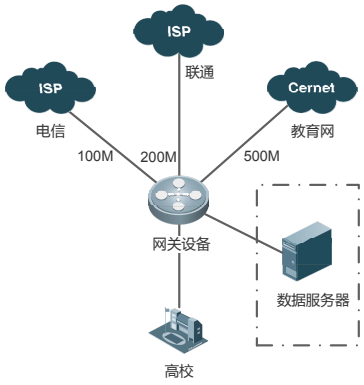
典型应用	场景描述
数据流原路返回	外部网络请求访问高校数据服务器，数据服务器数据答复流沿原路返回

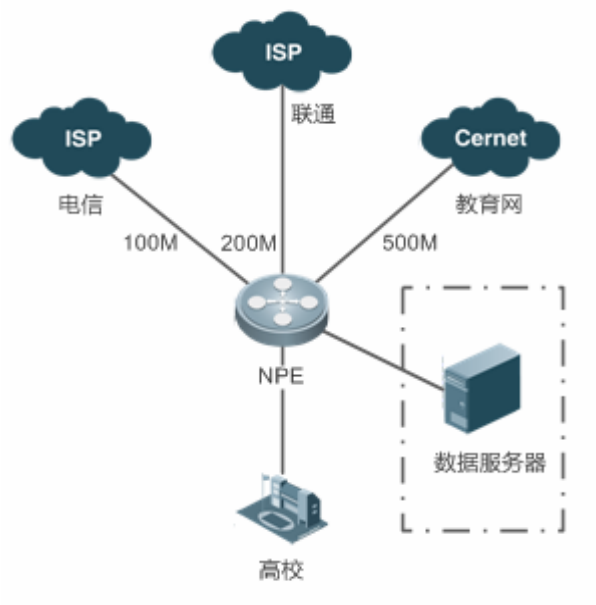
2.2.1 数据流原路返回

应用场景

- 由需要数据流原路返回的接口

图 2-1





【注释】 -

功能部署

- 配置接口开启 RPL 模块功能。

2.3 功能详解

基本概念

↘ 流

流或流会话(session)，即一段时间内一组目的 IP、目的端口、源 IP、源端口、协议号五元组相同的报文。

同一条流有正向流和反向流之分，以首次到达设备的报文方向为正向流，反之为反向流。例如：内网访问发起访问外网资源，外网应答，则从设备上看，正向流为“LAN”-> “WAN” 口，反向流为”WAN”->”LAN”。如果是外网主动访问内网的某个资源，则正向流为“WAN”->”LAN”，反向流为”LAN”->”WAN”。

工作原理

如果在某个接口开启了 RPL 功能，则从该接口收到的”正向流”在建立时，“RPL”功能会记录该正向流的“源接口”和“源 MAC “地址。当反向流到达设备时，“源进源出” 根据先前的记录，将反向流的目的接口改为正向流的 “源接口”，目的 MAC 为正向流的源 MAC 地址，从而不需要查找路由表，实现反向流的路径与正向流一致。

RPL 不区分 LAN 口和 WAN 口。但如果对端有作 VRRP，则取到的 “源 MAC” 可能是一个虚拟 MAC 地址，导致无法正确选路到真实的下一跳，所以 RPL 不支持 VRRP 场景

功能特性

功能特性	作用
RPL 开关	用于开启/关闭 RPL 模块。

2.3.1 RPL开关

RPL 开关用于开启/关闭 RPL 模块。

工作原理

开启 RPL 模块开关，将会对数据流按照原路返回。

关闭 RPL 模块开关，将不会保证数据流按照原路返回。

相关配置

↘ 启动 RPL 模块功能

缺省情况下，锐捷网关设备接口 RPL 模块功能关闭。

接口模式下使用 **reverse-path** 命令开启 RPL 模块功能。

↘ 关闭 RPL 模块功能

缺省情况下，锐捷网关设备接口 RPL 模块功能关闭。

若需要关闭接口 RPL 模块功能，则接口模式下使用 **no reverse-path** 命令。

2.4 配置详解

配置项	配置建议 & 相关命令	
配置 RPL 功能	⚠ 必须配置。配置反向路径限制功能。	
	reverse-path	接口模式下启动 RPL 模块开关

2.4.1 配置RPL功能

配置效果

在接口模式下配置 RPL 功能，使数据流按原路返回。

注意事项

- 要想获得反向流按原路返回的效果，所涉及的接口必须有相对应的路由可以查找(即 show ip route 能够看到这个出口的路由，还能看到下一跳 IP 地址)。

配置方法

↘ 启动 RPL 模块开关功能

- 必须配置，在接口模式下配置。

检验方法

- 无

相关命令

↘ 启动 RPL 模块功能

【命令格式】 **reverse-path**
【参数说明】 -
【命令模式】 接口模式
【使用指导】 -

配置举例

ℹ 以下配置举例，仅介绍与 RPL 模块相关的配置。

↘ 在设备上开启 RPL 功能

【网络环境】 -

【配置方法】 ● 接口模式配置 RPL 功能。

```
Ruijie(config-if-GigabitEthernet 0/1)# reverse-path
```

【检验方法】 查看接口配置信息：

● show running-config interface gigabitEthernet 0/1 查看接口配置信息。

```
Ruijie(config)# show running-config interface gigabitEthernet 0/1
Building configuration...
Current configuration : 73 bytes
!
interface GigabitEthernet 0/1
 duplex auto
 speed auto
 reverse-path
```

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

无

查看调试信息

无

3 REF-RNFP

3.1 概述

RNFP（Ruijie Network Foundation Protection，锐捷网络基础平台保护）是诸多设备抗攻击手段的集合。

当遭受网络攻击或高负荷情况下，RNFP 能够保护路由器控制和管理平面的关键资源，避免设备瘫痪，提高设备的可用性。

协议规范

无

3.2 典型应用

典型应用	场景描述
在网络中存在大量攻击设备的流量	在网络中存在大量异常流量，使得设备 cpu 利用率过高；cli 响应缓慢或停滞；链路或网络控制协议报文丢失，最后导致链路或者网络抖动；处理带宽被非法报文占用，导致重要的协议报文无法得到处理。

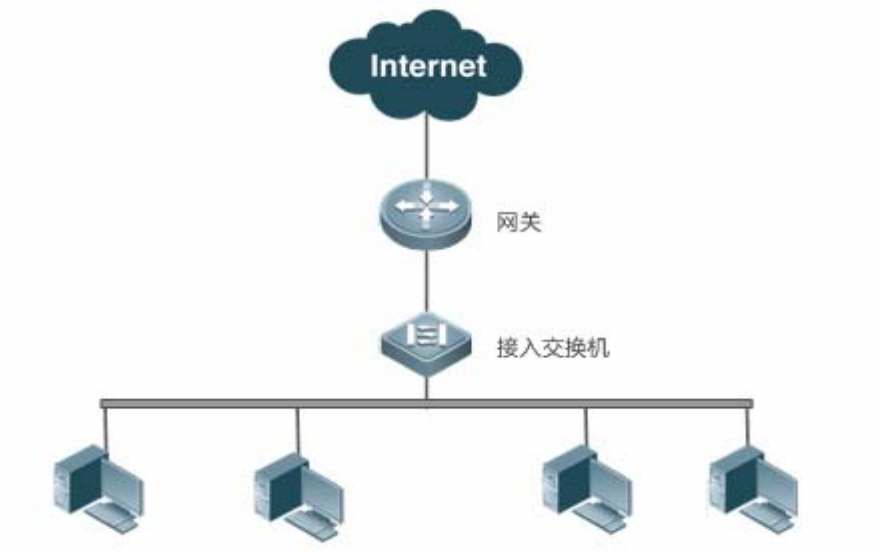
3.2.1 在网络中存在大量攻击设备的流量

应用场景

在存在攻击的网络环境中，降低设备被攻击时的 cpu 使用率，保障关键协议报文，使管理员可以正常访问设备。

- 对攻击流量进行限制。
- 对非攻击流量进行保障。

图 3-1



功能部属

- 在设备上配置对应的本地防攻击限速策略。
- 将管理员的 ip 加入到白名单，使管理员管理设备的流量得到保障。

3.3 功能详解

基本概念

Classify

对上送控制平面的数据流量进行识别和分类。分成协议控制类（protocol），本地管理类(manage)，业务传输类(data)这三类，这样方便后续子模块有区分地进行限速和过滤。

子接口

所有上送控制平面的流量被 Classify 分成三大类，该三大类分别对应如下三个子接口。

- protocol sub-interface：所有送往本地的协议控制流。例如链路层协议的协议报文，路由协议报文等。
- manage sub-interface：所有送往本地的管理协议流。例如 ftp，telnet，snmp 等，另外 arp 也属于这一类。
- data sub-interface：所有快转平面无法处理的数据流都属于这一类。

SCPP

SCPP（Segregate Control Plane Protection）：分类控制平面保护。根据用户定制的策略，针对三个子接口内的流量，匹配不同的 acl 进行更细粒度的限速和保护。

Glean-CAR

Glean-CAR：针对快转平面匹配到 REF Glean 邻接的流量（匹配到直连路由，但没有找到匹配目的 IP 的主机路由，需要上送控制平面来进行目的 ip 的解析）进行限速。

ARP-CAR

ARP-CAR：因为快转平面无法完成 ARP 报文的处理，需要上到控制平面来处理；ARP-CAR 可以限制每个邻居的 ARP 报文速率。

Port-Filter

Port-Filter：针对到本地的 TCP 和 UDP 报文，检查本地应用是否打开了对应的端口，在进入控制平面前就过滤掉发送到本地而本地又未启用的网络服务的流量。

MPP

MPP（Management Plane Protection）：管理平面保护。允许管理员指定一个或多个接口为带内管理接口（既允许接收管理报文，又能转发正常业务的接口）。启用了 MPP 功能以后，只有指定的带内管理接口才允许接收指定协议的管理报文。但业务报文，协议报文，以及 ARP 等报文不受影响。

ACPP

ACPP（Aggregate Control Plane Protection）：集中控制平面保护，针对 classify 的分类结果，应用缺省的或用户定制的速率来分别对 protocol sub-interface，manage sub-interface 和 data sub-interface 上的流量进行限速，确保其流量不会超出控制平面的处理能力，从而保护控制平面。

本地防攻击白名单

当设备受到攻击的时候，用户访问设备就会感觉到卡或者访问不了，通过配置本地防攻击白名单，在白名单中的用户不受到所有防攻击策略的影响，访问设备的报文就不会因为限速而丢弃，也就不会造成访问卡和访问不了的情况。

用户管理设备限制

不通过关联 acl 来实现禁止内/外网 ping 设备，禁止内/外网访问设备的 web 界面，禁止内/外网用户 telnet ssh 设备，禁止内/外网用户使用 snmp 协议管理设备。

arp 攻击检测

在二层环境中，如果内网中存在着 arp 攻击，那么对内网的用户正常上网可能会有影响，本功能就是对网络中可能存在的 arp 攻击进行检测，列出 arp 攻击嫌疑主机，以便管理员排查故障。

设备防攻击中的子接口术语不同于设备中传统意义上的子接口。它仅仅代表了一条传输某一类上送控制层面的流量的内部通路，这样方便针对这些的流量进行防攻击的配置和处理。

设备防攻击的各子功能（SCPP，Glean-CAR，ARP-CAR，Port-Filter，MPP，ACPP）的配置任务之间没有直接关联关系，用户可以根据需要和策略来进行组合和配置。但需要注意的是有的子功能有应用的子接口方面的限制。

功能特性

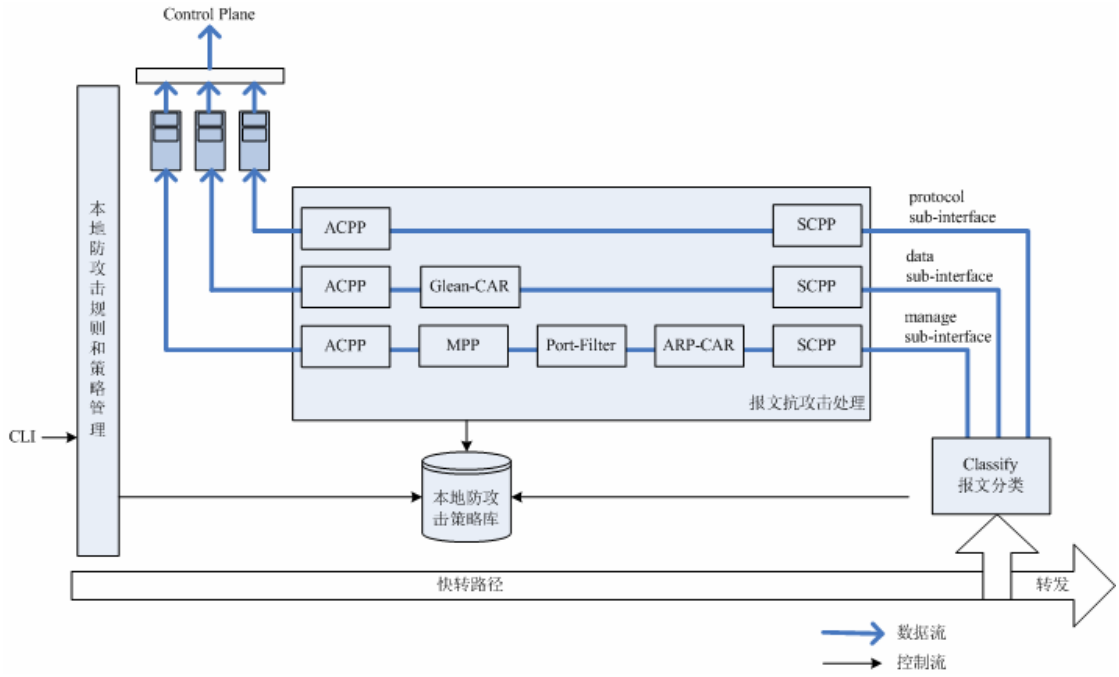
功能特性	作用

本地防攻击	对进入控制层面的报文根据报文类型分到不同的子接口下，进行限速。
攻击检测	对网络中的攻击行为进行检测。
本地防攻击白名单	对白名单的用户本模块不进行限速，确保管理流量。
用户管理设备限制	对内外网 ping 设备，内外网访问设备 web 界面，内外网 telnet-ssh 登录设备，内外网 snmp 管理设备的行为进行禁止。

3.3.1 本地防攻击

通过对需要进入控制层面处理的数据报文进行分类，过滤，限速，从而达到保护控制层面的关键资源的目的。

工作原理



从上图可以看到报文分类限速由众多子模块构成。首先对所有需要进入控制层面处理的报文进行分类，接着针对不同的子接口上不同的策略进行限速。

- **protocol sub-interface**

protocol sub-interface 对所有送往本地的协议控制流量进行限速和过滤。在其下面包含了 2 个子模块 scpp 与 acpp，处理顺序为 scpp->acpp。

- **data sub-interface**

data sub-interface 对所有快转平面无法处理的流进行限速和过滤。在其下面包含了 3 个子模块 scpp，glean-car 和 acpp，处理顺序为 scpp->glean-car->acpp。

- **manage sub-interface**

manage sub-interface 对所有送往本地的管理协议流进行限速和过滤。在其下面包含了 5 个子模块 scpp、arp-car、port-filter、mpp 和 acpp，处理顺序为 scpp->arp-car->port-filter->mpp->acpp。

对于 SCPP 已经允许通过的报文，ARP 报文，GLEAN 报文，这三类报文，ACPP 直接放行不进行流量限速。

相关配置

本地防攻击

缺省情况下，所有限速功能均是关闭的。

使用 **control-plane** [**protocol** | **manage** | **data**]进入到不同的子接口，在不同的子接口下配置不同的功能策略。

使用 **ef-rnfp enable** 开启报文分类限速总开关。

使用 **scpp list** *acl_no* { [**bw-rate** *rate* **bw-burst-rate** *brust-rate*] [**conn-create-rate** *create-rate* **conn-create-burst-rate** *create-burst-rate*] [**conn-total** *num*] } [**log**] 配置 scpp 对匹配 acl 的报文才进行限速，以及调整 SCPP 限速的各项值。

使用 **acpp bw-rate** *rate* **bw-burst-rate** *burst-rate* [**log**]配置 acpp 限速。

使用 **glean-car** *packet_rate_per_group* [**log**]配置 glean-car，对符合 glean-car 的报文进行限速操作。

使用 **port-filter** [**log**]配置 port-filter，禁止接受本地未开放的端口的报文。

使用 **management-interface** *interface* **allow** { **ftp** | **http** | **ssh** | **snmp** | **telnet** | **tftp** } [**log**]配置 management-interface，配置管理接口接收指定的管理协议，非配置接口无法接收这些协议。

使用 **arp-car** *packet_rate_per_group* [**log**] 配置 arp-car，对 arp 报文进行限速。

3.3.2 攻击检测

对网络中存在的攻击行为进行检测以及记录。

工作原理

当各个子接口上的各个子模块所丢弃的报文的总和超过一个阀值的时候，设备就认为网络中存在流量攻击，并对攻击的报文类型，ip 地址，报文总数，报文大小进行统计。

当本设备收到的 arp 报文有异常，那么记录为 arp 攻击嫌疑主机。如下情况列为 arp 欺骗，并加入 arp 欺骗嫌疑列表：主机对整个网络进行 ARP 扫描 (默认在 10s 内发送了超过 200 个 ARP 请求报文)；主机的 MAC 值对应多个 IP；ARP 请求报文企图更新的 MAC 与已存在的 MAC 不同。

相关配置

流量攻击检测

缺省情况下，攻击检测功能是关闭的。当报文分类限速总开关 **ef-rnfp enable** 开启的时候本功能也默认打开。

使用 **attack threshold** *drop-num* 设置攻击判断阀值。默认值为 500。

使用 **show attack** { **current** | **history** }查看攻击信息。

↘ arp 攻击检测

缺省情况下，攻击检测功能是关闭的。

使用 **anti-arp-spoof** 开启 arp 攻击检测。

使用 **anti-arp-spoof** [**scan** *arp-num*]设置 arp 扫描阀值。默认值为 20。

使用 **show arp-suspect** 查看 arp 攻击嫌疑列表。

3.3.3 本地防攻击白名单

当网络中存在攻击的时候，配置管理员 ip 为白名单，管理员可以正常管理设备。

工作原理

在白名单中的 ip，本地防攻击模块不对其进行限速，直接放行。

相关配置

↘ 本地防攻击白名单

缺省情况下，白名单中无任何 ip 信息。

使用 **security web permit** *low-ip-address* [*high-ip-address*]可以配置白名单的范围。最多支持配置 32 个 ip 或 ip 段。

3.3.4 用户管理设备限制

针对目前网络上经常采用 ping，web，telnet，ssh，snmp 攻击的行为，不通过 acl 来分别禁止内外网的 ping 或者 web 访问，更加灵活方便。

工作原理

对 ping 报文，对设备访问的 web 报文进行拦截，对 telnet 或 ssh 登录设备的报文，和对 snmp 管理设备的报文进行拦截。以达到禁 ping，禁 web 访问，禁 telnet-ssh，禁 snmp 的效果。

相关配置

↘ 用户管理设备限制

缺省情况下，功能关闭。

使用 **security deny { lan-ping | lan-web | wan-ping | wan-web | lan-telnet-ssh | lan-snmp | wan-telnet-ssh | wan-snmp }** 可以配置用户管理设备限制功能。

3.4 配置详解

配置项	配置建议 & 相关命令	
配置本地防攻击	⚠ 可选配置，用于配置各个限速规则。	
	control-plane	进入 control-plane 配置模式
	scpp	配置分类控制平面保护
	glean-car	配置 glean 限速
	arp-car	配置 arp 限速
	port-filter	配置端口过滤
	mpp	配置管理平面保护
	acpp	配置集中控制平面保护
	ef-rnfp	配置本地防攻击生效
配置攻击检测	⚠ 可选配置，用于配置攻击检测规则。	
	attack threshold	配置攻击确认阀值
	anti-arp-spoof	配置 arp 攻击检测功能
配置本地防攻击白名单	⚠ 可选配置，用于配置本地防攻击白名单用户。	
	security web permit	配置白名单 ip
用户管理设备限制	⚠ 可选配置，用于配置禁止内外网 ping 设备，访问设备的 web 界面，telnet-ssh 登录设备，snmp 管理设备。	
	security deny	配置禁 ping，禁 web 访问，telnet-ssh 登录设备，snmp 管理设备

3.4.1 配置本地防攻击

配置效果

- 网络中存在攻击时，降低设备的 cpu 利用率。
- 网络中存在攻击时，提高 cli 响应速度。
- 网络中存在攻击时，链路或网络控制协议等重要报文可以得到保障。

注意事项

- 如果在配置本功能后，telnet、web 访问发现缓慢，可以将 ip 加入到本地防攻击白名单中，确保其流量。

配置方法

进入 control-plane 配置模式

- 必选配置。
- 进入不同的子接口。

配置限速

- 必选配置。
- 配置限速，通过配置不同的功能实现限速。

检验方法

- 检查 cpu 利用率高低。
- 检查 cli 响应速度。
- 检查重要协议报文是否有被保障。

相关命令

进入 control-plane 配置模式

【命令格式】 **control-plane** [**protocol** | **manage** | **data**]

【参数说明】 **protocol**：进入协议子接口。

manage：进入管理子接口。

data：进入业务传输类子接口。

不加任何参数的话，配置非子接口的功能。

【命令模式】 全局模式

【使用指导】 -

配置分类控制平面保护

【命令格式】 **scpp list** *acl_no* { [**bw-rate** *rate* **bw-burst-rate** *burst-rate*] [**conn-create-rate** *create-rate* **conn-create-burst-rate** *create-burst-rate*] [**conn-total** *num*] } [**log**]

【参数说明】 **list** *acl_no*：acl 规则，用来选出需要进行 scpp 处理的流量。

bw-rate *rate*：速率限制（单位为 pps）。

bw-burst-rate *burst-rate*：突发速率限制（单位为 pps）。

conn-create-rate *create-rate*：每秒新建连接速率限制。

conn-create-burst-rate *create-burst-rate*：每秒突发新建连接速率限制。

conn-total *num*：总连接数限制。

log：是否输出 log 信息。

【命令模式】 Control-plane 模式。

【使用指导】 三个子接口上都可以针对其上的流量进行 SCPP 处理。

默认情况，SCPP 是关闭的，需要用户显式配置了 SCPP 规则后才会启用。

配置 glean 限速

【命令格式】 **glean-car** *packet_rate_per_group*

【参数说明】 *packet_rate_per_group*：对哈希到同一个组的用户（源）发起的匹配到 Glean 邻接的流量配置限速值，单位为 pps。

【命令模式】 control-plane 模式

【使用指导】 glean-CAR 功能只能配置在 data 子接口上。

目前的哈希算法是取源地址的低 N 位（N 根据产品来决定）。

需要注意的是，Glean-CAR 能够限制哈希到同一个组的用户发起的匹配到 Glean 邻接的流量的速率。如 A（192.168.52.57）和 B（192.168.60.57）这两个用户（哈希结果相同）都向与设备直连的目的主机 C（172.16.0.5）发送流量，当 172.16.0.5 的 ARP 没有解析成功之前，如果配置了 glean-car 5，则 A 和 B 发起的流量中，每秒钟分别最多只有 5 个报文能够被送到控制平面，请求控制平面进行目的 IP 的 ARP 解析。

默认情况，Glean-CAR 是关闭的，需要用户显式配置了 Glean-CAR 规则后才启用。

配置 arp 限速

【命令格式】 **arp-car** *packet_rate_per_group*

【参数说明】 *packet_rate_per_group*：对哈希到同一个组的用户（源）发起的匹配到 ARP 流量配置限速值，单位为 pps。

【命令模式】 control-plane 模式

【使用指导】 ARP-CAR 功能只能配置在 manage 子接口上。

前的哈希算法是取源地址的低 N 位（N 根据产品来决定）。

需要注意的是，ARP-CAR 能够限制哈希到同一个组的用户发起的 ARP 流量的速率。如 A（192.168.52.57）和 B（192.168.60.57）这两个用户（哈希结果相同）都向设备发起 192.168.52.1 的 ARP 请求，如果配置了 arp-car 5，则 A 和 B 发起的流量中，每秒钟分别最多只有 5 个报文能够被送到控制平面，请求控制平面进行 ARP 响应。

默认情况，ARP-CAR 是关闭的，需要用户显式配置了 ARP-CAR 规则后才启用。

配置端口过滤

【命令格式】 **port-filter**

【参数说明】 -

【命令模式】 control-plane 模式

【使用指导】 配置 Port-Filter 来过滤到达本地的未启用服务的传输层报文。

Port-Filter 功能只能配置在 manage 子接口上。

默认情况，Port-Filter 是关闭的，需要用户显式配置了 Port-Filter 后才启用。

配置管理平面保护

【命令格式】 **management-interface** *interface* **allow** { **ftp** | **http** | **ssh** | **snmp** | **telnet** | **tftp** }

【参数说明】 *interface*：指定的带内管理接口。

allow { **ftp** | **http** | **ssh** | **snmp** | **telnet** | **tftp** }：配置允许的管理协议。

【命令模式】 control-plane 模式

【使用指导】 配置 MPP 来指定带内管理接口及该接口上允许接收的管理协议。

MPP 子功能只能配置在 manage 子接口上。

可以最多配置 16 个带内管理接口，每个接口上可以接收多个或全部的管理协议报文。

启用了 MPP 功能以后，非带内管理接口上也不允许接收管理报文，带内管理接口只允许接收指定的管理协议报文。

默认情况，MPP 是关闭的，需要用户显式配置了 MPP 规则后才启用

配置集中控制平面保护

【命令格式】 **acpp bw-rate** *rate* **bw-burst-rate** *burst-rate*

【参数说明】 *rate*：速率限制（单位为 pps）。

burst-rate：突发速率限制（单位为 pps）。

【命令模式】 control-plane 模式

【使用指导】 为已经分类的上控制层面的流量配置 ACPP（集中控制平面保护）。

三个子接口上都可以针对其上的流量进行 ACPP 处理。

默认情况下，ACPP 是关闭的，需要用户显式配置了 ACPP 规则后才启用。

配置本地防攻击生效

【命令格式】 **ef-rnfp** { **enable** | **disable** }

【参数说明】 **enable**：开启本地防攻击功能。

disable：关闭本地防攻击功能。

【命令模式】 control-plane 模式

【使用指导】 当没有配置任何本地防攻击策略的时候，开启开关会自动开启默认策略（每个子接口的 acpp，管理子接口的 port-filter，业务传输类子接口的 glean-car）。默认的防攻击柜子和策略是根据不同的产品和平台来设定的。

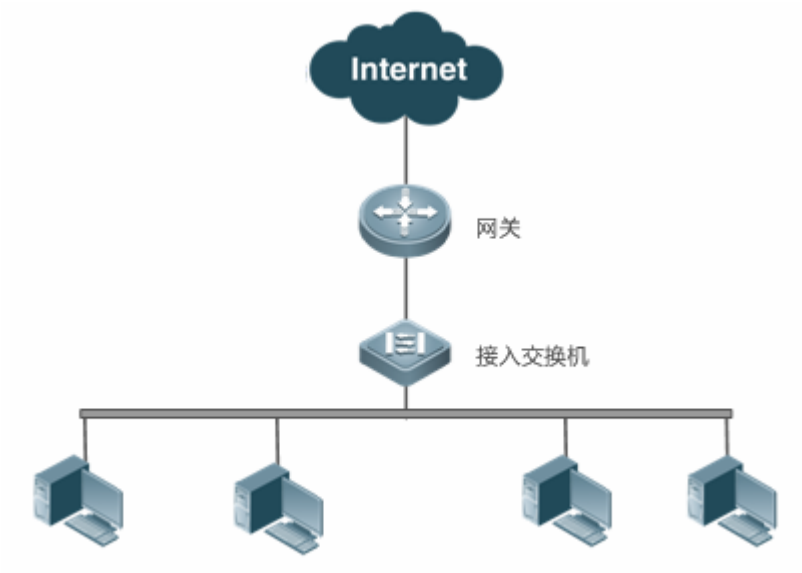
关闭开关后，各个限速功能均不起作用。

配置举例

在网关上配置本地防攻击功能

【网络环境】

图 3-2



【配置方法】

- 在网关上配置本地防攻击限速策略。
- 在 protocol 子接口上配置 ACPP，protocol 上的流量限速为 500pps，允许的突发峰值为 600pps。
- 在 data 子接口上配置 ACPP，data 上的流量限速为 500pps，允许的突发峰值为 600pps。
- 配置 Glean-CAR，对每个源允许每秒 10 个匹配到 glean 邻接的报文。
- 在 manage 子接口上配置 ACPP，manage 上的流量限速为 500pps，允许的突发峰值为 600pps。
- 配置 ARP-CAR，对每个源允许每秒 10 个 ARP 报文。
- 配置 Port-Filter 子功能。
- 配置 MPP 规则，指定 gi0/0 口为带内管理接口，并只允许接收 telnet，snmp 的协议报文。
- 开启本地防攻击全局开关。

A

```
Ruijie # configure terminal
Ruijie(config)# control-plane protocol
Ruijie(config-cp)# acpp bw-rate 500 bw-burst-rate 600
Ruijie(config)# control-plane data
Ruijie(config-cp)# acpp bw-rate 500 bw-burst-rate 600
Ruijie(config-cp)# glean-car 10
Ruijie(config)# control-plane manage
Ruijie(config-cp)# acpp bw-rate 500 bw-burst-rate 600
Ruijie(config-cp)# arp-car 10
Ruijie(config-cp)# port-filter
Ruijie(config-cp)# management-interface gi0/0 allow telnet snmp
Ruijie(config)# control-plane
Ruijie(config-cp)# ef-rnfp enable
```

【检验方法】 使用 show ef-rnfp alll 查看配置信息。

A

```
Ruijie# show ef-rnfp all
Aggregate control plane protection information:
```

```
  Data subinterface: enable
    RULE:
      bandwidth rate limit: 500(pps), burst: 600(pps)
      log: off
    STATISTIC:
      dropped 0 packets
  Manage subinterface: enable
    RULE:
      bandwidth rate limit: 500(pps), burst: 600(pps)
      log: off
    STATISTIC:
      dropped 0 packets
  Protocol subinterface: enable
    RULE:
      bandwidth rate limit: 500(pps), burst: 600(pps)
      log: off
    STATISTIC:
      dropped 0 packets
Segregate control plane protection information:
  Data subinterface: disable
  Manage subinterface: disable
  Protocol subinterface: disable
ARP CAR information:
  Manage subinterface: enable
    RULE:
      allow packet rate per source: 10(pps)
      log: off
    STATISTIC:
      dropped 0 packets
Glean CAR information:
  Data subinterface: enable
    RULE:
      allow packet rate per source: 10(pps)
      log: off
    STATISTIC:
      dropped 0 packets
Port Filter information:
  Manage subinterface: enable
    RULE:
      TCP open port:
        23, 80, 1723, 2650, 4430, 8081,
```

```
      UDP open port:
        67, 68, 161, 514, 3784, 3785, 6000,
        log: off
    STATISTIC:
      dropped 0 tcp packets
      dropped 0 udp packets
Management plane protection information:
  Manage subinterface: enable
    RULE: management interface: GigabitEthernet 0/0, id: 1fa52
      allow:  snmp telnet
      log: off
    STATISTIC:
      dropped 0 disallow management protocol packets
  dropped 0 management protocol packet from non management interface
```

常见错误

- 仅配置某个口为带内管理口导致其他口上无法进行正常管理。

3.4.2 配置攻击检测

配置效果

- 当网络中存在攻击的时候，设备可以检测到，并记录下来。

注意事项

- 必须开启本地防攻击功能。

配置方法

↘ 进入 control-plane 全局模式

- 必选配置。

↘ 配置流量攻击检测阀值

- 必选配置。
- 配置流量攻击检测阀值。

↘ 配置 arp 攻击检测

- 必选配置。
- 配置 arp 攻击检测策略。

检验方法

- 当网络中有流量攻击的时候，设备可以检测到。
- 当网络中有 arp 攻击的时候，设备可以检测到。

相关命令

配置攻击确认阀值

【命令格式】 **attack threshold** *drop-num*

【参数说明】 *drop-num*：当本地防攻击模块丢弃的报文速率达到多少 pps 时，认为网络中存在攻击。

【命令模式】 control-plane 模式

【使用指导】 -

配置 arp 攻击检测功能

【命令格式】 **anti-arp-spoof** [**scan** *arp-num*]

【参数说明】 *arp-num*：10 秒内平均每秒收到的某个 ip 发出的 arp 报文超过这个值那么认为这个 ip 在进行 arp 扫描。
不加任何参数代表开启 arp 攻击检测功能。

【配置模式】 control-plane 模式

【使用指导】 开启 ARP 抗攻击功能，如果用户配置了此命令，将能够识别 ARP 欺骗，将下列情形列为 ARP 欺骗，并加入 ARP 欺骗嫌疑列表：主机对整个网络进行 ARP 扫描（在限定 10s 内发送了超过 200 个 ARP 请求报文）；主机的 MAC 值对应多个 IP；ARP 请求报文企图更新的 MAC 与已存在的 MAC 不同。

配置举例

配置攻击检测。

【配置方法】
- 开启本地防攻击总开关。
- 设置流量攻击阀值。
- 配置 arp 攻击检测

```
Ruijie# configure terminal
Ruijie(config)# control-plane
Ruijie(config-cp)# ef-rnfp enable
Ruijie(config-cp)# attack threshold 500
Ruijie(config-cp)# anti-arp-spoof scan 10
Ruijie(config-cp)# anti-arp-spoof
```

【检验方法】
- 查看流量攻击信息。
- 查看 arp 攻击信息。

```
Ruijie# show ip pim sparse-mode mroute
Ruijie# show attack-info current
System currently not in attack!
Ruijie# show attack-info history
System attack record at 1970-1-2 15:53:18, System in attack 8s
ALL: 6958 packets, 584680 bytes
PROTOCOL          packets         bytes
ARP               1733            103980
UDP               5225            480700
TOP5 IP attack:
IP                packets         bytes             interface
172.18.3.84       2797            257324            Gi0/5
172.18.3.52       2428            223376            Gi0/5
172.18.3.80       1635            98100             Gi0/5
192.168.205.196   92              5520              Gi0/5
3.3.3.6           6               360               Gi0/5
Ruijie#show arp-suspect
IP address      MAC address
192.168.1.1     00d0.f800.0002
```

常见配置错误

- -

3.4.3 配置本地防攻击白名单

配置效果

- 设备再受到攻击的时候白名单用户可以正常的通过 telnet、web 来管理设备。

注意事项

- 仅将管理员 ip 加入到白名单即可。

配置方法

↘ **进入 control-plane 全局模式**

- 必选配置。

配置白名单用户

- 可选配置。

检验方法

模拟网络攻击对设备发起攻击，开启本地防攻击，配置白名单用户。

- 非白名单用户 telnet、访问设备 web 界面很卡或无法连上。
- 白名单用户可以顺畅的 telnet、访问设备的 web 界面。

相关命令

配置防攻击白名单用户

【命令格式】 **security web permit** *low-ip-address* [*high-ip-address*]

【参数说明】 *low-ip-address*：允许的 ip 地址或者允许的 ip 地址范围起始地址。

group-or-source-address：允许地址范围的结束 ip 地址。

【配置模式】 control-plane 模式

【使用指导】 如果用户通过 security deny 配置了禁止访问 web，又想让一些指定 IP 地址可以特许访问 web，用户可以通过此命令在 web permit ip 白名单中添加允许访问的 IP 地址，此命令指定 IP 可以访问 web（不受本地防攻击限速、不受 deny 命令影响）。

配置举例

配置本地防攻击白名单，白名单地址范围（192.168.1.2～192.168.1.10）。

【配置方法】

- 配置白名单用户。

```
Ruijie# configure terminal
Ruijie(config)# control-plane
Ruijie(config-cp)# security web permit 192.168.1.2 192.168.1.10
```

【检验方法】 模拟网络攻击，配置本地防攻击白名单用户。

- 没在本地防攻击白名单中的用户，无法正常 telnet、web 访问设备。
- 在本地防攻击白名单中的用户，可以正常 telnet、web 访问设备。

-

常见配置错误

- 将内网所有的用户都加入到白名单用户，导致如果内网有用户攻击网络的话设备 cpu 利用率等依然会异常。

3.4.4 用户管理设备限制

配置效果

- 配置禁 ping 后，非白名单用户无法 ping 通设备。
- 配置禁 web 访问后，非白名单用户无法访问设备的 web 界面。
- 配置禁 telnet-ssh 访问后，非白名单用户无法使用 telnet 或 ssh 登录设备。
- 配置禁 snmp 管理后，非白名单用户无法使用 snmp 协议管理设备。

注意事项

- 本功能可以和本地防攻击白名单一起配合使用。

配置方法

↘ **进入 control-plane 全局模式**

- 必选配置。

↘ **配置禁内/外网 ping**

- 可选配置。

↘ **配置禁内/外网 web 访问**

- 可选配置。

↘ **配置禁内/外网 telnet-ssh 登录设备**

- 可选配置。

↘ **配置禁内/外网 snmp 管理设备**

- 可选配置。

检验方法

开启内外网禁 ping，禁 web 访问，禁 telnet-ssh 登录，禁 snmp 管理。

- 非白名单用户无法 ping 通设备，无法访问设备的 web 界面，无法 telnet-ssh 登录设备，无法使用 snmp 协议管理设备。
- 白名单用户可以 ping 通设备，可以访问设备的 web 界面，可以使用 telnet-ssh 登录设备，可以使用 snmp 协议管理设备。

相关命令

↘ 配置用户管理设备限制

【命令格式】 **security deny** { **lan-ping** | **lan-web** | **wan-ping** | **wan-web** | **lan-telnet-ssh** | **lan-snmp** | **wan-telnet-ssh** | **wan-snmp** }

【参数说明】 **lan-ping**：禁止用户从 lan 口 ping 设备。

lan-web：禁止用户从 lan 口登录设备的 web 界面。

wan-ping：禁止用户从 wan 口 ping 设备。

wan-web：禁止用户从 wan 口访问设备的 web 界面。

lan-telnet-ssh：禁止用户从 lan 口使用 telnet 或 ssh 访问设备。

lan-snmp：禁止用户从 lan 口使用 snmp 管理设备。

wan-telnet-ssh：禁止用户从 wan 口使用 telnet 或 ssh 访问设备。

wan-snmp：禁止用户从 wan 口 snmp 管理设备。

【命令模式】 control-plane 模式

【使用指导】 配置禁止来自内外网的 ping 和 web 访问 ,如果同时开启而又没配置对应的白名单的话 ,那么需要通过 console 或者 telnet 来进行配置的修改。

配置举例

↘ 配置本地防攻击白名单，白名单地址范围（192.168.1.2～192.168.1.10）。

【配置方法】

- 配置白名单用户。
- 配置禁内/外网禁 ping 设备，内/外网禁 web 访问设备，内/外网禁 telnet/ssh，内/外网禁 snmp 管理。

```
Ruijie# configure terminal
Ruijie(config)# control-plane
Ruijie(config-cp)# security web permit 192.168.1.2 192.168.1.10
Ruijie(config-cp)# security deny wan-ping
Ruijie(config-cp)# security deny wan-web
Ruijie(config-cp)# security deny lan-ping
Ruijie(config-cp)# security deny lan-web
Ruijie(config-cp)# security deny lan-snmp
Ruijie(config-cp)# security deny wan-snmp
Ruijie(config-cp)# security deny lan-telnet-ssh
Ruijie(config-cp)# security deny wan-telnet-ssh
Ruijie(config-cp)#
```

【检验方法】

- 非白名单用户无法 ping 通设备，无法访问设备的 web 界面，无法 telnet-ssh 登录设备，无法使用 snmp 协议管理设备。
- 白名单用户可以 ping 通设备，访问设备的 web 界面，可以使用 telnet-ssh 登录设备，可以使用 snmp 协议管理设备。

常见配置错误

- 禁 ping 和禁 web 访问后，没添加对应的白名单用户，导致无法登陆设备的 web 界面。

3.5 监视与维护

清除各类信息

作用	命令
清除历史攻击信息。	**clear attack-info history**

查看运行情况

作用	命令
查看设备防攻击的配置和统计等信息。	**show ef-rnfp** {**acpp** { **data** | **manage** | **protocol** } | **scpp** { **data** | **manage** | **protocol** } | **glean-car** | **arp-car** | **port-filter** | **mpp** | **all** | **web-permit-ip** | **anti-arp-spoof** }
查看设备当前攻击流量信息。	**show attack-info current**
查看设备历史攻击流量信息。	**show attack-info history**
查看 arp 欺骗嫌疑列表	**show arp-suspect**

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
打开本地防攻击 debug 开关。	**debug** { **acpp** | **scpp** | **glean-car** | **arp-car** | **port-filter** | **mpp** | **all** }
开始记录 debug 信息到 buf。	**show ef-rnfp debug-buf clear**
输出 debug 信息。	**show ef-rnfp debug-buf echo**

4 SSH

4.1 概述

SSH（Secure Shell，安全外壳）连接提供的功能类似于一个 Telnet 连接，与 Telnet 不同的是基于该连接所有的传输都是加密的。当用户通过一个不能保证安全的网络环境远程登录到设备时，SSH 特性可以提供安全的信息保障和强大的认证功能，以保护设备不受诸如 IP 地址欺诈、明文密码截取等攻击。

设备支持 SSH 服务器功能，可以接受多个 SSH 客户端的连接。同时，设备还支持 SSH 客户端功能，允许用户与支持 SSH 服务器功能的设备建立 SSH 连接，从而实现本地设备通过 SSH 安全登录到远程设备上进行管理的功能。

目前，设备作为 SSH 服务器或 SSH 客户端时，支持 SSHv1 和 SSHv2 两个版本。锐捷 SSH 服务同时支持 IPv4 和 IPv6 两种协议。

下文仅介绍 SSH 的相关内容。如无特殊说明，文中的 SSH 均指 SSHv2。

协议规范

- RFC 4251：The Secure Shell (SSH) Protocol Architecture
- RFC 4252：The Secure Shell (SSH) Authentication Protocol
- RFC 4253：The Secure Shell (SSH) Transport Layer Protocol
- RFC 4254：The Secure Shell (SSH) Connection Protocol
- RFC 4419：Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol
- RFC 4716：The Secure Shell (SSH) Public Key File Format
- RFC 4819：Secure Shell Public Key Subsystem
- RFC 3526：More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)
- RFC 2409：The Internet Key Exchange (IKE)
- RFC 1950：ZLIB Compressed Data Format Specification version 3.3
- draft-ietf-secsh-filexfer-05：SSH File Transfer Protocol
- draft-ylonen-ssh-protocol-00：The SSH (Secure Shell) Remote Login Protocol 其协议版本为 1.5，Comware 实现了协议的 Server 功能，没有实现 Client 功能

4.2 典型应用

典型应用	场景描述
SSH 设备管理	用户使用 SSH 对设备进行管理
SSH 本地线路认证	采用本地线路口令认证方式进行 SSH 用户认证

SSH 的 AAA 认证	采用 AAA 认证方式进行 SSH 用户认证
SSH 公钥认证	采用公钥认证方式进行 SSH 用户认证
SSH 文件传输	用户使用客户端的 SCP 命令与 SSH 服务器端进行数据传输

4.2.1 SSH设备管理

应用场景

用户可以使用 SSH 对设备进行管理，前提是必须打开 SSH Server 功能，默认情况下是关闭该功能的。由于 Windows 自带的 Telnet 组件不支持 SSH，因此必须使用第三方客户端软件，当前兼容性较好的客户端包括：Putty，Linux，SecureCRT。下面以客户端软件 Putty 为例介绍 SSH Client 的配置，组网图如下所示。

图 4-1 SSH 设备管理组网图



功能部署

SSH Client 的配置要点如下：

- 打开 Putty 客户端工具软件。
- 在 Putty 中的 Session 选项卡中填写 SSH Server 的主机 IP、SSH 端口号 22 以及连接类型为 SSH。
- 在 Putty 中的 SSH 选项卡中选择 SSH 协议版本号为 2。
- 在 Putty 中的 SSH 选项卡中选择认证方式为“Keyboard-interactive”。
- 点击 open 按钮连接服务器主机。
- 在用户名密码认证窗口输入正确的用户名与密码进入终端登录界面。

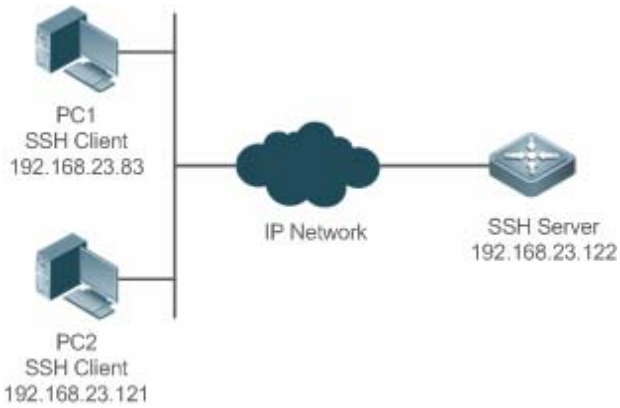
4.2.2 SSH本地线路认证

应用场景

SSH 用户可以采用本地线路口令认证方式进行用户认证，如下图所示。为了保证数据信息交换的安全，PC1、PC2 作为 SSH 客户端，采用 SSH 协议登录到打开 SSH Server 的网络设备上。具体要求如下：

- SSH 用户采用的认证方式为线路口令认证。
- 同时启用 0-4 这五条线路，其中线路 0 的登录口令为“passzero”，其余四条线路的登录口令均为“pass”，用户名任意。

图 4-2 SSH 本地线路口令保护组网图



功能部署

- SSH Server 的配置要点如下：

1. 全局打开 SSH Server。SSH Server 默认支持 SSH1 和 SSH2 两个版本。
2. 配置密钥。通过该密钥，SSH 服务器将从 SSH 客户端收到的口令密文进行解密，将解密后的明文同服务器上保存的口令进行比较，并返回认证成功或失败的消息。SSH 1 使用 RSA 密钥；SSH 2 使用 RSA 或者 DSA 密钥。
3. 配置 SSH 服务器 FastEthernet 0/1 接口的 IP 地址。SSH 客户端通过该地址连接 SSH 服务器。SSH 客户端至 SSH 服务器路由可达。

- SSH Client 的配置要点如下：

SSH 客户端软件有多种，例如 Putty、Linux、OpenSSH 等，本文中仅以客户端软件 Putty 为例，说明 SSH 客户端的配置方法。

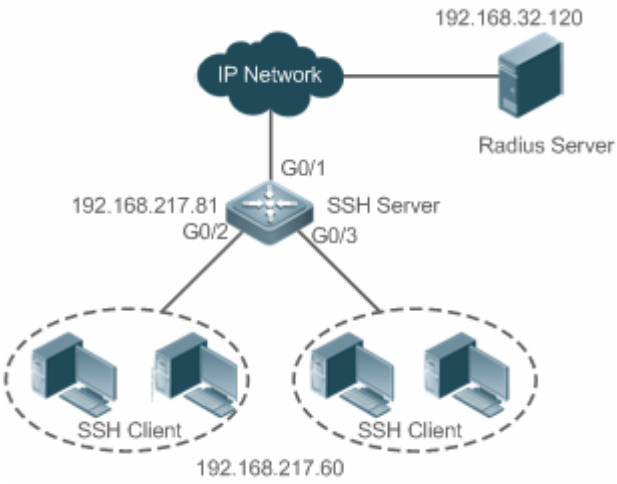
1. 打开 Putty 的连接框，选择使用 SSH1 进行认证登录，使用 SSH2 认证方法类似。
2. 设置 SSH 服务器的 IP 地址与连接端口号，由组网拓扑图可知，服务器主机 IP 为 192.168.23.122，连接端口号为 22，点击 open 按钮进行连接。由于当前认证方式不需要用户名，此处“用户名”可以任意输入，但是不能为空（本例用户名设置为 anyname）。

4.2.3 SSH的AAA认证

应用场景

SSH 用户可以采用 AAA 认证方式进行用户认证，如下图所示。为了保证数据信息交换的安全，PC 作为 SSH 客户端，采用 SSH 协议登录到打开 SSH Server 的网络设备上。为了更好地进行安全管理，SSH 客户端登录用户界面采用 AAA 认证方式；同时出于稳定性方面考虑，在 AAA 认证方法列表中配置两种认证方法：Radius 服务器认证和本地认证。优先选择 Radius 服务器，当 Radius 服务器没有响应时选择本地认证方法。

图 4-3 SSH AAA 认证组网图



功能部署

- SSH 客户端到 SSH 服务器端的路由可达，SSH 服务器到 Radius 服务器端的路由可达。
- 在网络设备上进行 SSH Server 相关配置。
- 在网络设备上进行 AAA 认证相关配置。AAA 通过创建方法列表来定义身份认证、类型，然后将这些方法列表应用于特定的服务或接口上。

4.2.4 SSH公钥认证

应用场景

SSH 用户可以采用 Public-key 认证方式进行用户认证，公钥算法为 RSA 或 DSA，如下图所示。通过配置客户端使用 SSH 协议与服务器端进行安全连接。

图 4-4 SSH 公钥认证组网图



功能部署

- 客户端公钥认证方式，首先要在客户端生成一个密钥对（RSA 或 DSA），然后将其中的公钥放置在 SSH 服务器上，并选择使用 Public-Key 认证方式。
- 在客户端生成了密钥以后，SSH 服务器端需要将客户端的公钥文件复制到 flash 中，并且与 SSH 用户名关联。每个用户可以关联一个 RSA 公钥和一个 DSA 公钥。

4.2.5 SSH文件传输

应用场景

服务器端开启 SCP 服务，客户端通过 SCP 命令与服务器端进行数据传输，如下图所示。

图 4-5 SSH 文件传输组网图



功能部署

- 服务器端开启 SCP 服务。
- 客户端使用 SCP 命令上传文件至服务器端，或从服务器端下载文件。

4.3 功能详解

基本概念

用户认证机制

- password 认证

password 认证是指客户端向服务器发出用户认证请求，并将加密的用户名和密码发送给服务器；服务器将收到信息进行解密，同时将此信息与设备上保存的客户端用户名和密码进行比较，然后返回用户认证成功或失败的消息。

- public-key 认证

public-key 认证是指利用 RSA 或 DSA 等数字签名算法对客户端进行认证。客户端向服务器发送 public-key 认证请求，包括用户名、公钥和公钥算法等信息。服务器收到该信息后先检查公钥的合法性，如果不合法，则直接发送认证失败；否则，服务器对客户端进行数字签名认证，并返回用户认证成功或失败的消息。

public-key 认证仅针对客户端版本为 SSH2.0 的用户。

SSH 的通讯交互

在整个服务器端与客户端的 SSH 通讯交互过程中，为了实现安全通道，需要经历如下七个阶段：

- 建立连接阶段

服务器端在端口 22 监听，等待客户端的连接。当客户端发起 Socket 初始连接请求时，客户端与服务器端建立起了 TCP Socket 连接。

- 版本号协商阶段

如果连接成功，服务器端向客户端发送版本协商报文，客户端收到该报文后进行解析，并向服务端回应客户端决定采用的协议版本号。服务器端将对此信息进行分析，协商版本成功或失败。

- 密钥交换与算法协商阶段

如果版本号协商成功，进入密钥交换与算法协商。服务器端与客户端互相向对端发送算法协商报文，并根据本端支持的算法来确定最终使用的算法。另外，服务器端与客户端利用密钥交换算法、主机密钥等相关信息，生成会话密钥以及会话 ID，利用它们进行后续的用户认证以及数据传输的加解密。

- 用户认证阶段

在加密通道建立起来之后，进入用户认证阶段。客户端向服务器端发送认证请求，服务器端对客户端进行认证，直到认证成功或者认证次数达到设定的上限，服务器端关闭连接为止。

- 会话请求阶段

认证成功后，客户端向服务器端发送会话请求，服务器等待并处理客户端的请求，请求被处理成功之后，SSH 进入会话交互阶段。

- 会话交互阶段

在会话请求成功之后，进入会话交互阶段。加密的数据在双向就可以进行传送并处理。客户端将需要执行的命令发送给服务器端，服务器接收到该命令后进行解密、解析并处理，并将执行的结果进行加密后发给客户端进行解密处理。

- 会话关闭阶段

在服务器端和客户端结束会话时，断开 socket 连接，会话被关闭。

功能特性

功能特性	作用
SSH Server	网络设备上打开 SSH Server，用户可以通过 SSH 客户端安全地连接网络设备。
SCP 服务	开启 SCP 服务后，用户可以直接下载网络设备上的文件，以及将本地文件上传至网络设备，同时所有交互数据以密文形式进行传输，具有认证和安全性等特性。

4.3.1 SSH Server

网络设备上打开 SSH Server，用户可以通过 SSH 客户端安全地连接网络设备；同时，可以关闭 SSH Server，断开全部 SSH 用户的连接。

工作原理

SSH Server 具体工作原理可参考基本概念章节中的“SSH 的通讯交互”小节。在实际以应用中，开启 SSH Server 服务，同时可根据相关应用需求设置以下功能点。

设置版本号：使 SSH Server 支持 SSHv1 与 SSHv2 两种客户端的连接。

设置用户认证超时时间：使 SSH Server 从接受用户连接请求开始计时，存在两种情况：用户认证成功或认证超时断开客户端的连接。

设置用户重认证次数：使 SSH Server 从接受用户连接请求开始进行认证，如果达到重认证次数仍未认证成功，则提示认证失败。

公钥认证：公钥算法为 RSA 或 DSA，在客户端与服务端之间提供安全连接。通过将客户端的公钥文件与用户名进行关联，同时，在客户端配置公钥认证方式，而且指定对应的私钥文件。这样，在客户端登录认证时，即可实施公钥认证进行安全连接。

相关配置

SSH Server 开启

缺省情况下，SSH Server 处于关闭状态。

在全局配置模式下，执行**[no] enable service ssh-server** 命令可以打开或关闭 SSH Server.

同时需要生成 SSH 密钥，使 SSH Server 的状态成为 ENABLE。

设置 SSH Server 支持的版本

缺省情况下，SSH Server 所支持的版本兼容 SSH1 与 SSH2，使用 SSH 1 或者 SSH2 的客户端都可以连接。

使用 **ip ssh version** 命令来配置 SSH Server 所支持的 SSH 连接的协议版本。

如果设置了版本 1 或者 2，只允许对应版本的 SSH 客户端才能够连接。

设置 SSH Server 的用户认证超时时间

缺省情况下，超时时间为 120 秒。

执行 **ip ssh time-out** 命令配置 SSH Server 用户认证的超时时间。执行 **no** 命令可以使超时时间恢复为缺省值。从接受用户连接请求开始计时，当超过指定时间没有认证成功时，则认为认证超时失败。

设置 SSH Server 的重认证次数

缺省情况下，重认证次数为 3 次。

执行 **ip ssh authentication-retries** 命令配置 SSH Server 进行用户认证的重认证次数。执行 **no** 命令可以使重认证次数恢复为缺省值。当超过 SSH Server 配置的重认证次数，仍没有认证成功，则认为用户认证失败。

设置 SSH Server 支持的加密模式

缺省情况下，SSH Server 支持的加密模式为兼容模式（支持 cbc、ctr 和其它类）。

执行 **ip ssh cipher-mode** 命令配置 SSH Server 支持的加密模式。执行 **no** 命令将 SSH Server 支持的加密模式为缺省设置。

设置 SSH Server 支持的消息认证算法

缺省情况下 SSH Server 支持的消息认证算法为：SSHv1 不支持，SSHv2 支持 4 种（MD5、SHA1、SHA1-96、MD5-96）。

执行 **ip ssh hmac-algorithm** 命令配置 SSH Server 支持的消息认证算法。执行 **no** 命令将 SSH Server 支持的消息认证算法恢复为缺省设置。

启动 SSH Server 的公钥认证

执行 **ip ssh peer** 命令开启或取消客户端的公钥文件和用户名关联，客户端登录认证时，通过用户名指定使用的公钥文件。

4.3.2 SCP服务

SSH Server 提供 SCP（Secure Copy，安全复制）服务，用于服务器端与客户端之间文件的安全传输。

工作原理

SCP 协议是一个支持网络文件传输的协议。它运行在 22 端口，基于 BSD RCP 协议；而 RCP 又基于 SSH 协议提供加密和认证。其中，RCP 负责文件的传输，而 SSH 协议负责认证和加密。

在服务器端开启 SCP 服务后，当用户使用 SCP 客户端进行文件上传与下载时，SCP 客户端会先解析命令行参数，然后打开一个到远程服务器的连接，再通过这个连接起另一个 SCP 进程。这个进程的运行方式可以是源模式(source)，也可以是宿模式(sink)，（前者是数据提供者；后者是数据的目的地）。前者读取文件并通过 SSH 连接发送到另一端，后者通过 SSH 连接接收文件。

相关配置

↘ 启动 SCP 服务

缺省不开启 SCP 服务器功能。

执行 **ip scp server enable** 命令在网络设备上打开或关闭 SCP 服务器功能。

4.4 产品说明

NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE 支持 SSH V6 功能；NBR800G、NBR950G、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR108G-P、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1500G、NBR2000G 不支持 SSH V6 功能。

4.5 配置详解

配置项	配置建议 & 相关命令	
配置 SSH Server	⚠ SSH Server 打开功能必须配置。	
	enable service ssh-server	配置 SSH Server 打开功能
	disconnect ssh [**vty**] *session-id*	断开已经建立的 SSH 连接
	crypto key generate { **rsa** | **dsa** }	生成密钥
	ip ssh version { **1** | **2** }	配置 SSH Server 支持版本
	ip ssh time-out *time*	配置 SSH 用户认证超时时间
	ip ssh authentication-retries *retry times*	配置 SSH 重认证次数
	ip ssh cipher-mode { **cbc** | **ctr** | **others** }	配置 SSH Server 支持的加密模式

	ip ssh hmac-algorithm { **md5** | **md5-96** | **sha1** | **sha1-96** }	配置 SSH Server 支持的消息认证算法

4.5.1 配置SSH Server

配置效果

- 在网络设备上打开 SSH Server 功能，用户可以通过 SSH 客户端安全地连接网络设备，同时所有交互信息均以密文形式进行传输，具有认证和安全性等特性。
- 用户可以采用多种认证方式进行 SSH 用户认证，包括：本地线路口令认证、AAA 认证、公钥认证等认证方式。
- 用户可以生成或删除服务器密钥。
- 用户可以配置服务器支持的 SSH 协议版本。
- 用户可以设置认证超时时间。
- 用户可以设置重认证次数。
- 用户可以设置服务器支持的加密模式。
- 用户可以设置服务器支持的消息认证算法。
- 用户可以设置服务器的 ACL 过滤。

注意事项

- 配置设备为 SSH Server，前提是必须保证设备所处网络环境通信正常，管理员能够连接到设备的管理界面进行相应地配置。
- 删除密钥时，不存在命令 **no crypto key generate**；而是通过命令 **crypto key zeroize** 命令删除密钥。
- SSH 模块不支持热备，因此在支持管理板热备份的产品中，管理板切换动作发生后，若新的主板上没有 SSH 密钥文件，则必须通过命令 **crypto key generate** 重新生成密钥后方可使用 SSH。

配置方法

↘ 配置 SSH Server 打开功能

- 必须配置。
- 缺省情况下，SSH Server 处于关闭状态。在全局配置模式下，打开 SSH Server，同时需要生成 SSH 密钥，使 SSH Server 的状态成为 ENABLE。

↘ 配置 SSH Server 支持版本

- 可选配置。

- 缺省情况下，SSH Server 兼容版本 1 和 2，使用 SSH 1 或者 SSH2 的客户端都可以连接。如果设置了版本 1 或者 2，只允许对应版本的 SSH 客户端才能够连接。

配置 SSH 用户认证超时时间

- 可选配置。
- 缺省情况下，SSH Server 的用户认证超时时间为 120 秒。可以根据需要配置用户认证的超时时间，取值范围为 1~120s，单位为秒。

配置 SSH 重认证次数

- 可选配置。
- 设置 SSH 用户请求连接的认证重试次数，防止恶意猜测等非法行为。缺省情况下，SSH Server 的重认证次数为 3 次，即可以允许用户尝试三次输入用户名与密码进行认证尝试。可以根据需要配置用户认证的重认证次数，取值范围为 0~5。

配置 SSH Server 支持的加密模式

- 可选配置。
- 设置 SSH Server 支持的加密模式。缺省情况下，SSH Server 支持的加密模式为兼容模式（支持 cbc、ctr 和其它类）。

配置 SSH Server 支持的消息认证算法

- 可选配置。
- 设置 SSH Server 支持的消息认证算法。缺省情况下，SSH Server 支持的消息认证算法为：SSHv1 不支持，SSHv2 支持 4 种（MD5、SHA1、SHA1-96、MD5-96）。

配置 SSH Server 的 ACL 过滤

- 可选配置。
- 设置 SSH Server 的 ACL 过滤。缺省情况下，SSH Server 的所有连接不进行 ACL 过滤。可以根据需要对 SSH Server 的所有连接进行 ACL 过滤。

配置 SSH 基于公钥的认证

- 可选配置。
- 根据 SSH 协议，只有 SSHv2 才支持基于公钥的认证，SSHv1 不支持。该配置将客户端的公钥文件和用户名关联，客户端登录认证时，通过用户名指定使用的公钥文件。

检验方法

- 使用 **show ip ssh** 命令，可以查看 SSH Server 当前支持的 SSH 协议版本、用户认证的超时时间及重认证次数。
- 通过执行 **show crypto key mypubkey** 命令，查看密钥的公开部分信息是否存在来确认密钥是否已经生成。
- 在 SSH 客户端配置相应的公钥认证登录方式，并指定对应的私钥文件，观察是否可以正常登录。如果可以正常登录，表示客户端的公钥文件与用户名关联成功，公钥认证通过。

相关命令

配置 SSH Server 打开功能

【命令格式】 **enable service ssh-server**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 关闭 SSH Server，需要在全局配置模式下，执行 **no enable service ssh-server** 命令，使 SSH Server 的状态成为 DISABLE。

断开已经建立的 SSH 连接

【命令格式】 **disconnect ssh** [**vty**] *session-id*

【参数说明】 **vty**：已经建立的 vty 连接

session-id：已经建立的 SSH 连接会话号，取值范围为 0~35

【命令模式】 特权用户模式

【使用指导】 通过输入指定的 SSH 连接会话号，断开已经建立的 SSH 连接。或者输入指定的 VTY 连接会话号，断开指定的 SSH 连接。只能断开 SSH 类型的连接。

生成密钥

【命令格式】 **crypto key generate** { **rsa | dsa** }

【参数说明】 **rsa**： 生成 rsa 密钥

dsa：生成 dsa 密钥

【命令模式】 全局模式

【使用指导】 删除密钥时，不存在命令 no crypto key generate；而是通过命令 **crypto key zeroize** 命令删除密钥。

根据SSH协议，SSH 1使用RSA密钥；SSH 2使用RSA或DSA密钥。

如果已生成 RSA 密钥，则 SSH1 与 SSH2 都可用；如果仅生成 DSA 密钥，则仅有 SSH2 可以使用。

配置 SSH Server 支持版本

【命令格式】 **ip ssh version** { **1 | 2** }

【参数说明】 **1**： 配置 SSH Server 仅支持 SSH1 的客户端连接请求

2： 配置 SSH Server 仅支持 SSH2 的客户端连接请求

【命令模式】 全局模式

【使用指导】 **no ip ssh version** 命令恢复 SSH 为缺省配置，支持 SSHv1 与 SSHv2。

配置 SSH 用户认证超时时间

【命令格式】 **ip ssh time-out** *time*

【参数说明】 *time*：配置用户认证的超时时间，取值范围为 1~120s，单位为秒

【命令模式】 全局模式

【使用指导】 **no ip ssh time-out** 命令恢复 SSH 的缺省用户认证超时时间为 120 秒。

配置 SSH 重认证次数

【命令格式】 **ip ssh authentication-retries** *retry times*

【参数说明】 *retry times*： 配置用户认证的重认证次数，取值范围为 0~5

【命令模式】 全局模式

【使用指导】 **no ip ssh authentication-retries** 命令恢复 SSH 的重认证次数为 3 次。

配置 SSH Server 支持的加密模式

【命令格式】 **ip ssh cipher-mode** { **cbc** | **ctr** | **others** }

【参数说明】 **cbc**：配置 SSH Server 支持的加密模式为 cbc 模式（密码分组链接模式：cipher block chaining mode），其对应的加密算法为：DES-CBC、3DES-CBC、AES-128-CBC、AES-192-CBC、AES-256-CBC、Blowfish-CBC

ctr：配置 SSH Server 支持的加密模式为 ctr 模式（计数器模式：counter mode），其对应的算法为：AES128-CTR、AES192-CTR、AES256-CTR

others：配置 SSH Server 支持的加密模式为 others，其对应的加密算法为：RC4

【命令模式】 全局模式

【使用指导】 配置 SSH Server 支持的加密模式。

在锐捷设备当中，SSHv1 Server 支持的加密算法为：DES-CBC、3DES-CBC、Blowfish-CBC；SSHv2 Server 支持的加密算法为：AES128-CTR、AES192-CTR、AES256-CTR、DES-CBC、3DES-CBC、AES-128-CBC、AES-192-CBC、AES-256-CBC、Blowfish-CBC、RC4。在这些加密算法当中，可以归为三类不同的加密模式："cbc"（密码分组链接模式：cipher block chaining mode）、"ctr"（计数器模式：counter mode）和 others（其它类）。

随着密码学的不断发展，"cbc"和"others"加密模式的加密算法，都被证明可以在有限时间内进行破解。所以，在一些安全性要求比较高的组织或单位，可以通过配置 SSH Server 支持的加密模式为"ctr"模式，来提高 SSH Server 的安全级别。

配置 SSH Server 支持的消息认证算法

【命令格式】 **ip ssh hmac-algorithm** { **md5** | **md5-96** | **sha1** | **sha1-96** }

【参数说明】 **md5**：配置 SSH Server 支持的消息认证算法为 md5

md5-96：配置 SSH Server 支持的消息认证算法为 md5-96

sha1：配置 SSH Server 支持的消息认证算法为 sha1

sha1-96：配置 SSH Server 支持的消息认证算法为 sha1-96

【命令模式】 全局模式

【使用指导】 配置 SSH Server 支持的消息认证算法。

在锐捷设备当中，SSHv1 Server 不支持消息认证算法；SSHv2 Server 支持的消息认证算法为：md5、sha1、sha1-96、md5-96。用户可以依据实际需要选择 SSH Server 支持的消息认证算法。

配置 SSH 基于 rsa 公钥的认证

【命令格式】 **ip ssh peer** *test* **public-key rsa flash**:*rsa.pub*

【参数说明】 *test*：用户名

rsa： public-key 类型为 rsa

rsa.pub：公钥文件名

【命令模式】 全局模式

【使用指导】 设置用户 *test* 关联的 RSA 公钥文件。

根据 SSH 协议，只有 SSHv2 才支持基于公钥的认证，SSHv1 不支持。该命令将客户端的公钥文件和用户名关联，客户端登录认证时，通过用户名指定使用的公钥文件。

配置 SSH 基于 dsa 公钥的认证

【命令格式】 **ip ssh peer** *test* **public-key dsa flash**:*dsa.pub*

【参数说明】 *test*：用户名

dsa： public-key 类型为 dsa

dsa.pub：公钥文件名

【命令模式】 全局模式

【使用指导】 设置用户 *test* 关联的 DSA 公钥文件。

根据 SSH 协议，只有 SSHv2 才支持基于公钥的认证，SSHv1 不支持。该命令将客户端的公钥文件和用户名关联，客户端登录认证时，通过用户名指定使用的公钥文件。

配置举例

以下配置举例，仅介绍与 SSH 相关的配置。

生成服务器端的公共密钥

【配置方法】 ● 使用 crypto key generate { rsa | dsa }命令生成服务器公共密钥，以 rsa 为例如下。

SSH Server

```
Ruijie# configure terminal
Ruijie(config)# crypto key generate rsa
Choose the size of the rsa key modulus in the range of 512 to 2048
and the size of the dsa key modulus in the range of 360 to 2048 for your
Signature Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]:
```

● rsa 密钥生成成功提示信息：

```
% Generating 512 bit RSA1 keys ...[ok]
% Generating 512 bit RSA keys ...[ok]
```

● rsa 密钥生成失败提示信息：

```
% Generating 512 bit RSA1 keys ...[fail]
% Generating 512 bit RSA keys ...[fail]
```

【检验方法】 ● 使用 **show crypto key mypubkey rsa** 命令，通过查看 rsa 密钥的公开部分信息是否存在来确认 rsa 是否已经生成。

SSH Server

```
Ruijie(config)#show crypto key mypubkey rsa
% Key pair was generated at: 1:49:47 UTC Jan 4 2013
 Key name: RSA1 private
 Usage: SSH Purpose Key
```

```
Key is not exportable.
Key Data:
        AAAAAwEA AQAAAHJM 6izXt1pp rUSOEGZ/ UhFpRRrW nngP4BU7 mG836apf jajSYwcU
        8O3LojHL ayJ8G4pG 7j4T4ZSf FKgO9kfr 92JpRNHQ gbwaPc5/ 9UnTtX9t qFIKDj1j
        OdKBcCfN trOr/CT+ cs5tlGKV SOICGifz oB+pYaE=

% Key pair was generated at: 1:49:47 UTC Jan 4 2013
Key name: RSA private
Usage: SSH Purpose Key
Key is not exportable.
Key Data:
        AAAAAwEA AQAAAHJf LwKnzOgO F3RlKhTN /7PmQYoE vOa2VXTX 8ZCa7Sll EghLDLJc
        w3T5JQXk Rr3iBD5s b1EeOL4b 21ykZt/u UetQOQ8O sISgIfZ9 8o5No3Zz MPMOLnQR
        G4c7/28+ GOHzYkTk 4IiQuTIL HRgtbyEY XCFaaxU=
```

设置 SSH Server 的版本

【配置方法】 SSH Server

- 使用 **ip ssh version { 1 | 2 }**命令设置 SSH Server 的版本，以只使用版本 2 为例。

```
Ruijie# configure terminal
Ruijie(config)# ip ssh version 2
```

【检验方法】 SSH Server

- 使用 **show ip ssh** 命令，可以查看 SSH Server 当前支持的 SSH 协议版本。

```
Ruijie(config)#show ip ssh
SSH Enable - version 2.0
Authentication timeout: 120 secs
Authentication retries: 3
SSH SCP Server: disabled
```

设置 SSH Server 的用户认证超时时间

【配置方法】 SSH Server

- 使用 **ip ssh time-out** *time* 命令设置用户认证超时时间，以配置 100s 为例。

```
Ruijie# configure terminal
Ruijie(config)# ip ssh time-out 100
```

【检验方法】 SSH Server

- 使用 **show ip ssh** 命令，可以查看 SSH Server 用户认证的超时时间配置信息。

```
Ruijie(config)#show ip ssh
SSH Enable - version 2.0
Authentication timeout: 100 secs
Authentication retries: 3
SSH SCP Server: disabled
```

设置 SSH Server 的用户重认证次数

【配置方法】

- 使用 **ip ssh authentication-retries** *retry times* 命令设置 SSH Server 用户认证的重认证次数 ,以 2 次为

例。

SSH Server

```
Ruijie# configure terminal
Ruijie(config)# ip ssh authentication-retries 2
```

【检验方法】

- 使用 **show ip ssh** 命令，可以查看 SSH Server 用户认证的重认证次数配置信息。

SSH Server

```
Ruijie(config)#show ip ssh
SSH Enable - version 2.0
Authentication timeout: 100 secs
Authentication retries: 3
SSH SCP Server: disabled
```

设置 SSH Server 支持的加密模式

【配置方法】

- 使用 **ip ssh cipher-mode** { **cbc** | **ctr** | **others** }命令来设置 SSH Server 支持的加密模式。以 ctr 加密模式为例，如下：

SSH Server

```
Ruijie# configure terminal
Ruijie(config)# ip ssh cipher-mode ctr
```

【检验方法】

- 在 SSH 客户端也选择 ctr 相关加密模式，观察是否可以正常登录。

设置 SSH Server 支持的消息认证算法

【配置方法】

- 使用 **ip ssh hmac-algorithm** { **md5** | **md5-96** | **sha1** | **sha1-96** }命令来设置 SSH Server 支持的消息认证算法。以 sha1 算法为例，如下：

SSH Server

```
Ruijie# configure terminal
Ruijie(config)# ip ssh hmac-algorithm sha1
```

【检验方法】

- 在 SSH 客户端也选择 sha1 消息认证算法，观察是否可以正常登录。

公钥认证

【配置方法】

- 使用 **ip ssh peer** *username* **public-key** { **rsa** | **dsa** } *filename* 命令 ,将客户端的公钥文件和用户名关联，客户端登录认证时，通过用户名指定使用的公钥文件。以 rsa 为例如下：

SSH Server

```
Ruijie# configure terminal
Ruijie(config)# ip ssh peer test public-key rsa flash:rsa.pub
```

【检验方法】

- 在 SSH 客户端配置相应的公钥认证登录方式，并指定对应的私钥文件，观察是否可以正常登录。如果可以正常登录，表示客户端的公钥文件与用户名关联成功，公钥认证通过。

配置 SSH 设备管理

【网络环境】

图 4-6



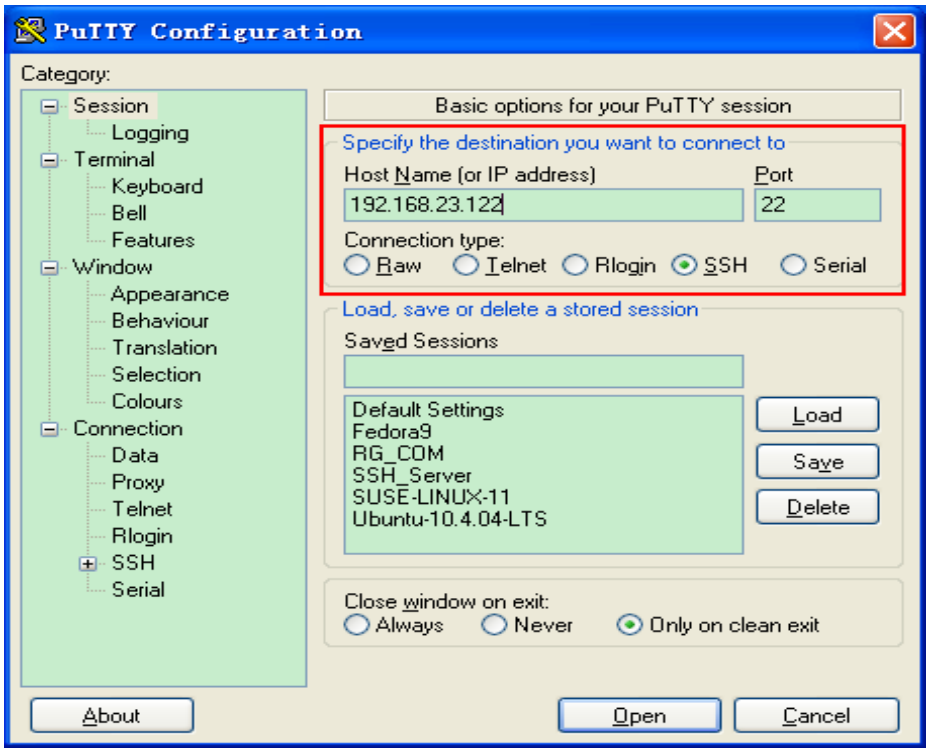
用户可以使用 SSH 对设备进行管理，前提是必须打开 SSH Server 功能，默认情况下是关闭该功能的。由于 Windows 自带的 Telnet 组件不支持 SSH，因此必须使用第三方客户端软件，当前兼容性较好的客户端包括：Putty，Linux，SecureCRT。以客户端软件 Putty 为例介绍 SSH Client 的配置。

【配置方法】

- 打开 Putty 客户端工具软件。
- 在 Putty 中的 Session 选项卡中填写 SSH Server 的主机 IP（192.168.23.122）、SSH 端口号 22 以及连接类型为 SSH。
- 在 Putty 中的 SSH 选项卡中选择 SSH 协议版本号为 2。
- 在 Putty 中的 SSH 选项卡中选择认证方式为“Keyboard-interactive”。
- 点击 open 按钮连接服务器主机。
- 在用户名密码认证窗口输入正确的用户名与密码进入终端登录界面。

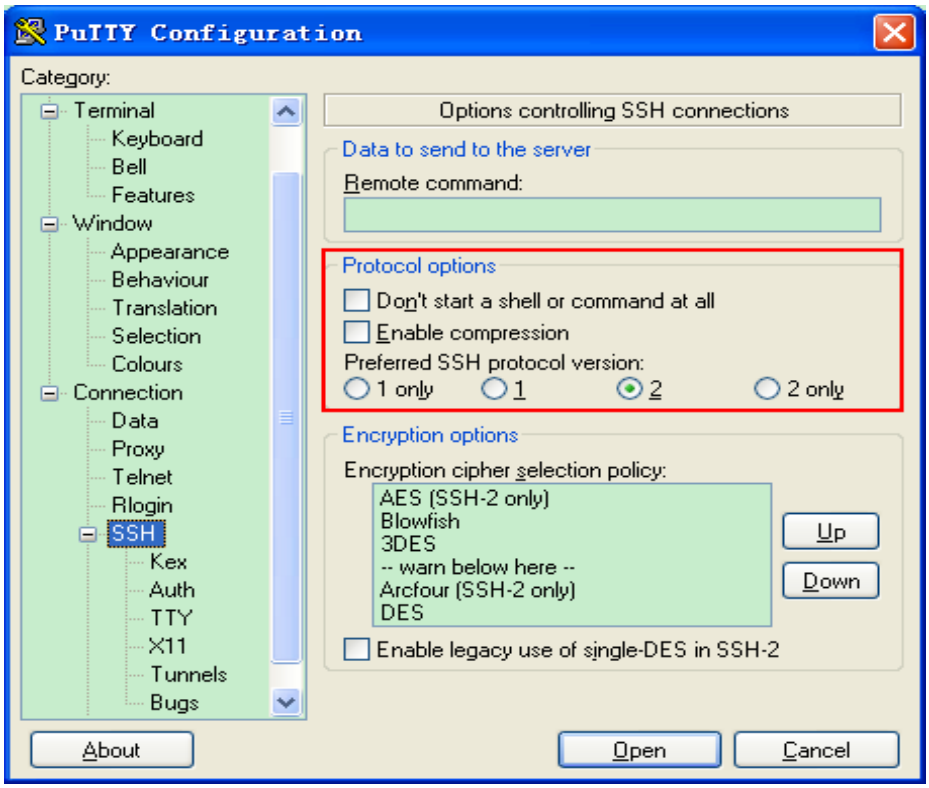
SSH Client

图 4-7



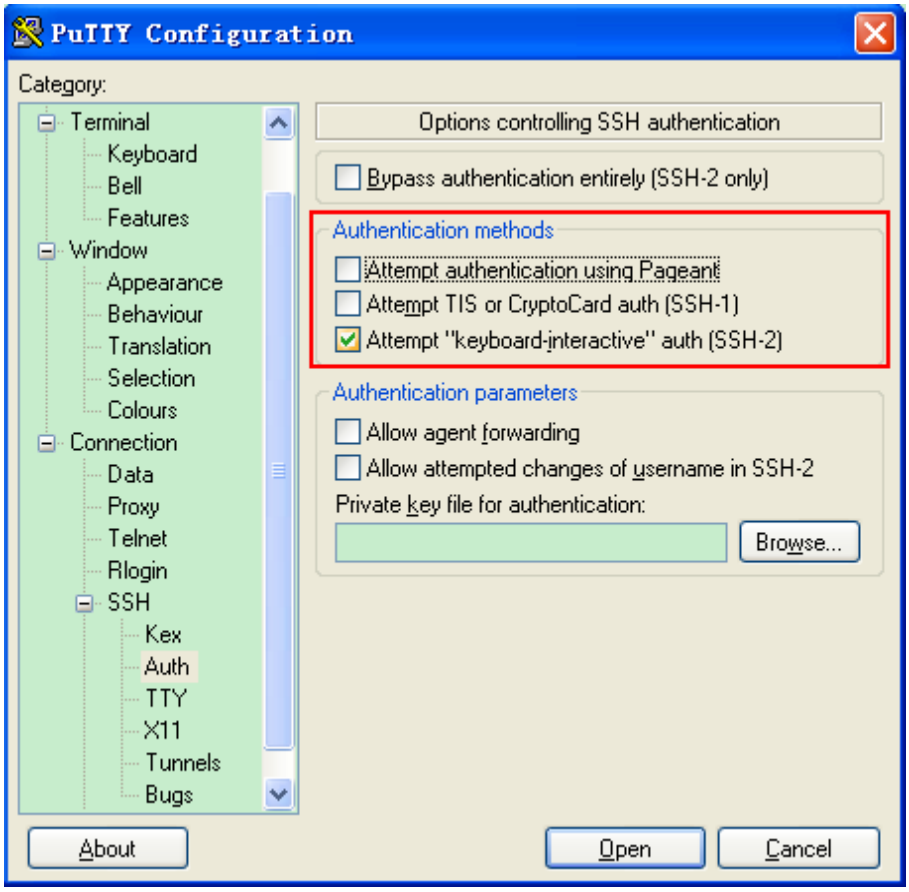
Host Name(or IP address) 就是要登陆的主机的 IP 地址 ,这里为 192.168.23.122。Port 为端口号 22 ,即 SSH 监听的默认端口号。Connection type 为连接类型 SSH。

图 4-8



如上图，使用 SSH 协议 2 进行登陆，因此在 Protocol options 中 Preferred SSH protocol version 选择 2。

图 4-9



如上图，配置 SSH 的认证方式，在 Authentication methods 复选框中，我们选择“keyboard-interactive”，支持用户名密码的认证方式。

然后，点击 open 按钮，连接刚配置的服务器主机，如下图所示：

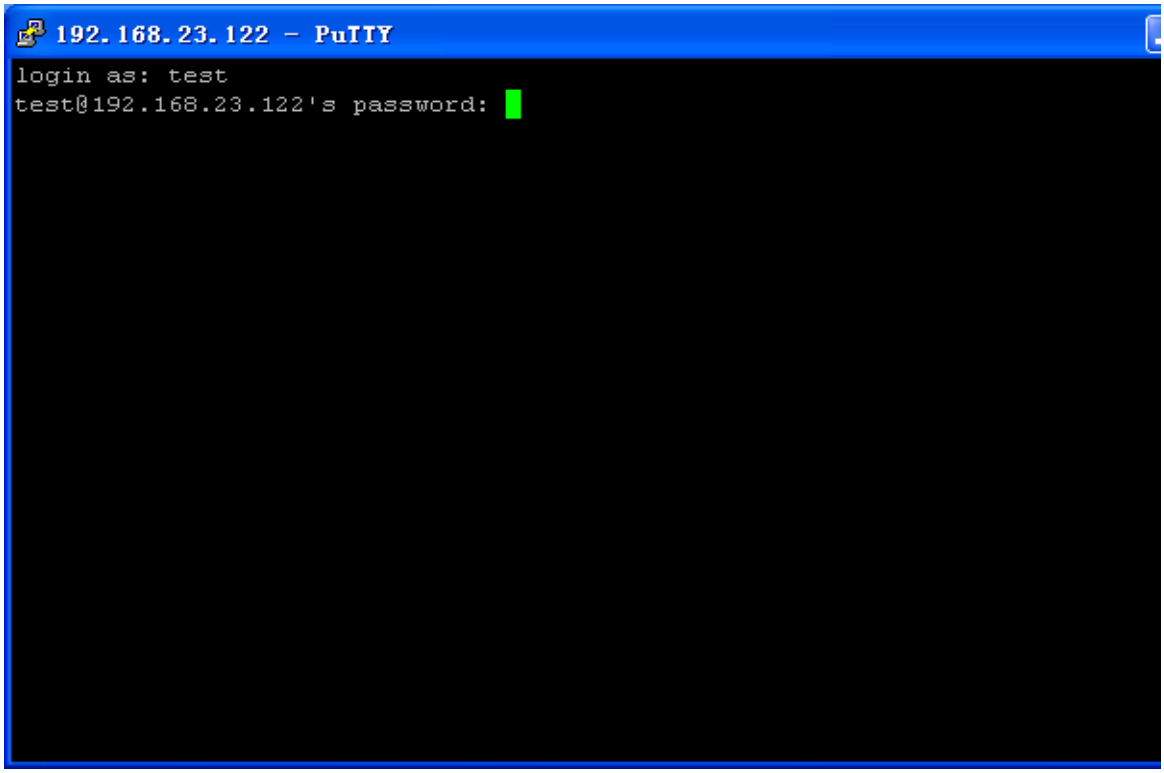
图 4-10



这里询问正在登陆服务器主机 192.168.23.122 的客户端，是否接收服务端发送过来的密钥，选择“是”（接受而且保存），选择“否”（只接受一次），选择“取消”（放弃连接）。

如果选择“是”，接着，会出现下面的用户名密码登录认证对话框，如下图所示：

图 4-11



此时，输入正确的用户名和密码，即可登录 SSH 终端界面，如下图所示：

图 4-12



【检验方法】

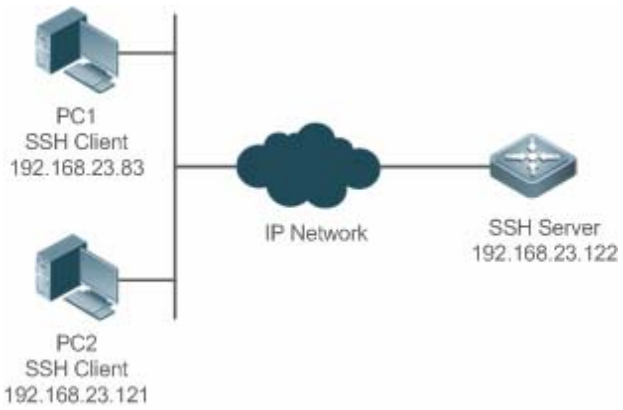
- 通过 **show ip ssh** 命令来显示 SSH Server 当前生效的配置信息。
- 通过 **show ssh** 命令来显示已经建立的 SSH 连接的每个连接信息。

```
Ruijie#show ip ssh
SSH Enable - version 1.99
Authentication timeout: 120 secs
Authentication retries: 3
Ruijie#show ssh
Connection Version Encryption       Hmac         State           Username
         0     2.0 aes256-cbc       hmac-sha1    Session started test
```

配置 SSH 本地线路认证

【网络环境】

图 4-13



SSH 用户可以采用本地线路口令认证方式进行用户认证，如图所示。为了保证数据信息交换的安全，PC1、PC2 作为 SSH 客户端，采用 SSH 协议登录到打开 SSH Server 的网络设备上。具体要求如下：

- SSH 用户采用的认证方式为线路口令认证。
- 同时启用 0-4 这五条线路 ,其中线路 0 的登录口令为“passzero”,其余四条线路的登录口令均为“pass”，用户名任意。

【配置方法】

- SSH Server 的配置要点如下：
- 全局打开 SSH Server。SSH Server 默认支持 SSH1 和 SSH2 两个版本。
- 配置密钥。通过该密钥，SSH 服务器将从 SSH 客户端收到的口令密文进行解密，将解密后的明文同服务器上保存的口令进行比较，并返回认证成功或失败的消息。SSH 1 使用 RSA 密钥；SSH 2 使用 RSA 或者 DSA 密钥。
- 配置 SSH 服务器 FastEthernet 0/1 接口的 IP 地址。SSH 客户端通过该地址连接 SSH 服务器。SSH 客户端至 SSH 服务器路由可达。
- SSH Client 的配置要点如下：
- SSH 客户端软件有多种，例如 Putty、Linux、OpenSSH 等，本文中仅以客户端软件 Putty 为例，说明 SSH 客户端的配置方法。具体配置方法请参见“配置步骤”。

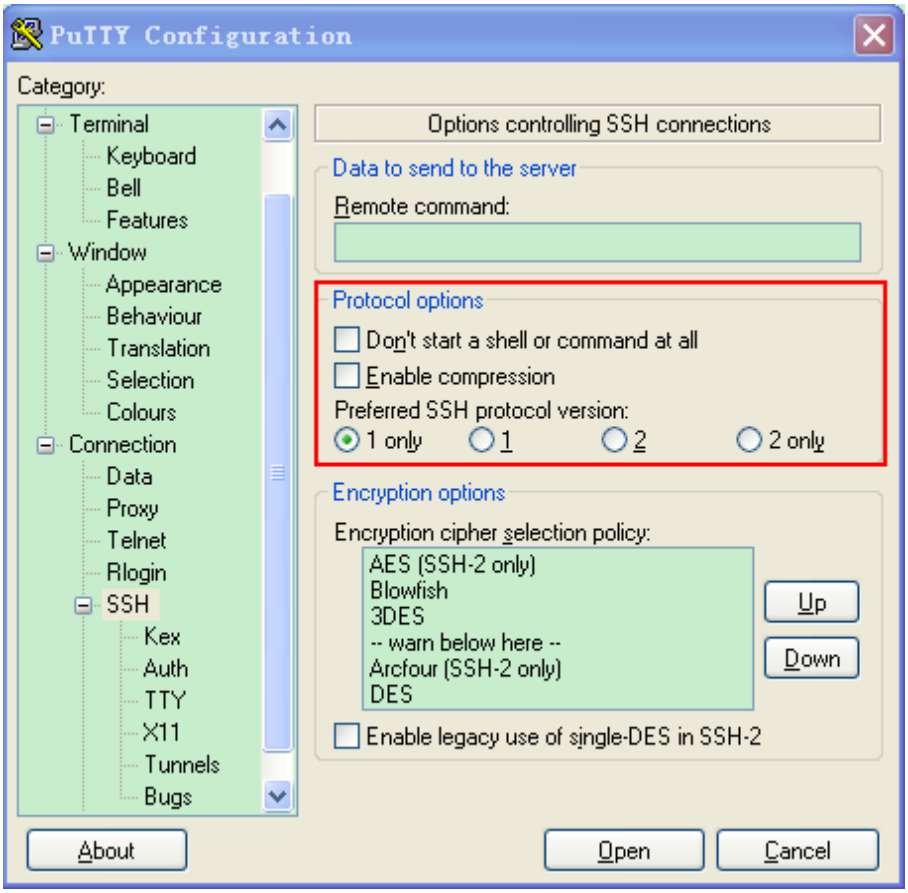
SSH Server

配置 SSH 相关功能之前，请先确保 SSH 用户到 SSH 服务器所在网段的路由可达。接口 IP 配置如拓扑图所示。具体 IP 及路由配置过程此处省略。

```
Ruijie(config)# enable service ssh-server
Ruijie(config)#crypto key generate rsa
% You already have RSA keys.
% Do you really want to replace them? [yes/no]:
Choose the size of the key modulus in the range of 360 to 2048 for your
Signature Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]:
% Generating 512 bit RSA1 keys ...[ok]
% Generating 512 bit RSA keys ...[ok]
Ruijie(config)#interface fastEthernet 0/1
Ruijie(config-if- fastEthernet 0/1)#ip address 192.168.23.122 255.255.255.0
Ruijie(config-if- fastEthernet 0/1)#exit
Ruijie(config)#line vty 0
Ruijie(config-line)#password passzero
Ruijie(config-line)#privilege level 15
Ruijie(config-line)#login
Ruijie(config-line)#exit
Ruijie(config)#line vty 1 4
Ruijie(config-line)#password pass
Ruijie(config-line)#privilege level 15
Ruijie(config-line)#login
Ruijie(config-line)#exit
```

SSH Client（PC1/PC2）

图 4-14



然后，设置 SSH 服务器的 IP 地址与连接端口号，由组网拓扑图可知，服务器主机 IP 为 192.168.23.122，连接端口号为 22（具体设置方式可参考《SSH 设备管理配置举例》），点击 open 按钮进行连接。由于当前认证方式不需要用户名，此处“用户名”可以任意输入，但是不能为空（本例用户名设置为 anyname）。

【检验方法】

- 通过 show running-config 命令来查看当前配置信息的正确性
- 验证 SSH Client 的配置

SSH Server

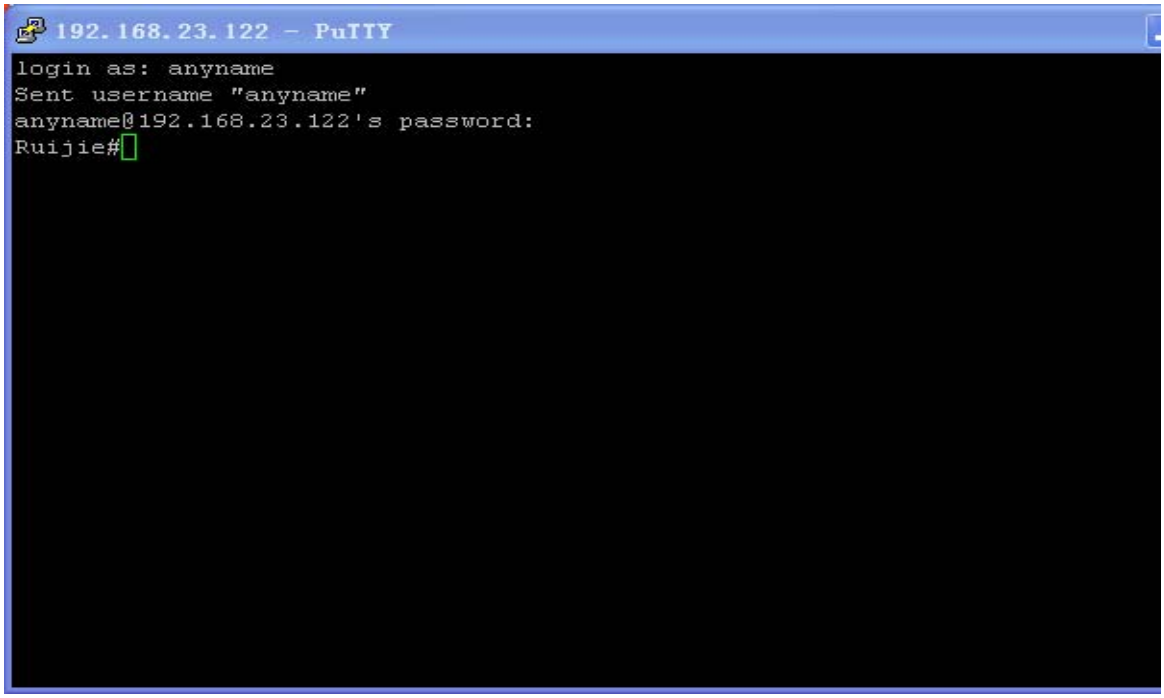
```
Ruijie#show running-config
Building configuration...
!
enable secret 5 $1$eyy2$xs28FDw4s2q0tx97
enable service ssh-server
!
interface fastEthernet 0/1
 ip address 192.168.23.122 255.255.255.0
!
line vty 0
privilege level 15
```

```
 login
 password passzero
line vty 1 4
privilege level 15
 login
 password pass
!
end
```

SSH Client

建立连接，输入正确的口令。线路 0 的登录口令为“passzero”，其余四条线路的登录口令均为“pass”，即可进入 SSH Server 的操作界面。如图所示：

图 4-15

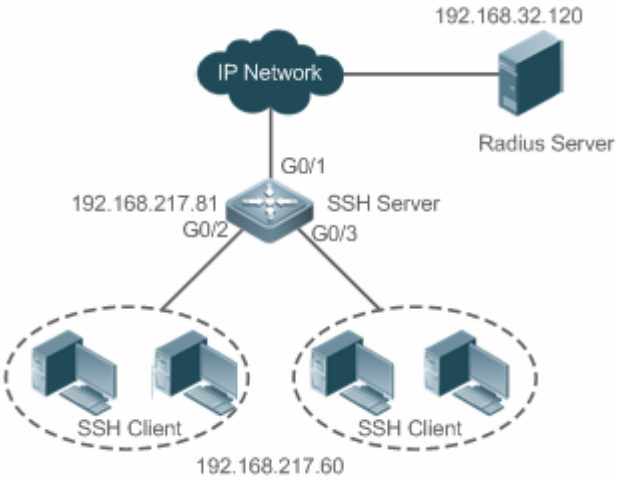



```
Ruijie#show users
Line             User         Host(s)              Idle       Location
---------------- ------------ -------------------- ---------- ------------------
*  0 con 0       ---          idle                 00:00:00   ---
   1 vty 0       ---          idle                 00:08:02   192.168.23.83
   2 vty 1       ---          idle                 00:00:58   192.168.23.121
```

配置 SSH 的 AAA 认证

【网络环境】

图 4-16



SSH 用户可以采用 AAA 认证方式进行用户认证，如图所示。为了保证数据信息交换的安全，PC 作为 SSH 客户端，采用 SSH 协议登录到打开 SSH Server 的网络设备上。为了更好地进行安全管理，SSH 客户端登录用户界面采用 AAA 认证方式；同时出于稳定性方面考虑，在 AAA 认证方法列表中配置两种认证方法：Radius 服务器认证和本地认证。优先选择 Radius 服务器，当 Radius 服务器没有响应时选择本地认证方法。

【配置方法】

- SSH 客户端到 SSH 服务器端的路由可达，SSH 服务器到 Radius 服务器端的路由可达。
- 在网络设备上进行 SSH Server 相关配置。配置要点在上一个例子中已有描述，不再重复说明。
- 在网络设备上进行 AAA 认证相关配置。AAA 通过创建方法列表来定义身份认证、类型，然后将这些方法列表应用于特定的服务或接口上。

SSH Server

```
Ruijie(config)# enable service ssh-server
Ruijie(config)#crypto key generate rsa
% You already have RSA keys.
% Do you really want to replace them? [yes/no]:
Choose the size of the key modulus in the range of 360 to 2048 for your
Signature Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]:
% Generating 512 bit RSA1 keys ...[ok]
% Generating 512 bit RSA keys ...[ok]
Ruijie(config)#crypto key generate dsa
Choose the size of the key modulus in the range of 360 to 2048 for your
Signature Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]:
% Generating 512 bit DSA keys ...[ok]
Ruijie(config)#interface gigabitEthernet 1/1
Ruijie(config-if-gigabitEthernet 1/1)#ip address 192.168.217.81 255.255.255.0
Ruijie(config-if-gigabitEthernet 1/1)#exit
Ruijie#configure terminal
```

```
Ruijie(config)#aaa new-model
Ruijie(config)#radius-server host 192.168.32.120
Ruijie(config)#radius-server key aaaradius
Ruijie(config)#aaa authentication login method group radius local
Ruijie(config)#line vty 0 4
Ruijie(config-line)#login authentication method
Ruijie(config-line)#exit
Ruijie(config)#username user1 privilege 1 password 111
Ruijie(config)#username user2 privilege 10 password 222
Ruijie(config)#username user3 privilege 15 password 333
Ruijie(config)#enable secret w
```

【检验方法】

- 通过 show running-config 命令来查看当前配置信息的正确性
- 在 Radius Server 上的设置。本例以 SAM 服务器为例进行说明。
- 在 PC 机上建立远程 SSH 连接。
- 查看登录用户。

```
Ruijie#show run
aaa new-model
!
aaa authentication login method group radius local
!
username user1 password 111
username user2 password 222
username user2 privilege 10
username user3 password 333
username user3 privilege 15
no service password-encryption
!
radius-server host 192.168.32.120
radius-server key aaaradius
enable secret 5 $1$hbgz$ArCsyqty6yyzzp03
enable service ssh-server
!
interface gigabitEthernet 1/1
 no ip proxy-arp
 ip address 192.168.217.81 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 192.168.217.1
!
line con 0
line vty 0 4
```

```
 login authentication method
!
End
```

【系统管理】-【设备管理】中，添加设备 IP 地址：192.168.217.81，添加设备 Key：aaaradius

【安全管理】-【设备管理权限】中，设置登录用户的权限。

【安全管理】-【设备管理员】中，添加用户名：user；口令：pass。

SSH 客户端软件设置、建立连接；SSH 客户端的创建方法请参见上例。

输入正确的口令，SSH 用户名为：user；口令为：pass。登录成功。

```
Ruijie#show users
    Line         User         Host(s)              Idle       Location
   0 con 0                    idle                 00:00:31
 * 1 vty 0      user          idle                 00:00:33    192.168.217.60
```

配置 SSH 公钥认证

【网络环境】

图 4-17



SSH 用户可以采用 Public-key 认证方式进行用户认证，公钥算法为 RSA 或 DSA，如图所示。通过配置客户端使用 SSH 协议与服务器端进行安全连接。

【配置方法】

- 客户端公钥认证方式，首先要在客户端生成一个密钥对（这里以 RSA 密钥对为例），然后将其中的公钥放置在 SSH 服务器上，并选择使用 Public-Key 认证方式。

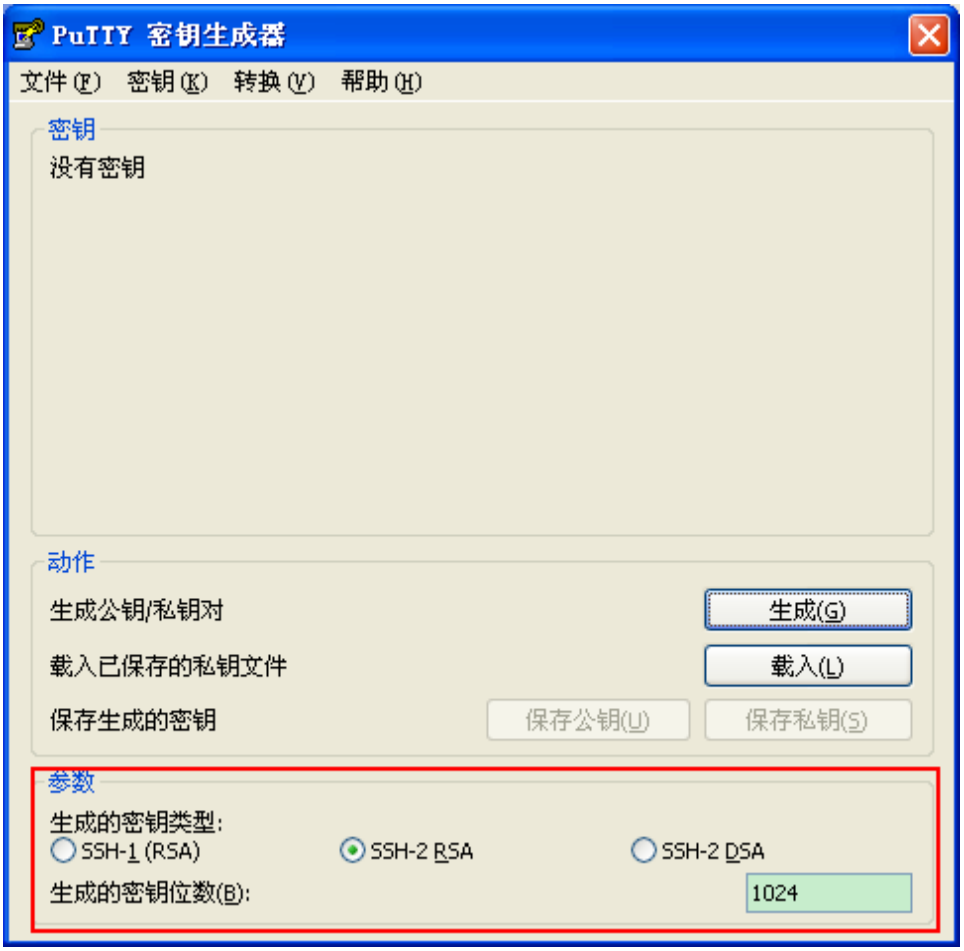
> 在客户端生成密钥对之后，需要将保存的公钥文件上传至服务器端，同时完成服务器的相关配置之后，才可以继续进行客户端的配置以及客户端与服务器端的连接。

- 在客户端生成了密钥以后，SSH 服务器端需要将客户端的公钥文件复制到 flash 中，并且与 SSH 用户名关联。每个用户可以关联一个 RSA 公钥和一个 DSA 公钥。

SSH Client

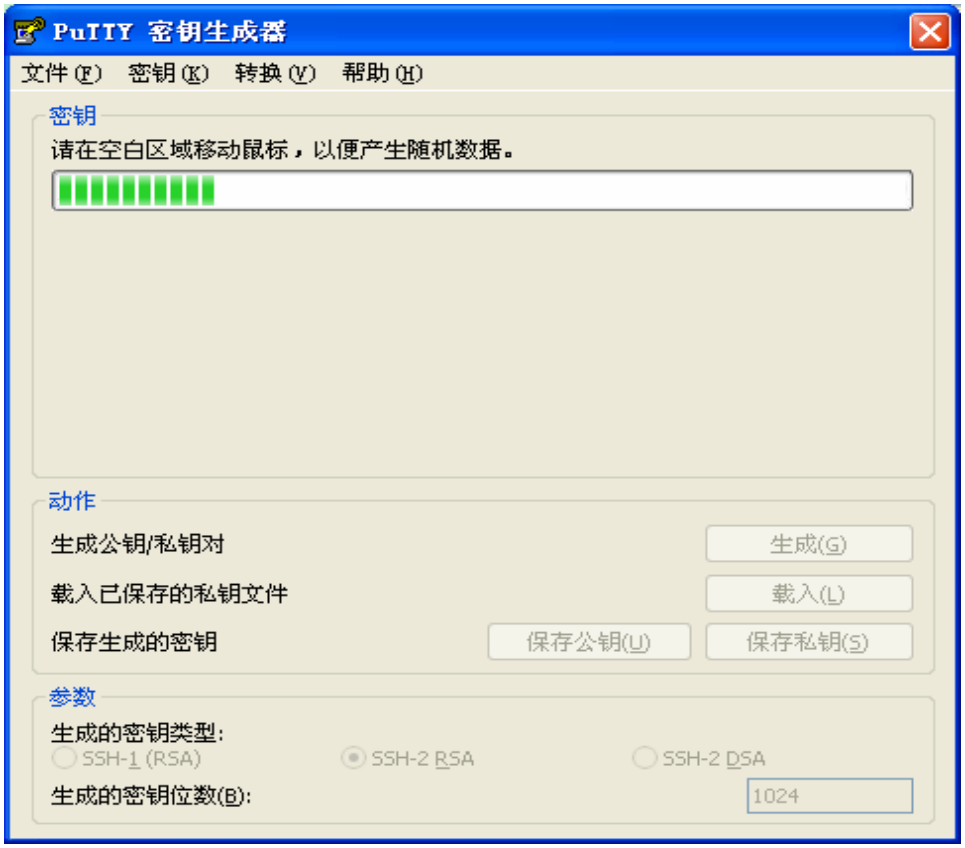
在客户端运行 puttygen.exe 软件，在参数选项栏中选择“SSH-2 RSA”，单击“生成”按钮产生密钥。如下图所示：

图 4-18



生成密钥的时候要除了绿色进度条外的地方不断晃动鼠标，否则进度条显示不动，密钥产生停止，如下图所示：

图 4-19



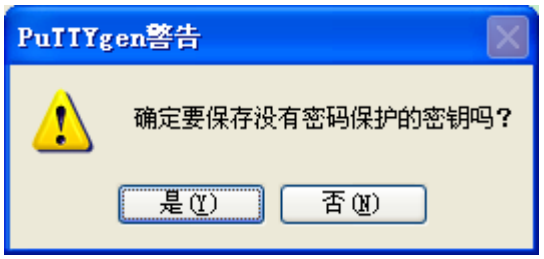
为了保证 RSA 公钥认证的安全性，生成 RSA 密钥对时，RSA 密钥对的长度必须大于或等于 768 位。这里设置为 1024：

图 4-20



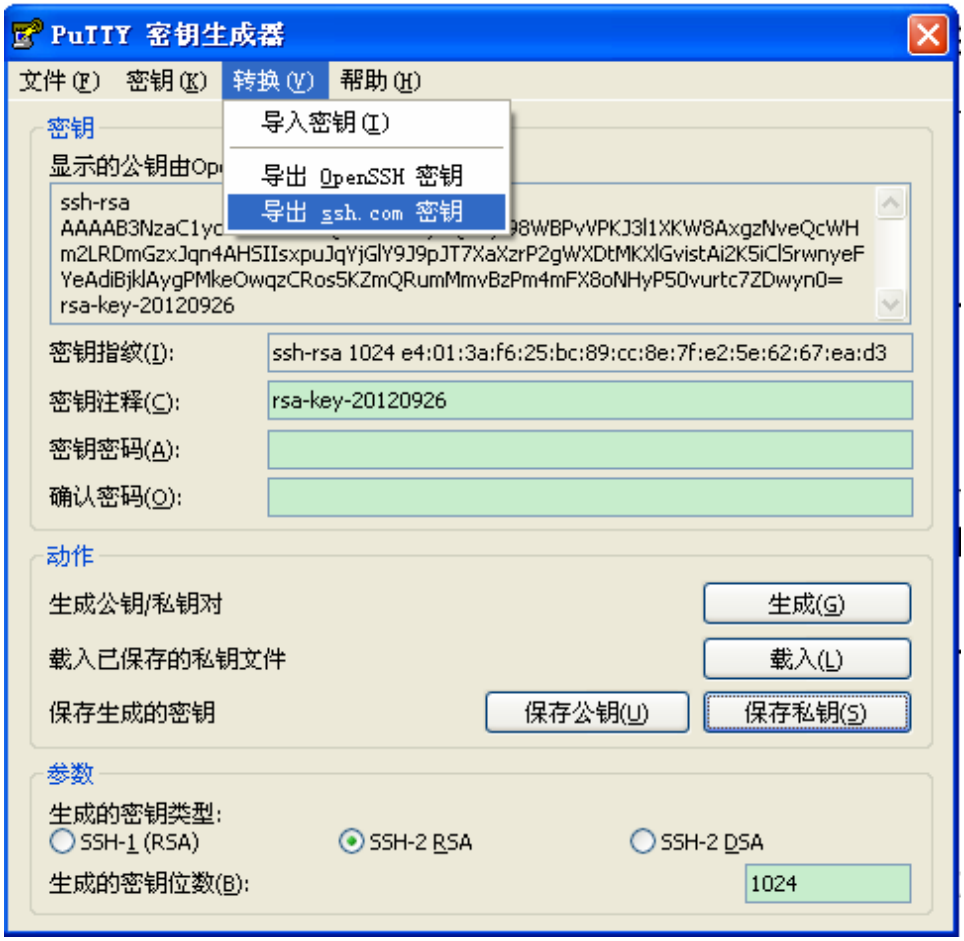
密钥对产生之后，点击“保存公钥”按钮，输入公钥名“test_key.pub”，选择保存路径，点击保存；点击“保存私钥”按钮，弹出如下图所示的警告，选择“是”，输入私钥文件名“test_private”，并点击保存。

图 4-21



一定要选择使用 OpenSSH 格式的密钥文件，否则不能使用。puttygen.exe 能生成 OpenSSH 格式的密钥对，但是 Putty 客户端却不能直接使用，还需要使用 puttygen.exe 工具把私钥转换成 Putty 格式。放在服务器上的公钥文件不需要转换，还是 OpenSSH 格式。如下图所示。

图 4-22



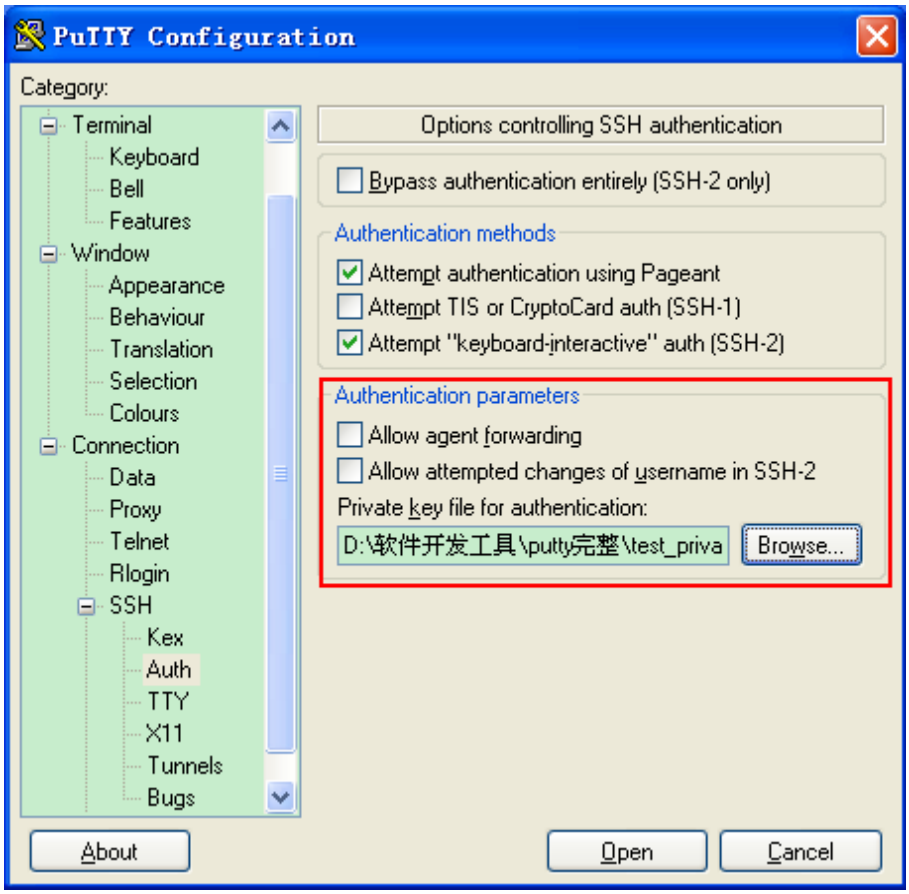
SSH Server

```
Ruijie# configure terminal
Ruijie(config)# ip ssh peer test public-key rsa flash:test_key.pub
```

【检验方法】

- 客户端与服务器端的基本配置完成之后，在 Putty 客户端中指定私钥文件 test_private，并设置服务器主机 IP 为 192.168.23.122，端口号为 22，建立客户端与服务器端的连接，这样，客户端就可以使用公钥认证方式登录网络设备了。

图 4-23



常见错误

- 使用命令 **no crypto key generate** 删除密钥。

4.5.2 配置SCP服务

配置效果

在网络设备上打开 SCP 服务器功能，用户可以直接对网络设备上的文件进行下载，以及将本地文件上传至网络设备，同时所有交互数据以密文形式进行传输，具有认证和安全性等特性。

注意事项

- SSH Server 已经完成配置。

配置方法

配置 SCP 服务功能

- 必须配置。
- 缺省情况下，SCP 功能处于关闭状态。在全局配置模式下，通过 **ip scp server enable** 命令开启 SCP 功能。

检验方法

使用 **show ip ssh** 命令，可以查看 SCP 服务器功能是否打开。

相关命令

配置 SCP 服务功能

【命令格式】 **ip scp server enable**
【参数说明】 -
【命令模式】 全局模式
【使用指导】 该命令打开开启 SCP 服务器功能。
no ip scp server enable 命令关闭 SCP 服务器功能。

配置举例

开启 scp 功能

【配置方法】
- 使用 ip scp server enable 开启 SCP 服务器功能。

```
Ruijie# configure terminal
Ruijie(config)# ip scp server enable
```

【检验方法】
- 使用 **show ip ssh** 命令，可以查看 SCP 服务器功能是否打开。

```
Ruijie(config)#show ip ssh
SSH Enable - version 1.99
Authentication timeout: 120 secs
Authentication retries: 3
SSH SCP Server: enabled
```

配置 SSH 文件传输

【网络环境】
图 4-24



服务器端开启 SCP 服务，客户端通过 SCP 命令与服务器端进行数据传输。

【配置方法】
- 服务器端开启 SCP 服务。

SCP 服务器使用的是 SSH 线程，客户端连接网络设备进行 SCP 传输时候会占用一个 VTY 连接（通过 show user 命令查看的时候，会发现用户类型为 SSH）。

- 客户端使用 SCP 命令上传文件至服务器端，或从服务器端下载文件。

SCP 命令的语法：

```
scp [-1246BCpqrv] [-c cipher] [-F ssh_config] [-i identity_file]
    [-l limit] [-o ssh_option] [-P port] [-S program]
    [[user@]host1:]file1 [...] [[user@]host2:]file2
```

部分选项说明：

-1 ：使用 SSH1 版本（若不指定则默认使用 SSH2）；
-2 ：使用 SSH2 版本（默认）；
-C ：指定使用压缩传输；
-c ：指定使用的加密算法；
-r ：指定传输整个目录；
-i ：指定使用的密钥文件；
-l ：限制传输速度（单位 Kbits）；
其他具体的参数可以查看 scp.0 文件。

选项大部分与客户端有关，少数是客户端和服务器都需要支持的选项，锐捷网络设备上的 SCP 服务器端不支持-d -p -q -r 选项，使用这些选项时候会提示不支持。

SSH Server

```
Ruijie# configure terminal
Ruijie(config)# ip scp server enable
```

【检验方法】

- 文件传输举例，以在 Ubuntu 7.10 系统上操作为例：

指定用户名是 test，从 IP 为 192.168.23.122 的网络设备上，将 config.text 文件复制到本地的/root 目录下。

```
root@dhcpd:~# scp test@192.168.23.122:/config.text /root/config.text
test@192.168.195.188's password:
config.text                   100% 1506     1.5KB/s   00:00
Read from remote host 192.168.195.188: Connection reset by peer
```

常见配置错误

无

4.6 监视与维护

查看运行情况

作用	命令
显示 SSH Server 的当前生效的配置信息	**show ip ssh**

显示已经建立的 SSH 连接的每个连接信息	**show ssh**
显示 SSH Server 公共密钥的公开密钥部分的信息	**show crypto key mypubkey**

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 SSH 基本连接信息的调试开关	**debug ssh**

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。DHCP Snooping 记录生成的用户数据表项可以为 IP Source Guard 等安全应用提供服务。

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。
IP/MAC 欺骗攻击防范	在网络上存在恶意用户，发送伪造的 IP 报文，如篡改了报文的源地址字段。
用户私设 IP 限制	在网络上存在用户，不按规定从 DHCP 服务器获取 IP 地址，私设 IP 地址。
ARP 入侵检测	在网络上存在恶意用户，伪造 ARP 响应报文，意图拦截正常用户之间通信的报文。

5.2.1 DHCP服务欺骗攻击防范

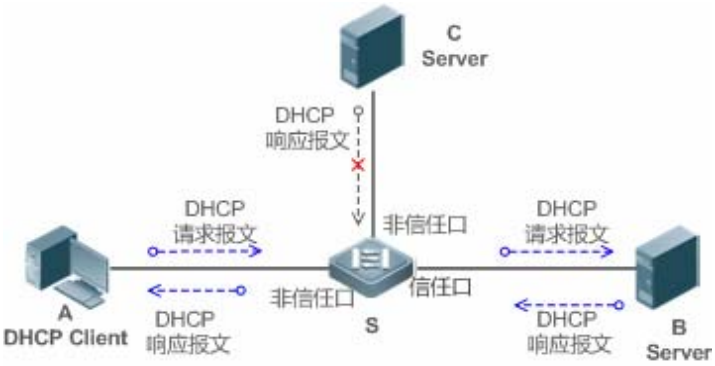
应用场景

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阀值。
- 超出限定的报文被丢弃。
- 开启 DHCP Snooping 与 ARP 模块的联动，删除不存在用户的用户表项。

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。
- 启动与 ARP 模块的联动，检测用户是否在线。

5.2.3 伪造DHCP报文攻击防范

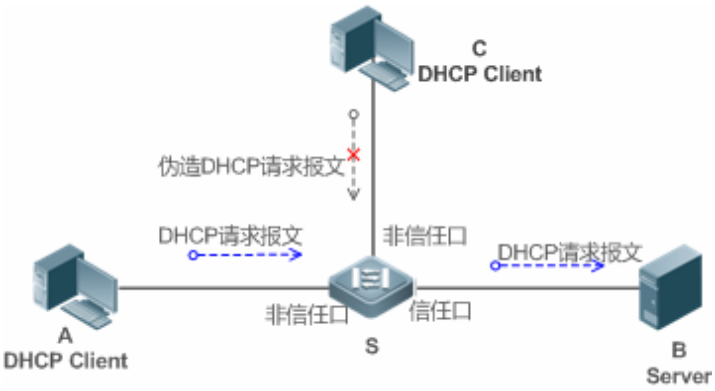
应用场景

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。

5.2.4 IP/MAC欺骗攻击防范

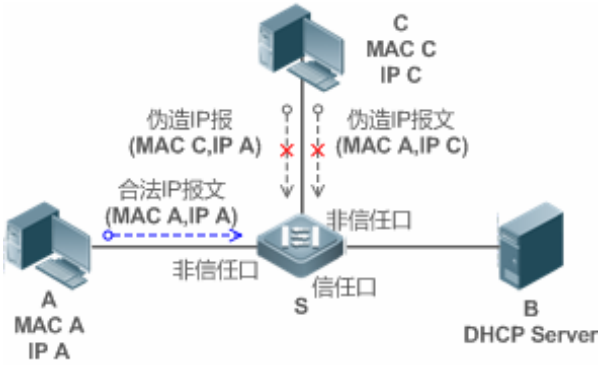
应用场景

检查来自 UNTRUST 口的 IP 报文，可以仅检查 IP 字段，也可以检查 IP+MAC 字段，过滤掉伪造的 IP 报文。

以下图为例，DHCP 客户端发送的 IP 报文将被检查。

- IP 报文的源地址字段必须和 DHCP 分配的 IP 地址匹配。
- 二层报文的源 MAC 字段必须和客户端 DHCP 请求报文中的客户硬件地址匹配。

图 5-3



【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 上所有下行端口为 DHCP UNTRUST 口。
- 在接入设备 S 上，开启 IP Source Gourd 功能，实现 IP 报文过滤。
- 在接入设备 S 上，设置 IP Source Gourd 的匹配模式为 IP+MAC，实现对 IP 报文 MAC 字段与 IP 字段的检查。

5.2.5 用户私设IP限制

应用场景

检查来自 UNTRUST 口的 IP 报文，检查报文源地址是否和 DHCP 分配的地址一致。

若 IP 报文的源地址、连接端口、二层源 MAC 端口，与设备窥探的 DHCP 服务器分配记录不匹配，则丢弃报文。

该场景下设备的工作过程与上图一致。

功能部署

- 同场景“IP/MAC 欺骗攻击防范”。

5.2.6 ARP入侵检测

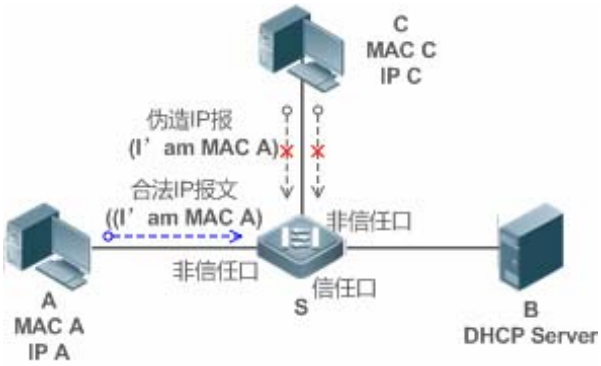
应用场景

检查来自 UNTRUST 口的 ARP 报文，过滤掉与 DHCP 服务器分配记录不匹配的 ARP 报文。

以下图为例，DHCP 客户端发送的 ARP 报文将被检查。

- 接收 ARP 报文的端口、报文的二层 MAC 地址、ARP 报文的发送者硬件地址必须与设备窥探的 DHCP 报文记录一致。

图 5-4



【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 上所有下行端口为 DHCP UNTRUST 口。
- 在接入设备 S 上所有 UNTRUST 口上，开启 IP Source Guard 和 ARP Check 功能，实现 ARP 报文过滤。

⚠ 上述所有安全控制功能仅对 DHCP UNTRUST 口生效。

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 层封装子接口默认均为 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 层封装子接口均为 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。

基于 VLAN 的 DHCP Snooping

DHCP Snooping 功能生效是以 VLAN 为单位的，默认情况下打开 DHCP Snooping 功能，会在当前设备上的所有 VLAN 上使能 DHCP Snooping 功能，可以通过配置灵活的控制 DHCP Snooping 生效的 VLAN。

DHCP Snooping 绑定数据库

在 DHCP 环境的网络里经常会出现用户随意设置静态 IP 地址的问题，用户随意设置的 IP 地址不但使网络难以维护，而且会导致一些合法的使用 DHCP 获取 IP 的用户因为冲突而无法正常使用网络，DHCP Snooping 通过窥探 Client 和 Server 之间交互的报文，把用户获取到的 IP 信息以及用户 MAC、VID、PORT、租约时间等信息组成用户记录表项，从而形成 DHCP Snooping 的用户数据库，配合 ARP 检测功能或 ARP CHECK 功能的使用，进而达到控制用户合法使用 IP 地址的目的。

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。因为其选项编号为 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、DHCPOFFER 等。
- UNTRUST 口收到的带有网关信息【giaddr】的 DHCP request 报文。
- 打开 mac 校验时，源 MAC 与 DHCP 报文携带的【chaddr】字段值为不同的报文。
- DHCPRELEASE 报文中的用户在 DHCP Snooping 绑定数据库中存在，但是 DHCPRELEASE 报文的 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；修改报文的目的端口，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。

↘ 设置 VLAN 上的 DHCP Snooping 功能

缺省情况下，当全局 DHCP Snooping 功能生效时，DHCP Snooping 功能对所有 VLAN 生效。

使用[**no**] **ip dhcp snooping vlan** 命令可以配置 DHCP Snooping 在某个 VLAN 上生效，或将该 VLAN 从 DHCP Snooping 生效的 VLAN 范围中去除。命令参数的取值范围为实际的 VLAN 编号范围。

↘ 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 产品说明

NBR800G、NBR950G、NBR1500G、NBR2000G 不支持 IPv4 Snooping。NBR108G-P、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 IPv4 Snooping。

5.5 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。	
	ip dhcp snooping	启动 DHCP Snooping 功能
	ip dhcp snooping suppression	启动 DHCP 报文抑制功能
	ip dhcp snooping vlan	开关指定 VLAN 的 DHCP Snooping 功能
	ip dhcp snooping verify mac-address	配置 DHCP 源 MAC 检查功能
	ip dhcp snooping database write-delay	启动 DHCP Snooping Binding 记录定时保存功能
	ip dhcp snooping database write-to-flash	手动保存 DHCP Snooping Binding 记录
	renew ip dhcp snooping database	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

5.5.1 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。

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 记录任然能够生效，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。

启动 DHCP Snooping 监控功能

- 可选配置。
- 若需要在路由口上生成 DHCP Snooping 绑定表项，应在三层设备上开启该功能。

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 DHCP Snooping 功能生效的 VLAN

【命令格式】 [**no**] **ip dhcp snooping vlan** { *vlan-rng* | {*vlan-min* [*vlan-max*] } }

【参数说明】 *vlan-rng*：DHCP Snooping 功能生效的 vlan 范围。

vlan-min：DHCP Snooping 功能生效的 vlan 下限。

vlan-max：DHCP Snooping 功能生效的 vlan 上限。

【命令模式】 全局配置模式

【使用指导】 通过配置该命令，将在指定的 VLAN 内打开 DHCP Snooping 功能，也可关闭指定 VLAN 的 DHCP Snooping 功能。该功能必须在打开 DHCP Snooping 全局开关的基础上生效。

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 DHCP Snooping 绑定数据库文件备份

【命令格式】 **ip dhcp snooping database sata0** [interval *time*]

【参数说明】 *time*：两次将 DHCP Snooping 数据库写入备份文件的时间间隔。

不带参数配置时使用默认周期，默认周期为 300 秒。

【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 数据库写入指定备份类型文件。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。

不同备份类型配置切换后，使用切换后的配置方式备份。

配置支持 BOOTP 功能

【命令格式】 [**no**] **ip dhcp snooping bootp**

【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。

配置启动 DHCP Snooping 监控功能

【命令格式】 [**no**] **ip dhcp snooping monitor**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 开启此功能后，DHCP Snooping 通过拷贝 DHCP 报文根据交互过程生成绑定表项，但是不检查报文合法性。

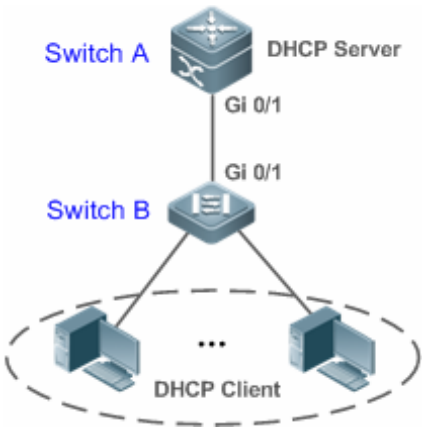
配置举例

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 5-5



【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

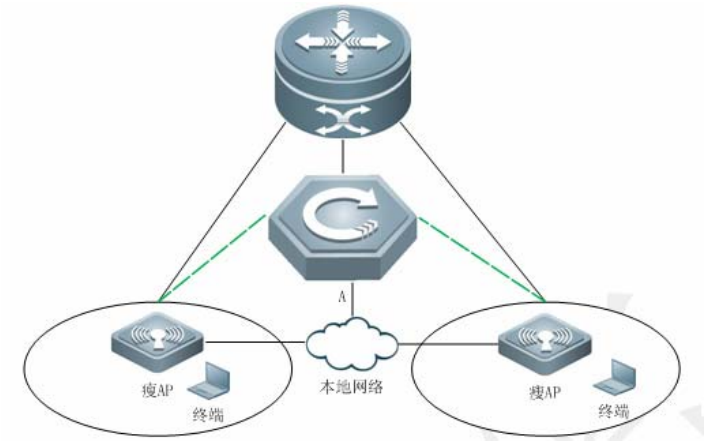
```
B#show running-config
!
ip dhcp snooping
!
interface GigabitEthernet 0/1
B#show ip dhcp snooping
Switch DHCP Snooping status                    :   ENABLE
DHCP Snooping Verification of hwaddr status    :   DISABLE
DHCP Snooping database write-delay time        :   0 seconds
DHCP Snooping option 82 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
```

↘ 下面是无线瘦 AP 本地转发场景下配置 DHCP Snooping 功能

【网络环境】

图 5-6



【配置方法】

- 无线控制器上配置 DHCP Snooping 基本功能

A

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

【检验方法】 查看 DHCP Snooping 配置。

A

```
A#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)
-------------------------    -------         ----------------
Default                      No              unlimited
```

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。

5.5.2 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，做出更佳的地址分配。
- 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 | dot1x-format**]

【参数说明】 **standard-format**：Option82 选项使用标准格式。

dot1x-format：Option82 选项使用 dot1x 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。

使用 dot1x-format 格式时，如果本机有部署 DHCP relay 且与 DHCP Server 连接的上联端口为 SVI 口时，那么 SVI 口所在 VLAN 要关闭 DHCP Snooping 功能。

↘ 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

```
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

5.6 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* | **wlan** *wlan-id*]
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。

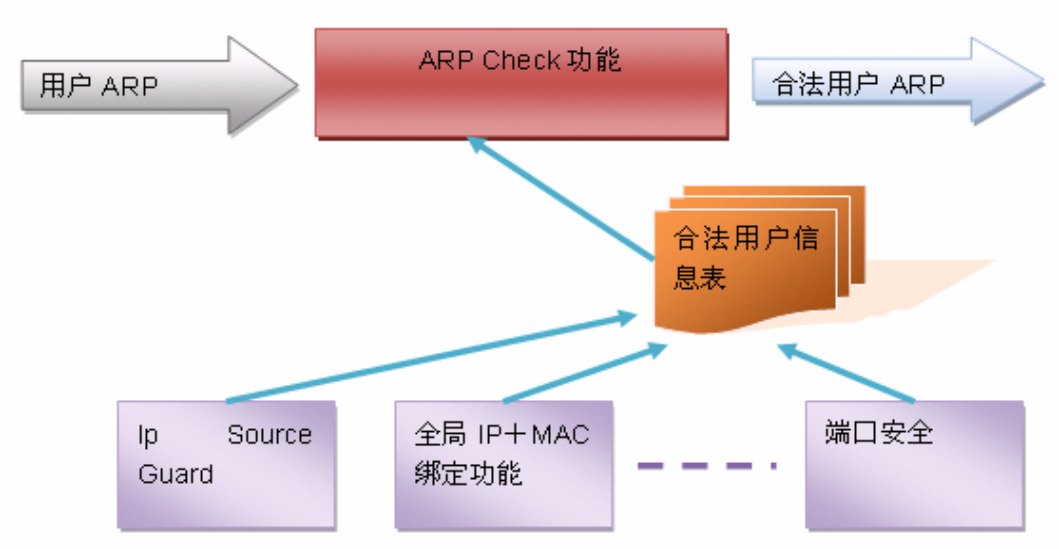
作用	命令
打开 DHCP Snooping 事件的调试开关。	**debug snooping ipv4 event**
关闭 DHCP Snooping 事件的调试开关。	**no debug snooping ipv4 event**
打开 DHCP Snooping 报文的调试开关。	**debug snooping ipv4 packet**
关闭 DHCP Snooping 报文的调试开关。	**no debug snooping ipv4 packet**
打开 DHCP Snooping 基于 MAC 的调试开关	**debug snooping ipv4 mac-address** *H.H.H*
关闭 DHCP Snooping 基于 MAC 的调试开关	**no debug snooping ipv4 mac-address** *H.H.H*
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**

6 ARP Check

6.1 概述

ARP 报文检查（ARP-Check）功能，对端口下（包括有线接入的 2 层交换口、2 层 AP 口或者 2 层封装子接口和无线接入的 WLAN）的所有的 ARP 报文进行过滤，对所有非法的 ARP 报文进行丢弃，能够有效的防止网络中 ARP 欺骗，提高网络的稳定性。在支持 ARP Check 功能的设备中，ARP Check 功能能够根据 IP Source Guard、全局 IP+MAC 绑定、802.1X 认证、GSN 绑定、WEB 认证或者端口安全等安全应用模块所生成的合法用户信息(IP 或 IP+MAC)产生相应的 ARP 过滤信息，从而实现对网络中的非法 ARP 报文的过滤。

图 6-1



如上图所示，设备安全功能模块产生的合法用户信息(仅有 IP 或 IP＋MAC)，ARP Check 功能使用这些信息用于检测端口下的所有的 ARP 报文中的 Sender IP 字段或<Sender IP, Sender MAC>是否满足合法用户信息表中的匹配关系，所有不在合法用户信息表中的 ARP 报文将被丢弃。

下文仅介绍 ARP Check 的相关内容。

协议规范

- RFC826：An Ethernet Address Resolution Protocol or Converting Network Protocol Addresses

6.2 典型应用

典型应用	场景描述
过滤网络上的非法 ARP 报文	网络上存在非法的用户，使用伪造的 ARP 报文进行攻击。

6.2.1 过滤网络上的非法ARP报文

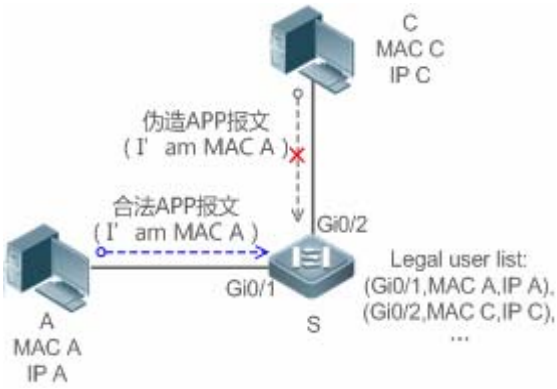
应用场景

检查来自非信任端口的 ARP 报文，过滤掉与 DHCP 服务器分配记录不匹配的 ARP 报文。

以下图为例，DHCP 客户端发送的 ARP 报文将被检查。

- 接收 ARP 报文的端口、ARP 报文的发送者 MAC 地址、ARP 报文的发送者 IP 地址必须与设备窥探的 DHCP 报文记录一致。

图 6-2



【注释】 S 为接入设备。
A、C 为用户 PC。

功能部属

- 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 上所有下行端口为 DHCP 非信任端口。
- 在接入设备 S 上所有非信任端口上，开启 IP Source Guard 与 ARP Check 功能，实现 ARP 报文过滤。

6.3 功能详解

基本概念

↘ ARP Check 支持的安全功能模块

目前 ARP Check 支持的安全功能模块包括：

- 仅检测 IP 字段：端口安全的仅 IP 模式，Ip Source Guard 手工配置的仅 IP 模式。

- 检测 IP+MAC 字段：端口安全的 IP + MAC 绑定模式，全局 IP + MAC 绑定功能，802.1x IP 授权功能，IP Source Guard 功能，GSN 绑定功能，WEB 认证功能。

↘ ARP-Check 两种模式

ARP-Check 有 2 种模式：打开和关闭，默认为关闭。

1. 打开模式

ARP Check 功能根据如下模块提供的 IP/IP+MAC 信息对 ARP 报文的合法性进行检测。

- 全局 IP + MAC 绑定
- 802.1X 的 IP 授权
- IP Source Guard
- GSN 绑定
- 端口安全
- WEB 认证
- 端口安全 IP+Mac 或 IP 绑定

⚠ 如果端口上仅开启 ARP-Check 功能，而没有开启上述模块提供合法用户信息，将导致来自这个端口的所有 ARP 报文被丢弃。

⚠ 当接口开启 arp-check 功能时，如果接口同时启用了 vrrp 功能，对于接口的实地址和虚地址都能当网关，需要配置放行接口实 ip 地址和 vrrp ip 地址，否则可能导致发往网关的 arp 报文被过滤。

2. 关闭模式

不检查端口上的 ARP 报文。

功能特性

功能特性	作用
非法 ARP 报文过滤	检查 ARP 报文的源 IP 与源 MAC 字段，达到过滤非法 ARP 报文的目的。

6.3.1 非法ARP报文过滤

在指定端口上开启 ARP 检查功能，达到过滤非法 ARP 报文的目的。

工作原理

设备把端口下接收到 ARP 报文的源 IP 与源 MAC 字段，与设备安全数据库中的合法用户记录进行匹配。若匹配成功，则正常转发报文；若匹配失败，则丢弃报文。

相关配置

↘ 启动端口上的 ARP Check 功能

缺省情况下，端口上的 ARP Check 功能关闭。

使用 **arp-check** 命令可以启动端口上的 ARP Check 功能。

若无特殊需求，一般在接入设备的端口上设置该功能。

6.4 产品说明

NBR800G、NBR950G、NBR1500G、NBR2000G 不支持 IPv4 Snooping。NBR108G-P、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 IPv4 Snooping。

6.5 配置详解

配置项	配置建议 & 相关命令	
配置 ARP-Check	⚠ 必须配置。用于使能 ARP-Check 服务。	
	arp-check	设置 ARP Check 功能为打开模式

6.5.1 配置ARP-Check

配置效果

- 过滤非法的 ARP 报文。

注意事项

- 打开 ARP Check 检测功能可能会使相关安全应用的策略数/用户数减少。
- 无法在镜像的目的口上配置 arp-check 功能。
- 无法在 DHCP Snooping 信任端口上配置 ARP Check 功能。
- 无法在全局 IP+MAC 的例外口配置 ARP Check 功能。
- 只能在有线的交换口、2 层 AP 口、2 层封装子接口以及无线的 WLAN 下配置开启，有线接入是在接口模式下配置，无线接入是在无线安全配置模式下配置。
- 瘦 AP 的有线接入 ARP Check 功能在 ap-config all 模式下配置开启

配置方法

启动 ARP Check 功能

- 必选配置。功能默认关闭，如果管理员希望使用 ARP Check 功能，需要输入命令开启。

检验方法

- 使用 **show run** 命令，查看功能配置。
- 使用 **show interfaces** { *interface-type interface-number* } **arp-check list** 命令，查看过滤表项。

相关命令

开启 ARP 报文检查

【命令格式】 **arp-check**

【参数说明】 -

【命令模式】 接口配置模式、无线安全配置模式或者无线 ap-config all 配置模式

【使用指导】 根据安全应用模块的合法用户信息产生相应的 ARP 过滤信息，实现对网络中的非法 ARP 报文的过滤。
无线 ap-config all 模式下打开 ARP Check 功能等同于所有 AP 的有线口打开 ARP Check 功能。

配置举例

以下配置举例，仅介绍与 ARP Check 相关的配置。

配置接口 ARP Check 模式为打开模式。

【配置方法】

- 开启 ARP Check 功能，限制 ARP 报文必须符合 IP Source Guard、端口安全或是全局 IP+MAC 绑定的表项。

```
Ruijie# configure terminal
Ruijie(config)#address-bind 192.168.1.3 00D0.F800.0003
Ruijie(config)#address-bind install
Ruijie(config)#ip source binding 00D0.F800.0002 vlan 1 192.168.1.4 interface gigabitEthernet 0/1
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#arp-check
Ruijie(config-if-GigabitEthernet 0/1)#ip verify source port-security
Ruijie(config-if-GigabitEthernet 0/1)#switchport port-security
Ruijie(config-if-GigabitEthernet 0/1)#switchport port-security binding 00D0.F800.0001 vlan 1
192.168.1.1
Ruijie(config-if-GigabitEthernet 0/1)#exit
Ruijie(config)#interface gigabitEthernet 0/4
Ruijie(config-if-GigabitEthernet 0/4)#switchport port-security
Ruijie(config-if-GigabitEthernet 0/4)#switchport port-security binding 192.168.1.5
Ruijie(config-if-GigabitEthernet 0/4)#arp-check
```

```
Ruijie(config-if-GigabitEthernet 0/4)#exit
Ruijie(config)#interface gigabitEthernet 0/5
Ruijie(config-if-GigabitEthernet 0/5)#arp-check
Ruijie(config-if-GigabitEthernet 0/5)#end
Ruijie# configure terminal
Ruijie#conf
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# ip source binding 0026.c79f.6e4c vlan 1 172.168.131.1 wlan 1
```

【检验方法】 使用 **show interfaces arp-check list** 命令，可以查看接口下实际生效的 ARP Check 表项。

```
Ruijie# show interfaces arp-check list

INTERFACE               SENDER MAC           SENDER IP            POLICY SOURCE
----------------------- -------------------- -------------------- --------------------
GigabitEthernet 0/1     00d0.f800.0003       192.168.1.3          address-bind
GigabitEthernet 0/1     00d0.f800.0001       192.168.1.1          port-security
GigabitEthernet 0/1     00d0.f800.0002       192.168.1.4          DHCP snooping
GigabitEthernet 0/4     00d0.f800.0003       192.168.1.3          address-bind
GigabitEthernet 0/4                          192.168.1.5          port-security
GigabitEthernet 0/5     00d0.f800.0003       192.168.1.3          address-bind
```

常见配置错误

- 接口需要检查 ARP 报文，但是将接口的 ARP Check 模式设置为关闭模式，导致功能无法生效。

6.6 监视与维护

清除各类信息

无

查看运行情况

作用	命令
查看端口下实际生效的 ARP Check 表项。	**show interface**s [*interface-type interface-number*] **arp-check list**
查看 WLAN 下实际生效的 ARP Check 表项。	**show wlan** [*wlan-id*] **arp-check list**

查看调试信息

无

7 IP Source Guard

7.1 概述

通过 IP Source Guard 绑定功能，可以通过硬件对 IP 报文进行过滤，从而保证只有 IP 报文硬件过滤数据库中存在对应信息的用户才能正常使用网络，防止了用户私设 IP 地址及伪造 IP 报文。下文仅介绍 IP Source Guard 的相关内容。

协议规范

- 无

7.2 典型应用

典型应用	场景描述
IP/MAC 欺骗攻击防范	在网络环境中，防止用户私设 IP 地址或防止用户伪造 IP 报文进行攻击。

7.2.1 IP/MAC欺骗攻击防范

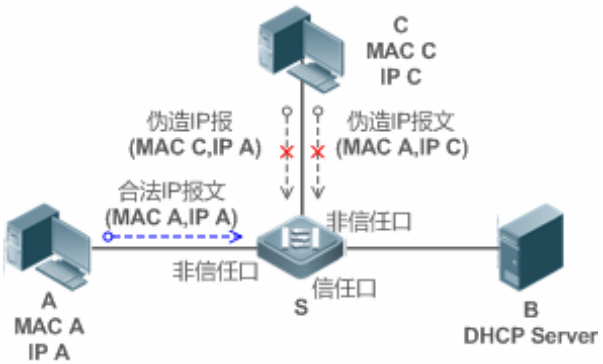
应用场景

检查来自非 DHCP 信任口的 IP 报文，可以仅检查 IP 字段，也可以检查 IP+MAC 字段，过滤掉伪造的 IP 报文。

以下图为例，DHCP 客户端发送的 IP 报文将被检查。

- IP 报文的源地址字段必须和 DHCP 分配的 IP 地址匹配。
- 二层报文的源 MAC 字段必须和客户端 DHCP 请求报文中的客户硬件地址匹配。

图 7-1



【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 上所有下行接口为 DHCP 非信任口。
- 在接入设备 S 上，开启 IP Source Guard 功能，实现 IP 报文过滤。
- 在接入设备 S 上，设置 IP Source Guard 的匹配模式为 IP+MAC，实现对 IP 报文 MAC 字段与 IP 字段的检查。

7.3 功能详解

基本概念

源 IP

用户 IP 报文的源 IP 地址字段。

源 MAC

用户二层报文的源 MAC 地址字段。

基于源 IP 的过滤

IP 报文的过滤策略，检查所有经过该接口的 IP 报文（DHCP 报文除外），仅对报文的源 IP 地址进行检测。IP Source Guard 的缺省过滤策略。

基于源 IP + 源 MAC 的过滤

IP 报文的过滤策略，会对所有 IP 报文的源 IP + 源 MAC 进行检查，仅允许绑定用户记录数据库中存在的用户报文通过。

绑定用户记录数据库

IP Source Guard 安全控制的依据。 目前，绑定用户记录数据库中数据来自两个方面。一方面数据来自 DHCP Snooping 绑定数据库，当启动 IP Source Guard 功能后，DHCP Snooping 数据库信息将同步到 IP Source Guard 的绑定用户数据库中，这样 IP Source Guard 就可以在打开 DHCP Snooping 功能的设备上对客户端的 IP 报文进行严格过滤。另一方面数据来自用户的静态配置。

例外 VLAN

默认情况下端口开启 IP Source Guard 后，会对该端口包含的所有 VLAN 生效，用户可以指定例外 VLAN 不对该 VLAN 范围内的 IP 报文进行检查和过滤，即不受 IP Source Guard 的控制，每个端口最多可以指定 32 个例外 VLAN。

功能特性

功能特性	作用
检查报文源地址字段	对经过接口的 IP 报文进行基于源 IP 过滤，或是基于源 IP + 源 MAC 的过滤。

7.3.1 检查报文源地址字段

对经过端口的 IP 报文进行基于源 IP 过滤，或是基于源 IP + 源 MAC 的过滤。防止恶意用户伪造报文进行攻击。当用户不需要检查和过滤某 VLAN 范围内的 IP 报文时，可以指定例外 VLAN 对报文进行放行。

工作原理

打开 IP Source Guard 功能后，设备对经过端口的报文进行源地址检查，端口可以是有线接入的交换口、2 层 AP 口或者 2 层封装子接口，也可以是无线接入的 WLAN。只有源地址字段和 DHCP Snooping 生成的绑定用户记录集匹配，或是和管理员静态配置的用户集匹配的报文才能经过端口。匹配的方式有两种：

基于源 IP 地址过滤

只要报文的源 IP 字段属于绑定用户记录中的 IP 地址集合，就可以通过端口。

基于 IP+MAC 地址过滤

报文的二层源 MAC 与三层源 IP 必须和合法用户集中的某条记录完全匹配上，才能通过端口。

指定例外 VLAN

该 VLAN 范围的报文不被检查和过滤，直接通过端口。

相关配置

启动端口上的 IP Source Guard 功能

缺省情况下，端口上的 IP Source Guard 功能关闭。

使用 **ip verify source** 命令可以启动或关闭端口上的 IP Source Guard 功能。

通常 IP Source Guard 功能需要 DHCP Snooping 功能的配合，因此，还需要启动 DHCP Snooping 功能。锐捷设备对启动 DHCP Snooping 功能的时机不做限制，用户可以在 IP Source Guard 启动之前或之后启动 DHCP Snooping。

配置静态 IP Source Guard 用户

缺省情况下，IP Source Guard 检查的合法用户集全部来自 DHCP Snooping 的绑定用户。

使用 **ip source binding** 命令可以添加额外的绑定用户记录。

端口上指定 IP Source Guard 的例外 VLAN

缺省情况下，IP Source Guard 对端口上包含的所有 VLAN 生效。

使用 **ip verify source exclude-vlan** 命令可以指定例外 VLAN 不受 IP Source Guard 的控制。

与端口下的 IP Source Guard 配合使用，端口下必须先启动 IP Source Guard 才可以指定例外 VLAN，端口下关闭 IP Source Guard 后会自动清除指定的例外 VLAN。

端口可以是有线接入的交换口、2 层 AP 口或者 2 层封装子接口，也可以是无线接入的 WLAN。

7.4 产品说明

NBR800G、NBR950G、NBR1500G、NBR2000G 不支持 IPv4 Snooping。NBR108G-P、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 IPv4 Snooping。

7.5 配置详解

配置项	配置建议 & 相关命令	
配置 IP Source Guard	必须配置。用于开启 IP Source Guard 服务。	
	ip verify source	启动端口上的 IP Source Guard 功能。
	ip source binding	配置静态绑定用户。
	Ip verify source exclude-vlan	端口上指定 IP Source Guard 的例外 VLAN

7.5.1 配置IP Source Guard

配置效果

- 对输入 IP 报文进行检查，过滤非法 IP 报文。

注意事项

- 打开 IP Source Guard 功能可能会影响 IP 报文的转发，一般情况下，该功能需要结合 DHCP Snooping 功能使用。
- 无法在 DHCP Snooping 信任端口上配置 IP Source Guard 功能。
- 无法在全局 IP+MAC 的例外口配置 IP Source Guard 功能。
- 只能在有线的交换口、2 层 AP 口、2 层封装子接口以及无线的 WLAN 下配置开启，有线接入是在接口模式下配置，无线接入是在无线安全配置模式下配置。
- 瘦 AP 的有线接入 IP Source Guard 功能在 ap-config all 模式下配置开启

配置方法

- 开启 DHCP Snooping。

- 开启 IP Source Guard。

检验方法

使用设备提供的监控命令，查看 IP Source Guard 用户过滤表项。

相关命令

打开端口上的 IP Source Guard 功能

【命令格式】 **ip verify source** [**port-security**]

【参数说明】 **port-security**：配置 IP Source Guard 功能进行基于 IP+MAC 检测。

【命令模式】 接口模式、无线安全配置模式或者无线 ap-config all 配置模式

【使用指导】 通过该命令打开端口的 IP Source Guard 功能，可以对用户进行基于 IP 的检测，或者进行基于 IP+MAC 的检测。

无线 ap-config all 模式下打开 IP Source Guard 功能等同于所有 AP 的有线口打开 IP Source Guard 功能。

在 IP 源地址绑定数据库中添加静态用户信息

【命令格式】 ip source binding mac-address { vlan vlan-id } ip-address { interface interface-id | wlan wlan-id | ip-mac | ip-only }

【参数说明】 mac-address：静态添加的用户的 MAC 地址。

vlan-id：静态添加的用户的 vlan id，若是 QINQ 终结的用户，指的是用户的外层 vlan id。

ip-address：静态添加的用户的 IP 地址。

interface-id：静态添加的用户所属的有线接口。

wlan-id：静态添加的用户所属的无线 WLAN

ip-mac：全局绑定的类型为 IP+MAC 绑定。

ip-only：全局绑定的类型为仅 IP 绑定。

【配置模式】 全局模式

【使用指导】 通过配置此命令可以允许部分用户通过 IP Source Guard 的检测，不需要通过 DHCP 方式进行统一控制。

无线瘦 AP 环境下，不支持 AC 添加无线 AP 的有线口接入用户静态信息。

接口上指定 IP Source Guard 的例外 VLAN

【命令格式】 **ip verify source exclude-vlan** *vlan-id*

【参数说明】 *vlan-id*：不受接口上 IP Source Guard 控制的 vlan id。

【命令模式】 接口模式或者无线安全配置模式

【使用指导】 启动 IP Source Guard 的接口上，通过该命令可以控制该端口的某些 VLAN 不受 IP Source Guard 控制，这些 VLAN 范围内的 IP 报文不被检查和过滤而是直接放行。

配置举例

↘ 配置打开接口 1 的 IP Source Guard 功能。

【配置方法】
- 打开 DHCP Snooping 功能。略
- 开启 IP Source Guard。

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ip verify source
Ruijie(config-if-GigabitEthernet 0/1)# end
Ruijie(config)# wlansec 1
Ruijie(config-wlansec)# ip verify source port-security
Ruijie(config-wlansec)# end
```

【检验方法】 查看 IP Source Guard 用户过滤表项

```
Ruijie# show ip verify source
```

↘ 添加一个静态绑定用户。

【配置方法】
- 打开 DHCP Snooping 功能。略
- 开启 IP Source Guard。略
- 添加静态用户

```
Ruijie# configure terminal
Ruijie(config)# ip source binding 00d0.f801.0101 vlan 1 192.168.4.243 interface GigabitEthernet 0/3
Ruijie(config)# end
```

【检验方法】 查看 IP Source Guard 用户过滤表项

```
Ruijie# show ip verify source
NO.    INTERFACE                FilterType FilterStatus           IPADDRESS       MACADDRESS
VLAN TYPE
-----  ------------------------ ---------- ---------------------  --------------- --------------
---- -------------
1      GigabitEthernet 0/3      UNSET      Inactive-restrict-off  192.168.4.243
00d0.f801.0101 1    Static
2      GigabitEthernet 0/1      IP-ONLY    Active                 Deny-All
3      WLAN 1                   IP-MAC     Active                 Deny-All
```

↘ 配置打开端口的 IP Source Guard 功能并指定例外 VLAN。

【配置方法】
- 打开 DHCP Snooping 功能。略
- 开启 IP Source Guard。

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ip verify source
Ruijie(config-if-GigabitEthernet 0/1)# ip verify source exclude-vlan 1
Ruijie(config-if)# end
Ruijie(config)# wlansec 1
Ruijie(config-wlansec)# ip verify source
```

```
Ruijie(config-wlansec)# ip verify source exclude-vlan 1
Ruijie(config-wlansec)# end
```

【检验方法】 查看接口上指定的例外 VLAN

```
Ruijie# show run
```

常见配置错误

- 在 DHCP Snooping 信任口开启 IP Source Guard。
- 未启动 IP Source Guard 就指定例外 VLAN。

7.6 监视与维护

清除各类信息

无

查看运行情况

作用	命令
查看 IP Source Guard 用户过滤表项。	**show ip verify source** [**interface** *interface-id* | **wlan** *wlan-id*]
查看 IP Source Guard 用户过滤表项。	**show ip verify source** [**interface** *interface-id*]
查看 IP 源地址绑定数据库的信息	**show ip source binding**

查看调试信息

无

8 SEC-VPDN

8.1 概述

VPDN 英文为 Virtual Private Dial - up Networks，又称为虚拟专用拨号网，是 VPN 业务的一种，是基于拨号用户的虚拟专用拨号网业务。即以拨号接入方式上网，是利用 IP 网络的承载功能结合相应的认证和授权机制建立起来的安全的虚拟专用网，是近年来随着 Internet 的发展而迅速发展起来的一种技术。主要使用与地点分散，在各地有分支机构，移动人员特别多的用户，例如企业用户、远程教育用户。我司产品支持的 VPDN 隧道类型为：L2TP 和 PPTP。

- L2TP(Layer Two Tunneling Protocol)；
- PPTP(Point-to-Point Tunneling Protocol)。

这两种 VPDN 隧道协议有着各自的历史，它们的配置与使用说明请参考后面的章节。PPTP 常见于 MicroSoft Windows 系列产品，而 L2TP 常见于 Cisco 等网络设备上。作为工业标准，L2TP 被 Windows 2000/XP 所支持。

⚠ 本篇除非特指，路由器泛指一般意义上的路由和安全网关。

8.2 典型应用

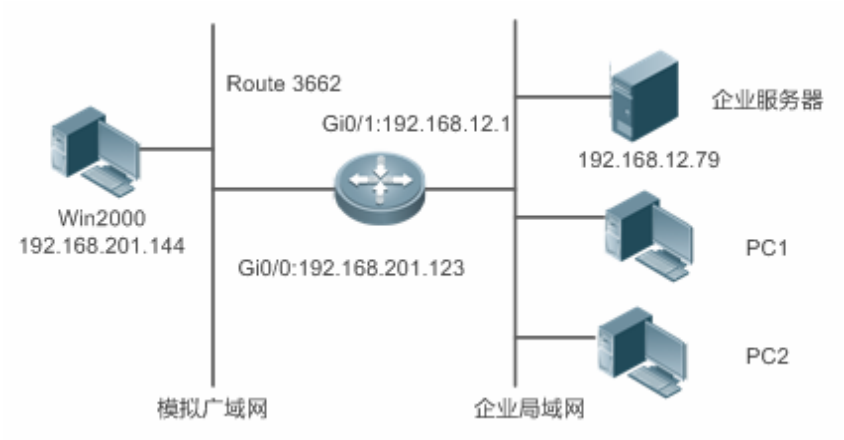
典型应用	场景描述
提供 VPDN 拨入服务	使用 RUIJIE 路由器作企业局域网网关，并使用 PPTP 协议提供 VPDN 拨入服务

8.2.1 提供VPDN拨入服务

应用场景

网络拓扑如下图所示，使用 RUIJIE 路由器作企业局域网网关，并使用 PPTP 协议提供 VPDN 拨入服务。使用一台 Win2000 PC 作为 VPDN 远程客户端创建到 RUIJIE 路由器的 PPTP 隧道，并访问企业局域网内的服务器。为便于测试，远程客户端和 RUIJIE 路由器之间使用以太网模拟广域 IP 网络环境。相关的 IP 地址定义如图所示。

图 8-1



【注释】 为使远程 VPDN 用户能够访问内部网服务器，这些服务器的必须配置可以到达远程拨入用户的路由。一般情况下，只要将这些服务器的默认网关设为路由器的内部网关地址就可以了，在本例中即为 192.168.12.1。

功能部属

配置本地地址池(可选):分配 IP 地址给客户端。

配置用户信息(可选)：为了对试图远程 PPTP 接入本地的客户端进行用户身份验证。

配置 VPDN 全局参数(必须)：全局参数的设置。

配置 Virtual-template 接口(必须)：该接口将成为绑定并负载 PPTP 会话 Virtual-access 接口的模板。

配置 VPDN-group(必须)：设定 VPDN-group 工作参数。

8.3 功能详解

基本概念

↘ 本地地址池

作为 PNS，为了接受远程客户端发起的 PPTP 连接，如果远程客户端没有设置在 VPN 内使用的 IP 地址就需要为其分配 IP 地址。一般情况下，是从一个设定的地址池内将空闲的 IP 地址分配给客户端。

↘ 用户信息

对于配置 PPTP 服务端，这一步骤是可选的。配置用户信息，是为了对试图远程 PPTP 接入本地的客户端进行用户身份验证

↘ VPDN 全局参数

VPDN 全局参数包括：

- 启用/禁用 VPDN 功能：如果用户要求路由器接受远程客户端 PPTP 接入并建立 PPTP 隧道与会话，那么就必须在路由器上启用 VPDN 功能；
- VPDN 源地址：设置了 VPDN 源地址后，远程客户端设置的隧道目的地址必须与之一致才能正常建立 PPTP 隧道；

- VPDN 最大会话数：设置了 VPDN 最大会话数后，超过最大值的接入请求将被拒绝；
- VPDN 限速功能：让用户限制 VPDN 的建立速度，可以限制 VPDN 一次建立隧道的个数；

Virtual-template 接口

Virtual-template 包括：

- Virtual-template 接口(必须)：创建的 Virtual-template 将作为绑定并负载 PPTP 会话的 Virtual-access 接口的配置模板；
- 本地 IP 地址(必须)；
- 对端 IP 地址(可选)；

VPDN-group

VPDN-group 包括：

- VPDN-group(必须)：远程客户端发送的隧道建立请求中的目的地址必须与之匹配，对应的 VPDN-group 才会被应用
- 隧道模式(必须)：可以设置是否允许接受远程客户端拨入，如果用户希望本地路由器承担 PNS 的功能就必须允许接受远程客户端拨入
- 隧道协议(必须)：隧道协议包括 l2tp 和 pptp，如果用户希望本地路由器承担 PNS 的功能就必须配置 **protocol pptp** 或者 **protocol any**
- 对端名称(可选)
- 本地名称(可选)：如果设定了对端名称，那么该 VPDN-group 将只对匹配主机名称的远程客户端有效。如果没有设置对端名称，那么该 VPDN-group 将成为系统默认的 VPDN-group，它可以为任意远程客户端提供 VPDN 服务。
- PPTP 隧道参数(可选)：远程客户端发送的隧道建立请求中的目的地址必须与之匹配，对应的 VPDN-group 才会被应用

VPDN 最大会话数

用户设置 VPDN 服务器允许接入的最大会话数

L2TP-class 接口

L2TP-class 包括：

- L2TP-class 单元：可以通过它来设置 L2TP 控制连接的相关参数，创建的 L2TP-class 可以被 Pseudowire-class 按其名称引用
- L2TP 控制连接的维护更新参数：主要是更新设置 Hello 消息发送间隔

Pseudowire-class 接口

Pseudowire-class 包括：

- Pseudowire-class 单元：可以被 **Interface Virtual-ppp** 接口的 Peudowire 规则按其名称引用
- L2TP 数据传输封装模式：一旦 L2TP 通道的数据传输封装模式被设定便不能再更改；如果用户需要在 Peudowire-class 接口上设置 L2TP 数据传输参数就必须首先设置 L2TP 数据传输封装模式

- L2TP 控制连接参数：控制参数可设置为 l2tpv2，这里 L2TPv2 是遵循用 RFC 2661 规范的 L2TP 协议来创建控制连接，这里使用参数 *L2TP-class-name* 来引用已经存在的 L2TP-class 来限制控制连接参数 ,如果没有这个参数就使用系统默认的 L2TP 控制连接参数

↘ Virtual-ppp 接口

Virtual-ppp 接口包括：

- Virtual-ppp 接口：用于创建一个指定的 L2TP 会话，创建的 virtual-ppp 接口将用以创建并绑定 L2TP 会话
- IP 地址
- 身份验证参数：用户名和密码的设置
- Pseudowire 规则：用户可以在 Virtual-ppp 接口上设置建立 L2TP 会话的 Pseudowire 规则，一旦在 virtual-ppp 接口上设置了 Pseudowire 规则，virtual-ppp 接口就会自动尝试与指定的 LNS 建立 L2TP 会话，如果尝试失败，virtual-ppp 会在 10 秒后再次尝试建立 L2TP 会话。

功能特性

功能特性	作用
建立 PPTP 服务端	使用 PPTP 协议提供 VPDN 拨入服务
建立本地客户端发起的 L2TP 通道	路由器充当 L2TP 客户端并主动发起协商与远程 L2TP 服务器建立隧道
建立远程客户端发起的 L2TP 通道	路由器接受来自远程 L2TP 客户端的连接请求并协商建立隧道

8.3.1 建立PPTP服务端

PPTP（Point to Point Tunneling Protocol），即点对点隧道协议。该协议是在 PPP 协议的基础上开发的一种新的增强型安全协议，支持多协议虚拟专用网（VPN），可以通过密码验证协议（PAP）、可扩展认证协议（EAP）等方法增强安全性。可以使远程用户通过拨入 ISP、通过直接连接 Internet 或其他网络安全地访问企业网。

我司产品目前支持作为 PNS 接入服务器，即接受远程客户端发起的 PPTP 隧道。在这种情况下，路由器接受来自远程 PPTP 客户端的连接请求并协商建立隧道。

工作原理

Point-to-Point-Tunneling Protocol (PPTP) 是支持多协议 VPN 的一种网络技术，使得远程用户通过 Microsoft Windows NT® Workstation、Windows® 95、Windows® 98 、Windows® 2000 以及其它具备 PPP 功能的系统拨到本地 ISP ,就能跨越 Internet 安全地连接并访问公司网络。其标准说明文档为 RFC 2637，最早由 Microsoft 和几家业内领先的通讯设备开发商共同提出，现已推荐到 Internet Engineering Task Force(IETF)。

PPTP 定义了一种在 IP 网络上通过隧道传送 PPP 报文的协议，它没有对 PPP 协议进行任何修改，不过定义了一个新的 PPP 报文承载工具。通过定义客户端 - 服务器的体系结构，PPTP 把网络服务器（Network Access Servers ，NAS）的功能分开由 PNS（PPTP Network Server）和 PAC(PPTP Access Concentrator)共同实现。PNS 设计运行在通用操作系统，基于 TCP/IP 网络，只须具备 IP 接口硬件；而 PAC 则一般具有一个或多个 PSTN、ISDN 或其它具备 PPP 功能的物理接口。

我司产品目前支持作为 PNS 接入服务器，即接受远程客户端发起的 PPTP 隧道。在这种情况下，路由器接受来自远程 PPTP 客户端的连接请求并协商建立隧道。

相关配置

↘ 配置本地地址池

必须配置。

在全局配置模式中，使用 **ip local pool poolname** *first-ip* [*last-ip*]命令可以创建/设置本地地址池。

在全局配置模式中，使用 **no ip local pool** *poolname* 命令可以删除指定名称的地址池。

↘ 配置用户信息

缺省情况下，除天表、周表、月表外其它信息表保留天数为 60 天

使用 **username user-name password** *password* 可以配置用户信息

要删除相关配置，可以在全局配置模式下执行 **no username** *user-name* 命令来执行

↘ 配置 VPDN 全局参数

缺省情况下，天表历史数据保留天数为 60 天。

设置 VPDN 全局参数包括：

- 启用/禁用 VPDN 功能，全局配置模式下，分别使用 **vpdn enable** 和 **no vpdn enable**

  必须配置

- 设置/取消 VPDN 源地址，全局配置模式下，分别使用 **vpdn source-ip** *ip-address* 和 **no vpdn source-ip**

  缺省情况下，系统不会检测接收到的隧道建立请求中的目的地址是否为某一特定值

- 设置/恢复 VPDN 最大会话数，全局配置模式下，分别使用 **vpdn session-limit** *sessions* 和 **no vpdn session-limit**

  缺省情况下，最大会话数即为本命令可配置的最大值

- 设置 VPDN 限速功能，使用 **vpdn limit_rate** *rate_num*，可以改变连接限制的速率，*rate_num* 为每秒可以建立隧道的个数，最小 5 个最大 100 个；使用 **no vpdn limit_rate**，关闭限速功能

  缺省情况下，系统默认开启限速功能，默认的限制速率为 15 路每秒。

↘ 配置 virtual-template 接口

缺省情况下，周表历史数据保留周数为 8 周。

配置 Virtual-template 包括：

- 设置 Virtual-template 接口(必须)；

  全局配置模式中，使用 **interface virtual-template** *number*，创建/配置指定 Virtual -template 接口；使用 **no interface virtual-template** *number*，删除指定 Virtual- template 接口。其中 *number* 是指定的 Virtual-template 接口的序号。创建的 Virtual-template 将作为绑定并负载 PPTP 会话的 Virtual-access 接口的配置模板

- 设置本地 IP 地址(必须)；

- 设置身份验证模式(可选)；
- 设置对端 IP 地址(可选)；

其中，设置本地 IP 地址，设置身份验证模式与设置对端 IP 地址可以参考说明接口配置指导的相关章节。

配置 VPDN-group

缺省情况下，月表历史数据保留月数为 12 个月。

配置 VPDN-group 包括：

- 设置 VPDN-group(必须)

  全局配置模式中，使用 **vpdn-group** *name*，创建/配置指定 VPDN-group 单元；使用 **no vpdn-group** *name*，删除指定 VPDN-group 单元。其中 *name* 是指定的 VPDN-group 的名称。创建的 VPDN-group 单元将允许对应的客户端接入并建立隧道。

- 设置隧道模式(必须)

  在 config-vpdn 配置模式中，使用 **accept-dialin**，允许接受远程客户端拨入；使用 **no accept-dialin**，禁止接受远程客户端拨入。如果用户希望本地路由器承担 PNS 的功能就必须允许接受远程客户端拨入。

- 设置隧道协议(必须)

  在 config-vpdn-acc-in 模式下，使用 **protocol** { any | l2tp | pptp }，设置隧道协议；使用 **no protocol**，取消隧道协议设置。在设置隧道协议之前，必须首先设定隧道模式。如果用户希望本地路由器承担 PNS 的功能就必须配置 **protocol pptp** 或者 **protocol any** 在设置隧道协议之前，必须首先设定隧道模式。如果用户希望本地路由器承担 PNS 的功能就必须配置 **protocol pptp** 或者 **protocol any**

- 设置使用的虚模板(必须)

  在 config-vpdn-acc-in 模式下，使用 **virtual-template** *number*，设置使用的虚模板；使用 **no virtual-template**，取消虚模板引用。在设置 VPDN-group 使用的虚模板之前，必须首先设定隧道模式。

- 设置对端名称(可选)

  在 config-vpdn 模式下，使用 **terminate-from hostname** *name*，设置对端主机名称，其中 *name* 为对端主机名称；使用 **no terminate-from**，取消对端名称设置。如果设定了对端名称，那么该 VPDN-group 将只对匹配主机名称的远程客户端有效。如果没有设置对端名称 ,那么该 VPDN-group 将成为系统默认的 VPDN-group ,它可以为任意远程客户端提供 VPDN 服务。如果配置的多个 VPDN-group 都没有设定对端名称，则系统将使用找到的第一个满足条件的 VPDN-group 接受远程拨入。

- 设置本地名称(可选)

  在 config-vpdn 模式下，使用 **local name** *name*，设置本地名称；使用 **no local name**，取消本地名称设置。其中 *name* 为本地名称。默认情况下，我司产品使用路由器的名称作为本地名称发送给隧道的对端主机。

- 设置 VPDN-group 源地址(可选)

  在 config-vpdn 模式下，使用 **source-ip** *src-ip*，设置 VPDN-group 源地址；使用 **no source-ip**，取消 VPDN-group 源地址设置，其中 *src-ip* 为 VPDN-group 源地址。远程客户端发送的隧道建立请求中的目的地址必须与之匹配，对应的 VPDN-group 才会被应用。

- 设置 PPTP 流控参数(可选)

在 config-vpdn 模式下，使用 **pptp flow-control receive-window** *winsize*，设置 PPTP 会话的接收窗口大小，取值范围是 1-64；使用 **no pptp flow-control receive-window**，取消 PPTP 会话接收窗口的设置，恢复为默认值，PAC 为 16，PNS 为 64；使用 **pptp flow-control static-rtt** *interval*，设置 PPTP 会话报文收发等待 ACK 的静态参考时间，取值范围是 100-5000 毫秒；使用 **no pptp flow-control static-rtt**，取消 PPTP 会话报文收发等待 ACK 的静态参考时间，恢复为默认值 1500 毫秒，其中 winsize 为 PPTP 会话接收窗口大小，interval 为等待 ACK 的静态参考时间。在一般应用中，此参数可以不用设置而使用默认值。

- 设置 PPTP 隧道参数(可选)

  在 config-vpdn 模式下，使用 **pptp tunnel echo** *interval*，设置 PPTP 隧道主动发送 echo 的间隔时间，取值范围是 0 - 1000 秒；使用 **no pptp tunnel echo**，取消 PPTP echo 发送间隔设置，恢复成默认值 60 秒。其中 interval 为 PPTP 隧道主动发送 ECHO 的间隔时间，当为 0 时表示不主动发送 ECHO，当不为 0 时表示在持续此时间间隔没有收到隧道对端的任何合法报文后主动发送 ECHO 探测隧道状态。

8.3.2 L2TP配置

L2TP 是一种工业标准的 Internet 隧道协议，功能大致和 PPTP 协议类似，比如同样可以对网络数据流进行加密。不过也有不同之处，比如 PPTP 要求网络为 IP 网络，L2TP 要求面向数据包的点对点连接；PPTP 使用单一隧道，L2TP 使用多隧道；L2TP 提供包头压缩、隧道验证，而 PPTP 不支持。

我司产品支持两种模式的 L2TP 隧道：

- 本地客户端发起的 L2TP 通道。在这种情况下，路由器充当 L2TP 客户端并主动发起协商与远程 L2TP 服务器建立隧道。
- 远程客户端发起的 L2TP 通道。在这种情况下，路由器接受来自远程 L2TP 客户端的连接请求并协商建立隧道。

工作原理

Layer 2 Tunnel Protocol(L2TP)是 Internet Engineering Task Force(IETF)综合两种已有的隧道协议即 Cisco 公司的 Layer 2 Forwarding(L2F)协议与微软的 Point-to-Point Tunneling Protocol (PPTP)协议而提出的一项具有标准意义的隧道协议，其标准说明文档为 RFC 2661。

L2TP 是对 Point-to-Point Protocol(PPP)的一种扩展，它依靠利用 PPP 实现用户身份验证和传输数据。与 PPTP 不同的是，L2TP 使用 UDP 作为控制消息与数据消息的传输协议。

L2TP 也是实现 VPN 的一种重要和有效的方法。VPN 使得网络用户访问公司内部网更方便与安全，无论是拨号用户还是其他网络接入方式的用户都可以通过 VPN 轻松达到这个目的。

8.3.2.1 建立本地客户端发起的L2TP通道

相关配置

↘ 创建并配置 l2tp-class（可选）

设置 L2TP-class 包括：

- 设置 L2TP-class 单元

  在 config 模式下，使用 **l2tp-class l2tp-class-name**，创建/配置指定名称的 L2TP-class 接口；使用 **no l2tp-class l2tp-class-name**，删除指定名称的 L2TP-class 接口。

  其中 L2TP-class-name 是创建/设置的 L2TP-class 单元的名称 ,这里创建的 L2TP-class 可以被 Pseudowire-class 按其名称引用。

- 设置 L2TP 控制连接的时间参数

  在 config-l2tp-class 模式下，使用 **receive-window** *size*，设置控制连接的接受窗口大小；**no receive-window**，恢复系统默认的控制连接接受窗口大小；**retransmit { initial { retries** *initial-retries* **| timeout { max | min }** *initial-timeout* **} | retries** *retries* **| timeout { max | min }** *timeout* **}**，设置控制连接重传参数；**no retransmit { initial { retries | timeout { max | min } } | retries | timeout { max | min } }**，恢复系统默认的控制连接重传参数；**timeout setup** *seconds*，设置建立控制连接可花费的最长时间；**no timeout setup**，设置建立控制连接时间花费上限为默认值。

  其中 ,size 为接受窗口尺寸 ,系统默认值为 8; initial-retries 为 SCCRQ 重传次数 ,系统默认值为 2;initial-timeout 是 SCCRQ 重传的时间间隔，系统默认的最小时间间隔为 1 秒，系统默认的最大时间间隔为 8 秒；retries 是控制消息的重传次数，系统默认是 5；timeout 是控制消息重传的时间间隔，系统默认得最小时间间隔为 1 秒，系统默认的最大时间间隔为 8 秒；seconds 是建立控制连接(Tunnel)的时间花费上限，系统默认值为 120 秒。

- 设置 L2TP 控制连接验证参数

  在 config-l2tp-class 模式下，使用 **authentication** 要求进行通道身份验证；**no authentication**，取消通道验证设置；**no hostname**，使用默认的本地主机名；**hostname** *host-name*，设置该控制连接对应的本地主机名称；**password** *pass-words*，设置通道口令；**no password**，取消通道口令设置。

  在默认情况下，我司产品不要求进行通道验证，并且使用路由器的名称作为本地主机名称。如果要求通道验证，那么两端必须使用相同的通道口令。其中， host-name 是用户设置的本地主机名称，pass-words 是用于通道验证的口令。

- 设置 L2TP 控制连接的维护更新参数

  在 config-l2tp-class 模式下，使用 **hello** *interval*，设置 Hello 消息发送间隔；**no hello**，恢复默认的 Hello 消息发送间隔。

  在这里，*interval* 是 Hello 消息发送间隔，系统默认值为 60 秒。

↘ 创建并配置 Pseudowire-class 接口(可选)

设置 Pseudowire-class 包括：

- 设置 Pseudowire-class 单元

  在 config 模式下，使用 **pseudowire-class** *pseudowire- class-name*，创建/配置指定名称的 Pseudowire-class 接口；**no pseudowire-class** *pseudowire- class-name*，删除指定名称的 Pseudowire-class 接口。

  其中 pseudowire-class-name 是创建/设置的 Pseudowire-class 单元的名称，这里创建的 Pseudowire-class 可以被 Interface Virtual-ppp 接口的 Peudowire 规则按其名称引用。

- 设置 L2TP 数据传输封装模式

  在 config-pw-class 模式下，使用 **encapsulation l2tpv2**，设置数据传输封装模式。

  需要注意的是，一旦 L2TP 通道的数据传输封装模式被设定便不能再更改；如果用户需要在 Peudowire-class 接口上设置 L2TP 数据传输参数就必须首先设置 L2TP 数据传输封装模式。

- 设置 L2TP 数据传输 IP 参数

  在 config-pw-class 模式下，使用 **ip dfbit set**，禁止通道数据分片；**no ip dfbit set**，允许通道数据分片；

  ip ttl *ttl-value*，设置通道的 IP 头的 TTL；**no ip ttl**，使用默认 TTL 值；**ip local interface** *interface-name*，指定通道的本地接口(地址)；**no ip local interface** *interface-name*，取消通道本地接口(地址)指定。

  设置 L2TP 数据传输的 IP 参数实际上是设置负载 L2TP 的 UDP 数据的 IP 头参数。在默认情况下，系统允许对通道数据分片，默认的 TTL 为 255 并且系统会按照指定的对端地址为其设置在路由上最接近的本地地址(接口)。

- 设置 L2TP 控制连接参数

  在 config-pw-class 模式下，使用 **protocol l2tpv2** [**l2tp-class-name**]，设置 L2TP 控制连接参数；**no protocol**，使用默认的控制连接参数。

  这里 L2TPv2 是遵循用 RFC 2661 规范的 L2TP 协议来创建控制连接，这里使用参数 L2TP-class-name 来引用已经存在的 L2TP-class 来限制控制连接参数，如果没有这个参数就使用系统默认的 L2TP 控制连接参数

↘ 创建并配置 Virtual-ppp 接口(必须)

设置 Virtual-ppp 接口包括：

- 设置 Virtual-ppp 接口

  在 config 模式下，使用 **interface virtual-ppp** *number*，创建/配置指定的 Virtual-ppp 接口；**no interface virtual-ppp** *number*，删除指定 Virtual-ppp 接口。

  其中 *number* 是指定的 virtual-ppp 接口的名称。创建的 virtual-ppp 接口将用以创建并绑定 L2TP 会话。

- 设置 IP 地址

  设置 IP 地址可以参考说明接口配置指导的相关章节

- 设置身份验证参数

  设置身份验证参数可以参考说明接口配置指导的相关章节

- 设置 Pseudowire 规则

  我司产品提供下面的命令让用户可以在 Virtual-ppp 接口上设置建立 L2TP 会话的 Pseudowire 规则。

  在 config-if 模式下，使用 **pseudowire** *peer-ip-address vcid* { **encapsulation l2tpv2** [**pw-class** *pw-class-name*] | **pw-class pw-class-name** }，设置 Pseudowire 规则；**no pseudowire**，删除 Pseudowire 规则。

  一旦在 virtual-ppp 接口上设置了 Pseudowire 规则，virtual-ppp 接口就会自动尝试与指定的 LNS 建立 L2TP 会话，如果尝试失败，virtual-ppp 会在 10 秒后再次尝试建立 L2TP 会话。这里 *peer-ip-address* 是远程 LNS 的地址，*vcid* 是全局标号，参数 *pw-class-name* 是引用的 Pseudowire-class 的名称。

  我司产品还提供用指定的 LNS 的名称建立 L2TP 会话，前提是必须开启 DNS 服务，我司的产品只提供 DNS client 服务，并且所指定的 LNS 的名称必须在 DNS 服务器上注册过。

  在 config-if 模式下，**pseudowire hostname** *peer-hostname* **vcid** {**encapsulation l2tpv2** [**pw-class** *pw-class-name*] | **pw-class pw-class-name** }，设置 Pseudowire 规则；**no pseudowire**，删除 Pseudowire 规则。

  一旦在 virtual-ppp 接口上设置了 Pseudowire 规则，virtual-ppp 接口就会自动尝试与指定的 LNS 建立 L2TP 会话，如果尝试失败，virtual-ppp 会在 10 秒后再次尝试建立 L2TP 会话。这里 *peer-hostname* 是远程 LNS 的 hostname，我司的

DNS 会将这个 *hostname* 转换为 LNS 的具体 IP 地址（注意这个 *hostname* 必须在 DNS 服务器上有注册），*vcid* 是全局标号，参数 *pw-class-name* 是引用的 Pseudowire-class 的名称

8.3.2.2 建立远程客户端发起的L2TP通道

相关配置

↘ 配置本地地址池(可选)

对于实现远程客户端发起的 L2TP 隧道，这一步骤是可选的。作为 LNS，为了接受远程客户端发起的 L2TP 连接，如果远程客户端没有设置在 VPN 内使用的 IP 地址就需要为其分配 IP 地址。一般情况下，是从一个设定的地址池内将空闲的 IP 地址分配给客户端，我司产品提供下面的命令来配置本地地址池。

在 config 模式下，使用 **ip local pool** *poolname first-ip* [*last-ip*]，创建/设置本地地址池；**no ip local pool** *poolname*，删除指定名称的地址池。

其中 *poolname* 是创建/设置的本地地址池的名称，*first-ip* 是本地地址池设定的地址范围的首地址，*last-ip* 是本地地址池设定的地址范围的末地址。

↘ 配置用户信息(可选)

对于实现远程客户端发起的 L2TP 隧道，这一步骤是可选的。配置用户信息，是为了试图对远程 L2TP 接入本地的客户端进行用户身份验证。我司产品提供下面的命令来配置用户信息。

在 config 模式下，使用 **username** *user-name password* **{ 0 | 7 } password**，配置用户信息；**no username** *user-name*，删除指定用户。

其中 *user-name* 是允许拨入的用户名称，*password* 是用户对应的口令。路由器在本地维护一个允许访问的(拨入)用户的名称与对应口令的数据库。

↘ 配置 VPDN 全局参数(必须)

对于实现远程客户端发起的 L2TP 隧道，这一步骤是必须的。它将 VPDN 的全局工作参数。设置 VPDN 全局参数包括：

- 启用/禁用 VPDN 功能

  我司产品提供下面的命令让用户可以决定是否启用 VPDN 功能。如果用户要求路由器接受远程客户端 L2TP 接入并建立 L2TP 隧道与会话，那么就必须在路由器上启用 VPDN 功能。

  在 config 模式下，使用 **vpdn enable**，启用 VPDN 功能；**no vpdn enable**，禁用 VPDN 功能。

  需要注意的是，我司产品支持 VPDN 启用/禁用的即配即用功能，如果禁用 VPDN 功能那么所有已经存在的 L2TP 隧道以及会话都会被拆除

- 设置 VPDN 源地址

  我司产品提供下面的命令让用户设置 VPDN 功能使用(本地)源地址。在设置了 VPDN 源地址后，远程客户端设置的隧道目的地址必须与之一致才能正常建立 L2TP 隧道。

  在 config 模式下，使用 **vpdn source-ip** *ip-address*，设置 VPDN 源地址；**no vpdn source-ip**，取消 VPDN 源地址设置。

在默认情况下，系统不会检测接受到的隧道建立请求中的目的地址是否为某一特定值。

- 设置 VPDN 最大会话数；

  我司产品提供下面的命令让用户设置 VPDN 服务器允许接入的最大会话数。在设置了 VPDN 最大会话数后，超过最大值的接入请求将被拒绝。

  在 config 模式下，**vpdn session-limit** *sessions*，设置 VPDN 最大会话数；**no vpdn session-limit**，恢复 VPDN 最大会话数的默认值。

  在默认情况下，最大会话数即为本命令可配置的最大值。

- 设置 VPDN 忽略源地址检查命令；

  本命令用于忽略对方设备发过来的不符合 RFC 规范的 L2TP 控制报文的错误，使得协商可以正常进行

  在 config-vpdn 模式下，使用 **vpdn ignore_source**，忽略对方发送过来的报文源地址检查；**no vpdn ignore_source**，严格检查对方发送来的报文源地址。

  在默认情况下，系统严格检查源地址匹配情况。

- 设置 VPDN 限速功能；

  我司产品提供下面的命令让用户限制 VPDN 的建立速度，可以限制 VPDN 一次建立隧道的个数。

  在 config 模式下，**vpdn limit_rate** *rate_num*，可以改变连接限制的速率，*rate_num* 为每秒可以建立隧道的个数，最小 5 个最大 100 个；**no vpdn limit_rate**，关闭限速功能。

  默认情况下，系统默认开启限速功能，默认的限制速率为 15 路每秒。

其中,启用/禁用 VPDN 是必须，而设置 VPDN 源地址则是可选的

↘ 配置 Virtual-template 接口(必须)

对于实现远程客户端发起的 L2TP 隧道，这一步骤是必须的。它将成为绑定并负载 L2TP 会话 Virtual-access 接口的模板。配置 Virtual-template 包括：

- 设置 Virtual-template 接口(必须)

  我司产品提供下面的命令让用户可以设置 Virtual-template 接口

  在 config 模式下，使用 **interface virtual-template** *number*，创建/配置指定 Virtual -template 接口；**no interface virtual-template** *number*，删除指定 Virtual-template 接口。

  其中 *number* 是指定的 Virtual-template 接口的序号。创建的 Virtual-template 将作为绑定并负载 L2TP 会话的 Virtual-access 接口的配置模板。

- 设置本地 IP 地址(必须)
- 设置身份验证模式(可选)
- 设置对端 IP 地址(可选)

其中，设置本地 IP 地址，设置身份验证模式与设置对端 IP 地址可以参考说明接口配置指导的相关章节

↘ 配置 Vpdn-group(必须)

对于实现远程客户端发起的 L2TP 隧道，这一步骤是必须的。它将设定 VPDN-group 工作参数。配置 VPDN-group 包括：

- 设置 VPDN-group(必须)

  我司产品提供下面的命令让用户可以设置 VPDN-group 接口

  在 config 模式下，**vpdn-group** *name*，创建/配置指定 VPDN-group 单元；**no vpdn-group** *name*，删除指定 VPDN-group 单元。

  其中 *name* 是指定的 VPDN-group 的名称。创建的 VPDN-group 单元将允许对应的客户端接入并建立隧道

- 设置隧道模式(必须)

  我司产品提供下面的命令让用户可以设置隧道模式

  在 config-vpdn 模式下，**accept-dialin**，允许接受远程客户端拨入；**no accept-dialin**，禁止接受远程客户端拨入。

  如果用户希望本地路由器承担 LNS 的功能就必须允许接受远程客户端拨入

- 设置隧道协议(必须)

  我司产品提供下面的命令让用户可以设置隧道协议

  在 config-vpdn-acc-in 模式下，**protocol { any | l2tp | pptp }**，设置隧道协议；**no protocol**，取消隧道协议设置。

  在设置隧道协议之前，必须首先设定隧道模式。

- 设置使用的虚模板(必须)

  我司产品提供下面的命令让用户可以设置 VPDN-group 使用虚模板

  在 config-vpdn-acc-in 模式下，**virtual-template number**，设置使用的虚模板；**no virtual-template**，取消虚模板引用

  在设置 VPDN-group 使用的虚模板之前，必须首先设定隧道模式

- 设置对端名称(可选)

  我司产品提供下面的命令让用户可以设置对端名称。如果设定了对端名称，那么该 VPDN-group 将只对主机名称与之匹配的远程客户端有效。如果没有设置对端名称，那么该 VPDN-group 将成为系统默认的 VPDN-group，它可以为任意远程客户端提供 VPDN 服务

  在 config-vpdn 模式下，**terminate-from hostname** *name*，设置对端主机名称；**no terminate-from**，取消对端名称设置。

  其中 *name* 为对端主机名称

- 设置本地名称(可选)

  我司产品提供下面的命令让用户可以设置本地名称，该名称将作为一个记录性的属性发送给对端

  在 config-vpdn 模式下，使用 **local name** *name*，设置本地名称；**no local name**，取消本地名称设置。

  其中 *name* 为本地名称。默认情况下，我司产品使用路由器的名称作为本地名称发送给隧道的对端主机。

- 设置 VPDN-group 源地址(可选)

  我司产品提供下面的命令让用户可以设置 VPDN-group 源地址。远程客户端发送的隧道建立请求中的目的地址必须与之匹配，对应的 VPDN-group 才会被应用。

  在 config-vpdn 模式下，使用 **source-ip** *src-ip*，设置 VPDN-group 源地址；**no source-ip**，取消 VPDN-group 源地址设置。

其中 *src-ip* 为 VPDN-group 源地址。

- 设置 L2TP 控制连接参数(可选)

  我司产品提供下面的命令让用户可以设置 L2TP 控制连接参数。

  在 config-vpdn 模式下，使用 **l2tp tunnel authentication**，启用通道验证；**no l2tp tunnel authentication**，禁用通道验证；**l2tp tunnel hello** *interval*，设置 Hello 发送间隔；**no l2tp tunnel hello**，取消 Hello 发送间隔设置； **l2tp tunnel password** *pass-word* ,设置通道口令 ;**no l2tp tunnel password** ,取消通道口令设置 ;l**2tp tunnel receive-window** *size*，设置通道控制连接接受窗口尺寸使用默认值 ;**no l2tp tunnel receive- window** ,通道控制连接接受窗口尺寸使用默认值；**l2tp tunnel retransmit { retries number | timeout { min | max }** *seconds* **}**，设置通道控制消息重传参数；**no l2tp tunnel retransmit { retries | timeout { min | max } }**，使用默认的控制消息重传参数；**l2tp tunne l timeout { no-session | setup }** *seconds*，设置通道最大的无会话/控制连接建立时间间隔；

  no l2tp tunnel timeout { no-session | setup}，通道最大的无会话/控制连接建立时间间隔采用默认值；**no l2tp tunnel timeout { no-session | setup}**，通道最大的无会话/控制连接建立时间间隔采用默认值；**l2tp tunnel force_ipsec**，在外加密的情况下使用，配置该命令后表示报文必须通过加密后才能通过 VPDN 隧道；**no l2tp tunnel force_ipsec**，不启用强制加密；**l2tp tunnel avp-hidden-compatible**，兼容支持 RFC2661 标准的 AVP Hidden 解析算法；**no l2tp tunnel avp-hidden-compatible**，默认采用 Cisco 标准的 AVP Hidden 解析算法。

  在默认情况下，L2TP 隧道的建立不要求通道验证(而 Cisco 在默认情况下要求通道验证)。系统默认的 Hello 控制消息的发送间隔为 60 秒，默认的控制消息的接受窗口尺寸为 4，默认的控制消息的重传次数为 5，默认的最小控制消息重传间隔为 1 秒，默认的最大控制消息重传间隔为 8 秒，默认的通道最大无会话时间间隔为 600 秒，默认的通道能允许的最长的控制连接建立时间为 300 秒。如果要求进行 L2TP 通道验证，L2TP 通道的两端必须配置相同的通道口令，然而在默认情况下，系统没有为任何 L2TP 通道配置通道口令，也没有要求进行通道验证。其中，参数 interval 是 Hello 消息发送间隔，单位为秒；参数 seconds 的单位也是秒。系统默认不启用强制 ipsec 加密验证；系统默认支持的 AVP Hidden 解析算法采用 Cisco 标准，在配置兼容支持 RFC2661 标准的 AVP Hidden 解析算法后，采用 RFC2661 标准来解析隐藏 AVP

- 设置 L2TP 数据传输参数(可选)

  我司产品提供下面的命令让用户可以设置传输 L2TP 消息的 IP/UDP 参数。

  在 config-vpdn 模式下，**l2tp ip udp checksum**，要求 UDP 校验和非空；**no l2tp ip udp checksum**，要求 UDP 校验和为空；**ip tos** *tos-value*，设置 IP TOS 域；**no ip tos**，取消 IPTOS 域设置；**ip precedence** *value*，设置 IP Precedence 域；**no ip precedence**，取消 IP Precedence 域设置。

  其中 tos-value 为负载 L2TP 消息的 IP 头的 TOS 域的值，value 为该 IP 头的 Precedence 域的值。在默认情况下，我司产品的 L2TP 通道要求负载 L2TP 消息的 UDP 的 Checksum 域为空，要求负载 L2TP 消息的 IP 头 TOS 为 0 并且该 IP 头的 Precedence 域也为 0。

  需要说明的是 tos，precedence 只有 L2TP 支持，PPTP 虽然可以配置，但不生效。

- 设置重新进行 PPP 协商(可选)

  本命令用于强制 PPP 重新进行完整的认证，在 Client 触发 LAC 开始拨号时，LAC 会代理 LNS 对 Client 进行认证，本命用来在 L2TP 隧道建立后重新对 Client 进行认证。该命令只在 LNS 上有效。

  在 config-vpdn 模式下，使用 **force-local-chap**，强制重新 PPP 认证；**no force-local-chap**，不进行 PPP 重新认证。

- 设置忽略控制报文错误(可选)

  本命令用于忽略对方设备发过来的不符合 RFC 规范的 L2TP 控制报文的错误，使得协商可以正常进行。

在 config-vpdn 模式下，使用 **lcp renegotiation always**，忽略对方报文错误；**no lcp renegotiation always**，检查控制报文是否符合 RFC。

8.4 配置详解

配置项	配置建议 & 相关命令	
PPTP 服务端配置	必须配置。使用 PPTP 协议提供 VPDN 拨入服务。	
	ip local pool *poolname first-ip* [*last-ip*]	创建/设置本地地址池。
	username *user-name* **password** *password*	配置用户信息
	vpdn congestion_avoidanc	启用 VPDN 拥塞控制
	vpdn enable	启用 VPDN 功能
	vpdn source-ip *ip-address*	设置 VPDN 源地址
	vpdn session-limit *sessions*	设置 VPDN 最大会话数
	vpdn limit_rate *rate_num*	设置连接限速的速率，*rate_num* 为每秒可以建立隧道的个数，最小 5 个最大 100 个
	vpdn-group *name*	创建/配置指定 VPDN-group 单元
	interface virtual-template *number*	创建/配置指定 Virtual -template 接口
	accept-dialin	允许接受远程客户端拨入
	protocol { **any** | **l2tp** | **pptp**}	设置隧道协议
	virtual-template *number*	设置使用的虚模板
	terminate-from hostname *name*	设置对端主机名称
	local name *name*	设置本地名称
	source-ip *src-ip*	设置 VPDN-group 源地址
	pptp flow-control receive-window *winsize*	设置 PPTP 会话的接收窗口大小 ,取值范围是 1—64
	pptp flow-control static-rtt *interval*	设置 PPTP 会话报文收发等待 ACK 的静态参考时间，取值范围是 100—5000 毫秒
	pptp tunnel echo *interval*	设置 PPTP 隧道主动发送 echo 的间隔时间，取值范围是 0 - 1000 秒
本地客户端发起的 L2TP 配置	必须配置，由本地客户端发起的 L2TP 配置	
	l2tp-class *l2tp-class-name*	创建/配置指定名称的 L2TP-class 接口
	receive-window *size*	设置控制连接的接受窗口大小。
	retransmit { **initial** { **retries** *initial-retries* | **timeout** { **max** | **min** } *initial-timeout* } | **retries** *retries* | **timeout** { **max** | **min** } *timeout* }	设置控制连接重传参数。
	timeout setup *seconds*	设置建立控制连接可花费的最长时间。
	authentication	要求进行通道身份验证
	hostname *host-name*	设置该控制连接对应的本地主机名称
	password *pass-words*	设置通道口令
	hello *interval*	设置 Hello 消息发送间隔

	pseudowire-class *pseudowire- class-name*	创建/配置指定名称的 Pseudowire-class 接口
	encapsulation l2tpv2	设置数据传输封装模式
	ip dfbit set	禁止通道数据分片
	ip ttl *ttl-value*	设置通道的 IP 头的 TTL
	ip local interface *interface-name*	指定通道的本地接口(地址)
	protocol l2tpv2 [*l2tp-class-name*]	设置 L2TP 控制连接参数
	interface virtual-ppp *number*	创建/配置指定的 Virtual-ppp 接口
	pseudowire *peer-ip-address vcid* {**encapsulation l2tpv2** [**pw-class** *pw-class-name*] | **pw-class** *pw-class-name* }	设置 Pseudowire 规则
远程客户端发起的 L2TP 配置	必须配置，由远程客户端发起的 L2TP 配置	
	ip local pool *poolname first-ip* [*last-Ip*]	创建/设置本地地址池。
	username *user-name* **password { 0 | 7 }** *password*	配置用户信息
	vpdn congestion_avoidanc	启用 VPDN 拥塞控制
	vpdn enable	启用 VPDN 功能
	vpdn source-ip *ip-address*	设置 VPDN 源地址
	vpdn session-limit *sessions*	设置 VPDN 最大会话数
	vpdn ignore_source	忽略对方发送过来的报文源地址检查
	vpdn limit_rate *rate_num*	设置连接限速的速率，*rate_num* 为每秒可以建立隧道的个数，最小 5 个最大 100 个
	vpdn-group *name*	创建/配置指定 VPDN-group 单元
	interface virtual-template *number*	创建/配置指定 Virtual -template 接口
	accept-dialin	允许接受远程客户端拨入
	protocol { **any** | **l2tp** | **pptp** }	设置隧道协议
	virtual-template *number*	设置使用的虚模板
	terminate-from hostname *name*	设置对端主机名称
	local name *name*	设置本地名称
	source-ip *src-ip*	设置 VPDN-group 源地址
	l2tp tunnel authentication	启用通道验证
	l2tp tunnel hello *interval*	设置 Hello 发送间隔
	l2tp tunnel password *pass-word*	设置通道口令
	l2tp tunnel receive-window *size*	设置通道控制连接接受窗口尺寸使用默认值
	l2tp tunnel retransmit { **retries** *number* | **timeout** { **min** | **max** } *seconds*}	设置通道控制消息重传参数
	l2tp tunnel timeout { **no-session**| **setup** } *seconds*	设置通道最大的无会话/控制连接建立时间间隔
	l2tp tunnel force_ipsec	在外加密的情况下使用 ,配置该命令后表示报文必须通过加密后才能通过 VPDN 隧道
	l2tp tunnel avp-hidden-compatible	兼容支持 RFC2661 标准的 AVP Hidden 解析算法

	l2tp ip udp checksum	要求 UDP 校验和非空
	ip tos *tos-value*	设置 IP TOS 域
	ip precedence *value*	设置 IP Precedence 域
	force-local-chap	强制重新 PPP 认证
	force-local-lcp	强制重新 lcp 认证
	lcp renegotiation always	忽略对方报文错误

8.4.1 PPTP服务端配置

配置效果

提供 VPDN 拨入服务。

注意事项

启用/禁用 VPDN 是必须，而设置 VPDN 源地址是可选的。

如果禁用 VPDN 功能那么所有已经存在的 PPTP 隧道以及会话继续保留，但新的 PPTP 隧道和会话不允许再创建。

在设置隧道协议之前，必须首先设定隧道模式。如果用户希望本地路由器承担 PNS 的功能就必须配置 **protocol pptp** 或者 **protocol any**。

在设置 VPDN-group 使用的虚模板之前，必须首先设定隧道模式。

配置方法

↘ 创建/设置本地地址池

- 可选配置
- 作为 PNS，为了接受远程客户端发起的 PPTP 连接，如果远程客户端没有设置在 VPN 内使用的 IP 地址就需要为其分配 IP 地址。一般情况下，是从一个设定的地址池内将空闲的 IP 地址分配给客户端。

↘ 配置用户信息

- 可选配置
- 配置用户信息，是为了对试图远程 PPTP 接入本地的客户端进行用户身份验证；路由器在本地维护一个允许访问的(拨入)用户的名称与对应口令的数据库

↘ 启用 VPDN 拥塞控制

- 可选配置
- 如果用户要求启用 VPDN 拥塞控制，必须配置此选项

↘ 启用 VPDN 功能

- 可选配置
- 如果用户要求路由器接受远程客户端 PPTP 接入并建立 PPTP 隧道与会话，那么就必须在路由器上启用 VPDN 功能

设置 VPDN 源地址

- 可选配置
- 在设置了 VPDN 源地址后，远程客户端设置的隧道目的地址必须与之一致才能正常建立 PPTP 隧道；在默认情况下，系统不会检测接收到的隧道建立请求中的目的地址是否为某一特定值

设置 VPDN 最大会话数

- 可选配置
- 在设置了 VPDN 最大会话数后，超过最大值的接入请求将被拒绝；在默认情况下，最大会话数即为本命令可配置的最大值

打开限速功能

- 可选配置
- 让用户限制 VPDN 的建立速度，可以限制 VPDN 一次建立隧道的个数；在默认情况下，系统不会开启限速功能

创建/配置指定 Virtual -template 接口

- 必须配置
- 创建的 Virtual-template 将作为绑定并负载 PPTP 会话的 Virtual-access 接口的配置模板

创建/配置指定 VPDN-group 单元

- 必须配置
- 创建的 VPDN-group 单元将允许对应的客户端接入并建立隧道

允许接受远程客户端拨入

- 可选配置
- 如果用户希望本地路由器承担 PNS 的功能就必须允许接受远程客户端拨入

设置隧道协议

- 必须配置
- 在设置隧道协议之前，必须首先设定隧道模式。如果用户希望本地路由器承担 PNS 的功能就必须配置 **protocol pptp** 或者 **protocol any**

设置使用的虚模板

- 必须配置
- 在设置 VPDN-group 使用的虚模板之前，必须首先设定隧道模式

设置对端主机名称

- 可选配置
- 如果设定了对端名称，那么该 VPDN-group 将只对匹配主机名称的远程客户端有效。如果没有设置对端名称，那么该 VPDN-group 将成为系统默认的 VPDN-group，它可以为任意远程客户端提供 VPDN 服务。如果配置的多个 VPDN-group 都没有设定对端名称，则系统将使用找到的第一个满足条件的 VPDN-group 接受远程拨入

设置本地名称

- 可选配置
- 让用户可以设置本地名称，该名称将作为一个记录性的属性发送给对端；默认情况下，我司产品使用路由器的名称作为本地名称发送给隧道的对端主机

设置 VPDN-group 源地址

- 必须配置
- 远程客户端发送的隧道建立请求中的目的地址必须与之匹配，对应的 VPDN-group 才会被应用

设置 PPTP 会话的接收窗口大小

- 可选配置
- 设置 PPTP 流控参数；在一般应用中，此参数可以不用设置而使用默认值

设置 PPTP 会话报文收发等待 ACK 的静态参考时间

- 可选配置
- 设置 PPTP 流控参数；在一般应用中，此参数可以不用设置而使用默认值

设置 PPTP 隧道主动发送 echo 的间隔时间

- 可选配置
- 设置 PPTP 隧道参数。在一般应用中，此参数可以不用设置而使用默认值

检验方法

使用 VPDN 拨入服务，能够访问企业局域网内的服务器。

相关命令

创建/设置本地地址池

【命令格式】 **ip local pool** *poolname first-ip [last-ip]*

【参数说明】 *poolname*：创建/设置的本地地址池的名称。
first-ip：本地地址池设定的地址范围的首地址
last-ip：本地地址池设定的地址范围的末地址

【命令模式】 全局模式

【使用指导】 -

配置用户信息

【命令格式】 **username** *user-name* **password** *password*

【参数说明】 *user-name*：允许拨入的用户名称；

password：用户对应的口令。

【命令模式】 全局模式

【使用指导】 -

启用 VPDN 功能

【命令格式】 **vpdn enable**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 -

设置 VPDN 源地址

【命令格式】 **vpdn source-ip** *ip-address*

【参数说明】 *Ip-address*：VPDN 源地址。

【命令模式】 全局模式

【使用指导】 -

设置 VPDN 最大会话数

【命令格式】 **vpdn session-limit** *sessions*

【参数说明】 *sessions*：VPDN 最大会话数。

【命令模式】 全局模式

【使用指导】 -

打开限速功能

【命令格式】 **vpdn limit_rate** *rate_num*

【参数说明】 *rate_num*：每秒可以建立隧道的个数，最小 5 个最大 100 个。

【命令模式】 全局模式

【使用指导】 -

创建/配置指定 Virtual -template 接口

【命令格式】 **interface virtual-template** *number*

【参数说明】 *number*：指定的 Virtual-template 接口的序号

【命令模式】 全局模式

【使用指导】 -

创建/配置指定 VPDN-group 单元

【命令格式】 **vpdn-group** *name*

【参数说明】 *name*：指定的 VPDN-group 的名称

【命令模式】 全局模式

【使用指导】 -

允许接受远程客户端拨入

【命令格式】 **accept-dialin**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 -

设置隧道协议

【命令格式】 **protocol** { **any** | **l2tp** | **pptp** }

【参数说明】 -

【命令模式】 config-vpdn-acc-in 模式

【使用指导】 在设置隧道协议之前 ,必须首先设定隧道模式。如果用户希望本地路由器承担 PNS 的功能就必须配置 **protocol pptp** 或者 **protocol any**

设置使用的虚模板

【命令格式】 **virtual-template** *number*

【参数说明】 *number*：指定的 Virtual-template 接口的序号。

【命令模式】 config-vpdn-acc-in 模式

【使用指导】 -

设置对端主机名称

【命令格式】 **terminate-from hostname** *name*

【参数说明】 *name*：对端主机名称

【命令模式】 config-vpdn 模式

【使用指导】 -

设置本地名称

【命令格式】 **local name** *name*

【参数说明】 *name*：本地名称

【命令模式】 config-vpdn 模式

【使用指导】 -

设置 VPDN-group 源地址

【命令格式】 **source-ip** *src-ip*

【参数说明】 *src-ip*：VPDN-group 源地址

【命令模式】 config-vpdn 模式

【使用指导】 -

设置 PPTP 会话的接收窗口大小

【命令格式】 **pptp flow-control receive-window** *winsize*

【参数说明】 *winsize*：PPTP 会话接收窗口大小。

【命令模式】 config-vpdn 模式

【使用指导】 -

设置 PPTP 会话报文收发等待 ACK 的静态参考时间

【命令格式】 **pptp flow-control static-rtt** *interval*

【参数说明】 *interval*：PPTP 会话报文收发等待 ACK 的静态参考时间，取值范围是 100—5000 毫秒。

【命令模式】 config-vpdn 模式

【使用指导】 -

设置 PPTP 隧道主动发送 echo 的间隔时间

【命令格式】 **pptp tunnel echo** *interval*

【参数说明】 *interval*：PPTP 隧道主动发送 echo 的间隔时间，取值范围是 0 - 1000 秒。

【命令模式】 config-vpdn 模式

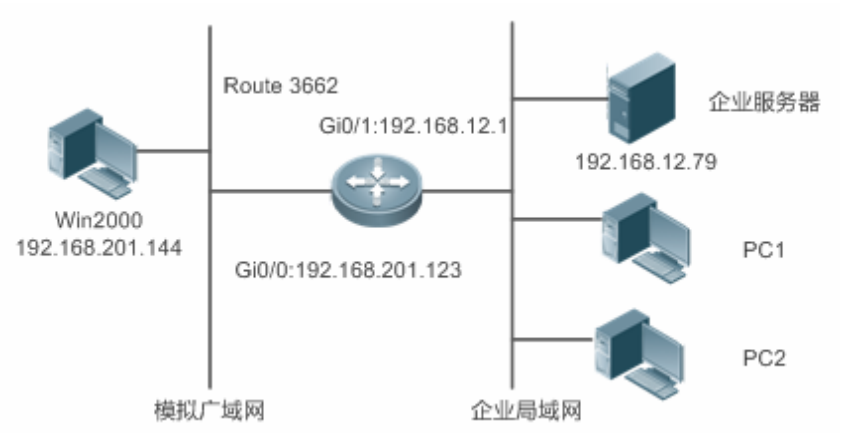
【使用指导】 -

配置举例

使用 RUIJIE 路由器作企业局域网网关，并使用 PPTP 协议提供 VPDN 拨入服务

【网络环境】

图 8-2



【配置方法】

- RUIJIE 路由器作为 PPTP 服务端，提供 PPTP 拨入服务，配置启用 VPDN 服务。
- 配置 VPDN-group 单元，允许接收远程客户端拨入，设置隧道协议为 PPTP。
- 配置本地地址池，为拨入的客户端分配虚拟 IP 地址。
- 配置用于认证客户端的用户名和密码。
- 配置虚模板，设置 PPP 认证方式，并关联本地地址池。

路由器	Ruijie # configure terminal Ruijie (config)# vpdn enable Ruijie (config)# vpdn-group pptp Ruijie (config-vpdn)# accept-dialin Ruijie (config-vpdn)# protocol pptp Ruijie (config-vpdn)# virtual-template 1 Ruijie (config)# ip local pool pptp 1.1.1.2 1.1.1.254 Ruijie (config)# username pc password 0 1111 Ruijie (config)# interface Virtual-Template 1 Ruijie (config-if-virtual-template-1)# ppp authentication pap Ruijie (config-if-virtual-template-1)# ip unnumbered FastEthernet 0/1 Ruijie (config-if-virtual-template-1)# peer default ip address pool pptp
【检验方法】	在 Win2000 的“网络和拨号连接”中新建连接，“网络连接类型”选择“通过 Internet 连接到专用网络”，“公用网络”选择“不拨初始连接”，填入目标地址为 192.168.201.123，命名此连接名称为 Vpdnconnect。在 Vpdnconnect 的属性中，指定 VPDN 服务器的类型为 PPTP，并在安全设置中定义使用 PAP 认证及可选加密。在点击呼叫时，输入路由器所配置的用户名 pc 和密码 1111。 配置完成，Win2000 拨入到路由器后，即可访问公司内部网的服务器，如服务器 192.168.12.79。

常见错误

无

8.4.2 本地客户端发起的L2TP配置

配置效果

本地客户端发起的 L2TP 通道。在这种情况下，路由器充当 L2TP 客户端并主动发起协商与远程 L2TP 服务器建立隧道。

注意事项

一旦 L2TP 通道的数据传输封装模式被设定便不能再更改；如果用户需要在 Peudowire-class 接口上设置 L2TP 数据传输参数就必须首先设置 L2TP 数据传输封装模式。

用户可以在 Virtual-ppp 接口上设置建立 L2TP 会话的 Pseudowire 规则，一旦在 virtual-ppp 接口上设置了 Pseudowire 规则，virtual-ppp 接口就会自动尝试与指定的 LNS 建立 L2TP 会话，如果尝试失败，virtual-ppp 会在 10 秒后再次尝试建立 L2TP 会话。

我司产品还提供用指定的 LNS 的名称建立 L2TP 会话，前提是必须开启 DNS 服务，我司的产品只提供 DNS client 服务，并且所指定的 LNS 的名称必须在 DNS 服务器上注册过，一旦在 virtual-ppp 接口上设置了 Pseudowire 规则，virtual-ppp 接口就会自动尝试与指定的 LNS 建立 L2TP 会话，如果尝试失败，virtual-ppp 会在 10 秒后再次尝试建立 L2TP 会话。

配置方法

创建/配置指定名称的 L2TP-class 接口

- 必须配置
- 其中 L2TP-class-name 是创建/设置的 L2TP-class 单元的名称 ,这里创建的 L2TP-class 可以被 Pseudowire-class 按其名称引用

设置控制连接的接受窗口大小

- 可选配置
- 设置 L2TP 控制连接的时间参数；接受窗口尺寸系统默认值为 8

设置控制连接重传参数

- 可选配置
- 设置 L2TP 控制连接的时间参数；*initial-retries* 为 SCCRQ 重传次数，系统默认值为 2；*initial-timeout* 是 SCCRQ 重传的时间间隔，系统默认的最小时间间隔为 1 秒，系统默认的最大时间间隔为 8 秒；*retries* 是控制消息的重传次数，系统默认是 5；*timeout* 是控制消息重传的时间间隔，系统默认得最小时间间隔为 1 秒，系统默认的最大时间间隔为 8 秒

设置建立控制连接可花费的最长时间

- 可选配置
- 设置 L2TP 控制连接的时间参数；建立控制连接(Tunnel)的时间花费上限，系统默认值为 120 秒

要求进行通道身份验证

- 可选配置
- 在默认情况下，我司产品不要求进行通道验证，并且使用路由器的名称作为本地主机名称；如果要求通道验证，那么要进行下面两个配置

设置该控制连接对应的本地主机名称

- 可选配置
- 使用路由器的名称作为本地主机名称

设置通道口令

- 可选配置
- 两端必须使用相同的通道口令

设置 Hello 消息发送间隔

- 可选配置
- 消息发送间隔，系统默认值为 60 秒

创建/配置指定名称的 Pseudowire-class 接口

- 必须配置
- 创建的 **Pseudowire-class** 可以被 **Interface Virtual-ppp** 接口的 Peudowire 规则按其名称引用

设置数据传输封装模式

- 可选配置
- 一旦 L2TP 通道的数据传输封装模式被设定便不能再更改；如果用户需要在 Peudowire-class 接口上设置 L2TP 数据传输参数就必须首先设置 L2TP 数据传输封装模式

禁止通道数据分片

- 可选配置
- L2TP 数据传输 IP 参数的设置，设置 L2TP 数据传输的 IP 参数实际上是设置负载 L2TP 的 UDP 数据的 IP 头参数。在默认情况下，系统允许对通道数据分片

设置通道的 IP 头的 TTL

- 可选配置
- L2TP 数据传输 IP 参数的设置；默认的 TTL 为 255

指定通道的本地接口(地址)

- 可选配置
- L2TP 数据传输 IP 参数的设置；系统会按照指定的对端地址为其设置在路由上最接近的本地地址(接口)

设置 L2TP 控制连接参数

- 可选配置
- 这里 L2TPv2 是遵循用 RFC 2661 规范的 L2TP 协议来创建控制连接，这里使用参数 *L2TP-class-name* 来引用已经存在的 L2TP-class 来限制控制连接参数，如果没有这个参数就使用系统默认的 L2TP 控制连接参数

创建/配置指定的 Virtual-ppp 接口

- 可选配置
- 创建的 virtual-ppp 接口将用以创建并绑定 L2TP 会话

设置 Pseudowire 规则

- 可选配置
- 可以在 Virtual-ppp 接口上设置建立 L2TP 会话的 Pseudowire 规则；一旦在 virtual-ppp 接口上设置了 Pseudowire 规则，virtual-ppp 接口就会自动尝试与指定的 LNS 建立 L2TP 会话 ,如果尝试失败 ,virtual-ppp 会在 10 秒后再次尝试建立 L2TP 会话。这里 peer-ip-address 是远程 LNS 的地址，vcid 是全局标号，参数 pw-class-name 是引用的 Pseudowire-class 的名称

检验方法

使用 Cisco 2620 作为 L2TP Server，RUIJIE 路由器作为 L2TP 客户端发起连接

相关命令

创建/配置指定名称的 L2TP-class 接口

【命令格式】 **l2tp-class** *l2tp-class-name*

【参数说明】 L2TP-class-name:创建/设置的 L2TP-class 单元的名称

【命令模式】 全局模式

【使用指导】 -

设置控制连接的接受窗口大小

【命令格式】 **receive-window** *size*

【参数说明】 size: 接受窗口尺寸，系统默认值为 8

【命令模式】 config-l2tp-class 模式

【使用指导】 -

设置控制连接重传参数

【命令格式】 **retransmit** { **initial** { **retries** *initial-retries* | **timeout** { **max** | **min** } *initial-timeout* } | **retries** *retries* | **timeout** { **max** | **min** } *timeout* }

【参数说明】 *initial-retries*：SCCRQ 重传次数，系统默认值为 2

initial-timeout :SCCRQ 重传的时间间隔 ,系统默认的最小时间间隔为 1 秒 ,系统默认的最大时间间隔为 8 秒；

retries：控制消息的重传次数，系统默认是 5；

timeout：控制消息重传的时间间隔，系统默认得最小时间间隔为 1 秒，系统默认的最大时间间隔为 8 秒

【命令模式】 config-l2tp-class 模式

【使用指导】 -

设置建立控制连接可花费的最长时间

【命令格式】 **timeout setup** *seconds*

【参数说明】 *seconds*：建立控制连接(Tunnel)的时间花费上限，系统默认值为 120 秒

【命令模式】 全局模式

【使用指导】 -

要求进行通道身份验证

【命令格式】 **authentication**

【参数说明】 -

【命令模式】 config-l2tp-class 模式

【使用指导】 -

设置该控制连接对应的本地主机名称

【命令格式】 **hostname** *host-name*
【参数说明】 *host-name*：用户设置的本地主机名称
【命令模式】 config-l2tp-class 模式
【使用指导】 -

设置通道口令

【命令格式】 **password** *pass-words*
【参数说明】 *pass-words*：用于通道验证的口令
【命令模式】 config-l2tp-class 模式
【使用指导】 -

设置 Hello 消息发送间隔

【命令格式】 **hello** *interval*
【参数说明】 *Interval*：Hello 消息发送间隔，系统默认值为 60 秒
【命令模式】 config-l2tp-class 模式
【使用指导】 -

创建/配置指定名称的 Pseudowire-class 接口

【命令格式】 **pseudowire-class** *pseudowire-class-name*
【参数说明】 *pseudowire-class-name*：创建/设置的 **Pseudowire-class** 单元的名称
【命令模式】 全局模式
【使用指导】 -

设置数据传输封装模式

【命令格式】 **encapsulation l2tpv2**
【参数说明】 -
【命令模式】 config-pw-class 模式
【使用指导】 -

禁止通道数据分片

【命令格式】 **ip dfbit set**
【参数说明】 -
【命令模式】 config-pw-class 模式
【使用指导】 -

设置通道的 IP 头的 TTL

【命令格式】 **ip ttl** *ttl-value*
【参数说明】 *ttl-value*: IP 头的 TTL，默认的 TTL 为 255
【命令模式】 config-pw-class 模式

【使用指导】 -

指定通道的本地接口(地址)

【命令格式】 **ip local interface** *interface-name*

【参数说明】 *interface-name*: 通道的本地接口，系统会按照指定的对端地址为其设置在路由上最接近的本地地址(接口)

【命令模式】 config-pw-class 模式

【使用指导】 -

设置 L2TP 控制连接参数

【命令格式】 **protocol l2tpv2** [*l2tp-class-name*]

【参数说明】 *l2tp-class-name*: 来引用已经存在的 L2TP-class 来限制控制连接参数 ,如果没有这个参数就使用系统默认的 L2TP 控制连接参数

【命令模式】 config-pw-class 模式

【使用指导】 -

创建/配置指定的 Virtual-ppp 接口

【命令格式】 **interface virtual-ppp** *number*

【参数说明】 *number*：指定的 virtual-ppp 接口的名称

【命令模式】 全局模式

【使用指导】 -

设置 Pseudowire 规则

【命令格式】 **pseudowire** *peer-ip-address vcid* { **encapsulation l2tpv2** [**pw-class** *pw-class-name*] | **pw-class** *pw-class-name* }

【参数说明】 peer-ip-address：远程 LNS 的地址；
vcid：全局标号；
pw-class-name：引用的 Pseudowire-class 的名称

【命令模式】 config-if 模式

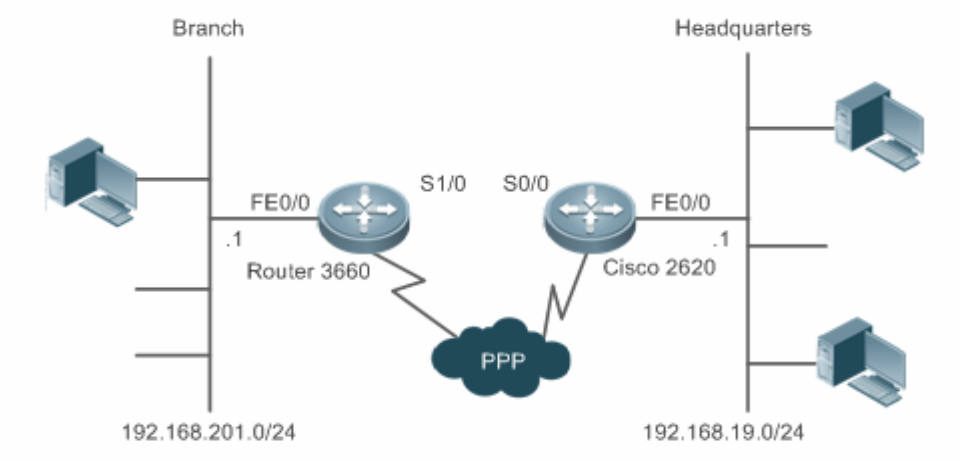
【使用指导】 -

配置举例

使用 Cisco 2620 作为 L2TP Server，RUIJIE 路由器作为 L2TP 客户端发起连接。

【网络环境】

图 8-3



【配置方法】

- 配置 Cisco 2620 作为 L2TP 服务端，设置允许客户端使用 L2TP 接入。
- 配置服务端采用 pap 认证方式，用户名密码为 rgnos。
- 配置服务端地址池，在客户端认证通过后动态分配隧道 IP 地址。
- 配置 RUIJIE 路由器为 L2TP 客户端。
- 配置客户端使用 L2TP 数据传输封装模式。
- 配置客户端的隧道接口，设置 Pseudowire 规则，指定连接的服务端地址。
- 配置客户端采用 pap 认证方式，用户名密码为 rgnos。
- 配置客户端隧道地址采用协商方式，由服务端再认证通过后动态分配。
- 配置客户端 Branch 内部网络访问服务端 Headquarters 内部网络的路由走 virtual-ppp 接口。

路由器

```
Ruijie # configure terminal
Ruijie (config)# l2tp-class 1
Ruijie (config)# pseudowire-class 1
Ruijie (config-pw-class)# encapsulation l2tpv2
Ruijie (config)# interface Virtual-ppp 1
Ruijie (config-if-virtual-ppp 1)# pseudowire hostname mm.hxs.meibu.com 1 encapsulation l2tpv2
Ruijie (config-if-virtual-ppp 1)# ppp pap sent-username rgnos password rgnos
Ruijie (config-if-virtual-ppp 1)# ip address negotiate
Ruijie (config)# ip route 192.168.19.0 255.255.255.0 Virtual-ppp 1
```

【检验方法】

Branch 内网 PC 无需进行 L2TP 配置，网络管理员只需要给它分配一个内部网地址(这里是 192.168.201.213)并设置其网关为 192.168.201.1 即可。检查内网 PC 访问服务端 Headquaters 内部网段 192.168.19.0 正常。

常见错误

无

8.4.3 远程客户端发起的L2TP配置

配置效果

远程客户端发起的 L2TP 通道。在这种情况下，路由器接受来自远程 L2TP 客户端的连接请求并协商建立隧道。

注意事项

我司产品支持 VPDN 启用/禁用的即配即用功能，如果禁用 VPDN 功能那么所有已经存在的 L2TP 隧道以及会话都会被拆除。

配置方法

创建/设置本地地址池

- 可选配置
- 作为 PNS，为了接受远程客户端发起的 L2TP 连接，如果远程客户端没有设置在 VPN 内使用的 IP 地址就需要为其分配 IP 地址。一般情况下，是从一个设定的地址池内将空闲的 IP 地址分配给客户端，我司产品提供下面的命令来配置本地地址池

配置用户信息

- 可选配置
- 配置用户信息，是为了对试图远程 L2TP 接入本地的客户端进行用户身份验证；路由器在本地维护一个允许访问的(拨入)用户的名称与对应口令的数据库

启用 VPDN 拥塞控制

- 可选配置
- 如果用户要求启用 VPDN 拥塞控制，必须配置此选项

启用 VPDN 功能

- 必须配置
- 如果用户要求路由器接受远程客户端 L2TP 接入并建立 L2TP 隧道与会话，那么就必须在路由器上启用 VPDN 功能

设置 VPDN 源地址

- 可选配置
- 在设置了 VPDN 源地址后，远程客户端设置的隧道目的地址必须与之一致才能正常建立 L2TP 隧道；在默认情况下，系统不会检测接收到的隧道建立请求中的目的地址是否为某一特定值

设置 VPDN 最大会话数

- 可选配置
- 在设置了 VPDN 最大会话数后，超过最大值的接入请求将被拒绝；在默认情况下，最大会话数即为本命令可配置的最大值

忽略对方发送过来的报文源地址检查

- 可选配置

- 本命令用于忽略对方设备发过来的不符合 RFC 规范的 L2TP 控制报文的错误，使得协商可以正常进行；在默认情况下，系统严格检查源地址匹配情况

打开限速功能

- 可选配置
- 让用户限制 VPDN 的建立速度，可以限制 VPDN 一次建立隧道的个数；在默认情况下，系统不会开启限速功能

创建/配置指定 Virtual -template 接口

- 必须配置
- 创建的 Virtual-template 将作为绑定并负载 L2TP 会话的 Virtual-access 接口的配置模板

创建/配置指定 VPDN-group 单元

- 必须配置
- 创建的 VPDN-group 单元将允许对应的客户端接入并建立隧道

允许接受远程客户端拨入

- 必须配置
- 如果用户希望本地路由器承担 PNS 的功能就必须允许接受远程客户端拨入

设置隧道协议

- 必须配置
- 在设置隧道协议之前，必须首先设定隧道模式。如果用户希望本地路由器承担 PNS 的功能就必须配置 **protocol pptp** 或者 **protocol any**

设置使用的虚模板

- 必须配置
- 在设置 VPDN-group 使用的虚模板之前，必须首先设定隧道模式

设置对端主机名称

- 可选配置
- 如果设定了对端名称，那么该 VPDN-group 将只对匹配主机名称的远程客户端有效。如果没有设置对端名称，那么该 VPDN-group 将成为系统默认的 VPDN-group，它可以为任意远程客户端提供 VPDN 服务。如果配置的多个 VPDN-group 都没有设定对端名称，则系统将使用找到的第一个满足条件的 VPDN-group 接受远程拨入

设置本地名称

- 必须配置
- 让用户可以设置本地名称，该名称将作为一个记录性的属性发送给对端；默认情况下，我司产品使用路由器的名称作为本地名称发送给隧道的对端主机

设置 VPDN-group 源地址

- 必须配置
- 远程客户端发送的隧道建立请求中的目的地址必须与之匹配，对应的 VPDN-group 才会被应用

启用通道验证

- 可选配置
- 设置 L2TP 控制连接参数；在默认情况下，L2TP 隧道的建立不要求通道验证(而 Cisco 在默认情况下要求通道验证)

设置 Hello 发送间隔

- 可选配置
- 设置 L2TP 控制连接参数；系统默认的 Hello 控制消息的发送间隔为 60 秒

设置通道口令

- 必须配置
- 设置 L2TP 控制连接参数

设置通道控制连接接受窗口尺寸使用默认值

- 可选配置
- 设置 L2TP 控制连接参数；默认的控制消息的接受窗口尺寸为 4

设置通道控制消息重传参数

- 可选配置
- 设置 L2TP 控制连接参数；默认的控制消息的重传次数为 5，默认的最小控制消息重传间隔为 1 秒，默认的最大控制消息重传间隔为 8 秒

设置通道最大的无会话/控制连接建立时间间隔

- 可选配置
- 设置 L2TP 控制连接参数；默认的通道最大无会话时间间隔为 600 秒，默认的通道能允许的最长的控制连接建立时间为 300 秒

在外加密的情况下使用，配置该命令后表示报文必须通过加密后才能通过 VPDN 隧道

- 必须配置
- 设置 L2TP 控制连接参数；

兼容支持 RFC2661 标准的 AVP Hidden 解析算法

- 必须配置
- 设置 L2TP 控制连接参数；

要求 UDP 校验和非空

- 可选配置
- 设置传输 L2TP 消息的 IP/UDP 参数；在默认情况下，我司产品的 L2TP 通道要求负载 L2TP 消息的 UDP 的 Checksum 域为空

设置 IP TOS 域

- 可选配置
- 设置传输 L2TP 消息的 IP/UDP 参数；在默认情况下，要求负载 L2TP 消息的 IP 头 TOS 为 0

设置 IP Precedence 域

- 可选配置
- 设置传输 L2TP 消息的 IP/UDP 参数；在默认情况下，该 IP 头的 Precedence 域也为 0

强制重新 PPP 认证

- 必须配置
- 在 Client 触发 LAC 开始拨号时，LAC 会代理 LNS 对 Client 进行认证，本命用来在 L2TP 隧道建立后重新对 Client 进行认证。该命令只在 LNS 上有效

忽略对方报文错误

- 可选配置
- 用于忽略对方设备发过来的不符合 RFC 规范的 L2TP 控制报文的错误，使得协商可以正常进行

检验方法

远程客户端发起的 L2TP 通道。路由器接受来自远程 L2TP 客户端的连接请求并协商建立隧道。

相关命令

创建/设置本地地址池

【命令格式】 **ip local pool** *poolname first-ip [last-ip]*

【参数说明】 *poolname*：创建/设置的本地地址池的名称。
first-ip：本地地址池设定的地址范围的首地址
last-ip：本地地址池设定的地址范围的末地址

【命令模式】 全局模式

【使用指导】 -

配置用户信息

【命令格式】 **username** *user-name* **password** *password*

【参数说明】 *user-name*：允许拨入的用户名称；

password：用户对应的口令。

【命令模式】 全局模式

【使用指导】 -

启用 VPDN 功能

【命令格式】 **vpdn enable**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 -

设置 VPDN 源地址

【命令格式】 **vpdn source-ip** *ip-address*

【参数说明】 *Ip-address*：VPDN 源地址。

【命令模式】 全局模式

【使用指导】 -

设置 VPDN 最大会话数

【命令格式】 **vpdn session-limit** *sessions*

【参数说明】 *sessions*：VPDN 最大会话数。

【命令模式】 全局模式

【使用指导】 -

忽略对方发送过来的报文源地址检查

【命令格式】 **vpdn ignore_source**

【参数说明】 -

【命令模式】 config-vpdn 模式

【使用指导】 -

打开限速功能

【命令格式】 **vpdn limit_rate** *rate_num*

【参数说明】 *rate_num*：每秒可以建立隧道的个数，最小 5 个最大 100 个。

【命令模式】 全局模式

【使用指导】 -

创建/配置指定 Virtual -template 接口

【命令格式】 **interface virtual-template** *number*

【参数说明】 *number*：指定的 Virtual-template 接口的序号

【命令模式】 全局模式

【使用指导】 -

创建/配置指定 VPDN-group 单元

【命令格式】 **vpdn-group** *name*

【参数说明】 *name*：指定的 VPDN-group 的名称

【命令模式】 全局模式

【使用指导】 -

允许接受远程客户端拨入

【命令格式】 **accept-dialin**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 -

设置隧道协议

【命令格式】 **protocol** { **any** | **l2tp** | **pptp** }

【参数说明】 -

【命令模式】 config-vpdn-acc-in 模式

【使用指导】 在设置隧道协议之前 必须首先设定隧道模式。如果用户希望本地路由器承担 PNS 的功能就必须配置 **protocol l2tp** 或者 **protocol any**

设置使用的虚模板

【命令格式】 **virtual-template** *number*

【参数说明】 *number*：指定的 Virtual-template 接口的序号。

【命令模式】 config-vpdn-acc-in 模式

【使用指导】 -

设置对端主机名称

【命令格式】 **terminate-from hostname** *name*

【参数说明】 *name*：对端主机名称

【命令模式】 config-vpdn 模式

【使用指导】 -

设置本地名称

【命令格式】 **local name** *name*

【参数说明】 *name*：本地名称

【命令模式】 config-vpdn 模式

【使用指导】 -

设置 VPDN-group 源地址

【命令格式】 **source-ip** *src-ip*

【参数说明】 *src-ip*：VPDN-group 源地址
【命令模式】 config-vpdn 模式
【使用指导】 -

启用通道验证

【命令格式】 **l2tp tunnel authentication**
【参数说明】 -
【命令模式】 config-vpdn 模式
【使用指导】 -

设置 Hello 发送间隔

【命令格式】 **l2tp tunnel hello** *interval*
【参数说明】 *Interval*：Hello 消息发送间隔，单位为秒
【命令模式】 config-vpdn 模式
【使用指导】 -

设置通道口令

【命令格式】 **l2tp tunnel password** *pass-word*
【参数说明】 *pass-word*：通道口令
【命令模式】 config-vpdn 模式
【使用指导】 -

设置通道控制连接接受窗口尺寸使用默认值

【命令格式】 **l2tp tunnel receive-window** *size*
【参数说明】 *size*：通道控制连接接受窗口尺寸
【命令模式】 config-vpdn 模式
【使用指导】 -

设置通道控制消息重传参数

【命令格式】 **l2tp tunnel retransmit** { **retries** *number* | **timeout** { **min** | **max** } *seconds* }
【参数说明】 *number*：重传次数
seconds：超时时长，单位为秒
【命令模式】 config-vpdn 模式
【使用指导】 -

设置通道最大的无会话/控制连接建立时间间隔

【命令格式】 **l2tp tunnel timeout** { **no-session** | **setup**} *seconds*
【参数说明】 *seconds*：时间间隔，单位为秒
【命令模式】 config-vpdn 模式
【使用指导】 -

在外加密的情况下使用，配置该命令后表示报文必须通过加密后才能通过 VPDN 隧道

【命令格式】 **l2tp tunnel force_ipsec**
【参数说明】 -
【命令模式】 config-vpdn 模式
【使用指导】 -

兼容支持 RFC2661 标准的 AVP Hidden 解析算法

【命令格式】 **l2tp tunnel avp-hidden-compatible**
【参数说明】 -
【命令模式】 config-vpdn 模式
【使用指导】 -

要求 UDP 校验和非空

【命令格式】 **l2tp ip udp checksum**
【参数说明】 -
【命令模式】 config-vpdn 模式
【使用指导】 -

设置 IP TOS 域

【命令格式】 **ip tos** *tos-value*
【参数说明】 *tos-value*：负载 L2TP 消息的 IP 头的 TOS 域的值
【命令模式】 config-vpdn 模式
【使用指导】 -

设置 IP Precedence 域

【命令格式】 **ip precedence** *value*
【参数说明】 *Value*：该 IP 头的 Precedence 域的值
【命令模式】 config-vpdn 模式
【使用指导】 -

强制重新 PPP 认证

【命令格式】 **force-local-chap**
【参数说明】 -
【命令模式】 config-vpdn 模式
【使用指导】 -

强制重新 lcp 认证

【命令格式】 **force-local-lcp**
【参数说明】 -
【命令模式】 config-vpdn 模式
【使用指导】 -

忽略对方报文错误

【命令格式】 **lcp renegotiation always**

【参数说明】 -

【命令模式】 config-vpdn 模式

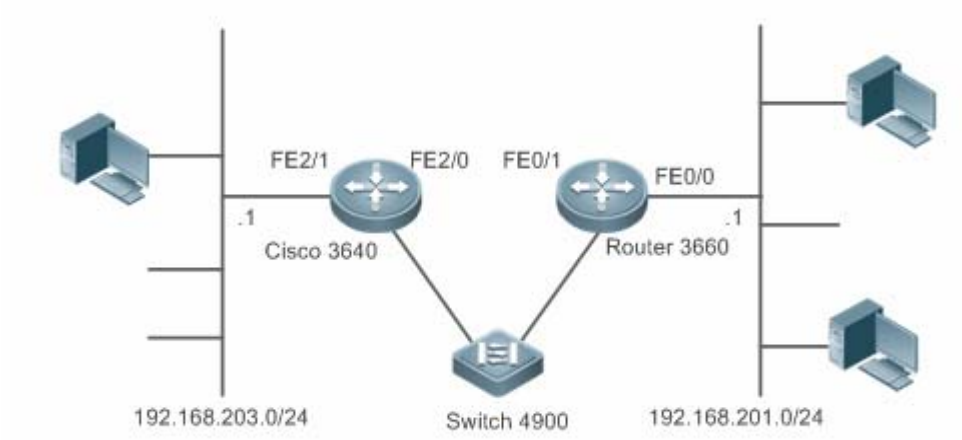
【使用指导】 -

配置举例

与 Cisco 3640 建立隧道

【网络环境】

图 8-4



【配置方法】

- RUIJIE 路由器作为 L2TP 服务端，提供 L2TP 拨入服务，配置启用 VPDN 服务。
- 配置服务端 VPDN-group 单元，允许接收远程客户端拨入，设置隧道协议为 L2TP。
- 配置服务端本地地址池，为拨入的客户端分配虚拟 IP 地址。
- 配置服务端用于认证客户端的用户名和密码分别为 user 和 pass。
- 配置服务端虚模板，设置 PPP 认证方式，并关联本地地址池。
- 配置 Cisco 3640 作为 L2TP 客户端，使用用户名密码进行 L2TP 拨号。

路由器

```
Ruijie # configure terminal
Ruijie (config)# vpdn enable
Ruijie (config)# vpdn-group pptp
Ruijie (config-vpdn)# accept-dialin
Ruijie (config-vpdn)# protocol l2tp
Ruijie (config-vpdn)# virtual-template 1
Ruijie (config)# ip local pool l2tp 1.1.1.2 1.1.1.254
Ruijie (config)# username user password 0 pass
Ruijie (config)# interface Virtual-Template 1
Ruijie (config-if-virtual-template-1)# ppp authentication pap
Ruijie (config-if-virtual-template-1)# ip unnumbered FastEthernet 0/1
Ruijie (config-if-virtual-template-1)# peer default ip address pool l2tp
```

【检验方法】 配置 Cisco 3640 作为 L2TP 客户端，指定 VPDN 服务器的类型为 L2TP，并设置使用 PAP 认证，用户名 pc 和密码分别为 user 和 pass。配置完成，L2TP 拨入后，客户端内网网段 192.168.203.0 即可访问服务端内部

网的服务器，如服务器 192.168.201.79。

常见错误

无

8.5 监视与维护

清除各类信息

无

查看运行情况

作用	命令
显示当前的 vpdn 通道以及会话信息；显示指定 id 的隧道信息	**show vpdn** [**session | tunnel** [**l2tp** *locid*]]
显示当前日志文件中所有的或指定用户的上下线信息	**show vpdn log [user** *username*] 注：首次支持项目 11_1_PJ5
查看当前系统配置所有 l2tp-class 接口或指定的 l2tp-class 接口的详细配置信息	**show l2tp-class [** *l2tp-class-name* **]**
查看当前系统配置所有 pseudowire-class 接口或指定的 pseudowire-class 接口的详细配置信息	**show pseudowire-class** [*pseudowire-class-name*]
强制清除指定的隧道	**clear vpdn tunnel** [{ **l2tp** | **pptp** } [**id** *locid*] | [*remote-host-name*] **]**
清除日志文件中的用户上下线消息	**clear vpdn log** 注：首次支持项目 11_1_PJ5

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 vpdn error 调试开关	**debug vpdn error**
关闭 vpdn error 调试开关	**no debug vpdn error**
打开 vpdn event 调试开关	**debug vpdn event**
关闭 vpdn event 调试开关	**no debug vpdn event**

打开 vpdn packet 调试开关	**debug vpdn packet**
关闭 vpdn packet 调试开关	**no debug vpdn packet**
打开 vpdn l2x-data 调试开关	**debug vpdn l2x-data**
关闭 vpdn l2x-data 调试开关	**no debug vpdn l2x-data**
打开 vpdn l2x-errors 调试开关	**debug vpdn l2x-errors**
关闭 vpdn l2x-errors 调试开关	**no debug vpdn l2x-errors**
打开 vpdn l2x-events 调试开关	**debug vpdn l2x-events**
关闭 vpdn l2x-events 调试开关	**no debug vpdn l2x-events**
打开 vpdn l2x-packets 调试开关	**debug vpdn l2x-packets**
关闭 vpdn l2x-packets 调试开关	**no debug vpdn l2x-packets**

9 IPSEC

9.1 概述

IPSec（IP Security）是 IETF 制定的三层隧道加密协议，它为 Internet 上传输的数据提供了高质量的、可互操作的、基于密码学的安全保证。特定的通信方之间在 IP 层通过加密与数据源认证等方式，提供了以下的安全服务：

- **数据机密性**（Confidentiality）：IPSec 发送方在通过网络传输包前对包进行加密。
- **数据完整性**（Data Integrity）：IPSec 接收方对发送方发送来的包进行认证，以确保数据在传输过程中没有被篡改。
- **数据来源认证**（Data Authentication）：IPSec 在接收端可以认证发送 IPSec 报文的发送端是否合法。
- **防重放**（Anti-Replay）：IPSec 接收方可检测并拒绝接收过时或重复的报文。

可以通过 IKE（Internet Key Exchange，因特网密钥交换协议）为 IPSec 提供自动协商交换密钥、建立和维护安全联盟的服务，以简化 IPSec 的使用和管理。IKE 协商并不是必须的，IPSec 所使用的策略和算法等也可以手工协商。

IPSec 的实现

IPSec 通过如下两种协议来实现安全服务：

- **AH**（Authentication Header）是认证头协议，协议号为 51。主要提供的功能有数据源认证、数据完整性校验和防报文重放功能，可选择的认证算法有 MD5（Message Digest）、SHA-1（Secure Hash Algorithm）等。AH 报文头插在标准 IP 包头后面，保证数据包的完整性和真实性，防止黑客截获数据包或向网络中插入伪造的数据包。
- **ESP**（Encapsulating Security Payload）是报文安全封装协议，协议号为 50。与 AH 协议不同的是，ESP 将需要保护的用户数据进行加密后再封装到 IP 包中，以保证数据的机密性。常见的加密算法有 DES、3DES、AES 等。同时，作为可选项，用户可以选择 MD5、SHA-1 算法保证报文的完整性和真实性。

AH 和 ESP 可以单独使用，也可以联合使用。设备支持的 AH 和 ESP 联合使用的方式为：先对报文进行 ESP 封装，再对报文进行 AH 封装，封装之后的报文从内到外依次是原始 IP 报文、ESP 头、AH 头和外部 IP 头。

下文仅介绍 IPSEC 标准相关内容。

协议规范

我司产品实现以下 RFC 标准：

- 2401 Security Architecture for the Internet Protocol. S. Kent, R. Atkinson. November 1998. (Format: TXT=168162 bytes) (Obsoletes RFC1825) (Obsoleted by RFC4301) (Updated by RFC3168) (Status: PROPOSED STANDARD)
- 2402 IP Authentication Header. S. Kent, R. Atkinson. November 1998. (Format: TXT=52831 bytes) (Obsoletes RFC1826) (Obsoleted by RFC4302, RFC4305) (Status: PROPOSED STANDARD)
- 2403 The Use of HMAC-MD5-96 within ESP and AH. C. Madson, R. Glenn. November 1998. (Format: TXT=13578 bytes) (Status: PROPOSED STANDARD)

- 2404 The Use of HMAC-SHA-1-96 within ESP and AH. C. Madson, R. Glenn. November 1998. (Format: TXT=13089 bytes) (Status: PROPOSED STANDARD)
- 2405 The ESP DES-CBC Cipher Algorithm With Explicit IV. C. Madson, N. Doraswamy. November 1998. (Format: TXT=20208 bytes) (Status: PROPOSED STANDARD)
- 2406 IP Encapsulating Security Payload (ESP). S. Kent, R. Atkinson. November 1998. (Format: TXT=54202 bytes) (Obsoletes RFC1827) (Obsoleted by RFC4303, RFC4305) (Status: PROPOSED STANDARD)
- 3948 UDP Encapsulation of IPsec ESP Packets. A. Huttunen, B. Swander, V. Volpe, L. DiBurro, M. Stenberg. January 2005. (Format: TXT=30366bytes) (Status: PROPOSED STANDARD)

9.2 典型应用

典型应用	场景描述
通过 IPSEC VPN 将异地私网互联	通过 IPSEC VPN 建立隧道，连接异地局域网，不支持动态路由，只能静态路由方式建立网络
通过 L2TP OVER IPSEC 连入私网	通过 L2TP OVER IPSEC 方式建立隧道，连接异地局域网，适用动态 IP 上网的小型网络接入

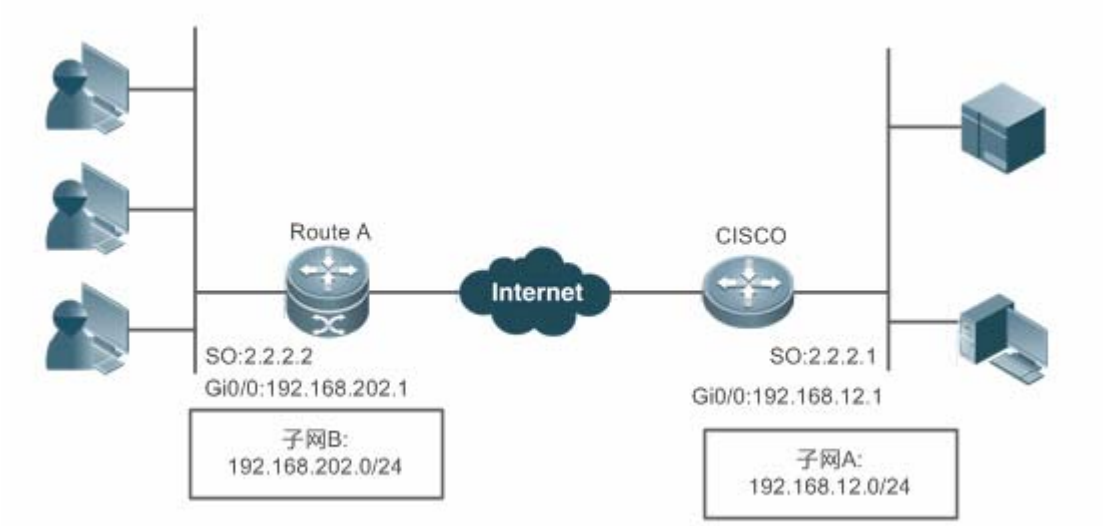
9.2.1 通过IPSEC VPN将异地私网互联

应用场景

子网 A 和子网 B 通过 IPSEC VPN 隧道互访

- RouteA 和 CISCO 设备通过广域网连接，IP 互相可达
- 子网 B 通过隧道，经由广域网，访问子网 A
- 子网 A 通过隧道，经由广域网，访问子网 B

图 9-1



【注释】 RouteA 是放在公网的网关设备
CISCO 是其他厂商设备放在公网做 VPN 网关

功能部属

- 通过 ADSL 或者其他形式连接至广域网
- 通过 IPSEC VPN 隧道实现内网路由互联

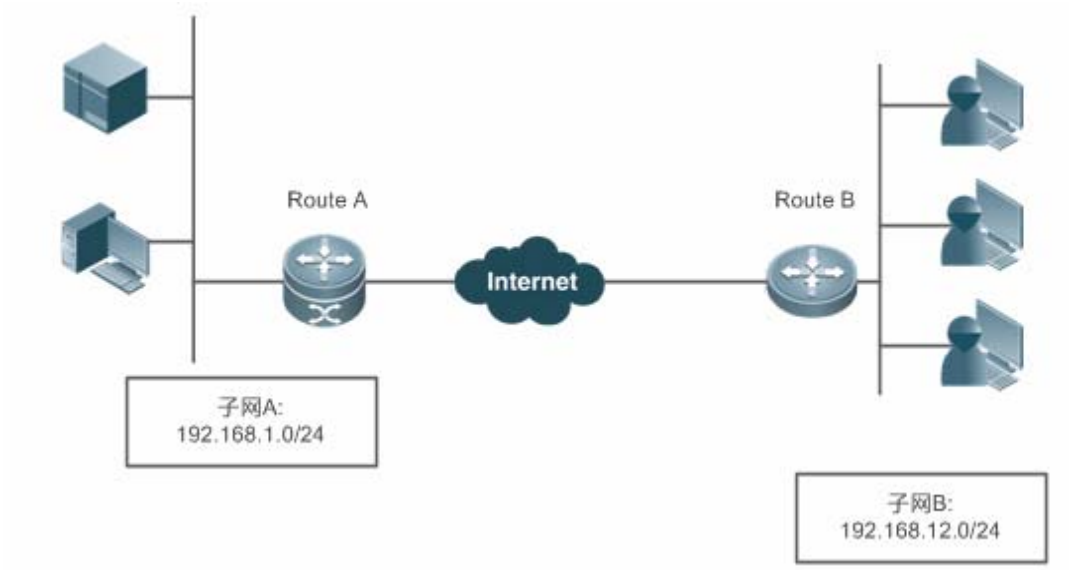
9.2.2 通过L2TP OVER IPSEC连入私网

应用场景

远端私网是 ADSL 拨号上网，IP 地址为动态，建立 VPN，连入私网。

通单独的 IPSEC VPN 效果类似。建立 L2TP OVER IPSEC 隧道，不受 IPSEC 隧道组播广播地址限制，也不受感兴趣流限制，可以 DHCP 分配地址，动态路由等方式建立网络，同样达到双向路由可达的效果。

图 9-2



【注释】 RouteA 是放在公网的网关设备
RouteB 通过动态地址上网的 VPN 网关设备

功能部属

- RouteB 和 RouteA 之间建立 IPSEC 隧道，保护地址是 L2TP 数据（udp1701）
- RouteB 通过拨 VPDN 连入私网
- 通过 AAA 分配地址，添加路由
- 通过 DHCP 分配子网地址
- 通过动态路由建立 RouteA 到 RouteB 的路由

9.3 功能详解

基本概念

↘ 安全联盟（Security Association，SA）

IPSec 在两个端点之间提供安全通信，端点被称为 IPSec 对等体。

SA 是 IPSec 的基础，也是 IPSec 的本质。SA 是通信对等体间对某些要素的约定，例如，使用哪种协议（AH、ESP 还是两者结合使用）、协议的封装模式（传输模式和隧道模式）、加密算法（DES、3DES 和 AES）、特定流中保护数据的共享密钥以及密钥的生存周期等。

SA 是单向的，在两个对等体之间的双向通信，最少需要两个 SA 来分别对两个方向的数据流进行安全保护。同时，如果两个对等体希望同时使用 AH 和 ESP 来进行安全通信，则每个对等体都会针对每一种协议来构建一个独立的 SA。

SA 由一个三元组来唯一标识，这个三元组包括 SPI（Security Parameter Index，安全参数索引）、目的 IP 地址、安全协议号（AH 或 ESP）。

SPI 是为唯一标识 SA 而生成的一个 32 比特的数值，它在 AH 和 ESP 头中传输。在手工配置安全联盟时，需要手工指定 SPI 的取值。使用 IKE 协商产生安全联盟时，SPI 将随机生成。

SA 是具有生存周期的，且只对通过 IKE 方式建立的 SA 有效。分为两种类型：

- 基于**时间**，定义一个 SA 从建立到失效的时间；
- 基于**流量**，定义一个 SA 允许处理的最大流量。

生存周期到达指定的时间或指定的流量，SA 就会失效。SA 失效前，IKE 将为 IPSec 协商建立新的 SA，这样，在旧的 SA 失效前新的 SA 就已经准备好。在新的 SA 开始协商而没有协商好之前，继续使用旧的 SA 保护通信。在新的 SA 协商好之后，则立即采用新的 SA 保护通信。

↘ 封装模式

IPSec 有如下两种工作模式：

- **隧道（tunnel）模式**：用户的整个 IP 数据包被用来计算 AH 或 ESP 头，AH 或 ESP 头以及 ESP 加密的用户数据被封装在一个新的 IP 数据包中。通常，隧道模式应用在两个安全网关之间的通讯。
- **传输（transport）模式**：只是传输层数据被用来计算 AH 或 ESP 头，AH 或 ESP 头以及 ESP 加密的用户数据被放置在原 IP 包头后面。通常，传输模式应用在两台主机之间的通讯，或一台主机和一个安全网关之间的通讯，不能用转发数据保护上。

↘ 认证算法与加密算法

(1) 认证算法

认证算法的实现主要是通过杂凑函数。杂凑函数是一种能够接受任意长的消息输入，并产生固定长度输出的算法，该输出称为消息摘要。IPSec 对等体计算摘要，如果两个摘要是相同的，则表示报文是完整未经篡改的。IPSec 使用两种认证算法：

- **MD5**：MD5 通过输入任意长度的消息，产生 128bit 的消息摘要。
- **SHA-1**：SHA-1 通过输入长度小于 2 的 64 次方 bit 的消息，产生 160bit 的消息摘要。

MD5 算法的计算速度比 SHA-1 算法快，而 SHA-1 算法的安全强度比 MD5 算法高。

(2) 加密算法

加密算法实现主要通过对称密钥系统，它使用相同的密钥对数据进行加密和解密。目前设备的 IPSec 实现三种加密算法：

- **DES**（Data Encryption Standard）：使用 56bit 的密钥对一个 64bit 的明文块进行加密。
- **3DES**（Triple DES）：使用三个 56bit 的 DES 密钥（共 168bit 密钥）对明文进行加密。
- **AES**（Advanced Encryption Standard）：使用 128bit、192bit 或 256bit 密钥长度的 AES 算法对明文进行加密。

这三个加密算法的安全性由高到低依次是：AES、3DES、DES，安全性高的加密算法实现机制复杂，运算速度慢。对于普通的安全要求，DES 算法就可以满足需要。

↘ 协商方式

有如下两种协商方式建立 SA：

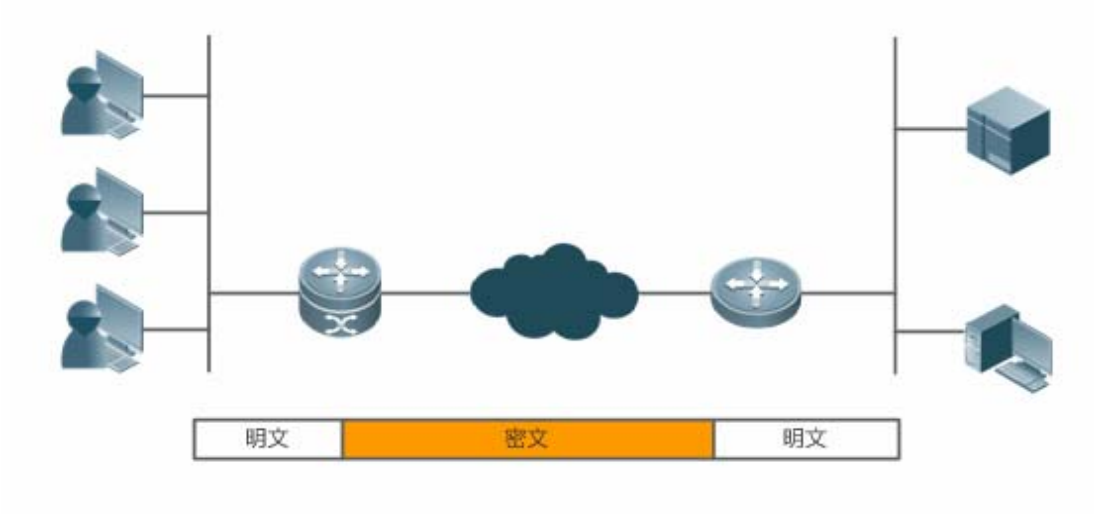
- **手工方式**（manual）配置比较复杂，创建 SA 所需的全部信息都必须手工配置，而且不支持一些高级特性（例如定时更新密钥），但优点是可以不依赖 IKE 而单独实现 IPSec 功能。
- **IKE 自动协商**（isakmp）方式相对比较简单，只需要配置好 IKE 协商安全策略的信息，由 IKE 自动协商来创建和维护 SA。

当与之进行通信的对等体设备数量较少时，或是在小型静态环境中，手工配置 SA 是可行的。对于中、大型的动态网络环境中，推荐使用 IKE 协商建立 SA。

安全隧道

安全隧道是建立在本端和对端之间可以互通的一个通道，它由一对或多对 SA 组成

图 9-3 是一个在子网间实施 IPSec 保护的例子：



IPSEC 模型要求：对感兴趣流检测按照优先级匹配，协议无法处理感兴趣流冲突的情况

功能特性

功能特性	作用	
配置 IPSEC 隧道	配置默认生命周期	密码安全性保证，隧道密码需要定期更新，周期可通过配置生命周期修改
	IPSec 隧道的 DF bit 覆盖功能	隧道封装后 DF 位控制
	创建加密访问列表	隧道封装对应的感兴趣流，只有感兴趣流内的数据进行封装
	定义变换集合	定义封装格式以及对应算法
	创建加密映射条目	定义隧道特性集合
	配置组播策略	Rfc 协议中隧道不支持组播报文，但某些设备实现并未过滤组播报文，根据实际情况调整封装逻辑，达到兼容效果

9.3.1 IPSEC隧道

工作原理

常见的手工隧道是通过 CLI 配置一些静态策略，创建隧道。

而 ISAKMP 自协商建立的隧道，是通过 IKE（后面章节消息描述）建立一个加密通道，在通过 IKE 隧道协商 IPSEC 隧道。IKE 隧道和 IPSEC 隧道互相独立，并没有直接的关联，IKE 隧道删除后，IPSEC 隧道仍然可以存在，IPSEC 隧道删除，IKE 隧道也可以独立存在。因此 IPSEC 隧道相关控制也仅对 IPSEC 隧道生效。

相关配置

配置默认生命周期

这是个可选步骤，可以通过这条命令来修改系统默认的生命周期值。若无特别说明，IKE 将采用该生命周期值进行协商，从而使 IPSec 的生命周期将不会超过默认生命周期的长度。

系统缺省的生命周期为通讯 1 小时（3600 秒）或通讯量达到 4,608,000KB（以每秒 10 兆字节的速度持续通信 1 小时），如果用户能接受缺省值，可以跳过此步骤。加密映射条目中若没有特别说明，将采用此默认生命周期。IKE 在协商 IPSec 的生命期的时候，取本地与对等体中的较小值。当 IPSec 安全联盟的生命到期时，IKE 将重新协商并为 IPSec 的安全联盟更换一套新的参数以及密钥，使其重新开始工作。

安全联盟（以及相关密钥）依据最先到期的生命周期超时：使用秒数（由 seconds 关键字指定）或传输通信量的千字节数（由 kilobytes 关键字指定）。手工建立的安全联盟（由标识为 ipsec-manual 的加密映射条目所建立）没有生命周期限制。

为了保证当原有安全联盟到期时，新安全联盟已经准备好交付使用，新安全联盟必须在原有安全联盟超时前被协商。新安全联盟在生命周期到期前 30 秒，或当通过这条通道的通信量离生命周期还差 256K 字节时（依据哪个对等体先达标）被协商。

如果在安全联盟的整个生命周期中没有通信通过这条通道，那么当生命周期超时的时候，该安全联盟将被释放，但不协商新安全联盟，在这种情况下，只有当 IPSec 看到另一个应当被保护的包时，新的安全联盟才会被协商。

系统默认有配置，一般情况下使用不需要修改，只有特殊场合下才会修改。

支持全局配置和针对某个加密映射集的配置

IPSec 隧道的 DF bit 覆盖功能

设置 IPSec 封装的 IP 报文是否允许分片。

DF bit 覆盖功能允许客户指定是否设备清 0，置 1，拷贝被封装的头。

IP 头上的 DF bit 决定设备是否可以分片，值为 1 时表示该报文不允许分片，为 0 则表示可以分片。IPsec 隧道模式下这个功能使得设备在全局或接口层上可以控制经过 IPSec 封装的报文 ip 头的 DF bit 是否根据原始的 ip 头的 DF bit 值而定。这个特征只有隧道模式才能支持。

默认情况下直接 clear 操作，允许分片。有特殊要求的场景中才需要配置

只支持全局配置

创建加密访问列表

配置加密访问列表就是告诉设备，要保护什么样的数据流。IPSec 需要依靠加密访问列表对进出的数据包进行过滤，对匹配的外出数据进行 IPSec 保护，而对匹配的进入包则检查它的合法性。

加密访问列表实际就是普通 acl list 配置，在加密映射条目里面引用。在静态配置情况下必须配置，动态模式可以学习，profile 可以通过隧道配置学习。

IPSec 加密映射条目指定的加密访问列表有以下四个主要功能：

- 引用 ACL list 中配置 deny 的内容不参加隧道协商，只是作为特殊内容，符合这些条目的不会被加密。
- 筛选使用 IPSec 进行加密保护的出站通信（permit=保护），镜像筛选策略自动生成，无需配置双方向
- 当开始协商 IPSec 安全联盟时，指示什么样的数据流由新的安全联盟进行保护
- 处理入站通信，其目的是过滤和丢弃那些本应受到 IPSec 保护而没有保护的通信。
- 在处理 IPSec 对等体发起的 IKE 协商时，决定是否接受代表所申请数据流的 IPSec 安全联盟申请（只有 ipsec-isakmp 加密映射条目需要协商）。必须确保两端对等体的访问列表匹配，我们建议，两端对等体访问列表配置成一致。

IPSec 需要依靠加密访问列表对进出的数据包进行过滤，对匹配的外出数据进行 IPSec 保护，而对匹配的进入包则检查它的合法性。同一个接口下，每个加密映射集都有不同的感兴趣流，不能冲突，否则后配置隧道无法转发数据。

感兴趣流只有动态模式不需要配置，其他情况必须配置。

定义变换集合

定义变换集合可以告诉设备，怎样保护数据流。变换集是特定安全协议和算法的组合，它指定了算法、安全协议和数据封装模式。用户需要对数据进行什么程度和要求的保护必须事先在这里定义对应的变换集合。

系统支持的所有变换组合如下：

算法组合	说明
ah-md5-hmac	AH 协议，MD5 HMAC 验证算法
ah-sha-hmac	AH 协议，SHA HMAC 验证算法
esp-des	ESP 协议，DES 加密算法
esp-3des	ESP 协议，3DES 加密算法
esp-aes-128	ESP 协议，aes 加密算法，密钥长度 128
esp-aes-192	ESP 协议，aes 加密算法，密钥长度 192
esp-aes-256	ESP 协议，aes 加密算法，密钥长度 256
ah-md5-hmac esp-des	AH 协议在外，使用 MD5 HMAC 验证算法；ESP 协议在内，使用 DES 加密算法
ah-sha-hmac esp-des	AH 协议在外，使用 SHA HMAC 验证算法；ESP 协议在内，使用 DES 加密算法
ah-md5-hmac esp-des esp-md5-hmac	AH 协议在外，使用 MD5 HMAC 验证算法；ESP 协议在内，使用 DES 加密算法和 MD5 HMAC 验证算法

ah-md5-hmac esp-null esp-md5-hmac	AH 协议在外，使用 MD5 HMAC 验证算法；ESP 协议在内，使用零加密算法和 MD5 HMAC 验证算法
ah-md5-hmac esp-des esp-sha-hmac	AH 协议在外，使用 MD5 HMAC 验证算法；ESP 协议在内，使用 DES 加密算法和 SHA HMAC 验证算法
ah-md5-hmac esp-null esp-sha-hmac	AH 协议在外，使用 MD5 HMAC 验证算法；ESP 协议在内，使用零加密算法和 SHA HMAC 验证算法
ah-sha-hmac esp-des esp-md5-hmac	AH 协议在外，使用 SHA HMAC 验证算法；ESP 协议在内，使用 DES 加密算法和 MD5 HMAC 验证算法
ah-sha-hmac esp-null esp-md5-hmac	AH 协议在外，使用 SHA HMAC 验证算法；ESP 协议在内，使用零加密算法和 MD5 HMAC 验证算法
ah-sha-hmac esp-des esp-sha-hmac	AH 协议在外，使用 SHA HMAC 验证算法；ESP 协议在内，使用 DES 加密算法和 SHA HMAC 验证算法
ah-sha-hmac esp-null sp-sha-hmac	AH 协议在外，使用 SHA HMAC 验证算法；ESP 协议在内，使用零加密算法和 SHA HMAC 验证算法
esp-des esp-md5-hmac	ESP 协议，采用 DES 加密算法和 MD5 HMAC 验证算法
esp-null esp-md5-hmac	ESP 协议，采用零加密算法和 MD5 HMAC 验证算法
esp-des esp-sha-hmac	ESP 协议，采用 DES 加密算法和 SHA HMAC 验证算法
esp-null esp-sha-hmac	ESP 协议，采用零加密算法和 SHA HMAC 验证算法
esp-3des	ESP 协议，3DES 加密算法
esp-3des esp-sha	ESP 协议，采用 3DES 加密算法和 SHA HMAC 验证算法
esp-3des esp-md5	ESP 协议，采用 3DES 加密算法和 MD5 HMAC 验证算法
ah-md5-hmac esp-des	AH 协议在外，使用 MD5 HMAC 验证算法；ESP 协议在内，使用 3DES 加密算法
ah-sha-hmac esp-des	AH 协议在外，使用 SHA HMAC 验证算法；ESP 协议在内，使用 3DES 加密算法
ah-md5-hmac esp-3des esp-sha	AH 协议在外，使用 MD5 HMAC 验证算法；ESP 协议在内，使用 3DES 加密算法和 SHA HMAC 验证算法
ah-sha-hmac esp-3des esp-sha	AH 协议在外，使用 SHA HMAC 验证算法；ESP 协议在内，使用 3DES 加密算法和 SHA HMAC 验证算法
ah-md5-hmac esp-3des esp-md5	AH 协议在外，使用 MD5 HMAC 验证算法；ESP 协议在内，使用 3DES 加密算法和 MD5 HMAC 验证算法

ah-sha-hmac esp-3des esp-md5	AH 协议在外，使用 SHA HMAC 验证算法；ESP 协议在内，使用 3DES 加密算法和 MD5 HMAC 验证算法

一般情况下，选择 esp-des（没有数据验证）组合就可以满足需求，如果您需要对数据进行验证，可以选择 esp-des esp-md5-hmac 或 esp-des esp-sha-hmac。

交换集合是必选项，必须配置，并且可以在多个加密映射集引用。同一个加密映射集可以配置多个交换集合，匹配过程按照优先级匹配，重复内容不影响协商结果

创建加密映射条目

创建加密映射条目就是将先前定义的访问列表和变换集合关联起来，并定义密钥，对等体地址，形成一套完整的 IPSec 方案描述。

加密映射集为必选，可以在多个接口引用。

配置组播策略

关闭对组播、广播报文的 IPSec 封装处理。

默认情况下只要满足感兴趣流配置，都会加密，无论是否组播报文

该配置可选。

将加密映射条目应用到接口上

这是一个激活定义 IPSec 方案的动作，将加密映射条目应用到接口上使加密映射集合在接口上开始工作。

创建 Profile 加密映射条目

要配置使用 IKE 来建立安全联盟的 Profile 加密映射条目

将 Profile 加密映射条目应用到 Tunnel 接口上

要将 Profile 加密映射集合应用于 Tunnel 接口

应用配置后激活隧道，在此之前隧道不影响数据转发

加密映射集只能应用到三层口，二层口如交换口无法配置

9.4 配置详解

配置项	配置建议 & 相关命令	
配置 IPSEC	**crypto ipsec security-association lifetime**	配置默认生命周期
	crypto ipsec df-bit	IPSec 隧道的 DF bit 覆盖功能
	access-list	创建加密访问列表
	crypto ipsec transform-set	定义变换集合
	crypto map **crypto ipsec profile**	创建加密映射条目
应用 IPSEC	**crypto map**	接口应用 IPSEC

9.4.1 配置IPSEC

配置效果

- 配置 IPSEC 隧道协商内容，建立隧道

注意事项

- 配置不完整不会发起协商
- 传输模式感兴趣流必须是 host to host，否则会自动按照隧道模式协商
- 感兴趣流冲突无法检测，静态配置按照配置顺序匹配，动态模式按照后建优先的方式匹配

配置方法

↘ 配置默认生命周期(可选)

- 这是个可选步骤，可以通过这条命令来修改系统默认的生命周期值。若无特别说明，IKE 将采用该生命周期值进行协商，从而使 IPSec 的生命周期将不会超过默认生命周期的长度。
- 系统默认有配置，一般情况下使用不需要修改，只有特殊场合下才会修改。
- 支持全局配置和针对某个加密映射集的配置

↘ IPSec 隧道的 DF bit 覆盖功能(可选)

- 设置 IPSec 封装的 IP 报文是否允许分片。
- 默认情况下直接 clear 操作，允许分片。有特殊要求的场景中才需要配置
- 只支持全局配置

↘ 创建加密访问列表

- 配置加密访问列表就是告诉设备，要保护什么样的数据流。IPSec 需要依靠加密访问列表对进出的数据包进行过滤，对匹配的外出数据进行 IPSec 保护，而对匹配的进入包则检查它的合法性。同一个接口下，每个加密映射集都有不同的感兴趣流，不能冲突，否则后配置隧道无法转发数据。
- 感兴趣流只有动态模式不需要配置，其他情况必须配置。
- 感兴趣流配置引用扩展 acl 配置，在加密映射集中引用。

↘ 定义变换集合

- 定义变换集合可以告诉设备，怎样保护数据流。变换集是特定安全协议和算法的组合，它指定了算法、安全协议和数据封装模式。用户需要对数据进行什么程度和要求的保护必须事先在这里定义对应的变换集合。
- 交换集合是必选项，必须配置，并且可以在多个加密映射集引用。同一个加密映射集可以配置多个交换集合，匹配过程按照优先级匹配，重复内容不影响协商结果

↘ 创建加密映射条目

- 创建加密映射条目就是将先前定义的访问列表和变换集合关联起来，并定义密钥，对等体地址，形成一套完整的 IPSec 方案描述。
- 加密映射集为必选，可以在多个接口引用。

检验方法

- 通过 **show crypto map** 显示配置完整性，如果显示内容表示配置完整
- 通过 **show crypto transform-set** 显示配置内容
- 通过 **show crypto map detail** 显示配置内容

相关命令

↘ 配置默认生命周期

【命令格式】 **crypto ipsec security-association lifetime** { **seconds** *seconds* | **kilobytes** *kilobytes* }

【参数说明】 *seconds*：安全联盟超时时间（秒）。缺省值为 3600 秒（1 小时）。可以配置 0，表示不启用时间超时功能

kilobytes：安全联盟的超时通信量（以千字节计）。缺省为 4,608,000KB。可配置为 0，表示不启用字节超时功能

【命令模式】 全局模式

【使用指导】 -

↘ IPSec 隧道的 DF bit 覆盖功能

【命令格式】 **crypto ipsec df-bit** { **clear** | **set** | **copy** }

【参数说明】 **clear：**外部 IP 头会把 DF Bit 清除，设备可能分片报文并加上 IPSEC 封装。

set：外部 IP 头会把 DF Bit 置 1，然而如果原始的 IP 头的 DF Bit 是清除的，设备可能会分片报文

copy：设备会把原始的 DF Bit 值作为 外部头的 DF Bit 值，copy 是缺省的。

【命令模式】 全局模式

【使用指导】 -

↘ 创建加密访问列表

【命令格式】 **access-list** *access-list-number* { **deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**log**]

【参数说明】 **deny:**忽略目标

permit:感兴趣目标

protocol：协议

source source-wildcar：感兴趣流源 ip/网段

destination destination-wildcard：目的 ip/网段

log:打开 acl log 功能

【命令模式】 全局模式

【使用指导】 从数据流的源目的地址及其通配符、通讯协议和通讯端口来描述数据流。使用 permit 关键字将使得满足指定条件的所有 IP 通信都受到相应加密映射条目中所描述策略的加密保护。使用 deny 关键字可以防止通信受到特定加密映射条目的加密保护。

定义变换集合

【命令格式】 **crypto ipsec transform-set** *transform-set-name transform1 [transform2 [transform3]]*

【参数说明】 *transform-set-name:*加密交换集名称

*transform1, transform2, transform3:*加密模式，验证模式

【命令模式】 全局模式

【使用指导】 1.集合是安全协议、算法以及将用于受 IPSec 保护的通信的其它设置的组合。在 IPSec 安全联盟协商过程中，对等体必须使用同一个特定的变换集合来保护特定的数据流。

2.配置多个变换集合，然后在加密映射条目中指定这些变换集合中的一个或多个。在加密映射条目中定义的变换集合用于协商 IPSec 安全联盟，以保护由加密映射条目对应的访问列表所指定的那些数据流。在协商过程中，双方对等体寻找一个在双方对等体上都有的相同变换集合。当找到了一个这样的变换集合时，此集合将被选中，并作为双方对等体 IPSec 安全联盟的一部分被运用到受保护的通信上。

3.是通过手工来建立安全联盟，由于手工建立的安全联盟不协商参数，因此必须两端对等体必须指定一个相同的变换集合。

【命令格式】 **mode** {**tunnel** | **transport**}

【参数说明】 **tunnel:**隧道模式

transport:传输模式

【命令模式】 加密交换集定义模式

【使用指导】 模式设置只对那些源和目标地址都是 IPSec 对等体的通信有用；对于其他通信无用（所有其他通信都在通道模式下进行）。

如果要被保护的通信具有和 IPSec 对等体相同的 IP 地址即那些源和目标地址都是 IPSec 对等体，并且指定了传输模式，那么在协商期间，设备将申请传输模式，但既可接受传输模式又可接受隧道模式。如果指定了通道模式，那么设备将申请通道模式，并且只接受通道模式。

创建加密映射条目

【命令格式】 **crypto map** *map-name seq-num* **ipsec-isakmp**

crypto ipsec profile *profile-name*

【参数说明】 加密映射集名称和优先级，profile 模式无优先级

【命令模式】 全局模式

【使用指导】 IPSEC 隧道必选参数配置都在加密映射集模式下配置，配置对端地址，加密交换集，引用感兴趣流等

【命令格式】 **match address** *access-list-id*

【参数说明】 访问列表编号（100-199，2000-2699，2900-3899），加密映射只使用 IP 扩展访问列表

【命令模式】 加密映射配置模式

【使用指导】 该命令指定加密映射条目的访问列表。加密映射条目使用访问列表来判断那些数据应该受到 IPSec 保护。

该命令指定的访问列表既用于出站通信也用于进站通信。在出站的情况下，检测到匹配的数据，如果已经有安全联盟，则对数据进行加密转发，如果没有建立安全联盟，将触发安全联盟协商（IKE）。在进站的情况下，

检测到匹配的数据，如果是已经加密的数据，那么进行解密，如果是没有加密的数据，直接丢弃。

【命令格式】 **set peer** { *hostname* | *ip-address* }
【参数说明】 *ip-address*:远程对等体的 IP 地址。
Hostname:远程对等体的主机名。
【命令模式】 加密映射配置模式
【使用指导】 对使用的加密映射都必须指定一个远程对等体。
可以配置多个，协商的时候会按照配置顺序发起协商，失败的时候更换下一个 peer 地址协商

【命令格式】 **set transform-set** *transform-set-name1* [*transform-set-name2…transform-set-name6*]
【参数说明】 引用加密交换集
【命令模式】 加密映射配置模式
【使用指导】 变换集合是安全联盟成功建立的必要条件。配置任何加密映射都必须使用该命令指定变换集合
可以配置多个，选择其中一个进行协商

9.4.2 应用IPSEC

配置效果

- 应用 IPSEC 配置到接口，创建隧道控制信息

注意事项

- 接口应用前，所有配置不生效
- IPSEC 隧道只能应用到三层接口上
- 同一个加密映射集可以使用到多个接口，相互独立

配置方法

↘ 将加密映射条目应用到接口上

- 这是一个激活定义 IPSec 方案的动作，将加密映射条目应用到接口上使加密映射集合在接口上开始工作。必选配置，只支持三层口。

检验方法

- 通过 **show crypto ipsec sa** 显示配置完整性，如果显示内容表示配置完整

- 通过 **show crypto map detail** 显示配置内容

相关命令

将加密映射条目应用到接口上

【命令格式】 **crypto map** *map-name*

【参数说明】 加密映射集名称

【命令模式】 接口配置模式

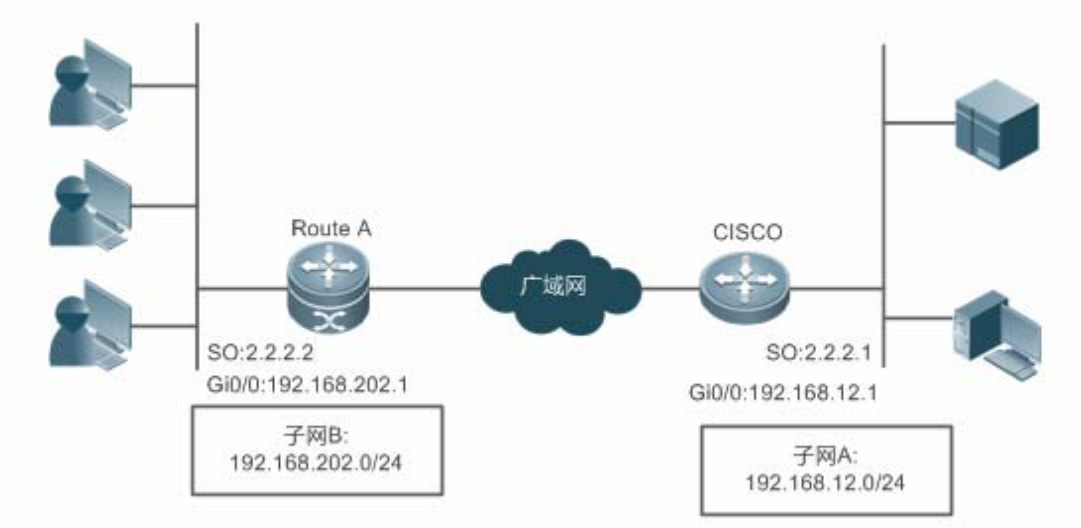
【使用指导】 使用此命令将加密映射集合应用于接口。要在接口上提供对数据进行 IPSec 加密保护，必须将一个加密映射集合应用于此接口。对于一个接口 ,只能关联一个加密映射集合。如果多个加密映射条目具有相同的 map-name 和不同的 seq-num，那么它们位于同一集合，并被应用于同一接口上，那么 Seq-num 越小的加密映射条目优先级越高，并且先进行判断。

配置举例

中心设备与远程设备连接采用 IPSEC

【网络环境】

图 9-4



【配置方法】

- IPSEC VPN 隧道是点对点加密隧道 ,隧道两端设备通过协商好的密钥进行数据加密解密 ,要建立 IPSEC VPN 隧道先要 IKE（配置密钥交换协议）
- RouteA 对应配置

RouteA

开放 IKE

```
Ruijie(config)#crypto isakmp enable
Ruijie(config)#crypto isakmp policy 1
Ruijie(isakmp-policy)#authentication pre-share
Ruijie(isakmp-policy)#encrytiong 3des
```

配置预共享密钥和变换集合

```
Ruijie(config)#crypto isakmp key 0 preword address 2.2.2.1
```

```
Ruijie(config)#crypto ipsec transform-set myset  esp-des esp-md5-hmac
```

定义一个加密映射集合

```
Ruijie(config)#crypto map mymap 5 ipsec-isakmp
Ruijie(config-crypto-map)# set peer 2.2.2.1
Ruijie(config-crypto-map)# set transform-set myset
Ruijie(config-crypto-map)# match address 101
```

将加密映射应用到接口

```
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#ip address 192.168.202.1 255.255.255.0
Ruijie(config)#interface Serial 0
Ruijie(config-if- Serial 0)#ip address 2.2.2.2 255.255.255.0
Ruijie(config-if- Serial 0)#encapsulation ppp
Ruijie(config-if- Serial 0)#crypto map mymap
```

定义加密访问列表，对 192.168.202.0/24 和 192.168.12.0/24 子网之间的 IP 通信进行保护

```
Ruijie(config)#access-list 101 permit ip 192.168.202.0 0.0.0.255 192.168.12.0 0.0.0.255
```

也可以通过手工模式建立隧道，同样可以达到加密隧道的效果，不过因为没有 IKE，密钥不会定期更新，安全性和易用性都要稍差一些

定义变换集合

```
Ruijie(config)#crypto ipsec transform-set myset  esp-des esp-md5-hmac
```

定义一个加密映射集合

```
Ruijie(config)#crypto map mymap 5 ipsec-manual
Ruijie(config-crypto-map)# set peer 2.2.2.1
Ruijie(config-crypto-map)# set session-key inbound esp 300 cipher abcdef1234567890 authenticator
abcdef1234567890abcdef1234567890
Ruijie(config-crypto-map)# set session-key outbound esp 301 cipher abcdef1234567890 authenticator
abcdef1234567890abcdef1234567890
Ruijie(config-crypto-map)# set transform-set myset
Ruijie(config-crypto-map)# match address 101
```

将加密映射应用到接口

```
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#ip address 192.168.202.1 255.255.255.0
Ruijie(config)#interface Serial 0
Ruijie(config-if- Serial 0)#ip address 2.2.2.2 255.255.255.0
Ruijie(config-if- Serial 0)#encapsulation ppp
Ruijie(config-if- Serial 0)#crypto map mymap
```

定义加密访问列表，对 192.168.202.0/24 和 192.168.12.0/24 子网之间的 IP 通信进行保护

```
Ruijie(config)#access-list 101 permit ip 192.168.202.0 0.0.0.255 192.168.12.0 0.0.0.255
```

监控和调试

使用 IKE 建立安全联盟的监控和调试

在子网 B 任一个主机上，发一个数据报文到子网 A 中，IKE 协商被触发，最后，成功建立 IPSec 安全联盟。

打开 IKE 和 IPSec 的调试开关：

```
RouterA# debug  crypto ipsec
IPSEC debugging is on
RouterA# debug  crypto isakmp
ISAKMP debugging is on
```

在协商的时候，可以看到以下调试信息：

```
Get acquire: 192.168.202.0/0.0.0.255 -> 192.168.12.0/0.0.0.255 , prot 0, port 0/0
Acquire negotiate with 2.2.2.1
(36) Beginning Quick Mode exchange, M-ID of 4445127
(36) sending packet to 2.2.2.1 (I) QM_SI1_WR1
ipsec_output:423, get item acclist 101
ipsec_output:429, match  3
(36) received packet from 2.2.2.1 (I) QM_SI1_WR1
payload format: <Hdr>,<hash> <sa> <nonce> <id>
(36) processing SA payload. message ID = 4445127
(36) Creating IPSec SAs.
inbound SA has spi 4445127
protocol esp, DES_CBC
auth MD5
outbound SA has spi 275385850
protocol esp, DES_CBC
auth MD5
lifetime of 3600 seconds, soft 3570 seconds
lifetime of 4608000 kilobytes, soft 256 kilobytes
ipsec_output:423, get item acclist 101
ipsec_output:429, match  3
(36) sending packet to 2.2.2.1 (I) QM_IDLE
(36) Phase_2 negotiate complete!
```

【检验方法】

RouteA

- 为了查看并确认 IKE 和 IPSec 的安全联盟是否已经建立，通过以下命令查看相关信息：

```
RouterA# show crypto isakmp sa
destination     source          state                   conn-id          lifetime(second)
2.2.2.1         2.2.2.2         QM_IDLE                 36               5013
```

从以上信息可以看出已经成功建立一个 IKE 安全联盟

```
RouterA# show crypto ipsec sa
Interface: Serial0
Crypto map tag:mymap, local addr  2.2.2.2  //目前的加密映射集名 mymap，使用本地地址 2.2.2.2
media mtu 1500
local  ident (addr/mask/prot/port): (192.168.202.0/0.0.0.255/0/0))
remote  ident (addr/mask/prot/port): (192.168.12.0/0.0.0.255/0/0))
PERMIT                //保护 192.168.202.0/24 和 192.168.12.0/24 之间的通信
```

```
current_peer: 2.2.2.1                          //对方对等体地址为 2.2.2.1
#pkts encaps: 3, #pkts encrypt: 3, #pkts digest 3
#pkts decaps: 3, #pkts decrypt: 3, #pkts verify 3
#send errors 0, #recv errors 0
//统计数据，依次为：封装包数，加密包数，摘要包数，拆封包数，加密包数，验证包数，发送错误，接收错误
inbound esp sas:                        //进入包处理的安全联盟，协议为 ESP
spi:0x43D3C7 (4445127)                                  //spi 的值为 4445127
transform: esp-des esp-md5-hmac            //变换集合为 esp-des-md5
in use settings={Tunnel,}                                  //通道模式
sa timing: remaining key lifetime (k/sec): (4607999/3578)
//离安全联盟的生命周期到期还有：4607999 千字节/3578 秒
IV size: 8 bytes                                        //IV 向量长度为 8
Replay detection support:Y                                 //抗重播处理
outbound esp sas:                       //外出包处理的安全联盟，协议为 ESP
spi:0x106A0DFA (275385850)                        //spi 的值为 275385850
transform: esp-des esp-md5-hmac           //变换集合为 esp-des-md5
in use settings={Tunnel,}                                  //通道模式
sa timing: remaining key lifetime (k/sec): (4607999/3577)
//离安全联盟的生命周期到期还有：4607999 千字节/3577 秒
IV size: 8 bytes                                        //IV 向量长度为 8
Replay detection support:Y                                 //抗重播处理
```

从统计数据可以看出，IPSec 已经建立起来并有数据报得到保护。

使用手工方式建立安全联盟的监控和调试

由于手工建立的安全联盟是一开始就起来的，不需要协商，无法查看调试信息，只能查看一些统计数据：

```
RouterA# show crypto ipsec sa
Interface: Serial0
Crypto map tag:mymap, local addr  2.2.2.2  //目前的加密映射集名 mymap，使用本地地址 2.2.2.2
media mtu 1500
local  ident (addr/mask/prot/port): (192.168.202.0/0.0.0.255/0/0))
remote  ident (addr/mask/prot/port): (192.168.12.0/0.0.0.255/0/0))
PERMIT                //保护 192.168.202.0/24 和 192.168.12.0/24 之间的通信
current_peer: 2.2.2.1                          //对方对等体地址为 2.2.2.1
#pkts encaps: 8, #pkts encrypt: 8, #pkts digest 8
#pkts decaps: 8, #pkts decrypt: 8, #pkts verify 8
#send errors 0, #recv errors 0
//统计数据，依次为：封装包数，加密包数，摘要包数，拆封包数，加密包数，验证包数，发送错误，接收错误
inbound esp sas:                        //进入包处理的安全联盟，协议为 ESP
spi: 0x12C (300)                                        //spi 的值为 300
transform: esp-des esp-md5-hmac            //变换集合为 esp-des-md5
```

```
in use settings={Tunnel,}                                    //通道模式
no sa timing                                                 //无生命周期
IV size: 8 bytes                                          //IV 向量长度为 8
Replay detection support:N                                //无抗重播处理
outbound esp sas:                        //外出包处理的安全联盟，协议为 ESP
spi: 0x12D (301)                                          //spi 的值为 301
transform: esp-des esp-md5-hmac              //变换集合为 esp-des-md5
in use settings={Tunnel,}                                    //通道模式
no sa timing                                                 //无生命周期
IV size: 8 bytes                                          //IV 向量长度为 8
Replay detection support:N                                //无抗重播处理
```

从统计数据可以看出，IPSec 已经建立起来并有数据报得到保护。

9.5 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
清空整个安全联盟数据库 ,这也将删除所有活动的安全线程	**clear crypto sa**
清空有特定对等体地址的安全联盟	**clear crypto sa peer** { *ip-address* | *peer-name* }
清空特定加密映射集合的安全联盟	**clear crypto sa map** *map-name*
清空有指定的<目的地址，协议，SPI>的安全联盟	**clear crypto sa spi** *destionation-address* { **ah** | **esp** } *spi*

查看运行情况

作用	命令
查看变换集合配置。	**show crypto ipsec transform-set**
查看全部或指定的加密映射配置。	**show crypto map** [*map-name*]
查看 IPSec 安全联盟信息。	**show crypto ipsec sa**
查看动态加密映射的信息。	**show crypto dynamic-map** [*tag map-name*]

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
显示关于 ipsec 事件的 debug 消息。	**debug crypto ipsec**

显示关于 ipsec 事件的 debug 消息。	**debug crypto engine**

10 IKE

10.1 概述

在实施 IPSec 的过程中，可以使用 IKE（Internet Key Exchange，因特网密钥交换）协议来建立 SA，该协议建立在由 ISAKMP（Internet Security Association and Key Management Protocol，互联网安全联盟和密钥管理协议）定义的框架上。IKE 为 IPSec 提供了自动协商交换密钥、建立 SA 的服务，能够简化 IPSec 的使用和管理，大大简化 IPSec 的配置和维护工作。

IKE 不是在网络上直接传输密钥，而是通过一系列数据的交换，最终计算出双方共享的密钥，并且即使第三者截获了双方用于计算密钥的所有交换数据，也不足以计算出真正的密钥。

IKE 在 IPSec 中的作用

- 因为有了 IKE，IPSec 很多参数（如：密钥）都可以自动建立，降低了手工配置的复杂度。
- IKE 协议中的 DH 交换过程，每次的计算和产生的结果都是不相关的。每次 SA 的建立都运行 DH 交换过程，保证了每个 SA 所使用的密钥互不相关。
- IPSec 使用 IP 报文头中的序列号实现防重放。此序列号是一个 32 比特的值，此数溢出后，为实现防重放，SA 需要重新建立，这个过程需要 IKE 协议的配合。
- 对安全通信的各方身份的的认证和管理 将影响到 IPSec 的部署。IPSec 的大规模使用 必须有 CA（Certificate Authority，认证中心）或其他集中管理身份数据的机构的参与。
- IKE 提供端与端之间动态认证。

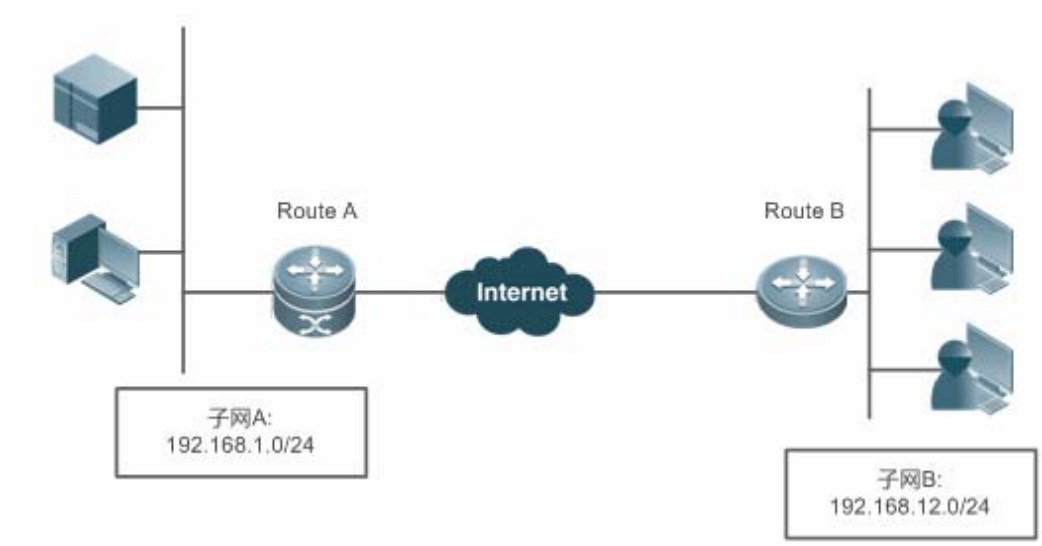
10.2 典型应用

10.2.1 建立动态VPN隧道

应用场景

汇聚侧不知道对端 IP 的情况下，建立星型拓扑的 VPN 隧道

图 10-1



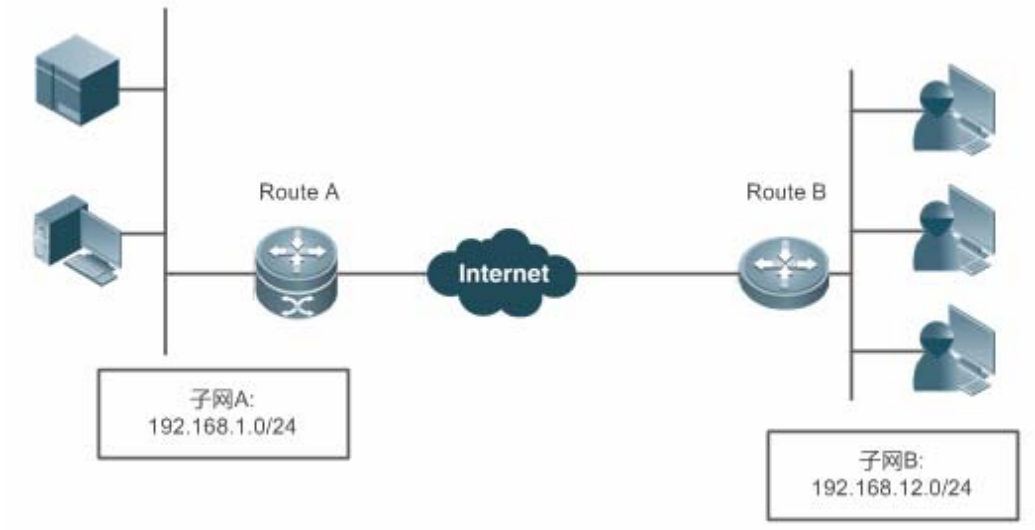
功能部属

- 通过 ADSL 或者其他形式连接至广域网
- 通过公共密钥建立 IKE 隧道
- 通过 IPSEC VPN 隧道实现内网路由互联
- 通过反向路由建立路由

10.2.2 使用域名建立隧道

接入侧不知道服务器 IP 的情况下，使用域名方式建立 IKE 隧道

图 10-2



功能部属

- 通过域名解析找到服务器 IP
- 通过域名作为认证 ID，查询预设密钥，互相认证设备，建立 IKE 隧道
- 通过 IPSEC VPN 隧道实现内网路由互联
- 通过反向路由建立路由

10.3 功能详解

IKE 的安全机制

IKE 具有一套自保护机制，可以在不安全的网络上安全地认证身份、分发密钥、建立 IPSec SA。

1. 数据认证

数据认证有如下两方面的概念：

- 身份认证：身份认证确认通信双方的身份。支持两种认证方法：预共享密钥（pre-shared-key）认证和基于 PKI 的数字签名（rsa-signature）认证。
- 身份保护：身份数据在密钥产生之后加密传送，实现了对身份数据的保护。

2. DH

DH（Diffie-Hellman，交换及密钥分发）算法是一种公共密钥算法。通信双方在不传输密钥的情况下通过交换一些数据，计算出共享的密钥。即使第三者（如黑客）截获了双方用于计算密钥的所有交换数据，由于其复杂度很高，不足以计算出真正的密钥。所以，DH 交换技术可以保证双方能够安全地获得公有信息。

3. PFS

PFS（Perfect Forward Secrecy，完善的前向安全性）特性是一种安全特性，指一个密钥被破解，并不影响其他密钥的安全性，因为这些密钥间没有派生关系。对于 IPSec，是通过在 IKE 阶段 2 协商中增加一次密钥交换来实现的。PFS 特性是由 DH 算法保障的。

IKE 的交换过程

IKE 使用了两个阶段为 IPSec 进行密钥协商并建立 SA：

(1) 第一阶段，通信各方彼此间建立了一个已通过身份认证和安全保护的通道，即建立一个 ISAKMP SA。第一阶段有主模式（Main Mode）和野蛮模式（Aggressive Mode）两种 IKE 交换方法。

(2) 第二阶段，用在第一阶段建立的安全隧道为 IPSec 协商安全服务，即为 IPSec 协商具体的 SA，建立用于最终的 IP 数据安全传输的 IPSec SA。

第一阶段主模式的 IKE 协商过程中包含三对消息：

- 第一对叫 SA 交换，是协商确认有关安全策略的过程；

- 第二对消息叫密钥交换，交换 Diffie-Hellman 公共值和辅助数据（如：随机数），密钥材料在这个阶段产生；
- 最后一对消息是 ID 信息和认证数据交换，进行身份认证和对整个第一阶段交换内容的认证。野蛮模式交换与主模式交换的主要差别在于，野蛮模式不提供身份保护，只交换 3 条消息。在对身份保护要求不高的场合，使用交换报文较少的野蛮模式可以提高协商的速度；在对身份保护要求较高的场合，则应该使用主模式。

工作原理

IKE 是一种密钥管理协议标准，与 IPSec 标准一起使用。IPSec 是提供稳健认证及 IP 包加密的一种 IP 安全功能。IPSec 可以不用 IKE 进行配置，然而，IKE 通过提供额外功能、灵活性以及使得 IPSec 标准更易于配置，从而增强了 IPSec 的功能。IKE 是一种混合协议，该协议在因特网安全联盟及密钥管理协议（ISAKMP）框架内实现了 Oakley 密钥交换和 Skeme 密钥交换（ISAKMP、Oakley 和 Skeme 是 IKE 实现的安全协议）。

要使 IKE 工作之前，必须对 IPSec 做好配置(依赖 IKE 的 IPSec)，并应用到接口。当在接口上检测到符合要求的外出的数据包时，IPSec 触发 IKE 和对等体 IKE 进行协商，它们在对等体之间建立一条安全的通道，传递所支持的各种 IPSec 参数，最终在两端建立一致的安全联盟，使双方的 IPSec 能够工作。经过一段时间，IPSec 安全联盟的生命期到达时，如果还有符合要求的数据需要传送，双方的 IKE 将重新开始协商 IPSec，这样周而复始。

使用 IKE 避免了在通信双方的加密映射表中手工指定所有的 IPSec 参数和密钥；能指定 IPSec 安全联盟的生命期限；使 IPSec 定期更换的密钥，增加安全性；IKE 使 IPSec 能提供抗重播服务。

功能特性

功能特性	作用	
IKE 隧道	开放或关闭 IKE	调试过程可暂时禁用 IKE 功能
	确保访问列表和 IKE 兼容	检查配置有效性
	创建 IKE 策略	IKE 协商策略配置
	选择工作模式	选择主模式，积极模式
	配置本地身份	本地身份是发出的 ID，需要和协商对象进行交互，需按照约定配置
	设置模式的自动识别	自动识别主模式积极模式
	配置预共享密钥	设置预共享密钥，可根据 ip，主机名等方式设定
	配置 DPD 检测	启用 DPD 功能，设置参数
	设置 IKE 的协商速率	IKE 协商速率的设定
	配置 nat 穿越超时参数	设置 nat 穿越参数

10.3.1 IKE隧道

工作原理

配置 IKE 协商参数，用于建立 IKE 隧道协商过程。

相关配置

开放或关闭 IKE

缺省时 IKE 功能是打开的。如果不想将 IKE 与 IPSec 实现一起使用，可以使用命令关闭它，但此时只有手工方式的 IPSec 安全联盟才能工作。

默认情况下，IKE 打开状态，特殊情况下通过命令关闭。

确保访问列表和 IKE 兼容

IKE 是运行在 UDP 上的应用程序，其通信报文为 UDP 数据，端口为 500。如果在设备上配置了访问列表（防火墙），并将此通信报文禁止，将导致 IKE 协商失败。所以，必须确保 IKE 的通信报文没有被禁止。

创建 IKE 策略

参与 IKE 协商的双方至少拥有一套一致的 IKE 策略，这是 IKE 协商成功的必要条件。必须在每台对等体上创建多个具有优先级的策略，以确保至少有一个策略能够匹配远程对等体的策略。

在每个 IKE 策略中定义以下五个参数：

参数	关键字	可取值	缺省值
加密算法	des	56 比特 DES-CBC	56 比特 DES-CBC
	3des	168 比特 3DES-CBC	
	aes	128 比特 AES-CBC	
HASH 算法	sha	SHA-1（HMAC 变体）	SHA-1（HMAC 变体）
	md5	MD5(HMAC 变体)	
验证方法	pre-share	预共享密钥	数字签名验证
	rsa-sig	数字签名验证	
Diffie-Hellman 组标识	1	768 比特 Diffie-Hellman 组	768 比特 Diffie-Hellman 组
	2	1024 比特 Diffie-Hellman 组	
	5	1536 比特 Diffie-Hellman 组	
IKE 安全联盟的生命期	空	1 分钟到一天内的秒数	一天（86400 秒）

IKE 协商开始时，IKE 试图去寻找在两个对等体上一致的策略。发起协商的一方将策略全部发送给远程响应方，响应方在接收到的另一端对等体的策略中按优先顺序寻找与本地匹配的策略。

当协商双方的策略均包括相同的加密、HASH、认证及 Diffie-Hellman 参数值，并且当远程对等体的策略所指定的生命周期小于或等于所比较的策略生命周期时作出匹配选择（如果没有指明生命周期，则将使用较短的远程对等体的策略生命周期）。如

果没有发现可接受的匹配策略，IKE 拒绝协商，从而不会建立 IPSec。如果找到一种匹配的策略，IKE 将完成协商，并且创建 IPSec 安全联盟。

可以在安全性和性能之间进行平衡，选择每个参数的值：

- 加密算法：当前支持 56 比特 DES-CBC,168 比特 3DES-CBC,128 比特 AES-CBC
- 哈氏算法：SHA-1 和 MD5。MD5 的摘要信息较少，通常认为要比 SHA-1 稍稍快一些。针对 MD5 的攻击被证明有一种方法是成功的，但极其困难，然而，由 IKE 使用的 HMAC 变体（MD5）能阻止这种攻击。
- 认证方法：RGOS 目前支持预共享方式验证和数字证书验证。采用预共享方式验证双方需要配置正确的预共享密钥，如果采用数字证书验证双方需要正确的证书配置（参看证书配置相应章节）。
- Diffie-Hellman 组标识三个选项：768 比特、1024 比特和 1536 比特 Diffie-Hellman。1024 比特 Diffie-Hellman 较难于攻克，但会占用更多的 CPU 时间。
- IKE 安全联盟的生命周期不同于 IPSec 的安全联盟的生命周期，它指的是 IKE 参数协商的有效期，可以设置为任意值。作为一条通用的规则，生命期越短（达到某一临界点），IKE 协商将越安全。然而，如果使用较长的生命期，新的 IPSec 安全联盟协商更快些。

可以创建多重 IKE 策略，每条策略对应不同的参数值组合。对所创建的每一条策略，需分配唯一的优先权（1 到 10000，1 是最高优先级）。

可以在每台对等体上配置多重策略，然而必须确保这些策略中的某条策略与远程对等体上的某个策略完全拥有一样的加密、HASH、认证及 Diffie-Hellman 参数值（生命期参数可以不一样）。如果不配置任何策略，则设备使用缺省的策略，该策略被设为最低优先级，并包含每个参数的缺省值。

在使用查看设备配置时，缺省策略和已经配置的策略的缺省值不会在配置中显示出来。要查看缺省策略和所配置的策略内的任何缺省值，请使用 show crypto isakmp policy 命令。

默认情况下系统默认提供一组优先级最低的 IKE 策略，缺省配置参见后面章节。

选择工作模式

工作模式有两种：主模式和积极模式（默认情况下是主模式）

配置本地身份

选择工作模式时主要用于设置发起方采用何种模式（主模式或积极模式）发起第一个协商消息，如果是主模式，此项配置不会影响协商。如果是积极模式，该项配置就指定了发起方第一个协商消息中的身份类型，直接影响积极模式的协商，目前可以制定三种形势：一、本地地址。二、域名。三、用户名@域名。

默认情况下预共享密钥协商采用 IP 地址作为 ID，而数字签名认证采用证书 DN 做 ID。某些厂商数字签名认证采用 IP 地址做 ID，遇到这种情况，可以通过手工指定 ID 类型方式兼容。也有其他情况，因为对端配置，需要本段配置做对应兼容修改。其余情况可以使用默认值。

该配置属于全局配置，不针对特定的隧道

设置模式的自动识别

设备作为中心，需要接受多种方式的拨入（有些采用主模式，有些采用积极模式），这样作为中心需要对这两种不同的发起都要做出响应并完成协商，所以该命令主要用于这种工作环境下，发起方配置该项命令没有影响。

默认情况下只能识别主模式协商，因为野蛮模式不保护 ID，安全性略低于主模式。某些设备默认使用野蛮模式发包，需要配置自动识别来兼容

配置预共享密钥

预共享密钥是参与 IKE 协商的两个对等体之间共同拥有的密钥，因此每个预共享密钥是对应一对 IKE 对等体。在给定的对等体上应当指定与共享的多重远程对等体相同的密钥；为了安全起见，最好在不同的对等体对之间配置不同的密钥。

预共享密钥协商必须配置，数字签名认证采用证书包含公私钥对，不需要配置。

配置 DPD 检测

目前 DPD 实现上采用了两种机制：一、on-demand 机制，该机制在隧道闲置时间超过配置的时间，此时有报文发送，会刺激发送 DPD 探测消息。二、periodic 机制，该机制是在超过配置的时间后就会主动发送 DPD 探测消息。最大重传次数 5 次。

DPD 功能默认不开启，配置参数后开启 DPD 功能。当链路不稳定的情况下，建议配置 DPD 功能。

设置 IKE 的协商速率

在几千路隧道同时进行协商的情况下，可能会导致协商无法收敛或者收敛较慢，继而使得整个协商过程耗时几个小时甚至更长。基于此不足，使用该命令限制协商速率，保证正在协商的隧道数量控制在一定的范围之内，提高协商效率。

IKE 协商限速功默认为打开状态，默认限速值为 1000，即同时最大允许 1000 路隧道协商。在大量隧道同时协商的情况下，如果采用默认限速值，协商速度依然很慢甚至协商不起来，可以调整限速值。也可以通过 crypto isakmp limit disable 关闭协商限速功能。

配置 nat 穿越超时参数

支持 RFC3947，IPSEC NAT-t，使用增加 UDP 头方式，解决 nat 穿透问题。为了避免 nat 连接超时，所以需要使用 keepalive 方式发送报文。不配置的情况下使用默认时间 5 分钟

NAT 穿越功能是协议自动判断，提供默认参数。配置需要根据 NAT 的配置情况修改，当没有数据的时候通过 keepalive 保证 NAT 转换记录有效，避免 NAT 重建重新分配端口导致隧道数据中断。

10.4 配置详解

配置项	配置建议 & 相关命令	
配置 IKE	**crypto isakmp enable**	开放或关闭 IKE
	crypto isakmp policy *priority*	创建 IKE 策略
	self-identity	配置本地身份
	crypto isakmp mode-detect	设置模式的自动识别
	crypto isakmp key	配置预共享密钥
	crypto isakmp keepalive	配置 DPD 检测
	crypto isakmp limit rate	设置 IKE 协商速率
	crypto isakmp nat	配置 nat 穿越超时参数

10.4.1 配置IKE

配置效果

- 配合 IKE 协商策略

注意事项

- IKE 策略优先级按照策略数字排序
- 默认策略编号为 65535，不配置的情况下使用默认策略

配置方法

↘ 开放或关闭 IKE(可选)

- 使用时，请确保 IKE 正在工作，而没有被关闭。
- 默认情况下，IKE 打开状态，特殊情况下通过命令关闭。

↘ 确保访问列表与 IKE 兼容

- 如果设备配置了访问列表，请确保没有将 IKE 的通讯流禁止。
- 如果出现冲突的会导致隧道数据转发异常，且系统无法自己发现，需要配置的人保证。

↘ 创建 IKE 策略

- 指定 IKE 协议使用的参数。属于全局配置
- 默认情况下系统默认提供一组优先级最低的 IKE 策略，缺省配置参见后面章节。

↘ 选择工作模式

- IKE 协商的时候存在两种工作模式（主模式和积极模式）（注：积极模式在某些文献上也称为野蛮模式）。
- 野蛮模式因为不保护 ID，但是协商报文少一些，根据情况选择。

↘ 配置本地身份(可选)

- 配置 IKE 协商过程中本地 ID 身份标识。
- 默认情况下预共享密钥协商采用 IP 地址作为 ID，而数字签名认证采用证书 DN 做 ID。某些厂商数字签名认证采用 IP 地址做 ID，遇到这种情况，可以通过手工指定 ID 类型方式兼容。也有其他情况，因为对端配置，需要本段配置做对应兼容修改。其余情况可以使用默认值。
- 该配置属于全局配置，不针对特定的隧道。

↘ 设置模式的自动识别(可选)

- 作为 IKE 协商的响应方，是否自动接受积极模式协商。
- 默认情况下只能识别主模式协商，因为野蛮模式不保护 ID，安全性略低于主模式。某些设备默认使用野蛮模式发包，需要配置自动识别来兼容。

配置预共享密钥

- IKE 和对等体之间共同的密钥。预共享密钥可以针对某一个特定 IP 或者某一个域名配置，同时支持通配密码。
- 预共享密钥协商必须配置，数字签名认证采用证书包含公私钥对，不需要配置。

配置 DPD 检测(可选)

- DPD 探测报文目前可配置成两种方式（on-demand 方式和 periodic 方式）。检测对端设备是否正常，解决隧道黑洞问题。
- DPD 功能默认不开启，配置参数后开启 DPD 功能。当链路不稳定的情况下，建议配置 DPD 功能。

设置 IKE 协商速率(可选)

- 设置 IKE 的协商速率，可以有效避免因大量隧道同时协商而导致的协商失败或者协商耗时较长。
- IKE 协商限速功默认为打开状态，默认限速值为 1000，即同时最大允许 1000 路隧道协商。在大量隧道同时协商的情况下，如果采用默认限速值，协商速度依然很慢甚至协商不起来，可以调整该限速值。也可以通过 crypto isakmp limit disable 关闭协商限速功能。

配置 nat 穿越超时参数(可选)

- nat-t 使用增加 udp 头方式解决 nat 穿越问题，为了避免 nat 上连接超时，需要使用 keepalive 报文保证 udp 连接一直存在。
- NAT 穿越功能是协议自动判断，提供默认参数。配置需要根据 NAT 的配置情况修改，当没有数据的时候通过 keepalive 保证 NAT 转换记录有效，避免 NAT 重建重新分配端口导致隧道数据中断。

检验方法

- 通过 show crypto policy 显示配置完整性，和对端配置是否一致

相关命令

开放或关闭 IKE(可选)

【命令格式】 **crypto isakmp enable**
【参数说明】 无
【命令模式】 全局模式
【使用指导】 缺省情况下，IKE 是打开的，故如果要使用 IKE 进行 IPSec 安全联盟协商，没有必要使用该命令。如果不使用 IKE 进行 IPSec 安全联盟协商，可以使用该命令的 **no** 形式关闭 IKE。

创建 IKE 策略

【命令格式】 **crypto isakmp policy** *priority*

【参数说明】 *priority:*优先级

【命令模式】 全局模式

【使用指导】 使用该命令指定在 IKE 协商进行 IKE 安全联盟的参数。执行该命令进入 IKE 策略配置模式。在 IKE 策略配置模式中，可以对以下参数进行设置：

encryption(IKE policy) ：缺省值=56 比特 DES-CBC

hash(IKE policy) ：缺省值=SHA-1

authentication(IKE policy) ：缺省值=RSA 签名

group(IKE policy) ：缺省值=768 比特

Diffie-Hellmanl lifetime(IKE policy) ：缺省值=86400 秒（1 天）

如果某个参数值没有指定，则将使用该参数的缺省值。在设备上可以配置多个 IKE 策略。在 IKE 协商开始时，它将试图找到在两端配置的公共策略，从远程对等体上所指定的最高优先级的策略开始。

【命令格式】 **encryption des | 3des | aes-128 | aes-192 | aes-256**

【参数说明】 **des**: 指定 56 比特的 DES-CBC 作为加密算法。

3des:指定 168 比特的 3DES-CBC 作为加密算法。

aes-128: 指定密钥长度为 128 比特的 AES 作为加密算法。

aes-192: 指定密钥长度为 192 比特的 AES 作为加密算法。

aes-256: 指定密钥长度为 256 比特的 AES 作为加密算法。

【命令模式】 IKE 策略配置模式

【使用指导】 该命令指定的数据加密算法是用于进行 IKE 安全联盟数据加密的，不同于 IPSec 安全联盟的加密算法，模式使用 3des

【命令格式】 **hash** {**sha** | **md5**}

【参数说明】 **sha:**指定 SHA-1(HMAC 变体)作为 HASH 算法。

md5:指定 MD5(HMAC 变体)作为 HASH 算法。

【命令模式】 IKE 策略配置模式

【使用指导】 使用该命令指定 IKE 策略中使用的 HASH 算法，默认使用 sha

【命令格式】 **authentication** {**pre-share | rsa-sig}**

【参数说明】 **pre-share：**预共享密钥

rsa-sig：数字证书

【命令模式】 IKE 策略配置模式

【使用指导】 目前 IKE 协商策略中验证方式默认采用数字签名验证，这与 Cisco 相同，如果希望采用预共享密钥方式验证则需要增加一个 IKE 策略（配置成预共享方式）

【命令格式】 **group** { **1 | 2 | 5 }**

【参数说明】 **1：**指定 768 比特 Diffie-Hellman 组

2：指定 1024 比特 Diffie-Hellman 组。

5：指定 1536 比特 Diffie-Hellman 组

【命令模式】 IKE 策略配置模式

【使用指导】 使用该命令指定 IKE 策略中使用的 group，默认使用 group 1

【命令格式】 **lifetime** *seconds*

【参数说明】 *seconds* :IKE 隧道超时时间

【命令模式】 IKE 策略配置模式

【使用指导】 使用该命令指定 IKE 安全联盟的生命周期。当 IKE 开始协商时，它所做的第一件事情是为其对话在安全参数上达成一致。这些一致的参数就在每个对等体上由 IKE 安全联盟引用，在每个对等体上保留直到 IKE 安全联盟生命期超时。

新的 SA 必须在当前 SA 失效之前协商。

由于 IPSec 安全联盟协商是建立在 IKE 安全联盟基础上的，因此，要节省协商 IPSec 安全联盟的时间，应配置较长的 IKE 安全联盟生命期。然而，被破解的可能性和生命周期是成正比的，即生命周期越长，被破解的可能性就越大，生命周期越短，被破解的可能性就小，因此要根据需要设置一个合适的生命周期（如半天）。

缺省 86400s

↘ 选择工作模式

【命令格式】 **set exchange-mode** { **main | aggressive** }

【参数说明】 **main :**主模式

aggressive :野蛮模式

【命令模式】 加密映射配置模式

【使用指导】 IKE 协商的过程中分为两个阶段：

第一个阶段——实现在两个 ISAKMP 实体之间建立安全的、经过验证的通道来进行通信，该阶段采用的模式有主模式和积极模式。

第二个阶段——主要是协商代表服务的安全联盟（SA）

而在第一个阶段中有两种工作模式，根据各自的优缺点，在默认的情况下，

我们采用主模式，但在 IP 地址不固定的情况下，可以使用积极模式。

↘ 配置本地身份(可选)

【命令格式】 **self-identity** { **address** | **trustpoint** *trustpoint* | **fqdn** *fqdn* | **user-fqdn** *user-fqdn* }

【参数说明】 本地 id 类型以及名称

address:本地 IP 地址

trustpoint : 指定本地证书

fqdn : 使用全称域名

user-fqdn:使用电子邮件地址

【命令模式】 全局模式

【使用指导】 主要用于完成积极模式发起协商中身份标识的设定，可以通过域名指定本地身份，也可以通过地址指定本地身份。

↘ 设置模式的自动识别(可选)

【命令格式】 **crypto isakmp mode-detect**

【参数说明】 无

【命令模式】 全局模式

【使用指导】 目前有做安全产品的厂商很多，各个商家在实现上并不是统一的，但是 IKE 的协商中的第一阶段工作模式只有两种，所以为了确保兼容性，采用以上命令针对无法完成对方发起 IKE 协商这种情况，自动采用积极模式完成协商。

配置预共享密钥

【命令格式】 **crypto isakmp key** { **0 | 7** } *keystring* { **hostname** *peer-hostname* | **address** *peer-address* [*mask*] }

【参数说明】 **address:**指定地址指定密钥

hostname:制定域名用密钥

【命令模式】 全局模式

【使用指导】 IKE 一般使用预共享协商，要使 IKE 成功建立 IKE 安全联盟，必须使用该命令在进行通讯的两个对等体上配置相同的预共享密钥。如果指定的对等体为一个网段，采用 mask 来标识它的子网掩码。当 peer-address 和 Mask 都为 0.0.0.0 时是配置默认的预共享密钥。

配置 DPD 检测(可选)

【命令格式】 **crypto isakmp keepalive** *seconds* [*retries*] [**on-demand | periodic**]

【参数说明】 *seconds:*检测时长

*retries:*检测间隔

periodic:间隔模式

on-demand:包触发模式

【命令模式】 全局模式

【使用指导】 默认情况下关闭，包触发模式可以减少额外开销，间隔模式时间反应要快一些，根据情况选择使用

设置 IKE 协商速率

【命令格式】 **crypto isakmp limit rate** *numbers*

【参数说明】 *numbers* 限速速率

【命令模式】 全局模式

【使用指导】 默认情况下限速功能为打开状态，默认限速值为 1000，可以根据实际情况修改该限速值，也可以使用 crypto isakmp limit disable 关闭限速功能。

配置 nat 穿越超时参数(可选)

【命令格式】 **crypto isakmp nat keepalive** *secs*

【参数说明】 *secs:*保活报文发送间隔

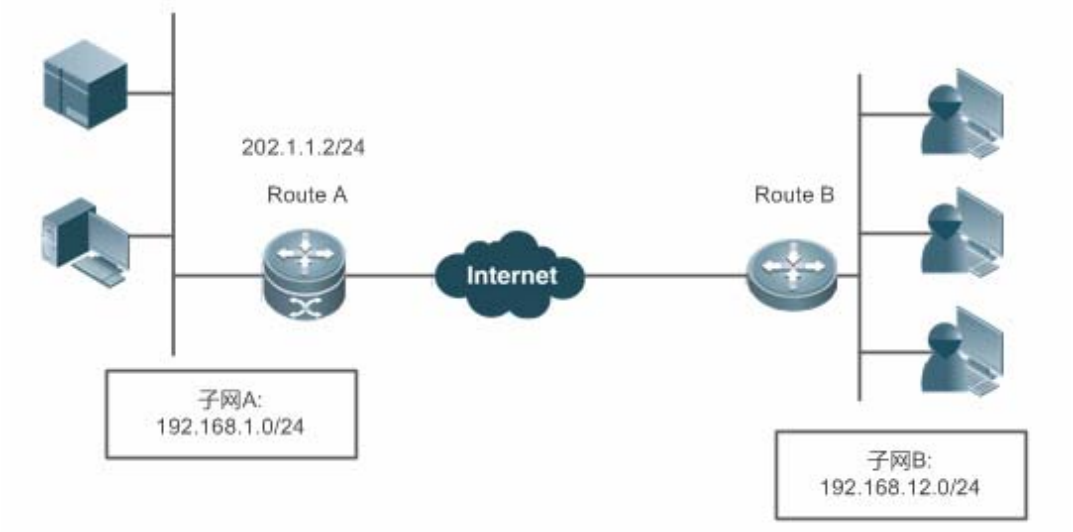
【命令模式】 全局模式

【使用指导】 支持 RFC3947，IPSEC NAT-t，使用增加 UDP 头方式，解决 nat 穿透问题。为了避免 nat 连接超时，所以需要使用 keepalive 方式发送报文。配置 crypto isakmp nat keepalive 命令指定用户配置的 keepalive 发送间隔，不配置的情况下使用默认时间 5 分钟。

配置举例

【网络环境】

图 10-3



该案例保护两个子网之间的 IP 数据通信，一边是锐捷路由器 A 作为中心网关，连接子网 A，另一边是锐捷路由器 B 作为分支网关，连接子网 B。要求实现以下要求：

- 采用通道模式
- 保护方式为 ESP-DES-MD5（提供加密和验证服务）。
- 路由器 A 的广域口 ip 是固定的:202.1.1.2/24，通过专线接入 Internet
- 路由器 B 通过 ADSL 线路用 pppoe 协议拨入 Internet ，ip 地址由 ISP 动态分配
- 采用预共享密钥，且中心路由器通过主机名指定预共享密钥

采用 IKE 建立安全联盟

【配置方法】

- IPSEC VPN 隧道是点对点加密隧道，隧道两端设备通过协商好的密钥进行数据加密解密，要建立 IPSEC VPN 隧道先要 IKE（配置密钥交换协议）
- RouteA 对应配置

RouteA

定义 IkE 策略，认证方法为预共享密钥，其他的参数采用默认值

```
Ruijie(config)#crypto isakmp policy 1
Ruijie(isakmp-policy)#authentication pre-share
```

配置默认的预共享密钥，由于对端的 ip 地址是动态的，通过指定 hostname 来找预共享密钥

```
Ruijie(config)#crypto isakmp key 0 preword hostname www.google.com
```

中心配置成模式自动识别

```
Ruijie(config)#crypto isakmp mode-detect
```

定义变换集合

```
Ruijie(config)#crypto ipsec transform-set myset esp-des esp-md5-hmac
```

定义动态加密映射

```
Ruijie(config)#crypto dynamic-map dymymap 5
Ruijie(config-crypto-map)#set transform-set myset
```

```
Ruijie(config-crypto-map)#match address 101
```

添加一个动态的加密映射集到静态的加密映射集

```
Ruijie(config)#crypto map mymap 10 ipsec-isakmp dynamic  dymymap
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#ip address 192.168.1.1 255.255.255.0
```

将加密映射应用到接口上

```
Ruijie(config)#interface serial 0
Ruijie(config-if-serial 0)#ip address 202.1.1.2 255.255.255.0
Ruijie(config-if-serial 0)#encapsulation ppp
Ruijie(config-if-serial 0)#crypto map mymap
Ruijie(config)#ip route 0.0.0.0 0.0.0.0  Serial0
```

定义加密访问列表，对 192.168.1.0/24 和 192.168.12.0/24 子网之间的 IP 通信进行保护

```
Ruijie(config)#access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.12.0 0.0.0.255
```

- RouterB 对应配置

开放 IKE

```
Ruijie(config)#crypto isakmp enable
```

配置本地身份

```
Ruijie(config)#self-identity fqdn www.google.com
```

定义 IkE 策略，认证方法为预共享密钥，其他的参数采用默认值

```
Ruijie(config)#crypto isakmp policy 1
Ruijie(isakmp-policy)#authentication pre-share
```

配置预共享密钥和变换集合

```
Ruijie(config)#crypto isakmp key 0 preword address 202.1.1.2
Ruijie(config)#crypto ipsec transform-set myset  esp-des esp-md5-hmac
```

定义一个加密映射集合

```
Ruijie(config)#crypto map mymap 5 ipsec-isakmp
Ruijie(config-crypto-map)#set peer 202.1.1.2
Ruijie(config-crypto-map)#set exchange-mode aggressive
Ruijie(config-crypto-map)#set transform-set myset
Ruijie(config-crypto-map)#match address 101
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#ip address 192.168.12.1 255.255.255.0
Ruijie(config)#interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#no ip addrsss
Ruijie(config-if-GigabitEthernet 0/1)#pppoe enable
Ruijie(config-if-GigabitEthernet 0/1)#pppoe-client 1 dial-pool-number 1 dial-on-demand
```

将加密映射应用到接口

```
Ruijie(config)#interface dialer 0
Ruijie(config-if-dialer 0)#mtu 1488
Ruijie(config-if-dialer 0)#ip address negotiate
Ruijie(config-if-dialer 0)#encapsulation ppp
Ruijie(config-if-dialer 0)#ppp pap sent-username xxx password xxx
Ruijie(config-if-dialer 0)#crypto map mymap
Ruijie(config-if-dialer 0)#dialer idle-timeout 2400
Ruijie(config-if-dialer 0)#dialer pool 1
Ruijie(config-if-dialer 0)#dialer-group 1
Ruijie(config)#dialer-list protocol ip permit
Ruijie(config)#ip route 0.0.0.0 0.0.0.0 Dialer0 permanent
```

定义加密访问列表，对 192.168.12.0/24 和 192.168.1.0/24 子网之间的 IP 通信进行保护

```
Ruijie(config)#access-list 101 permit ip 192.168.12.0 0.0.0.255 192.168.1.0 0.0.0.255
```

10.5 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 IKE 连接	**clear crypto isakmp** [*connection-id*]
清除 IPSecVPN 的登录注销日志	**clear crypto log**

查看运行情况

作用	命令
浏览所有 IKE 策略参数	**show crypto isakmp policy**
浏览所有当前 IKE 安全联盟	**show crypto isakmp sa**
浏览所有 IPSecVPN 的登录注销日志	**show crypto log**

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
显示关于 IKE 事件的 debug 消息	**debug crypto isakmp**

11 AAA

11.1 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网络资源的情况进行记账、统计、跟踪。

尽管 AAA 是最主要的访问控制方法，锐捷产品同时也提供了在 AAA 范围之外的简单控制访问，如本地用户名身份认证、线路密码身份认证等。不同之处在于它们提供对网络保护程度不一样，AAA 提供更高级别的安全保护。

使用 AAA 有以下优点：

- 灵活性和可控制性强
- 可扩充性
- 标准化认证
- 多个备用系统

协议规范

- 暂无相应规范

11.2 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

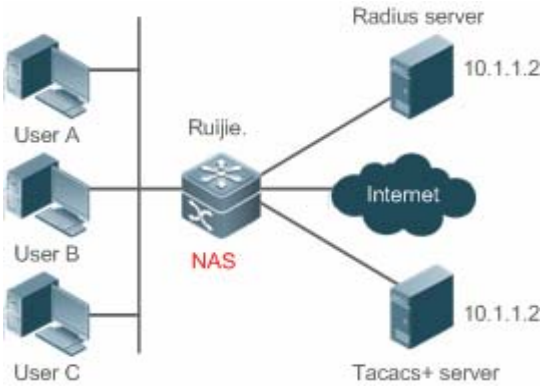
11.2.1 无域环境下的认证、授权、记账

应用场景

在 图 11-1 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：

3. 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。
4. 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。
5. 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。
6. 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。
7. 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 11-1



【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

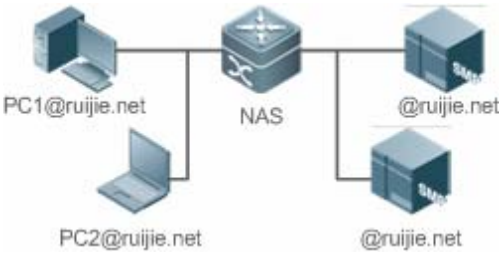
11.2.2 多域环境下的认证、授权、记账

应用场景

通过配置网络访问控制器设备实现基于域名的 AAA 服务，包括认证、授权、记账功能：

- 使用 802.1x 客户端进行登录认证，使用用户名为 PC1@ruijie.net 或 PC2@ruijie.com.cn，再输入正确的密码进行认证就可认证成功。
- 对用户进行分权限管理：把网络管理用户分为超级用户和普通用户。其中，超级用户对网络设备拥有查看和配置的权限，普通用户对网络设备只拥有特定的查看权限。
- 认证服务器端可将用户的认证信息、授权信息和网络行为记录在服务器中，以供日后查看和审计。

图 11-2



【注释】 PC1@ruijie.net，PC2@ruijie.com.cn 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。
SAM 为锐捷公司提供的通用 RADIUS 服务器。

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 上定义 AAA 服务的方法列表
- 在 NAS 上打开基于域名的 AAA 服务开关
- 在 NAS 上创建域并配置域属性集

11.3 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。

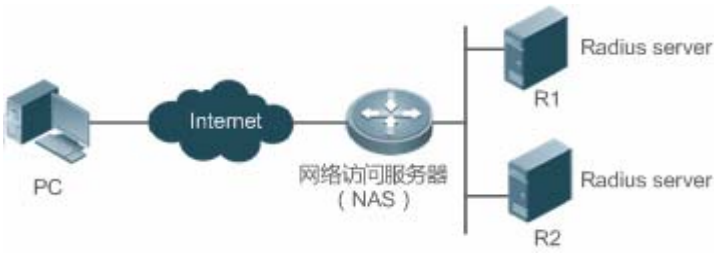
方法列表

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 11-3



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
AAA 多域	针对不同域的用户，创建认证、授权和记账方案。

11.3.1 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。

- PPP 认证

针对 PPP 拨号接入用户进行身份认证。

- iportal（内置 portal）认证

针对使用一代 portal 服务器来进行身份认证。

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。

11.3.2 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，则需要在 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。

11.3.3 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（如 802.1X、WEB 认证等用户）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。

11.3.4 AAA多域

在多域环境下，同一台网络访问服务器（NAS）设备可为不同域中的用户提供 AAA 服务，各域中用户的属性（例如用户名及密码、服务类型、权限等）有可能各不相同，因此有必要通过设置域的方法把它们区分开，并为每个域单独配置包括 AAA 服务方法列表（例如使用的 RADIUS）在内的属性集。

本产品支持以下几种的形式的用户名

8. userid@domain-name
9. domain-name\userid
10. userid.domain-name
11. userid

对于第 4 种不带 domain-name 的形式的用户名（即以上第 4 种：userid），认为其域名称为 default，即为默认的域名。

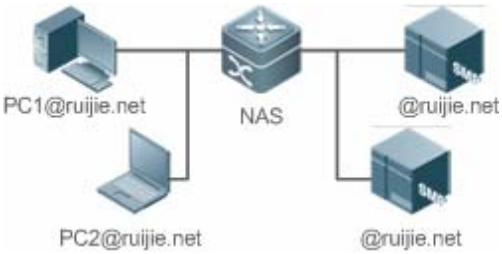
设备基于域名的 AAA 服务基本原理如下：

- 解析用户携带的域名称
- 根据域名称查找用户所配置的域
- 根据设备上域配置信息查找相应的 AAA 服务的方法列表名
- 根据方法列表名在系统中查找对应的方法列表
- 使用该方法列表提供 AAA 服务

上述任何一个步骤失败，用户将无法使用申请的 AAA 服务。

以下是典型的多个域环境拓扑图：

图 11-4



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。

定义 AAA 服务的方法列表

缺省情况下，没有配置任何 AAA 服务的方法列表。

配置方法列表请参照 5.2.1、5.2.2、5.2.3 章节

启用基于域名的 AAA 服务

缺省情况下，基于域名的 AAA 服务没有启动。

使用 **aaa domain enable** 命令可以启动基于域名的 AAA 服务。

创建域

缺省情况下，没有配置任何域。

使用 **aaa domain** *doman-name* 命令配置域名。

配置域属性集

缺省情况下，没有域属性集。

域属性集包括该域使用的认证、授权、记账方法列表；域的同时在线人数；是否去除用户名中的域名；域是否生效等。

查看域配置

使用 **show aaa domain** 查看域配置

系统最多支持配置 32 个域。

11.4 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。

11.4.1 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。

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。

定义 PPP 认证的方法类型和执行顺序。

- 使用命令 **aaa authentication ppp** 配置 ppp 认证的方法类型和执行顺序。
- 如果为 PPP 拨号用户配置认证方法列表，则必须配置此命令。
- 缺省情况下，没有配置 ppp 认证方法列表。

定义 Web 认证的方法类型和执行顺序。

- 使用命令 **aaa authentication web-auth** 配置 Web 认证的方法类型和执行顺序。
- 如果为 Web 认证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 Web 认证方法列表。

定义内置 Web 认证的方法类型和执行顺序。

- 使用命令 **aaa authentication iportal** 配置内置 Web 认证的方法类型和执行顺序。
- 如果为内置 Web 认证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，没有配置内置 Web 认证方法列表。

定义 SSLVPN 认证的方法类型和执行顺序。

- 使用命令 **aaa authentication sslvpn** 配置 Web 认证的方法类型和执行顺序。
- 如果为 SSLVPN 认证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 SSLVPN 认证方法列表。

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。

设置 Web 认证或者内置 Web 认证的情况下，本地账户（username 或者 subs）的能否被多个终端共享。

- 可选配置，该配置仅在 EG 系列产品上支持，其他产品默认支持本地账户可被多个终端共享。
- 缺省情况下，本地账户不能被多个终端共享。

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、dot1x 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、subs”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。

subs：**使用 subs 数据库进行身份认证。**

【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。

↘ 定义 PPP、Web 认证、内置 Web 认证和 SSLVPN 认证的方法类型和执行顺序。

【命令格式】 **aaa authentication** { **ppp | iportal** | **sslvpn** } { **default** | *list-name* } *method1* [*method2*...]

【参数说明】 **ppp**：**配置 PPP 拨号认证的方法列表。**

iportal：**配置内置 Web 认证的方法列表。**

sslvpn：**配置 SSLVPN 认证的方法列表。**

default：使用该参数，则后面定义的方法列表作为 PPP 认证的默认方法。

list-name：定义一个 PPP 认证的方法列表，可以是任何字符串。

method：必须是“local、none、group、subs”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。

subs：**使用 sub 数据库进行身份认证。**

【命令模式】 全局模式

【使用指导】 如果设备启用 AAA PPP 安全服务，用户就必须使用 AAA 进行 PPP 用户认证协商。您必须使用 **aaa authentication ppp** 命令配置默认的或可选的方法列表用于 PPP 用户认证。

只有前面的方法没有响应，才能使用后面的方法进行认证。

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。

设置 login 用户被锁定的时间长度。

【命令格式】 **aaa local user allow public account**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 Web 认证或者内置 Web 认证的情况下，本地账户（username 或者 subs）的能否被多个终端共享。

配置举例

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 11-5



【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 11-6



【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。如果使用 enable 密码认证，则需要在 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。

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#
```

AAA 802.1x 认证配置示例。对 802.1x 接入用户先用 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 11-7



【配置方法】 第一步：开启 AAA。

第二步：如果用户使用远程服务器认证，则需要先配置 RADIUS 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）。目前，802.1X 认证不支持使用 TACACS+认证。

第三步：根据不同接入用户类型（本例为 802.1x 接入用户），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：应用 AAA 认证方法。如果使用的是 default 认证方法，则可不必配置该步骤。

第五步：接口开启 802.1x 认证功能。

NAS

```
Ruijie#configure terminal
Ruijie(config)#username user1 password  pass1
Ruijie(config)#username user2 password  pass2
Ruijie(config)#aaa new-model
Ruijie(config)#radius-server host 10.1.1.1
Ruijie(config)#radius-server key ruijie
Ruijie(config)#aaa authentication dot1x default group radius local
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-gigabitEthernet 0/1)#dot1 port-control auto
Ruijie(config-if-gigabitEthernet 0/1)#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 dot1x default group radius local

Accounting method-list:

Authorization method-list:
```

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。

11.4.2 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。

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）。目前是对于通过了 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对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

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 11-8



【配置方法】 第一步：开启 AAA。

第二步：如果用户使用远程服务器授权，则需要先配置 RADIUS 或 TACACS+服务器。如果使用 local 授权，则需要在 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。

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 11-9



【配置方法】 第一步：开启 AAA。

第二步：如果用户使用远程服务器授权，则需要先配置 RADIUS 或 TACACS+服务器。如果使用 local 授权，则需要在 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 11-10



【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

11.4.3 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。

定义 network 记账的方法类型及方法执行顺序。

- 使用命令 **aaa accounting network** 配置 network 记账的方法类型及方法执行顺序。
- 如果要为 network 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。
- 缺省情况下，没有配置记账方法。

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，则可不必配置此命令。
- 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，则可不必配置此命令。
- 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。

定义 network 记账的方法类型及方法执行顺序。

【命令格式】 **aaa accounting network** { **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 network 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。

start-stop：在用户访问活动开始和结束时均发送记账报文，开始记账报文无论是否成功启用记账，都允许用户开始进行网络访问。

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 network 记账。

group：使用服务器组进行 network 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 通过给安全服务器发送记录属性对来用户活动进行记账。使用关键字 **start-stop**，制定用户记账选项。

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间隔。

配置举例

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 11-11



【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 11-12



【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
```

↘ 配置 network 记账。为 802.1x 用户配置记账方法列表，采用 RADIUS 远程服务器认证和记账。

【网络环境】

图 11-13



【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 服务器。

第三步：根据不同接入方式和服务类型，配置 AAA 方法列表。

第四步：应用方法列表。如果使用的是 default 认证方法，则可以不必配置该步骤。

802.1X 用户在认证通过后才能进行记账。

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 dot1x aut1x group radius local
Ruijie(config)#aaa accounting network acc1x start-stop group radius
Ruijie(config)#dot1x authentication aut1x
Ruijie(config)#dot1x accounting acc1x
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#dot1 port-control auto
Ruijie(config-if-GigabitEthernet 0/1)#exit
```

【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 dot1x aut1x group radius local
Accounting method-list:
aaa accounting network acc1x start-stop group radius
Authorization method-list:
```

常见配置错误

无

11.4.4 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 sever 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。

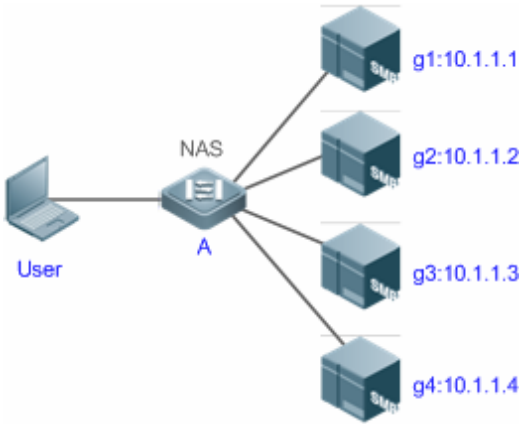
配置举例

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 11-14



【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。

11.4.5 配置基于域名的AAA服务

配置效果

针对不同域的 802.1x 用户，创建认证、授权和记账方案。

注意事项

关于域中引用方法列表：

- 在域配置模式下，选择 AAA 服务方法列表时，这些方法列表是在进入域配置模式前已经定义；否则在域配置模式下，允许选择 AAA 方法列表名，但提示配置不存在。
- 域选择的 AAA 服务方法列表名称必须和 AAA 服务所定义的方法列表名称必须一致。若不一致，不能够为该域中的用户提供合适的 AAA 服务。

关于缺省域：

- 缺省域（default）：在基于域名的 AAA 服务开关打开情况下，如果用户没有携带域信息，则使用缺省域。如果用户携带的域在系统中没有配置，则判定为非法用户，不提供 AAA 服务。初始时没有配置 default 域，需要手工指定创建。
- 基于域名的 AAA 服务开关打开时，默认情况下没有配置缺省域，需要手动配置完成。缺省域的名称为“default”，若配置缺省域后，用户不携带域信息时，使用缺省域进行提供 AAA 服务。若缺省域没有配置，则未携带域信息的用户不能使用 AAA 服务。

关于域名：

- 用户所携带的域名称与设备上所配置的域名的匹配采用最准确匹配。例如：设备上配置了 domain.com 和 domain.com.cn 两个域，一个用户的请求信息携带为 aaa@domain.com。则设备认为会判定该用户所属于的域为 domain.com 而不是域 domain.com.cn。
- 如果认证用户携带有域信息，而域没有在设备上配置，不能为该用户提供 AAA 服务。

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。

开启基于域名的 AAA 服务。

- 必选配置。
- 使用 **aaa domain enable** 开启基于域名的 AAA 服务。
- 缺省情况下，基于域名的 AAA 服务关闭。

创建域，并进入域配置模式。

- 必选配置。
- 使用 **aaa domain** 命令创建域或者进入已配置的域。
- 缺省情况下，没有配置任何域。

在域中，关联 802.1X 认证方法列表。

- 使用 **authentication dot1x** 命令关联 802.1x 认证方法列表。
- 如果要在域中应用指定的 801.1x 认证方法，则必须配置此命令。

- 目前基于域名的 AAA 服务，仅被应用于 802.1x 接入服务。

在域中，关联 Network 记账方法列表。

- 使用 **accounting network** 命令关联 network 记账方法列表。
- 如果要在域中应用指定的记账方法，则必须配置此命令。
- 如果域中没有关联方法列表，则默认使用全局的 default 方法列表进行记账。

在域中，关联 Network 授权方法列表。

- 使用 **authorization network** 命令关联 network 授权方法列表。
- 如果要在域中应用指定的授权方法，则必须配置此命令。
- 如果域中没有关联方法列表，则默认使用全局的 default 方法列表进行授权。

设置域的状态。

- 可选配置
- 当域的状态为 block 时，属于该域的用户不能登录。
- 缺省情况下，当域被创建以后，其状态为 active，即允许任何属于该域的用户请求网络服务。

设置是否在用户名中携带域名信息。

- 可选配置
- 缺省情况下，NAS 与服务器交互时用户名中携带域信息。

设置当前域可容纳接入用户的数目限制。

- 可选配置
- 缺省情况下，不对当前域可容纳的接入用户数作限制。

检验方法

使用命令 **show aaa domain** 查看配置的域信息是否生效。

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。

开启基于域名的 AAA 服务。

【命令格式】 **aaa domain enable**
【参数说明】 无
【命令模式】 全局模式
【使用指导】 进行基于域名的 AAA 服务配置，需要打开这个配置开关。

↘ 创建域，并进入域配置模式。

【命令格式】 **aaa domain** { **default** | *domain-name* }
【参数说明】 **default**：使用该参数，进行缺省域的配置
domain-name：指定域的名称
【命令模式】 全局模式
【使用指导】 指定基于域名的 AAA 服务配置。default 为缺省域配置，也就是如果用户没有携带域信息，网络设备所使用的方法列表。*domain-name* 为指定域名配置，如果用户携带该域名，则指定使用这个域所关联的方法列表。目前系统支持最多配置 32 个域。

↘ 在域中，关联 802.1X 认证方法列表。

【命令格式】 **authentication dot1x** { **default** | *list-name* }
【参数说明】 **default**：使用该参数，指定使用缺省配置方法列表
list-name：指定方法列表名称
【命令模式】 域配置模式
【使用指导】 为域指定一个 802.1x 认证方法列表。

↘ 在域中，关联 web 认证方法列表。

【命令格式】 **authentication web-auth** { **default** | *list-name* }
【参数说明】 **default**：使用该参数，指定使用缺省配置方法列表
list-name：指定方法列表名称
【命令模式】 域配置模式
【使用指导】 为域指定一个 webauth 认证方法列表。

↘ 在域中，关联 Network 记账方法列表。

【命令格式】 **accounting network** { **default |** *list-name* }
【参数说明】 **default**：使用该参数，指定使用缺省配置方法列表
list-name：指定方法列表名称
【命令模式】 域配置模式
【使用指导】 为域指定使用的 Network 记账方法列表。

↘ 在域中，关联 Network 授权方法列表。

【命令格式】 **authorization network** { **default** | *list-name* }
【参数说明】 **default**：使用该参数，指定使用缺省配置方法列表
list-name：指定方法列表名称
【命令模式】 域配置模式
【使用指导】

设置域的状态。

【命令格式】 **state** { **block** | **active** }

【参数说明】 **block**：配置的域无效

active：配置的域有效

【命令模式】 域配置模式

【使用指导】 指定配置的域是否有效。

设置是否在用户名中携带域名信息。

【命令格式】 **username-format** { **without-domain** | **with-domain** }

【参数说明】 **without-domain**：剥离域信息

with-domain：不剥离域信息

【命令模式】 域配置模式

【使用指导】 在域配置模式下，配置 NAS 针对指定域与服务器交互时，用户名中是否携带域信息。

设置当前域可容纳接入用户的数目。

【命令格式】 **access-limit** *num*

【参数说明】 *num*：域用户的数量限制，只限制 802.1x 用户

【命令模式】 域配置模式

【使用指导】 使用该命令对域的用户数量进行限制。

配置举例

以下配置举例，仅介绍与多域 AAA 相关的配置。

配置基于域的 AAA 认证记账服务。实现使用 RADIUS 服务器对通过 NAS 接入的 802.1X 域用户（用户名为 user@domain.com）进行认证和记账。NAS 向服务器发送的用户名不携带域名，不限制接入用户数。

【网络环境】

图 11-15



【配置方法】 本例使用 RADIUS 认证和记账，需要提前配置 RADIUS 服务器。

第一步：开启 AAA

第二步：定义 AAA 服务的方法列表

第三步：开启基于域名的 AAA 服务

第四步：创建域

第五步：在指定域中关联 AAA 方法列表

第六步：设置域属性

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 authentication dot1x default group radius
Ruijie(config)#aaa accounting network list3 start-stop group radius
Ruijie(config)# aaa domain enable
Ruijie(config)# aaa domain domain.com
Ruijie(config-aaa-domain)# authentication dot1x default
Ruijie(config-aaa-domain)# accounting  network list3
Ruijie(config-aaa-domain)# username-format without-domain
```

【检验方法】 在 NAS 设备上，通过 **show run**、**show aaa domain** 命令查看配置效果。

NAS

```
Ruijie#show aaa domain domain.com

=============Domain domain.com=============
State: Active
Username format: With-domain
Access limit: No limit
802.1X Access statistic: 0

Selected method list:
 authentication dot1x default
 accounting network list3
```

```
Ruijie#show run

Building configuration...
Current configuration : 1449 bytes
version RGOS 10.4(3) Release(101069)(Wed Oct 20 09:12:40 CST 2010 -ngcf67)
co-operate enable
!
aaa new-model
aaa domain enable
!
aaa domain domain.com
 authentication dot1x default
 accounting network list3
!
aaa accounting network list3 start-stop group radius
aaa authentication dot1x default group radius
!
nfpp
!
```

```
no service password-encryption
!
radius-server host 10.1.1.1
radius-server key test
!
line con 0
line vty 0 4
!
end
```

常见配置错误

无

11.5 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。	**clear aaa local user lockout** {**all** | **user-name** *username* }

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**
显示当前所有配置域信息。	**show aaa domain**
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

12 RADIUS

12.1 概述

RADIUS (Remote Authentication Dial-In User Service，远程认证拨号用户服务)是一种分布式的客户机/服务器系统。
RADIUS 与 AAA 配合对试图连接的用户进行身份认证，防止未经授权的访问。在 RGOS 的实现中，RADIUS 客户端运行在设备或网络访问服务器（NAS）上，并向中央 RADIUS 服务器发出身份认证请求，中央服务器包含了所有的用户身份认证和网络服务信息。除了提供认证服务之外，RADIUS 服务器还提供接入用户的授权和记账的服务。
RADIUS 常应用在既要求较高安全性、又允许远程用户访问的各种网络环境中。由于 RADIUS 是一种完全开放的协议，很多系统如 UNIX、WINDOWS 2000、WINDOWS 2008 等均将 RADIUS 服务器作为一个组件安装，因此 RADIUS 是目前应用最广泛的安全服务器。
RADIUS 动态授权扩展协议（Dynamic Authorization Extensions to Remote Authentication Dial In User Service），在 IETF 的 RFC3576 中进行定义。该协议定义了一种针对用户下线管理方法。设备和 RADIUS 服务器之间通过 Disconnect-Messages(简称 DM)消息，将已认证通过的用户下线。该协议使得不同厂商间的设备和 RADIUS 服务器，在用户下线的处理上能够兼容。DM 消息机制，由 RADIUS 服务器主动向设备发起用户下线请求，设备依据请求报文中携带的用户会话、用户名等信息来匹配用户并对其进行下线处理，然后将处理结果以回应报文形式返回给 RADIUS 服务器，以实现服务器对用户的下线管理功能。

协议规范

- RFC2865：Remote Authentication Dial In User Service (RADIUS)
- RFC2866：RADIUS Accounting
- RFC2867：RADIUS Accounting Modifications for Tunnel Protocol Support
- RFC2868：RADIUS Attributes for Tunnel Protocol Support
- RFC2869：RADIUS Extensions
- RFC3576：Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)

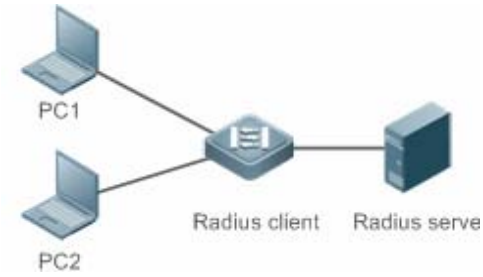
12.2 典型应用

典型应用	场景描述
为接入用户提供认证、授权、记账服务	对网络中的接入用户进行认证、授权、记账，以防止未经授权的访问或操作。
已上线用户被服务器强制下线	对于已经认证的用户，服务器强制其下线

12.2.1 为接入用户提供认证、授权、记账服务

应用场景

RADIUS 的典型应用为对接入用户进行认证、授权、记账。网络设备作为 RADIUS 客户端，将用户信息发送给 RADIUS 服务器。RADIUS 服务器处理完成，给 RADIUS 客户端返回认证接受/认证拒绝/记账响应等信息。RADIUS 客户端根据 RADIUS 服务器的响应信息对接入用户进行相应处理。
图 12-1 典型的 RADIUS 网络配置



【注释】 PC1 和 PC2 作为接入用户通过有线或者无线方式和 RADIUS 客户端连接，并发起认证、记账请求。
Radius Client 通常为接入交换机或者汇聚交换机。
Radius Server 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。

功能部署

- 在 Radius Server 配置接入设备信息，包括接入设备 IP，共享密钥等。
- 在 Radius Client 配置 AAA 的认证、授权、记账方法列表。
- 在 Radius Client 配置 Radius server 信息，包括 IP，共享密钥等。
- 在 Radius Client 配置接入端口开启访问控制。
- 配置网络，使 Radius Client 和 Radius Server 之间通讯正常。

12.2.2 用户强制下线

应用场景

出于管理需要，RADIUS 服务器对于已经认证上线的用户，采取强制下线的措施。
网络配置请参考图 1-1

功能部署

在 1.2.1 的功能部署基础上加上以下部署：

- 在 Radius Client 使能 RADIUS 动态授权扩展功能

12.3 功能详解

基本概念

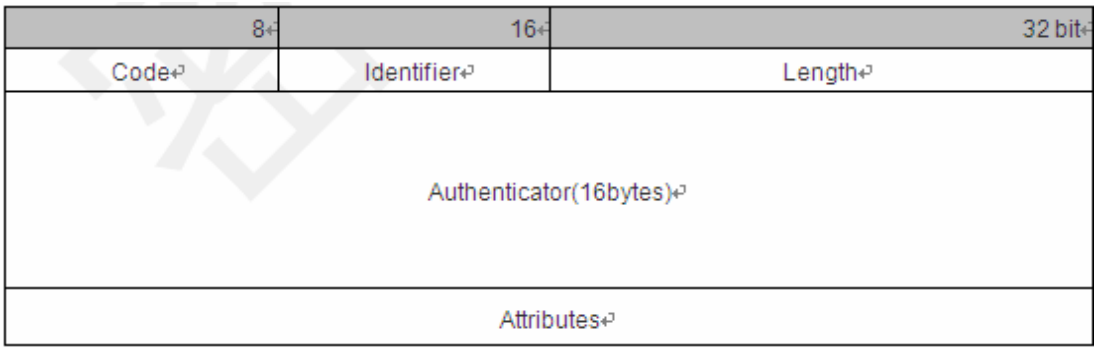
客户端/服务器模式

- 客户端：RADIUS 客户端作为 RADIUS 请求的发起端，通常运行在设备或者网络访问服务器(NAS)上，负责把用户信息发送给 RADIUS 服务器，并接受 RADIUS 服务器的返回信息，进行相应的处理。处理包括接受用户接入或者拒绝用户接入或者收集更多用户信息提供给服务器进行处理。

- 服务器：RADIUS 客户端和 RADIUS 服务器通常是多对一的关系。RADIUS 服务器维护所有的 RADIUS 客户端的 IP 和共享密钥信息，以及所有认证用户的信息。RADIUS 服务器接收 RADIUS 客户端的请求信息，并进行认证、授权、记账处理，然后返回客户端需要的认证、授权、记账信息。

RADIUS 报文结构

RADIUS 的报文结构如下图所示：



- Code — Code 域长度为一个字节，用于标识 RADIUS 报文的类型，取值及含义参考下表。

Code	报文类型	Code	报文类型
1	Access-Request 认证请求报文	4	Accounting-Request 记账请求报文
2	Access-Accept 认证接受报文	5	Accounting-Response 记账相应报文
3	Access-Reject 认证拒绝报文	11	Access-Challenge 认证质询报文

- Identifier — Identifier 域占用 1 个字节，用于匹配请求和响应报文。同一类型的请求报文和响应报文的 Identifier 值相同。
- Length — Length 域占用 2 个字节 ,标识整个 RADIUS 报文的长度 ,包括 Code、Identifier、Length、Authenticator、Attributes 在内。超过 Length 域的字节将被忽略。如果接收到的报文的实际长度小于 Length 的值，则丢弃该报文。
- Authenticator — Authenticator 域占用 16 个字节。RADIUS 客户端使用该域来验证服务器的回应报文。Authenticator 域也用于用户密码的加密/解密。
- Attributes — Attributes 域的长度是不定的，用于携带认证、授权、记账信息。Attributes 域通常包含多个属性。每个属性采用 TLV(Type、Length、Value)三元组的结构表示。其中，Type 为 1 个字节，表示属性的类型，下表列出了 RADIUS 认证、授权、记账常用的属性；Length 为 1 个字节，表示该属性的长度，单位为字节；Value 为该属性的信息。

属性号	属性名	属性号	属性名
1	User-Name	43	Acct-Output-Octets
2	User-Password	44	Acct-Session-Id
3	CHAP-Password	45	Acct-Authentic
4	NAS-IP-Address	46	Acct-Session-Time
5	NAS-Port	47	Acct-Input-Packets
6	Service-Type	48	Acct-Output-Packets
7	Framed-Protocol	49	Acct-Terminate-Cause
8	Framed-IP-Address	50	Acct-Multi-Session-Id

9	Framed-IP-Netmask	51	Acct-Link-Count
10	Framed-Routing	52	Acct-Input-Gigawords
11	Filter-ID	53	Acct-Output-Gigawords
12	Framed-MTU	55	Event-Timestamp
13	Framed-Compression	60	CHAP-Challenge
14	Login-IP-Host	61	NAS-Port-Type
15	Login-Service	62	Port-Limit
16	Login-TCP-Port	63	Login-LAT-Port
18	Reply-Message	64	Tunnel-Type
19	Callback-Number	65	Tunnel-Medium-Type
20	Callback-ID	66	Tunnel-Client-Endpoint
22	Framed-Route	67	Tunnel-Server-Endpoint
23	Framed-IPX-Network	68	Acct-Tunnel-Connection
24	State	69	Tunnel-Password
25	Class	70	ARAP-Password
26	Vendor-Specific	71	ARAP-Features
27	Session-Timeout	72	ARAP-Zone-Access
28	Idle-Timeout	73	ARAP-Security
29	Termination-Action	74	ARAP-Security-Data
30	Called-Station-Id	75	Password-Retry
31	Calling-Station-Id	76	Prompt
32	NAS-Identifier	77	Connect-Info
33	Proxy-State	78	Configuration-Token
34	Login-LAT-Service	79	EAP-Message
35	Login-LAT-Node	80	Message-Authenticator
36	Login-LAT-Group	81	Tunnel-Private-Group-id
37	Framed-AppleTalk-Link	82	Tunnel-Assignment-id
38	Framed-AppleTalk-Network	83	Tunnel-Preference
39	Framed-AppleTalk-Zone	84	ARAP-Challenge-Response
40	Acct-Status-Type	85	Acct-Interim-Interval
41	Acct-Delay-Time	86	Acct-Tunnel-Packets-Lost
42	Acct-Input-Octets	87	NAS-Port-Id

↘ 共享密钥

RADIUS 客户端和 RADIUS 服务器进行通讯，相互之间通过共享密钥来确定对方的身份。共享密钥不能通过网络传输。此外，在传输过程中，为保证安全性，用户密码都是加密的。

↘ RADIUS 服务器组

RADIUS 安全协议，也称 RADIUS 方法，是以 RADIUS 服务器组为单位进行配置的。每一个 RADIUS 方法对应一个 RADIUS 服务器组，每一个 RADIUS 服务器组可配置一至多台 RADIUS 服务器（关于使用 RADIUS 方法的细节信息，请参见“AAA 配置”章节）。如果您在一个 RADIUS 服务器组中配置了多台 RADIUS 服务器，那么当设备同第一台 RADIUS 服务器通讯失败，

或者第一台 RADIUS 服务器变成不可达的状态时，设备将自动尝试同第二台 RADIUS 服务器通讯，以此类推，直到成功或者全部失败为止。

RADIUS 属性类型

- 标准属性

RFC 相关标准规定了 RADIUS 的属性号和属性的内容，但是对于某些属性类型，没有规定属性内容的格式。因此，为适应不同的 RADIUS 服务器要求，需要配置属性内容的格式。目前支持设置 RADIUS Calling-Station-ID 属性（属性号为 31）。

RADIUS Calling-Station-ID 属性用于网络设备向 RADIUS Server 发送请求报文时候，标识认证用户的身份。Calling-Station-ID 属性内容是字符串，可以有多种组成格式，由于要求必须能唯一标识一个用户，因此常选择使用用户的 MAC 地址作为其内容。例如在使用 IEEE 802.1X 认证时，选择使用安装 IEEE 802.1X 客户端所在设备的 MAC 地址。关于这 MAC 地址的格式，有以下几种：

格式	说明
ietf	IETF（RFC3580）规定的标准格式，使用 ‘-’ 作为分隔符。例如：00-D0-F8-33-22-AC
normal	常用的表示 MAC 地址的格式（点分十六进制格式），使用 ‘.’ 作为分隔符。例如：00d0.f833.22ac
unformatted	无格式，没有任何分隔符，默认使用这个格式。例如：00d0f83322ac

- 私有属性

RADIUS 协议是一个可扩展的协议。RFC2865 中定义了 26 号属性（Vendor-Specific）用于设备厂商对 RADIUS 协议进行扩展，以实现其私有的或者标准 RADIUS 没有定义的功能。锐捷公司支持的私有属性如表 1-3 所示。其中 TYPE 为锐捷产品私有属性类型的默认配置；扩展 TYPE 为扩展厂商类型的默认配置。

ID	功能	TYPE	扩展 TYPE
1	max-down-rate	1	76
2	port-priority	2	77
3	user-ip	3	3
4	vlan-id	4	4
5	last-supplicant-version	5	5
6	net-ip	6	6
7	user-name	7	7
8	password	8	8
9	file-directory	9	9
10	file-count	10	10
11	file-name-0	11	11
12	file-name-1	12	12
13	file-name-2	13	13
14	file-name-3	14	14
15	file-name-4	15	15
16	max-up-rate	16	16
17	current-supplicant-version	17	17

18	flux-max-high32	18	18
19	flux-max-low32	19	19
20	proxy-avoid	20	20
21	dailup-avoid	21	21
22	ip-privilege	22	22
23	login-privilege	42	42
27	ipv4-multicast-address	87	87
62	sdg-type	62	62
85	sdg-zone-name	85	85
103	sdg-group-name	103	103

功能特性

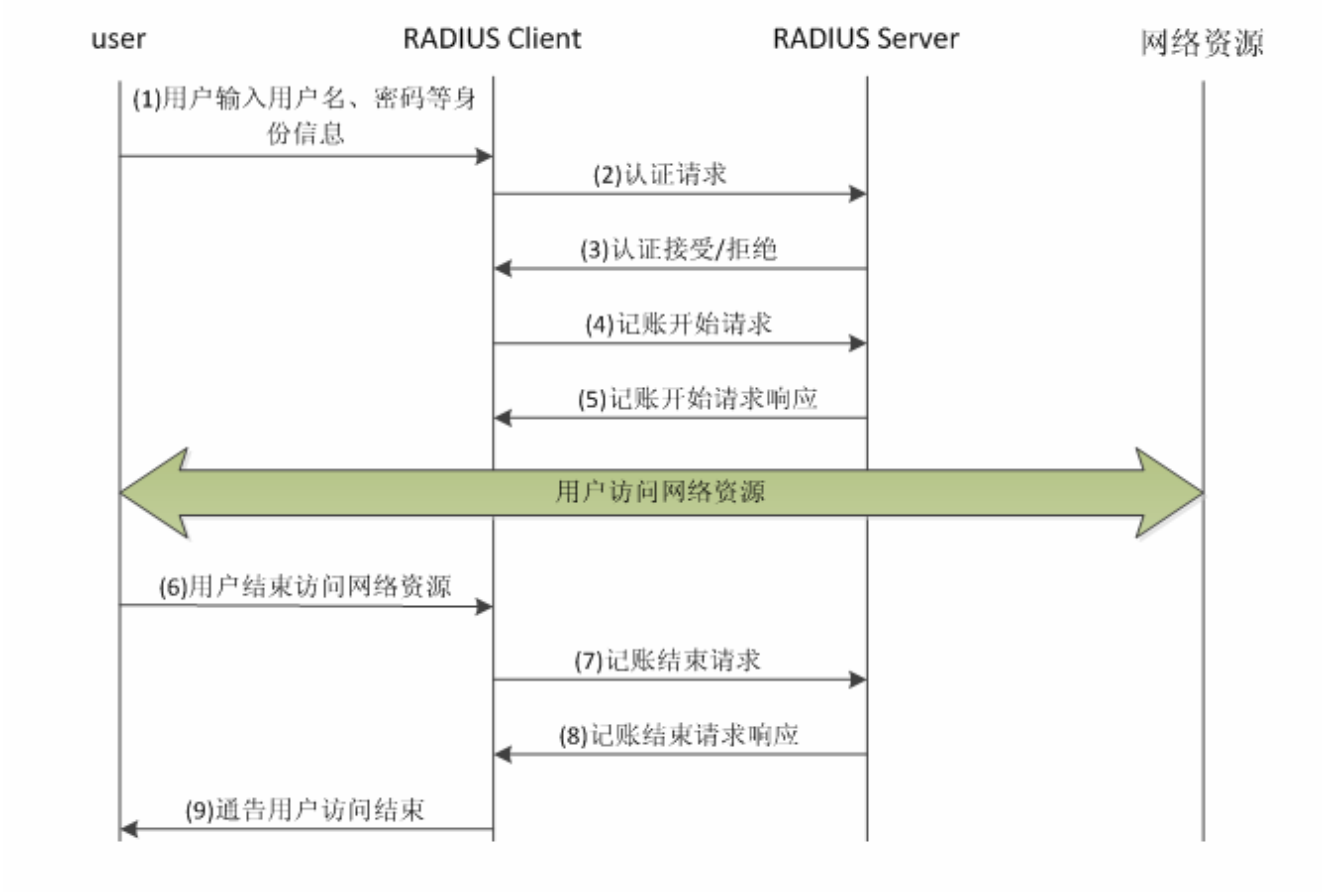
功能特性	作用
RADIUS 认证、授权	对访问用户进行身份认证、记账，保护网络安全以及便于网络管理员进行管理。
指定 RADIUS 报文源地址	指定 RADIUS 客户端向 RADIUS 服务器传送报文时的源 IP 地址。
RADIUS 超时重传	指定 RADIUS 服务器对 RADIUS 客户端传送的报文一定的时间内无响应时 RADIUS 客户端重传报文的参数。
RADIUS 服务器可达性检测	RADIUS 客户端主动探测 RADIUS 服务器是否可达，并维护各 RADIUS 服务器的可达性状态。进行业务处理时，总是优先选择状态为可达的服务器，以提高 RADIUS 业务的处理性能。
RADIUS 强制下线	对于已认证的用户，RADIUS 服务器主动要求其下线

12.3.1 RADIUS认证、授权、记账

对访问用户进行身份认证、记账，保护网络安全以及便于网络管理员进行管理。

工作原理

图 12-2



RADIUS 的认证和授权流程为：

产品支持情况 用户输入用户名、密码等身份信息，传送给 RADIUS 客户端。

产品支持情况 RADIUS 客户端获取用户的用户名、密码信息，向 RADIUS 传送认证请求报文。其中密码是加密的，加密方法请参照 RFC2865。

产品支持情况 RADIUS 服务器根据用户名、密码信息，决定接受或拒绝此次认证请求。如果接受，同时下发授权信息。不同类型的访问用户，其授权信息也不相同。

RADIUS 的记账流程为：

(4)如果步骤(3)中 RADIUS 服务器返回认证接受，则 RADIUS 客户端紧接着发送记账开始请求报文。

(5)RADIUS 服务器回应记账开始响应报文，开始记账。

(6)用户结束访问网络资源，请求 RADIUS 客户端断开连接。

(7)RADIUS 客户端发送记账结束请求报文。

(8)RADIUS 服务器返回记账结束响应报文，停止记账。

(9)用户断开连接，无法再访问网络资源

相关配置

配置 RADIUS 服务器参数

缺省情况下，没有配置任何 RADIUS 服务器。

使用 **radius-server host** 命令可以配置 RADIUS 服务器的相关信息。

必须至少配置一个 RADIUS 服务器，RADIUS 相关业务才能正常运转。

↘ 配置 AAA 认证方法列表

缺省情况下，没有配置任何 AAA 认证方法列表。

使用 **aaa authentication** 命令配置不同用户类型的方法列表，并且认证方法选择 group radius。

必须配置相应用户类型的 aaa 认证方法列表，才能进行 radius 认证。

↘ 配置 AAA 授权方法列表

缺省情况下，没有配置任何 AAA 授权方法列表。

使用 **aaa authorization** 命令配置不同类型的授权方法列表，并且授权方法选择 group radius。

必须配置相应类型的 aaa 授权方法列表，才能进行 radius 授权。

↘ 配置 AAA 记账方法列表

缺省情况下，没有配置任何 AAA 记账方法列表。

使用 **aaa accounting** 命令配置不同类型的记账方法列表，并且记账方法选择 group radius。

必须配置相应类型的 aaa 记账方法列表，才能进行 radius 记账。

12.3.2 指定RADIUS报文源地址

指定 RADIUS 客户端向 RADIUS 服务器传送报文时的源 IP 地址。

工作原理

配置 RADIUS 时，通过指定 RADIUS 客户端向 RADIUS 服务器发送 RADIUS 报文的源 IP 地址，可以减少在 RADIUS 服务器上维护大量的 NAS 信息的工作量。

相关配置

缺省配置为使用全局路由寻路，确定发送 RADIUS 报文的源地址。

使用 **ip radius source-interface** 命令指定发送 RADIUS 报文的源接口，设备将把指定接口的第一个 ip 地址作为 radius 报文的源地址。

12.3.3 RADIUS超时重传

工作原理

RADIUS 客户端向 RADIUS 服务器传送报文后，启动定时器检测 RADIUS 服务器的响应，如果一定时间内 RADIUS 服务器没有响应，则 RADIUS 客户端重传报文。

相关配置

↘ 配置 RADIUS 服务器超时时间

缺省配置的超时时间为 5 秒。

使用命令 **radius-server timeout** 命令可以配置超时时间，时间范围为 1 到 1000 秒。

RADIUS 服务器的响应时间和其自身的性能、网络环境有关。需要根据实际情况配置合适的超时时间。

↘ 配置重传次数

缺省配置的重传次数为 3 次。

使用命令 **radius-server retransmit** 命令配置重传次数，范围 1 到 100 次。

↘ 配置记账更新是否重传

缺省配置为不会对计费更新报文进行重传。

使用命令 **radius-server account update retransmit** 命令配置认证用户的记账更新报文进行重传的功能。

12.3.4 RADIUS服务器可达性检测

工作原理

RADIUS 客户端主动探测 RADIUS 服务器是否可达，并维护各 RADIUS 服务器的可达性状态。进行业务处理时，总是优先选择状态为可达的服务器，以提高 RADIUS 业务的处理性能。

相关配置

↘ 配置设备判定 RADIUS 安全服务器不可达的标准

缺省配置的判定 RADIUS 服务器不可达的标准为同时满足以下两个条件：一、设备在 60 秒内内没有收到来自 RADIUS 安全服务器的正确响应报文；二、设备向同一个 RADIUS 安全服务器发送的请求报文连续超时次数达到 10 次。

使用命令 **radius-server dead-criteria** 可以配置设备判定 RADIUS 安全服务器不可达的标准。

↘ 配置主动探测 RADIUS 安全服务器的测试用户名

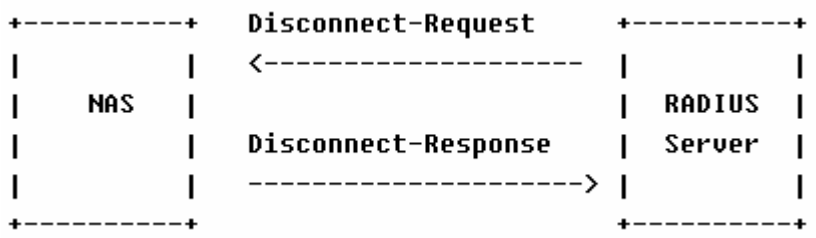
缺省配置时，不对 RADIUS 安全服务器指定主动探测的测试用户名。

使用命令 **radius-server host x.x.x.x testusername xxx** 来配置测试用户名。

12.3.5 RADIUS强制下线

工作原理

图 3-3 RADIUS 动态授权扩展 DM 消息交互图



12.3.6 RADIUS 服务器和设备之间的 DM 消息交互图如上。RADIUS 服务器发送 Disconnect-Request消息到设备的 3799 UDP端口，设备处理结束之后，将处理结果通过Disconnect-Response消息返回给RADIUS服务器。

12.4 产品说明



NBR108G-P 不支持 radius；NBR800G、NBR950G、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 radius。

12.5 配置详解

配置项	配置建议 & 相关命令	
RADIUS 基本配置	⚠ 必须配置。用于 radius 认证、授权、记账	
	radius-server host	配置远程 RADIUS 安全服务器的 IP 地址
	radius-server key	配置设备和 RADIUS 服务器进行通讯的共享密钥
	radius-server retransmit	配置设备在确认 RADIUS 无效以前发送请求的次数
	radius-server timeout	配置设备重传请求以前等待的时间
	radius-server account update retransmit	配置认证用户的记账更新报文进行重传的功能
	ip radius source-interface	配置 RADIUS 报文的源地址
配置 RADIUS 属性类型	⚠ 可选配置。用于定义设备封装和解析 radius 报文时对属性的处理。	
	radius-server attribute 31	配置 RADIUS 的 31 号属性（Calling-Stationg-ID）的 MAC 地址格式。
	radius-server attribute class	配置 RADIUS 的 Class 属性的解析方式。
	radius attribute	配置 RADIUS 私有属性类型
	radius set qos cos	配置设备处理服务器下发的私有属性 port-priority 为接口 cos 值。Cos 相关概念请参考“配置 Qos”
	radius support cui	配置设备支持 cui 属性
	radius vendor-specific	配置设备解析私有属性的方式
	radius-server authentication attribute	配置 RADIUS 认证请求报文中是否携带指定属性
	radius-server account attribute	配置 RADIUS 记帐请求报文中是否携带指定属性
	radius-server authentication vendor	配置 RADIUS 认证请求报文是否携带其它产商的私有属性
	radius-server account vendor	配置 RADIUS 记帐请求报文是否携带其它产商的私有属性
配置 RADIUS 可达性检测	⚠ 可选配置。用于检测 RADIUS 服务器是否可达，以及维护 RADIUS 服务器的可达性状态。	
	radius-server dead-criteria	配置全局的 RADIUS 安全服务器不可达的判定标准

	radius-server deadtime	配置设备停止向不可达状态的 RADIUS 服务器发送请求报文的时长
	radius-server host	配置远程 RADIUS 安全服务器的 IP 地址 ,指定认证端口和记帐端口，指定主动探测的相关参数

12.5.1 RADIUS基本配置

配置效果

- 完成 RADIUS 基本配置，即可进行 RADIUS 认证、授权、记账。

注意事项

- 在设备上配置 RADIUS 之前，应确保 RADIUS 服务器的网络通讯良好。
- 使用命令 **ip radius source-interface** 配置 RADIUS 报文的源地址时，应确保此源地址和 RADIUS 服务器通讯良好。

配置方法

配置远程 RADIUS 安全服务器

- 必须配置。
- 配置 RADIUS 安全服务器的 IP 地址、认证端口、记账端口、共享密钥。

配置设备和 RADIUS 服务器进行通讯的共享密钥。

- 可选配置。
- 这里通过全局配置对所有未配置共享密钥选项的服务器配置一个共享密钥。

⚠ 设备上的共享密钥和 RADIUS 服务器上的共享密钥必须一致。

配置设备在确认 RADIUS 无效以前发送请求的次数

- 可选配置。
- 根据实际网络环境，配置设备确认 RADIUS 无效以前发送请求的次数。

配置设备重传请求以前等待的时间

- 可选配置。
- 根据实际网络环境，配置设备重传请求以前等待的时间。

⚠ 在使用 RADIUS 安全协议的 802.1x 认证环境中，如果网络设备作为 802.1x 认证者，并且采用锐捷 SU 作为 802.1x 客户端软件时，建议在网络设备上设置 **radius-server timeout** 值为 3 秒（默认为 5 秒），设置 **radius-server retransmit** 值为 2 次（默认为 3 次）

配置认证用户的记账更新报文进行重传的功能

- 可选配置。
- 根据实际实际需要，决定是否开启认证用户的记账更新报文重传功能。

配置 RADIUS 报文的源地址

- 可选配置。
- 根据实际网络环境，配置 RADIUS 报文的源地址。

检验方法

- 配置 AAA 方法列表使用 RADIUS 方法，用户进行认证、授权、记账。

- 设备与 RADIUS 服务器进行交互，通过抓包可以看到是通过 RADIUS 协议进行通信的。

相关命令

配置远程 RADIUS 安全服务器

【命令格式】 **radius-server host** { *ipv4-address* } [**auth-port** *port-number*] [**acct-port** *port-number*] [**test username** *name* [**idle-time** *time*] [**ignore-auth-port**] [**ignore-acct-port**]] [**key** [**0** | **7**] *text-string*]

【参数说明】 *ipv4-address* ：RADIUS 安全服务器主机的 IPv4 地址。

auth-port *port-number* ：RADIUS 身份认证的 UDP 端口，取值范围 0 - 65535，如果设置为 0，则该主机不进行身份认证。

acct-port *port-number* ：RADIUS 记帐的 UDP 端口，取值范围 0 - 65535，如果设置为 0，则该主机不进行记帐。

test username *name* ：开启对该 RADIUS 安全服务器的主动探测功能，并指定主动探测所使用的用户名。

idle-time *time*：配置设备向处于可达状态的 RADIUS 安全服务器发送测试报文的时间间隔。默认值为 60 分钟，可配置的范围为 1-1440 分钟（24 小时）。

ignore-auth-port：关闭对 RADIUS 安全服务器的认证端口的检测，默认开启。

ignore-acct-port：关闭对 RADIUS 安全服务器的记账端口的检测，默认开启。

key [**0** | **7**] *text-string* ：配置用于该服务器的共享密钥，未配置则使用全局配置。配置的密钥可以指定加密类型，0 为无加密，7 简单加密，默认为 0。

【命令模式】 全局模式。

【使用指导】 为了使用 RADIUS 实现 AAA 安全服务，必须定义 RADIUS 安全服务器。您可以使用 **radius-server host** 命令定义一个或多个 RADIUS 安全服务器。如果没有把 RADIUS 安全服务器配置在某个 RADIUS 服务器组中，则设备向 RADIUS 服务器发送 radius 报文时使用全局路由表。

配置设备和 RADIUS 服务器进行通讯的共享密钥。

【命令格式】 **radius-server key** [**0** | **7**] *text-string*

【参数说明】 *text-string* ：共享密钥的文本。

0 | **7**：口令的加密类型，0 无加密，7 简单加密，默认为 0。

【命令模式】 全局模式

【使用指导】 共享密钥是设备和 RADIUS 安全服务器进行正确通信的基础。为了使设备和 RADIUS 安全服务器能进行通信，必须在设备和 RADIUS 安全服务器上定义相同的共享密钥。

配置设备在确认 RADIUS 无效以前发送请求的次数

【命令格式】 **radius-server retransmit** *retries*

【参数说明】 *retries*：RADIUS 尝试重发次数，取值范围是 1-100

【命令模式】 全局模式

【使用指导】 AAA 在使用下一个方法对用户进行认证的前提是当前认证的安全服务器没有反应。设备判断安全服务器没有反应的标准是安全服务器在设备重发指定次数 RADIUS 报文期间均没有应答，每次重发之间有超时间隔。

配置设备重传请求以前等待的时间

【命令格式】 **radius-server timeout** *seconds*

【参数说明】 *seconds* ：超时时间（单位为秒）。可设置的值范围为 1-1000 秒。

【命令模式】 全局模式

【使用指导】 使用该命令对重发报文的超时时间进行调整。

配置认证用户的记账更新报文进行重传的功能

【命令格式】 **radius-server account update retransmit**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 配置认证用户的记账更新报文进行重传的功能，默认不重传。该配置不影响其他类型的用户。

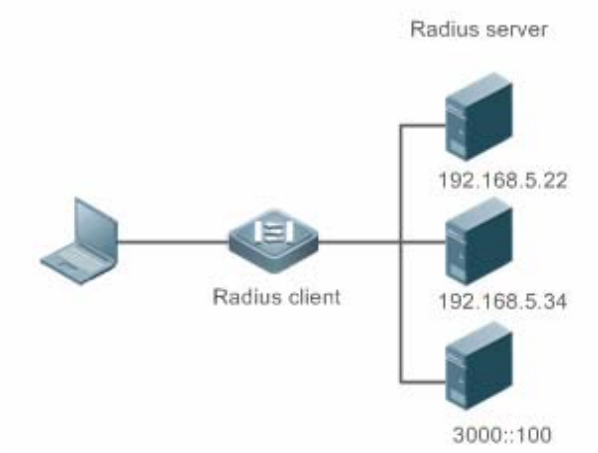
配置举例

以下配置举例，仅介绍与 RADIUS 相关的配置。

Login 用户使用 RADIUS 认证、授权、记账

【网络环境】

图 12-4



【配置方法】

- 配置启用 aaa。
- 配置 radius-server 信息。
- 配置使用 radius 的认证方法、授权方法、记账方法。
- 在接口上应用配置认证方法。

RADIUS Client

```
Ruijie# configure terminal
Ruijie (config)# aaa new-model
Ruijie (config)# radius-server host 192.168.5.22
Ruijie (config)# radius-server host 3000::100
Ruijie (config)# radius-server key aaa
Ruijie (config)# aaa authentication login test group radius
Ruijie (config)# aaa authorization exec test group radius
Ruijie (config)# aaa accounting exec test start-stop group radius
Ruijie (config)# line vty 0 4
Ruijie (config-line)# login authentication test
Ruijie (config-line)# authorization exec test
Ruijie (config-line)# accounting exec test
```

【检验方法】 在 PC 上 telnet 到设备上，要求输入用户名和密码。输入正确的用户名和密码，能够登录到设备上。并且被服务器授予一定的权限级别，仅运行执行该权限级别下的命令。在 RADIUS 服务器上可以查看到此用户的认证日志。用户对设备进行管理操作后退出登录，在 RADIUS 服务器上可以查看到此用户的记账信息。

```
Ruijie#show running-config
```

```
!
radius-server host 192.168.5.22
radius-server host 3000::100
radius-server key aaa
aaa new-model
aaa accounting exec test start-stop group radius
aaa authorization exec test group radius
aaa authentication login test group radius
no service password-encryption
ip tcp not-send-rst
!
vlan 1
!
line con 0
line vty 0 4
 accounting exec test
 authorization exec test
 login authentication test
!
```

常见错误

- 设备配置的 key 与服务器配置的 key 不一致。
- 没有配置方法列表。

12.5.2 配置RADIUS属性类型

配置效果

- 定义设备封装和解析 radius 报文时对属性的处理。

注意事项

- 设置 RADIUS 属性类型一节所涉及的私有属性均指锐捷公司的私有属性。

配置方法

↘ 配置 RADIUS 的 31 号属性（Calling-Stationg-ID）的 MAC 地址格式

- 可选配置
- 根据服务器类型，配置 Calling-Station-Id 的 MAC 地址格式为服务器支持的类型。

↘ 配置 RADIUS 的 Class 属性的解析方式

- 可选配置
- 根据服务器类型，配置对 Class 属性的解析方式。

↘ 配置 RADIUS 私有属性类型

- 可选配置

- 如果服务器为锐捷公司的应用服务器，则需要配置 RADIUS 私有属性类型来适应。

配置设备处理服务器下发的私有属性 port-priority 为接口的 cos 值

- 可选配置
- 根据需要，配置服务器下发的私有属性 port-priority 为接口的 cos 值。

配置设备支持 cui 属性

- 可选配置
- 根据需要，配置设备是否支持 RADIUS 的 CUI 属性。

配置设备解析私有属性的方式

- 可选配置
- 根据需要，配置设备解析锐捷私有属性时私有属性号的索引。

配置 RADIUS 认证请求报文中是否携带指定属性

- 可选配置
- 根据需要，配置 RADIUS 认证请求报文是否指定属性类型。

配置 RADIUS 记帐请求报文中是否携带指定属性

- 可选配置
- 根据需要，配置 RADIUS 记帐请求报文中是否指定属性类型。

配置 RADIUS 认证请求报文中是否携带指定产商的私有属性

- 可选配置
- 根据需要，配置 radius 认证请求报文携带指定产商的私有属性。

配置 RADIUS 记帐请求报文中是否携带指定产商的私有属性

- 可选配置
- 根据需要，配置 RADIUS 记帐请求报文是否携带指定产商的私有属性。

配置 RADIUS 是否支持解析报文中思科、华为、微软的私有属性

- 可选配置
- 根据需要，配置 RADIUS 是否支持解析报文中思科、华为、微软的私有属性，缺省支持。

配置 RADIUS 报文 Nas-Port-Id 封装的格式

- 可选配置
- 根据是否 qinq 场景，配置 RADIUS 报文中 Nas-Port-Id 封装的格式。缺省是正常格式封装。

检验方法

- 配置 AAA 方法列表使用 RADIUS 方法，用户进行认证、授权、记账
- 设备与 RADIUS 服务器进行交互，通过抓包查看 Calling-Station-Id 的 MAC 地址格式。
- 设备与 RADIUS 服务器进行交互，通过设备 debug 信息查看锐捷公司的私有属性被设备正确的解析。
- 设备与 RADIUS 服务器进行交互，通过设备 debug 信息查看 CUI 属性被设备正确的解析。

相关命令

配置 RADIUS 的 31 号属性（Calling-Stationg-ID）的 MAC 地址格式

【命令格式】 **radius-server attribute 31 mac format** { **ietf | normal | unformatted** }

【参数说明】 **ietf** ：指定 ETF（RFC3580）规定的标准格式，使用 ‘-’ 作为分隔符。例如：00-D0-F8-33-22-AC。

normal：指定常用的表示 MAC 地址的格式(点分十六进制格式),使用 ‘.’ 作为分隔符。例如 :00d0.f833.22ac。

unformatted：指定无格式，没有任何分隔符，默认使用这个格式。例如：00d0f83322ac。

【命令模式】 全局模式

【使用指导】 部分 RADIUS 安全服务器（主要用于 802.1x 认证）可能只识别 IETF 的格式，这种情况下需要将 Calling-Station-ID 属性设置为 IETF 格式类型。

配置 RADIUS 的 Class 属性的解析方式

【命令格式】 **radius-server attribute class user-flow-control { format-16bytes | format-32bytes }**

【参数说明】 **user-flow-control**：配置从 class 属性中解析限速配置。

format-16bytes：配置 class 属性中的限速值格式为 16 字节。

format-32bytes：配置 class 属性中的限速值格式为 32 字节。

【命令模式】 全局模式

【使用指导】 如果服务器通过 Class 属性下发限速值，则需要配置该命令。

配置设备处理服务器下发的私有属性 port-priority 为接口的 cos 值

【命令格式】 **radius set qos cos**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 配置该命令，可以将传下的 qos 值作为 cos 值，默认时作为 dscp 值。

配置设备支持 cui 属性

【命令格式】 **radius support cui**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 配置该命令，使 radius 支持 cui 属性。

配置设备解析私有属性的方式

【命令格式】 **radius vendor-specific extend**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 使用该命令可对所有厂商 id 的属性按照配置是由类型识别。

配置 radius 认证请求报文中是否携带指定属性

【命令格式】 **radius-server authentication attribute *type* package**

radius-server authentication attribute *type* unpackage

【参数说明】 ***type***, Radius 属性类型。可设置范围为 1-255

【命令模式】 全局模式

【使用指导】 使用该命令可对认证请求报文中携带的属性进行指定。

配置 radius 记帐请求报文中是否携带指定属性

【命令格式】 **radius-server account attribute *type* package**

radius-server account attribute *type* unpackage

【参数说明】 ***type***, Radius 属性类型。可设置范围为 1-255

【命令模式】 全局模式

【使用指导】 使用该命令可对记帐请求报文中携带的属性进行指定。

配置 radius 认证请求报文中是否携带指定产商的私有属性

【命令格式】 **radius-server authentication vendor *vendor_name* package**

【参数说明】 ***vendor_name*, 产商的名称，可为 cmcc、microsoft、cisco。**

【命令模式】 全局模式

【使用指导】 使用该命令可配置认证请求报文中是否携带指定产商的私有属性。

配置 radius 记帐请求报文中是否携带指定产商的私有属性

【命令格式】 **radius-server account vendor *vendor_name* package**

【参数说明】 ***vendor_name*，产商的名称，可为 cmcc、microsoft、cisco。**

【命令模式】 全局模式

【使用指导】 使用该命令可配置记帐请求报文中是否携带指定产商的私有属性。

配置 RADIUS 是否支持解析报文中思科、华为、微软的私有属性

【命令格式】 **radius vendor-specific attribute support *vendor_name***

【参数说明】 ***vendor_name*，产商的名称，可为 cisco、huawei、ms。**

【命令模式】 全局模式

【使用指导】 使用该命令可以配置是否支持对报文中的思科、华为、微软的私有属性进行解析。

配置举例

以下配置举例，仅介绍与 RADIUS 相关的配置。

配置 RADIUS 属性类型

【网络环境】 单设备

【配置方法】
- 配置 RADIUS 的 Calling-Station-Id 的 MAC 地址格式。
- 配置私有属性类型值。
- 配置 radius 传下的 qos 值为接口 cos 值。
- 配置 radius 支持 cui 属性。
- 扩展为不区别私有厂商 id。
- 认证请求不封装 NAS-PORT-ID 属性
- 记帐请求携带中移动要求的私有属性
- 配置对收到的 radius 报文不支持解析思科的私有属性
- 配置 nas-port-id 的封装格式为 qinq 场景的格式

```
Ruijie(config)# radius-server attribute 31 mac format ietf
Ruijie(config)# radius attribute 16 vendor-type 211
Ruijie(config)# radius set qos cos
Ruijie(config)# radius support cui
Ruijie(config)# radius vendor-specific extend
Ruijie(config)# radius-server authentication attribute 87 unpackage
Ruijie(config)# radius-server account vendor cmcc package
Ruijie(config)# no radius vendor-specific attribute support cisco
Ruijie(config)# radius-server attribute nas-port-id format qinq
```

【检验方法】 通过抓包或者设备 debug 信息查看 radius 标准属性和私有属性的封装/解析是否正确。

12.5.3 配置RADIUS可达性检测

配置效果

设备维护所配置的每台 RADIUS 服务器的可达性状态：可达或者不可达。设备不会向处于不可达状态的 RADIUS 服务器发送接入用户的认证、授权和记账请求，除非，该 RADIUS 服务器所在的 RADIUS 服务器组的所有服务器均为不可达状态。
设备支持对指定的 RADIUS 服务器进行主动探测，默认关闭。如果您为指定的 RADIUS 服务器开启主动探测功能，那么设备将会根据配置，定期向该 RADIUS 服务器发送探测请求（认证请求或者记账请求）。其时间间隔周期为：

- 处于可达状态的 RADIUS 服务器：该 RADIUS 服务器的可达状态的主动探测间隔时间（默认值为 60 分钟）。
- 处于不可达状态的 RADIUS 服务器：固定为 1 分钟。

注意事项

为指定的 RADIUS 服务器开启主动探测功能，需要满足如下所有条件：

- 在设备上配置了该 RADIUS 服务器的测试用户名。
- 在设备上至少配置了一个该 RADIUS 服务器的被测端口（认证端口或者记账端口）。

对于一台处于可达状态的 RADIUS 服务器，当以下两个条件均满足时，设备认为该 RADIUS 服务器进入不可达状态：

- 距离上次收到该 RADIUS 服务器的正确响应超过 radius-server dead-criteria time seconds 设定的时间。
- 在上次收到该 RADIUS 服务器的正确响应之后 ,设备发往该 RADIUS 服务器的请求而未收到正确响应的次数(包括重传), 达到 radius-server dead-criteria tries number 设定的次数。

对于一台处于不可达状态的 RADIUS 服务器，当以下任一条件满足时，设备认为该 RADIUS 服务器进入可达状态：

- 设备收到来自该 RADIUS 服务器的正确响应。
- 该 RADIUS 服务器处于不可达状态超过 **radius-server deadtime** 设定的时间，并且该 RADIUS 服务器没有启用主动探测功能。
- 在设备上更新该 RADIUS 服务器的认证端口或者记账端口。

配置方法

↘ 配置全局的 RADIUS 安全服务器不可达的判定标准

- 必须配置
- 配置全局的 RADIUS 安全服务器不可达的判定标准是开启主动探测功能的必要条件。

↘ 配置远程 RADIUS 安全服务器的 IP 地址，指定认证端口和记帐端口，指定主动探测的相关参数

- 必须配置
- 指定 RADIUS 服务器主动探测的相关参数是开启主动探测功能的必要条件。

↘ 配置设备停止向不可达状态的 RADIUS 服务器发送请求报文的时长

- 可选配置
- RADIUS 服务器没有启用主动探测功能时 ,配置设备停止向不可达状态的 RADIUS 服务器发送请求报文的时长才会生效。

检验方法

- 通过 **show radius server** 命令可以查看各个 RADIUS 服务器的可达性信息。

相关命令

配置全局的 RADIUS 安全服务器不可达的判定标准

【命令格式】 **radius-server dead-criteria** { **time** *seconds* [**tries** *number*] | **tries** *number* }

【参数说明】 **time** *seconds*：配置时间条件参数。设备在指定的时间内没有收到来自 RADIUS 安全服务器的正确响应报文，则认为该 RADIUS 安全服务器满足不可达的时长条件。可设置的值的范围为 1-120 秒。

tries *number*：配置请求连续超时次数条件参数。当设备向同一个 RADIUS 安全服务器发送的请求报文连续超时次数达到所设定的次数，则认为该 RADIUS 安全服务器满足不可达的连续超时次数条件。可设置的值的范围为 1-100。

【命令模式】 全局模式

【使用指导】 如果一台 RADIUS 安全服务器同时满足时间条件和请求连续超时次数条件，则设备认为该 RADIUS 安全服务器不可达。使用该命令，用户可以对时间条件和请求连续超时次数条件的参数进行调整。

配置设备停止向不可达状态的 RADIUS 服务器发送请求报文的时长

【命令格式】 **radius-server deadtime** *minutes*

【参数说明】 *minutes*：配置设备停止向处于不可达状态的 RADIUS 安全服务器发送请求的时间，单位为分钟。可设置的值的范围为 1-1440 分钟（24 小时）。

【命令模式】 全局模式

【使用指导】 如果设备对一台 RADIUS 安全服务器启用了主动探测功能，那么 **radius-server deadtime** 的时间参数对该 RADIUS 安全服务器不起作用；否则，该 RADIUS 安全服务器，将在处于不可达状态的时间超过 **radius-server deadtime** 指定的时间时，被设备自动恢复为可达状态。

配置举例

以下配置举例，仅介绍与 RADIUS 相关的配置。

配置对 RADIUS 服务器进行不可达检测

【网络环境】

图 12-5



【配置方法】

- 配置全局的 RADIUS 安全服务器不可达的判定标准。
- 配置远程 RADIUS 安全服务器的 IP 地址，指定认证端口和记帐端口，指定主动探测的相关参数。

RADIUS Client

```
Ruijie(config)# radius-server dead-criteria time 120 tries 5
Ruijie(config)# radius-server host 192.168.5.22 test username test ignore-acct-port idle-time 90
```

【检验方法】 使设备与 192.168.5.22 服务器网络通讯断开。通过设备进行 radius 认证。120 秒后，使用命令 **show radius server** 命令查看服务器状态为 dead。

```
Ruijie#show running-config
…
radius-server host 192.168.5.22 test username test ignore-acct-port idle-time 90
radius-server dead-criteria time 120 tries 5
```

...

12.6 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
将 RADIUS 动态授权扩展功能的统计信息清零，重新开始统计。	**clear radius dynamic-authorization-extension statistics**

查看运行情况

作用	命令
显示 RADIUS 服务器全局参数。	**show radius parameter**
显示 RADIUS 服务器配置情况。	**show radius server**
显示 RADIUS 私有属性类型配置。	**show radius vendor-specific**
显示 RADIUS 动态授权扩展相关统计信息。	**show radius dynamic-authorization-extension statistics**
显示 RADIUS 认证相关统计信息	**show radius auth statistics**
显示 RADIUS 计费相关统计信息	**show radius acct statistics**
显示 RADIUS 服务器组的配置	**show radius group**
显示 RADIUS 标准属性	**Show radius attribute**

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 radius 事件的调试开关。	**debug radius event**
打开 radius 报文打印的调试开关。	**debug radius detail**
打开 radius 动态授权扩展功能的调试开关。	**debug radius extension event**
打开 radius 动态授权扩展报文打印的调试开关。	**debug radius extension detail**

13 TACACS+

13.1 概述

TACACS+是在 TACACS（Terminal Access Controller Access Control System，终端访问控制器访问控制系统）基础上进行了功能增强的安全协议。用于实现多种用户的 AAA 功能，包括认证、授权、记账。

协议规范

- RFC 1492Terminal Access Controller Access Control System

13.2 典型应用

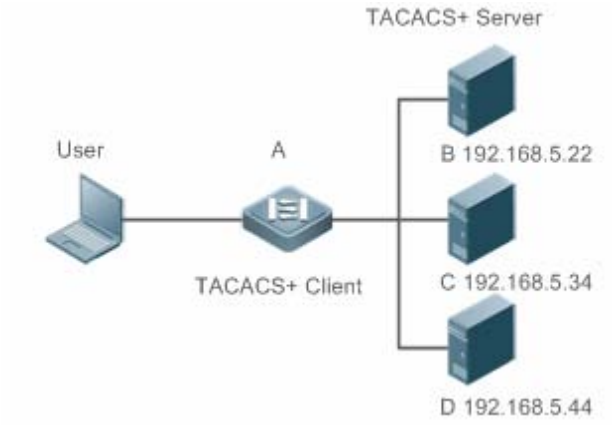
典型应用	场景描述
终端用户的登陆管理控制	对终端用户进行密码校验并进行授权。

13.2.1 终端用户的登陆管理控制

应用场景

TACACS+的典型应用为终端用户的登陆管理控制，网络设备作为 TACACS+的客户端，将用户名和密码发给 TACACS+服务器进行验证，验证通过并得到授权之后可以登录到网络设备上进行操作。下图所示：

图 13-1



【注释】
- A 为发起 TACACS+请求的客户端。
- B、C、D 为处理 TACACS+请求的服务器。

功能部署

- 在服务器 B, C, D 上启动 TACACS+ Server，并且配置接入设备（设备 A）的信息，以便能够为设备提供基于 TACACS+ 协议的 AAA 功能。
- 。在设备 A 上开启 AAA 功能，为用户登录过程启用认证过程。
- 在设备 A 上启用 TACACS+ Client 功能，并且添加 TACACS+ Server（服务器 B，C，D）的 IP 地址和对应的共享密钥，以便设备 A 能和 TACACS+ Server 进行 TACACS+协议通信来实现 AAA 功能。

13.3 功能详解

基本概念

↘ TACACS+的报文格式

图 13-2

4	8	16	24	32 bit
Major	Minor	Packet type	Sequence no.	Flags
Session ID				
Length				

- Major Version — 主要 TACACS+ 版本号。
- Minor Version — 次要 TACACS+ 版本号。
- Packet Type — 可能值包括：
  TAC_PLUS_AUTHEN： = 0x01 （认证）;
  TAC_PLUS_AUTHOR：= 0x02 （授权）;
  TAC_PLUS_ACCT：= 0x03 （记账）。
- Sequence Number — 当前会话中的数据包序列号。会话中的第一个 TACACS+ 数据包序列号必须为 1，其后的每个数据包序列号逐次加 1。因此客户机只发送奇序列号数据包，而 TACACS+ Daemon 只发送偶序列号数据包。
- Flags — 该字段包括各种位图格式的标志（flag）。Flag 值表明数据包是否进行加密。
- Session ID — 该 TACACS+ 会话的 ID。
- Length — TACACS+ 数据包主体长度（不包括头部），报文全部以加密形式在网络上传输。

功能特性

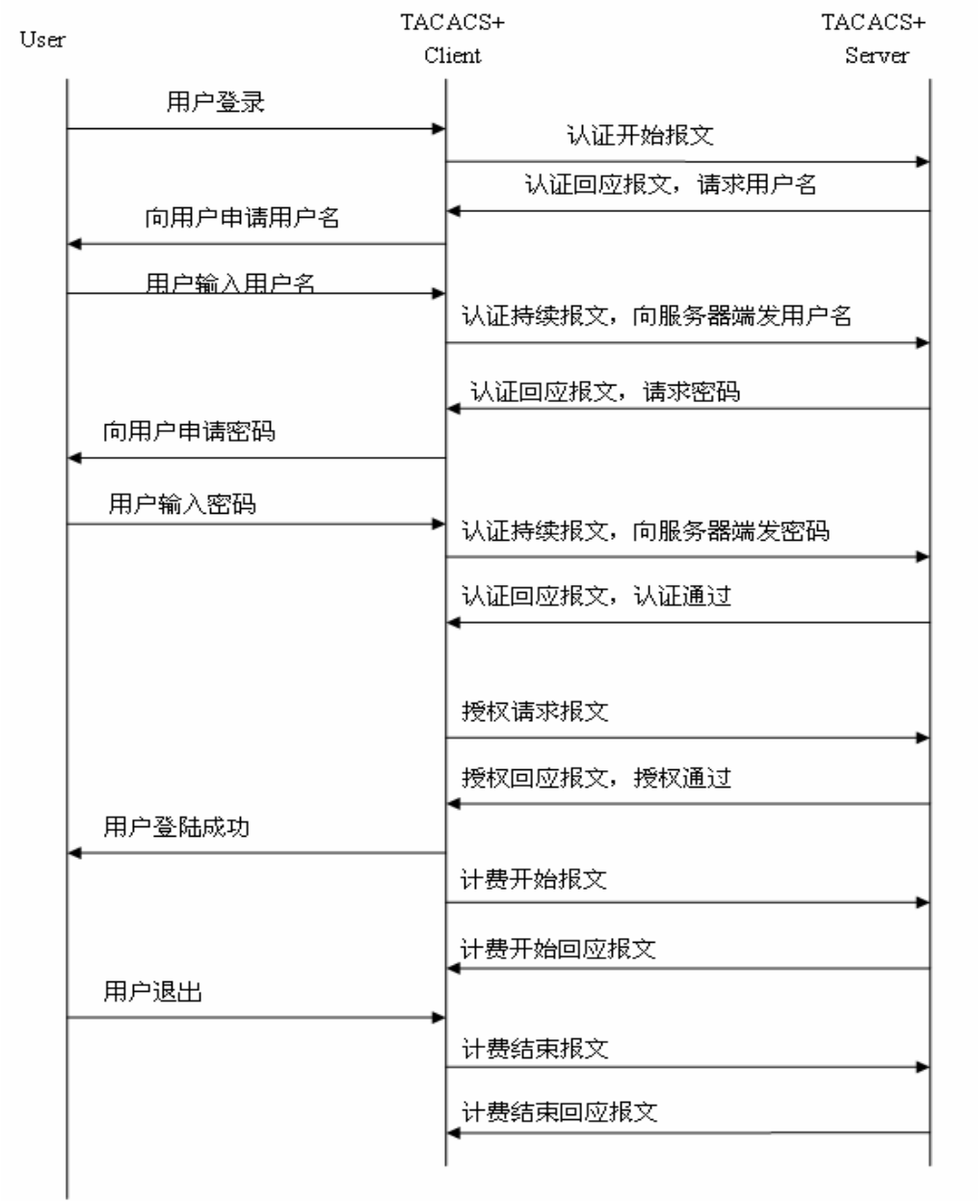
功能特性	作用
TACACS+认证、授权、记账	对终端用户进行认证、授权、记账

13.3.1 TACACS+认证、授权、记账

工作原理

下边以 Login 登录的基本认证、授权和记账说明 TACACS+运行中的数据报文的交互：

图 13-3



在整个过程中的基本消息交互流程可以分为三个部分：

1. 认证过程包含：
   1) 用户请求登录网络设备。

2) TACACS+客户端收到请求之后，向 TACACS+服务器发送认证开始报文。
3) TACACS+服务器发送认证回应报文，请求用户名；
4) TACACS+客户端向用户询问用户名。
5) 用户输入登陆的用户名信息。
6) TACACS+客户端收到用户名后，向 TACACS+服务器发送认证持续报文，其中包括了用户名。
7) TACACS+服务器发送认证回应报文，请求登录密码；
8) TACACS+客户端收到向用户询问登录密码。
9) 用户输入登陆的密码信息。
10) TACACS+客户端收到登录密码后，向 TACACS+服务器发送认证持续报文，其中包括了登录密码。
11) TACACS+服务器发送认证回应报文，指示用户通过认证。

2. 认证通过后对用户进行授权：
1) TACACS+客户端向 TACACS+服务器发送授权请求报文。
2) TACACS+服务器发送授权回应报文，指示用户通过授权。
3) TACACS+客户端收到授权回应成功报文，向用户输出网络设备的配置界面。

3. 授权通过后，需要对登陆的用户进行记账，审计。
1) TACACS+客户端向 TACACS+服务器发送记账开始报文。
2) TACACS+服务器发送记账回应报文，指示记账开始报文已经收到。
3) 用户退出。
4) TACACS+客户端向 TACACS+服务器发送记账结束报文。
5) TACACS+服务器发送记账回应报文，指示记账结束报文已经收到。

13.4 配置详解

配置项	配置建议&相关命令	
配置 TACACS+基本功能	⚠ 必须配置。用于使能 TACACS+安全服务。	
	tacacs-server host	配置 tacacs+服务器
	tacacs-server key	指定服务器与网络设备共享的密钥
	tacacs-server timeout	配置设备与 TACACS+服务器通信时，等待服务器的全局超时时间
配置 TACACS+的认证、授权、记账分离处理功能	⚠ 可选配置。用于分离处理认证、授权、记账请求。	
	aaa group server tacacs+	配置 TACACS+服务器组，将不同的 TACACS+服务器划分到不同的组
	server	添加 TACACS+服务器组的服务器

13.4.1 配置TACACS+基本功能

配置效果

- 配置完成，TACACS+的基本功能准备就绪。配置 AAA 的方法列表时，指定使用 TACACS+方法，即可实现 TACACS+的认证、授权、记账。
- 进行认证、授权、记账操作时，TACACS+依据配置顺序向所配置的 TACACS+服务器发起认证、授权、记账请求。如果服务器响应超时，则依次遍历 TACACS+服务器列表。

注意事项

- TACACS+安全服务是 AAA 服务的一种，需要使用命令 **aaa new-model** 来使能安全服务。
- 配置了 TACACS+基本功能后，只是提供了一种安全服务，需要在配置 AAA 方法列表时指定使用 TACACS+服务，TACACS+的功能才会生效。

配置方法

↘ 启用 AAA

- 必须配置，启用 AAA 之后，才能配置 AAA 方法列表。TACACS+提供服务供是依赖于 AAA 方法列表的。

【命令格式】 **aaa new-model**
【参数说明】 -
【缺省配置】 AAA 功能没有打开。
【命令模式】 全局模式
【使用指导】 启用 AAA 之后，才能配置 AAA 方法列表。TACACS+提供服务供是依赖于 AAA 方法列表的。

↘ 配置 TACACS+服务器的 IP 地址

- 必须配置，否则设备无法和 TACACS+服务器通信来实现 AAA 功能。

【命令格式】 **tacacs-server host** {*ipv4-address* } [**port***integer*] [**timeout** *integer*][**key** [**0** | **7**] *text-string*]
【参数说明】 *ipv4-address*：TACACS+服务器的 ipv4 地址。
port*integer*：TACACS+通信使用的 TCP 端口，默认为 TCP 端口 49。
timeout *integer*：与该 TACACS+服务器通信的超时时间，默认使用全局配置的超时时间。
key [**0** | **7**] *text-string*：配置用于该服务器的共享密钥，未配置则使用全局配置。配置的密钥可以指定加密类型，0 为无加密，7 简单加密，默认为 0。。
【缺省配置】 没有配置任何 TACACS+服务器
【命令模式】 全局模式
【使用指导】 可以在配置 IP 地址的同时指定该服务器的共享密钥，如果没有指定，则使用 **tacacs-server key** 命令配置的全局密钥作为该服务器的共享密钥。共享密钥必须与服务器上配置的完全相同。
可以在配置 IP 地址的同时指定该服务器的通信端口。
可以在配置 IP 地址的同时指定与该服务器通信的超时时间。

↘ 配置 TACACS+服务器的共享密钥

- 可选配置。

- 如果没有通过该命令配置全局的通信协议，则在使用 **tacacs-server host** 命令添加服务器信息时，需要通过 **key** 关键字指定基于服务器的共享密钥，否则设备将无法和 TACACS+服务器进行通信。
- 如果在使用 **tacacs-server host** 命令添加服务器时没有通过 **key** 关键字指定共享密钥，则使用该全局密钥。

【命令格式】 **tacacs-server** [**key** [**0** | **7**] *text-string*]
【参数说明】 *text-string*：共享口令的文本
0 | 7：口令的加密类型，**0** 无加密，**7** 简单加密。
【缺省配置】 没有配置任何 TACACS+服务器的共享密钥。
【命令模式】 全局模式
【使用指导】 该命令配置全局使用的共享密钥服务器当我们需要为每个服务器指定不同的密钥时，我们使用 **tacacs-server host** 命令中的 **key** 选项实现。

配置 TACACS+服务器的超时时间

- 可选配置。
- 当设备和服务器之间的链路不稳定时，可以将超时时间改大。

【命令格式】 **tacacs-server timeout***seconds*
【参数说明】 *seconds*：超时时间（单位为秒）。可设置的值范围为 1-1000 秒。
【缺省配置】 5 秒
【命令模式】 全局模式
【使用指导】 配置全局的服务器响应超时时间。当我们需要为每个服务器指定不同的超时时间时，使用 **tacacs-server host** 命令中的 **timeout** 选项实现。

检验方法

配置 AAA 方法列表使用 TACACS+方法，用户进行认证、授权、记账

- 设备与 TACACS+服务器进行交互，通过抓包可以查看设备与服务器间的 TACACS+协议的交互过程。
- 通过服务器的日志确认认证、授权、记账是否正常。

配置举例

Login 认证使用 TACACS+

【网络环境】

图 13-4



【注释】
- A 为发起 TACACS+请求的客户端。

【配置方法】
- B 为处理 TACACS+请求的服务器。
- 配置启用 AAA。
- 配置 tacacs+ server 信息。
- 配置使用 tacacs+的认证方法。
- 在接口上应用配置认证方法。

A

```
Ruijie#configure terminal
Ruijie(config)#aaa new-model
Ruijie(config)# tacacs-server host 192.168.5.22
Ruijie(config)#tacacs-server key aaa
Ruijie(config)#aaa authentication login test group tacacs+
Ruijie(config)# line vty 0 4
Ruijie(config-line)#login authentication test
```

【检验方法】 在 PC 上 telnet 到设备上 ,要求输入用户名和密码。输入正确的用户名和密码 ,能够登录到设备上。在 TACACS+服务器上可以查看到此用户的认证日志。

常见错误

- 没有使能 AAA 安全服务。
- 设备配置的 key 与服务器配置的 key 不一致。
- 没有配置方法列表。

13.4.2 配置TACACS+的认证、授权、记账分离处理功能

配置效果

- 安全服务中的认证、授权、记账分别由不同的 TACACS+服务器处理。可以提高安全性，并实现一定负载均衡。

注意事项

- TACACS+安全服务是 AAA 服务的一种，需要使用命令 **aaa new-model** 来使能安全服务。
- 配置了 TACACS+基本功能后，只是提供了一种安全服务，需要在配置 AAA 方法列表时指定使用 TACACS+服务，TACACS+的功能才会生效。

配置方法

↘ 配置 TACACS+服务器组

- 必须配置。默认情况下，只有 tacacs+这一个服务器组，无法实现认证、授权、记账分离处理。

- 配置三个 TACACS+服务器组分别用于认证、授权、记账处理。

【命令格式】 **aaa group server tacacs+***group-name*
【参数说明】 *group-name*：组的名称，组名称不可为”radius”和”tacacs+”（不包括引号），这两个名字为内置组名字
【缺省配置】 没有配置 TACACS+服务器组
【命令模式】 全局模式
【使用指导】 通过对 TACACS+服务器进行分组，认证、授权、计帐可以使用不同的服务器组来完成。

配置 TACACS+服务器组引用服务器

- 必须配置。如果没有配置，则服务器组内没有服务器，设备无法与 TACACS+服务器通信。
- 在服务器组配置模式下，引用已经使用 **tacacs-server host** 命令配置好的服务器。

【命令格式】 Server {*ipv4-address* }
【参数说明】 *ipv4-address*：TACACS+服务器的 IPv4 地址。
【缺省配置】 无服务器配置。
【配置模式】 TACACS+服务器组配置模式
【使用指导】 配置此命令前，必须通过命令 **aaa group server tacacs+**进入 TACACS+组配置模式。
TACACS+服务器组中配置的服务器地址，必须在全局配置模式下，通过 **tacacs-server host** 命令配置此服务器。
如果一个服务器组内引用了多个服务器时，当一个服务器没有响应时，设备会继续向组内的下一个服务器发送 TACACS+请求。

检验方法

配置 AAA 方法列表使用 TACACS+方法，用户进行认证、授权、记账。

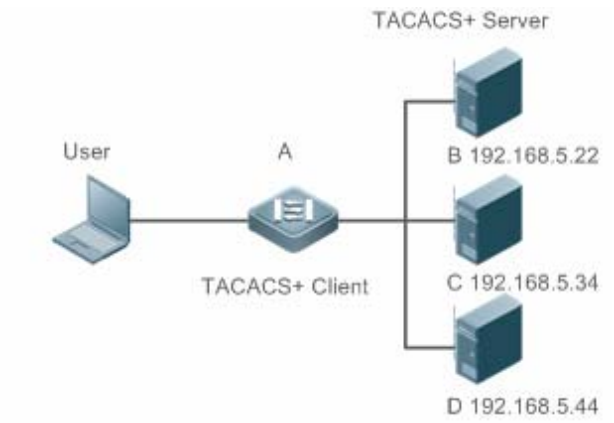
- 设备与 TACACS+服务器进行交互，通过抓包可以看到认证、授权、记账报文分别和不同的服务器交互，以及报文的源地址。

配置举例

配置认证、授权、记账使用不同 TACACS+服务器组。

【网络环境】

图 13-5



【注释】

- A 为发起 TACACS+请求的客户端。
- B 为处理 TACACS+认证请求的服务器。
- C 为处理 TACACS+授权请求的服务器。
- D 为处理 TACACS+记账请求的服务器。

【配置方法】

- 配置启用 AAA。
- 配置 TACACS+ server 信息。
- 配置 TACACS+服务器组。
- 向服务器组中添加服务器
- 配置使用 TACACS+的认证方法。
- 配置使用 TACACS+的授权方法。
- 配置使用 TACACS+的记账方法。
- 在接口上应用认证方法。
- 在接口上应用授权方法。
- 在接口上应用记账方法。

```
Ruijie#configure terminal
Ruijie(Ruijie(config)#aaa new-model
Ruijie(config)# tacacs-server host 192.168.5.22
Ruijie(config)# tacacs-server host 192.168.5.34
Ruijie(config)# tacacs-server host 192.168.5.44
Ruijie(config)#tacacs-server key aaa
Ruijie(config)#aaa group server tacacs+ tacgrp1
Ruijie(config-gs-tacacs)# server 192.168.5.22
Ruijie(config-gs-tacacs)# exit
Ruijie(config)#aaa group server tacacs+ tacgrp2
Ruijie(config-gs-tacacs)# server 192.168.5.34
Ruijie(config-gs-tacacs)# exit
Ruijie(config)#aaa group server tacacs+ tacgrp3
Ruijie(config-gs-tacacs)# server 192.168.5.44
Ruijie(config-gs-tacacs)# exit
Ruijie(config)#aaa authentication login test1 group tacacs+
Ruijie(config)#aaa authentication enabledefault group tacgrp1
Ruijie(config)#aaa authorizationexectest2 group tacgrp2
Ruijie(config)#aaa accountingcommands15 test3 start-stop group tacgrp3
Ruijie(config)# line vty 0 4
Ruijie(config-line)#login authentication test1
Ruijie(config-line)#authorization exec test2
Ruijie(config-line)# accounting commands 15 test3
```

【检验方法】 在 PC 上 telnet 到设备上 ,要求输入用户名和密码。输入正确的用户名和密码 ,能够登录到设备上。输入 **enable** 命令，输入正确的 **enable** 密码，发起 **enable** 认证，认证通过后，进入特权模式。对设备进行操作后，用户退出设备。

在服务器 192.168.5.22 上可以查看到此用户的认证日志。

在服务器 192.168.5.22 上可以查看到此用户的 **enable** 认证日志。

在服务器 192.168.5.34 上可以查看到此用户的 **exec** 授权日志。

在服务器 192.168.5.44 上可以查看到此用户的命令记账日志。

常见配置错误

- 没有使能 AAA 安全服务。
- 设备配置的 key 与服务器配置的 key 不一致。
- 服务器组引用为定义的服务器。
- 没有配置方法列表。

13.5 监视与维护

清除各类信息

无

查看运行情况

作用	命令
显示和各 TACACS+服务器的交互运行情况。	**show tacacs**

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 TACACS+的调试开关。	**debug tacacs+**

14 Web 认证

14.1 概述

14.1.1 Web认证概述

Web 认证是一种对用户访问网络的权限进行控制的身份认证方法，这种认证方法不需要用户安装专用的客户端认证软件，使用普通的浏览器软件就可以进行身份认证。

未认证用户使用浏览器上网时，网络设备会强制浏览器访问特定站点，也就是 Web 认证服务器，通常称为 Portal 服务器。用户无需认证即可访问 Portal 服务器上的服务，比如下载安全补丁、阅读公告信息等。当用户需要访问认证服务器以外的其它网络资源时，就必须通过浏览器在 Portal 服务器上进行身份认证，只有认证通过后才可以使用网络资源。

除了认证上的便利性之外，由于 Portal 服务器和用户的浏览器有页面交互，可以利用这个特性在 Portal 服务器页面放置一些广告、通知、业务链接等个性化的服务。

锐捷 Web 认证概述

锐捷 web 认证有 3 个版本，不同版本的 Web 认证流程不同，我们将其分别称为锐捷一代 Web 认证、锐捷二代 Web 认证、锐捷内置 Portal Web 认证。细节详见功能详解章节。

⚠ 由于三个版本的 Web 证存在较大差异，配置参数也差别很大，因此在配置 Web 认证相关功能前必须仔细阅读对应章节内容，避免配置错误。

⚠ 二代 Web 认证和内置 Portal Web 认证均支持设备的本地帐号认证，但是由于 RADIUS 认证在实际网络部署中更为常见，因此应用举例中使用了 RADIUS 认证。

⚠ 不同产品端口的概念不一样，比如交换机的端口表示具体的物理端口，路由器则有可能是子接口，无线则可能是一个 WLAN，本文统一采用术语端口，使用具体产品时再依据产品的概念找到对应的配置位置。

⚠ Web 认证支持低流量检测用户下线，具体参考 Layer23 组件的配置手册。

⚠ EG 产品上的 Web 认证基于全局开关，本文档主要介绍接口上的配置，实际使用 EG 产品时在全局配置模式配置。

⚠ Web 认证支持域认证，也就是帐号采用"用户名@域名"的形式，该功能需要 AAA 开启域认证功能，详细参考 AAA 的配置手册。

ℹ 下文仅介绍 Web 认证的相关内容。

协议规范

- HTTP：RFC1945 RFC2068

- HTTPS：RFC2818
- SNMP： RFC1157 RFC 2578
- RADIUS： RFC2865 RFC2866 RFC3576
- 与 MAC 短信认证相关的规范参照《中国移动无线局域网(WLAN)设备接口规范 V3.1.0_20130901(MAC 认证扩展).doc》，《浙江移动 WLAN 快速认证方案-接口规范 V1.1-2011.3.22.doc》，《基于 MAC+短信的 WLAN 快速认证方案 V1.1-2011.3.21.doc》

14.2 典型应用

典型应用	场景描述
web 认证基本场景	常见的二层基本认证场景，设备、portal 服务器、RADIUS 服务器组成认证体系，用户通过二层网络连接设备

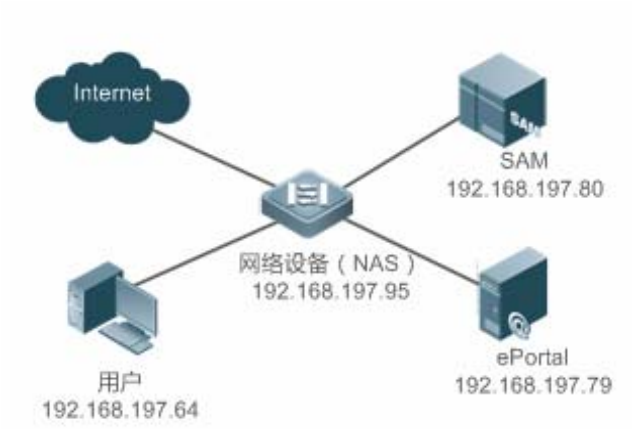
14.2.1 Web认证基本场景

应用场景

如 图 21-1 所示

- 在网络设备上部署 Web 认证方案
- 下联用户需要通过 Web 认证才能访问 internet

图 14-1 Web 认证方案网络拓扑图



【注释】 Web 认证方案可以用于二三层网络。相比于二层网络，三层网络的特点是报文经过了路由后 mac 地址和 vid 信息变了，此时对终端的唯一性识别只有 ip，因此在三层设备上，web 认证的绑定策略只能用仅 ip 模式。此处以二层接入设备为例。

RADIUS 服务器安装了锐捷 SAM 服务器软件， Portal 服务器安装了锐捷 ePortal 服务器软件。

功能部属

- 在 NAS 上用户所在端口或者全局开启 Web 认证受控(EG 设备上为全局开启)。
- 在 NAS 上配置 Web 认证服务器信息和通信加密密钥(仅一代认证和二代认证)。
- 在 NAS 上配置 Web 认证服务器 SNMP 通信参数(仅一代认证和二代认证)。
- 在 Portal 服务器和 SAM 服务器上配置两个服务器间相匹配的通信参数(仅一代 Web 认证)。
- 在 SAM 服务器上配置开通用户账户。
- 在 NAS 上配置 AAA 功能和方法列表(仅二代认证和内置认证)。
- 在 NAS 上配置 RADIUS 服务器地址(仅二代认证和内置认证)。
- 在 NAS 上配置 Web 认证方法列表名(仅二代认证和内置认证)。

14.3 功能详解

基本概念

↘ 一代 Web 认证方案

一代 Web 认证方案需要锐捷专有 ePortal 服务器软件的配合，用户通过 ePortal 软件提供的认证页面提交认证信息， ePortal 服务器直接向相应的 RADIUS 服务器请求认证，认证通过后将用户信息通过 SNMP 协议通告设备，由设备完成用户的准入控制。一代 Web 认证通过私有 SNMP 节点进行认证通信，认证记账功能由 ePortal 服务器承载，减轻了设备的业务压力。

↘ 二代 Web 认证方案

二代 Web 认证方案兼容中国移动 Portal 协议规范。Portal 服务器单纯负责用户页面交互部分，较为简单；而 RADIUS 服务器认证交互部分由设备来实现；Portal 服务器和设备间的交互遵循《中移动 portal 协议规范》。用户通过 Portal 服务器提供的认证页面提交认证信息， Portal 服务器将用户信息通过 Portal 协议告知网络设备，网络设备利用该身份信息完成 RADIUS 服务器认证，对合法用户进行准入，同时将结果信息回应给 Portal 服务器。

二代 Web 认证方案由于主要流程都是在设备上完成，对设备的要求比较高，处理能力压力大；但是 Portal 服务器得到了简化，同时使用业界支持度较高的中国移动 Portal 规范进行交互，使得各设备厂商和服务器厂商能够开发出兼容的产品。

↘ 锐捷内置 Portal Web 认证

内置 Portal Web 认证由设备集成页面交互功能，以及 RADISU 服务器认证交互部分的功能。设备默认预置了页面包，用户也可以按照配置手册中介绍的页面包定制规范制作自己的页面包并下载到设备的存储介质上生效。

↘ 锐捷各类 Web 认证的对比

认证角色：

- 客户端：功能一样。
- 网络设备：锐捷一代 Web 认证里面，设备只做重定向，以及和 Portal 服务器交互用户的上下网通知。

- Portal 服务器：锐捷一代 Web 认证里面，Portal 服务器负责和客户端的页面交互、用户的认证、通告网络设备用户认证是否可上网。
- 网络设备：锐捷二代 Web 认证里面，设备需要负责重定向、用户的认证、通告 Portal 服务器认证是否成功。
- Portal 服务器：锐捷二代 Web 认证里面，Portal 服务器负责和客户端的页面交互、通告网络设备用户的认证信息、接收网络设备通告的用户是否认证成功。
- 网络设备：内置 Portal Web 认证里面，设备集成重定向、页面交互、以及用户的认证等功能。
- Portal 服务器：锐捷内置 Web 认证中，Portal 服务器由设备内置实现，功能较为简单，主要负责页面交互过程。
- Radius 服务器：功能一样。

认证流程：

- 锐捷二代 Web 认证将认证记账从 Portal 服务器迁移到网络设备。
- 锐捷二代 Web 认证由于认证在网络设备上，因此就无需等待来自 Portal 服务器发送的用户是否可上网的通告。
- 锐捷内置 Web 认证将一二代中 Portal 服务器功能简化，并移到设备上进行支持。

下线流程

- 锐捷一代 Web 认证中，下线动作可能来自 Portal 服务器的通告或者本机的流量检测、端口状态检测。
- 锐捷一代 Web 认证中，计费结束报文是 Portal 服务器发起的。
- 锐捷二代 Web 认证中，下线动作可能来自 Portal 服务器的通告、RADIUS 服务器的踢线通告、或者本机的流量检测、端口状态检测。
- 锐捷二代 Web 认证中，计费结束报文是设备发起的。
- 锐捷内置 Portal Web 认证中，下线动作可能来自用户主动点击页面的下线按钮、RADIUS 服务器的踢线通告、或者本机的流量检测、端口状态检测。
- 锐捷内置 Portal Web 认证中，计费报文也是由设备发起。

实际网络中是部署一代 Web 认证，还是部署二代 Web 认证或内置 Web 认证，取决于所使用的 Portal 服务器的类型。

各类 Web 认证中有部分参数是可以共用，有些是不能共用的，请仔细阅读，避免参数配置不当导致 Web 认证使用不正常。

功能特性

功能特性	作用
锐捷一代 Web 认证	网络中部署了 Portal 服务器且 Portal 服务器仅支持一代 Web 认证
锐捷二代 Web 认证	网络中的部署了 Portal 服务器且 Portal 服务器兼容中移动 portal 规范
锐捷内置 Portal Web 认证	网络中没有部署 Portal 服务器，需要设备支持页面交互功能

14.3.1 锐捷一代Web认证

HTTP 拦截

HTTP 拦截指网络设备将原本需要转发的 HTTP 报文拦截下来，不进行转发。这些 HTTP 报文是连接在网络设备下的用户的浏览器所发出的，但目的并不是网络设备本身。例如，某用户通过 IE 浏览器访问 www.google.com，网络设备本应该将这些 HTTP 请求报文转发到网关的，但如果启动 HTTP 拦截，这些报文将不被转发。

HTTP 拦截之后，网络设备需要将用户的 HTTP 连接请求转向自己，于是网络设备和用户之间将建立起连接会话。网络设备将利用 HTTP 重定向功能，将重定向页面推送给用户，用户的浏览器上将弹出一个页面，这个页面可以是认证页面，也可以是下载软件的链接等等。

在 Web 认证功能中，哪些用户所发出的到哪个目的端口的 HTTP 报文需要进行拦截，哪些不需要，都是可以设置的。一般地，未经过认证的用户发出的 HTTP 请求报文会被拦截，已通过认证的用户将不被拦截。HTTP 拦截是 Web 认证功能的基础，一旦浏览器发出的 HTTP 报文被拦截，就会自动触发 Web 认证的过程。

HTTP 重定向

根据 HTTP 协议规定，正常情况下，用户的浏览器发出 HTTP GET 或 HEAD 请求报文后，如果接收一方能够提供资源，则以 200 报文响应，如果本地不能提供资源，则可以使用 302 报文响应。在 302 响应报文中，提供了一个新的站点路径，用户收到响应后，可以向这个新的站点重新发出 HTTP GET 或 HEAD 报文请求资源，这就是重定向。

HTTP 重定向是 Web 认证的重要环节，是发生在 HTTP 拦截之后的，利用的就是 HTTP 协议中的 302 报文的特性。HTTP 拦截过程将使得网络设备和用户之间建立起连接会话，随后用户将（本应发给其他站点的）HTTP GET 或 HEAD 报文发给网络设备，网络设备收到后，回应以 302 报文，并且在 302 报文中加入重定向页面的站点路径，这样用户将向这个站点路径重新发出请求，就会获取到重定向的页面。

由于越来越多的应用程序基于 HTTP 协议运行，采用 302 重定向报文有可能会将大量的非浏览器发出的 HTTP 流引向 Portal 服务器，影响网络认证，因此设备的重定向技术采用的是通过 js 脚本代替 302 报文，这一技术称为降噪。

工作原理

组网拓扑图同 图 14-1 Web 认证方案网络拓扑图。

Web 认证的角色：

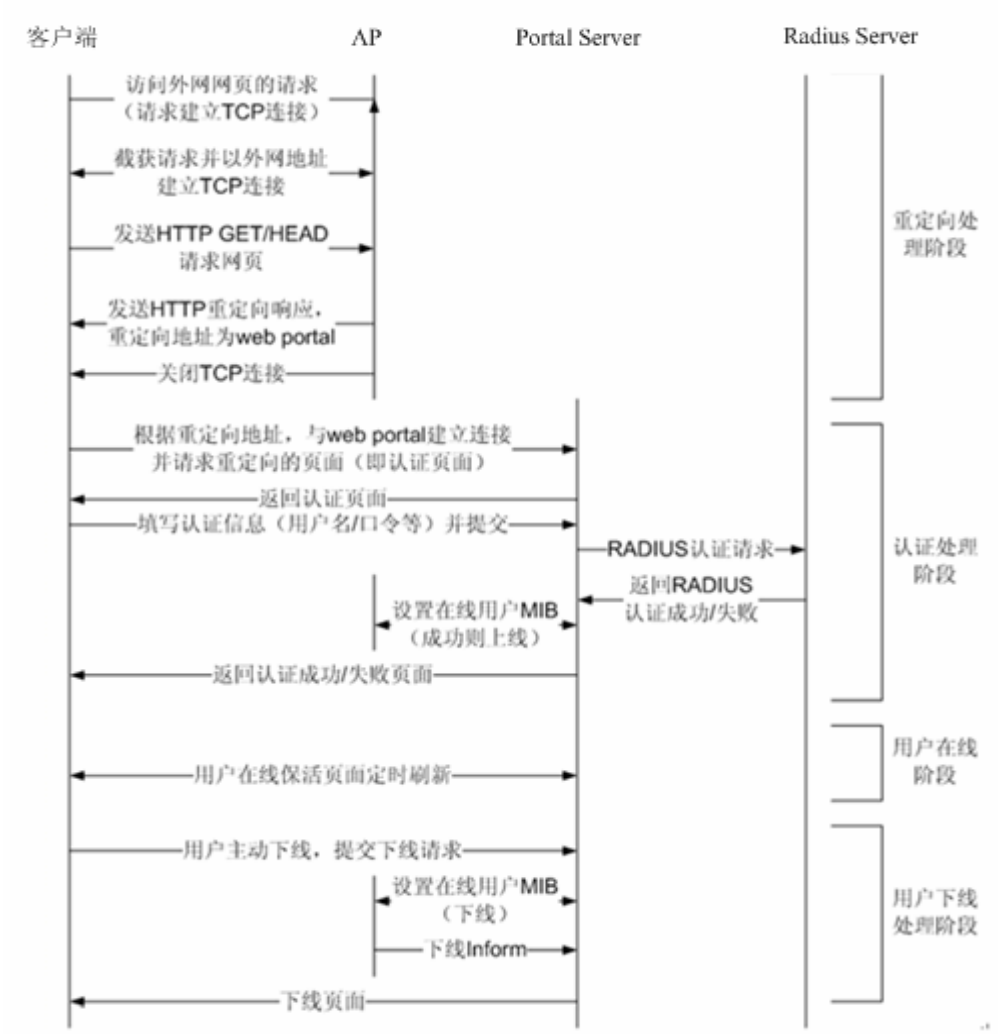
认证客户端：通常是浏览器，运行 HTTP 协议，用户通过浏览器上网时浏览器将发出 HTTP 请求。
网络设备：在网络拓扑中一般是接入层设备（例如在无线网络中可以是无线 AP），一般与用户终端设备直接相连接，在设备上需要启动 Web 认证功能。
Portal 服务器：提供 Web 认证的认证界面和相关操作。Portal 服务器接受认证客户端发出的基于 HTTP 的认证请求，提取其中的账号信息，将此信息发送到认证服务器进行认证，然后通告用户和网络设备认证结果。图中为锐捷 ePortal 服务器。
Radius 服务器：提供基于 RAIUS 协议的远程用户认证，Portal 服务器从 HTTP 中获取用户的认证账号信息，然后通过 RADIUS 协议向 Radius 服务器请求认证。Radius 服务器通过 RADIUS 协议向 Portal 服务器反馈认证结果。图中为锐捷 SAM 服务器。
Web 认证的流程：

4. 在认证之前，设备将未认证用户发出的所有 HTTP 请求都拦截下来，并重定向到 Portal 服务器去，这样在用户的浏览器上将弹出一个认证页面。

在认证过程中，用户在认证页面上输入认证信息（用户名、口令、校验码等等）与 Portal 服务器交互，完成身份认证的功能。在认证通过后，Portal 服务器将通知设备该用户已通过认证，设备将允许用户访问互联网资源。

详细的原理图如下图所示：(图中以 AP 为例)

图 14-2 锐捷一代 Web 认证流程图



用户下线流程：

用户下线分两种类型,一种是设备端检测到用户下线,比如用户时长到达,流量用完,链路断开等;一种是 Portal 服务器端发现用户下线,比如用户通过下线页面触发了下线申请,保活页面失效等。

5. 第一种情况，设备发现用户下线时,通告 Portal 服务器用户下线，服务器设置设备删除用户信息(通过 SNMP 协议)。Portal 服务器向用户返回下线页面。

第二种情况， Portal 服务器发现用户下线后,通告设备用户下线（通过 SNMP 协议)。Portal 服务器向用户返回下线页面。

2 种情况下，Portal 服务器都会向 Radius 服务器发起计费结束请求，通告 Radius 服务器用户下线。

相关配置

创建配置模板

缺省情况下无配置。

在全局配置模式下使用 **web-auth template eportalv1** 命令创建模板。

可以使用该配置模板进行 web 认证功能。

配置服务器 IP 地址

缺省情况下无配置。

在模板配置模式使用 **ip** { *ip-address* }来配置服务器 IP 地址。

访问服务器的请求被设备放行，并且支持对发往服务器的请求进行限速保护。

配置服务器认证 URL

缺省情况下无配置。

在模板配置模式使用 **url** { *url-string* }来配置。

用户重定向到的 URL 地址，通常使用 portal 认证页面地址。

配置绑定模式

EG，NBR 缺省情况下为仅 ip 绑定。

在模板配置模式使用 **bindmode** 来配置。

对于跨三层网络认证的环境，由于经过路由后 mac 地址已经变了，需要配置为仅 ip 绑定模式。

配置通信加密密钥

缺省情况下无配置。

在全局配置模式下使用 **web-auth portal key** { *string* }来配置通信加密密钥。

用作 URL 参数加密，避免信息泄漏。

开启 web 认证

缺省情况下该功能关闭。

在全局模式下使用 **web-auth enable** 命令开启 web 认证受控。

开启认证后未认证用户会被重定向到认证页面。

配置 web 认证 SNMP 协议服务器

缺省情况下无配置。

在全局配置模式下使用 **snmp-server host** { *ip-address* } **version 2c** { *community-string* } **web-auth** 来配置 web 认证 SNMP 协议服务器。

设备可以通过 inform/trap 报文通告用户下线消息给配置的服务器。

配置服务器 SNMP 通信团体字

缺省情况下无配置。

在全局配置模式下使用 **snmp-server community** {*community-string*} **rw** 来配置服务器 SNMP 通信团体字。

服务器通过该团体字来读写设备的用户表项信息。

启用 SNMP TRAP/INFORM 通告功能

缺省情况下无配置。

在全局配置模式下使用 **snmp-server enable traps web-auth** 来配置启用 SNMP TRAP/INFORM 通告功能。

使能通告功能，用于设备向服务器通告用户下线消息。

14.3.2 锐捷二代Web认证

HTTP 拦截

同锐捷一代 Web 认证的 HTTP 拦截技术。

HTTP 重定向

同锐捷一代 Web 认证的 HTTP 重定向技术。

工作原理

组网拓扑图同 图 14-1 Web 认证方案网络拓扑图。

Web 认证的角色：

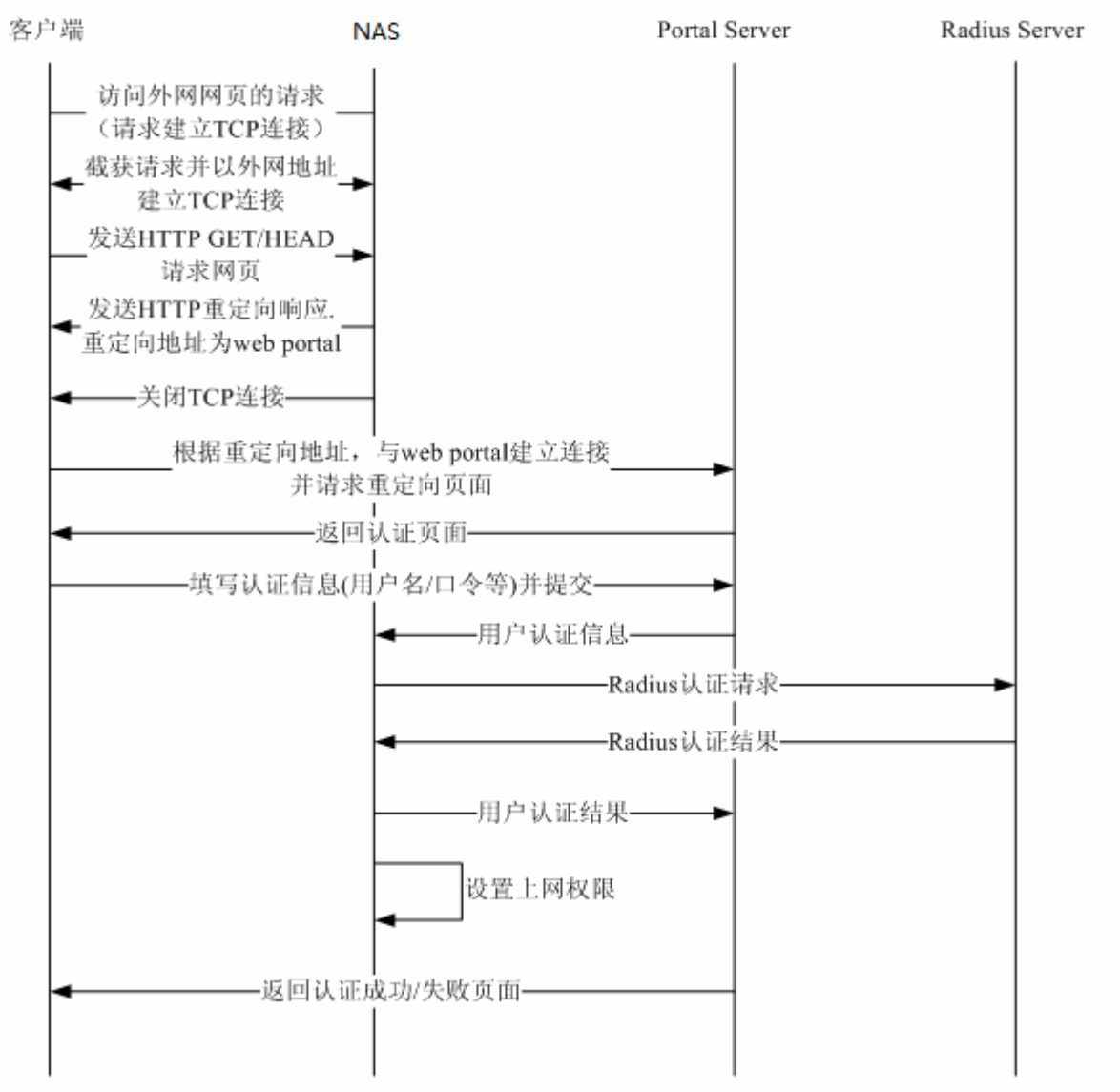
1. 认证客户端：通常是一个浏览器，运行 HTTP 协议，用户通过浏览器上网时浏览器将发出 HTTP 请求。
2. 网络设备：在网络拓扑中一般是接入层设备（例如在无线网络中可以是无线 AP），一般与用户终端设备直接相连接，在设备上需要启动 Web 认证功能。设备接收 Portal 服务器发过来的用户认证信息，并向 Radius 服务器发起认证请求，根据认证结果设置用户是否可以上网，同时向 Portal 服务器反馈认证结果。
3. Portal 服务器：提供 Web 认证的认证界面和相关操作。Portal 服务器接受认证客户端发出的基于 HTTP 的认证请求，提取其中的账号信息，将此信息发送到网络设备，同时根据网络设备反馈的认证结果，通过页面反馈给用户。图中为锐捷 ePortal 服务器。
4. Radius 服务器：提供基于 RADIUS 协议的远程用户认证。图中为锐捷 SAM 服务器。

Web 认证主要流程：

6. 在认证之前，设备将未认证用户发出的所有 HTTP 请求都拦截下来，并重定向到 Portal 服务器去，这样在用户的浏览器上将弹出一个认证页面。

在认证过程中，用户在认证页面上输入认证信息（用户名、口令、校验码等等）与 Portal 服务器交互。
Portal 服务器将用户的认证信息发给设备
设备向 Radius 服务器发起认证，并将认证结果反馈给 Portal 服务器。
Portal 服务器向用户返回页面，提示认证结果（成功或失败）。

图 14-3 锐捷二代 Web 认证流程



用户下线流程：

用户下线分两种类型,一种是设备端检测到用户下线,比如用户时长到达,流量用完,链路断开等;一种是 portal 服务器端发现用户下线,比如用户通过下线页面触发了下线申请等。

7. 用户主动点击页面上的下线按钮，选择下线，Portal 服务器通告设备将用户下线。
设备检测到终端低流量将用户下线，具体依赖所配置的低流量检测参数而定。

RADIUS 服务器因为某种策略原因，将用户踢线，设备通告 Portal 服务器，Portal 服务器向终端推送下线页面。

相关配置

创建配置模板

缺省情况下无配置。

在全局配置模式下使用 **web-auth template{eportalv2 |** *template-name* **v2}**命令创建二代模板。

可以使用该配置模板进行 web 认证功能。

配置服务器 IP 地址

缺省情况下无配置。

在模板配置模式使用 **ip** { *ip-address* }来配置服务器 IP 地址。

访问服务器的请求被设备放行，并且支持对发往服务器的请求进行限速保护。

配置服务器认证 URL

缺省情况下无配置。

在模板配置模式使用 **url** { *url-string* }来配置。

用户重定向到的 URL 地址，通常使用 portal 认证页面地址。

配置绑定模式

EG，NBR 缺省情况下为仅 ip 绑定。

在模板配置模式使用 **bindmode** 来配置。

对于跨三层网络认证的环境，由于经过路由后 mac 地址已经变了，需要配置为仅 ip 绑定模式。

配置通信加密密钥

缺省情况下无配置。

在全局配置模式下使用 **web-auth portal key** { *string* }来配置通信加密密钥。

用作 URL 参数加密，避免信息泄漏。

开启 web 认证

缺省情况下该功能关闭。

在全局模式下使用 **web-auth enable** 命令开启 web 认证受控。

开启认证后未认证用户会被重定向到认证页面。

配置启用 AAA 认证

缺省情况下关闭 AAA 认证。

在全局配置模式下使用 **aaa new-model** 命令来开启 AAA 认证功能。

二代 Web 认证功能需要依赖于 AAA 认证功能，使用时需要开启 AAA 功能。

↘ 配置 RADIUS 服务器和通信密钥

缺省情况下无配置。

在全局配置模式下使用 **radius-server host** 命令来配置 RADIUS 服务器和通信密钥。

对应于 web 认证中的 RADIUS 服务器。用于为 Web 认证用户进行身份校验。

↘ 配置 AAA 模块 web 认证的方法列表

缺省情况下无配置。

在全局配置模式下使用 **aaa authentication web-auth** 命令来配置二代 web 认证的认证方法。

Web 认证功能可以配置使用该方法列表来进行认证交互。

↘ 配置 AAA 模块网络记账方法列表

缺省情况下无配置。

在全局配置模式下使用 **aaa accounting network** 命令来配置网络记账方法。

Web 认证功能可以配置使用该方法列表来进行记账交互。

↘ 配置 web 认证使用的 AAA 认证方法列表名

缺省情况下使用 default 方法。

在模板配置模式下使用 **authentication** 命令来配置。

Web 认证功能通过该方法列表名字向 AAA 功能发起认证请求。

↘ 配置 web 认证使用的 AAA 认证记账列表名

缺省情况下使用 default 方法。

在模板配置模式下使用 **accounting** 命令来配置。

Web 认证功能通过该方法列表名字向 AAA 功能发起记账请求。

↘ 配置 portal 服务器的通信 UDP 端口号

缺省情况下使用 50100 端口号。

在模板配置模式下使用 **port** 命令来配置。

设备通过发送报文到该端口来同 portal 服务器进行交互。

14.3.3 锐捷内置Portal Web认证

HTTP 拦截

同锐捷一代 Web 认证的 HTTP 拦截技术。

HTTP 重定向

同锐捷一代 Web 认证的 HTTP 重定向技术。

工作原理

相比图 14-1 Web 认证方案网络拓扑图，内置 Portal Web 认证没有 Portal 服务器。

Web 认证的角色：

8. 认证客户端：通常是一个浏览器，运行 HTTP 协议，用户通过浏览器上网时浏览器将发出 HTTP 请求。

网络设备：在网络拓扑中一般是接入层设备，一般与用户终端设备直接相连接(有线或者无线)，在设备上需要启动内置 Portal Web 认证功能。由设备解析用户在页面中输入的帐号并向 Radius 服务器发起认证请求，根据认证结果设置用户是否可以上网，同时向终端浏览器推送认证结果。

Radius 服务器：提供基于 RADIUS 协议的远程用户认证。图中为锐捷 SAM 服务器。

Web 认证主要流程：

9. 在认证之前，设备将未认证用户发出的所有 HTTP 请求都拦截下来，并重定向到本机内置 Portal，这样在用户的浏览器上将弹出一个认证页面。

在认证过程中，用户在认证页面上输入认证信息（用户名、口令、校验码等等）与内置 Portal 交互。

设备向 Radius 服务器发起认证，并根据认证结果向用户返回页面，提示认证结果（成功或失败）。

用户下线流程：

10. 用户主动点击页面上的下线按钮，选择下线，设备检测到此页面动作，将用户下线。

设备检测到终端低流量将用户下线，具体依赖所配置的低流量检测参数而定。

RADIUS 服务器因为某种策略原因，将用户踢线，设备向终端推送下线页面。

相关配置

↘ 创建配置模板

缺省情况下无配置。

在全局配置模式下使用 **web-auth template iportal** 命令创建模板。

可以使用该配置模板配置内置 Portal Web 认证相关参数。

↘ 配置页面包

缺省情况下使用设备出厂自带的页面包。

在模板配置模式使用 **page-suite** 来配置使用指定的页面包。

指定页面包之前需要先将页面包下载到 FLASH 中。

↘ 配置广告推送地址

缺省情况下无配置。

在模板配置模式使用 **popup** *url* 来配置。

该功能允许给用户推送指定页面地址。

配置广告推送方式

缺省情况认证后推送。

在模板配置模式使用 **popup mode** 来配置推送模式，有登录推送、认证后推送两种选项。

配置绑定模式

EG，NBR 缺省情况下为仅 ip 绑定。

在模板配置模式使用 **bindmode** 来配置。

对于跨三层网络认证的环境，由于经过路由后 mac 地址已经变了，需要配置为仅 ip 绑定模式。

开启 web 认证

缺省情况下该功能关闭。

在全局模式下使用 **web-auth enable** 命令开启用户所在端口 web 认证受控。

开启认证后端口下未认证用户会被重定向到认证页面。

配置启用 AAA 认证

缺省情况下关闭 AAA 认证。

在全局配置模式下使用 **aaa new-model** 命令来开启 AAA 认证功能。

内置 Web 认证功能需要依赖于 AAA 认证功能，使用时需要开启 AAA 功能。

配置 RADIUS 服务器和通信密钥

缺省情况下无配置。

在全局配置模式下使用 **radius-server host** 命令来配置 RADIUS 服务器和通信密钥。

对应于 Web 认证中的 RADIUS 服务器，用于为 Web 认证用户进行身份校验。

配置 AAA 模块 web 认证的方法列表

缺省情况下无配置。

在全局配置模式下使用 **aaa authentication iportal** 命令来配置内置认证的认证方法。

Web 认证功能可以配置使用该方法列表来进行认证交互。

配置 AAA 模块网络记账方法列表

缺省情况下无配置。

在全局配置模式下使用 **aaa accounting network** 命令来配置网络记账方法。

Web 认证功能可以配置使用该方法列表来进行记账交互

↘ 配置 web 认证使用的 AAA 认证方法列表名

缺省情况下使用 default 方法。

在模板配置模式下使用 **authentication** 命令来配置。

Web 认证功能通过该方法列表名字向 AAA 功能发起认证请求。

↘ 配置 web 认证使用的 AAA 认证记账列表名

缺省情况下使用 default 方法。

在模板配置模式下使用 **accounting** 命令来配置。

Web 认证功能通过该方法列表名字向 AAA 功能发起记账请求。

14.4 产品说明



NBR108G-P、NBR1500G、NBR2000G、NBR2000G-C、NBR3000G-S、NBR1000G-C 不支持 WEB 认证功能；NBR800G、NBR950G、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 WEB 认证功能。

NBR800G、NBR950G、NBR1000G-E、NBR6120-E 不支持二代 PORTAL；NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持二代 PORTAL。

NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1500G、NBR2000G 不支持内置认证跨三层无感知，NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR800G、NBR950G、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持内置认证跨三层无感知。

NBR800G、NBR950G、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持聚合口 WEB 认证；NBR1500G、NBR2000G、NBR2000G-C、NBR3000G-S、NBR1000G-C 不支持聚合口 WEB 认证。

14.5 配置详解

配置项	配置建议 & 相关命令	
配置一代 Web 认证功能	⚠ 必须配置。用于配置一代 Web 认证功能基本参数	
	web-auth template eportalv1	创建一代 eportalv1 模板
	ip { *ip-address* }	配置服务器的 IP 地址
	url { *url-string* }	配置服务器的主页地址
	web-auth portal key { *key-string* }	配置服务器通信密钥
	snmp-server community { *community-string* } **rw**	配置 SNMP 通信团体字

	snmp-server host { *ip-address* } **inform version** 2c { *community-string* } **web-auth**	配置 SNMP 通信服务器
	snmp-server enable traps web-auth	使能 web 认证 trap/inform 通告
	web-auth enable	使能 web 认证
配置二代 web 认证功能	⚠ 必须配置。用于配置二代 Web 认证功能基本参数	
	aaa new-model	开启 AAA 功能
	radius-server host { *ip-address* } [**auth-port** *port-number*] [**acct-port** *port-number*] **key** { *string* }	配置 RADIUS 服务器和密钥
	aaa authentication web-auth { **default** | *list-name* } *method1* [*method2*...]	配置 Web 认证方法列表(使用 RADIUS 认证)
	aaa accounting network { **default** | *list-name* } **start-stop** *method1* [*method2*...]	配置网络记账方法列表(使用 RADIUS 记账)
	web-auth template { **eportalv2 |** *portal-name* **v2** }	创建二代认证模板
	ip { *ip-address* }	配置服务器的 IP 地址
	url { *url-string* }	配置服务器的主页地址
	web-auth portal key { *key-string* }	配置服务器通信密钥
	web-auth enable	使能 Web 认证
配置内置 Portal Web 认证	⚠ 必须配置。用于配置内置 Portal Web 认证功能基本参数	
	aaa new-model	开启 AAA 功能
	radius-server host { *ip-address* } [**auth-port** *port-number*] [**acct-port** *port-number*] **key** { *string* }	配置 RADIUS 服务器和密钥
	aaa authentication iportal { **default** | *list-name* } *method1* [*method2*...]	配置 Web 认证方法列表(使用 RADIUS 认证)
	aaa accounting network { **default** | *list-name* } **start-stop** *method1* [*method2*...]	配置网络记账方法列表(使用 RADIUS 记账)
	web-auth template iportal	创建内置 Portal Web 认证模板
	web-auth enable	使能 Web 认证
配置认证方法列表名	⚠ 可选配置。在 template 模板下指定认证方法列表名，和 AAA 模块的方法列表配置保持一致	
	authentication { *mlist-name* }	配置认证方法列表名(仅二代)
配置记账方法列表名	⚠ 可选配置。在 template 模板下指定记账方法列表名，和 AAA 模块的方法列表配置保持一致	
	accounting { *mlist-name* }	配置记账方法列表名(仅二代)
配置 Portal 服务器通信端口	⚠ 可选配置。在 template 模板下指定 Portal 服务器通信端口，需要和服务器端的的通信端口一致	
	port { *port-num* }	配置 portal 服务器通信端口
配置绑定模式	⚠ 可选配置。在 template 模板下指定用户表项绑定模式	

	bindmode {ip-only-l3mode}	配置模板表项绑定模式
	bindmode {ip-mac-mode | ip-only-mode}	配置模板表项绑定模式
配置定制页面包	⚠ 选配置。在 template 模板下指定内置 Portal Web 认证使用特定的页面包。	
	page-suite *file-name*	指定内置 Portal 使用特定的页面包
配置广告推送方式	⚠ 可选配置。在 template 模板下配置广告推送方式。	
	login-popup *url*	认证前弹出 ,也是登录的时候弹出的地址
	online-popup *url*	认证成功后前弹出的地址
设置重定向的 HTTP 端口	⚠ 可选配置。用于指定重定向 TCP 拦截端口，补充拦截环境中的特定端口报文进行重定向	
	http redirect port { *port-num* }	配置重定向 TCP 拦截端口
设置 Web 认证模块 SYSLOG 功能	⚠ 可选配置。用于配置 web 认证 SYSLOG 功能	
	web-auth logging enable {*num* }	配置 web 认证 SYSLOG 输出速率
设置未认证用户的最大 HTTP 会话数	⚠ 可选配置。用于调整 HTTP 会话数限制，对于后台会话数较多的场景需要放宽限制	
	http redirect session-limit { *session-num* } [**port** { *port-session-num* }]	配置用户的 HTTP 会话限制数
设置维持重定向连接的超时时间	⚠ 可选配置。用于修改重定向连接超时时间，在网络环境较差时调大参数有利于完成重定向	
	http redirect timeout { *seconds* }	用于设置重定向连接超时时间
设置直通 ARP 资源范围	⚠ 可选配置。用于放行指定地址的 ARP，开启 ARP CHECK 时需要放行网关 ARP	
	http redirect direct-arp { *ip-address* [*ip-mask*] }	用于配置直通 ARP 资源范围
设置无需认证用户 IP 范围	⚠ 可选配置。用于配置特殊用户不用认证就能上网	
	web-auth direct-host { *ip-address* [*ip-mask*] [**arp**] } [**port** *interface-name*]	用于配置免认证用户
设置在线用户信息的更新时间间隔	⚠ 可选配置。用于配置用户信息的更新周期	
	web-auth update-interval *{ seconds }*	用于配置用户信息更新周期
配置 Portal 检测	⚠ 可选配置。用于检测 Portal 服务器是否可用，如果不可用，则进行切换，该功能要结合主备 Portal 使用。	
	web-auth portal-check [**interval** *intsec* [**timeout** *tosec]* [**retransmit** retries]	配置 Portal 检测的周期、超时时间、超时重传次数
配置黑白名单	⚠ 可选配置。配置黑名单表示某些网络资源认证通过也不可访问，配置白名单表示某些资源不用认证也可以访问。	
	web-auth acl {black-ip *ip*|**black-port** *port*|**black-url** *name*|**white-url** *name***}**	配置黑白名单

配置默认认证方法	⚠ 可选配置。EG 上配置使用的认证方法。	
	web-auth webauth-type { internal | external *name* **}**	
配置 Portal 通信端口	⚠ 可选配置。配置后设备与 Portal 服务器通信的源端口为所配置端口。	
	ip portal source-interface interface-type interface-num	指定设备与 Portal 服务器的通信接口
配置多 Portal 映射	⚠ 可选配置。配置不同网段用户使用不同 Portal 进行认证。	
	web-auth portal { eportalv1 | iportal | *name* **} ip-mapping** *ipv4 mask*	配置不同网段用户使用不同 Portal 进行认证
配置内置 WEB 认证 NAT 功能	⚠ 可选配置。配置内置 web 认证支持 NAT。	
	iportal nat enable	支持内置 web 认证 NAT
配置内置 WEB 认证重传次数	⚠ 可选配置。配置内置 web 认证 http 连接重传次数。	
	iportal retransmit *count*	配置内置 web 认证 http 连接重传次数
配置内置 WEB 认证服务选择	⚠ 可选配置。配置内置 web 认证使用的服务类型。	
	iportal service [internet *internet-name*] **[local** *local-name* **]**	配置内置 web 认证使用的服务类型
配置内置 WEB 认证用户 UA 字段	⚠ 可选配置。配置用户的 UA 字段对应的终端名称。	
	iportal user-agent *ua-name* **type mobile** *ua-string*	配置用户的 UA 字段对应的终端名称

14.5.1 配置一代Web认证功能

配置效果

未认证用户能够被重定向到认证页面并完成认证

注意事项

无

配置方法

↘ 配置 portal 服务器

- 必须配置，要成功应用 Web 认证功能，必须设置并应用 portal 服务器。
- 当接入/汇聚设备发现未认证用户试图通过 HTTP 访问网络资源时，设备将用户的访问请求重定向到指定的 portal 认证页面，通过认证页面，引导用户向认证服务器发起认证。Portal 服务器地址将被设置为一个特殊的免认证的网络资源，未认证用户才可以直接与这个地址进行 HTTP 通讯。

配置设备与认证服务器之间的通信密钥

- 必须配置，要成功应用 Web 认证功能，必须设置接入/汇聚设备与认证服务器进行通信的密钥。
- 当设备发现未认证用户在访问网络资源时，设备将通过重定向功能，向用户弹出认证页面，通过认证页面，引导用户向认证服务器发起认证。在认证过程中，设备与认证服务器间通过密钥对部分数据进行加密，以加强安全性。

设置设备与认证服务器之间的 SNMP 网管参数

- 必须配置，要成功应用 Web 认证功能，必须设置设备与认证服务器之间的 SNMP 网管通信参数。
- 接入/汇聚设备和认证服务器之间通过 SNMP/MIB 对认证用户进行管理，在设备上，使用 MIB 来管理认证用户表，认证服务器通过访问这个 MIB，可以获取用户相关的统计信息，以及进行控制用户的上线、下线的操作。当用户下线时，设备将发送 SNMP-Inform 消息给认证服务器。

在端口上开启 Web 认证功能

- 必须配置。
- 当 Web 认证功能基于端口开启时，默认情况下，端口未开启 Web 认证功能，此时这个端口下所连接的用户不进行 Web 认证。

检验方法

- 未认证用户被要求认证
- 已认证用户可以正常使用网络

相关命令

创建模板

【命令格式】 **web-auth template eportalv1**
【参数说明】 -
【命令模式】 全局配置模式
【使用指导】 eportalv1 为默认的一代 web 认证模板

配置服务器 IP

【命令格式】 **ip** { *ip-address* }
【参数说明】 portal 服务器的地址
【命令模式】 web 认证模板配置模式
【使用指导】 -

配置服务器 URL

【命令格式】 **url** { *url-string* }
【参数说明】 portal 服务器的认证页面地址
【命令模式】 Web 认证模板配置模式
【使用指导】 以 http://或 https://开头

配置 Portal 服务器 URL 格式

【命令格式】 **fmt { ace | ruijie }**
【参数说明】 portal 服务器的 url 格式
【命令模式】 Web 认证模板配置模式
【使用指导】 fmt 参数为 ace 时，支持 ACE 联动。

配置用户绑定模式

【命令格式】 **bindmode {ip-only-l3mode}**
【参数说明】 用户的绑定模式
【命令模式】 Web 认证模板配置模式
【使用指导】 -

配置重定向方式

【命令格式】 **redirect { http | js }**
【参数说明】 重定向报文的封装格式
【命令模式】 Web 认证模板配置模式
【使用指导】 某些 app 无法执行 javascript 脚本动作时，需要配置成 http 封装格式触发重定向

配置服务器加密密钥

【命令格式】 **web-auth portal key** { *key-string* }
【参数说明】 portal 服务器的加密密钥，配置设备与认证服务器进行通信的密钥；密钥最大长度为 255 个字符。
【命令模式】 全局配置模式
【使用指导】 -

配置服务器 SNMP 通信团体字

【命令格式】 **snmp-server community** { *community-string* } **rw**
【参数说明】 *community-string*：Community 字符串；
rw：由于需要对 MIB 进行 Set 操作，因此需要设置成 RW，支持读写操作；
【命令模式】 全局配置模式
【使用指导】 设置 SNMP Community，认证服务器可以使用这个 Community 管理接入/汇聚设备上的在线用户。

配置服务器 SNMP 通信服务器

【命令格式】 **snmp-server host** { *ip-address* } **inform version** 2c { *community-string* } **web-auth**
【参数说明】 *ip-address*：目的主机地址，也就是认证服务器的地址。
community-string：通信团体字，发送 SNMP-Inform 消息使用的 Community 字符串。

【命令模式】 全局配置模式

【使用指导】 设置发送 Web 认证消息的目的主机，类型、版本、Community 等参数。

inform：设置发送 SNMP-Inform 类型的消息。由于接入/汇聚设备在用户下线的时候向认证服务器发送消息，为了防止消息丢失，所以采用 SNMP-Inform 而不是 SNMP-Trap。

version 2c：SNMPv2 以后的版本才支持 SNMP-Inform 类型，因此这里不能设置为 SNMPv1。

web-auth：指明发送 Web 认证消息采用上述的参数。

SNMP 的配置命令和其他具体内容参见“SNMP 配置指南”中的相关章节。

这里列出的 SNMP 通信参数是以 SNMPv2 的设置为例的，如果要求设备和认证服务器之间的 SNMP 网管通信有更高的安全性，可以考虑采用 SNMPv3。这样，SNMP Community 的设置需要改为 SNMP User，并且 SNMP-Inform 的版本也需要改为 SNMPv3 版本的，另外还需要设置和 SNMPv3 相关的安全参数，具体参见“SNMP 配置”中相关的章节，这里不再进行详细介绍。

配置使能 web 认证 trap/inform 通告

【命令格式】 **snmp-server enable traps web-auth**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 设置接入/汇聚设备允许向外发送 Web 认证的消息，消息类型包括 Trap 和 Inform。

web-auth：即 Web 认证的消息。

配置接口上启用 web 认证

【命令格式】 **web-auth enable**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 -

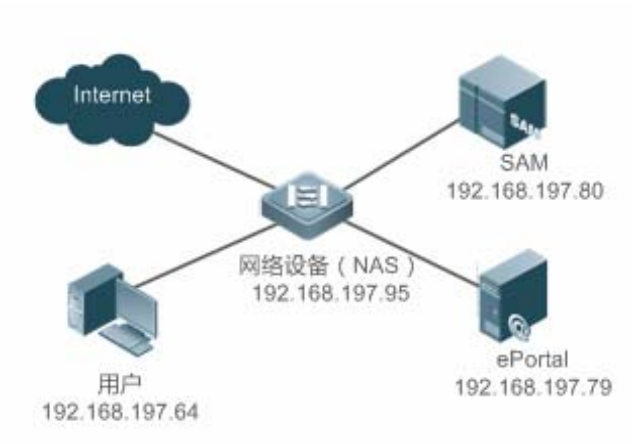
配置举例

以下配置举例，仅介绍与 Web 认证相关的配置。

一代 web 认证

【网络环境】

图 14-4



【配置方法】

- 在网络设备上设置认证服务器的 IP 地址及与认证服务器进行通信的密钥(ruijie)
- 在网络设备上设置认证页面的主页地址
- 设置网络设备与认证服务器之间的 SNMP 网管参数(团体字 public)
- 在网络设备上对 GigabitEthernet 0/2、GigabitEthernet 0/3 两个端口上开启 Web 认证功能

```
Ruijie# config
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#web-auth template eportalv1
Ruijie(config.tmplt.eportalv1)#ip 192.168.197.79
Ruijie(config.tmplt.eportalv1)#exit
Ruijie(config)# web-auth portal key ruijie
```

```
Ruijie(config)# web-auth template eportalv1
Ruijie(config.tmplt.eportalv1)#url http://192.168.197.79:8080/eportal/index.jsp
Ruijie(config.tmplt.eportalv1)#exit
```

```
Ruijie(config)# snmp-server community public rw
Ruijie(config)# snmp-server enable traps web-auth
Ruijie(config)# snmp-server host 192.168.197.79 inform version 2c public web-auth
Ruijie(config)# exit
```

```
Ruijie(config)# interface range GigabitEthernet 0/2-3
Ruijie(config-if-range)# web-auth enable
Ruijie(config-if-range)# exit
```

【检验方法】

- web 认证配置是否成功

```
Ruijie(config)#show running-config
…
snmp-server host 192.168.197.79 inform version 2c public web-auth
snmp-server enable traps web-auth
snmp-server community public rw
…
web-auth template eportalv1
```

```
 ip 192.168.197.79
 url http://192.168.197.79:8080/eportal/index.jsp
!
web-auth portal key ruijie
…
interface GigabitEthernet 0/2
 web-auth enable
!
interface GigabitEthernet 0/3
 web-auth enable
```

```
Ruijie#show web-auth control
 Port                       Control  Server Name           Online User Count
 -------------------------- -------- --------------------- -----------------
…
 GigabitEthernet 0/2         On       eportalv1             0
 GigabitEthernet 0/3         On       eportalv1             0
…
```

```
Ruijie#show web-auth template
Webauth Template Settings:
-------------------------------------------------------------
  Name:      eportalv1
  Url:       http://17.17.1.21:8080/eportal/index.jsp
  Ip:        17.17.1.21
  BindMode:  ip-mac-mode
  Type:      v1
……
```

常见错误

- Portal 服务器和设备间的 SNMP 参数配置不正确导致用户无法认证上线。
- 跨三层部署 Web 认证，模板中的绑定模式需要选择 ip-only-mode。
- 和 vrrp 一起使用的时候，需要通过 `snmp-server trap-source ip` 命令指定 `vrrp` 地址，否则 `Portal` 服务器无法正确处理 `trap` 报文。

14.5.2 配置二代Web认证功能

配置效果

未认证用户能够被重定向到认证页面并完成认证。

注意事项

- 二代 Web 认证支持中移动 Portal 规范，同时做了扩展以支持锐捷 Portal 服务器，实际部署时需要根据服务器情做相关兼容性配置，具体参考后续章节的说明。
- 在配置二代 Web 认证的 Portal 服务器的 URL 时，如果 URL 里面带有 IPv6 地址，需要将 ipv6 地址用中括号包含起来。例如：配置 IPv6 地址为 2001::1 时，实际配置应该为 url **错误！超链接引用无效。**配置。
- fmt 参数为 cmcc-normal 和 cmcc-ext1 时，其中 IP 仅支持 IPV4 形式。

配置方法

配置开启 AAA 认证

- 必须配置，要使用二代 Web 认证功能，必须开启 AAA 认证。
- 二代 web 认证向服务器发起认证的功能由设备完成，在设备 AAA 功能实现。

配置 RADIUS 服务器和密钥

- 必须配置，要成功应用二代 Web 认证功能，必须设置 RADIUS 服务器。
- 用户账户信息保存在 RADIUS 服务器上，设备需要连接 RADIUS 服务器来确认用户身份合法性。

配置 AAA 中 web 认证方法

- 必须配置，要成功应用二代 Web 认证功能，必须设置 AAA 认证方法。
- 认证方法列表将 web 认证的请求和 RADIUS 服务器关联起来，设备依据认证方法列表来选择认证方式和对应的服务器。

配置 AAA 网络记账方法

- 必须配置，要成功应用二代 Web 认证功能，必须设置 AAA 网络记账方法。
- 记账方法用于关联对应的记账方式和服务器，web 认证需要记账功能记录用户信息或费用。

配置 portal 服务器

- 必须配置，要成功应用二代 Web 认证功能，必须设置并应用 portal 服务器。
- 当接入/汇聚设备发现未认证用户试图通过 HTTP 访问网络资源时，设备将用户的访问请求重定向到指定的 portal 认证页面，通过认证页面，引导用户向认证服务器发起认证。Portal 服务器地址将被设置为一个特殊的免认证的网络资源，未认证用户才可以直接与这个地址进行 HTTP 通讯。

配置设备与认证服务器之间的通信密钥

- 必须配置，要成功应用二代 Web 认证功能，必须设置接入/汇聚设备与认证服务器进行通信的密钥。
- 当设备发现未认证用户在访问网络资源时，设备将通过重定向功能，向用户弹出认证页面，通过认证页面，引导用户向认证服务器发起认证。在认证过程中，设备与认证服务器间通过密钥对部分数据进行加密，以加强安全性。

设置全局/接口上使用的 portal 服务器

- 二代认证必须配置，要成功应用二代 Web 认证功能，必须在全局/接口上指定使用二代 portal。
- 设备会优先选择所在接口配置的 portal 服务器，如果所在接口不存在 portal 服务器配置，设备会选择全局配置的 portal 服务器，全局不存在配置时默认使用 eportalv1。设备将用户重定向到所选择的 portal 服务器。

在端口上开启 Web 认证功能

- 必须配置。
- 当 Web 认证功能基于端口开启时，默认情况下，端口未开启 Web 认证功能，此时这个端口下所连接的用户不进行 Web 认证。

检验方法

- 未认证用户被要求认证
- 已认证用户可以正常使用网络

相关命令

开启 AAA 功能

【命令格式】 **aaa new-model**
【参数说明】 -
【命令模式】 全局配置模式
【使用指导】 aaa 的方法列表等命令需要在功能开启后才能输入

配置 RADIUS 服务器和密钥

【命令格式】 **radius-server host** { *ip-address* } [**auth-port** *port-number1*] [**acct-port** *port-number 2*] **key** { *string* }
【参数说明】 *ip-address*：服务器 IP 地址
port-number1：认证端口号
port-number2：记账端口号
string：密钥字符串
【命令模式】 全局配置模式
【使用指导】 认证端口默认 1812，记账端口默认 1813

配置 AAA 中 Web 认证方法列表

【命令格式】 **aaa authentication web-auth** { **default** | *list-name* } *method1* [*method2*...]
【参数说明】 *list-name*：方法列表名
method1：方法 1
method2：方法 2
【命令模式】 全局配置模式
【使用指导】 二代 web 认证通常使用 RADIUS 认证方法

配置网络记账方法列表

【命令格式】 **aaa accounting network** { **default** | *list-name* } **start-stop** *method1* [*method2*...]
【参数说明】 *list-name*：方法列表名
method1：方法 1
method2：方法 2
【命令模式】 全局配置模式
【使用指导】 二代 web 认证通常使用 RADIUS 记账方法

创建模板

【命令格式】 **web-auth template** { **eportalv2 |** *portal-name* **v2** }
【参数说明】 自定义的 portal 服务器名
【命令模式】 全局配置模式
【使用指导】 eportalv2 为默认的二代 web 认证模板

配置服务器 IP

【命令格式】 **ip** { *ip-address* | *ipv6-address* }
【参数说明】 portal 服务器的地址
【命令模式】 Web 认证模板配置模式
【使用指导】 -

配置服务器 URL

【命令格式】 **url** { *url-string* }
【参数说明】 portal 服务器的认证页面地址
【命令模式】 Web 认证模板配置模式
【使用指导】 以 http://或 https://开头

配置 Portal 服务器 URL 格式

【命令格式】 **fmt { cmcc-ext1 | cmcc-ext2 | cmcc-mtx | cmcc-normal | cmcc-ext3 | ruijie | custom}**
【参数说明】 portal 服务器的 url 格式
【命令模式】 Web 认证模板配置模式
【使用指导】 fmt 参数为 cmcc-normal 和 cmcc-ext1 时，其中 IP 仅支持 IPV4 形式。
fmt 默认为 ruijie 格式。
fmt 参数为 custom 时，定制化格式。
fmt 参数为 cmcc-ext2，支持辽宁移动 portal 格式。
fmt 参数为 cmcc- ext3 时，支持宁波/嘉兴移动 AC 厂商 URL 格式。
fmt 参数为 cmcc-mtx 时，支持移动 AC 厂商 URL 格式。

配置用户绑定模式

【命令格式】 **bindmode {ip-only-l3mode}**
【参数说明】 用户的绑定模式
【命令模式】 Web 认证模板配置模式
【使用指导】 -

配置重定向方式

【命令格式】 **redirect { http | js }**
【参数说明】 重定向报文的封装格式
【命令模式】 Web 认证模板配置模式
【使用指导】 某些 app 无法执行 javascript 脚本动作时，需要配置成 http 封装格式触发重定向

配置服务器加密密钥

【命令格式】 **web-auth portal key** { *key-string* }
【参数说明】 portal 服务器的加密密钥 。配置设备与认证服务器进行通信的密钥；密钥最大长度为 255 个字符。
【命令模式】 全局配置模式
【使用指导】 -

配置启用 Web 认证

【命令格式】 **web-auth enable**
【参数说明】
【命令模式】 全局配置模式
【使用指导】 -

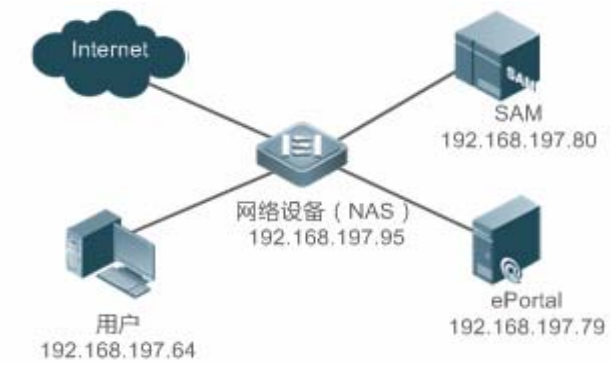
配置举例

以下配置举例，仅介绍与 Web 认证相关的配置。

二代 Web 认证

【网络环境】

图 14-5



【配置方法】
- 在网络设备上开启 AAA
- 在网络设备配置 RADIUS 服务器和密钥
- 在网络设备配置 AAA 的 web 认证默认方法列表和默认网络记账方法列表
- 在网络入设备上设置认证服务器的 IP 地址及与认证服务器进行通信的密钥(ruijie)
- 在网络设备上设置认证页面的主页地址
- 在网络设备上配置全局使用二代 portal 进行认证
- 在网络设备上对 GigabitEthernet 0/2、GigabitEthernet 0/3 两个端口上开启 Web 认证功能

```
Ruijie#configure
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#aaa new-model
Ruijie(config)#radius-server host 192.168.197.79 key ruijie
Ruijie(config)#aaa authentication web-auth default group radius
Ruijie(config)#aaa accounting network default start-stop group radius
Ruijie(config)#web-auth template eportalv2
Ruijie(config.tmplt.eportalv2)#ip 192.168.197.79
Ruijie(config.tmplt.eportalv2)#exit
Ruijie(config)#web-auth portal key ruijie
Ruijie(config)# web-auth template eportalv2
Ruijie(config.tmplt.eportalv2)#url http://192.168.197.79:8080/eportal/index.jsp
Ruijie(config.tmplt.eportalv2)#exit
Ruijie(config)# interface range GigabitEthernet 0/2-3
Ruijie(config-if-range)# web-auth enable eportalv2
Ruijie(config-if-range)# exit
```

【检验方法】

- web 认证配置是否成功

```
Ruijie(config)#show running-config
…
aaa new-model
aaa authentication web-auth default group radius
aaa accounting network default start-stop group radius
…
radius-server host 192.168.197.79 key ruijie
…
web-auth template eportalv2
 ip 192.168.197.79
 url http://192.168.197.79:8080/eportal/index.jsp
!
web-auth portal key ruijie
!
web-auth enable
!
interface GigabitEthernet 0/2
interface GigabitEthernet 0/3
```

```
Ruijie#show web-auth control
 Port                       Control  Server Name           Online User Count
 -------------------------- -------- --------------------- -----------------
…Global                      On       eportalv2            1
```

```
…
Ruijie#show web-auth template
Webauth Template Settings:
------------------------------------------------------------
  Name:      eportalv2
  Url:       http://17.17.1.21:8080/eportal/index.jsp
  Ip:        17.17.1.21
  BindMode:  ip-mac-mode
  Type:      v2
  Port:      50100
  State:     Active
  Acctmlist: default
  Authmlist: default
…
```

常见错误

- Portal 服务器和设备间的 key 配置错误或者有一方配置了加密，一方未配置导致认证异常
- Radius 服务器和设备间参数配置不正确导致认证异常
- Portal 服务器不支持中移动 portal 协议规范导致无法对接

14.5.3 配置内置Portal Web认证

配置效果

未认证用户能够被重定向到认证页面并完成认证，无需外置 Portal 服务器。

注意事项

- 部分设备，比如 AP110 并没有内置页面包，使用前需要先导入页面包，具体产品对页面包的支持情况，请参考具体产品的说明。
- EG 设备上是基于全集配置内置 Portal Web 认证。
- 如果要使用自定义页面包，必须严格按照定制规范章节给出的说明实现。

配置方法

↘ 配置开启 AAA 认证

- 必须配置，要使用二代 Web 认证功能，必须开启 AAA 认证。

- 内置 Portal Web 认证向服务器发起认证的功能由设备完成，在设备 AAA 功能实现。

配置 RADIUS 服务器和密钥

- 必须配置，要成功内置 Portal Web 认证功能，必须设置 RADIUS 服务器。
- 用户账户信息保存在 RADIUS 服务器上，设备需要连接 RADIUS 服务器来确认用户身份合法性。

配置 AAA 中 Web 认证方法

- 必须配置，要成功应用内置 Portal Web 认证功能，必须设置 AAA 认证方法。
- 认证方法列表将 Web 认证的请求和 RADIUS 服务器关联起来，设备依据认证方法列表来选择认证方式和对应的服务器。

配置 AAA 网络记账方法

- 可选配置，部分服务器要求认证和记账必须同时开启，因此是否配置记账要根据服务器特性决定。
- 记账方法用于关联对应的记账方式和服务器，Web 认证需要记账功能记录用户信息或费用。

配置内置 iportal 模板

- 必须创建 iportal 模板。
- 如果之前创建的认证、计费方法不是 default，则需要在模板中配置对应名字，否则默认使用 default。

在全局或者端口上开启 Web 认证功能

- 必须配置。

检验方法

- 未认证用户被要求认证，弹出页面为内置页面包中的对应页面文件。
- 已认证用户可以正常使用网络。

相关命令

开启 AAA 功能

【命令格式】 **aaa new-model**
【参数说明】 -
【命令模式】 全局配置模式
【使用指导】 aaa 的方法列表等命令需要在功能开启后才能输入

配置 RADIUS 服务器和密钥

【命令格式】 **radius-server host** { *ip-address* } [**auth-port** *port-number1*] [**acct-port** *port-number 2*] **key** { *string* }
【参数说明】 *ip-address*：服务器 IP 地址
port-number1：认证端口号
port-number2：记账端口号

string：密钥字符串

【命令模式】 全局配置模式

【使用指导】 认证端口默认 1812，记账端口默认 1813

配置 AAA 中 Web 认证方法列表

【命令格式】 **aaa authentication iportal** { **default** | *list-name* } *method1* [*method2*...]

【参数说明】 *list-name*：方法列表名

method1：方法 1

method2：方法 2

【命令模式】 全局配置模式

【使用指导】 方法名需要和 AAA 的配置一致

配置网络记账方法列表

【命令格式】 **aaa accounting network** { **default** | *list-name* } **start-stop** *method1* [*method2*...]

【参数说明】 *list-name*：方法列表名

method1：方法 1

method2：方法 2

【命令模式】 全局配置模式

【使用指导】 方法名需要和 AAA 的配置一致

创建模板

【命令格式】 **web-auth template iportal**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 -

配置用户认证前广告推送 URL

【命令格式】 **login-popup** { *url-string* }

【参数说明】 推送广告的地址

【命令模式】 Web 认证模板配置模式

【使用指导】 以 http://或 https://开头

配置用户认证成功后广告推送 URL

【命令格式】 **online-popup {**url-string**}**

【参数说明】 推送广告的地址

【命令模式】 Web 认证模板配置模式

【使用指导】 以 http://或 https://开头

配置定制页面包

【命令格式】 **page-suit** { *filename* }

【参数说明】 指定页面包的文件名。

【命令模式】 Web 认证模板配置模式
【使用指导】 -

配置内置广告弹出周期

【命令格式】 **time-interval** {*hour*}
【参数说明】 广告弹出周期。
【命令模式】 Web 认证模板配置模式
【使用指导】 -

配置接口上启用 web 认证

【命令格式】 **web-auth enable**
【参数说明】
【命令模式】 全居配置模式
【使用指导】 -

配置举例

以下配置举例，仅介绍与 Web 认证相关的配置。

内置 Portal Web 认证

【配置方法】
- 在网络设备上开启 AAA
- 在网络设备配置 RADIUS 服务器和密钥
- 在网络设备配置 AAA 的 Web 认证默认方法列表和默认网络记账方法列表
- 在网络设备上配置全局使用内置 Portal 进行认证
- 在网络设备上对 GigabitEthernet 0/2、GigabitEthernet 0/3 两个端口上开启 Web 认证功能

```
Ruijie#configure
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#aaa new-model
Ruijie(config)#radius-server host 192.168.197.79 key ruijie
Ruijie(config)#aaa authentication iportal default group radius
Ruijie(config)#aaa accounting network default start-stop group radius
Ruijie(config)#web-auth template iportal
Ruijie(config.tmplt.iportal)#exit
Ruijie(config)# interface range GigabitEthernet 0/2-3
Ruijie(config-if-range)# web-auth enable iportal
Ruijie(config-if-range)# exit
```

【检验方法】
- web 认证配置是否成功

```
Ruijie(config)#show running-config
…
aaa new-model
```

```
aaa authentication web-auth default group radius
aaa accounting network default start-stop group radius
…
radius-server host 192.168.197.79 key ruijie
…
web-auth template iportal
!
web-auth enable
!
interface GigabitEthernet 0/2
interface GigabitEthernet 0/3
```

```
Ruijie#show web-auth control
 Port                      Control  Server Name           Online User Count
 ------------------------- -------- --------------------- -----------------
…Global                     On       iportal               1
…
```

```
Ruijie#show web-auth template
Webauth Template Settings:
-------------------------------------------------------------
  Name:      iportal
  Page-suit: default
  BindMode:  ip-mac-mode
  Type:      Intral Portal
  Advertising: null
  Advertising mode : online-popup
  Acctmlist: default
  Authmlist: default
…
```

常见错误

- 定制新页面包时未按定制规范制作
- 指定了定制页面包但是页面包未下载到 FLASH 或者未下载到指定目录

14.5.4 配置认证方法列表名

配置效果

- 当用户提交认证信息时，Portal 服务器会向设备发起认证请求，设备依据配置的认证方法列表名解析认证服务器等信息，发起认证过程。
- 配置认证方法列表名后，设备可以通过指定的方法列表名选择认证服务器进行认证。

注意事项

- 配置认证方法列表名前 ,必须保证在 AAA 中已经定义了该方法。对应定义命令为 **aaa authentication web-auth** { **default** | *list-name* } *method1* [*method2*...]。
- 无法分别给 ipv4 和 ipv6 认证指定不同的认证方法。

配置方法

- 可选配置
- 默认使用 default 方法，在 AAA 修改方法列表名或存在多个方法列表名时，使用本命令进行配置。

检验方法

- 在 AAA 中配置两个方法列表，方法列表 1 使用服务器 1，方法列表 2 使用服务器 2
- 在服务器 1 创建用户 a 和密码；服务器 2 创建用户 b
- 配置使用方法列表 1
- 用户使用账号 b 进行认证，认证失败
- 用户使用账户 a 进行认证，认证成功

相关命令

↘ 配置认证方法列表名

【命令格式】 **authentication** { *mlist-name* }
【参数说明】 方法列表名
【命令模式】 Web 认证模板配置模式
【使用指导】 应与 AAA 中 web 认证方法列表名一致

配置举例

↘ 配置认证方法列表名

【配置方法】
- 配置认证方法列表名为 mlist1

```
Ruijie(config.tmplt.iportal)#authentication mlist1
```

【检验方法】
- 查看配置是否成功

【配置方法】
- 配置认证方法列表名为 mlist1

```
Ruijie(config.tmplt.iportal)#authentication mlist1
```

【检验方法】
- 查看配置是否成功

```
Ruijie#show web-auth template
Webauth Template Settings:
------------------------------------------------------------
  Name:      eportalv2
  Url:       http://17.17.1.21:8080/eportal/index.jsp
  Ip:        17.17.1.21
  BindMode:  ip-only-mode
  Type:      v2
  Port:      50100
  State:     Active
  Acctmlist: default
  Authmlist: mlist1
```

14.5.5 配置记账方法列表名

配置效果

- 用户认证通过后，设备会自动发起记账请求，请求的对象依赖于记账方法列表的配置，通常为认证所在服务器。
- 配置记账方法列表名后，设备可以通过指定的方法列表名选择记账服务器进行记账。

注意事项

- 配置记账方法列表名前，必须保证在 AAA 中已经定义了该方法。对应定义命令为 **aaa accounting network** { **default** | *list-name* } **start-stop** *method1* [*method2*...]。
- 无法分别给 ipv4 和 ipv6 认证指定不同的记账方法。

配置方法

- 可选配置
- 默认使用 default 方法，在 AAA 修改方法列表名或存在多个方法列表名时，使用本命令进行配置。

检验方法

- 在 AAA 中配置两个记账方法列表，方法列表 1 使用服务器 1，方法列表 2 使用服务器 2
- 配置使用方法列表 1

- 用户使用合法账号进行认证上线
- 在服务器 1 和服务器 2 上分别查看用户记账信息；只有服务器 1 存在

相关命令

配置记账方法列表名

【命令格式】 **accounting** { *mlist-name* }
【参数说明】 方法列表名
【命令模式】 Web 认证模板配置模式
【使用指导】 应与 AAA 中网络记账方法列表名一致

配置举例

配置记账方法列表名

【配置方法】
- 配置记账方法列表名为 mlist1

```
Ruijie(config.tmplt.eportalv2)#accounting mlist1
```

【检验方法】
- 查看配置是否成功

```
Ruijie#show web-auth template
Webauth Template Settings:
------------------------------------------------------------
  Name:      eportalv2
  Url:       http://17.17.1.21:8080/eportal/index.jsp
  Ip:        17.17.1.21
  BindMode:  ip-mac-mode
  Type:      v2
  Port:      50100
  State:     Active
  Acctmlist: mlist1
  Authmlist: mlist1
```

14.5.6 配置Portal服务器通信端口

配置效果

- 设备检测到用户下线等情况时，需要同时通告 portal 服务器用户下线；设备和 portal 服务器使用 portal 协议进行交互，协议使用约定的端口号进行报文侦听和收发。
- 当 portal 服务器侦听端口改变时，设备需要修改 portal 服务器通信端口才能进行交互。

- 如果是内置 Portal Web 认证，此功能用于配置本机监听的 http 端口，默认是 8081.

注意事项

- 端口号配置需要和服务器实际使用端口相一致。
- 适用于二代 Web 认证和内置 Portal Web 认证 ,且两种认证的默认端口号不一样。二代 Web 认证端口号用于设备和 Portal 服务器交互 Portal 协议，内置 Portal Web 认证的端口号用于本机报文监听。

配置方法

- 可选配置
- 服务器不使用默认端口号或者本机监听端口有冲突需要调整时，使用本命令配置来保持一致。

检验方法

- 配置二代 Web 认证
- 改变服务器侦听端口为 10000
- 通过本命令配置端口号为 10000
- 用户 web 认证上线
- 在设备端踢用户下线，刷新在线页面，提示用户下线

相关命令

↘ 配置 portal 服务器通信端口

【命令格式】 **port** *port-num*
【参数说明】 *port-num*：端口号
【命令模式】 web 认证模板配置模式
【使用指导】 -

配置举例

↘ 配置 portal 服务器通信端口

【配置方法】
- 配置服务器通信端口为 10000

```
Ruijie(config.tmplt.eportalv2)#port 10000
```

【检验方法】
- 查看配置是否成功

```
Ruijie#show web-auth template
Webauth Template Settings:
```

【配置方法】
- 配置服务器通信端口为 10000

```
Ruijie(config.tmplt.eportalv2)#port 10000
```

【检验方法】
- 查看配置是否成功

```
------------------------------------------------------------
  Name:       eportalv2
  Url:        http://17.17.1.21:8080/eportal/index.jsp
  Ip:         17.17.1.21
  BindMode:   ip-only-mode
  Type:       v2
  Port:       10000
  Acctmlist:
  Authmlist:
```

14.5.7 配置绑定模式

配置效果

- 用户成功上线时，需要将用户表项写到转发规则中，指定不同的绑定模式，可以改变转发规则的匹配方式，影响用户的上网规则。比如仅 IP 绑定时，只要符合该 IP 的报文都被放行，用户都能上网；而 IP+MAC 绑定时，只有同时符合该 IP 和 MAC 的用户能访问网络。

注意事项

- 在三层认证场景中，设备看到的 MAC 地址都是用户网关地址，MAC 地址都不准确，此时应该采用仅 IP 绑定模式。

配置方法

- 可选配置，缺省默认：IP+MAC 绑定。
- 依据设备能获得的用户准确信息决定选择哪种绑定模式 ,当用户 IP、MAC 均准确时 ,比如二层网络部署 ,优先选择 IP+MAC 绑定；否则优先选择仅 IP 绑定模式。

检验方法

- 改变绑定模式为仅 IP 模式
- 用户认证上线
- 修改用户 MAC，或者使用另一台同 IP，不同 MAC 的客户端访问网络
- 用户上网正常

相关命令

↘ 配置绑定模式

【命令格式】 **bindmode {ip-only-l3mode}**
【参数说明】 **ip-only-l3mode**：仅 IP 绑定
【命令模式】 web 认证模板配置模式
【使用指导】 -

14.5.8 配置定制页面包

配置效果

- 用户可以指定内置 Portal 使用特定页面包，然后在这些页面包上嵌入一些特色内容或者信息，比如特有的 LOGO 或者公告信息等。

注意事项

- 页面包需要手工下载到设备的 FLASH 中，并且固定存放在./portal 目录下，如果未事先存放页面包或者存放目录错误，会导致无法推送页面，进而导致 web 认证时效。如果对页面包没特殊要求，可以使用设备默认页面包。
- 页面包的定制规范请参考”页面包定制规范”。

配置方法

- 可选配置，缺省使用设备自带的页面包。

检验方法

- 配置内置 Portal Web 认证。
- 下载新的页面包。
- 指定使用该页面包。
- 用户上网，登录页面为定制页面。

相关命令

↘ 配置定制页面包

【命令格式】 **page-suit** *filename*
【参数说明】 *filename*：定制页面包的文件名

【命令模式】 web 认证模板配置模式

【使用指导】 新的页面包需要提前下载到 FLASH 的./porta/zipl 目录。

配置举例

↘ 配置定制页面包

【配置方法】

- 配置定制页面包

```
Ruijie(config.tmplt.iportal)#page-suit ruijiepage
```

【检验方法】

- 查看配置是否成功

```
Ruijie#show web-auth template
Webauth Template Settings:
-------------------------------------------------------------
  Name:      iportal
  Page-suit:    ruijiepage
  Advertising url:  default
  Advertising mode: online-popup
  Type:      Intral Portal
  Acctmlist:default
  Authmlist:default
```

14.5.9 配置广告推送方式

配置效果

- 可选则认证前弹出广告、认证后弹出广告。

注意事项

- 需要先配置好广告 url。
- 默认是认证成功后弹广告。
- 如果要实现用户不认证，只弹广告的效果，请选择 Advertising 功能，具体参考 Advertising 的配置手册。

配置方法

- 可选配置，缺省认证成功后弹广告。

检验方法

- 配置内置 Portal Web 认证
- 配置一个可访问互联网 url 地址
- 用户上网，认证成功后浏览器弹出一个新窗口并显示指定 url 的页面信息

相关命令

配置广告推送地址

【命令格式】 **login-popup** *url*
【参数说明】 *url* ：认证前弹出，也是登录的时候弹出的地址
【命令模式】 web 认证模板配置模式
【使用指导】
【命令格式】 **online-popup** *url*
【参数说明】 *url*：认证成功后前弹出的地址
【命令模式】 web 认证模板配置模式
【使用指导】

配置举例

配置广告推送模式

【配置方法】
- 配置广告推送模式为仅推送不认证

```
Ruijie(config.tmplt.iportal)#popup http://www.ruijie.com.cn/
Ruijie(config.tmplt.iportal)#popup mode login-popup
```

【检验方法】
- 查看配置是否成功

```
Ruijie#show web-auth template
Webauth Template Settings:
-----------------------------------------------------------
  Name:      iportal
  Page-suit:   default
  Advertising url:  http://www.ruijie.com.cn/
  Advertising mode: login-popup
  Type:      Intral Portal
  Acctmlist:default
  Authmlist:default
```

14.5.10 设置重定向的HTTP端口

配置效果

- 当用户访问网络资源时（例如使用浏览器上网），此时用户会发出 HTTP 报文，接入/汇聚设备通过拦截来自用户的 HTTP 报文，来判断用户是否在访问网络资源。当设备检测到未认证的用户在访问网络资源时，将阻止用户访问网络资源，并向用户弹出认证页面。缺省情况下，网络设备通过拦截用户发出的端口号为 80 的 HTTP 报文，来检测用户是否在访问网络资源。
- 设置重定向的 HTTP 端口后，可以对用户发出的特定目的端口号的 HTTP 请求进行重定向。

注意事项

- 接入/汇聚设备上常用的管理协议端口（例如 22、23、53）以及系统内部保留的端口，不允许被设置为重定向端口。实际上，除了 80 端口外，HTTP 协议很少会使用小于 1000 的端口号。为了避免与知名 TCP 协议端口冲突，除非必要，尽量不要设置较小端口号的端口作为重定向端口。

配置方法

- 可选配置
- 在配置自动获取客户端时，如果要新增网络设备拦截用户发出的特定端口号的 HTTP 报文，可以进行该配置。

检验方法

- 配置拦截端口
- 未认证 pc，使用浏览器访问该端口的外网网络
- 用户访问请求被重定向到认证页面

相关命令

↘ 设置重定向的 HTTP 端口

【命令格式】 **http redirect port** *port-num*

【参数说明】 *port-num*：端口号

【命令模式】 全局配置模式

【使用指导】 最大允许配置 10 个不同的目的端口号，默认端口号(80，443)不含在该总数量范围内。

配置举例

↘ 设置重定向的 HTTP 端口

【配置方法】
- 配置 8080 端口为重定向的 HTTP 端口

```
Ruijie(config)#http redirect port 8080
```

【检验方法】
- 查看配置是否成功

```
Ruijie(config)#show web-auth rdport
```

【配置方法】
- 配置 8080 端口为重定向的 HTTP 端口

```
Ruijie(config)#http redirect port 8080
```

【检验方法】
- 查看配置是否成功

```
Rd-Port:
80 443 8080
```

14.5.11 设置Web认证模块SYSLOG功能

配置效果

- 当用户上下线时，web 认证模块会通过 SYSLOG 将上下线的用户信息和事件呈现给管理员。缺省情况下，该 SYSLOG 信息被屏蔽。
- 设置 SYSLOG 限速功能后，可以按照一定的速率将该信息呈现出来。

注意事项

- 当认证上下线速率很高时，频繁的 SYSLOG 输出会影响设备性能，同时导致输出信息刷屏。

配置方法

- 可选配置
- 需要查看基本上下线 SYSLOG 信息时，可以配置 SYSLOG 限速功能。

检验方法

- 配置 SYSLOG 限速
- 用户按照一定速率上下线
- SYSLOG 按照限制要求打印输出

相关命令

↘ 设置 SYSLOG 限速

【命令格式】 **web-auth logging enable** *num*

【参数说明】 *num*：SYSLOG 输出速率（条/秒）

【命令模式】 全局配置模式

【使用指导】 0 为不限制速率；不输出受限的 SYSLOG。受限的 SYSLOG 不包括严重级 SYSLOG，及异常错误输出的 SYSLOG。

配置举例

↘ 设置 SYSLOG 限速

【配置方法】
- 配置不限制 SYSLOG 输出

```
Ruijie(config)#web-auth logging enable 0
```

【检验方法】
- 查看配置是否成功

```
Ruijie(config)#show running-config
…
web-auth logging enable 0
…
```

14.5.12 设置未认证用户的最大HTTP会话数

配置效果

- 未认证的用户在访问网络资源时，用户 PC 会发出 HTTP 会话连接请求，HTTP 报文会被接入/汇聚设备拦截，并通过重定向要求用户进行 Web 认证。为了防止同一个未认证用户发起过多的 HTTP 连接请求，以节约网络设备的资源，需要在设备上限制未认证用户的最大 HTTP 会话数。
- 由于用户在认证时，会占用一个 HTTP 会话，而用户的其他应用程序也可能占用着 HTTP 会话，因而不建议设置未认证用户的最大 HTTP 会话数为 1。缺省情况下，全局每个未认证用户的最大 HTTP 会话数为 255，而每个端口下的未认证用户的 HTTP 会话总数最大为 300。

注意事项

- 如果一个用户在进行 Web 认证时，出现经常无法弹出认证页面的情况，则很可能是受到最大 HTTP 会话数的限制了。此时，应该建议用户暂时关闭一些可能会占用 HTTP 会话的应用程序，然后再进行 Web 认证。

配置方法

- 可选配置
- 要更改每个未认证用户的最大 HTTP 会话数及每个端口下的未认证用户的 HTTP 会话总数时，可进行该配置。
- 在配置自动获取 SU 客户端功能时， 需要进行该配置。

检验方法

- 修改未认证用户最大会话数
- 未认证用户构造相同会话不间断对设备进行连接

- 未认证用户通过浏览器访问外网，访问请求不被重定向，设备提示用户会话数超过限制

相关命令

设置每个未认证用户的最大 HTTP 会话数

【命令格式】 **http redirect session-limit** { *session-num* } [**port** { *port-session-num* }]

【参数说明】 *session-num*：最大会话数。取值范围 1-255，默认为 255。

port-session-num：端口最大会话数。取值范围 1-65535，默认为 300。

【命令模式】 全局配置模式

【使用指导】 无

配置举例

设置每个未认证用户的最大 HTTP 会话数

【配置方法】

- 设置每个未认证用户的最大 HTTP 会话数为 3

```
Ruijie(config)#http redirect session-limit 3
```

【检验方法】

- 查看配置是否成功

```
Ruijie(config)#show web-auth parameter
HTTP redirection setting:
  session-limit: 3
  timeout:       3
Ruijie(config)#
```

14.5.13 设置维持重定向连接的超时时间

配置效果

- 设置维持重定向连接的超时时间。因为未认证的用户通过 HTTP 访问网络资源时，其 TCP 连接请求将被拦截，实际上是与接入/汇聚设备建立起 TCP 连接。在连接建立后，设备需要等待用户发出的 HTTP 的 GET/HEAD 报文，然后回复 HTTP 重定向报文后才能关闭连接。设置这个限制可以防止用户不发 GET/HEAD 报文，而又长时间占用 TCP 连接。缺省情况下，维持重定向连接的超时时间为 3 秒。

注意事项

- 无

配置方法

- 可选配置
- 要更改维持重定向连接的超时时间时，可进行该配置。

检验方法

- 修改超时时间配置
- 使用网络发包工具构造建立 tcp 连接
- 查看设备上该 tcp 连接状态，超过超时时间后连接被关闭

相关命令

↘ 设置维持重定向连接的超时时间

【命令格式】 **http redirect timeout** { *seconds* }

【参数说明】 *Seconds*：重定向连接超时时间，单位为秒。取值范围 1-10。默认为 3 秒。

【命令模式】 全局配置模式

【使用指导】 无

配置举例

↘ 设置维持重定向连接的超时时间

【配置方法】

- 设置维持重定向连接的超时时间 5

```
Ruijie(config)#http redirect timeout 5
```

【检验方法】

- 查看配置是否成功

```
Ruijie(config)#show web-auth parameter
HTTP redirection setting:
  session-limit: 255
  timeout:       5
```

14.5.14 设置免认证网络资源范围

配置效果

- 在端口上启动 Web 认证或者 802.1x 认证后，未认证用户需先通过 Web 认证或者 802.1x 认证，才能访问网络资源。
- 使用此命令设置免认证的网络资源，可以允许未认证用户，也可以访问一些免认证的网络资源。
- 设置了免认证的网络资源，如果某网站属于免认证的网络资源，那么所有用户（包括未认证用户）都可以访问该网站。缺省情况下，没有设置免认证的网络资源，未认证用户不能访问网络资源。

注意事项

- 设置免认证的网络资源和设置无需认证用户共享资源，这两者各自都不能超过 1000 个。此外，实际可用数量也会受其它安全功能占用表项的影响而减少。因此，如果需要设置的地址较多，请尽量使用网段的方式进行设置。
- http redirect direct-site 是配置免认证访问地址，http redirect 是配置 web 认证的服务器地址。从效果上看，用这两条命令配置的地址都是可以不用认证就直接访问的，但是实际用途是不一样的，因此实际使用时建议不要用 http redirect direct-site 来配置 web 认证服务器地址，否则会引起误解。

配置方法

- 可选配置
- 如果需要让未认证用户能够访问网络中的资源，使用本命令实现。

检验方法

- 配置免认证网络资源
- 未认证用户 PC 直接访问该资源，访问成功

相关命令

↘ 设置免认证网络资源范围

【命令格式】 **http redirect direct-site** { *ipv4-address* [*ip-mask*] [**arp**] | *mac-address* | range *starip-address endip-address* } [description *description-str*] [group *group-name*]

【参数说明】 *Ipv4-address*：免认证网络 IPv4 地址
ip-mask：免认证网络 IPv4 地址掩码
mac-address：免认证网络目的 MAC 地址
Startip-address: 连续免认证网络的起始 ip
Endip-address: 连续免认证网络的结束 ip
Group-name: 免认证网络的所属的组
Description-str: 免认证网络的描述信息

【命令模式】 全局配置模式

【使用指导】 ARP 放行请优先采用直通 ARP 命令

配置举例

↘ 设置免认证网络资源范围

【配置方法】
- 设置免认证的网络资源范围 192.168.0.0/16

```
Ruijie(config)#http redirect direct-site 192.168.0.0 255.255.0.0
```

- 设置连续免认证的范围为 10.0.0.1 到 12.0.0.1

```
Ruijie(config)# http redirect direct-site range 10.0.0.1 12.0.0.1
```

【检验方法】
- 查看配置是否成功

```
Ruijie(config)#show web-auth direct-site
```

【配置方法】
- 设置免认证的网络资源范围 192.168.0.0/16

```
Ruijie(config)#http redirect direct-site 192.168.0.0 255.255.0.0
```

- 设置连续免认证的范围为 10.0.0.1 到 12.0.0.1

```
Ruijie(config)# http redirect direct-site range 10.0.0.1 12.0.0.1
```

【检验方法】
- 查看配置是否成功

```
Direct sites:
  Address         Mask            ARP Binding Group       Description
  --------------- --------------- ----------- ----------- -------------
  192.168.0.0     255.255.0.0     Off         N/A         N/A
Ruijie(config)#
Ruijie(config)#show web-auth direct-site range
Direct site Ranges: 1
  Start Address   End Address     Group           Description
  --------------- --------------- --------------- -------------
  10.0.0.1        12.0.0.1        N/A             N/A
Ruijie(config)#
```

14.5.15 设置直通ARP资源范围

配置效果

- 开启 ARP CHECK 或类似功能时，用户的 ARP 学习受控，导致用户无法学到网关及其他设备的 ARP，影响用户使用。此时可以通过设置直通 ARP 资源来对指定地址的 ARP 学习报文进行放行

注意事项

- 对于开启 ARP Check 情况，需要将二层接入设备下联 PC 的网关设置为直通 ARP 资源。需要注意以下问题：
  对同一地址/网段同时设置直通网站和直通 ARP 时，命令会自动进行合并；如果直通网站的配置没有指定 ARP 选项，合并后该选项会自动增加。
- 对于开启 ARP Check 情况，若下联 PC 的出口地址不是网关地址，也需要将出口地址设置为直通 ARP 资源。若存在多个出口地址，这些出口地址也需要设置为直通 ARP 资源。

配置方法

- 可选配置
- 如果设备启用了 ARP CHECK 功能，那么需要对免认证的网络资源范围和网关配置 ARP 直通。

检验方法

- 配置直通 ARP 资源
- 未认证用户 PC 上清空 ARP 缓存(Windows 执行命令 arp -d)
- 未认证用户 PC 执行 ping 直通 ARP 资源
- 未认证用户 PC 查看 ARP 缓存(Windows 执行命令 arp -a)，学习到直通 ARP 资源的 ARP 地址

相关命令

设置直通 ARP 资源范围

【命令格式】 **http redirect direct-arp** { *ip-address* [*ip-mask*] }

【参数说明】 *ip-address*：免认证网络 ip 地址

ip-mask：免认证网络掩码

【命令模式】 全局配置模式

【使用指导】 -

配置举例

设置直通 ARP 资源范围

【配置方法】

- 设置直通 ARP 资源范围 192.168.0.0/16

```
Ruijie(config)#http redirect direct-arp 192.168.0.0 255.255.0.0
```

【检验方法】

- 查看配置是否成功

```
Ruijie(config)#show web-auth direct-arp
Direct arps:
  Address         Mask
  --------------- ---------------
  192.168.0.0     255.255.0.0
Ruijie(config)#
```

14.5.16 设置无需认证用户范围

配置效果

- 如果用户属于无需认证用户范围，那么该用户不需要通过 Web 认证，也能访问所有可达的网络资源。缺省时，没有设置无需认证用户，所有用户都必须先通过 Web 认证，才能访问网络资源。
- 支持 IP 地址和 MAC 地址设置。

注意事项

无

配置方法

- 可选配置
- 要设置无需认证用户时，可进行该配置。

检验方法

- 配置用户为无需认证用户
- 用户直接访问网络，访问成功

相关命令

↘ 设置无需认证用户 IP 范围

【命令格式】 **web-auth direct-host** { *ipv4-address* [*ipv4-mask*] [**arp**] [**port** *interface-name*] | *mac-address* | range *starip-address endip-address* } [description *description-str*] [group *group-name*]

【参数说明】 *Ipv4-address*：免认证用户 IPv4 地址

ip-mask：免认证用户 IPv4 地址掩码

interface-name：接口名

mac-address：免认证用户 mac 地址

Startip-address: 连续免认证用户的起始 ip

Endip-address: 连续免认证用户的结束 ip

Group-name: 免认证用户的所属的组

Description-str: 免认证用户的描述信息

【命令模式】 全局配置模式

【使用指导】 arp 字段用来设置放行 arp 报文，当开启 ARP-CHECK 功能时需要配置

配置 port 字段后，用户仅在所配置接口下时免认证功能生效，在其余接口上不生效

配置举例

↘ 设置无需认证用户 IP 范围

【配置方法】

- 设置无需认证用户 IP 范围

```
Ruijie (config)# web-auth direct-host 192.168.197.64
```

- 设置连续免认证用户的范围为 10.0.0.1 到 12.0.0.1

```
Ruijie(config)# web-auth direct-host range 10.0.0.1 12.0.0.1
```

【检验方法】

- 查看配置是否成功

```
Ruijie(config)#show web-auth direct-host
Direct hosts:
  Address         Mask            Port           ARP Binding   Group      Description
  --------------- --------------- -------------- ------------- ---------- ------------
```

```
  192.168.197.64   255.255.255.255                Off           N/A         N/A
Ruijie(config)#
Ruijie# show web-auth direct-host range
Direct host Ranges: 1
  Start Address     End Address       Port        Group         Description
  ----------------- ----------------- ----------- ------------- -----------
  10.0.0.1          12.0.0.1          Gi0/2       N/A           N/A
```

14.5.17 设置在线用户信息的更新时间间隔

配置效果

- 接入/汇聚设备维护着在线用户信息，设备需要定时地更新在线用户信息，包括在线时间等，以监控在线用户使用网络资源的情况，比如：用户的在线时间大于或等于在线时限，该用户会被停止使用网络。

注意事项

- 用户更新时间必须配置为 60 的倍数，否则实际配置自动向上取最近的 60 倍数来生效。

配置方法

- 可选配置
- 要设置无需认证用户时，可进行该配置。

检验方法

- 配置用户信息更新时间
- 超过更新时间间隔后，查看在线用户信息

相关命令

↘ 设置在线用户信息更新时间间隔

【命令格式】 **web-auth update-interval** *{ seconds }*

【参数说明】 *Seconds*：信息更新时间间隔，单位为秒。取值范围 30-3600。默认为 180 秒。

【命令模式】 全局配置模式

【使用指导】 如果要恢复更新时间间隔为默认值，在全局配置模式下，使用 **no web-auth update-interval**

配置举例

↘ 设置已认证用户信息的更新时间间隔为 60 秒

【配置方法】
- 设置已认证用户信息的更新时间间隔为 60 秒

```
Ruijie (config)# web-auth update-interval 60
```

【检验方法】
- 查看配置是否成功

```
Ruijie(config)#show run | include web-auth update-interval
web-auth update-interval 60
```

14.5.18 配置Portal检测

配置效果

- 定时检测 Portal 服务器是否可用，如果不可用，切换到备用 Portal 服务器。
- 对于二代认证有两种检测方法，第一种方法，是设备构造 Portal 协议报文发给 Portal 服务器，并通过检测 Portal 服务器是否响应来确定服务器是否可用。第二种方法，是设备向服务器发 ping 报文，通过是否响应 ping 报文来检测。由于部分服务器或者中间网络会过滤 ping 报文，因此大部分情况下是选择方法一作为检测方法，只有在极个别环境，比如有特殊规范要求的，才选择 ping 检测。而一代认证，采用 connect 服务器端口是否可达的方式来判断服务是否可用。
- 针对二代认证的第一种检测方法，检测算法为每隔 **interval** 时间进行一次检测，每次检测最多发 **retransmit** 个报文，如果些报文服务器都不响应，则判断服务器不可用，否则可用。每个报文的超时时间由参数 **timeout** 决定。一代认证同样支持此配置。
- 该功能对一代，二代 Web 认证都有效。
- 如果配置了多个个 Portal 服务器，则称为主备 Portal。

注意事项

- 需要配置多个 Portal 服务器，这样检测到错误时才能实现切换。
- 为避免检测算法冲突，两种检测方法只能选一个，同时配置会引起检测冲突或者检测结果不准确。
- 配置时如果使用一代认证，系统会自动选择一代检测方式，二代认证同样会自动选择二代认证的检测方式

配置方法

- 可选配置。
- 配置多个一，二代 Web 认证的 Portal 模板。

检验方法

- 配置两个二代或一代 Portal 服务器模板，第一个模板指向的服务器不可用，第二个模板指向的服务器可用。
- 控制台出现 Portal 不可用的 log 时，用户打开浏览器登录认证，被重定向到第二个 Portal 服务器。

相关命令

设置 Portal 检测

【命令格式】 **web-auth portal-check** [**interval** *intsec* [**timeout** *tosec]* [**retransmit** retries]

【参数说明】 *intsec*：检测周期，默认 10 秒

tosec ：报文超时时间，默认 5 秒

intsec：超时重传次数，默认 3 次

【命令模式】 全局配置模式

【使用指导】 大部分网络环境中只有一台服务器，无需配置此功能，如果有多台，参数不宜配置太小，否则会出现短时间内设备发出太多报文，影响设备性能。

【命令格式】 **web-auth ping** [**interval** *minutes*] [**retry** *times*]

【参数说明】 *minutes*：检测周期，默认 1 分钟

times ：超时重传次数，默认 3 次

【命令模式】 全局配置模式

【使用指导】 大部分网络环境中只有一台服务器，无需配置此功能，如果有多台，参数不宜配置太小，否则会出现短时间内设备发出太多报文，影响设备性能。

配置举例

设置 Portal 检测

【配置方法】

- 配置 Portal 检测

```
Ruijie(config)# web-auth portal-check interval 20 timeout 2 retransmit 2
```

【检验方法】

- 查看配置是否成功

```
Ruijie(config)#show running-config
…
web-auth portal-check interval 20 timeout 2 retransmit 2
…
```

14.5.19 配置Portal逃生

配置效果

- 当配置的 Portal 服务器都不可用时，新接入网络的用户免认证。

注意事项

- 需要同时配置 Portal 检测功能。
- 如果配置了多个 Portal 服务器，则需要所有 Portal 服务器均不可用时逃生功能才会生效。
- 此功能仅针对 Portal 服务器，不针对 RADIUS 服务器。

配置方法

- 可选配置。
- 配置 Portal 检测功能。
- 配置 Portal 逃生功能。

检验方法

- 配置一个 Portal 服务器，服务器不可用。
- 配置 Portal 检测功能和逃生功能。
- 设备检测出 Portal 不可用后，用户接入网络，无需认证即可访问网络。

相关命令

设置 Portal 逃生

【命令格式】 **web-auth portal-escape**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 如果网络中有一些关键业务不允许中断，可以配置此功能，这样当 Portal 服务器出现异常时，可以保证业务不受影响。配置此功能要同时配置 Portal 检测功能。

配置举例

设置 Portal 逃生

【配置方法】
- 配置 Portal 逃生

```
Ruijie(config)# web-auth portal-escape
```

【检验方法】
- 查看配置是否成功

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

【配置方法】
- 配置 Portal 逃生

```
Ruijie(config)# web-auth portal-escape
```

【检验方法】
- 查看配置是否成功

```
…
web-auth portal-escape
…
```

14.5.20 配置黑白名单

配置效果

- 白名单可以使用户在认证前可以访问部分网络资源，黑名单可以使用户在认证后无法访问部分网络资源。
- 黑白名单支持端口、url、ip 等信息过滤的过滤。

注意事项

- 黑白名单只支持配置最多 1000 条。
- 如果以域名形式配置，需要配置设备的 DNS 功能，使得设备可以正确解析 IP 地址。
- 部分域名有多 IP，仅支持一个域名最多 8 个 IP 地址。

配置方法

- 可选配置。
- 配置 DNS 域名解析。
- 配置黑白名单。

检验方法

- 配置一条白名单和一条黑名单。
- 终端认证前可以访问白名单地址。
- 终端认证后无法访问黑名单地址。

相关命令

↘ 配置黑白名单

【命令格式】 **web-auth acl {black-ip** *ip***|black-port** *port***|black-url** *name***|white-url** *name***}**

【参数说明】 *ip*：黑名单 ip 地址

port：黑名单端口

name：黑白名单的 url

【命令模式】 全局模式配置模式，无线上黑名单还支持 wlansec 模式

【使用指导】 允许认证前访问采用白名单，禁止认证后访问采用黑名单。

配置举例

↘ 配置认证模式

【配置方法】

- 配置黑白名单

```
Ruijie(config)# web-auth acl black-ip 192.168.1.2
Ruijie(config)# web-auth acl white-url www.ruijie.com.cn
```

【检验方法】

- 查看配置是否成功

```
Ruijie(config)#show running-config
…
web-auth acl black-ip 192.168.1.2
web-auth acl white-url www.ruijie.com.cn
…
```

14.5.21 配置Portal通信端口

配置效果

- 配置后设备与 Portal 服务器通信的源端口为所配置端口。

注意事项

- 端口只能配置一个。

配置方法

- 配置指定端口为 portal 通信口。

检验方法

- 开启 web 受控后，认证时服务器上抓包，认证报文源 IP 为指定端口的 IP。

相关命令

配置通信端口

【命令格式】 **ip portal source-interface interface-type interface-num**

【参数说明】

【命令模式】 全局模式配置模式。

【使用指导】

配置举例

配置 portal 通信端口

【配置方法】

- 使用聚合口当作 portal 通信口地址。

```
Ruijie(config)# ip portal source-interface Aggregateport 1
```

【检验方法】

- 查看配置是否成功

```
Ruijie(config)#show running-config
ip portal source-interface Aggregateport 1
```

14.5.22 配置多Portal映射

配置效果

- 配置不同网段用户使用不同 Portal 进行认证。

注意事项

- 可配置多个映射，用户不在映射范围内，会使用默认 Portal 进行认证。
- 不同的映射范围不可相互覆盖。

配置方法

配置多 Portal 映射

- 全局模式下配置映射参数。

【命令格式】 **web-auth portal { eportalv1 | iportal |** *name* **} ip-mapping** *ipv4 mask*

【参数说明】 name: 使用的模板名称
ipv4:使用该模板的 ip 网段
mask:使用该模板的 ip 掩码

【命令模式】 全局配置模式。

【使用指导】 无。

检验方法

- 配置后使用不同网段进行认证，用户可以使用不同的 Portal 进行认证。

配置举例

配置多 Portal 映射

【配置方法】
- 配置映射网段。

```
Ruijie(config)# web-auth portal eportalv1 ip-mapping 192.168.2.0 255.255.255.0
```

【检验方法】
- 查看配置是否成功

```
Ruijie(config)#show running-config
…
web-auth portal eportalv1 ip-mapping 192.168.2.0 255.255.255.0
```

14.5.23 配置内置WEB认证NAT功能

配置效果

- 配置内置 web 认证支持 NAT。

注意事项

- 只对内置 WEB 认证有效。

配置方法

配置 NAT 支持功能

- 全局模式下开启功能。

【命令格式】 **iportal nat enable**

【参数说明】

【命令模式】 全局配置模式。

【使用指导】 无。

检验方法

- 配置后 NAT 场景可以使用内置 web 认证。

配置举例

↘ 配置 NAT 功能支持

【配置方法】

- 配置 NAT 功能支持。

```
Ruijie(config)# iportal nat enable
```

【检验方法】

- 查看配置是否成功

```
Ruijie(config)#show running-config
…
iportal nat enable
```

14.5.24 配置内置WEB认证重传次数

配置效果

- 配置内置 web 认证 http 连接重传次数。

注意事项

- 重传次数只对内置页面推送的 http 连接有效。

配置方法

↘ 配置内置 web 认证 http 重传次数

- 全局模式下配置参数。

【命令格式】 **iportal retransmit** *count*

【参数说明】 count: 重传次数

【命令模式】 全局配置模式。

【使用指导】 无。

检验方法

- 配置后发送内置 web 认证请求后，断开连接，设备可以发出重传。

配置举例

↘ 配置重传次数

【配置方法】
- 配置重传次数。

```
Ruijie(config)# iportal retransmit 5
```

【检验方法】
- 查看配置是否成功

```
Ruijie(config)#show running-config
…
iportal retransmit 5
```

14.5.25 配置内置WEB认证服务选择

配置效果

- 配置内置 web 认证使用的服务类型。

注意事项

- 无。

配置方法

↘ 配置内置 web 认证服务类型

- 全局模式下配置服务类型。

【命令格式】 **iportal service [internet** *internet-name*] **[local** *local-name* **]**

【参数说明】 internet-name: 使用的外部服务名称

local-name:使用的内部服务名称

【命令模式】 全局配置模式。

【使用指导】 无。

检验方法

- 。

配置举例

↘ 配置服务类型

【配置方法】
- 配置服务类型。

```
Ruijie(config)# iportal service local local-srv
```

【检验方法】
- 查看配置是否成功

```
Ruijie(config)#show running-config
…
iportal service local local-srv
```

14.5.26 配置内置WEB认证用户UA字段

配置效果

- 配置用户的 UA 字段对应的终端名称。

注意事项

- 用终端识别功能代替该功能，命令已经无效。

配置方法

↘ 配置内置 web 认证用户 UA 字段

- 全局模式下配置 UA 字段。

【命令格式】 **iportal user-agent** *ua-name* **type mobile** *ua-string*
【参数说明】 ua-name: UA 字段对应的名称
ua-string:UA 字符串内容
【命令模式】 全局配置模式。

【使用指导】 无。

检验方法

- 无。

配置举例

↘ 无

14.5.27 页面包定制规范

配置效果

- 使用内置 Porttal Web 认证时，允许定制自有 Web 页面，比如显示特定 LOGO 或者显示广告等。
- 单个页面包支持两套页面，以适配终端屏幕大小，比如小屏幕的移动终端。

注意事项

- 必须严格按照规范制作页面，避免新页面包无法使用。
- 页面包的文件数量不得超过 50 个（含 PC 版页面文件和移动终端版页面文件），每个页面文件名不得长于 32 字节
- 新页面包必须下载到./portal 目录下，新页面包名字不能默认页面包重叠，否则会覆盖默认页面包。
- 部分设备没有默认页面包，使用内置 Portal Web 认证时必须根据规范制定页面包并导入 FLASH。

配置方法

无

检验方法

- 用户连接到网络，打开浏览器认证，弹出定制页面。

相关命令

↘ 页面文件命名规范

页面文件名（含扩展名）	用途
login.htm	登录页面
online.htm	在线页面（用户登录成功之后的页面）
offline.htm	下线页面
login_mobile.htm	移动终端登录页面
online_mobile.htm	移动终端在线页面（用户登录成功之后的页面）
offline_mobile.htm	移动终端下线页面

↘ 登录页面制作规范

根据页面命名规范，PC 版的登录页面名称为 login.htm，移动终端版的登录页面名称为 login_mobile.htm。登录页面的内容规范说明如下：

- 表单元素

登录页面必须包含一个表单，提交方式固定为 POST。下面以 PC 版登录页面为例（移动终端版的类似），假设 PC 版的登录页面存放在/portal 目录下，相应的表单 html 编码大致如下：

```
<form method="post" action="/portal/login.htm">
...
</form>
```

一般来说，表单中需要包括以下页面元素：

1. 用户名文本框，用于给用户输入用户名，ID 为 username。(必选)
2. 密码文本框，用于给用户输入密码信息(不明文显示密码)，ID 为 password。(必选)
3. 登录按钮，用于 POST 方法提交表单。(必选)。
4. 显示认证失败原因的页面标签，ID 为 errormsg。(可选)，如果用户不关心登录失败的原因，那么登录页面中可以不包含该 errormsg 标签；如果想把认证失败的原因呈现给认证用户，那么就必须包括有这么一个可显示认证失败原因的区域，并且在页面加载的时候以 GET 的方式发送请求，请求内容为 errormessage，请求的结果将在 errormsg 标签中呈现。向服务器请求 errormsg 内容的脚本大致如下（以下只是一个例子，不代表是唯一写法）：

```
< script language=”javascript”>
//向服务器请求 errormessage 内容
function requestErrorMsg() {
    var _errormsg=document.getElementById(“errormsg”);
     var script=document.createElement(“script”);
script.src=”errormessage”+location.search;
_errormsg.appendChild(script);
}
```

```
//页面加载时需要调用 init 函数
function init() {
……
requestErrorMsg();
}
……
</script>
```

- 表单提交：

表单提交时，提交格式为 username=[AAAA]&password=[BBBB]&lang=[CCCC]，各个填充字段的含义如下：

[AAAA]：为用户在用户名文本框中填写的用户名。(必选)

[BBBB]：为用户在密码文本框中填写的密码。(必选)

[CCCC]：为用户当前的语言环境（可选），值 1 表示简体中文环境，2 表示英文环境，其他暂未定义，默认为简体中文，当语言环境是英文时，提交表单时需要将语言环境信息一并提交，否则象认证失败原因信息返回的是中文，与用户的实际语言环境就不一致了。

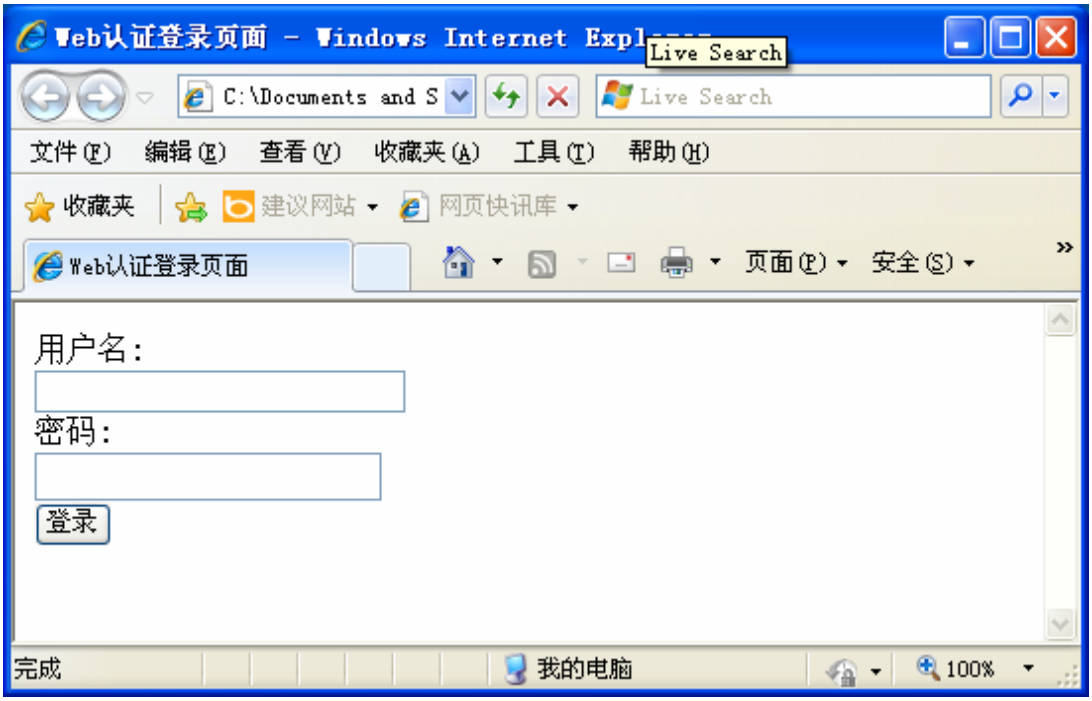
因此，登录页面的表单中至少要有 username 和 password 以及登录按钮这三个输入域（ 即 input 标签），如果登录页面有中英文环境，表单中还可能会有一个 lang 输入域，这个域一般是不可见的。

综上所述，可以得到登录页面最基本的 HTML 源码大致如下：

```
<html>
  <head>
  <title>Web 认证登录页面</title>
  </head>
  <script language=”javascript”>
   // 请求认证错误信息，如果认证成功或登录页面首次加载错误信息为空，不显示
   function requestErrorMsg() {
   var _errormsg=document.getElementById(“errormsg”);
     var script=document.createElement(“script”);
script.src=”errormessage”+location.search;
_errormsg.appendChild(script);
   }

function init() {
……
```

```
requestErrorMsg();
}

// 用户点登录按钮时执行的脚本。
function login() {
    document.getElementById('loginForm').action = "./login.htm"+location.search;
        document.getElementById('loginForm').submit();
        window.onbeforeunload = null;
        window.onunload = null;
}
……

</script>
    <body onload="init()">
        <form method="post" id=”loginForm”>
        用户名:<br>
        <input type="text" name="username" accesskey="u" size="25" value="" id="usrename">
        <br>
        密码:<br>
        <input type="password" name="password" accesskey="p" size="25"
              value="" id="password">
        <br>
<input type="button" onclick=”login()” value="登录" id=”loginButton”>
<input type="hidden" name="lang" value="" id="lan">
         <p name=”errormsg” id="errormsg"></p>
        </form>
    </body>
</html>
```

根据上述的定制，内置 portal 服务器向用户推送的登录页面样式大致如下：



通过上述的定制过程，登录页面已经具备了所有必要的元素，但这样的页面没有什么美观可言。用户可以在此基础之上进行美化，以及添加一些其他功能。比如添加背景、设置各种页面元素的样式等。

↘ 在线页面制作规范

在线页面的作用是告诉用户已经通过认证，可以正常使用网络。PC 版的在线页面名称为 online.htm，移动终端版的登录页面名称为 online_mobile.htm。

- 表单元素

在线页面必须包含一个表单，这个表单的作用是来提交下线请求的，因此，表单中也需要有一个下线按钮，表单的提交方式固定为 POST。下面以 PC 版的在线页面为例（移动终端版的类似），假设 PC 版的在线页面存放在/portal 目录下，相应的表单 html 编码大致如下：

```
<form method="post" action="/portal/online.htm">
...
</form>
```

在线页面的表单中需要包括以下页面元素：

1. ID 为 username 的页面标签，用于呈现用户的用户名信息。(可选)
2. ID 为 userip 的页面标签，用于呈现用户的 IP 地址。(可选)
3. ID 为 usermac 的页面标签，用于呈现用户的 MAC 地址。(可选)
4. ID 为 ssid 的页面标签，用于呈现用户所在的 SSID。(可选)
5. ID 为 availtime 的页面标签，用于呈现用户可用时长。(可选)

6. 下线按钮，用户想下线时可以点击该按钮，用于请求下线页面。(必选)

在线页面加载时需要通过 GET 方法向服务器请求用户信息，包括用户名、用户 IP 地址、用户 MAC 地址、关联的 SSID 以及可用时长，URI 为 getonlineinfo，为此需要实现 html 中 body 的 onload 方法。大致如下（只是举一个例子，不是唯一实现）：

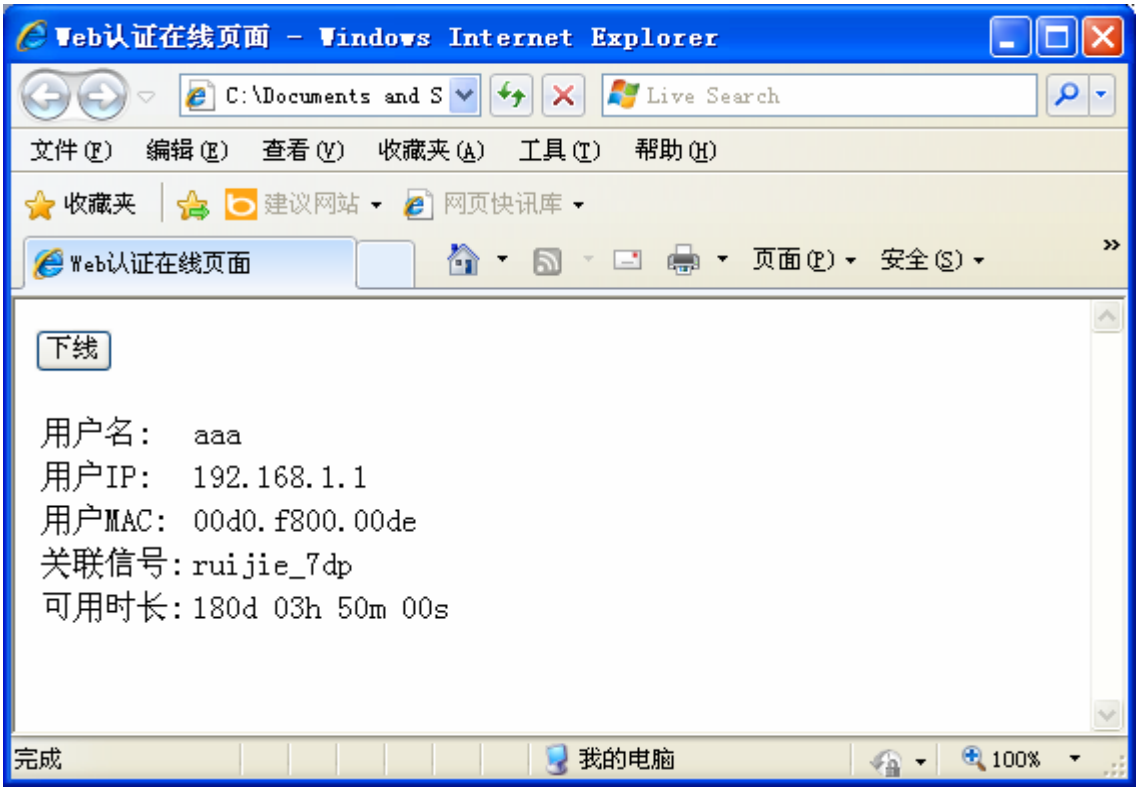
```
<script language="javascript">
    // 获取在线用户信息,包括用户名、IP、MAC、关联信号、可用时长
    function requestOnlineInfo() {
        var _availTime=document.getElementById("availtime");
        var script=document.createElement(“script”);
        script.src="getonlineinfo"+location.search;
        _availTime.appendChild(script);
    }

    function init() {
        requestOnlineInfo();
    }
  </script>
<body onload="init()">
……
</body>
```

综上所述，可以得到在线页面最基本的 HTML 源码大致如下：

```
<html>
  <head>
  <title>Web 认证在线页面</title>
  </head>
  <script language="javascript">
    // 获取在线用户信息,包括用户名、IP、MAC、关联信号、可用时长
    function requestOnlineInfo() {
        var _availTime=document.getElementById("availtime");
        var script=document.createElement(“script”);
```

```
            script.src="getonlineinfo"+location.search;
            _availTime.appendChild(script);
        }

        function init() {
            requestOnlineInfo ();
        }
        // 用户点下线按钮时执行的脚本，请求的 URI 为 offline.htm。
        function logout() {
            document.logoutform.action = "./offline.htm"+location.search;
            document.logoutform.submit();
            window.onbeforeunload = null;
            window.onunload = null;
        }

    </script>

    <body onload="init()">
        <form method="post" action="/portal/offline.htm" id="logoutform">
        <input type="button" onclick="logout()" value="下线" id="logoutButton">
        </form>
        <table>
        <tr><td>用户名:</td><td id="username"></td></tr>
        <tr><td>用户 IP:</td><td id="userip"></td></tr>
        <tr><td>用户 MAC:</td><td id="usermac"></td></tr>
        <tr><td>关联信号:</td><td id="ssid"></td></tr>
        <tr><td>可用时长:</td><td id="availtime"></td></tr>
        </table>
    </body>
</html>
```

根据上述的定制，内置 portal 服务器向用户推送的登录页面样式大致如下：



上述的在线页面就已具备了所有必要的元素。用户可以在此基础之上进行美化，以及添加一些其他功能。比如添加背景、设置各种页面元素的样式等。

下线页面制作规范

当用户在在线页面上点击下线按钮后就会引出下线页面，其作用是告诉用户已经下线成功，如果要使用网络，需要重新进行认证。PC 版的在线页面名称为 offline.htm，移动终端版的登录页面名称为 offline_mobile.htm。

页面元素：

1. ID 为 timeused 的页面标签，用于呈现用户已用时长的信息。(可选)

在下线页面的加载过程中 ,需要向服务器发送 GET 请求获取已经用时长信息 ,请求的 URI 为 getofflineinfo。为此需要实现 html 中 body 的 onload 方法。获取已用时长信息时 ,可以动态创建 script, 比如要发送的字段信息包含在 script 的 src 中 ,script.src="getofflineinfo"。大致如下（只是举一个例子，不是唯一实现）：

```
<script language="javascript">
    // 获取已用时长信息
    function requestOfflineInfo() {
    var _timeused =document.getElementById("timeused");
    var script=document.createElement("script");
    script.src="getofflineinfo"+location.search;
```

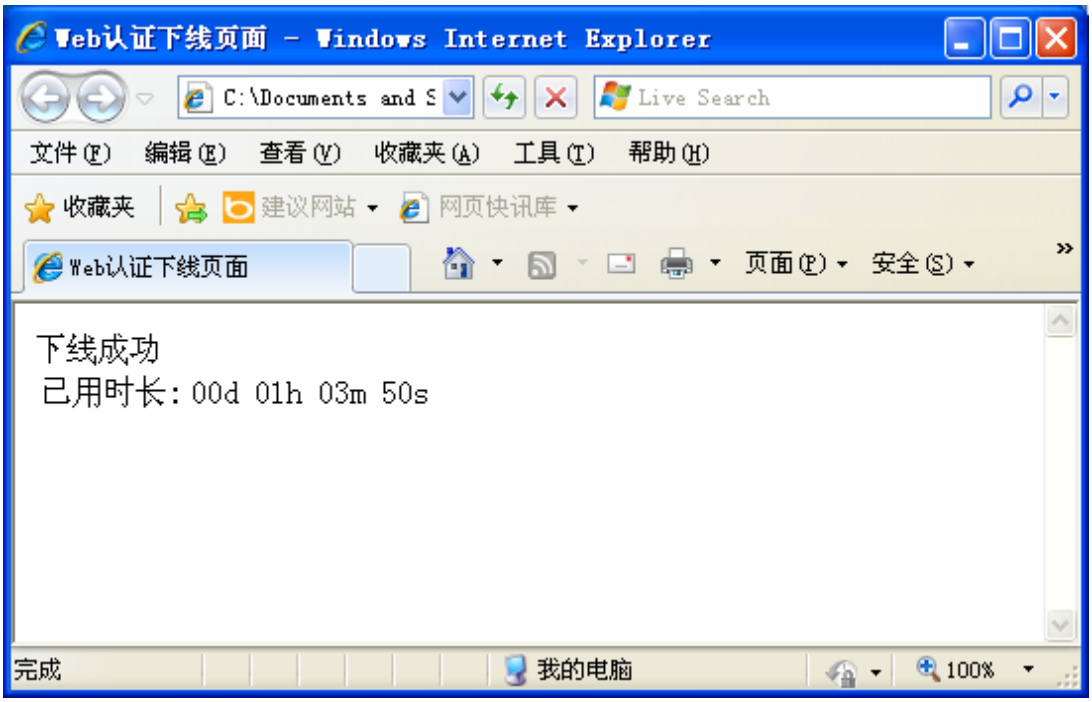
```
        _timeused.appendChild(script);
}

function init() {
        requestUserInfo();
}
</script>
<body onload="init()">
……
</body>
```

下线页面整体最基本的 HTML 源码大致如下：

```
<html>
  <head>
  <title>Web 认证下线页面</title>
  </head>
  <script language="javascript">
    // 获取已用时长信息
    function requestOfflineInfo() {
      var _timeused=document.getElementById("timeused");
      var script=document.createElement("script");
      script.src="getofflineinfo"+location.search;
      _timeused.appendChild(script);
}

function init() {
        requestOfflineInfo();
}
  </script>
```

```
<body onload="init()">
    下线成功<br>
<table>
<tr><td>已用时长:</td><td id="timeused"></td></tr>
</table>
  </body>
</html>
```

根据上述的定制，内置 portal 服务器向用户推送的下线页面样式大致如下



上述的下线页面就已具备了所有必要的元素。用户可以在此基础之上进行美化，以及添加一些其他功能。比如添加背景、设置各种页面元素的样式等

页面打包规范

按照本规范定制好页面后，需要将所有页面和页面元素文件打包，上传到设备，然后使用该页面包。有关压打包的相关规范如下：

1. 按照本规范定制好页面后，需要将所有页面和页面元素文件（如图片文件、样式表文件等）打包成 ZIP 格式的压缩包，比如 portal1_page.zip。
2. 页面包中可以包含目录。如下图所示，portal1_page.zip 中就包含有 style 目录。目录里包含了页面的 css 文件及其他图片资源文件。



..(上层目录)				
style	81.28 KB	60.69 KB	文件夹	2012-11-15 10:34:48
check_offline.htm	9.81 KB	3.34 KB	HTML 文档	2012-11-15 10:35:38
offline.htm	6.40 KB	2.65 KB	HTML 文档	2012-11-15 10:34:24
online.htm	13.13 KB	4.14 KB	HTML 文档	2012-11-15 10:34:10
login.htm	11.79 KB	3.90 KB	HTML 文档	2012-11-15 10:33:54
check_offline_mobile.htm	9.38 KB	3.22 KB	HTML 文档	2012-10-31 14:24:46
login_mobile.htm	10.39 KB	3.21 KB	HTML 文档	2012-10-31 11:47:16
online_mobile.htm	13.96 KB	3.91 KB	HTML 文档	2012-10-22 17:26:46
favicon.ico	1 KB	1 KB	图标	2012-07-02 09:41:58
offline_mobile.htm	5.09 KB	2.01 KB	HTML 文档	2012-06-30 11:07:18

页面包打包之后，然后通过 TFTP 等工具上传到设备的 flash:/portal/zip/目录下。然后要为 portal 服务器指定使用该页面包（也就是将 portal 服务器与页面包关联），为 portal 服务器指定页面包的具体过程，请参考 WEB 认证相关的配置指南。为 portal 服务器指定页面包之后，就可以看到 flash:/portal/ext_zip/目录下会生成一个与压缩包同名的目录，比如，压缩包名称为 portal1_page.zip ,就会生成 flash:/portal/ext_zip/protal1_page/这个目录 ,压缩包中的内容会自动解压到该目录下。之后 ,portal 服务器就可以为用户推送用户指定的 WEB 认证页面了。

配置举例

配置定制页面包

【配置方法】

- 配置定制页面包

```
Ruijie(config.tmplt.iportal)#page-suit ruijiepage
```

【检验方法】

- 查看配置是否成功

```
Ruijie#show web-auth template
Webauth Template Settings:
------------------------------------------------------------
  Name:      iportal
  Page-suit:    ruijiepage
  Advertising url:  default
  Advertising mode: online-popup
  Type:      Intral Portal
  Acctmlist:default
  Authmlist:default
```

14.5.28 升级兼容性说明

配置效果

- 部分配置命令在 11.X 系列软件上做了优化，格式上有所变化，具体参考后面的说明。
- 10.X 系列软件可以实现平滑升级，不会出现功能丢失的情况，但是升级后部分旧命令的显示会转化为新命令。
- 在 11.X 系列软件上对这部分旧命令执行 no 操作会提示不支持，需要用新的格式执行 no 操作。

注意事项

无

配置方法

- 部分格式变化的命令建议使用新格式配置。

检验方法

- 10.X 软件版本升级到 11.X 软件版本不会出现功能丢失，同时显示以及保存的格式采用新命令。
- 新格式命令的功能效果和旧命令一致。

相关命令

本小节

↘ 配置一代 web 认证的 portal 服务器资源地址

【命令格式】 **http redirect homepge** *url*

【参数说明】 *url*：一代 web 认证的 eportal 服务器资源地址

【命令模式】 全局配置模式

【使用指导】 11.X 版本首先会将该命令转化为一个 eportalv1 模板，然后用模板模式下的 url 命令配置和显示服务器地址，具体参考 1.4.1 章节。

↘ 配置一代 web 认证的 portal 服务器资源地址

【命令格式】 **http redirect homepge** *url*

【参数说明】 *url*：一代 web 认证的 eportal 服务器资源地址

【命令模式】 全局配置模式

【使用指导】 11.X 版本首先会将该命令转化为一个 eportalv1 模板，然后用模板模式下的 url 命令配置和显示服务器地址，具体参考 1.4.1 章节。

↘ 配置 portal-server

【命令格式】 **portal-server [eportal1 | eportalv2]**

【参数说明】 **eportav1**：一代 web 认证的 portal 信息

eportav2：二代 web 认证的 portal 信息

【命令模式】 全局配置模式

【使用指导】 11.X 版本首先会将该命令转化为一个 eportalv1 模板，然后用对应的信息填充，portal-server 主要参数包括服

务器 ip 地址和 url 地址，会被模板中的 ip 命令和 url 命令替代。

配置接口 web 认证受控

【命令格式】 **web-auth port-control**

【参数说明】 无

【命令模式】 接口配置模式

【使用指导】 11.X 版本会将该命令转化 web-auth enable <type>这里的 type 是指一代或者二代，默认是一代。

配置仅 ip 绑定模式

【命令格式】 **web-auth port-control ip-only-mode**

【参数说明】 无

【命令模式】 接口配置模式

【使用指导】 11.X 版本首先会将该命令转化为一个 eportalv1 模板，取决于实际配置。然后用模板模式下的 bindmode 命令配置和显示服务器绑定模式，具体参考 1.4.1 和 1.4.2 章节章节。

配置基于 vlan 的 web 认证功能

【命令格式】 **web-auth allow-vlan** *list*

【参数说明】 *list*：设置支持基于 VLAN 的 web 认证的 VLAN 列表为 list。

【命令模式】 全局配置模式

【使用指导】 11.X 版本会将该命令转化为一个 scc 免认证 vlan 命令。

显示一代 web 认证配置信息

【命令格式】 **show http redirect**

【参数说明】 无

【命令模式】 特权模式

【使用指导】 11.X 版本该旧命令不可用，改为 show web-auth template。

显示端口受控信息

【命令格式】 **show web-auth port-control**

【参数说明】 无

【命令模式】 特权模式

【使用指导】 11.X 版本该旧命令不可用，改为 show web-auth control。

配置举例

配置一代 web 认证

【配置方法】

- 产品运行 10.X 版本并且已经配置了一代 web 认证服务器 ip

```
Ruijie(config)# http redirect 192.168.197.64
```

- 产品升级到 11.X 版本

【检验方法】

- 升级后 show running-config，配置已更新为新命令格式

Ruijie#sh running-config

```
web-auth template eportalv1
  Ip 192.168.197.64
!
```

14.5.29 配置内置共享账号同名账号的用户限制

配置效果

- 对使用 local 认证，开启账号共享功能，此时可以限制同名账号登陆的用户个数。

注意事项

- 只针对内置 local 认证生效，对所有的用户生效

配置方法

↘ 配置账号共享个数

- 全局模式下配置。

【命令格式】 **web-auth account-share ip-limit xxx**
【参数说明】 0 为无限制
【命令模式】 全局模式
【使用指导】 无

检验方法

- 配置用户限制后，内置 local 认证同名用户只能允许一定个数的用户上线，当超过限制时，会自动把最先上线的用户踢下线，然后新的用户上线。

配置举例

↘ 配置用户个数限制

【配置方法】
- 配置用户个数限制。

```
Ruijie(config)# web-auth account-share ip-limit 2
```

【检验方法】
- 查看配置是否成功

【配置方法】
- 配置用户个数限制。

```
Ruijie(config)# web-auth account-share ip-limit 2
```

【检验方法】
- 查看配置是否成功

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

14.5.30 配置内置logo替换功能

配置效果

- 配置内置 logo 替换功能，可以替换内置 portal 所有页面的 logo

注意事项

- Logo 上传目录为/data/portal/logo，名字固定为 free_login_logo.jpg

配置方法

↘ 全局模式下配置。

【命令格式】 **web customized-logo enable**
【参数说明】 无
【命令模式】 全局模式
【使用指导】 无

检验方法

- 配置开启此功能后，上传图片，查看内置 portal 的页面的 logo 是否有被替换掉。

配置举例

↘ 配置 logo 替换开关命令

【配置方法】
- 打开 logo 替换功能开关功能。
- 非必须配置，在有需要替换内置认证页面的 logo 时开启

```
Ruijie(config)# web customized-logo enable
```

【检验方法】 ● 查看配置是否成功

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

14.6 监视与维护

清除各类信息

作用	命令
强制用户下线	**clear web-auth user** { **all** | **ip** *ip-address* | **mac** *mac-address* | **name** *name-string* | **session-id** *num* }
删除全部免认证网络资源	**clear web-auth direct-site**
删除全部免认证用户	**clear web-auth direct-host**
删除全部免认证 arp 资源	**Clear web-auth direct-arp**
删除全部的组信息	**Clear web-auth group**

查看运行情况

作用	命令
查看 web 认证基本参数配置。	**show web-auth parameter**
查看 web 认证模板配置信息	**show web-auth template**
查看免 Web 认证的用户范围。	**show web-auth direct-host [range]**
查看直通地址范围。	**show web-auth direct-site [range]**
查看直通 ARP 范围。	**show web-auth direct-arp**
查看 TCP 拦截端口。	**show web-auth rdport**
接口上的认证配置信息。	**show web-auth control**
查看所有用户或是指定用户的在线信息。	**show web-auth user**{ **all** | **ip** *ip-address* | **mac** *mac-address* | **name** *name-string* | **session-id** *num* }
显示 web 认证 CGI 配置	**show web-auth cgi**
查看全局 web 认证基本信息	**show web-auth global**
查看全局 web 认证方法	**show web-auth global authentication**
查看全局 web 认证定制页面包	**show web-auth global customized-pages**
查看内置认证服务器信息	**show web-auth global local-portal**
查看全局 web 认证模板信息	**show web-auth global template**
查看全局 web 认证类型	**show web-auth global webauth-type**
查看 web 认证配置信息	**show web-auth info**
查看内置 web 认证信息	**show web-auth local-portal**
查看 web 认证映射信息	**show web-auth ip-mapping**
查看用户的上下线记录	show web-auth syslog ip *ip-address*

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
web 认证 debug	**debug web-auth all**

15 全局 IP+MAC 绑定

15.1 概述

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

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

下文仅介绍全局 IP+MAC 绑定的相关内容。

协议规范

- 无

15.2 典型应用

典型应用	场景描述
全局 IP+MAC 地址绑定	仅指定 IP 的主机可以访问网络，主机在同一台设备下是可以移动的

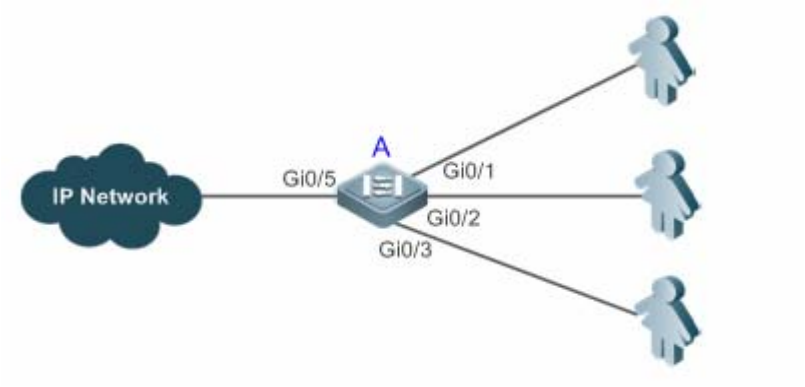
15.2.1 全局IP+MAC地址绑定

应用场景

为了方便管理，管理员为每台主机固定分配了一个 IP 地址。

- 仅指定 IP 的主机可以访问外部网络，防止非法主机盗用 IP。
- 主机可以在相同设备下可以自由移动。

图 15-1



【注释】 A 为接入设备。
User 为静态分配了 IP 地址的接入主机。
IP Network 为外部 IP 网络。

功能部属

- 手动配置全局 IP 和 MAC 地址绑定（本例列举 3 个用户）

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

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

15.3 功能详解

基本概念

↘ IPv6 地址绑定模式

IPv6 地址绑定模式包括兼容、宽松以及严格 默认为严格 ,针对 IPv4+MAC 绑定下的 IPv6 报文转发控制而言 ,不存在 IPv4+MAC 绑定时模式并不生效 , 所有 IPv4 报文和 IPv6 都可以放行 , 存在了 IPv4+MAC 绑定后模式生效 , 然后依据对应的转发规则控制 IPv4 和 IPv6 报文是否放行，转发规则如下表所示：

模式	IPv4 报文转发规则	IPv6 报文转发规则
严格	符合全局 IPv4+MAC 绑定条件的报文转发	符合 IPv6+MAC 绑定条件的报文转发(绑定由其他接入安全功能生成 ,比如端口安全、IPv6 Source Guard 等)

宽松	符合全局 IPv4+MAC 绑定条件的报文转发	如果存在 IPv6+MAC 的绑定那么符合绑定条件的报文转发（绑定由其他接入安全功能生成，比如端口安全、IPv6 Source Guard 等） 如果不存在 IPv6+MAC 的绑定，转发所有 IPv6 报文
兼容	符合全局 IPv4+MAC 绑定条件的报文转发	符合源 MAC 为全局 IPv4+MAC 绑定中的 MAC 地址的 IPV6 报文转发 符合全局 IPv6+MAC 绑定条件的报文转发(绑定由其他接入安全功能生成，比如端口安全、IPv6 Source Guard 等）

↘ 地址绑定例外端口

IP 地址和 MAC 地址绑定功能缺省对设备上的所有端口都生效，通过配置例外口的方式可以使绑定功能在部份端口上不生效。在应用中设备的上链端口的 IP 报文的绑定关系是不确定的，通常将设备的上链端口配置为例外口，此时上链端口则不进行 IP 地址与 MAC 地址的绑定检查。

功能特性

功能特性	作用
配置全局 IP+MAC 地址绑定	对 IPv4 报文或者 IPv6 报文进行转发控制
配置 IPv6 地址绑定模式	改变 IPv6 报文的转发控制规则
配置地址绑定例外端口	全局地址绑定功能在对应端口上不生效

15.3.1 配置全局IP+MAC地址绑定

工作原理

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

相关配置

↘ 配置 IP+MAC 地址绑定

全局模式下，使用 **address-bind** 命令添加或者删除 IPv4+MAC 地址绑定。

↘ 配置使得 IP+MAC 地址绑定生效

全局模式下，使用 **address-bind install** 命令配置地址绑定功能生效，默认不生效。

15.3.2 配置IPv6 地址绑定模式

工作原理

存在全局 IPv4+MAC 地址绑定并且绑定开启的情况下，根据不同的模式控制 IPv6 报文的转发，模式包括严格、宽松或者兼容等。

相关配置

↘ 配置 IPv6 地址绑定模式

缺省情况下，地址绑定模式为严格。

使用 address-bind ipv6-mode 命令指定地址绑定模式。

15.3.3 配置地址绑定例外端口

工作原理

通过配置例外口的方式可以使绑定功能在部份端口上不生效。

相关配置

↘ 配置地址绑定例外端口

使用 **address-bind uplink** 命令可以配置例外端口，默认全部都是非例外端口。

15.4 产品说明

NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE 支持 IPV6 转发功能；NBR800G、NBR950G、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR108G-P 、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1500G、NBR2000G 不支持 IPV6 转发模式。

15.5 配置详解

配置项	配置建议 & 相关命令	
配置全局 IP+MAC 地址绑定	⚠ 必须配置。用于生成地址绑定并开启绑定功能。	
	address-bind	配置生成全局 IPv4+MAC 地址绑定

	address-bind install	开启地址绑定功能
	address-bind binding-filter logging	配置全局 IPv4+MAC 绑定过滤日志
配置 IPv6 地址绑定模式	⚠ 可选配置。用于改变 IPv6 地址绑定模式。	
	address-bind ipv6-mode	配置 IPv6 地址绑定模式
配置地址绑定例外端口	⚠ 可选配置。用于配置部分端口的地址绑定功能不生效。	
	address-bind uplink	配置地址绑定的例外端口

15.5.1 配置全局IP+MAC地址绑定

配置效果

- 生成全局 IPv4+MAC 地址绑定
- 开启地址绑定功能对 IPv4 或者 IPv6 报文进行转发控制

注意事项

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

配置方法

↘ 配置全局 IP+MAC 地址绑定

- 必须配置，全局配置模式下配置。

↘ 开启地址绑定功能

- 必须配置，全局配置模式下配置。

↘ 配置全局 IPv4+MAC 绑定过滤日志

- 可选配置，全局配置模式下配置。

检验方法

使用 **show run** 或者 **show address-bind** 验证配置是否生效。

相关命令

↘ 配置全局 IP+MAC 地址绑定

【命令格式】 **address-bind** { *ip-address* | *ipv6-address* } *mac-address*

【参数说明】 *ip-address*：绑定的 IPv4 地址

ipv6-address：绑定的 IPv6 地址

mac-address：绑定的 MAC 地址

【命令模式】 全局配置模式

【使用指导】 配置 IP 地址和 MAC 地址的绑定关系。该命令仅无线 AC 产品不支持。

配置开启地址绑定功能

【命令格式】 **address-bind install**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 使全局 IP 和 MAC 地址绑定生效，控制 IPv4 或者 IPv6 报文的转发。该命令仅无线 AC 产品不支持。

配置开启地址绑定过滤日志功能

【命令格式】 **address-bind binding-filter logging** [**rate-limit** *rate*]

【参数说明】 **rate-limit** *rate*：表示全局 IPv4+MAC 绑定过滤日志打印速率。

【命令模式】 全局配置模式

【使用指导】 配置不带 rate-limit 参数时表示打开绑定过滤日志，速率采取默认速率即每分钟 10 条。

开启绑定过滤日志后，不符合全局 IPv4+MAC 绑定的报文，会打印日志告警。

开启绑定过滤日志后，绑定过滤日志打印超过配置速率后，会提示被抑制的日志个数。

配置举例

配置全局 IP+MAC 地址绑定并使能地址绑定功能

【配置方法】

- 配置生成全局 IPv4+MAC 地址绑定
- 开启地址绑定功能

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

【检验方法】 查看设备上的全局 IP+MAC 地址绑定

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

常见错误

- 无

15.5.2 配置IPv6 地址绑定模式

配置效果

- 改变 IPv6 地址绑定模式，IPv6 报文的转发规则发生变化。

注意事项

- 无

配置方法

↘ 配置 IPv6 地址绑定模式

- 可选配置，需要改变 IPv6 报文转发控制规则时来配置。

检验方法

- 使用 **show run** 验证配置是否生效。

相关命令

↘ 全局配置模式下配置 IPv6 地址绑定模式

【命令格式】 **address-bind ipv6-mode** { **compatible | loose | strict** }

【参数说明】 **compatible**：兼容模式

loose：宽松模式

strict：严格模式

【命令模式】 全局模式

【使用指导】 -

配置举例

↘ 配置 IPv6 地址绑定模式。

【配置方法】

- 配置全局 IP+MAC 地址绑定
- 开启地址绑定功能
- 配置 IPv6 地址绑定模式为兼容模式

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

```
Ruijie(config)# address-bind install
Ruijie(config)# address-bind ipv6-mode compatible
```

【检验方法】 **show run** 查看设备上的配置

常见配置错误

- 无

15.5.3 配置地址绑定例外端口

配置效果

- 配置指定端口的地址绑定功能不生效，所有 IP 报文都可以转发

注意事项

- 只能在交换口或者 L2AP 口进行配置

配置方法

↘ 配置地址绑定例外端口

- 可选配置，全局配置模式下配置，需要特殊指定地址绑定功能不生效的端口时配置。

检验方法

使用 **show run** 或者 **show address-bind uplink** 验证配置是否生效。

相关命令

↘ 配置地址绑定例外端口

【命令格式】 **address-bind uplink** *interface-id*
【参数说明】 *interface-id*：交换口或 L2AP 口
【命令模式】 全局配置模式
【使用指导】 该命令仅无线 AC 产品不支持。

配置举例

↘ 配置地址绑定例外端口

【配置方法】
- 配置生成全局 IPv4+MAC 地址绑定
- 开启地址绑定功能
- 配置地址绑定例外端口

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# address-bind 192.168.5.1 00d0.f800.0001
Ruijie(config)# address-bind install
Ruijie(config)# address-bind uplink GigabitEthernet 0/1
```

【检验方法】 查看设备上的全局 IP+MAC 地址绑定

```
Ruijie#show address-bind
Total Bind Addresses in System : 1
IP Address          Binding MAC Addr
---------------     ----------------
192.168.5.1         00d0.f800.0001
Ruijie#show address-bind uplink
Port        State
----------  ---------
Gi0/1       Enabled
Default     Disabled
```

常见错误

- 无

15.6 监视与维护

清除各类信息

无

查看运行情况

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

查看调试信息

无

16 IPoE

16.1 概述

IPoE 认证基于上网终端的 MAC 地址对用户进行认证和计费，用户上网时无需输入用户名和密码。

IPoE 支持 Authentication，Authorization，Accounting 三种安全应用，简称 AAA。

Authentication： 认证，用于判定用户是否可以获得访问权，限制非法用户；

Authorization： 授权，授权用户可以使用哪些服务，控制合法用户的权限；

Accounting： 计账，记录用户使用网络资源的情况，为收费提供依据。

IPoE 可以部署在对接入用户进行控制的网络中，以实现对接入用户身份验证、授权服务等

下文仅介绍 IPoE 的相关内容。

协议规范

- RFC2131：Dynamic Host Configuration Protocol
- RFC2132：DHCP Options and BOOTP Vendor Extensions
- RFC3046：DHCP Relay Agent Information Option

16.2 典型应用

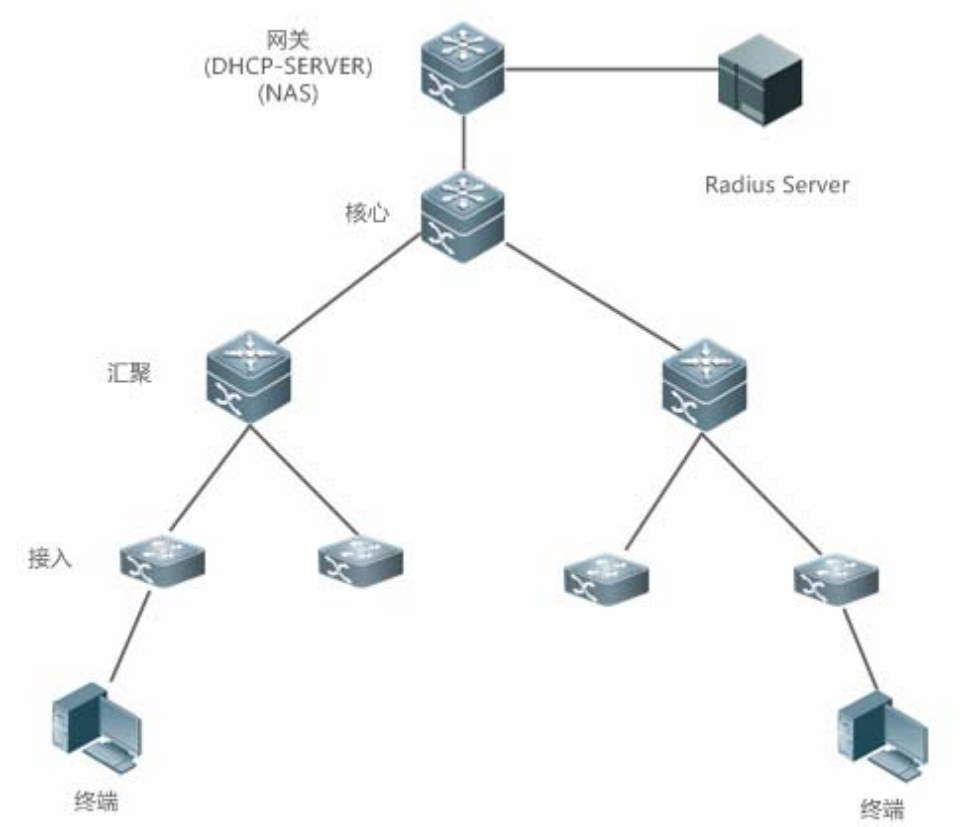
典型应用	场景描述
IPoE 用户认证	DHCP Client 经由三层网络以 IPoE 方式接入网关

16.2.1 IPoE用户认证

应用场景

- DHCP Client 经由二层网络接入到接入设备，经由三层网络以 IPoE 方式接入到网关。
- 接入设备作为 DHCP 中继向网关申请 IP 地址。
- 采用 RADIUS 作为认证、授权和计费服务器。

图 16-1 DHCP 报文触发 IPoE 接入



功能部属

- 在网关设备上使能 IPoE 功能。
- PC 客户端通过 dhcp 获取到 IP 地址。
- PC 客户端通过 web 认证，认证上网。

16.3 功能详解

基本概念

↘ radius

radius（remote authentication dial-in user service）是一种远程认证协议，在 RFC2865 中定义，有着广泛的支持。利用该协议，可以实现服务器远程部署并实施认证。实际部署 IPoE 时，server 通常都是选择远程部署，设备和 server 间的 IPoE 认证信息通过 radius 传输。

↘ 超时

认证过程中设备需要和终端、服务器通信，如果终端或服务器在协议指定的时间内没做出应答，则认为超时，超时会导致认证失败。实际部署时，需要注意 IPoE 有自己的超时时间，radius 协议也有自己的超时时间，配合使用时必须保证 IPoE 的超时时间大于 radius 的超时时间。

授权

授权是指用户认证通过后给用户绑定一定的服务，比如绑定 IP 地址、绑定 QoS 等。

计费

计费功能可以实现用户网络审计，比如使用网络的时间、产生的流量，这有利于网络运维和管理。

> 有些 radius 服务器，比如锐捷 SAM 和锐捷 SMP 软件，需要依靠计费报文来判断用户的上下线状态，因此选择这些服务器软件作为 radius 服务器时，必须要配置计费功能。

功能特性

功能特性	作用
IPoE 用户认证	提供用户的安全准入，通过认证的用户才可以访问网络。

16.3.1 IPoE用户认证

工作原理

IPoE 认证基于上网终端的 MAC 地址对用户进行认证和计费，用户上网时无需输入用户名和密码。

IPoE 认证提供如下功能：

IPoE 用户认证

IPoE 认证基于上网终端的 MAC 地址对用户进行认证和计费，用户上网时无需输入用户名和密码。

相关配置

开启 IPoE 功能

- 缺省情况下，设备上 IPoE 功能关闭。
- 使用 **ipoe-auth enable** 命令可以启动或关闭 IPoE 功能。
- 必须在设备上启用 IPoE 功能，IPoE 才能正常工作。

16.4 产品说明



NBR108G-P、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1500G、NBR2000G 不支持二层网络下内置 web 认证无感知功能 ;NBR800G、NBR950G、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持二层网络下内置 web 认证无感知功能。

16.5 配置详解

配置项	配置建议 & 相关命令	
开启 IPoE 功能	⚠ 必须配置。用于建立 IPoE 服务。	
	ipoe-auth enable	配置在设备上使能 IPoE 功能并指定用户的接入模式
	⚠ 可选配置。	
	ipoe-auth dhcp user-limit	配置设备上允许 DHCP 报文触发创建的 IPoE 会话的最大数
	ipoe-auth quiet-period	配置 IPoE 认证用户的静默时间
	ipoe-auth server-timeout	配置认证超时时间

16.5.1 开启IPoE功能

配置效果

启动 IPoE 功能后，提供用户的安全准入，通过认证的用户才可以访问网络。

注意事项

-

配置方法

↘ 使能 IPoE 功能

- 必须配置。
- 若无特殊要求，应启动 IPoE 功能。

↘ 配置允许 DHCP 报文触发创建的 IPoE 会话的最大数

- 可选配置。
- 默认情况下不限制 IPoE 会话的最大数，可配置 IPoE 会话的最大数。

配置 IPoE 认证用户的静默时间

- 可选配置。
- 默认情况下用户的静默时间功能处于关闭状态，可配置用户认证失败以后，设备需要等待的时间间隔。

配置 IPoE 认证超时时间

- 可选配置。
- 默认配置为 25 秒。如果 radius 超时时间更大，可配置一个比其更大的值。

检验方法

- **show run** 检查 IPoE 配置情况。

相关命令

使能 IPoE 功能

【命令格式】 **ipoe-auth enable**
【参数说明】 -
【命令模式】 全局模式
【使用指导】 若无特殊要求，应启动 IPoE 功能。

配置允许 DHCP 报文触发创建的 IPoE 会话的最大数

【命令格式】 **ipoe-auth user-limit** *number*
【参数说明】 *number*：允许 DHCP 报文触发创建的 IPoE 会话的最大数，输入范围 1～1000000，不输入默认为 0，表示不做限制。
【命令模式】 全局模式
【使用指导】 DHCPv4 报文触发创建的 IPv4 IPoE 认证用户数目达到最大值后 ,后续 DHCPv4 报文不能触发创建 IPv4IPoE 认证用户。

配置 IPoE 认证用户的静默时间

【命令格式】 **ipoe-auth quiet-period** *time*
【参数说明】 *time*：静默时间，输入范围 0～65535，单位：秒，不输入默认为 10。
【命令模式】 全局模式
【使用指导】 本命令用来设置用户认证失败以后，设备需要等待的时间间隔。在静默期间，设备不对来自认证失败用户的报文进行认证处理，直接丢弃，可以防止该类用户报文持续发送给服务器认证而对设备性能造成影响。

配置 IPoE 认证超时时间

【命令格式】 **ipoe-auth server-timeout** *time*

【参数说明】 *time*：认证超时时间，输入范围 1～65535，单位：秒，不输入默认为 30。

【命令模式】 全局模式

【使用指导】 若 radius 有配一个较大的认证超时时间，可使用本命令来保证 IPoE 的超时时间大于 radius 的超时时间。

配置举例

开启 IPoE 认证功能

【配置方法】

- 在网关上启动 IPoE 功能。

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

【检验方法】

- 检查是否启动 IPoE 功能。

```
Ruijie# show run | include ipoe-auth
 ipoe-auth enable
```

常见错误

-

16.6 监视与维护

清除各类信息

作用	命令
清除 IPoE 认证用户，强制用户下线	**clear ipoe-auth user**

查看运行情况

作用	命令
查看 IPoE 认证用户表项信息	**show ipoe-auth summary**
查看 IPoE 认证用户详细信息	**show ipoe-auth user**

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 IPoE 事件的调试开关。	**debug ipoe event**

17 IP-GROUP

17.1 概述

ip-group 使用 ip 列表提供 ip 匹配功能。目前支持以下 ip 列表：

11. ip 地址范围的列表
12. ip 网段的列表
13. 路由地址库列表

协议规范

无

17.2 典型应用

ip-group 主要是配合其他模块使用，不单独使用。比如用于计费模块特定 ip 地址免流量计费。

17.3 功能详解

基本概念

↘ ip-group 组

ip-group 组中可以定义一系列的 ip 网段和 ip 地址范围，用于匹配某个 ip 是否在定义的 ip-group 组中。

功能特性

功能特性	作用
ip-group 组功能	实现匹配某个 ip 地址是否在 ip-group 组中

17.3.1 ip-group组基本功能

匹配 ip 地址是否在 ip-group 组中。

工作原理

ip-group 组的功能匹配，包含以下几个步骤：

- 创建 ip-group 组
- ip-group 组配置 ip 网段或 ip 地址范围
- 使用 ip-group 组提供的服务来获取匹配的结果

相关配置

配置 ip-group

配置 ip-group 包括：

产品支持情况 配置 ip-group(可选)

全局配置模式中，使用 **ip-group** *id*，创建/配置指定 ip-group 组；使用 **no ip-group** *id*，删除指定 ip-group 单元。其中 *id* 是指定的 ip-group 的索引。

产品支持情况 配置 ip-group 组的描述(可选)

在 ip-group 配置模式中，使用 **descrption** *name*，来设置 ip-group 组的描述；使用 **no descrption** 来删除配置的描述。

产品支持情况 配置 ip 地址范围(可选)

在 ip-group 模式下，使用 **ip-range** *start [end]*，设置 ip 地址范围；使用 **no ip-range** *start [end]*，来删除已经配置的 ip 地址范围

产品支持情况 配置 ip 地址网段(可选)

在 ip-group 模式下，使用 ip-subnet subnet { mask | mask_len }设置 ip 网段；使用 no ip-subnet subnet { mask | mask_len }，来删除已经配置的 ip 网段。

产品支持情况 配置路由地址库(可选)

在 ip-group 模式下，使用 **route-db** *name* 配置路由地址库表；使用 **no route-db** name 来删除已经配置的路由地址库表。

17.4 配置详解

配置项	配置建议 & 相关命令	
配置 ip-group 基本功能	⚠ 必须配置。用于配置 ip-group 组的 ip 列表。	
	ip-group *id*	配置 ip-group 组
	ip-range *start [end]*	配置 ip 地址范围
	ip-subnet *subnet { mask | mask_len }*	配置 ip 地址网段
	route-db ***name***	配置路由地址库表

17.4.1 配置ip-group基本功能

配置效果

提供 ip 地址匹配服务。

注意事项

-

配置方法

↘ 配置 ip-group 组

- 可选配置。

【命令格式】 **ip-group** *id*
【参数说明】 Id 的范围是 1-1000
【缺省配置】 -
【命令模式】 全局模式
【使用指导】 使用 **no ip-group** *id* 命令，删除 ip-group 组

↘ 配置 ip-group 组的描述

- 可选配置。

【命令格式】 **descrption** *name*
【参数说明】 *Name* 说明字符串，不能包含空格，不能超过 32 个字符
【缺省配置】 缺省情况下没有 ip-group 组的描述
【命令模式】 ip-group 模式
【使用指导】 ip-group 模式下使用 **no descrption** 删除说明字符串

↘ 配置 ip 地址范围

- 可选配置。

【命令格式】 **ip-range** *start [end]*
【参数说明】 *start*：网段起始 ip 地址
end：网段结束 ip 地址。缺省情况 *end* 的值等于 *start* 值
【缺省配置】 缺省情况下没有配置 ip 地址范围
【命令模式】 ip-group 模式
【使用指导】 ip-group 模式下使用 **no ip-range** *start [end]* 删除配置的 ip 地址范围

配置 ip 地址网段

- 可选配置。

【命令格式】 **ip-subnet** *subnet { mask | mask_len }*
【参数说明】 *subnet：*ip 网段起始地址
mask：掩码
mask_len：掩码长度
【缺省配置】 缺省情况下没有配置 ip 网段
【命令模式】 ip-group 模式
【使用指导】 ip-group 模式下使用 **no ip-subnet** *subnet mask_len* 删除 ip 地址网段

配置路由地址库表

- 可选配置。

【命令格式】 **route-db *name***
【参数说明】 *name: 路由地址库表名称*
【缺省配置】 缺省情况下没有配置路由地址库表项
【命令模式】 ip-group 模式
【使用指导】 ip-group 模式下使用 **no route-db** *name* 删除配置的路由地址库表

检验方法

通过 show 命令查看。

- 查看 ip-group 的配置信息。
- 查看 show 命令查看 ip-group id 和 ip 地址匹配的结果。

配置举例

以下配置举例，仅介绍与 ip-group 模块相关的配置。

在设备上配置 ip-group，配置 ip 网段

【网络环境】 -
【配置方法】
- 配置 ip-group 组。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# ip-group 1
Ruijie(config-ip-group)# descrption test
Ruijie(config-ip-group)#ip-range 1.1.1.5 1.1.1.10
Ruijie(config-ip-group)#ip-subnet 1.1.10.0 24
Ruijie(config-ip-group)#route-db cmc
```

常见错误

- 无。

17.5 监视与维护

清除各类信息

无

查看运行情况

作用	命令
查看 ip-group 组的配置	**show ip-group** [*id*]
查看 ip-group 的统计信息	**show ip-group 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
打开 ip-group ctrl 调试开关	**debug ip-group ctrl**
关闭 ip-group ctrl 调试开关	**no debug ip-group ctrl**
打开 ip-group db-ctrl 调试开关	**debug ip-group db-ctrl**
关闭 ip-group db-ctrl 调试开关	**no debug ip-group db-ctrl**

18 APP-AUTH

18.1 概述

传统的 WEB 认证通常是基于 radius 协议的标准认证方式，认证交付过程复杂。APP-AUTH 提供了一种基于 HTTP 的开放式、轻量级的交互认证方法，交互原理类似 linux 标准的 wifidog 协议，可以与锐捷商业营销平台(wmc/mcp)进行对接，进行短信认证、固定账号认证、微信连 wifi 认证等。

下文仅介绍 APP-AUTH 的相关内容。

协议规范

- 无

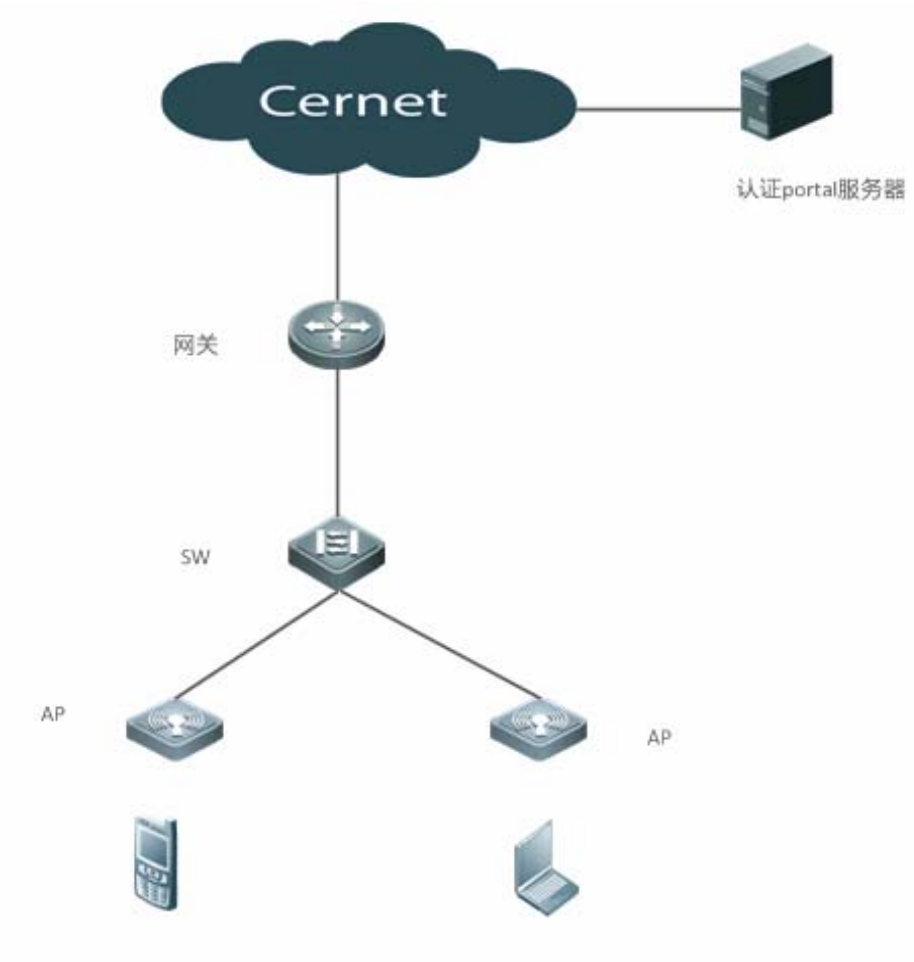
18.2 典型应用

典型应用	场景描述
APP-AUTH 的典型应用场景	描述 APP-AUTH 的典型应用场景

18.2.1 APP-AUTH典型应用场景

应用场景

如下图所示，移动终端通过网关与认证服务器的联动完成认证接入功能。



【注释】 认证服务器可以是锐捷 WMC 或 MCP，或者第三方遵循 APP-AUTH 标准认证协议的服务器。

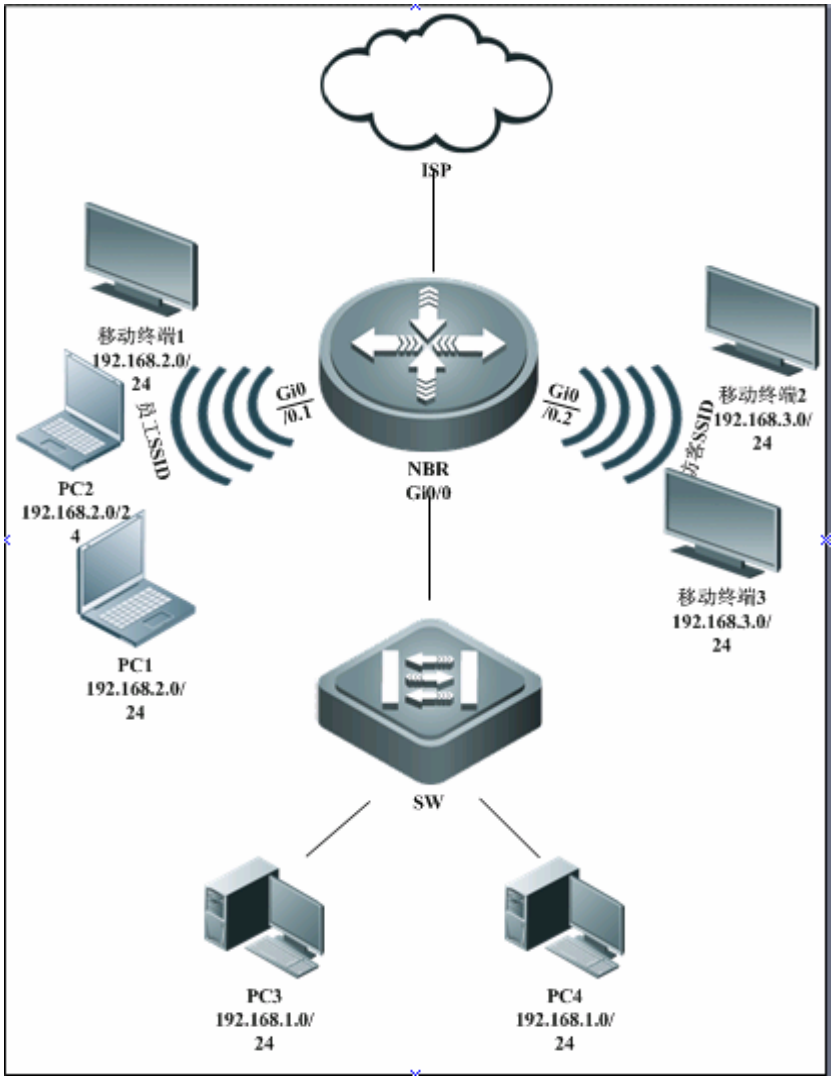
功能部属

- 部署网关与认证服务器进行 wifidog 的认证
- 部署网关与认证服务器进行微信连 wifi 认证

18.2.2 本地认证

应用场景

如下图所示，移动终端通过网关与接入公网，且认证由网关本身完成。



【注释】 无需外部认证服务器介入。

功能部属

- 部署网关本地认证

18.3 功能详解

基本概念

↘ 免认证应用

通常终端在未认证前是无法访问网络的。通过设置免认证应用，允许终端上的某些应用可以在认证前直接访问网络。认证应用是指应用识别库中定义的应用分类。

wifidog 协议

wifidog 是 linux 标准推荐的一种基于 token 校验的安全认证协议，该协议完全使用 http 通信。网关的 wifidog 是在 linux 基础上加入了相关设备信息上进行开发的。

微信连 wifi 协议

微信连 wifi 协议是微信推出的开放式认证协议，用户通过使用微信即可快速的完成认证过程，而不需要输入用户名、密码等繁琐的过程。通过微信连 wifi 协议，可以实现广告常驻与微信等功能。

认证策略

目前认证策略主要使用在 app-auth 的本地认证场景，根据不同的用户需求，配置不同的认证策略。

用户组

不同的用户组有不同的权限。

用户

用户可以属于各个用户组。

功能特性

功能特性	作用
基于 wifidog 的认证	网关使用 wifidog 协议与认证服务器进行交互认证
基于微信连 wifi 的认证	网关使用微信连 wifi 协议与认证服务器进行交互认证
本地认证	网关自身作为认证服务器进行认证

18.3.1 基于wifidog的认证

工作原理

采用类似 linux 标准的 wifidog 协议，通过 token 校验方法保证认证协议的安全。wifidog 协议只是提供了认证方法，具体表现形式可以是短信认证、固定账号认证等。表现形式由服务器进行控制。

相关配置

开启 APP-AUTH 模块功能

APP-AUTH 功能需要全局开启。开启命令为:**app-auth enable, app-auth cwmp enable**

配置 WIFIDOG 认证协议

缺省情况下无配置。

需要配置重定向方法为 wifidog。配置命令:**app-auth cfg-opt rdt-for-wifidog**

配置重定向地址，配置命令: **app-auth ad-ur**l url

配置 token 校验地址，配置命令: **webservice server-ur**l url

18.3.2 基于微信连wifi的认证

工作原理

微信连 wifi 协议是微信推出的开放式认证协议，用户通过使用微信即可快速的完成认证过程，而不需要输入用户名、密码等繁琐的过程。通过微信连 wifi 协议，可以实现广告常驻与微信等功能。微信连 wifi 的原理也类似 wifidog，但 token 的校验由微信服务器进行。

相关配置

↘ 开启 APP-AUTH 模块功能

APP-AUTH 功能需要全局开启。开启命令为:**app-auth enable, app-auth cwmp enable**

↘ 配置微信连 wifi 认证协议

缺省情况下无配置。

需要配置重定向方法为微信连 wifi。配置命令:**app-auth cfg-opt rdt-for-wx2**

配置重定向地址，配置命令: **app-auth ad-ur**l url

配置服务器地址，配置命令: **webservice server-ur**l url

18.3.3 本地认证

工作原理

网关自身作为认证服务器，根据用户的需求，推送不同的认证界面，完成不同的认证。

相关配置

↘ 开启本地认证功能

本地认证功能需要全局开启。开启命令为:**app-auth local-auth enable**

↘ 配置认证策略

缺省情况下无配置。

需要配置认证策略。配置命令: **app-auth policy**

配置特权用户组

缺省情况下无配置。

需要配置认证策略。配置命令: **app-auth local-auth vip-group**

配置用户

缺省情况下无配置。

需要配置认证策略。配置命令: **app-auth local-auth subs-name**

18.4 产品说明

NBR800G、NBR950G、NBR1000G-E、NBR6120-E、NBR2000G-C、NBR3000G-S、NBR1000G-C 不支持工厂 wifi 方案；NBR1500G、NBR2000G、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持工厂 wifi 方案。

NBR108G-P 不支持 app 认证，NBR800G、NBR950G 、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E 、 NBR2500D-E 、 NBR3000D-E 、 NBR3000D-UE 、 NBR1500G 、 NBR2000G 、 NBR1000G-C 、NBR2000G-C、NBR3000G-S、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 app 认证。

NBR800G、NBR950G、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持本地服务器认证，NBR108G-P、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1500G、NBR2000G 不支持本地服务器认证。

18.5 配置详解

配置项	配置建议 & 相关命令	
配置功能总开关功能	可选配置。全局功能开启	
	app-auth enable	全局开启 APP-AUTH 认证功能
	app-auth cwmp enable	开启与服务器联动功能
配置重定向方法	可选配置。根据协议选择不同的重定向方法	
	app-auth cfg-opt rdt-for-wifidog	配置重定向方法为 wifidog
	app-auth cfg-opt rdt-for-wx2	配置重定向方法为微信连 wifi
配置重定向地址	可选配置	
	app-auth ad-url	配置重定向页面的 portal 地址

配置免认证应用	⚠ 可选配置。免认证应用可以在用户未认证情况下直接访问外网	
	app-auth direct-app *app-name*	配置免认证应用
配置认证网段	⚠ 可选配置。开启 app 认证功能时，默认对所用所用进行进行处理。配置认证网段后，才有在认证网段内的用户才会进入 app 认证业务	
	app-auth auth-url ip start end	配置认证网段
配置内网免认证 IP 范围	⚠ 可选配置。在该范围内的 IP 可直接访问所有网络资源	
	app-auth direct-srcip *ip_start* **[** *ip_end* **]** **[aging-time** *time* **] [comment** *string* **]**	配置内网免认证 IP 范围
配置外网直通 IP 范围	⚠ 可选配置。认证通过前可直接外网 IP 范围的网络资源	
	app-auth direct-dstip *ip_start* **[** *ip_end* **]** **[aging-time** *time* **] [comment** *string* **]**	配置外网直通 IP 范围
配置 url 白名单	⚠ 可选配置。将该 url 对应的请求放行，支持通配方式	
	app-auth direct-url url	配置放行的 url
配置内网 mac 白名单	⚠ 可选配置。在 mac 白名单中终端无需认证即可访问网络	
	app-auth direct-mac mac **[aging-time** *time* **] [comment** *string* **]**	配置内网 mac 白名单
配置内网 mac 黑名单	⚠ 可选配置。在 mac 黑名单中终端无法访问网络	
	app-auth deny-mac mac **[aging-time** *time* **] [comment** *string* **]**	配置内网 mac 黑名单
配置流量监测下线	⚠ 可选配置。开启后，在 time 时间内流量小于 flow 则将用户下线	
	app-auth offline-detect [time-interval *time* **flowrate** *flow*]	配置流量监测下线
配置重定向私有信息	⚠ 可选配置。通常用于定制类客户中	
	app-auth priv-info info	配置重定向私有信息
配置网络类型	⚠ 可选配置。根据网络拓扑选择网络类型	
	app-auth cfg-opt [id-mac | id-ip]	开启网络类型
配置网段/SSID 信息	⚠ 可选配置。要求不同的 SSID 需要有不同的网段	
	app-auth set-ssid ssid-name **{ ip-range** ip-start ip-end**}**	配置网段和 SSID 信息
配置 tcp 长连接功能	⚠ 可选配置	

	app-auth tcp-socket [***enable*** **|** ***server*** *server-url* | ***keepalive*** *time_1* | ***user-inform*** *time_2*]	配置 tcp 长连接功能
删除在线用户	⚠ 删除在线用户	
	app-auth kick all	删除所有在线用户
	app-auth kick ip *ip-addr*	删除在线指定 ip 用户
配置本地认证总开关	⚠ 可选配置。	
	app-auth local-auth enable	配置总开关
配置本地认证用户	⚠ 可选配置。	
	app-auth local-auth subs-name *name* **type** { **ad** | **local** }	配置本地认证用户组
配置本地认证用户的终端信息	⚠ 可选配置。	
	mac *mac-address* { **auto** | **manual** } **type** { **pc** | **mobile** }	配置本地认证用户的终端信息
配置本地认证每用户可导入的终端上限	⚠ 可选配置。	
	app-auth local-auth subscirber mac-limit *limit-num*	配置本地认证每用户可导入的终端上限
配置本地认证用户账号自动绑定功能	⚠ 可选配置。	
	app-auth local-auth data-store enable	配置本地认证用户帐号自动绑定功能
配置本地认证用户数据库自动老化时间	⚠ 可选配置。	
	app-auth local-auth data-store age day *day*	配置本地认证用户数据库自动老化时间
配置认证服务器	⚠ 可选配置。	
	app-auth server *name* **type** { **act-directory** | **qrcode-alone** | **qrcode-authorize** | **sms** | **weixin** }	配置认证服务器
配置访问二维码的 ip 地址	⚠ 可选配置。	
	local-auth qrcode ip *ip-address*	配置访问二维码的 ip 地址
配置二维码的动态码	⚠ 可选配置。	
	local-auth qrcode key *key-str*	配置二维码的动态码
配置二维码的提示信息	⚠ 可选配置。	
	local-auth qrcode comment *comment-str*	配置二维码的提示信息

配置二维码授权相关参数	可选配置。	
	app-auth local-auth { **authorize** { **check** | **restrict-times** *times* } | **authorize-time** *minute* }	配置二维码授权相关参数
配置短信服务器相关参数	可选配置。	
	local-auth sms keyid *keyid-str* **keysecret** *keysecret-str* **sign** *sign-str* **templet** *templet-str*	配置短信服务器的各个参数
配置短信服务器类型	可选配置。	
	local-auth sms server { **aliyun-v1** | **aliyun-v2** }	配置短信服务器的类型
配置短信认证中的手机预先录入模式	可选配置。	
	local-auth sms mode prior	手机预先录入模式
配置微信认证相关参数	可选配置。	
	local-auth weixin shopid *shopid-str* **appid** *appid-str* **secretkey** *secretkey-str*	配置微信认证相关参数
配置认证服务器的 ssid	可选配置。	
	local-auth weixin ssid *ssid-str*	配置认证策略的 ssid
配置认证策略组	可选配置。	
	app-auth policy *name*	认证策略组
配置使能本认证策略	可选配置。	
	rule enable	配置使能本认证策略
配置认证策略的生效 ip 范围	可选配置。	
	rule ip-range { [*ip1* { *ip2* }] | **all** }	配置认证策略的生效 ip 范围
配置认证策略关联的认证服务器	可选配置。	
	relate server *server-name*	配置认证策略关联的认证服务器
配置认证策略的认证类型	可选配置。	
	rule type pwd	配置认证策略的认证类型
配置本地认证用户认证成功后的可用时长	可选配置。	
	app-auth local-auth online-time *time*	配置本地认证用户认证成功后的可用时长
配置限制终端类型上网	可选配置。	

	app-auth local-auth restrict { **pc** | **mobile** } [**exclude time-range** *time*]	配置限制终端类型上网

18.5.1 配置功能总开关功能

配置效果

- 全局启用 APP-AUTH 认证功能。开启此功能后，其他与 APP-AUTH 相关的配置才能生效。

注意事项

- 无

配置方法

- 功能开启时必须配置

检验方法

- 开启前用户可访问网络
- 开启后用户无法访问网络

相关命令

配置 APP-AUTH 功能

【命令格式】 **app-auth enable**
【参数说明】
【命令模式】 全局配置模式
【使用指导】

配置外置认证功能

【命令格式】 **app-auth cwmp enable**
【参数说明】 -
【命令模式】 全局配置模式
【使用指导】 与 **app-auth enable** 同时配置

配置举例

开启 APP-AUTH 功能

【配置方法】

- 在网关上开启 APP-AUTH 功能

```
Ruijie# configure terminal
Ruijie(config)# app-auth enable
Ruijie(config)# app-auth cwmp enable
```

【检验方法】

- show app-auth statistic 查看功能是否开启命令

```
Ruijie#show app-auth statistics
------------------------------start----------------------------------
app_auth_enable: on
cwmp_enable: on
cwmp_bak: off
non_http_pass: off
device_serialno: 1234942571228
basename: 401034050039
portal_key:
g_wan_ip: 0.0.0.0
priv_info: siteid=ruijie
time_limit: 0
server_status: 1
app_webs_sin_ip: 0.0.0.0
flow_detect status: on
        flow_detect time_interval: 60 (min)
        flow_detect flowrate: 0 (bit/s)
        flow_detect detect_limit: 120
advertising_url:
avoid app_name:
        新浪微博(1-6-1-0)
auth app_name:
        即时通讯(0-0-0-0)
auth_url:
        http://www.ruijie.com.cn

distri msg. up: 0, down: 0, inq: 0, attent:0
rcv_msg_num: 585, rcv_query_msg_num: 0
-----------------------------------end--------------------------------
```

app_auth_enable 和 cwmp enable 字段为 on 时表示功能开启

常见错误

- 无

18.5.2 配置重定向方法

配置效果

- 配置不同的重定向方法后，在重定向时会携带不同的参数

注意事项

- 无

配置方法

- 可选配置
- 依据选用的协议进行配置

检验方法

- 在 portal 页面上查看访问的 url 地址，不同配置携带的参数不同。

相关命令

配置认证方法为 wifidog

【命令格式】 **app-auth cfg-opt rdt-for-wifidog**
【参数说明】 -
【命令模式】 全局配置模式
【使用指导】 使用 wifidog 协议时配置

配置认证方法为微信连 wifi

【命令格式】 **app-auth cfg-opt rdt-for-wx2**
【参数说明】 -
【命令模式】 全局配置模式
【使用指导】 使用微信连 wifi 时配置

配置举例

配置重定向方法为 wifidog 协议

【配置方法】

```
Ruijie# configure terminal
Ruijie(config)# app-auth cfg-opt rdt-for-wifidog
```

【检验方法】 show app-auth cfg-opt 查看配置

常见配置错误

- 无

18.5.3 配置重定向地址

配置效果

- 用户认证前使用浏览器访问任意网站将被重定向到该地址

注意事项

- 与服务器约定好配置方式及重定向方法

配置方法

- 可选配置
- 根据服务器进行配置

检验方法

- 用户认证前使用浏览器访问任意网站将被重定向到该地址

相关命令

↘ 配置重定向地址

【命令格式】 **app-auth ad-url** *string*
【参数说明】 *string:重定向的 url*
【命令模式】 全局配置模式
【使用指导】 用户认证前使用广告 url 进行广告推送。url 配置时”http://”前缀可有可无。

配置举例

↘ 配置用户访问网页被重定向到 http://wmc.ruijieyun.com，并且重定向方法为 wifidog

【配置方法】

```
Ruijie# configure terminal
Ruijie(config)# app-auth ad-url http://wmc.ruijieyun.com
Ruijie(config)# app-auth cfg-opt rdt-for-wifidog
```

【检验方法】 用户使用浏览器访问 http://www.qq.com 被重定向到 http://wmc.ruijieyun.com.

常见配置错误

- 服务器未配置相对应的功能导致 portal 页面无法显示
- 服务器地址需要加入到免认证

18.5.4 配置免认证应用

配置效果

- 配置免认证应用后，用户在认证前可以直接使用该应用。

注意事项

- 配置的免认证应用必须是应用识别特征库中存在的。

配置方法

- 可选配置

检验方法

- show app-auth statistics 查看

相关命令

↘ 配置免认证应用

【命令格式】 **app-auth direct-app** app-name
【参数说明】 *app-name: 应用名称*
【命令模式】 全局配置模式
【使用指导】 可以基于应用直接放行

配置举例

设置新浪微博为免认证应用

【配置方法】
- 设置免认证应用

```
Ruijie (config)# app-auth direct-app 新浪微博
```

【检验方法】
- show app-auth statistics 查看免认证应用配置

```
------------------------------start---------------------------------
app_auth_enable: on
cwmp_enable: off
cwmp_bak: off
non_http_pass: off
device_serialno: 1234942571228
basename: 401034050039
portal_key:
g_wan_ip: 0.0.0.0
priv_info: siteid=ruijie
time_limit: 0
server_status: 1
app_webs_sin_ip: 0.0.0.0
flow_detect status: on
        flow_detect time_interval: 60 (min)
        flow_detect flowrate: 0 (bit/s)
        flow_detect detect_limit: 120
advertising_url:
avoid app_name:
        新浪微博(1-6-1-0)
auth app_name:
auth_url:
        http://www.ruijie.com.cn

distri msg. up: 0, down: 0, inq: 0, attent:0
rcv_msg_num: 2842, rcv_query_msg_num: 0
-----------------------------------end---------------------------------
```

常见配置错误

- 免认证应用名程在应用识别库中不存在

18.5.5 配置认证网段

配置效果

- 配置认证网段后，只有该认证网段内的用户才会进入 APP 认证业务进行处理

注意事项

- 无

配置方法

- 可选配置

检验方法

- 配置认证网段后，该网段内的用户需要进行认证，不在该网段内的用户则可以直接访问网络

相关命令

↘ 配置认证网段

【命令格式】 **app-auth auth-rule ip** *start end*

【参数说明】 *start*：起始 ip

end：结束 ip

【命令模式】 全局配置模式

【使用指导】 通常在同时开启 WEB 认证时使用

配置举例

↘ 设置 192.168.1.0/24 网段为认证网段

【配置方法】

- 设置认证网段

```
Ruijie (config)# app-auth auth-rule ip 192.168.1.1 192.168.1.255
```

【检验方法】

- show app-auth auth-rule 查看认证网段

```
Ruijie(config)#show app-auth auth-rule
auth-rule ip:
        192.168.10.2 - 192.168.10.100
```

- 该范围内的 IP 可直接访问网络资源

常见配置错误

- 无

18.5.6 配置内网免认证IP范围

配置效果

- 如果用户属于无需认证用户 IP 范围，那么该用户不需要经过认证，也能访问所有可达的网络资源。
- 缺省时，没有设置无需认证用户

注意事项

- 无

配置方法

- 可选配置
- 要设置无需认证用户时，可进行该配置。

检验方法

- 配置用户为无需认证用户
- 用户直接访问网络，访问成功

相关命令

↘ 设置无需认证用户 IP 范围

【命令格式】 **app-auth direct-srcip** *ip_start* **[** *ip_end* **] [aging-time** *time* **] [comment** *string* **]**

【参数说明】 *ip_start*：免认证用户 IP 起始地址

ip_end：免认证用户 IP 结束地址

time：该配置的老化时间

string：该配置的描述信息

【命令模式】 全局配置模式

【使用指导】

配置举例

↘ 设置无需认证用户 IP 范围

【配置方法】
- 设置无需认证用户 IP 范围

```
Ruijie (config)# app-auth direct-srcip 192.168.10.2 192.168.10.100
```

【检验方法】
- show app-auth direct-srcip 查看免认证 ip 范围

```
Ruijie(config)#show app-auth direct-srcip
direct src-ip:
        192.168.10.2 - 192.168.10.100
```

- 该范围内的 IP 可直接访问网络资源

常见配置错误

- 无

18.5.7 配置外网直通IP范围

配置效果

- 用户在认证通过前可以直接访问目的地址为外网 IP 范围的网络资源。

注意事项

- 无

配置方法

- 可选配置
- 认证通过前用户可访问部分 IP 地址时使用。

检验方法

- 未认证用户可访问目的 ip 为直通 IP 范围的网络资源。

相关命令

↘ 设置外网直通 IP 范围

【命令格式】 **app-auth direct-dstip** *ip_start* [*ip_end*] **[aging-time** *time* **] [comment** *string* **]**

【参数说明】 *ip_start*：直通 IP 起始地址

ip_end：直通 IP 结束地址

time：该配置的老化时间

string：该配置的描述信息

【命令模式】 全局配置模式

【使用指导】

配置举例

↘ 设置 www.baidu.com 的地址为直通 IP 地址

【配置方法】

- 通过 ping www.baidu.com 获取百度地址为 115.239.210.27

```
Ruijie (config)# app-auth direct-dstip 115.239.210.27
```

【检验方法】

- show app-auth direct-dstip 查看外网直通 IP

```
Ruijie(config)#show app-auth direct-dstip
direct dst-ip:
        115.239.210.27
```

-
- 未认证用户访问 http://115.239.210.27 可打开百度主页

常见配置错误

- 无

18.5.8 配置url白名单

配置效果

- 未认证用户可以直接 url 白名单的内的地址。

注意事项

- 支持通配方式，如配置放行 baidu.com，则访问 www.baidu.com 和 news.baidu.com 都会被放行
- 如果对该地址的访问是加密的，则需要依赖终端进行 dns 请求，因此白名单生效可能存在延迟。

配置方法

- 可选配置
-
- 检验方法

- 未认证用户可直接访 url 白名单

相关命令

设置外网直通 URL

【命令格式】 **app-auth direct-url** *url*
【参数说明】 *url:url 白名单*
【命令模式】 全局配置模式
【使用指导】

配置举例

设置 ruijie.com.cn 为 url 白名单

【配置方法】
- 设置 baidu.com 为 url 白名单

```
Ruijie (config)# app-auth direct-url ruijie.com.cn
```

【检验方法】
- show app-auth direct-url 查看 url 白名单

```
Ruijie(config)#show app-auth direct-url
direct url:
        ruijie.com.cn
```

- 未认证用户可以访问 ruijie.com.cn

常见配置错误

- 无

18.5.9 配置内网mac白名单

配置效果

- mac 白名单用户无需认证即可访问网络

注意事项

- 在二层网络情况下生效

配置方法

- 可选配置

- 需要对部分终端免认证时配置

检验方法

- 配置终端为 mac 白名单，该终端无需认证就可访问网络

相关命令

↘ 设置 mac 白名单

【命令格式】 **app-auth direct-mac** *mac-address* **[aging-time** *time* **] [comment** *string* **]**

【参数说明】 *mac-address: mac 地址*

time：该配置的老化时间

string：该配置的描述信息

【命令模式】 全局配置模式

【使用指导】

配置举例

↘ 设置内网 mac 白名单

【配置方法】

- 设置 Mac 78f5.df63.b014 为白名单 mac

```
Ruijie (config)# app-auth direct-mac 78f5.df63.b014
```

【检验方法】

- show app-auth direct-mac 查看白名单 mac

```
Ruijie#show app-auth direct-mac
app-auth direct-mac num: 1
        mac: 78f5.df63.b014, flag: 0
```

- 使用该 Mac 的终端无需认证就可以访问网络

18.5.10 配置内网mac黑名单

配置效果

- mac 黑名单用户无法访问网络，也无法进行认证

注意事项

- 在二层网络情况下生效

配置方法

- 可选配置
- 需要禁止部分终端访问网络时使用

检验方法

- 配置终端为 mac 黑名单，该终端无法访问网络

相关命令

↘ 设置 mac 黑名单

【命令格式】 **app-auth deny-mac** *mac-address* **[aging-time** *time* **] [comment** *string* **]**

【参数说明】 *mac-address: mac 地址*

time：该配置的老化时间

string：该配置的描述信息

【命令模式】 全局配置模式

【使用指导】

配置举例

↘ 设置内网 mac 黑名单

【配置方法】

- 设置 Mac d014.df63.b014 为黑名单 mac

```
Ruijie (config)# app-auth deny-mac d014.df63.b014
```

【检验方法】

- show app-auth deny-mac 查看黑名单 mac

```
Ruijie(config)#show app-auth deny-mac
app-auth deny-mac num: 1
        mac: d014.df63.b014, flag: 1
```

- 使用该 Mac 的终端无法进行认证，也无法访问网络

18.5.11 配置流量监测下线

配置效果

- 用户在一定时间内产生的流量小于设定值自动下线

注意事项

- 需要小于 dhcp 周期的一半。

配置方法

- 可选配置
- 需要开启流量监测下线用于回收用户 IP 地址场景中使用

检验方法

- 用户在一定时间内产生的流量小于设定值自动下线

相关命令

↘ 设置无流量监测下线

【命令格式】 **app-auth offline-detect [time-interval** *time* **flowrate** *flow]*

【参数说明】 *time:监测时间，单位分钟。配置范围 1~65535，不配置默认为 15*

flow:流量小于 flow 值时下线，单位 bps,不配置默认为 0

【命令模式】 全局配置模式

【使用指导】

配置举例

- 无

常见配置错误

- 无

18.5.12 配置重定向私有信息

配置效果

- 配置了重定向私有信息后，在重定向 url 中会携带该信息

注意事项

- 该功能提供了客户在重定向中携带额外信息的功能，通常是在客户有某些特殊要求时使用。因此通常在客户定制场景中使用。

配置方法

- 可选配置

检验方法

- 无

相关命令

↘ 配置重定向私有信息

【命令格式】 **app-auth priv-info** info
【参数说明】
【命令模式】 全局配置模式
【使用指导】 需要与客户约定携带的私有信息内容

配置举例

- 无

常见配置错误

- 无

18.5.13 配置网络类型

配置效果

- 根据网络拓扑是二层还是三层网络进行配置。选择二层网络时，设备上将使用 Mac 唯一标示一个终端;使用三层网络时，设备上使用 IP 唯一标示终端。

注意事项

- 根据网络拓扑选择正确的网络类型。未知网络类型时可以选择三层网络。
- 在变更网络类型后需要执行 app-auth kick all 删除所有用户， 所有用户都需要重新认证

配置方法

- 可选配置

检验方法

- show app-auth cfg-opt

相关命令

配置二层网络类型

【命令格式】 **app-auth cfg-opt id-mac**
【参数说明】
【命令模式】 全局配置模式
【使用指导】 网络拓扑必须为二层时使用

配置三层网络类型

【命令格式】 **app-auth cfg-opt id-ip**
【参数说明】
【命令模式】 全局配置模式
【使用指导】 网络拓扑为二层或者三层时都可以使用

配置举例

- 无

常见配置错误

- 变更网络类型后未将已存在的用户删除。

18.5.14 配置网段/SSID信息

配置效果

- 配置该命令后，网段会匹配用户的 IP 地址，如果匹配中，网关在重定向时会携带该 SSID 信息。

注意事项

- 确认服务器需要且支持 ssid 参数情况下使用。
- 支持配置一个全局 ssid

配置方法

- 可选配置

检验方法

- show app-auth ssid-cfg

相关命令

↘ 配置网段/SSID

【命令格式】 **app-auth set-ssid** ssid-name **{ ip-range** ip-start ip-end**}**

【参数说明】 ssid-name: ssid 名称

ip-start: 起始 ip 地址

ip-end：终止 ip 地址

【命令模式】 全局配置模式

【使用指导】 1、 如未配置网段，则配置为全局 ssid。

2、 网段对应的 ssid 高于全局 ssid。

配置举例

- 无

常见配置错误

- ssid 配置名称与实际不同（如 AC 上配置的真实 ssid）。

18.5.15 配置tcp长连接功能

配置效果

- 网关和服务器保持一个 tcp 长连接，该长连接可提供用户同步，用户上线/下线通告功能。

注意事项

- 确认服务器支持情况下开启，通常用于认证计费场景中。

配置方法

- 可选配置

检验方法

- show app-auth tcp-info 查看

相关命令

↘ 配置 tcp 长连接功能

【命令格式】 **app-auth tcp-socket** *[**enable** | **server** server-url | **keepalive** time_1 | **user-inform** time_2]*

【参数说明】 enable: 开启 tcp 长连接功能

server-url : 服务器地址

time_1: 控制 tcp 保活周期，默认 30 秒。

time_2: 控制用户同步周期，默认 5 分钟。

【命令模式】 全局配置模式

【使用指导】 服务器支持情况下才可配置，通常用于认证计费场景中。

配置举例

- 无

常见配置错误

- 无

18.5.16 删除在线用户

配置效果

- 已上线用户被删除后无法继续访问网络

注意事项

- 无

配置方法

- 可选配置

检验方法

- 无

相关命令

↘ 删除所有在线用户

【命令格式】 **app-auth kick all**
【参数说明】
【命令模式】 特权模式
【使用指导】

↘ 删除在线指定 ip 用户

【命令格式】 **app-auth kick ip** *ip-addr*
【参数说明】 ip-addr:在线 ip 地址
【命令模式】 特权模式
【使用指导】

配置举例

- 无

常见配置错误

- 无

18.5.17 配置HTTPS重定向

配置效果

- 配置后，可以对 HTTPS 流量进行重定向。

注意事项

- -

配置方法

- 可选配置

检验方法

- show app-auth proxy-option config 查看

相关命令

↘ 配置 https 重定向

【命令格式】 **app-auth proxy-option** [**https | session total** *total-num* **per-ip** *per-ip-num*]

【参数说明】 **session total** *total-num*：整机 https 会话数限制

per-ip *per-ip-num*：每 ip https 会话数限制

https：开启 https 重定向

【命令模式】 全局配置模式

【使用指导】 开启认证后对非在线用户生效

18.5.18 配置本地认证总开关

配置效果

- 开启后启用本地认证模式

注意事项

- 只能用于本地认证

配置方法

- 可选配置

检验方法

- show app-auth local-auth config 查看

相关命令

↘ 配置开启本地认证

【命令格式】 app-auth local-auth enable
【参数说明】 enable: 开启本地认证
【命令模式】 全局配置模式
【使用指导】 在本地认证场景中使用

配置举例

↘ 开启本地认证功能

【配置方法】
- 在网关上开启本地认证功能

```
Ruijie# configure terminal
Ruijie(config)# app-auth local-auth enable
```

【检验方法】
- 使用 show app-auth local-auth config 查看功能是否开启命令

```
Ruijie#show app-auth local-auth config
app-auth local-auth enable
```

常见错误

- 无

18.5.19 配置本地认证用户

配置效果

- 配置本地认证的用户信息。

注意事项

- 只能用于本地认证

配置方法

- 可选配置

检验方法

- show app-auth local-auth subs 查看

相关命令

配置本地认证用户

【命令格式】 app-auth local-auth subs-name *name* type local

【参数说明】 *name*: 用户名称

local: 本地用户

【命令模式】 全局配置模式

【使用指导】 该用户只对 loacl-auth 生效

配置举例

配置本地认证用户

【配置方法】

- 在网关上配置本地认证的 abc 用户

```
Ruijie# configure terminal
Ruijie(config)# app-auth local-auth subs-name abc
```

【检验方法】

- show app-auth local-auth subs all 查看本地认证用户信息

```
Ruijie#  show app-auth local-auth subs all
subs_cnt:1/1200, mac_cnt: 1/2500
-------------------------------------------------------------------------------------------------
Name                                                                    Mac_num Type        source
Mode
            Mac                    Auto/Manual terminal    time
-------------------------------------------------------------------------------------------------
abc                                                                     1           ad          ad
manual
 |---- 0011.2233.4455    manual          pc              2018-5-18 16:42:13
```

常见错误

- 和用户管理模块的用户独立使用，两个不影响。

18.5.20 配置本地认证用户的终端信息

配置效果

- 配置本地认证用户的终端信息。

注意事项

- 只能用于本地认证

配置方法

- 可选配置

检验方法

- show app-auth local-auth subs 查看

相关命令

配置本地认证用户的终端信息

【命令格式】 mac mac-address { auto | manual } type { pc | mobile }

【参数说明】 mac: 该终端的 mac 地址

mac-address: mac 地址格式为 xxxx.xxxx.xxxx

auto: 配置终端为自动导入

manual: 配置终端为手工配置

pc：配置该终端为 pc

mobile：配置该终端为移动设备

【命令模式】 app-auth 的用户配置模式

【使用指导】 该配置只对本地认证生效；

一个用户可以配置多个终端信息；

配置举例

配置本地认证用户

【配置方法】

- 在网关上配置本地认证的 abc，且其为 pc 用户，它的 mac 为 0011.2233.4455

```
Ruijie# configure terminal
Ruijie(config)# app-auth local-auth subs-name abc
Ruijie(config)# mac 0011.2233.4455 manual type pc
```

【检验方法】

- show app-auth local-auth subs all 查看本地认证用户信息

```
Ruijie# show app-auth local-auth subs all

subs_cnt:1/1200, mac_cnt: 1/2500
```

```
-----------------------------------------------------------------------------------------------------
Name                                                                                  Mac_num Type        source
Mode
            Mac                    Auto/Manual terminal    time
-----------------------------------------------------------------------------------------------------
abc                                                                                   1           ad          ad
manual
 |---- 0011.2233.4455    manual          pc              2018-5-18 16:42:13
```

常见错误

- 和用户管理模块的用户独立使用，两个用户为独立不影响。

18.5.21 配置特权用户

配置效果

- 特权用户在授权管控开启时具有对其他用户进行授权上网的权限。

注意事项

- 只能用于本地认证

配置方法

- 可选配置

检验方法

- show app-auth local-auth vip-group all 查看

相关命令

↘ 配置本地认证用户为特权用户

【命令格式】 app-auth local-auth vip-group user-name local

【参数说明】 vip-group: 特权组

user-name: 需要加入特权组的用户

local: 本地用户

【命令模式】 全局配置模式

【使用指导】 无

配置举例

↘ 配置本地用户为特权用户

【配置方法】

- 将用户 aaa 配置为特权用户

```
Ruijie# configure terminal
Ruijie(config)# app-auth local-auth vip-group aaa local
```

【检验方法】

- show app-auth local-auth vip-group all 可以查看到对应配置

```
Ruijie#  show app-auth local-auth vip-group all
cnt: 1/100. ad_any_vip: 0
Group-name                                                          type          idx
------------------------------------------------------------------------------
aaa                                                                 local         0
```

常见错误

- 无

18.5.22 配置本地认证每用户可导入的终端上限

配置效果

- 配置本地认证每用户可导入的终端上限。

注意事项

- 只能用于本地认证

配置方法

- 可选配置

检验方法

- show app-auth local-auth config 查看

相关命令

↘ 配置本地认证每用户可导入的终端上限

【命令格式】 app-auth local-auth subscirber mac-limit limit-num

【参数说明】 limit-num：上限个数，默认为 0，0 表示不限制

【命令模式】 全局配置模式

【使用指导】 为了网络异常导致自动生成的用户过多，所以需要限制没用户可导入的终端上限

配置举例

↘ 配置本地认证每用户可导入的终端上限

【配置方法】

- 在网关上配置本地认证每用户可导入的终端上限个数为 5

```
Ruijie# configure terminal
Ruijie(config)# app-auth local-auth subscirber mac-limit 5
```

【检验方法】

- show app-auth local-auth config 中的 user-mac-limit 可以查看到对应配置

```
Ruijie#show app-auth local-auth config
enable: False
data-store-enable: False
data-store-age-day: 60
user-mac-limit: 2
online-time: 0
authorize-time: 0
restrict-range information:
  mobile:
    global: false
    name:
    state:   Idle
  pc:
    global: false
    name:
    state:   Idle
```

常见错误

- 和用户管理模块的用户独立使用，两个用户为独立不影响。

18.5.23 配置本地认证用户账号自动绑定功能

配置效果

- 配置本地认证用户帐号自动绑定功能

注意事项

- 只能用于本地认证

配置方法

- 可选配置

检验方法

- show app-auth local-auth config 查看

相关命令

↘ 配置本地认证账号自动绑定

【命令格式】 app-auth local-auth data-store enable

【参数说明】 enable: 开启本功能

【命令模式】 全局配置模式

【使用指导】 用户认证成功之后，用户信息存储到数据库中。

配置举例

↘ 配置本地认证账号自动绑定

【配置方法】

- 在网关上开启用户帐号自动绑定功能

```
Ruijie# configure terminal
Ruijie(config)# app-auth local-auth data-store enable
```

【检验方法】

- show app-auth local-auth config 查看本地认证配置信息，其中 data-store-enable 项代表本配置。

```
Ruijie#show app-auth local-auth config
enable: False
data-store-enable: True
data-store-age-day: 60
```

```
user-mac-limit: 2
online-time: 0
authorize-time: 0
restrict-range information:
  mobile:
    global: false
    name:
    state:   Idle
  pc:
    global: false
    name:
    state:   Idle
```

常见错误

- 无

18.5.24 配置本地认证用户数据库自动老化时间

配置效果

- 配置本地认证用户数据库自动老化时间。

注意事项

- 只能用于本地认证

配置方法

- 可选配置

检验方法

- show app-auth local-auth config 查看

相关命令

↘ 配置本地认证用户数据库自动老化时间

【命令格式】 app-auth local-auth data-store age day day

【参数说明】 day: 老化周期

【命令模式】 全局配置模式

【使用指导】 用于用户数据库中的用户自动老化，过了老化周期后，用户数据库中存储的数据删除。

配置举例

↘ 配置认证用户数据库用户老化时间

【配置方法】

- 在网关上配置本地认证用户老化周期为 5 天

```
Ruijie# configure terminal
Ruijie(config)# app-auth local-auth data-store age day 5
```

【检验方法】

- show app-auth local-auth config 查看本地认证配置信息，其中 data-store-age-day 表示本配置

```
Ruijie#show app-auth local-auth config
enable: False
data-store-enable: True
data-store-age-day: 5
user-mac-limit: 2
online-time: 0
authorize-time: 0
restrict-range information:
  mobile:
    global: false
    name:
    state:   Idle
  pc:
    global: false
    name:
    state:   Idle
```

常见错误

- 无

18.5.25 配置认证服务器

配置效果

- 配置认证服务器。

注意事项

- 无

配置方法

- 可选配置

检验方法

- show app-auth policy 查看

相关命令

配置认证服务器

【命令格式】 app-auth server name type { qrcode-alone | qrcode-authorize | sms | weixin }

【参数说明】 name: 服务器名称

qrcode-alone: 自助扫码认证

qrcode-authorize: 授权扫码认证

sms: 短信认证

weixin: 微信认证

【命令模式】 全局配置模式

【使用指导】 用于配置认证策略。

配置举例

配置认证服务器

【配置方法】

- 在网关上配置认证服务器 abc，且其的认证方式为自助扫码认证

```
Ruijie# configure terminal
Ruijie(config)# app-auth server abc type qrcode-alone
```

【检验方法】

- show app-auth policy 查看认证服务器

```
Ruijie# show app-auth server all
server name: abc
type: qrcode-alone
    mode: alone
    comment: 欢迎 您上网！
    ip: 2.2.2.2
```

```
key: 1
```

常见错误

- 无

18.5.26 配置访问二维码的ip地址

配置效果

- 用户可以通过该 ip 访问二维码

注意事项

- 无

配置方法

- 可选配置

检验方法

- show app-auth server all 查看

相关命令

↘ 配置访问二维码的 ip 地址

【命令格式】 local-auth qrcode ip ip-address

【参数说明】 ip: 可以使用该 ip 访问二维码

ip-address: ip 地址

【命令模式】 认证服务器模式(config-app-auth-server)，需要在服务器类型为自助扫码(qrcode-alone)下才可以配置本命令

【使用指导】 用于配置访问二维码的 ip 地址。

配置举例

↘ 配置二维码认证

【配置方法】

- 在网关上配置认证服务器 qralone，认证方式为“自助扫码认证”，访问二维码的 ip 地址为 1.2.3.4

```
Ruijie# configure terminal
```

```
Ruijie(config)# app-auth server qralone type qrcode-alone
Ruijie(config-app-auth-server)# local-auth act-directory source-ip 1.2.3.4
```

【检验方法】

- show app-auth server all 查看认证服务器

```
Ruijie# show app-auth server all
server name: qralone
type: qrcode-alone
    mode: alone
    comment: zizhu
    ip: 1.2.3.4
    key: test
```

常见错误

- 无

18.5.27 配置二维码的动态码

配置效果

- 用户配置该二维码的动态码，该动态码用于识别二维码是否有效。

注意事项

- 无

配置方法

- 可选配置

检验方法

- show app-auth server all 查看

相关命令

↘ 配置二维码认证的动态码

【命令格式】 local-auth qrcode key key-str

【参数说明】 key：动态码

key-str：动态码字符串

【命令模式】 认证服务器模式(config-app-auth-server)，需要在服务器类型为自助扫码(qrcode-alone)下才可以配置本命令

【使用指导】 用于配置二维码的动态码。

配置举例

↘ 配置二维码认证

【配置方法】

- 在网关上配置认证服务器 qralone，认证方式为“自助扫码认证”，其动态码为“test”

```
Ruijie# configure terminal
Ruijie(config)# app-auth server qralone type qrcode-alone
Ruijie(config-app-auth-server)#  local-auth qrcode key test
```

【检验方法】

- show app-auth server all 查看认证服务器

```
Ruijie# show app-auth server all
server name: qralone
type: qrcode-alone
    mode: alone
    comment: zizhu
    ip: 1.2.3.4
    key: test
```

常见错误

- 无

18.5.28 配置二维码的提示信息

配置效果

- 用户配置该二维码的提示信息。用于提示外宾上网操作。

注意事项

- 无

配置方法

- 可选配置

检验方法

- show app-auth server all 查看

相关命令

配置二维码认证提示信息

【命令格式】 local-auth qrcode comment comment-str

【参数说明】 comment: 提示信息

comment-str: 提示信息字符串

【命令模式】 认证服务器模式(config-app-auth-server)，需要在服务器类型为二维码类(qrcode)下才可以配置本命令

【使用指导】 用于配置二维码的提示信息。

配置举例

配置二维码认证

【配置方法】

- 在网关上配置认证服务器 qralone，认证方式为“自助扫码认证”，其动态码为“test”

```
Ruijie# configure terminal
Ruijie(config)# app-auth server qralone type qrcode-alone
Ruijie(config-app-auth-server)# local-auth qrcode comment zizhu
```

【检验方法】

- show app-auth server all 查看认证服务器

```
Ruijie# show app-auth server all
server name: qralone
type: qrcode-alone
    mode: alone
    comment: zizhu
    ip: 1.2.3.4
    key: test
```

常见错误

- 无

18.5.29 配置二维码授权相关参数

配置效果

- 配置二维码授权相关参数

注意事项

- 无

配置方法

- 可选配置

检验方法

- show app-auth local-auth config 查看

相关命令

↘ 配置二维码授权认证相关参数

【命令格式】 app-auth local-auth { authorize { check | restrict-times times } | authorize-time minute }

【参数说明】 check：授权功能是否开启

restrict-times: 获取被授权上网用户再进行授权的次数限制

times: 具体的次数

authorize-time: 用户授权后可以上网的时长

minute: 授权认证后的可用时长

【命令模式】 全局配置模式

【使用指导】 无

配置举例

↘ 配置二维码授权认证相关参数

【配置方法】

- 在网关上配置开启二维码授权认证，且认证后可以使用的时长为 60 分钟，被授权用户可再次授权的用户次数为 3 次

```
Ruijie# configure terminal
Ruijie(config)# app-auth local-auth authorize check
Ruijie(config)# app-auth local-auth authorize restrict-times 3
Ruijie(config)# app-auth local-auth authorize-time 60
```

【检验方法】
- show app-auth local-auth config 查看本地认证配置

```
Ruijie#show app-auth local-auth config
enable: True
data-store-enable: True
data-store-age-day: 36
user-mac-limit: 2
online-time: 0
authorize-time: 60
restrict-range information:
  mobile:
    global: false
    name:
    state:   Idle
  pc:
    global: false
    name:
    state:   Idle
```

常见错误

- 无

18.5.30 配置短信服务器相关参数

配置效果

- 配置短信服务器的各个参数。

注意事项

- 无

配置方法

- 可选配置

检验方法

- show app-auth server all 查看

相关命令

配置短信认证参数

【命令格式】 local-auth sms keyid keyid-str keysecret keysecret-str sign sign-str templet templet-str

【参数说明】 Keyid:短信服务器验证的 appkey

Keyid-str: 具体的 appkey

Keysecret: 短信验证的 secret-key

Keysecret-str: Keysecret 具体的字符串

Sign：短信签名

Sign-str：短信签名字符串

Templet：短信模板

Templet-str：短信模板字符串

【命令模式】 认证服务器模式(config-app-auth-server)，需要在服务器类型为短信(sms)下才可以配置本命令

【使用指导】 用于配置短信服务器参数

配置举例

配置短信认证

【配置方法】

- 在网关上配置认证服务器 sms，认证方式为“短信”

```
Ruijie# configure terminal
Ruijie(config)# app-auth server sms-auth type sms
Ruijie(config-app-auth-server)# local-auth sms keyid aaabbb keysecret cccddd sign eeefff templet
ggghhh
```

【检验方法】

- show app-auth server all 查看认证服务器

```
Ruijie# show app-auth server all
server name: sms-auth
type: sms
    mode: 1
    server: aliyun-v1
    keyid: aaabbb
    keysecret: cccddd
    sign: eeefff
    templet: ggghhh
```

常见错误

- 无

18.5.31 配置短信服务器类型

配置效果

- 配置短信服务器的类型。

注意事项

- 无

配置方法

- 可选配置

检验方法

- show app-auth server all 查看

相关命令

↘ 配置短信服务器

【命令格式】 local-auth sms server { aliyun-v1 | aliyun-v2 }

【参数说明】 server: 短信服务器类型

aliyun-v1:阿里云短信 v1

aliyun-v2:阿里云短信 v2

【命令模式】 认证服务器模式(config-app-auth-server)，需要在服务器类型为短信(sms)下才可以配置本命令

【使用指导】 用于配置短信服务器类型

配置举例

↘ 配置短信认证

【配置方法】

- 在网关上配置认证服务器 sms，认证方式为“短信”，服务器类型为阿里云短信 v1

```
Ruijie# configure terminal
Ruijie(config)# app-auth server sms-auth type sms
Ruijie(config-app-auth-server)# local-auth sms server aliyun-v1
```

【检验方法】
- show app-auth server all 查看认证服务器

```
Ruijie# show app-auth server all
server name: sms-auth
type: sms
    mode: 1
    server: aliyun-v1
    keyid: aaabbb
    keysecret: cccddd
    sign: eeefff
    templet: ggghhh
```

常见错误

- 无

18.5.32 配置短信认证中的手机预先录入模式

配置效果

- 配置手机预先录入模式。

注意事项

- 无

配置方法

- 可选配置

检验方法

- show app-auth server all 查看

相关命令

↘ 配置预先录入模式

【命令格式】 local-auth sms mode prior

【参数说明】 mode：短信模式

prior：预先录入模式

【命令模式】 认证服务器模式(config-app-auth-server)，需要在服务器类型为短信(sms)下才可以配置本命令

【使用指导】 用于配置短信认证为预先录入模式

配置举例

↘ 配置短信认证

【配置方法】

- 在网关上配置认证服务器 sms，认证方式为“短信”，模式为预先录入模式

```
Ruijie# configure terminal
Ruijie(config)# app-auth server sms-auth type sms
Ruijie(config-app-auth-server)# local-auth sms mode prior
```

【检验方法】

- show app-auth server all 查看认证服务器

```
Ruijie# show app-auth server all
server name: sms-auth
type: sms
    mode: 1
    server: aliyun-v1
    keyid: aaabbb
    keysecret: cccddd
    sign: eeefff
    templet: ggghhh
```

常见错误

- 无

18.5.33 配置微信认证相关参数

配置效果

- 配置微信认证相关参数。

注意事项

- 无

配置方法

- 可选配置

检验方法

- show app-auth server all 查看

相关命令

配置微信认证参数

【命令格式】 local-auth weixin shopid shopid-str appid appid-str secretkey secretkey-str

【参数说明】 Shopid：门店 id

Shopid：门店 id 字符串

appid：微信公众平台账号

appid-str：appid 字符串

secretkey：签名密钥

secretkey-str：secretkey 字符串

【命令模式】 认证服务器模式(config-app-auth-server)，需要在服务器类型为微信(weixin)下才可以配置本命令

【使用指导】 用于配置微信认证相关参数

配置举例

配置微信认证

【配置方法】

- 在网关上配置认证服务器 wechat，认证方式为“微信”

```
Ruijie# configure terminal
Ruijie(config)# app-auth server wechat type weixin
Ruijie(config-app-auth-server)# local-auth weixin shopid 111 appid bbb secretkey ccc
```

【检验方法】

- show app-auth server all 查看认证服务器

```
Ruijie# show app-auth server all
server name: wechat
type: weixin
    decrypt-flag: 0
    shopid: 111
    appid: bbb
    secretkey: ccc
    ssid: ssid_test
```

常见错误

- 无

18.5.34 配置认证服务器的ssid

配置效果

- 配置认证策略的 ssid

注意事项

- 无

配置方法

- 可选配置

检验方法

- show app-auth policy 查看

相关命令

↘ 配置认证服务器关联的 ssid

【命令格式】 local-auth weixin ssid ssid-str

【参数说明】 ssid: 该服务器对应的 ssid

ssid-str: ssid 字符串

【命令模式】 认证服务器模式(config-app-auth-server)，需要在服务器类型为微信(weixin)下才可以配置本命令

【使用指导】 用于配置认证服务器的 ssid

配置举例

↘ 配置认证策略的 ssid

【配置方法】

- 在网关上配置认证服务器 wechat，且其类型为 weixin，ssid 为 ssid_test

```
Ruijie# configure terminal
Ruijie(config)# app-auth server wechat type weixin
Ruijie(config-app-auth-server)# local-auth weixin ssid ssid_test
```

【检验方法】

- show app-auth server all 查看认证服务器

```
Ruijie#  show app-auth server all
server name: wechat
type: weixin
      decrypt-flag: 0
      shopid: 111
      appid: bbb
      secretkey: ccc
      ssid: ssid_test
```

常见错误

- 无

18.5.35 配置认证策略组

配置效果

- 配置认证策略组。

注意事项

- 无

配置方法

- 可选配置

检验方法

- show app-auth policy all 查看

相关命令

↘ 配置认证策略组

【命令格式】 app-auth policy name

【参数说明】 policy: 配置认证策略

name：策略名

【命令模式】 全局配置模式

【使用指导】 用于配置认证策略。

配置举例

配置认证策略组

【配置方法】

- 在网关上配置认证策略 aaa

```
Ruijie# configure terminal
Ruijie(config)# app-auth policy aaa
```

【检验方法】

- show app-auth policy 查看认证策略

```
Ruijie#show app-auth policy all
Global information:
policy_cnt : 1
Global Ip-range
001. 0.0.0.0 ~ 255.255.255.255

Detail:
Policy aaa
   enable: True
   pid: 2
   mode: pwd
   state: 0
   ip-range number: 1
   cfile-path: plcy2.php
   sms: 1
   weixin: 1
ip-range info:
      1. ALL
   server number 2:
      1. name:adf       type: sms
      2. name:wechat       type: weixin
```

常见错误

- 无

18.5.36 配置使能认证策略

配置效果

- 配置使能本认证策略

注意事项

- 无

配置方法

- 可选配置

检验方法

- show app-auth policy all 查看

相关命令

↘ 配置使能认证策略

【命令格式】 rule enable
【参数说明】 enable: 使能本策略
【命令模式】 app-auth 的策略组配置模式
【使用指导】 用于使能认证策略，只能在 app-auth 的策略组模式下使用

配置举例

↘ 配置使能认证策略

【配置方法】
- 在网关上配置认证策略 abc，并使其生效

```
Ruijie# configure terminal
Ruijie(config)# app-auth policy aaa
Ruijie(app-auth-policy)# rule enable
```

【检验方法】
- show app-auth policy all 查看认证策略

```
Ruijie#show app-auth policy all

Global information:
```

```
policy_cnt : 1
Global Ip-range
001. 0.0.0.0 ~ 255.255.255.255

Detail:
Policy aaa
   enable: True
   pid: 2
   mode: pwd
   state: 0
   ip-range number: 1
   cfile-path: plcy2.php
   sms: 1
   weixin: 1
ip-range info:
      1. ALL
   server number 2:
      1. name:adf       type: sms
      2. name:wechat       type: weixin
```

常见错误

- 只能在 app-auth 的策略组模式下使用

18.5.37 配置认证策略生效的ip范围

配置效果

- 配置认证策略的生效 ip 范围

注意事项

- 无

配置方法

- 可选配置

检验方法

- show app-auth policy all 查看

相关命令

↘ 配置认证策略生效的 ip 范围

【命令格式】 rule ip-range { [ip1 { ip2 }] | all }

【参数说明】 ip1: 生效的起始 ip

ip2: 生效的终止 ip

all: 对所有 ip 生效

【命令模式】 app-auth 的策略组配置模式

【使用指导】 用于配置策略生效的 ip 范围，只能在 app-auth 的策略组模式下使用

配置举例

↘ 配置认证策略的生效 ip 范围

【配置方法】

- 在网关上配置认证策略 aaa，并使其对所有 ip 生效

```
Ruijie# configure terminal
Ruijie(config)# app-auth policy aaa
Ruijie(app-auth-policy)# rule ip-range all
```

【检验方法】

- show app-auth policy all 查看认证策略

```
Ruijie#show app-auth policy all

Global information:

policy_cnt : 1

Global Ip-range

001. 0.0.0.0 ~ 255.255.255.255


Detail:

Policy aaa

  enable: True
```

```
  pid: 2
  mode: pwd
  state: 0
  ip-range number: 1
  cfile-path: plcy2.php
  sms: 1
  weixin: 1
ip-range info:
    1. ALL
  server number 2:
    1. name:adf       type: sms
    2. name:wechat       type: weixin
```

常见错误

- 只能在 app-auth 的策略组模式下使用

18.5.38 配置认证策略关联的认证服务器

配置效果

- 配置认证策略关联的认证服务器

注意事项

- 无

配置方法

- 可选配置

检验方法

- show app-auth policy all 查看

相关命令

配置认证策略关联的认证服务器

【命令格式】 relate server server-name

【参数说明】 Server：关联的认证服务器

Server-name：认证服务器名

【命令模式】 app-auth 的策略组配置模式

【使用指导】 只能在 app-auth 的策略组模式下使用

配置举例

配置认证策略关联的认证服务器

【配置方法】

- 在网关上配置认证策略 aaa，并使关联认证服务器 wechat

```
Ruijie# configure terminal
Ruijie(config)# app-auth policy aaa
Ruijie(app-auth-policy)# relate server wechat
```

【检验方法】

- show app-auth policy all 查看认证策略

```
Ruijie#show app-auth policy all

Global information:

policy_cnt : 1

Global Ip-range

001. 0.0.0.0 ~ 255.255.255.255


Detail:

Policy aaa
   enable: True
   pid: 2
   mode: pwd
   state: 0
   ip-range number: 1
   cfile-path: plcy2.php
   sms: 1
   weixin: 1
ip-range info:
      1. ALL
```

```
server number 1:
  1. name:wechat      type: weixin
```

常见错误

- 只能在 app-auth 的策略组模式下使用

18.5.39 配置认证策略关联的认证类型

配置效果

- 配置认证策略的认证类型

注意事项

- 无

配置方法

- 可选配置

检验方法

- show app-auth policy all 查看

相关命令

↘ 配置认证策略的认证类型

【命令格式】 rule type pwd
【参数说明】 pwd： 帐号密码认证
【命令模式】 app-auth 的策略组配置模式
【使用指导】 只能在 app-auth 的策略组模式下使用

配置举例

↘ 配置认证策略的认证类型

【配置方法】
- 在网关上配置认证策略 aaa，并使关联认证服务器 wechat

```
Ruijie# configure terminal
```

```
Ruijie(config)# app-auth policy aaa
Ruijie(app-auth-policy)# rule type pwd
```

【检验方法】

- show app-auth policy all 查看认证策略

```
Ruijie#show app-auth policy all
Global information:
policy_cnt : 1
Global Ip-range
001. 0.0.0.0 ~ 255.255.255.255

Detail:
Policy aaa
  enable: True
  pid: 2
  mode: pwd
  state: 0
  ip-range number: 1
  cfile-path: plcy2.php
  sms: 1
  weixin: 1
ip-range info:
    1. ALL
  server number 1:
    1. name:wechat      type: weixin
```

常见错误

- 只能在 app-auth 的策略组模式下使用

18.5.40 配置本地认证的用户认证成功后的可用时长

配置效果

- 非授权类的用户认证成功后，使用该时长上网

注意事项

- 无

配置方法

- 可选配置

检验方法

- show app-auth local-auth config 查看

相关命令

↘ 配置本地认证用户认证成功后的可用时长

【命令格式】 app-auth local-auth online-time time

【参数说明】 online-time: 本地用户认证成功后的用户可用时长

time：时长，单位分钟

【命令模式】 全局配置模式

【使用指导】 不对授权类型的认证用户生效

配置举例

↘ 配置本地认证用户认证成功后的可用时长

【配置方法】

- 在网关上配置本地认证用户认证成功后的可用时长为 10 分钟

```
Ruijie# configure terminal
Ruijie(config)# app-auth local-auth online-time 10
```

【检验方法】

- show app-auth local-auth config 查看本地认证的配置

```
Ruijie#  show app-auth local-auth config
enable: True
data-store-enable: True
data-store-age-day: 36
user-mac-limit: 2
online-time: 10
authorize-time: 33
restrict-range information:
```

```
mobile:
   global: false
   name:
   state:   Idle
pc:
   global: false
   name:
   state:   Idle
```

常见错误

- 不对授权类认证的用户生效
-

18.5.41 配置限制终端类型上网

配置效果

- 配置限制终端类型上网

注意事项

- 无

配置方法

- 可选配置

检验方法

- show app-auth local-auth config 查看

相关命令

↘ 配置限制终端类型上网

【命令格式】 app-auth local-auth restrict { pc | mobile } [exclude time-range time]

【参数说明】 pc：限制 pc 上网

mobile：限制手机上网

time：不限制上网的起始时间

【命令模式】 全局配置模式

【使用指导】 用于限制用户的上网行为

配置举例

↘ 配置限制终端类型上网

【配置方法】

- 限制移动用户不能上网，其中在“day”这个时间段内不生效

```
Ruijie# configure terminal
Ruijie(config)# app-auth local-auth restrict mobile exclude time-range day
```

【检验方法】

- show app-auth local-auth config 查看本地认证配置

```
Ruijie#  show app-auth local-auth config
enable: True
data-store-enable: True
data-store-age-day: 36
user-mac-limit: 2
online-time: 1
authorize-time: 33
restrict-range information:
  mobile:
    global: true
    name:     day
    state:    Not exist
  pc:
    global: false
    name:
    state:    Idle
```

常见错误

- 无

18.6 监视与维护

清除各类信息

无

查看运行情况

作用	命令
查看在线用户	**show app-auth online**
查看所有用户信息	**show app-auth user all**
查看 app-auth 相关参数配置	**show app-auth statistics**
查看认证网段配置	**show app-auth auth-rule**
查看 app-auth 选项配置	**show app-auth cfg-opt**
查看内网免认证 IP	**show app-auth direct-srcip**
查看直通外网 IP	**show app-auth direct-dstip**
查看 mac 白名单	**show app-auth direct-mac**
查看 mac 黑名单	**show app-auth deny-mac**
查看认证网段配置规则	**show app-auth auth-rule**
查看网段/ssid 配置信息	**show app-auth ssid-cfg**
查看 tcp 长连接配置信息	**show app-auth tcp-info**
查看 HTTPS 重定向信息	**show app-auth proxy-option config**
查看本地认证配置	**show app-auth local-auth config**
查看认证策略信息	**show app-auth policy**
查看特权用户用信息	**show app-auth local-auth vip-group**
查看本地认证用户信息	**show app-auth local-auth subs**
查看本地认证在线用户信息	**show app-auth local-online**

查看调试信息

无

19 Webservice

19.1 概述

webservice 用于配合 app-auth 的认证功能，用于与服务器的 http 交互过程控制。

该功能类似 WEB 服务，具体业务逻辑主要还是有 app-auth 进行控制。

协议规范

- 无

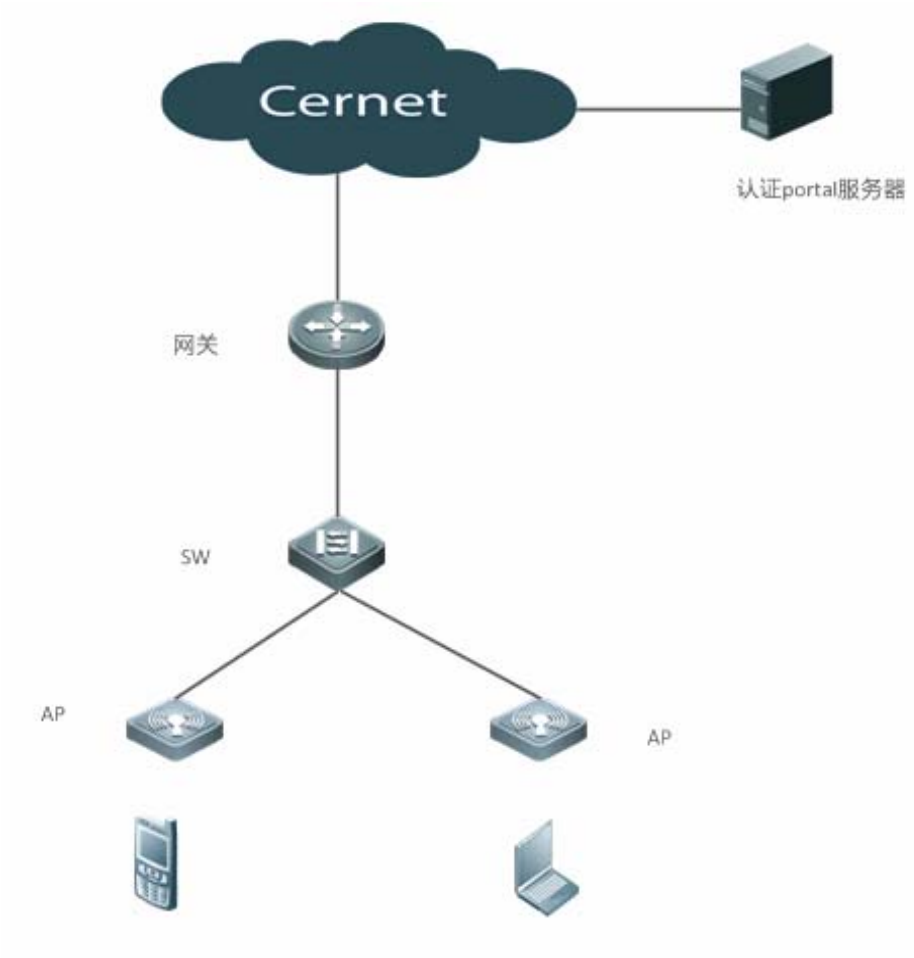
19.2 典型应用

典型应用	场景描述
Webservice 的典型应用场景	描述 Webservice 的典型应用场景

19.2.1 Webservice典型应用场景

应用场景

如下图所示，移动终端通过网关与认证服务器的联动完成认证接入功能。



【注释】 认证服务器可以是锐捷 WMC 或 MCP，或者第三方遵循 APP-AUTH 标准认证协议的服务器。

webservice 提供了 http server 和 http client 功能，可用于网关和认证服务器的 HTTP 交互部分。

功能部属

无

19.3 功能详解

工作原理

webservice 提供的 http server 可以接受终端的 http 请求，如 APP-AUTH 在 wifidog 业务中，由终端发起的 token 校验即由 webservice 进行接收。同时 webservice 也可以作为 http client 端向服务器发起 token 的校验。

19.4 配置详解

配置项	配置建议 & 相关命令	
配置服务器地址	⚠ 可选配置。提供连个服务器地址配置，在选择微信连 wifi 同时需要支持 wifidog 协议时，需要两个同时配置。	
	webservice service-url url	服务器地址 1
	webservice sec-service-url url	服务器地址 2
配置服务器检测	⚠ 可选配置。用于检测服务器是否正常	
	webservice portal-check [enable | interval time_1 **| retransmit** num**]**	服务器检测
配置监控服务器类型	⚠ 可选配置。用于配置监控服务器类型	
	webservice monitor fmt *xwc*	配置监控服务器类型

19.4.1 配置服务器地址

配置效果

- 网关和该服务器地址按照协议约定进行交互

注意事项

- 根据所选协议进行配置

配置方法

- 可选配置
- 如果不需要微信连 wifi 和 wifidog 共存，只需要配置 **webservice service-url** 即可，两个共存情况下 **webservice service-url** 配置为微信连 wifi 的地址， **webservice sec-service-url** 配置为 wifidog 地址

检验方法

- show webservice config 查看相关配置

相关命令

↘ **配置服务器地址 1**

【命令格式】 **webservice service-url** url

【参数说明】 url：服务器地址

【命令模式】 全局配置模式

【使用指导】 配置为微信连 wifi 或者 wifidog 服务器地址

配置服务器地址 2

【命令格式】 **webservice sec-service-url** url

【参数说明】 url：服务器地址

【命令模式】 全局配置模式

【使用指导】 需要同时开启微信连 wifi 和 wifidog 时使用。服务器地址 1 配置为微信连 wifi，服务器地址配置为 wifidog.

配置举例

配置微信连 wifi 和 wifidog 共存

【配置方法】
- 在 APP-AUTH 中先配置为微信连 wifi 功能
- Webservice 中分别把服务器地址 1 和地址 2 配置为微信连 wifi 和 wifidog。

```
Ruijie# configure terminal
Ruijie(config)# app-auth enable
Ruijie(config)# app-auth cwmp enable
Ruijie(config)# app-auth cfg-opt rdt-for-wx2
Ruijie(config)# app-auth ad-url http://wmc.ruijieyun.com/auth/servlet/standardAuthServlet/portal
Ruijie(config)# webservice service-url
http://wmc.ruijieyun.com/auth/servlet/standardAuthServlet/portal
Ruijie(config)# webservice sec-service-url http://wmc.ruijieyun.com/auth/wifidogAuth
```

【检验方法】
- 分别使用 show app-auth statistic 和 show webservice 查看

常见错误

- 无

19.4.2 配置服务器检测

配置效果

- 在服务器异常时，所有用户不需要进行认证

注意事项

- 需要确认服务器支持后再开启，否则会导致所有不需要认证

配置方法

- 可选配置

检验方法

- show webservice config 查看相关配置

相关命令

↘ 配置服务器检测

【命令格式】 **webservice portal-check** [**enable | interval** time_1 **| retransmit** num]

【参数说明】 enable：功能开启

time_1：检测间隔

num：重试次数

【命令模式】 全局配置模式

【使用指导】 配置服务器检测，可在服务器异常时使所用用户不需要认证。

配配置举例

- 无

常见错误

- 无

19.4.3 配置监控服务器类型

配置效果

- 用户认证成功后，将用户信息通告给监控服务器。

注意事项

- 需要确认服务器支持后再开启

配置方法

- 可选配置
- 在通用场景下使用。

检验方法

- show run | i monitor fmt 查看相关配置

相关命令

↘ 配置服务器检测

【命令格式】 **webservice monitor fmt** *xwc*

【参数说明】 *xwc:* 服务器类型为新网程

【命令模式】 全局配置模式

【使用指导】 配置监控服务器为新网程，可以在用户认证成功后将用户信息通告给监控服务器。

配配置举例

- 无

常见错误

- 无

19.5 监视与维护

清除各类信息

无

查看运行情况

作用	命令

查看 webservice 相关配置	**show webservice config**

查看调试信息

无

20 ANTI-PAP

20.1 概述

Anti-PAP（Anti Personal Access Point，防私接无线接入点）可对用户的私接 AP 行为进行检测。当检测到该行为时，可禁止用户访问外网一段时间。

本功能可防止网络中出现不可控的接入设备，在一定程度上保障网络安全。同时也防止私接 AP 影响正常 AP 的无线信号。

20.2 典型应用

典型应用	场景描述
防止内网用户私接 AP	内网终端直接通过接入设备上网，中间不可私接其它设备。

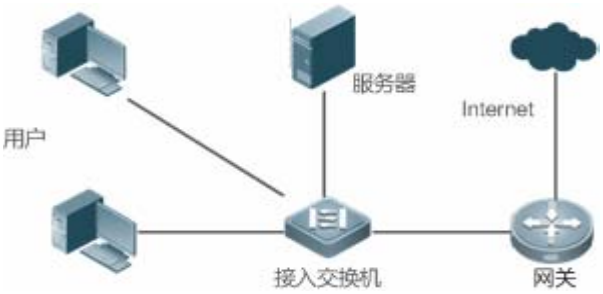
20.2.1 防止内网用户私接AP

应用场景

内网终端直接通过接入设备上网，中间不可私接其它设备。

- 内网中，多个终端共享同一个 IP 会被阻断访问 Internet。

图 20-1



功能部属

- 在设备上配置需要检测的用户组与阻断方式，实现对用户的私接 AP 行为检测与阻断。

20.3 功能详解

基本概念

无

功能特性

功能特性	作用
私接 AP 检测	检测用户是否有私接 AP。

20.3.1 私接AP检测

设备检测用户的网络流量，发现有私接行为时可通过阻断或限速等手段限制用户的网络访问。

工作原理

有私接行为，必然会出现多个终端。因此，私接行为检测本质是终端数量检测。

可用来检测终端的手段包括：User-Agent 检测、虚拟身份数量检测。

User-Agent 检测

User Agent（用户代理），简称 UA，是 HTTP 请求报文首部中的一个字段。其内容包含终端使用的操作系统及版本、CPU 类型、浏览器及版本、浏览器渲染引擎、浏览器语言、浏览器插件等，可用来识别终端。

虚拟身份数量检测

内容审计模块的虚拟身份审计功能可审计虚拟身份的上下线动作。对于一些使用普遍的应用（如微信、淘宝等），可基于同时在线的账号数量来判断是否有多个终端。

20.4 产品说明

NBR108G-P、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1500G、NBR2000G 不支持防私接 AP，NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR800G、NBR950G、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持防私接 AP。

20.5 配置详解

配置项	配置建议 & 相关命令	
配置待检测用户对象	必须配置。指定待检测的用户对象。	
	anti-pap monitor	配置待检测用户对象。
配置免阻断服务器资源	可选配置。防止对特殊服务器的访问被设备阻断。如访问认证服务器。	
	anti-pap avoid-block	添加免阻断服务器资源。

20.5.1 配置待检测用户对象

配置效果

- 开始检测指定用户对象的上网行为，判断是否有私接 AP。

注意事项

- 本功能有使用应用识别、流量审计、虚拟身份审计的处理结果，开启这三个功能有助于增强检测效果。
- 关闭防共享策略会清空之前检测的终端信息。
- 检测用户终端需要一定时间，流量充足时（例如正常浏览网页的流量），10 分钟内即可检测出一台终端。如果共享上网的设备无流量，则此时是无法被检测出来的。
- 两台 Windows 系统终端或两台相同品牌型号的手机终端，较难区分，因而此类共享行为较难检测出来。但可通过配置允许同时登录的同类型虚拟身份账号数来检测，即检测到的账号数超过所配数时认为有私接行为。
- 阻断用户后，用户访问的 HTTP 页面（非 HTTPS）会变成阻断提示信息，但此时浏览器仍然有可能访问其缓存的信息。惩罚到期后，用户之前的终端信息会被清空。

配置方法

↘ 配置待检测用户对象

- 必须配置。

【命令格式】 **anti-pap monitor** { **subscriber** { *subs-name1* | **any** } | **auth-subscriber** { *subs-name2* | **any** } } [**expected-terminal pc**] [{ **block** [*time*] | **limit** *down up* } **base** { **user** | **ip** }]

【参数说明】 **subscriber** *subs-name1*：指定待检测的本地用户名。

subscriber any：指定检测所有本地用户。

auth-subscriber *subs-name2*：指定待检测的认证用户名。

auth-subscriber any：指定检测所有认证用户。

expected-terminal { **pc** | **mobile** }：指定期望的终端类型为 PC。缺省为任意终端类型。

block：指定是否阻断。缺省不阻断。

time：阻断时间，取值范围 1 ~ 1440，单位：分。缺省为 10 分钟。

limit：限制用户带宽。缺省不限速。

down：下行带宽。

up：上行带宽。

user：基于用户名阻断用户。

ip：基于 IP 阻断用户。

【缺省配置】 不检测任何用户

【命令模式】 全局模式

【使用指导】 用户名通常配用户组名。认证用户的规则优先级高于本地用户的，下级用户的高于上级的。

检验方法

使用 **show anti-pap config** 命令检查设备上是否添加了待检测用户对象。

【命令格式】 **show anti-pap config**

【参数说明】 -

【命令模式】 特权模式、全局模式

【使用指导】 -

【命令展示】

```
Ruijie(config)#show anti-pap config
{
    "code": 0,
    "msg": "",
    "data": {
        "monitor": [
            {
                "User": "any",
                "Auth": "no",
                "Invalid": false,
                "Exp-Term": "any",
                "Ctrl": "block",
                "Time": 10,
                "ByUser": false
            }
        ]
    }
}
```

关于 show 信息的详细解释请参看对应功能的命令手册。

配置举例

对地址范围（192.168.1.2～192.168.1.254）内的用户进行检测。

【网络环境】

图 20-3



【配置方法】

- 定义用户组与用户。
- 将用户添加为待检测用户。

```
Ruijie# configure terminal
Ruijie(config)# subscriber static name "19#students" parent "/" ip-range 192.168.0.2 192.168.0.254
Ruijie(config)# anti-pap monitor 19#students
Ruijie(config)# end
```

【检验方法】

用户使用无线网卡做软 AP 为手机提供无线网络服务，并同时使用两台终端上网

- 用户访问 Internet 被阻断。

常见错误

- 无

20.5.2 配置免阻断服务器资源

配置效果

- 被阻断的用户仍然可访问指定的服务器。

注意事项

- 只有当用户访问这些服务器的报文会经过设备时才需要该配置。

配置方法

↘ 配置免阻断服务器资源

- 可选配置。

【命令格式】 **anti-pap avoid-block ip-group** *id*

【参数说明】 *id*：IP 对象组 ID。

【缺省配置】 无任何免阻断服务器。

【命令模式】 全局模式

【使用指导】 服务器资源必须先通过 **ip-group** 命令定义，然后才可被本命令引用。

检验方法

- 使用 **show anti-pap config** 命令检查设备上是否添加了待检测用户对象。

【命令格式】 **show anti-pap config**

【参数说明】 **-**

【命令模式】 特权模式、全局模式

【使用指导】 -

【命令展示】

```
Ruijie(config)#show anti-pap config
{
    "code": 0,
    "msg": "",
    "data": {
        "avoid-block": [
            1
        ],
        "monitor": []
    }
}
```

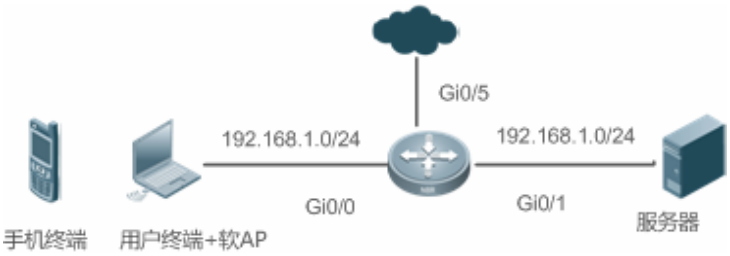
关于 show 信息的详细解释请参看对应功能的命令手册。

配置举例

将地址范围（192.168.10.2～192.168.10.254）加入免阻断服务器资源。

【网络环境】

图 20-3



【配置方法】

- 定义免阻断服务器 IP 对象组。
- 将 IP 对象组加入免阻断服务器资源中。

```
Ruijie# configure terminal
Ruijie(config)# ip-group 3
Ruijie(config-ip-group)# ip-range 192.168.10.2 192.168.10.254
Ruijie(config-ip-group)# exit
Ruijie(config)# anti-pap avoid-block ip-group 3
Ruijie(config)# end
```

【检验方法】 用户使用无线网卡做软 AP 为手机提供无线网络服务，并同时使用两台终端上网，导致用户被阻断；或者直接手动阻断用户。

- 用户可以访问服务器，但无法访问因特网。

20.6 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
取消对指定用户的限制。	**clear anti-pap control** { { { **subscriber** *subs-name1* | **auth-subscriber** *subs-name2* } } | **ip** *addr* }

查看运行情况

作用	命令
显示配置信息。	**show anti-pap config**
显示日志。	**show anti-pap log from** *y1 m1 d1* [*H1:M1:S1*] **to** *y2 m2 d2* [*H2:M2:S2*] [**subscriber** *subs-name1* | **auth-subscriber** *subs-name2*] [**ip** *addr*] **order-by** { **time** | **subscriber** | **auth-subscriber** | **ip** } { **asc** | **desc** } [**start-item** *num1* **end-item** *num2*]
显示用户检测信息。	**show anti-pap user** [**subscriber** *subs-name1* | **auth-subscriber** *subs-name2*] [**ip** *addr*]

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

无相关命令	-

21 广告推送

21.1 概述

广告推送是一种在用户使用浏览器上网的同时 ,网络设备强制浏览器打开特定的广告窗口的方法。它是 web 认证的一个子功能。主要原理是在锐捷 web 认证的 HTTP 拦截和 HTTP 重定向的技术的基础上 , 由设备先拦截广告用户的 http/https 报文 (其他报文不拦截) , 并做一次重定向(重定向到配置指定的广告地址) , 然后放行用户的 http/https 报文。

协议规范

- HTTP：RFC1945 RFC2068
- HTTPS：RFC2818

21.2 典型应用

典型应用	场景描述
广告推送基本场景	常见的二层广告推送基本场景，由设备负责广告推送，用户通过二层网络连接设备

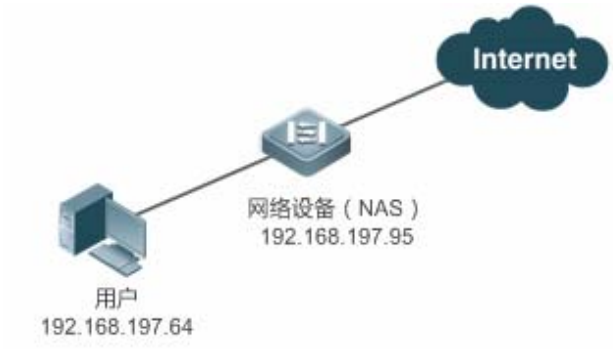
21.2.1 广告推送基本场景

应用场景

如 图 21-1 所示

- 在网络设备上部署广告推送方案
- 下联用户需要通过广告推送后才能访问 internet

图 21-1 广告推送方案网络拓扑图



功能部属

- 在 NAS 上全局开启广告推送。
- 在 NAS 上配置广告推送的网段范围。

21.3 功能详解

基本概念

↘ 广告推送方案

用户通过二层网络连接设备，设备先拦截广告用户的 http/https 报文（其他报文不拦截），并做一次重定向(重定向到配置指定的广告地址)，然后放行用户的 http/https 报文。

↘ HTTP 拦截

HTTP 拦截指网络设备将原本需要转发的 HTTP 报文拦截下来，不进行转发。这些 HTTP 报文是连接在网络设备下的用户的浏览器所发出的，但目的并不是网络设备本身。例如，某用户通过 IE 浏览器访问 www.google.com，网络设备本应该将这些 HTTP 请求报文转发到网关的，但如果启动 HTTP 拦截，这些报文将不被转发。

HTTP 拦截之后，网络设备需要将用户的 HTTP 连接请求转向自己，于是网络设备和用户之间将建立起连接会话。网络设备将利用 HTTP 重定向功能，将重定向页面推送给用户，用户的浏览器上将弹出一个页面，这个页面可以是认证页面，也可以是下载软件的链接等等。

在广告功能中，哪些用户所发出的到目的端口（目前仅支持 80 和 443 端口）的 HTTP 报文需要进行拦截，哪些不需要，都是可以设置的。一般地，未经过广告推送的用户发出的 HTTP 请求报文会被拦截，已经推送过的用户将不被拦截。HTTP 拦截是广告功能的基础，一旦浏览器发出的 HTTP 报文被拦截，就会自动触发广告推送的过程。

↘ HTTP 重定向

根据 HTTP 协议规定，正常情况下，用户的浏览器发出 HTTP GET 或 HEAD 请求报文后，如果接收一方能够提供资源，则以 200 报文响应，如果本地不能提供资源，则可以使用 302 报文响应。在 302 响应报文中，提供了一个新的站点路径，用户收到响应后，可以向这个新的站点重新发出 HTTP GET 或 HEAD 报文请求资源，这就是重定向。

HTTP 重定向是广告推送功能的重要环节，是发生在 HTTP 拦截之后的，利用的就是 HTTP 协议中的 302 报文的特性。HTTP 拦截过程将使得网络设备和用户之间建立起连接会话，随后用户将（本应发给其他站点的）HTTP GET 或 HEAD 报文发给网络设备，网络设备收到后，回应以 302 报文，并且在 302 报文中加入重定向页面的站点路径，这样用户将向这个站点路径重新发出请求，就会获取到重定向的页面。

功能特性

功能特性	作用
广告推送	通过网络设备向用户推送广告

21.3.1 广告推送

工作原理

广告推送的角色：

客户端：通常是浏览器，运行 HTTP 协议，用户通过浏览器上网时浏览器将发出 HTTP 请求。
网络设备：在网络拓扑中一般是接入层设备，一般与用户终端设备直接相连接，在设备上需要启动广告推送功能。
广告推送的流程：

1. 设备将广告用户发出的 http/https 报文拦截下来，通过 inpath 组件转发到 web 认证组件监听的特定端口。
2. web 认证组件收到报文后，发现广告功能已经开启，而且用户也在广告推送的网段范围内，于是将报文转给广告子模块，由广告子模块发出重定向响应，将其重定向到广告地址去，这样在用户的浏览器上将弹出一个广告页面。
3. 重定向完成后，广告子模块记录用户信息，并通过 SCC 接口配置接入用户表项，放行用户的 http/https 报文。

用户下线：

14. 第一种情况，关闭广告功能。通过 no advertising enable 关闭广告功能后，设备删除所有广告用户信息，强制用户下线。
15. 第二种情况，删除某个广告推送的网段配置，那么设备将删除在该网段内的广告用户信息，强制用户下线。
16. 第三种情况，如果开启了周期间性拦截功能，那么间隔时钟到期后，广告子模块找出超时的用户信息，通过 SCC 接口删除这些接入用户的表项，对用户后续的 http/https 报文重新开始广告推送。

相关配置

↘ 配置广告弹出框的页面地址

缺省情况下无配置

在全局配置模式下使用 **advertising url** { *url-string* }来配置页面地址

↘ 配置广告推送的网段范围

缺省情况下无配置

在全局配置模式下使用 **advertising free-user ip** { *ip-address* } **mask** { *ip-mask* }来配置

↘ 开启广告功能

缺省情况下该功能关闭

在全局配置模式下使用 **advertising enable** 命令开启

↘ 开启周期性拦截

缺省情况下无配置

在全局配置模式下使用 **advertising suppress** 命令开启

↘ 配置周期性拦截的时间间隔

缺省情况下无配置

在全局配置模式下使用 **advertising min-interval** { *interval-value* }命令来配置

↘ 开启确保广告弹出框不被浏览器拦截功能

缺省情况下无配置

在全局配置模式下使用 **advertising popup-page** 命令开启

21.4 产品说明

NBR108G-P、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1500G、NBR2000G 不支持广告推送，NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR800G、NBR950G、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持广告推送

21.5 配置详解

配置项	配置建议 & 相关命令	
配置广告推送功能	必须配置。用于配置广告功能基本参数	
	advertising url	设置广告弹出框的页面地址。
	advertising free-user ip mask	设置广告推送的网段范围。
	advertising enable	在全局上启动广告服务。
	以下为可选配置。用于配置广告功能附加参数	
	advertising suppress	开启周期性拦截。
	advertising popup-page	开启确保广告弹出框不被浏览器拦截功能。
	advertising min-interval	设置周期性拦截的时间间隔。

21.5.1 配置广告推送功能

配置效果

在用户浏览器弹出广告窗口

注意事项

无

配置方法

配置广告弹出框的页面地址

- 必须配置，要成功应用广告推送功能，必须设置广告弹出框的页面地址。

配置广告推送的网段范围

- 必须配置，要成功应用广告推送功能，必须设置广告推送的网段范围。
- 当设备发现未认证用户在访问网络资源时 ,设备将根据广告推送的网段范围及广告功能开关来判断是否对此用户进行广告推送功能。
- 最大允许配置 50 个网段

在全局口上开启广告功能

- 必须配置。
- 默认情况下，未开启广告功能，此时所有连接的用户不进行广告推送。

开启周期性拦截功能

- 可选配置。
- 默认情况下，未开启周期性拦截功能，此时所有连接的用户只推送一次广告。

配置周期性拦截的时间间隔

- 可选配置。
- 未开启周期性拦截，默认值为 0。
- 开启周期性拦截，默认值为 30。
- 开启周期性拦截后，将根据配置的时间间隔，周期性向连接的用户推送广告。

开启确保广告弹出框不被浏览器拦截功能

- 可选配置。
- 默认情况下，未开启。

检验方法

- 如果一个新用户(它的属性如 ip，符合推送广告的规则)，那么设备会先向该用户推送广告，之后让这个用户上线。
- 用户上线后，可以正常使用网络，设备不再对其推送广告。

相关命令

配置广告弹出框的页面地址

【命令格式】 **advertising url** { *url-string* }
【参数说明】 广告弹出框的页面地址
【命令模式】 全局配置模式

【使用指导】 以 http://或 https://开头

配置广告推送的网段范围

【命令格式】 **advertising free-user ip** { *ip-address* } **mask** { *ip-mask* }
【参数说明】 -。
【命令模式】 全局配置模式
【使用指导】 最大允许配置 50 个网段

配置全局口上开启广告功能

【命令格式】 **advertising enable**
【参数说明】 -
【命令模式】 全局配置模式
【使用指导】 -

开启周期性拦截功能

【命令格式】 **advertising suppress**
【参数说明】 -
【命令模式】 全局配置模式
【使用指导】 -

配置周期性拦截的时间间隔

【命令格式】 **advertising min-interval** { *interval-value* }
【参数说明】 -
【命令模式】 全局配置模式
【使用指导】 允许配置范围<30 -1440>

开启确保广告弹出框不被浏览器拦截功能

【命令格式】 **advertising popup-page**
【参数说明】 -
【命令模式】 全局配置模式
【使用指导】 -

配置举例

以下配置举例，仅介绍与广告相关的配置。

【网络环境】 -

【配置方法】
- 在网络设备的全局配置模式下开启广告功能

```
Ruijie# config
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# advertising url http://www.baidu.com/
```

```
Ruijie(config)# advertising free-user ip 192.168.197.0 mask 255.255.255.0
Ruijie(config)# advertising enable
Ruijie(config)# advertising suppress
Ruijie(config)# advertising min-interval 40
Ruijie(config)# advertising popup-page
```

【检验方法】

- 广告配置是否成功

```
Ruijie#show running-config
…
advertising popup-page
advertising enable
advertising free-user ip 192.168.197.0 mask 255.255.255.0
advertising min-interval 40
advertising url http://www.baidu.com/
advertising suppress
….
```

```
Ruijie#show advertising
advertising enable:       On
advertising url:          http://www.baidu.com/
advertising suppress:     On
advertising popup-page:   On
advertising min-interval: 40
advertising free-user:
  192.168.197.0    255.255.255.0
```

常见错误

无

21.6 监视与维护

清除各类信息

作用	命令
强制用户下线	**clear web-auth user** { **all** | **ip** *ip-address* | **mac** *mac-address* | **name** *name-string* | **session-id** *num* }

查看运行情况

作用	命令

查看广告基本参数配置。	**show advertising**
查看广告推送的网段范围	**show advertising free-user**
查看所有广告用户。	**show advertising user**
查看所有用户或是指定用户的在线信息。	**show web-auth user**{ **all** | **ip** *ip-address* | **mac** *mac-address* | **name** *name-string* | **session-id** *num* }

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
广告 debug	**debug web-auth advertising 或者 debug web-auth all**

22 LOCAL-ACCOUNT

22.1 概述

Local-Account（本地计费）是一种计费方式。当没有远程计费软件的时候，可以使用本地计费功能来代替。

- Local-Account 仅适用于设备做 PPPoE server 的场景。

下文仅介绍 Local-Account 的相关内容。

协议规范

- 无

22.2 典型应用

典型应用	场景描述
设备做 PPPoE Server 同时本地计费	设备做为 PPPoE Server 为下级终端、设备提供认证、计费服务。

22.2.1 设备做PPPoE Server同时本地计费

应用场景

在网关作为出口，在其上开启 PPPoE Server 功能、计费功能。下级终端、设备通过 PPPoE client 进行认证上网。

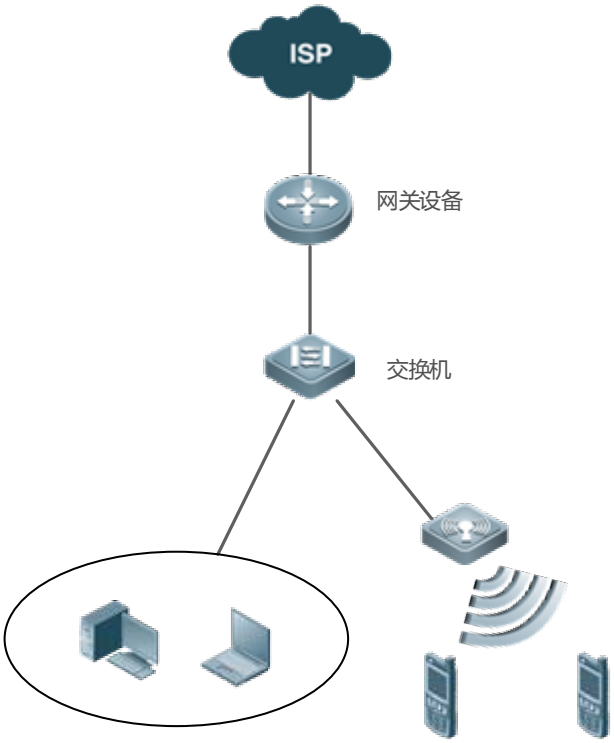


图 22-1

【注释】 网关设备作为 PPPoE server 与计费设备。
下联设备、终端作为 PPPoE client 接入网络。

功能部属

- 出口网关作为 PPPoE server，完成客户端的认证。
- 交换机作为接入设备。
- 终端、其他网络设备作为 PPPoE client 进行认证。
- 出口网关作为计费设备，对内网的用户进行计费。

22.3 功能详解

基本概念

PPPoE

Point to Point Protocol over Ethernet，在以太网上承载 PPP 协议。按照角色行为，可以分为 PPPoE server 与 PPPoE client。

本地计费

不依赖外部服务器，仅依靠设备自身对用户的上网行为进行计费与限制。

功能特性

功能特性	作用
用户管理	添加/删除 合法用户，并对用户赋予一定的功能属性。
计费通告系统	账号到期提前通告、上网到期通告、阻止上网通告。

22.3.1 用户管理

自身维护一个用户信息库，用于对用户身份合法性认证。

工作原理

Local-Account 自身维护一个用户数据库，当用户通过 PPPoE client 进行认证的时候，与数据库中的用户信息、策略匹配，作出合适的行为分配。

↘ 添加、删除用户

将用户从用户数据库中插入、删除。

↘ IP、MAC 绑定

管理员可以根据实际场景需要，对帐号进行 ip、mac、ip&mac 的绑定。

对于 IP 绑定的用户，这个用户只能使用该 IP 上网。

对于 MAC 绑定的用户，这个用户只能使用该 MAC 进行上网。

对于 MAC 自动绑定的用户，当该用户第一次认证成功后，系统会记录下此 MAC，后序该用户只能用这个 MAC 认证上线。

对于 IP&MAC 绑定的用户，这个用户只能只用该 IP 且该 MAC 上网。

↘ 计费策略

管理员可以对用户进行计费，当计费的条件到达(比如时间)的时候，禁止用户访问网络。

相关配置

↘ 添加、删除用户。

使用命令 **local-account username** *username* 进行添加用户。

使用命令 no **local-account username** *username* 进行删除用户

↘ IP、MAC 绑定

在 local-account 模式下使用 **ip** *ip-address* 命令进行该用户的 ip 绑定。

在 local-account 模式下使用 **mac** { *mac-address* | **auto** } 命令对该用户进行 mac 绑定、自动绑定。

↘ 计费策略

在 loacl-account 模式下使用 **policy** 进行计费策略的配置，目前的策略只有基于时间的策略。

22.3.2 计费通告系统

通告系统要实现的是账号到期提前通告、上网到期通告、阻止上网通告，通告的形式为一个 html 页面，在用户访问网页的时候跳转到此通告页面。

工作原理

当用户的帐号快到期的时候，对用户的 HTTP 流量进行代理，代理生成应答到一个预置的页面，提示用户。

↘ HTTP 代理

对 HTTP 流量进行拦截，并对 HTTP 请求构造“通告响应”报文，发送给客户端。

相关配置

↘ 配置通告策略。

使用命令 **local-account notice enable** 开启通告功能。

使用命令 **local-account notice date-rule** *hour interval-min* 配置距离用户到期多久(单位小时)开始通告 ,以及每次通告的时间间隔(单位分钟)

22.4 产品说明



NBR108G-P、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1500G、NBR2000G 不支持本地计费功能；NBR800G、NBR950G、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持本地计费功能。

22.5 配置详解

配置项	配置建议 & 相关命令	
配置用户管理.	⚠ 必须配置。用于用户管理	
	local-account user *username*	添加用户，进入到 local-account 模式配置用户参数
	description *string*	配置该用户的描述信息(local-account 模式下)
	ip *ip-address*	配置 ip 绑定(local-account 模式下)

	mac { *mac-address* | **auto** }	配置 mac 绑定(local-account 模式下)
	policy date *yyyy mm dd*	配置计费策略(local-account 模式下)
配置通告系统	可选配置。用于用户到期的通告。	
	local-account notice enable	开启通告功能
	local-account notice date-rule *hour interval-min*	配置通告策略
配置前端模块流量通告频率	可选配置。用于用户到期的通告。	
	loca-account period *second*	配置前端模块流量通告频率(单位 s)

22.5.1 配置用户管理

配置效果

- 添加用户、删除用户。
- 对用户的行为定制策略。

注意事项

- 无

配置方法

↘ 添加、删除用户

- 必须配置。
- 需要配置了用户，外部模块才能使用用户名进行认证(如 PPPoE server)。

↘ 配置用户行为

- 可选配置。

检验方法

配置完用户后，内网 PPPoE client 可以通过该用户名和密码进行登陆。

相关命令

↘ 添加用户并给用户赋予绑定策略

【命令格式】 **local-account username** *username*
【参数说明】 **username** *username*：用户名。
【命令模式】 全局模式
【使用指导】 -

给用户赋予 IP 绑定策略

【命令格式】 **ip** *ip-address*
【参数说明】 **ip** *ip-address*：IP 绑定
【命令模式】 local-account-user 模式
【使用指导】 -

给用户赋予 MAC 绑定策略

【命令格式】 **mac** { *mac-address* | **auto** }
【参数说明】 **mac** *mac-address*: MAC 手动绑定
mac auto: MAC 自动绑定
【命令模式】 local-account-user 模式
【使用指导】 -

添加用户并给用户赋予计费策略

【命令格式】 **policy date** *yyyy mm dd*
【参数说明】 **policy date**：使用日期作为计费策略
yyyy: 到期年份
mm: 到期月份
dd: 到期日
【命令模式】 local-account-user 模式
【使用指导】 -

配置举例

以下配置举例，仅介绍与 Local-Account 相关的配置。

在设备上添加新用户

【网络环境】 Pppoe-client --- EG --- isp

【配置方法】

- 在设备上添加用户 test，密码为 test，并赋予 ip 绑定的策略

A

```
A# configure terminal
```

```
A(config)# local-account user test password test ip 1.1.1.1
A(local-account-user)# ip 1.1.1.1
A(local-account-user)# mac 1111.2222.3333
A(local-account-user)# description test
A(local-account-user)# policy date 2018 1 21
```

【检验方法】 使用命令 show local-account users web，查看生成的用户。

A

```
Ruijie#show local-account users


(0) Online  (S) State: 0=Invalid 1=Normal 3=Overdue
-------------------------------------------------------------------------------------------
Name          0  S  Policy      Ip addr          Mac addr           Note
-------------------------------------------------------------------------------------------
test          0  3  2018/1/21   1.1.1.1          11:11:22:22:33:33  test


total:1    upper limit:150
Ruijie
```

常见错误

- 无。

22.5.2 配置计费通告系统

配置效果

- 完成配置后，当用户快要到期的时候，用户可以看到通告信息。

注意事项

- 必须配置 Local-Account 的基本功能。

配置方法

- 按照命令配置计费通告系统

检验方法

- 模拟快到期的用户，可以定期看到通告的信息。

相关命令

配置开启通告功能

【命令格式】 **local-account notice enable**

【参数说明】 **notice enable**：开启通告系统。

【命令模式】 全局模式

【使用指导】 -

配置通告策略

【命令格式】 **local-account notice date-rule** *hour interval-min*

【参数说明】 **notice date-rule**：按照到期日期通告。

hour：距离到期多久前开始通告

interval-min：每次通告的时间间隔

【配置模式】 全局模式

【使用指导】 -

配置举例

配置开启通告功能，并且再到期时间前 5 小时每隔 10 分钟通告一次。

【配置方法】

- 如下

```
Ruijie# configure terminal
Ruijie(config)# local-account notice enable
Ruijie(config)# local-account notice date-rule 5 10
Ruijie(config)# end
```

【检验方法】 查看配置。

```
Ruijie# show local-account config
users-limit: 150
acct-period: 20s
notice: on
notice-time: 5h
notice-interval: 10m
Ruijie#
```

常见配置错误

- 无。

22.5.3 配置前端模块流量通告频率

配置效果

- 完成配置后，前端模块(如 pppoe-server)会定期奖流量信息同步给本地计费模块。

注意事项

- 必须配置 Local-Account 的基本功能。
- 对于不要很精确的场景，建议该值配置大一些。

配置方法

- 按照命令配置前端模块流量通告频率

检验方法

- 查看配置，有该项配置存在。
- 前端模块定制奖流量信息刷给本地计费模块。

相关命令

↘ 配置开启通告功能

【命令格式】 **local-account period** *second*
【参数说明】 **period** *second*：通告频率。
【命令模式】 全局模式
【使用指导】 -

配置举例

↘ 配置外部通告频率，并且再到期时间前 5 小时每隔 10 分钟通告一次。

【配置方法】
- 如下

```
Ruijie# configure terminal
Ruijie(config)# local-account period 20
Ruijie(config)# end
```

【检验方法】 查看配置。

【配置方法】

- 如下

```
Ruijie# configure terminal
Ruijie(config)# local-account period 20
Ruijie(config)# end
```

【检验方法】

查看配置。

```
Ruijie# show local-account config
users-limit: 150
acct-period: 20s
notice: on
notice-time: 5h
notice-interval: 10m
Ruijie#
```

常见配置错误

- 无。

22.6 监视与维护

查看运行情况

作用	命令
查看配置。	show local-account config
查看用户	show local-account users
查看在线用户	show local-account online

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
打开客户端调试。	**debug local-account client**
打开 http 代理调试	**debug local-account http_proxy**
代开服务端调试	**debug local-account server**

23 防火墙

23.1 网络防攻击

23.1.1 概述

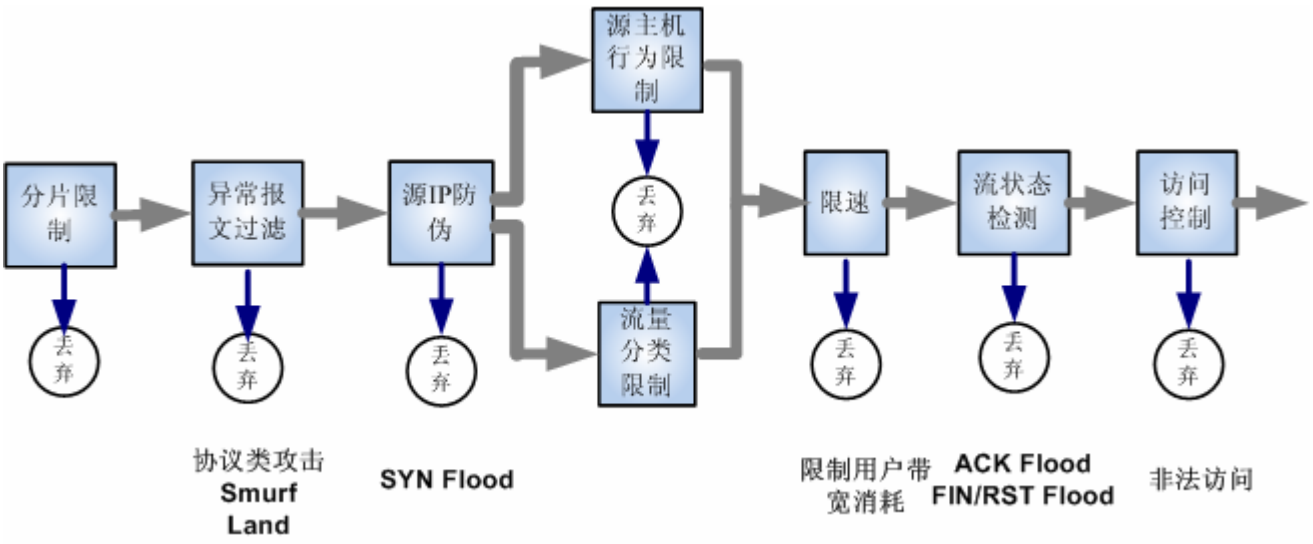
防火墙网络层攻击防范功能能够检测出多种类型的网络层攻击，并能采取相应的措施保护内部网络免受恶意攻击，保证内部网络及系统的正常运行。

防火墙抗攻击的优势主要体现在以下几个方面：

- 能够防范的网络层攻击齐全
- 传统的在交换机或路由器上配置 ACL 的方式在过滤流量和检测攻击方面存在局限性，它们不能过滤所有类型的攻击流量，无法很好的解决有状态连接的过滤，防火墙结合 ACL 应用可以有效地解决上述问题；
- 状态防火墙是通过跟踪会话的发起和状态来工作的。状态检测防火墙通过检查数据包头，分析和监视网络层(L3)和协议层(L4)，基于一套用户自定义的防火墙策略来允许、拒绝或转发网络流量。
- 针对流量的行为特征对攻击行为进行识别，并且能够有针对性的进行恶意流量的剥离。
- 根据子网、IP 集合划分防护域，并且根据每个防护域独立地进行流量监控、分析、策略实施、汇总详细的攻击报告。

攻击过滤的模型如下：

图 23-1



每个网络防攻击域都具有一套完全独立的防御体系。经过防火墙的流量传送到各个独立的网络防攻击域内实施恶意流量的剥离。用户可以配置直通流量，绕开攻击防御体系。

防火墙针对恶意流量采用多层次的过滤模型，通过对报文实施层层检测和过滤使恶意流量被识别和剥离出来。源 IP 防伪是网络防攻击的重要功能。通过将报文分为真实源报文和不可信源报文两类分别进行处理。对于来自真实源主机的报文，将进一步跟踪其源主机行为，从而发现来自真实源主机的攻击；对于不可信源报文，将对其进行分类限制，甚至直接丢弃。

限速是针对合法流量进行的，这样做的目的是为了尽量避免过早丢弃合法流量。

在防火墙上的访问控制功能，则可以由 ACL 和安全域组件进一步实现。

⚠ 本文所述的网络防攻击功能只支持 IPV4 协议。

23.1.2 典型应用

典型应用	场景描述
服务器区的安全威胁与攻击防御	防护服务器免受内外网的攻击
内网的安全威胁与攻击防御	监视、防护来自内网发出的攻击，如病毒传播等

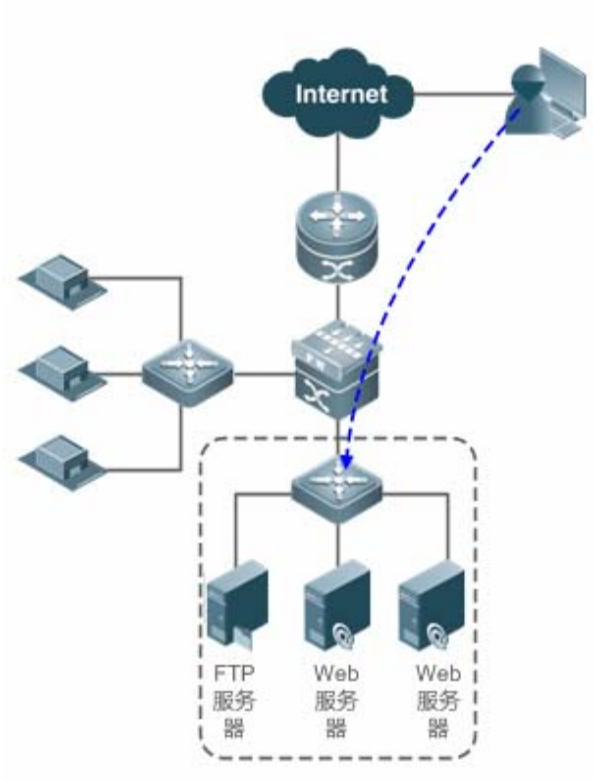
23.1.2.1 服务器区的安全威胁与攻击防御

应用场景

用户对互联网开放的服务器遭受攻击是最为常见的一种情况。来自互联网对服务器区发起的攻击可能导致服务器繁忙、瘫痪导致无法对外正常的提供服务。针对服务器的攻击主要是资源消耗类攻击，攻击者通过操控互联网上的傀儡主机对服务器区(通常是 WEB 类服务器)进行 DDoS 攻击(SYN Flood、ICMP Flood、CC 攻击等)。其中，最为常见的则是 SYN Flood 攻击，由于攻击者通常使用伪造的源 IP，因此难以识别、跟踪和防范。同时攻击者启动 SYN Flood 攻击的代价很小，而服务器则需要为此耗费大量的资源。

针对这类攻击，防火墙可以启用资源消耗类攻击的抵御策略，可以阻止此类攻击到达服务器区内。

图 23-2



功能部署

出口网关设备

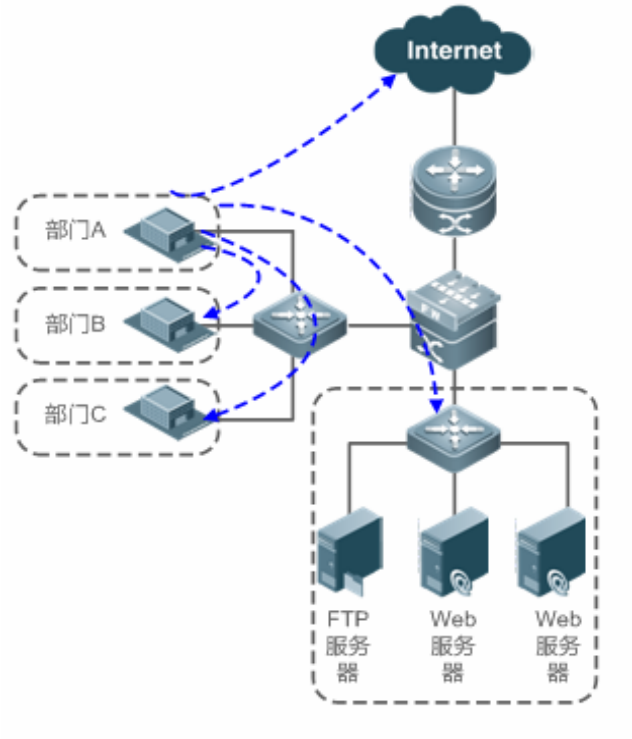
- 在网络出口部署出口网关设备，使所有进入服务器区的流量经过出口网关设备进行过滤。
- 为服务器区所在的网段划分一个网络防攻击域，部署专用的防御策略，对于进入服务器区的数据进行检查，对攻击进行防护且生成攻击报告。
- 在该网络防攻击域中监视服务器的持续流量并且记录流量情况。

23.1.2.2 内网的安全威胁与攻击防御

应用场景

内网面临的网络攻击通常包括资源消耗类攻击、网络窥探类攻击、蠕虫病毒传播类攻击。内网用户对内网的攻击行为往往危害更为严重，一旦发生蠕虫病毒爆发，或是攻击者有意嗅探网络信息寻找漏洞，都将给内网安全带来极大的挑战和影响。

图 23-3



功能部属

出口网关设备

- 在网络出口部署出口网关设备，使所有进入内网的流量经过出口网关设备进行过滤。
- 指定需要保护和监视的网络防攻击域，部署针对网络防攻击域部署出入的防护策略，如针对出域方向部署防扫描策略。
- 在各网络防攻击域中检测进出每个域的流量，进行攻击防护并且记录攻击报告。

23.1.3 功能详解

基本概念

↘ 网络防攻击域

网络防攻击域即具有相同防护策略的主机、子网的集合。通过对网络内的设备划分网络防攻击域，使网络防护的部署和配置更加简便。不同域的管理可以独立、互不干扰的进行。

↘ 防御策略自学习

通过启用网络防攻击域的策略自学习功能，可以收集网络防攻击域的日常业务数据，得到正常业务水平的数据基准值。管理员可以在这个数据基准值的基础上以一定的倍数导出对应异常业务量的识别阈值。自学习功能使管理员可以在更加了解自身业务情况的基础上部署更为合理的防护策略。

↘ 源验证

识别攻击首先需要确认报文的源是否是伪造的，甄别伪造源报文的过程就是源验证。auth 和 unauth 关键字就是针对源验证的不同结果将流量进行分类处理。识别主机源真实性的方法有 TTL 识别、TCP 代理。

> 并不是所有的报文都能够判断出是否来自真实源。某些情况下(例如主机首次接入网络防攻击域，且报文类型不是 TCP)，会出现无法判定的情况，此时也归入 unauth 一类。用户应该约束 unauth 类别的流量，而不建议将此类流量全部丢弃。比较好的方法是采用策略学习，得到正常的分类占比。

功能特性

功能特性	作用
网络防攻击使能	使能网络反攻击功能，部署防护模式
防御协议类攻击	防御 land，smurf、Fraggle 一类的攻击。
全局防护	部署针对经过防火墙的所有流量的策略，避免网络设备自身出现资源耗尽。
基于域的防护	划分网络防攻击保护区域，以该区域为单位实施策略学习和精细的网络防御。

23.1.3.1 网络防攻击使能

网络防攻击在通用平台提供防护功能，根据应用场景，部署防护工作模式。

工作原理

网络防攻击为设备提供网络防护。功能开启后，可以根据相应部署，对设备进行协议类防攻击、。全局防护、基于域的防护。环境中部署了 NAT 则需要设置网络反攻击的模式为 NAT 模式。

相关配置

缺省情况下，网络防攻击能是关闭，缺省工作在非 NAT 模式下。

使用 net-defend enable 命令可以启动和关闭网络防攻击。

使用 net-defend mode 命令可以切换网络防攻击的工作模式。

23.1.3.2 防御协议类攻击

协议类攻击主要利用目标设备上协议栈实现的漏洞，通过发送特定的流量或特定报文(畸形报文)，使目标设备发生异常以达到拒绝服务的目的。常见的协议类攻击包括 LAND、Smurf、Fraggle、TearDrop、WinNuke、异常 TCP 标记、ICMP 重定向攻击、ICMP 不可达攻击、超大 ICMP 报文攻击等。

工作原理

协议类攻击主要是针对协议处理的漏洞而言，通过配置相应的开关，将具有符合攻击特征的报文进行过滤即可。

Land

攻击原理/特征：用于 Land 攻击的数据包中的源地址和目标地址是相同的，早期的操作系统协议栈设计存在缺陷，当操作系统接收到这类数据包时，可能出现不知道该如何处理堆栈中通信源地址和目的地址相同的这种情况或者循环发送和接收该数据包，消耗大量的系统资源，从而有可能造成系统崩溃或死机等现象。

Smurf

攻击原理/特征：该攻击向一个子网的广播地址发一个带有特定请求(如 ICMP 回应请求)的包，并且将源地址伪装成想要攻击的主机地址。子网上所有主机都回应广播包请求而向被攻击主机发包，使该主机受到攻击。攻击者只需要较小的代价，就可以给被攻击主机产生大量的攻击流量。

Fraggle

攻击原理/特征：Fraggle 攻击对 Smurf 攻击作了简单的修改，使用的是 UDP 应答消息而非 ICMP 报文(攻击端口 7(echo)或 19(chargen))。

WinNuke

WinNuke 攻击又称“带外传输攻击”，它的特征是攻击目标端口，被攻击的目标端口通常是 139，而且 URG 位设为 1，即紧急模式。WinNuke 攻击就是利用了 Windows 操作系统的一个漏洞，向这些端口发送一些携带 TCP 带外(OOB)数据报文，但这些攻击报文与正常携带 OOB 数据报文不同的是，其指针字段与数据的实际位置不符，即存在重合。这样 Windows 操作系统在处理这些数据的时候，就会崩溃。通过下述配置，可以有效地进行该类攻击的防御。

ICMP 重定向攻击

攻击原理/特征：ICMP 重定向报文是当主机采用非最优路由发送数据报时，设备会发回 ICMP 重定向报文来通知主机最优路由的存在。一般情况下，设备仅向主机而不向其它设备发送 ICMP 重定向报文，但一些恶意的攻击可能跨越网段向另外一个网络的主机发送虚假的重定向报文，以改变主机的路由表，破坏路由，干扰主机正常的 IP 报文转发，并以此增强其窃听能力。

带源路由选项 IP 报文攻击

攻击原理/特征：为了实现一些附加功能，IP 协议规范在 IP 报头中增加了选项字段，这个字段可以有选择的携带一些数据，以指明中间设备或最终目标计算机对这些 IP 报文进行额外的处理，源路由选项便是其中一个。

源路由选项的目的为指导中间设备如何转发该数据报文，即明确指明了报文的传输路径。例如，让一个 IP 报文明确的经过三台设备 R1，R2，R3，则可以在源路由选项中明确指明这三台设备的接口地址，这样不论三台设备上的路由表如何，这个 IP 报文就会依次经过 R1，R2，R3。而且这些带源路由选项的 IP 报文在传输的过程中，其源地址不断改变，目标地址也不断改变，因此，通过合适的设置源路由选项，攻击者便可以伪造一些合法的 IP 地址，而蒙混进入网络。

相关配置

缺省情况下，防 land 攻击和防 smurf 攻击的功能是启用的，其中防 smurf 攻击没有相应的配置命令可以将其关闭。

使用 defend 命令可以启动和关闭协议类攻击防御的开关。

协议类攻击是独立配置的，对于其他防攻击命令无影响。

协议类攻击的过滤优先于全局防护和基于域的防护。

23.1.3.3 全局防护

全局防护是针对整个防火墙设备实施的防护，其主要目的是为了预防资源消耗类攻击对防火墙设备自身产生的拒绝服务。通过在整机范围内限定会话的消耗速度来确保防火墙设备自身资源的有效使用。

工作原理

网络防攻击域是针对特定区域进行的防护，防火墙上可以划分多个域。但是当攻击流量不属于某个特定的域，或者攻击流量没有固定目标时，这些策略覆盖不到的攻击流量就会对整个网络的带宽造成消耗。如果网络上出现大量的伪造的攻击报文，会导致防火墙在内的各种网络设备的相关资源耗尽，无法为正常业务提供相关的服务。

为了防御这种情况，可以为防火墙配置全局防护。其中，TCP syn cookie 功能能够过滤 TCP SYN flood 攻击；会话限制功能，将从新建会话中把可疑攻击报文过滤出来，并且限制这些可疑报文的传输速率，达到剥离恶意流量，保护防火墙自身服务能力。

防火墙将以下的新建会话定义为未能通过验证的：

1. 无法通过 TCP 源防伪技术（syn-cookie）的 TCP 会话。
2. 非 TCP 新建会话中，发起方到防火墙的跳数（TTL）可疑。

因此，在全局防攻击配置后，所有来自真实源的 TCP 会话将不受干扰的继续运行。而非 TCP 会话则受到防火墙 TTL 学习的影响。

相关配置

测试防火墙性能与容量的时候需要关闭全局防护。使用 defend-zone global 命令可以配置全局防护。

全局防护优先于网络防攻击域实施。

在全局防护中，策略之间的优先级为“未验证会话新建速率限制”优先于“udp、tcp、icmp、other-protocol 的会话速率限制”。

全局防护的缺省配置的阈值较高，仅保障防火墙正常工作。可以通过启用策略自学习来得到更合理的策略配置建议，与防攻击域的策略自学习类似。

23.1.3.4 基于域的防护

配置网络防攻击域是为了将网络中的主机、子网进行分类保护独立管理。不同的主机对象可以适用不同的防护策略，并且可以由不同的管理员进行维护管理。

工作原理

划分网络防攻击域

网络防攻击域通过将主机、子网划分成独立的域，可以在域上部署针对这个域的策略。域之间是独立控制的，可以独立进行策略学习、策略部署等。

配置策略自学习

在配置防御策略之前，用户可以启动策略自动学习功能，通过一段时间的流量监视，给出针对此网络防攻击域较为合理的策略配置建议。用户无法在策略学习期间同时启用手工配置的防御策略，因此在策略学习期内，如果遭受了攻击（例如感觉到网络防攻击域遭受攻击而出现异常等），系统学习的策略水线会不准确，建议用户重新学习策略。策略学习的时间建议不低于 7 天。

策略学习是根据监控期间对应网络防攻击域的各类流量峰值得出的，用户可以选择直接使用这些阈值，也可以选择对这些阈值进行调整，例如将水线适当上浮一定百分比。

配置流量监视

用户在对网络实施安全策略保护时常常会遇到的问题就是不清楚如何有针对性的配置本网络防攻击域的网络防护措施以及阈值。在安全策略实施之前，对网络防攻击域进行流量监控可以很好的帮助用户制定有效的防护措施。

用户在设定防护措施之后，可以通过流量监控结果的比对确定防护效果。甚至于用户可以通过流量监控，发现一些可疑主机并且针对这些可疑主机实施针对性的措施。

建议用户在指定网络防攻击域防护策略之前可以针对网络防攻击域实施 24 小时的流量监控，这样可以更有利于制定出合理的阈值范围。

防火墙可以监控各类协议的实时/历史流量的峰值、均值，针对 TCP 可以罗列具有相关特征的 TOPN 源主机。可以了解域内每台受保护主机的流量状况，对于可疑情况及时作出反应。

> 因为流量监控会对设备的性能带来损耗，因此流量监控功能缺省是关闭的。用户在相关的安全策略工作顺畅之后，可以关闭流量监控，以确保设备能够达到最大的业务处理能力。

配置防攻击策略

用户可以在网络防攻击域上部署防御策略用于防御各类攻击。

- 动态防御策略：针对资源消耗类攻击、蠕虫和网络窥探雷攻击实施的。此类防御策略是根据流量的实时变化而动态产生防护的。针对攻击将产生相应的攻击防御报告。

> 动态防御策略可以根据用户攻击的持续而自动延长防护。即如果一个攻击持续了 1 小时，则在发现攻击后产生的动态防护也将持续 1 小时。在攻击停止 1 小时后，动态防护还将继续保持策略指定的超时时间。

> 对于防护行为为 drop 或者 blocking 的策略，可能无法监视到攻击是否持续，故这些策略可能会在策略指定的超时时间后停止。如果攻击持续，则该策略将重新产生一个相同的防护。这样在攻击报告上会显示为出现多次攻击。

攻击流量可以分为两种，一种源 IP 地址是伪造的还有一种是使用真实的源 IP 地址。若属于前者，则攻击者不需要得到受害者的应答报文，如 TCP SYN Flood 攻击；后者，则攻击者则是通过大量的并发连接、应用服务请求来耗尽主机的资源。防火墙通过防伪机制，剥离伪造流量，对于剩余的来自真实源的流量则限制其连接等方式限制主机的行为，以防止对域内主机造成危害。

动态策略可以防御如下类型的攻击：

(1) 防御伪造源的攻击

对于 TCP 的流量，可以通过 Tcp syn cookie 机制来剥离伪造流量，使进入域的 TCP 流量是真实的。若一个真实的源主机，尚未对网络防攻击域内主机完成三次握手就向网络防攻击域发送非 TCP 的流量，这些流量也可能无法通过真实源 IP 的验证。一旦该主机与网络防攻击域内主机完成了三次握手，那么源自这个主机的非 TCP 流量就能通过真实源 IP 验证。对于未通过真实源验证的流量可以通过丢弃或者限速的方法限制其对网络防攻击内主机的危害。

(2) 来自真实源 IP 的攻击

通过对真实主机的数据统计，发现主机行为的异常，例如并发连接数量、扫描行为等等。

(3) 连接耗尽攻击

攻击者通过耗尽服务器的 TCP 连接数使服务器产生拒绝服务。通过在防火墙上设置策略，可发现此类攻击，并且使用相应的防御措施。

(4) 识别扫描行为

攻击者运用扫描工具探测目标地址/目标服务，对此作出响应的表示目标地址/服务是否存在，用来确定哪些目标系统/服务确实存活着并且连接在目标网络上。通过扫描，攻击者可以寻找他们能够成功攻击的目标主机/服务。连接在网络中的所有计算机都会运行许多使用 TCP 或 UDP 端口的服务，扫描可让攻击者找到可用于发动各种攻击的端口。通常攻击者扫描主机使用 ICMP 协议，扫描端口使用 TCP 协议。从本质上说，端口扫描包括向每一个端口发送消息，每次只发一条。所接收到的响应类型表明该端口是否被使用，进而可以对它进行探测以寻找其弱点。对端口所进行的扫描通常发生在面向连接的 TCP 端口上，所以攻击者会得到有效的反馈信息。网络防攻击的配置扫描检测功能，能够跟踪进出网络防攻击域的主机行为，确认主机行为是否符合扫描特征来判断一台主机是否正在实施扫描。

- 静态防御策略：如黑名单、直通流量、主机的报文限速策略、主机的新建会话速率限制。

  用户可以通过主机的报文限速功能，针对每台主机进出网络防攻击域的流量进行限制，以达到保护主机资源不被过度消耗的目的。

  用户可以通过主机的新建会话速率限制功能，针对每台主机进出网络防攻击域的新建会话速率进行限制，以达到保护主机资源不被过度消耗的目的。

  用户可以通过定义黑名单来阻止指定流量进出网络防攻击域。

  用户可以通过指定直通流量，使部分流量不需要经过网络防攻击的检测。

↘ 记录日志

当系统发生了攻击事件时，用户可以通过 show defend-zone net-defend-zone-name running-protect 看到正在发生的攻击事件。如果用户没有实时跟踪，则可以通过开启记录日志功能，将已经完结的攻击记录到数据库中。这样用户可以看到历史的攻击事件。

相关配置

↘ 划分网络防攻击域

防火墙缺省不会自动划分任何网络防攻击域。

使用 defend-zone 命令可以配置网络防攻击域。

配置网络防攻击域之后，才能够实施针对域的策略自学习和策略部署。

⚠ 出口网关启用 NAT 功能时，如果部署防攻击功能，需要将 NAT 转换前后的 IP 都加入防攻击域，且要求该 NAT 外网 IP 网段相对应的内网 IP 网段都加入该防攻击域。例如 NAT 内网 192.168.1.0/24，对应的 NAT 外网 IP 网段为 110.249.191.0/30，则这两个网段都需要加入该防攻击域保护的 IP 范围。

配置策略自学习

创建网络防攻击域后，不会自动进行策略自学习。

用户需要执行 net-defend learning 命令启动指定网络防攻击域的自学习。

必须在策略部署之前进行策略自学习。

配置流量监控

缺省情况下，不会对网络防攻击域进行任何流量监控。

用户可以配置 traffic-monitor 打开流量监控。

流量监控与防攻击策略可以同时部署。

配置防攻击策略

网络防攻击域缺省是没有部署任何防攻击策略的。

(1) 动态防御策略

防御策略由如下要件构成：

“策略类型”+“流量特征”+“监控对象”+“阈值”+“最小生效时长”+“行动”

策略解读如下：

这是某种**“策略类型”**的策略，当针对某个**“监控对象”**的某种“**流量特征”**超过设定“**阈值”**时必须对采取相应的**“行动”**，该行动执行的时间不小于**“最小生效时长”**。

- 策略类型

关键字	描述
tcp-auth	对于所有由真实源产生的 TCP 业务的可用策略。
tcp-unauth	所有的未通过真实源验证的 TCP 业务可用的策略。
icmp	针对 ICMP 可用的策略。
udp	针对 UDP 可用的策略。
other-protocol	针对除了 TCP/UDP/ICMP 以外的 IP 流量。
scan	针对扫描行为的流量。

- 流量特征

关键字	描述
syns-in	进入网络防攻击域的 TCP SYN 报文速率。
half-conn-in	向网络防攻击域发起的未完成的 TCP 握手的连接数量。

conn-in	向网络防攻击域发起的 TCP 连接数量。
pkt-in	进入网络防攻击域的所有类型的报文。
pkt-out	外出网络防攻击域的所有类型的报文。
unauth-src-in	进入网络防攻击域的未通过真实源验证的报文。
auth-src-in	进入网络防攻击域的来自真实性源主机的报文。

- 监控对象

关键字	描述
dst-ip	针对目的主机实施的监控。由于本类型的策略都是入方向的，也可以理解为针对网络防攻击域内的每一台主机。
src-ip	针对每个源主机实施的监控。由于本类型的策略都是入方向的，也可以理解为针对网络防攻击域外的每一台源主机。
global	监控对象是进入网络防攻击域的所有流量。

- 阈值

触发攻击防御策略的阈值。不同的策略具有不同的阈值单位。

- 最小生效时长

可选项。攻击防护策略一旦被触发，至少需要生效的时间。默认是 60s，时间可调整。在攻击持续的情况下，防护策略会一直生效。

- 行动

关键字	描述
anti-spoofing	防御源 IP 伪造。
limit	根据阈值限制
blocking	阻断指定主机的所有流量。
drop	丢弃策略指定的流量。
notify	仅仅记录攻击行为

(2) 静态防御策略

使用 ratelimit 命令配置限速

使用 bypass 配置直通流量

使用 blacklist 配置黑名单。

(3) 策略之间的优先级（从高到低）:

1) 直通流量（bypass）

2) 黑名单 （blacklist）

3) tcp,udp,icmp,other-protocol 报文防护策略

4) 主机报文限速策略（rate-limit）

5) tcp,udp,icmp,other-protocol 会话防护策略

6)主机新建会话限速策略（session-limit）

对于同一个协议的防护策略，global 优先级高于 src-ip 和 dst-ip，针对报文的过滤优先级高于针对连接数的过滤。

记录日志

防火墙缺省情况下不会记录任何攻击日志。

用户通过 log 命令开启日志记录，此后产生的攻击将被记录到设备的本地数据库中，出口网关可以通过为 **show defend-zone** *net-defend-zone-name* **report** 命令查看。系统记录最多 7 天的日志。

23.1.4 产品说明

NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持防火墙功能；NBR800G、NBR950G、NBR1000G-E、NBR6120-E 、 NBR1300G-E 、 NBR108G-P 、 NBR1700G-E 、 NBR2100G-E 、 NBR2500D-E 、 NBR3000D-E 、NBR3000D-UE、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1500G、NBR2000G 不支持防火墙功能。

23.1.5 配置详解

配置项	配置建议 & 相关命令	
配置防御协议类攻击	可选配置。当用户需要预防此类攻击时配置。	
	defend	启动防御协议类攻击。
配置网络防攻击域	可选配置。当用户需要划分域进行精细的攻击防护时。	
	defend-zone	创建网络防攻击域。
	description	配置网络防攻击域的描述信息。
	ip access-group	配置网络防攻击域关联的 ACL.
	net-defend learning	启动防御策略学习
	可选配置。当用户需要部署针对这个网络防攻击域的防护策略时。	
	tcp-unauth	启动针对未通过源验证的 TCP 流量防护策略
	tcp-auth	启动针对通过源验证的 TCP 流量防护策略
	udp	启动针对 UDP 流量防护策略
	icmp	启动针对 ICMP 流量防护策略
	other-protocol	启动针对除 TCP/UDP/ICMP 之外流量防护策略
	ratelimit	特定流量的限速
	session-limit	特定会话的新建速率限制
	bypass	设置直通流量
	blacklist	设置黑名单

配置全局防护	⚠ 可选配置。全局防攻击对经过防火墙整机的流量进行分类限制以预防网络设备自身出现拒绝服务攻击时。全局防火墙缺省启用，出口网关缺省关闭。	
	defend-zone global	启动全局防护
	net-defend learning	启动防御策略学习
	tcp	设置全局的 TCP syn cookie 代理
	session-limit	设置全局新建会话限速
配置网络防攻击使能	⚠ 必选配置。网络防攻击缺省关闭。	
	net-defend enable	启动网络反攻击功能
	⚠ 可选配置。网络防攻击缺省启用非 NAT 模式	
	net-defend mode { nat | no-nat }	设置网络防攻击模式

23.1.5.1 配置网络防攻击使能

配置效果

开启网络防攻击功能，设置工作模式。

配置方法

根据需要全局模式下配置网络防攻击使能。根据部署场景，设置网络防攻击的工作模式。

检验方法

启动攻击，并且检测是否被出口网关拦截。

相关命令

↘ 启动网络防攻击功能

【命令格式】 net-defend enable

【参数说明】 -

【命令模式】 出口网关：全局配置模式

【使用指导】 默认不开启防攻击功能。进入全局配置模式启动防攻击功能，同时必须开启 ip session tcp-state-inspection-enable fw、ip session track-state-strictly 命令。网络防攻击去使能的时候，需要同时关闭 ip session tcp-state-inspection-enable fw、ip session track-state-strictly 命令。

↘ 设置网络防攻击模式

【命令格式】 net-defend mode { nat | no-nat }

【参数说明】 no-nat：NAT 模式
no-nat：非 NAT 模式
【命令模式】 出口网关：全局配置模式
【使用指导】 网关模式缺省为 NAT 模式；网桥模式缺省为非 NAT 模式。环境中部署了 NAT 则需要设置网络防攻击的模式为 NAT 模式。网桥模式不支持 NAT，不可配置 NAT 模式

配置举例

以下配置举例，仅介绍网络防攻击使能配置。

配置网络防攻击功能使能

【配置方法】
- 出口网关配置网络防攻击使能命令

A

```
A# configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
A(config)# net-defend enable
A(config)# net-defend mode nat
A(config)# exit
```

【检验方法】
- show running 查看配置。

23.1.5.2 配置防御协议类攻击

配置效果

能够过滤包括 LAND、Smurf、Fraggle、TearDrop、WinNuke、异常 TCP 标记、ICMP 重定向攻击、ICMP 不可达攻击、超大 ICMP 报文攻击。

配置方法

根据需要为当前防火墙的全局配置模式下配置针对特定攻击的命令。

检验方法

启动攻击，并且检测是否被防火墙拦截。

相关命令

【命令格式】 defend { winnuke | source-route | route-record | icmp-unreachable | fraggle | land | large-icmp

[*icmp-length*] }

【参数说明】 *Icmp-length*： 单位字节。取值范围 28-65535，未配置 *icmp-length* 参数时缺省是 4000。

【命令模式】 出口网关：全局配置模式

【使用指导】 打开各种协议类攻击的防御开关。

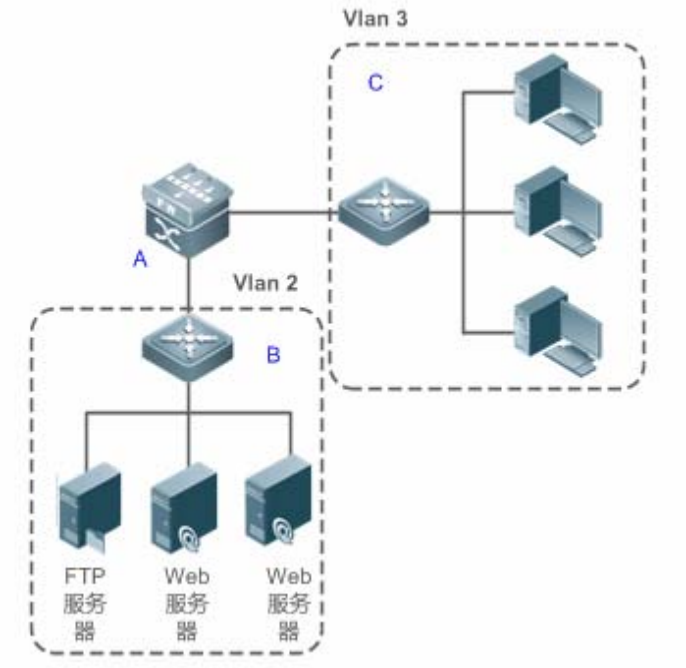
配置举例

以下配置举例，仅介绍协议类攻击防御的配置。

在 IPv4 网络上过滤协议类攻击

【网络环境】

图 23-4



【配置方法】

- 出口网关配置相关的防协议类攻击命令

A

```
A# configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
A(config)# defend winnuke
A(config)# defend source-route
A(config)# defend route-record
A(config)# defend icmp-unreachable
A(config)# defend fraggle
A(config)# defend land
A(config)# defend large-icmp
A(config)# exit
```

【检验方法】

- 发送源和目的 IP 相同的数据包经过出口网关，该数据包将被拦截。

A

```
A# show defend drop
        Drops packet:        5
                Land:                5
```

23.1.5.3 配置全局防护

配置效果

限制经过整个防火墙/出口网关的会话的消耗速度，预防网络设备资源耗尽。

配置方法

在全局配置模式下执行 defend-zone global，在“config-defend-global”配置模式下配置各种限速策略。

检验方法

启动攻击并且检测是否被防火墙/出口网关拦截。

相关命令

↘ 进入全局全局防攻击配置模式

【命令格式】 defend-zone global
【参数说明】 -
【命令模式】 出口网关：全局配置模式
【使用指导】 进入全局防攻击配置

↘ 启动全局防护的策略学习

【命令格式】 net-defend learning global [days days]
【参数说明】 days：策略学习的天数，取值范围 3~60，缺省值为 7。
【命令模式】 特权模式
【使用指导】 全局防护缺省启用，但缺省配置的阈值较高，仅保障防火墙正常工作。可以通过启用策略自学习来得到更合理的策略配置建议，与防攻击域的策略自学习类似。
建议基于策略学习得到的各策略的阈值，进行一定比率的上浮（例如上浮 50%或 100%）后再应用，避免正常流量被误判为攻击而阻断。

↘ 配置防御 TCP SYN Flood 攻击

【命令格式】 tcp { syns-in | half-conn-in } global threshold threshold-num action anti-spoofing
【参数说明】 threshold-num：
当配置 syns 时，单位 pps，范围 1～800,000；

当配置 half-conn 时，单位是半连接数，范围 1 ~ 10,000,000。

【命令模式】 config-defend-global

【使用指导】 当经过防火墙的 syn 报文速率超过阈值或者 TCP 半连接数超过阈值时，启动防攻击。

限制各类会话的建立速度

【命令格式】 session-limit { unauth-src-new-session | tcp | udp | icmp | other-protocol } new-session-per-second

【参数说明】 unauth-src-new-session： 限制所有未验证源的会话新建速率

tcp ： 限制所有 tcp 会话的新建速率

udp ： 限制所有 udp 会话的新建速率

Icmp ：限制所有 icmp 会话的新建速率

other-protocol ： 限制所有除了 tcp/udp/icmp 之外的 ip 报文的会话新建速率

new-session-per-second：每秒新建会话数量 ,取值范围 1~1,000,000

【命令模式】 config-defend-global

【使用指导】 限制各类会话的建立速度。

未验证源的限制优先于其他类型的流量限制。

当一个非 TCP 的新建会话到达防火墙时，防火墙尚未学习到这个网段的 TTL 跳数，则会被归入“未能通过源验证”这一类，而被限制新建。当来自同一网段的任意主机的 TCP 三次握手被防火墙检测到之后，防火墙就可以学习到这个网段的 TTL 跳数，从而解除上述限制。为了减少 TTL 的误判，建议用户配置 session-limit 命令时，设置较大的 new-session-per-second 参数，经过一周左右的 TTL 学习之后，再将会话数限制降低。

全局防护功能可以保障防火墙设备在处理大量攻击流量时提供持续服务的能力。但是如果攻击是专门针对防火墙本机发出的，并且导致防火墙配置管理出现迟滞，则必须增加 NFPP 的防护配置。

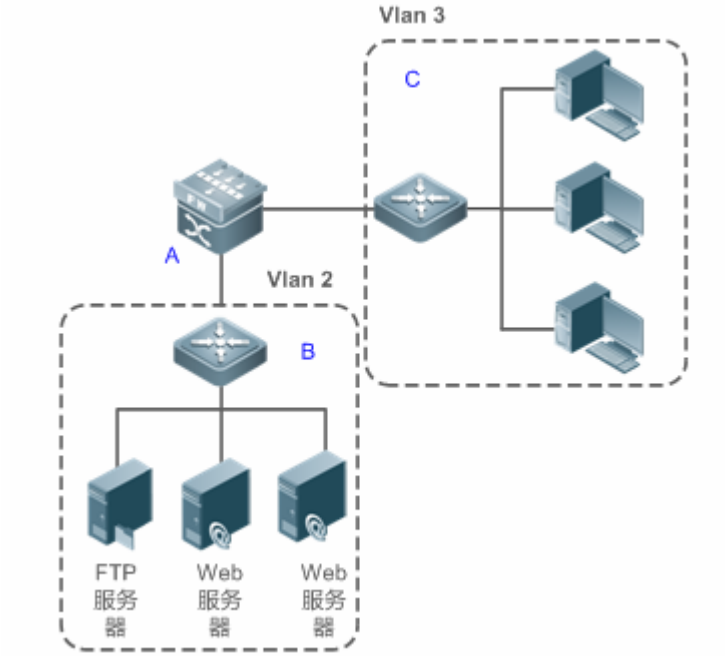
配置举例

以下配置举例，仅介绍全局攻击防御的配置。

启用全局防护

【网络环境】

图 23-5



【配置方法】

A

- 在出口网关上配置相关全局防护命令

```
A# configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
A(config)# defend-zone global
A(config-defend-global)# tcp half-conn-in global threshold 1000 action anti-spoofing
A(config-defend-global)# exit
```

【检验方法】

A

- 发送超过设定阈值的 TCP SYN 报文经过出口网关，超过阈值部分的报文将被拦截。

```
A# show defend drop
        Drops packet:              102
              Global protect:      102
```

常见错误

- 未设定恰当阈值。建议阈值先按照较高上限配置，根据实际情况逐步下调。
- 当用户在核心交换机上插入双防火墙业务模块时，全局防攻击的所有限制参数将减半在每张业务模块上实施。例如用户设定新建 UDP 会话速率不高于每秒 10,000 个。则在每个防火墙业务模块上实施时，单个业务模块的新建会话速率不超过每秒 5,000 个。

23.1.5.4 配置网络防攻击域

配置效果

- 针对某个区域的主机进行独立防护
- 动态策略自学习功能
- 抵御各种攻击类型
- 精细化的流量监视
- 手工指定直通流量与黑名单
- 设定主机限速
- 完整的攻击报告

注意事项

- 动态策略自学习不要与其他防攻击策略同时配置

配置方法

- 创建网络防攻击域
- 启动策略自学习
- 部署防攻击策略

检验方法

- 查看网络防攻击域的状态
- 向网络防攻击域发送攻击报文。
- 检查网络防攻击域的各项报文统计结果与实际数据拦截情况。

相关命令

↘ 建立网络防攻击域

【命令格式】 defend-zone net-defend-zone-name
【参数说明】 net-defend-zone-name：网络防攻击域名称。
【命令模式】 出口网关：全局配置模式
【使用指导】 建立网络防攻击域。

↘ 配置网络防攻击域的描述信息

【命令格式】 description description-string
【参数说明】 description-string：网络防攻击域的描述信息，不超过 100 个字符。
【命令模式】 网络防攻击域配置模式
【使用指导】 配置网络防攻击域的描述信息

关联 ACL

【命令格式】 ip access-group access-list
【参数说明】 access-list：关联的 ip 标准 acl 名称。
【命令模式】 网络防攻击域配置模式
【使用指导】 通过 ACL 指定网络防攻击域的范围。

. 若用户配置的 acl 尚未存在或者是错误的，这条命令依然可以配置上，只是会对用户进行错误提示。用户需要自行校正 acl 关联问题。错误的 acl 关联会导致该功能无法使用。通过执行 show defend-zone web 可知防攻击的工作情况。

. 防攻击关联的 ACL 中的 ACE 数量不超过 200 条。且只支持 access-list id permit {src src-wildcard | host src } ACE 构成的 ACL。(不支持 deny 策略、any 和 time-range 关键字) 当关联的 ACL 不满足此条件时，网络防攻击域不工作。

出口网关启用 NAT 功能时，如果部署防攻击功能，需要将 NAT 转换前后的 IP 都加入防攻击域，且要求该 NAT 外网 IP 网段相对应的内网 IP 网段都加入该防攻击域。例如 NAT 内网 192.168.1.0/24，对应的 NAT 外网 IP 网段为 110.249.191.0/30，则这两个网段都需要加入该防攻击域保护的 IP 范围。

策略自学习

【命令格式】 出口网关：net-defend learning net-defend-zone-name [days days]
【参数说明】 net-defend-zone-name： 网络防攻击域名称。
days：策略学习的天数，取值范围 3~60，缺省值为 7。
【命令模式】 特权模式
【使用指导】 . 防御策略学习给出的策略建议是针对常见的攻击问题产生的策略，并非是防火墙可以部署的所有策略。建议在策略学习期间可以同时开启流量监视，检查进出网络防攻击域的流量与种类，这些信息有助于访问控制的配置。

启用 TCP SYN Flood 防御策略

【命令格式】 出口网关：
tcp-unauth { syns-in | half-conn-in } global threshold threshold-num [timeout seconds] action { anti-spoofing | notify }
【参数说明】 threshold-num：当配置 syns 时，单位 pps，范围 1 ~ 800,000；当配置 half-conn 时，单位是半连接数，范围 1 ~ 10,000,000。
seconds：策略的最小执行时间，单位秒。可配置范围 10 ~ 86400 秒。
【命令模式】 网络防攻击域配置模式
【使用指导】 当进入网络防攻击域的未通过源验证的 SYN 报文速率 (syns-in) 超过阈值或者未完成的 TCP 握手的连接数(half-conn-in)超过阈值时，启动防御机制——即针对进入网络防攻击域的 SYN 报文实施抗伪造技术(anti-spoofing)或者仅仅记录攻击事件，执行时间不少于 seconds。
当针对网络防攻击域内任何一台目的主机(dst-ip)的未通过源验证的 SYN 报文速率超过阈值或者该目的主机的

未完成 TCP 握手的连接数超过阈值时，启动防御机制—--即针对发往该目的主机的所有 SYN 报文实施抗伪造技术(这里采用 syn-cookie 技术)，执行时间不少于 seconds。
此策略可以配置多条。
syn-cookie 使用 tcp cookie 验证技术对实现防源 IP 伪造的能力。syn-cookie 能够通过代理的方式实现对会话源真实性的验证。

针对来自真实源的 TCP 流量的防御策略

【命令格式】 tcp-auth { conn-in | half-conn-in | syns-in } src-ip threshold threshold-num [timeout seconds] action { limit | blocking | notify }

【参数说明】 threshold-num： 当配置 conn-in/half-conn-in 时，单位是连接数，范围 1～10,000,000。当配置 syns-in 时表示 pps，范围 1~800,000。
seconds：策略的最小执行时间，单位秒。可配置范围 10～86400 秒。

【命令模式】 网络防攻击域配置模式

【使用指导】 若任何一个真实的源(src-ip)主机，对网络防攻击域发起的 TCP 并发连接数(conn-in)超过阈值或者未完成握手的 TCP 半连接数（half-conn-in）超过阈值或者发起的 TCP SYN 报文速率超过阈值，设备将启动防御机制----限制并发连接数/限制速率(按照阈值进行限制)、阻塞该源主机对网络防攻击域的所有进出流量（按照策略执行时间进行阻塞）或者仅仅记录攻击事件。策略执行时间不少于 seconds。
此策略可以配置多条。

当配置此策略时，如果并发的流数已经超过指定 threshold-num，则超过部分将被中止。

针对未通过真实源验证的 UDP/ICMP/other-protocol 流量的策略

【命令格式】 出口网关：
{ udp | icmp | other-protocol } unauth-src-in global threshold threshold-num [timeout seconds] action { limit | drop | notify }

【参数说明】 threshold-num： pps，取值 1~100,000,000
seconds：策略的最小执行时间，单位秒。可配置范围 10～86400 秒

【命令模式】 网络防攻击域配置模式

【使用指导】 当进入网络防攻击域的未通过真实源验证的 UDP/ICMP/other-protocol 报文速率超过阈值，设备将启动防御机制---限制这些报文进入网络防攻击域的速率（速率不超过阈值）、全部丢弃此类报文或者仅仅记录攻击事件。
当进入网络防攻击域任何一台目的主机的未通过真实源验证的 UDP/ICMP/other-protocol 报文速率超过水线，设备将启动防御机制---限制这些报文进入该主机的速率（速率不超过阈值）或者全部丢弃针对该主机的此类报文。
此策略可以配置多条。

当配置此策略时，如果并发的流数已经超过指定 threshold-num，则超过部分将被中止。

针对来自真实源主机的 UDP/ICMP/other-protocol 流量的策略

【命令格式】 { udp | icmp | other-protocol } auth-src-in src-ip threshold threshold-num [timeout seconds] action { limit | blocking | notify }

【参数说明】 threshold-num： pps，取值 1~100,000,000
seconds：策略的最小执行时间，单位秒。可配置范围 10～86400 秒

【命令模式】 网络防攻击域配置模式

【使用指导】 当任何真实源主机发出的进入网络防攻击域的 UDP/ICMP/other-protocol 流量速率超过阈值 ,设备将启动防御机制---限制该源主机此类报文进入网络防攻击域的速率（速率不超过阈值）、阻塞该源主机对网络防攻击域的所有进出流量（按照策略执行时间进行阻塞）或者仅仅记录攻击事件。策略执行时间不少于 seconds.
此策略可以配置多条。

限制进入网络防攻击域的 UDP/ICMP/other-protocol 流量

【命令格式】 出口网关：
{ udp | icmp| other-protocol } pkt-in global threshold threshold-num [timeout seconds] action { limit | notify }

【参数说明】 threshold-num： pps，取值 1~100,000,000
seconds：策略的最小执行时间，单位秒。可配置范围 10～86400 秒

【命令模式】 网络防攻击域配置模式

【使用指导】 当进入网络防攻击域的 UDP/ICMP/other-protocol 流量速率超过阈值 ,设备将限制这些流量的速率不超过阈值设定或者仅仅记录攻击事件。策略执行时间不少于 seconds.
当进入网络防攻击域任何目的主机的 UDP/ICMP/other-protocol 流量速率超过阈值 ,设备将限制进入该主机的此类流量的速率不超过阈值设定。策略执行时间不少于 seconds
此策略可以配置多条。

配置防扫描

【命令格式】 scan { in | out } src-ip threshold { low | medium | high } [timeout seconds] action { notify | blocking | notify }

【参数说明】 in：表示防御由外部针对网络防攻击域内的扫描
out：表示防御来自网络防攻击域内部对外的扫描
low/medium/high：表示识别扫描行为的敏感度。
seconds:策略的最小执行时间，单位秒。可配置范围 10～86400 秒

【命令模式】 网络防攻击域配置模式

【使用指导】 防御进出网络防攻击域的扫描行为。此策略可以配置多条。
使用 scan policy 命令进行防扫描的参数调整。

> 防扫描功能灵敏度等级为 low 时不建议开启防 ICMP 不可达攻击。原因是防扫描灵敏度等级为 low 时依赖 ICMP 不可达报文判断扫描攻击，而防 ICMP 不可达攻击会过滤 ICMP 不可达报文，导致防扫描检测漏判。

限制出入网络防攻击域的流量带宽

【命令格式】 出口网关：
ratelimit { in | out } src-ip bandwidth bps-number

【参数说明】 src-ip：针对每个源 IP 进行带宽限制
dst-ip：针对每个目的 IP 进行带宽限制
bps-number： 限制的带宽，单位 bps，取值范围 1~1,000,000,000 bps

【命令模式】 网络防攻击域配置模式

【使用指导】 src-ip 和 dst-ip 都不做配置时，则表示针对网络防攻击域的所有进出流量的限制。如果流量来自未确认真实性的主机，则不会被此策略约束。
此策略可以配置多条。

限制出入网络防攻击域的新建会话速率

【命令格式】 session-limit { in | out } [src-ip | dst-ip] session-rate new-session-per-second

【参数说明】 src-ip：针对每个源 IP 进行新建会话速率限制

dst-ip：针对每个目的 IP 进行新建会话速率限制

new-session-per-second： 限制的新建会话速率，取值范围 1~100,000

【命令模式】 网络防攻击域配置模式

【使用指导】 src-ip 和 dst-ip 都不做配置时，则表示针对网络防攻击域的所有新建会话速率的限制。如果会话来自未确认真实性的主机，则不会被此策略约束。

此策略可以配置多条。

配置直通流量

【命令格式】 出口网关：

bypass src-ip-address [mask src-ip-mask] [proto { tcp | udp | icmp | protocol-num }]

【参数说明】 src-ip-address： 源 IP 地址

src-ip-mask： 源 IP 子网掩码

protocol-num： 协议编号

dest-port-num： 目的端口号

【命令模式】 网络防攻击域配置模式

【使用指导】 设置进入网络防攻击域的直通流量。通过此命令可以允许指定的源 IP 的报文不经过防攻击处理直接进入域；同时也允许从网络防攻击域内相反的方向的报文不经过防攻击处理直接返回。

可以定义多条,命中一条则将此流量作为直通流量。用户配置多条重叠的 bypass 命令并不会被系统自动优化合并。匹配直通流量的报文，将绕过所有的防攻击处理，也不会被防攻击流量监控所统计。

- 报文匹配直通策略后，将不再执行任何其他的网络防攻击域相关的策略。报文若同时命中 bypass 和 blacklist，则 bypass 规则优先执行。
- bypass 配置只对本网络防攻击域有效，对全局策略无效。
- bypass 命令配置使网络防攻击域外主机可以不受防御策略影响，自由访问网络防攻击域内的主机。用户不应该将网络防攻击域内的主机配置为 bypass 命令中的 src-ip-address。
- bypass 不支持自动关联父子流。即，用户如果需要配置访问网络防攻击域 ftp 业务的直通流量，则建议不要配置目的端口号，以免数据通路无法实现流量直通。

配置黑名单

【命令格式】 blacklist ip-address

【参数说明】 ip-address：主机 IP

【命令模式】 网络防攻击域配置模式

【使用指导】 将某一台主机列入黑名单，即禁止该主机针对此网络防攻击域的双向流量

此策略可以配置多个黑名单。

. 与 bypass 不同，用户可以将网络防攻击域内外的主机列入黑名单。一旦列入黑名单，将禁止该主机流量经过防火墙。

配置流量监控

【命令格式】 traffic-monitor { tcp | http | udp | icmp | ip | all }

【参数说明】 -

【命令模式】 网络防攻击域配置模式

【使用指导】 开启各类监控： TCP、HTTP、UDP、ICMP、IP 流量数据。

流量监控可以与策略自学习、防御策略同时部署。

配置日志

【命令格式】 log { tcp-auth | tcp-unauth | icmp | udp | other-protocol | scan | all } [syslog | save]

【参数说明】 --

【命令模式】 网络防攻击域配置模式

【使用指导】 配置日志可以开启指定类型策略的日志记录和打印功能。

此策略可以配置多条。

如果不带 syslog 或者 save 参数时表示同时将攻击信息打印到 syslog 以及数据库中。

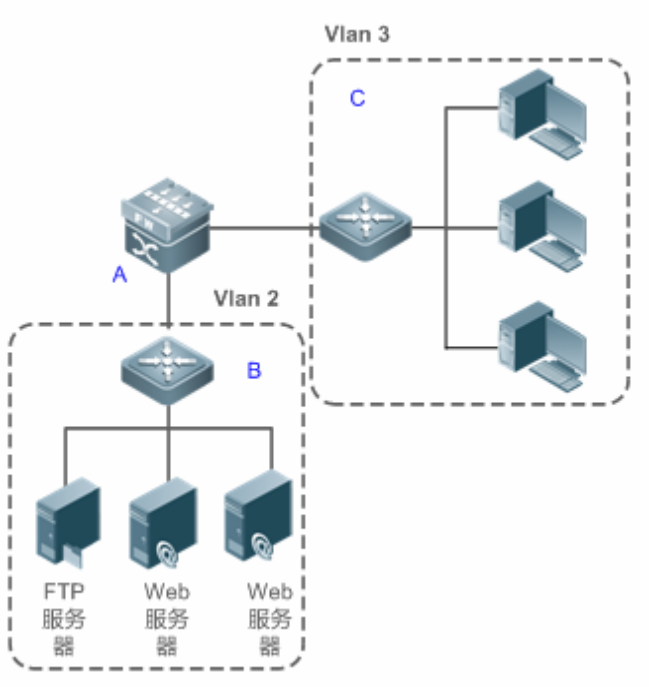
当出现策略阈值设置不合理或者瞬间发生大量攻击时，短时间内产生的大量日志信息可能会出现部分历史丢失的情况。

配置举例

构造网络防攻击域 web，启动网络防攻击域策略自学习和流量监视

【网络环境】

图 23-6



【配置方法】

- 在出口网关上创建网络防攻击域 web ,并且关联 ACL。NAT 场景下该 ACL 需要包含受保护区域的 NAT 内网 IP 和 NAT 外网 IP
- 配置网络防攻击域流量监视
- 启动网络防攻击域策略自学习

A

```
A# configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
A(config)#ip access-list standard servers
A(config-std-nacl)# permit 192.168.1.0 0.0.0.255
A(config-std-nacl)# exit
A(config)# defend-zone web
A(config-defend-zone)# description “Web server zone”
A(config-defend-zone)# ip access-group servers
A(config-defend-zone)# traffic-monitor all
A(config-defend-zone)# exit
A(config)# exit
A# net-defend learning web
```

【检验方法】

- 查看网络防攻击域 web 的状态
- 从外网主机向网络防攻击域中的任一服务器发送各类的流量
- 查看流量流量快照
- 等待 7 天后策略学习结束（如果验证功能可以将时间缩小为 1 天）
- 查看策略学习结果

A

```
A# show defend-zone web
```

```
Description: Web server zone
Zone state: Learning (End time: 2013-03-12 11:24:17)
ACL associated: servers
Traffic monitor: tcp, http, udp, icmp, ip

A# show defend-zone    web traffic-snapshot
                        Total Pkts        current bps
  Received              1234567891        12567893
  Dropped                     0                 0
  Replied               12114             1983

   TCP FLOW:
     Syns in: 672 pps
     Connections(in): 987374
     Half-connections (in): 23453
     Bandwidth (in): 573823453 bps
     Bandwidth (out): 829353321 bps

   HTTP FLOW:
     Syns in:1200 pps
     Connections(in): 987374

    UDP FLOW:
     Pkts (in):289 pps
     Pkts (out):289 pps
     Bandwidth (in): 57382 bps
     Bandwidth (out): 8293 bps

    ICMP FLOW:
     Pkts (in):289 pps
     Pkts (out):289 pps
     Bandwidth (in): 57382 bps
     Bandwidth (out): 8293 bps

    IP FLOW:
     Pkts (in):289 pps
     Pkts (out):289 pps
     Bandwidth (in): 57382 bps
     Bandwidth (out): 8293 bps

A# show net-defend learning    web
```

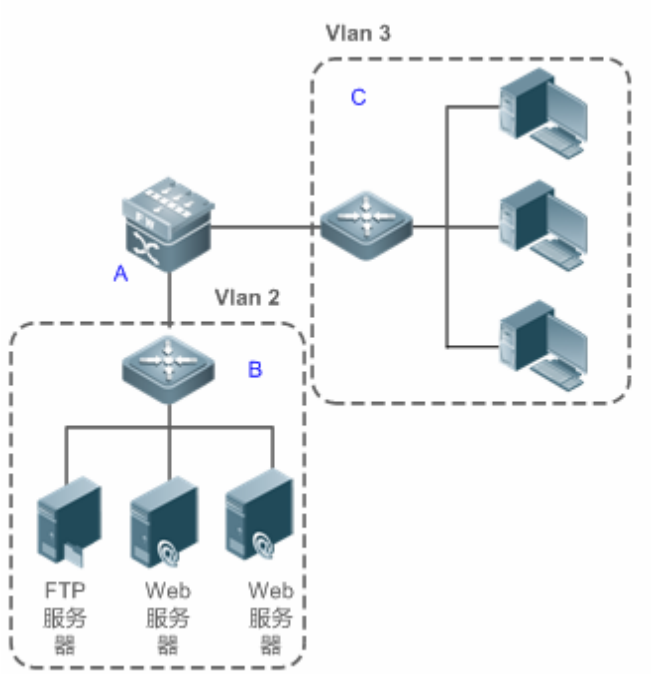
```
Learning status:Learning (End time:2013-03-12 11:24:17)
<TCP flow statistic (in)>
    Every auth-src-ip:
        Max half connection:20
        Max connection: 500
        Max syns (pps): 50
    Global:
        Max half connection: 293829
        Max syns (pps): 1453
<UDP flow statistic (in)>
    Unauth-src UDP flow rate(pps):  2000
    Every auth-src-ip:
        Max UDP flow rate(pps): 1020
    Global:
        Max UDP flow rate(pps): 60345
<ICMP flow statistic (in)>
    Unauth-src ICMP flow rate(pps):  10
    For every auth-src-ip:
        Max ICMP flow rate(pps): 3
<Other-protocol flow statistic (in)>
    Unauth-src Other-protocol flow rate(pps):  0
    For every auth-src-ip:
        Max Other-protocol flow rate(pps): 0

Advices net defend polices for defend-zone  'web'  :
! These policies for anti-spoofing (TCP SYN Flooding Attack)
tcp-unauth half-conn-in global threshold  293829 action anti-spoofing
tcp-unauth syns-in global threshold  1453 action anti-spoofing

! These policies for Client Attack
tcp-auth conn-in src-ip threshold 1000 action notify
tcp-auth half-conn-in src-ip threshold 20 action notify
tcp-auth syns-in src-ip threshold 50 action notify

! These policies for UDP/ICMP/Other-protocol Flooding Attack
udp unauth-src-in global threshold  2000 notify
udp auth-src-in src-ip threshold  1000 notify
udp pkt-in global threshold 60345 action notify
icmp unauth-src-in global threshold 10 timeout 600 notify
icmp auth-src-in src-ip threshold 3 timeout 600 notify
other-protocol unauth-src-in global threshold 10 timeout 600 notify
```

```
other-protocol auth-src src-ip threshold 5 timeout 600 notify
```

↘ 构造网络防攻击域 web，配置防御策略、记录日志

【网络环境】

图 23-7



【配置方法】

- 在出口网关上创建网络防攻击域 web，并且关联 ACL
- 配置网络防攻击域防御策略
- 设置网络防攻击域日志记录

A

```
A# configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
A(config)#ip access-list standard servers
A(config-std-nacl)# permit 192.168.1.0 0.0.0.255
A(config-std-nacl)# exit
A(config)# defend-zone web
A(config-defend-zone)# description “Web server zone”
A(config-defend-zone)# ip access-group servers
A(config-defend-zone)# tcp-unauth half-conn-in global threshold   30000 action anti-spoofing
A(config-defend-zone)# udp unauth-src-in global threshold   10000 notify
A(config-defend-zone)# log all
A(config-defend-zone)# exit
```

【检验方法】

- 查看网络防攻击域 web 的状态
- 从外网向网络防攻击域中的服务器发送发送伪造源的 TCP SYN 和 UDP 流量

- 查看正在发生的攻击（也可以打开 debug 开关得到攻击事件的通知）
- 停止攻击，查看攻击报告

A

```
A# show defend-zone web
    Description: Web server zone
    Zone state: Running
    ACL associated: servers

A# show defend-zone web running-protect
        Defend zone: ‘web’, Total report: 2
        Attack type: ‘TCP SYN Flood’
            id: 823
            Begin:2013-3-5 12:03:04 ,timeout 60s
            Flow: * -> *, Action: Anti-spoofing(syn cookie)
            Policy: tcp-unauth:half-conn:global
            Threshold:30000，current: 30000
            Received:2334354，Replied: 1453467, Dropped:0

        Attack type: ‘UDP Flood (Spoofed)’
            id: 824
            Begin:2013-3-5 12:21:53 ,timeout 60s
            Flow: * -> *, Action: notify
            Policy: udp: unauth-src-in:global
            Threshold:10000，current: 15235
            Received:567749，Replied: 0, Dropped: 0
```

攻击结束后，查看攻击报告：

```
A# show defend-zone    web report 2013-3-5
    Defend zone:’web’, Total report: 2
    Attack type:    ‘TCP SYN Flood’
            2013-3-5 12:03:04 ~ 2013-3-5 13:10:23
            Flow: * -> * ,   Action: Anti-spoofing(syn cookie)
            Policy: tcp-unauth:half-conn:global
            Threshold: 30000, Action:    Anti-spoofing(syn cookie)
            Received: 6343364, Replied: 4362364, Dropped: 0

    Attack type: ‘UDP Flood (Spoofed)’
          2013-3-5 12:21:53 ~ 2013-3-5 13:08:113
            Flow: * -> * ,   Action: notify
            Policy: tcp-unauth:half-conn:global
            Threshold: 10000, Action:    notify
            Received: 4345239, Replied: 0, Dropped: 0
```

常见配置错误

- 关联不支持的 ACL
- 出口网关上启用 NAT 时，防攻击域保护的网段，关联的 ACL 只包含其 NAT 内网 IP，没有包含 NAT 外网 IP 网段，或者外网网段没有完整包含，或者包含的外网网段所应的内网网段没有完全被包含在内。
- 划分过大的网络防攻击域。例如将互联网划入网络防攻击域。这会导致资源过度损耗。
- 当用户在核心交换机上插入双防火墙业务模块时，网络防攻击域的所有策略的限制参数将减半在每张业务模块上实施。例如用户对进入网络防攻击域每一个域内主机的速率不超过 1,000,000bps。则在每个防火墙业务模块上实施时，单个业务模块上进入网络防攻击域每一个域内主机的速率不超过 500,000bps。

23.1.6 监视与维护

清除统计信息信息

⚠ 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
清空网络防攻击域统计信息	出口网关： clear defend-zone net-defend-zone-name counters

查看运行情况

作用	命令
查看防攻击业务模块在线状态	show defend module
查看网络防攻击域状态	出口网关： show defend-zone net-defend-zone-name [counters | host]
查看防攻击丢包统计	出口网关： show defend drop
查看当前流量快照	出口网关： show defend-zone net-defend-zone-name traffic-snapshot { tcp [syns-in | conn-in | half-conn-in | bandwidth] [topn] | http [syns-in | conn-in] | { ip | udp | icmp } [bandwidth | pkts] }
按照策略类型查看当前正发生的攻击	出口网关： show defend-zone net-defend-zone-name running-protect [tcp-auth | tcp-unauth | icmp | udp | other-protocol | scan | protect-id]

按照攻击类型查看当前正在发生的攻击	出口网关： show defend-zone net-defend-zone-name running-protect attack { tcp-syn-flood | tcp-conn-flood | udp-spoof-flood | icmp-spoof-flood | other-spoof-flood | udp-flood | icmp-flood | other-flood | scan }
按照时间查看已经结束的防护	出口网关： show defend-zone net-defend-zone-name report [begin-date [begin-hour] [to end-date [end-hour]]] [tcp-auth | tcp-unauth | icmp | udp | other-protocol | scan | attack { tcp-syn-flood | tcp-conn-flood | udp-spoof-flood | icmp-spoof-flood | other-spoof-flood | udp-flood | icmp-flood | other-flood | scan }]
查看当前防扫描的配置参数	show scan parameter

故障恢复

作用	命令
将当前设备的配置同步到防火墙业务模块上	出口网关： sync defend config [net-defend-zone-name] [force] 当执行 show defend-zone net-defend-zone-name 命令时，网络防攻击域状态显示为“FWM error”时，说明网络防攻击域未能成功配置到防火墙业务模块上。此时可以执行本命令来重新尝试命令同步。

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
打开防攻击数据完整性检查开关	debug netdefend data
打开防攻击管理板和防火墙业务模块交互信息开关	debug netdefend rpc

23.2 安全域

23.2.1 概述

安全域是由一组具有相同安全保护需求，并相互信任的系统组成的逻辑区域，它由同一系统内根据信息的性质、使用主体、安全目标和策略等元素的不同划分而成。每一个逻辑区域有相同的安全保护需求，具有相同的安全访问控制和边界控制策略。划分安全域的目的是把一个大规模的复杂系统的安全问题，转化为更小区域的安全保护问题。当前使用安全域主要是用于访问控制。引入安全域概念以后，管理员将安全需求相同的接口或 IP 地址进行分类（划分到不同的域），能够实现策略的分层管理。比如，首先可以将连接到终端区不同网段的四个接口加入安全域 TERM，连接服务器区的两个接口加入安全域 Server，这样管理员只需要部署这两个域之间的安全策略即可。可见通过引入安全域的概念，可以简化策略的维护复杂度

协议规范

无

23.2.2 典型应用

典型应用	场景描述
利用安全域访问策略进行访问权限控制	以安全域作为基础，配置安全域访问策略，进行访问权限控制。

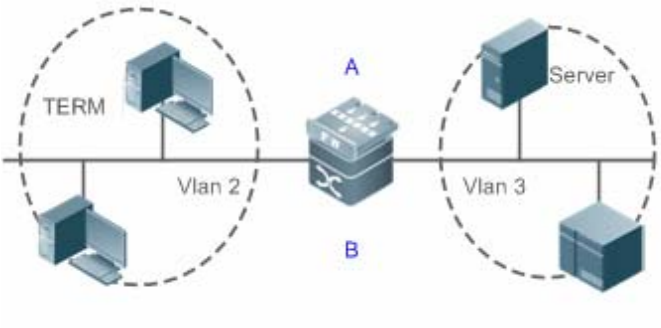
23.2.2.1 利用安全域访问策略进行访问权限控制

应用场景

在一个企业内部利用安全域访问策略进行访问权限控制。

以下图为例，防火墙模块对两个区域（终端区和服务器区）进行访问控制。

图 23-1



功能部属

- 添加两个安全域：TERM 安全域和 Server 安全域。
- 配置安全域访问策略：TERM 安全域只能访问 Server 安全域的特定服务。

23.2.3 功能详解

基本概念

安全域划分方式

安全域划分方式有两种方式 :基于 IP 地址集合来划分安全域和基于网络接口划分安全域。两种安全域配置方法不能同时使用 。缺省情况下是基于接口划分安全域。当前基于 IP 地址集合划分安全域时只支持 IPV4 地址集合，不支持 IPV6 地址集合。

安全域优先级

每个安全域可以配置一个安全域优先级，它控制安全域间的默认互访：高优先级安全域允许访问低优先级安全域，低优先级安全域不允许访问高优先级安全域，默认相同优先级的安全域间也不允许访问。

安全域内策略

安全域内策略用于同一个域内的访问控制，缺省情况下安全域内是不可互访的，除非配置了单个安全域内允许互访或配置全局访问策略允许安全域内互访。

安全域间策略

安全域间策略用于控制跨安全域的访问，用户可通过配置基于安全域的策略来实现安全域间的互访控制，域间策略在源安全域和目的安全域之间维护一个 ACL，该 ACL 中可以配置一系列的匹配规则，以识别出特定的报文，然后根据预先设定的操作允许或禁止该报文通过。除了基于 ACL 的域间访问策略，安全域间的访问控制还有两种配置方式（称为默认互访规则）:

- 通过配置安全域的优先级的方式控制安全域间的互访。
- 通过配置全局访问策略控制相同优先级的安全域间的互访。

安全域间的策略优先级高于默认互访控制规则，只有在安全域间的策略不存在时默认互访控制规则才起作用。

安全域全局访问策略

全局访问策略全局性地控制域内是否允许访问、相同优先级的安全域间是否允许访问。此外还控制匹配安全域策略在连接撤销时是否需要产生日志、违反安全域访问策略而丢弃报文时是否需要产生日志。

和本机的通信（包括本机发出的和到本机的）不受安全域策略的影响。

功能特性

功能特性	作用
基于 IP 地址集合划分安全域	确定安全域的划分方式
基于网络接口划分安全域	确定安全域的划分方式
安全域访问策略	配置从一个安全域到另外一个安全域的访问策略
安全域全局访问策略	控制全局的访问控制策略

23.2.3.1 基于IP地址集合划分安全域

管理员根据特定应用的要求设定安全域同信息系统集合的对应关系：

- 安全域用安全域名称做为唯一标识；
- 信息系统用 IP 地址进行标识，信息系统集合为 IP 地址的集合；

在定义了安全域和信息系统对应关系后，IP 地址无法和安全域的信息系统相匹配的 IP 地址被划入 default 安全域。default 安全域是一个特殊的安全域，默认存在也不能删除。

工作原理

报文到达防火墙模块后，防火墙模块识别出报文的源 IP 地址和目的 IP 地址，将 IP 地址和安全域关联的 ACL 进行匹配，确定报文所属的源安全域和目的安全域。

相关配置

↘ 设置基于 IP 地址集合划分安全域

缺省情况下，安全域的划分方式是基于网络接口的划分方式。

使用 **no security-zone-base interface** 命令将安全域划分方式切换为基于 IP 地址集合的安全域。

切换安全域的划分方式将删除已经配置的所有安全域和安全域访问策略以及全局访问策略。

↘ 配置安全域关联的 ACL

缺省情况下，创建的安全域没有关联 ACL，这时该安全域的配置不完整，不能工作。default 安全域不能配置关联的 ACL，如果报文无法匹配到任何创建的安全域将归属到 default 安全域。

23.2.3.2 基于网络接口划分安全域

管理员根据特定应用的要求设定安全域同网络接口的对应关系：

- 安全域用安全域名称做为唯一标识；

- 设置网络接口所属的安全域；

接口未配置所属安全域的被划入 default 安全域。default 安全域是一个特殊的安全域，默认存在也不能删除。

工作原理

报文到达防火墙模块后，防火墙模块识别出报文的源接口和目的接口，将报文的接口和安全域关联的网络接口进行匹配，确定报文所属的源安全域和目的安全域。

相关配置

设置以网络接口划分安全域

缺省情况下，安全域的划分方式就是基于网络接口的划分方式。

如果安全域划分方式是基于 IP 地址集合，使用 **security-zone-base interface** 命令切换为以网络接口划分安全域。

切换安全域的划分方式将删除已经配置的所有安全域和安全域访问策略以及全局访问策略。

配置接口加入安全域

缺省情况下，创建的安全域没有接口加入，这时该安全域的配置不完整，报文不能匹配到该安全域。default 安全域不能添加接口，如果报文无法匹配到任何创建的安全域将归属到 default 安全域。

使用安全域配置模式下 **interface** 命令将接口加入安全域。

23.2.3.3 安全域访问策略

工作原理

报文到达防火墙模块后 ,防火墙模块根据报文特征识别出报文所属的源安全域和目的安全域 ,如果源安全域不等于目的安全域，这是域间访问，先检查安全域间的访问策略，如果无法找到将比较源安全域和目的安全域的优先级，如果源安全域的优先级高于目的安全域的优先级则允许访问，如果源安全域的优先级低于目的安全域的优先级则不允许访问，如果源安全域的优先级等于目的安全域的优先级则根据一个全局开关判断是否允许优先级相同的安全域间允许访问。同理，如果源安全域等于目的安全域，这是域内访问，先检查是否存在域内的访问策略，如果无法找到将检查单个安全域是否使能允许域内访问，如果还是无法找到将检查一个全局开关判断是否允许域内访问。

基于网络接口划分的安全域支持基于 ACL 和基于对象两种安全域访问策略形态。基于 ACL 的策略的原理是提取 IP 报文的地址、端口信息和策略的 ACL 进行匹配，如果匹配则认为命中该规则，同时根据 ACL 对应的 ACE 属性是 permit 还是 deny 确定报文是允许通过还是禁止通过。基于对象的策略的原理是提取 IP 报文的地址和端口信息，将地址和策略地址对象进行匹配，将端口和策略的服务对象进行匹配，如果命中该规则，根据规则的属性是 permit 还是 deny 确定报文是允许通过还是禁止通过。

> 基于 ACL 和基于对象的访问策略不会同时存在，它受一个配置命令 **security-access-match-object** 控制，缺省是基于 ACL。基于对象的安全域策略当前只支持匹配 IPV4 报文，还不支持匹配 IPv6 报文。

相关配置

↘ 配置报文匹配安全域访问策略时使用对象进行匹配

缺省情况下，报文匹配安全域访问策略时使用 ACL 进行匹配。

使用 **security-access-match-object** 命令设置报文匹配安全域访问策略时使用对象进行匹配。

↘ 配置从一个安全域访问另外一个安全域的 IPV4 报文访问策略(基于 ACL)

缺省情况下，不存在从一个安全域到另外一个安全域的 IPV4 报文访问策略。

使用 **security-access** 命令添加一条从一个安全域到另外一个安全域的 IPV4 报文访问策略。

当规则的源安全域等于目的安全域时表示的是域内访问策略。

当规则的源安全域等于目的安全域时表示的是域内访问策略。

↘ 配置从一个安全域访问另外一个安全域的 IPV4 报文访问策略（基于对象）

缺省情况下，不存在从一个安全域到另外一个安全域的 IPV4 报文访问策略。

使用 **security-access** 命令添加一条从一个安全域到另外一个安全域的 IPV4 报文访问策略。

当规则的源安全域等于目的安全域时表示的是域内访问策略。

↘ 配置安全域访问策略默认增加的序号值

缺省情况下，安全域访问策略默认增加的序号值是 10。

使用 **security-access-step** 命令修改安全域访问策略默认增加的序号值。

23.2.3.4 安全域全局访问策略

全局访问策略全局性地控制安全域间和安全域内的访问策略。

工作原理

参见上一节说明。此外全局访问策略还控制满足安全域策略建立连接或不满足安全域策略丢弃报文时是否产生日志。

相关配置

↘ 设置允许安全域内互相访问

缺省情况下，安全域内访问策略无法匹配时不允许安全域内互相访问。

使用 **loose-inner-zone-access** 命令全局使能在安全域内访问策略无法匹配时允许域内互相访问。

↘ 配置允许相同优先级的安全域互相访问

缺省情况下，安全域间访问策略无法匹配时优先级相同的安全域互相不能访问。

使用 **loose-inter-zone-access** 命令全局使能在安全域间访问策略无法匹配时允许优先级相同的域间互相访问。

配置满足安全域策略在连接撤销时需要产生日志

缺省情况下，满足安全域策略撤销连接时不产生日志。

使用 **security-permit-access-log** 命令后满足安全域策略在连接建立和撤销时需要产生日志。

配置违反安全域访问策略而丢弃报文时需要产生日志

缺省情况下，违反安全域访问策略而丢弃报文时不产生日志。

使用 **security-deny-access-log** 命令后违反安全域访问策略而丢弃报文时需要产生日志。

当前日志以 SYSLOG 的形式输出，启用日志后性能将会有所下降，日志功能仅供故障诊断，建议一般正常情况下不启用。

23.2.4 产品说明

NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持防火墙功能；NBR800G、NBR950G、NBR1000G-E、NBR6120-E 、 NBR1300G-E 、 NBR108G-P 、 NBR1700G-E 、 NBR2100G-E 、 NBR2500D-E 、 NBR3000D-E 、NBR3000D-UE、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1500G、NBR2000G 不支持防火墙功能。

23.2.5 配置详解

配置项	配置建议 & 相关命令	
配置安全域	必须配置。用于创建新的安全域。	
	security-zone-base	配置安全域的划分方式
	security-zone	创建一个安全域或进入已经存在的安全域
	description	配置安全域描述字符串
	security-level	配置安全域优先级
	inner-zone-access	配置单个安全域内访问策略无法匹配时允许安全域内的 IP 互相访问
	interface	配置接口加入安全域
配置安全域访问策略	可选配置。用于配置安全域访问策略。	
	security-access-match-object	配置报文匹配安全域访问策略时使用对象进行匹配
	security-access	配置从一个安全域访问另外一个安全域的 IPV4 报文访问策略
	security-access-step	配置安全域访问策略默认增加的序号值
配置安全域全局访问策略	可选配置。用于配置全局的访问策略。	

	loose-inner-zone-access	全局配置安全域内访问策略无法匹配时允许安全域内的 IP 互相访问。
	loose-inter-zone-access	全局配置安全域间访问策略无法匹配时允许安全域优先级相同的安全域间互相访问。
	security-permit-access-log	配置报文流匹配安全域策略在连接撤销时需要产生日志
	security-deny-access-log	配置违反安全域访问策略而丢弃报文时需要产生日志

23.2.5.1 配置安全域

配置效果

确定安全域划分方式、创建安全域。

注意事项

应先确定安全域划分方式再配置安全域，如果切换安全域划分方式所有已经配置的安全域和安全域访问策略以及全局访问策略都会被删除。

配置方法

↘ 配置安全域的划分方式

- 可选配置，默认是基于接口划分安全域。
- 在特权配置模式下配置。

↘ 创建一个安全域或进入已经存在的安全域

- 可选配置，默认存在一个 default 安全域，通常需要再创建新的安全域。
- 在特权配置模式下配置。

↘ 配置安全域优先级

- 可选配置。在需要利用安全域优先级控制安全域间的访问时需要配置优先级。
- 在安全域模式下配置。

↘ 配置单个安全域内访问策略无法匹配时允许安全域内的 IP 互相访问

- 可选配置。要控制单个安全域内的互访时配置。
- 在安全域模式下配置。

↘ 配置安全域描述字符串

- 可选配置。
- 在安全域模式下配置，建议配置以方便记忆。

配置安全域关联的 ACL

- 基于 IP 地址集合划分的安全域，创建的安全域必须配置。
- 在安全域模式下配置。

配置接口加入安全域

- 基于网络接口划分的安全域，创建的安全域必须配置。
- 在安全域模式下配置。

检验方法

使用安全域的优先级进行访问控制，检查不同安全域间主机的访问控制是否符合安全域的优先级。

相关命令

配置安全域的划分方式

【命令格式】 **security-zone-base interface**

【参数说明】 -

【命令模式】 特权配置模式

【使用指导】

⚠ 当安全域的划分方式发生改变，将清除所有已经配置的安全域和安全域访问策略以及全局访问策略。

⚠ 基于 IP 地址集合划分安全域时，只有对 IPV4 报文会进行安全域的策略判断，IPV6 报文是直接通过的。

创建一个安全域或进入已经存在的安全域

【命令格式】 **security-zone** *zone-name*

【参数说明】 *zone-name*：安全域名称，长度为 1~32 个字符。default 是个保留的安全域名称，不能被创建和删除。

【命令模式】 特权配置模式

【使用指导】 默认存在一个 default 安全域，可以使用 security-zone default 命令进入该安全域配置模式。default 安全域不能被创建和删除。

配置安全域描述字符串

【命令格式】 **description** *string*

【参数说明】 *string*：安全域的描述字符串，长度为 1~40 字符。

【命令模式】 安全域模式

【使用指导】 -

配置安全域优先级

【命令格式】 **security-level** *level-num*

【参数说明】 *level-num*：安全域优先级，取值范围 1~100。数值越大优先级别越高。

【命令模式】 安全域模式

【使用指导】 缺省情况安全域没有优先级，不能用于比较优先级的大小。

配置单个安全域内访问策略无法匹配时允许安全域内的 IP 互相访问

【命令格式】 **inner-zone-access**

【参数说明】 -

【命令模式】 安全域模式

【使用指导】 缺省时单个安全域内访问策略无法匹配时不允许安全域内的 IP 互相访问。此命令优先级高于全局的 **loose-inner-zone-access**。如果未配置这个命令，以全局是否配置了 **loose-inner-zone-access** 为准。

配置接口加入安全域

【命令格式】 **interface** *interface-name*

【参数说明】 *interface-name*：接口的名称

【命令模式】 安全域模式

【使用指导】 一个安全域可以配置多个接口名称，一个接口只能属于一个安全域。

该配置只适合于基于网络接口划分安全域。

default 安全域不允许配置 interface 命令。

非路由模式虚墙下，只有 vlan 接口才可以加入安全域。路由模式虚墙下(route-mode-vfw)，三层物理口、三层 AP 口、虚拟 SVI 接口可以加入安全域

查看全部或单个安全域的配置

【命令格式】 **show security-zone** [*zone-name*]

【参数说明】 *zone-name*：安全域名称。缺省是所有的安全域。

【命令模式】 特权模式、全局模式、接口模式

【使用指导】 显示全部或单个安全域的配置。安全域信息包括：描述字符串、优先级、关联的 access-group 或包含的接口、域内是否允许访问。

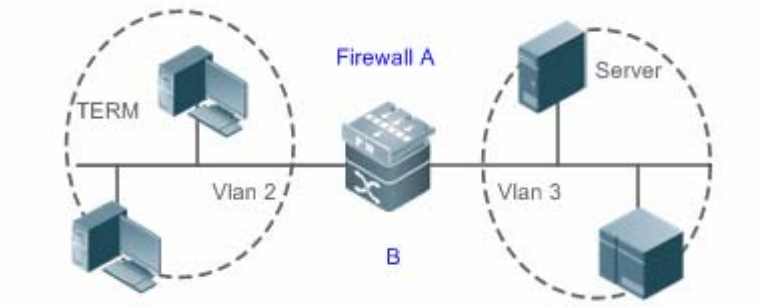
配置举例

以下配置举例，仅介绍与安全域相关的配置。

基于网络接口划分的安全域，使用安全域优先级进行访问控制，要求终端网络区可以自由访问服务器区，服务器区不可访问终端网络区

【网络环境】

图 23-2



【配置方法】

- 将进出 vlan 3 的数据流使用防火墙进行保护，使用 vlan 103 作为引流 VLAN，有关引流 VLAN 的概念请看“防火墙管理”有关的章节。
- 配置基于网络接口划分的安全域，创建两个安全域 TERM 安全域和 Server 安全域，TERM 安全域的优先级高于 Server 安全域的优先级。

B

```
B(config-vfw)#security-zone TERM
B(config-vfw-security-zone)#description terminal_client_zone
B(config-vfw-security-zone)#security-level 80
B(config-vfw-security-zone)#interface vlan 103
B(config-vfw-security-zone)#exit
B(config-vfw)#security-zone Server
B(config-vfw-security-zone)#description server_zone
B(config-vfw-security-zone)#security-level 10
B(config-vfw-security-zone)#interface vlan 3
B(config-vfw-security-zone)#exit
```

【检验方法】 终端区主机可访问服务器区主机，服务器区主机不能访问终端区主机。

B

```
B#show security-zone TERM
security-zone:TERM
description:terminal_client_zone
level: 80
inner-zone access:off
interface member:vlan 103
```

```
B#show security-zone Server
security-zone:Server
description: server_zone
level: 10
inner-zone access:off
interface member:vlan 3
```

常见错误

- 忘记设置安全域优先级，缺省安全域是没有优先级的，这时不能用于比较优先级的高低。

23.2.5.2 配置安全域访问策略

配置效果

配置安全域访问策略，控制不同安全域间的访问。

注意事项

无

配置方法

↘ 配置报文匹配安全域访问策略时使用对象进行匹配

- 可选配置。当报文匹配安全域访问策略时需要使用对象进行匹配时需要配置。
- 在特权配置模式下配置。

↘ 配置从一个安全域访问另外一个安全域的 IPV4 报文访问策略（基于 ACL）

- 可选配置。当需要利用一条关联 ACL 的规则控制从一个安全域到另外一个安全域的访问时需要配置。
- 在特权配置模式下配置。

↘ 配置从一个安全域访问另外一个安全域的 IPV4 报文访问策略（基于对象）

- 可选配置。当需要利用一条关联对象的规则控制从一个安全域到另外一个安全域的访问时需要配置。
- 在特权配置模式下配置。

↘ 配置安全域访问策略默认增加的序号值

- 可选配置。当需要改变安全域访问策略默认递增的序号值时需要配置。
- 在特权配置模式下配置。

检验方法

使用安全域访问策略进行访问控制，检查同一个域的不同主机访问其他域的访问控制是否符合安全域访问策略。

相关命令

↘ 配置

【命令格式】 **security-access-match-object**

【参数说明】 -

【命令模式】 特权配置模式

【使用指导】 当配置 **security-access-match-object** 后已经配置的基于 ACL 的安全域访问策略将被删除。同理当配置 **no security-access-match-object** 后已经配置的基于对象的安全域访问策略将被删除。

该命令只在基于网络接口划分的方式才生效。

基于对象的安全域策略当前只支持匹配 IPV4 报文，还不支持匹配 IPv6 报文。

配置从一个安全域访问另外一个安全域的 IPV4 报文访问策略（基于 ACL）

【命令格式】 **security-access** [**sequence** *sequence-number*]**from** *zone-name* **to** *zone-name access-list* [**inactive**] [**description** *string*]

【参数说明】 *access-list*：关联的 IPV4 ACL

zone-name：安全域名称

sequence-number：序号。其范围是 1 到 2147483647。序号越小越优先匹配。如果命令中没有包含这个序列号，则系统会为这条表项分配一个默认的序列号。第一个表项的默认序列号是 step-number，后续每一个未赋值的表项的默认序列号数值是比最后一个策略序号大 step-number（参见 **security-access-step** 命令）

inactive：规则未激活

string ：描述字符串，长度为 1～31 字符

【命令模式】 特权配置模式

【使用指导】 允许源安全域的名称和目的安全域的名称相同，当二者的名称相同时这条规则是表示安全域内的访问策略。

配置从一个安全域访问另外一个安全域的 IPV4 报文访问策略（基于对象）

【命令格式】 **security-access** [**sequence** *sequence-number*] **from** *zone-name* to *zone-name* { **deny** | **permit** } **src-address-object** *src-object-name* **dest-address-object** *dest-object-name* **service** *serv-name* [**time-range** *time-range-name*] [**inactive**] [**description** *string*]

【参数说明】 *access-list*：关联的 IPV4 ACL

zone-name：安全域名称

sequence-number：序号。其范围是 1 到 2147483647。序号越小越优先匹配。如果命令中没有包含这个序列号，则系统会为这条表项分配一个默认的序列号。第一个表项的默认序列号是 step-number，后续每一个未赋值的表项的默认序列号数值是比最后一个策略序号大 step-number（参见 **security-access-step** 命令）

deny：匹配规则后报文不允许通过

permit：匹配规则后报文允许通过

src-object-name：源地址对象，any_address 是个特殊的地址对象

dest-object-name：目的地址对象，any_address 是个特殊的地址对象

serv-name：服务对象，any_service 是个特殊的服务对象

time-range-name：规则关联的时间段

string：描述字符串，长度为 1～31 字符

inactive：规则未激活

【命令模式】 特权配置模式

【使用指导】 允许源安全域的名称和目的安全域的名称相同，当二者的名称相同时这条规则是表示安全域内的访问策略。

配置安全域访问策略默认增加的序号值

【命令格式】 **security-access-step** *step-number*

【参数说明】 *step-number*：security-access 命令默认递增的序号。

【命令模式】 特权配置模式

【使用指导】 -

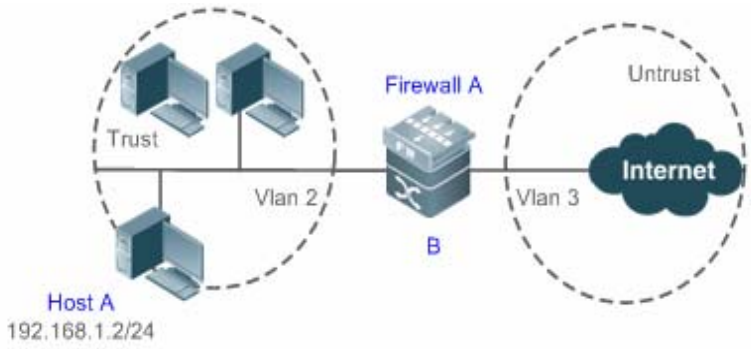
配置举例

以下配置举例，仅介绍与安全域访问策略相关的配置。

基于网络接口划分的安全域，内部网络通过防火墙与 Internet 互联，内部网络属于 Trust 安全域，外部网络属于 Untrust 安全域。只有内部主机 HostA 可以访问 Internet ，其他主机不能访问 Internet。

【网络环境】

图 23-3



【配置方法】

- 将进出 vlan 3 的数据流使用防火墙进行保护，使用 vlan 103 作为引流 VLAN。
- 配置基于网络接口划分的安全域 ,创建两个安全域 Trust 安全域和 Untrust 安全域 ,安全域 Trust 中 HostA 关联到一条安全域访问策略允许访问 Untrust 安全域；其他 Host 没有关联 ACL 不能访问 Untrust 安全域。

B

```
B(config-vfw)#security-zone Trust
B(config-vfw-security-zone)#description trust_zone
B(config-vfw-security-zone)#interface vlan 103
B(config-vfw-security-zone)#exit
B(config-vfw)#security-zone Untrust
B(config-vfw-security-zone)#description internet_zone
B(config-vfw-security-zone)#interface vlan 3
B(config-vfw-security-zone)#exit
B(config-vfw)#security-access 100 from Trust to Untrust
```

【检验方法】 Trust 安全域的 HostA 主机可访问 Internet，其他主机不能访问 Internet。

B

```
B#show security-zone Trust
```

```
security-zone:Trust
description:trust_zone
level not defined
inner-zone access:off
interface member:vlan 103
```

```
B#show security-zone Untrust
security-zone:Untrust
description: internet_zone
level not defined
inner-zone access:off
interface member:vlan 3
```

```
B#show security-access-rules
security-access 100 from Trust to Untrust 10
```

↘ 常见错误

无

23.2.5.3 配置安全域全局访问策略

配置效果

全局控制域内是否允许访问、相同优先级的安全域间是否允许访问。此外它还控制满足安全域策略连接撤销或不满足安全域策略丢弃报文时是否产生日志。

注意事项

无

配置方法

↘ 配置允许安全域内互相访问

- 可选配置。当需要全局性地允许域内访问时配置。
- 在特权配置模式下配置。

↘ 配置允许相同优先级的安全域互相访问

- 可选配置。当需要全局性地使能在安全域间访问策略无法匹配时允许优先级相同的安全域间互相访问时配置。
- 在特权配置模式下配置。

配置满足安全域策略在连接撤销时需要产生日志

- 可选配置。当需要全局性地使能满足安全域策略在连接撤销时要产生日志时配置。
- 在特权配置模式下配置。

配置违反安全域访问策略而丢弃报文时需要产生日志

- 可选配置。当需要全局性地使能违反安全域访问策略而丢弃报文时要产生日志时配置。
- 在特权配置模式下配置。

检验方法

- 验证同一个安全域内访问时使用全局命令 **loose-inner-zone-access** 进行访问控制。
- 验证两个优先级相同的安全域间访问时使用全局命令 **loose-inter-zone-access** 进行访问控制。
- 验证使用 **security-permit-access-log** 控制报文流匹配安全域策略在连接撤销时需要产生日志。
- 验证使用 **security-deny-access-log** 控制违反安全域访问策略而丢弃报文时需要产生日志。

相关命令

全局配置安全域内访问策略无法匹配时允许安全域内的 IP 互相访问

【命令格式】 **loose-inner-zone-access**
【参数说明】 -
【命令模式】 特权配置模式
【使用指导】 该命令优先级低于安全域模式下的 **inner-zone-access** 命令。

全局配置安全域间访问策略无法匹配时允许安全域优先级相同的安全域间互相访问

【命令格式】 **loose-inter-zone-access**
【参数说明】 -
【命令模式】 特权配置模式
【使用指导】 -

配置报文流匹配安全域策略在连接撤销时需要产生日志

【命令格式】 **security-permit-access-log**
【参数说明】 -
【命令模式】 特权配置模式
【使用指导】 该命令一般用于诊断。

配置违反安全域访问策略而丢弃报文时需要产生日志

【命令格式】 **security-deny-access-log**
【参数说明】 -
【命令模式】 特权配置模式

【使用指导】 该命令一般用于诊断。

查看全局安全域访问策略

【命令格式】 **show security-access-global**

【配置模式】 特权模式、全局模式、接口模式

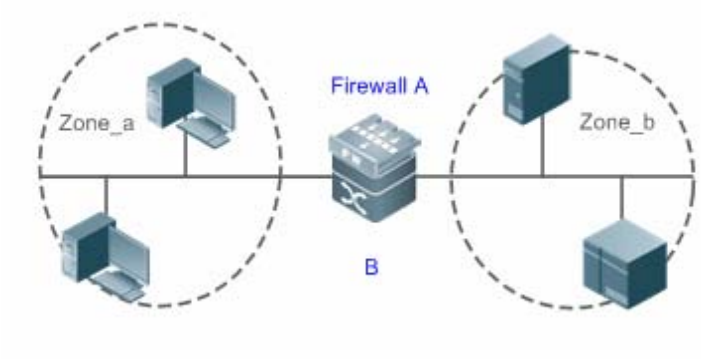
【使用指导】 该命令显示的全局信息有：全局域内是否允许访问、相同优先级的安全域间是否允许访问。此外还显示安全域划分方式、匹配安全域策略在连接撤销时是否需要产生日志、违反安全域访问策略而丢弃报文时是否需要产生日志、安全域访问策略命令递增的序号。

配置举例

基于 IP 地址集合划分的安全域，创建两个安全域，允许两个安全域内部互相访问，允许两个安全域间互相访问。

【网络环境】

图 23-4



【配置方法】

- 将进出 vlan 3（连接 zone_b）的数据流使用防火墙进行保护，使用 vlan 103 作为引流 VLAN。
- 配置基于 IP 地址集合划分的安全域，创建两个安全域 zone_a 安全域（对应网段 192.168.1.0/24）和 zone_b 安全域(对应网段 192.168.2.0/24)，两个安全域优先级相同，配置 loose-inner-zone-access 允许两个安全域内部互相访问，配置 loose-inter-zone-access 允许两个安全域间互相访问，使能报文流匹配安全域策略在连接撤销时需要产生日志，使能违反安全域访问策略而丢弃报文时需要产生日志。

B

```
B(config)#security-zone zone_a
B(config-security-zone)#description Azone
B(config-security-zone)#security-level 80
B(config-security-zone)#exit
B(config)#security-zone zone_b
B(config-security-zone)#description Bzone
B(config-security-zone)#security-level 80
B(config-security-zone)#exit
B(config)#loose-inner-zone-access
B(config)#loose-inter-zone-access
B(config)#security-permit-access-log
B(config)#security-deny-access-log
```

【检验方法】 安全域 zone_a 和 zone_b 内部可以互相访问，zone_a 和 zone_b 间也可以互相访问。报文不论是否匹配安全域策略都会产生日志。

B

```
B#show security-zone zone_a
security-zone:zone_a
description:Azone
leve:80
inner-zone access:off
```

```
B#show security-zone zone_b
security-zone:zone_b
description: Bzone
level:80
inner-zone access:off
```

```
B#show security-access-global
security zone is base ip
inner-zone access:on
inter-zone access between same level:on
permit access log:on
deny access log:on
access statistics:off
access rule step:10
```

常见错误

无

23.2.6 监视与维护

查看运行情况

作用	命令
查看全部或单个安全域的配置。	**show security-zone** [*zone-name*]
查看全局安全域访问策略。	**show security-access-global**
查看安全域 IPV4 报文访问策略。	**show security-access-rules { [from** *zone-name1*] *firewall-name* **| [to** *zone-name2*] }
基于接口划分的安全域，给定 IPV4 报文特征查询安全域策略的匹配情况。	**show security-zone-match** *ip-protocol source-ip dst-ip* **from** *src-interface* **to** *dst-interface*

基于接口划分的安全域，给定 IPV4 TCP或UDP报文特征查询安全域策略的匹配情况。	**show security-zone-match** { **6** | **17** | **tcp** | **udp** } *source-ip dst-ip* [*src-port dst-port*] **from** *src-interface* **to** *dst-interface* *firewall-name*
基于接口划分的安全域，给定 IPV4 ICMP 报文特征查询安全域策略的匹配情况。	**show security-zone-match** { **1** | **icmp** } *source-ip dst-ip* [*type code*] **from** *src-interface* **to** *dst-interface* *firewall-name*

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。

-

配置指南-可靠性

本分册介绍可靠性相关内容，包括以下章节：

1. VRRP
2. RNS

1 VRRP

1.1 概述

VRRP（Virtual Router Redundancy Protocol，虚拟路由冗余协议）是一种路由容错协议。

VRRP 设计采用主备模式，以保证当主路由设备发生故障时，备份路由设备可以在不影响内外数据通信的前提下进行功能切换，且不需要再修改内部网络的参数。VRRP 组内多个路由设备都映射为一个虚拟的路由设备。VRRP 保证同时有且只有一个路由设备在代表虚拟路由设备进行包的发送，而主机则是把数据包发向该虚拟路由设备，这个转发数据包的路由设备被选择成为主路由设备。如果这个主路由设备在某个时候由于某种原因而无法工作的话，则处于备份状态的路由设备将被选择来代替原来的主路由设备。VRRP 使得局域网内的主机看上去只使用了一个路由设备，并且即使在它当前所使用的首跳路由设备失败的情况下仍能够保持路由的连通性。

- VRRP 适用于需要对局域网中设备的路由出口进行冗余备份的场景。

下文仅介绍 VRRP 的相关内容。

协议规范

- RFC2338：Virtual Router Redundancy Protocol
- RFC3768：Virtual Router Redundancy Protocol (VRRP)
- RFC5798：Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6

1.2 典型应用

典型应用	场景描述
路由冗余	局域网中路由设备配置单备份组实现简单的路由冗余。
负载均衡	局域网中路由设备配置多备份组实现流量的负载均衡。

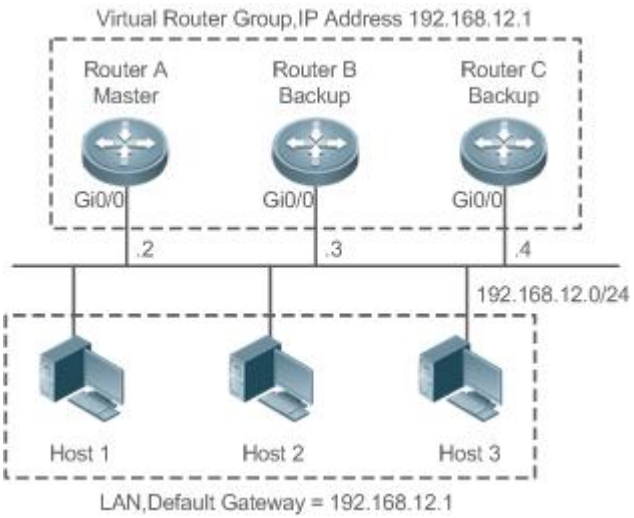
1.2.1 路由冗余

应用场景

在连接局域网的路由设备上配置单备份组，局域网中的主机以该备份组的虚拟 IP 作为默认网关。

- 局域网内主机 1、2 以及 3 发往其它网络的数据包将由选举出来的主路由设备(在 图 1-1 中是路由设备A)进行路由转发。
- 一旦主路由设备 A 失效，将在路由设备 B 与 C 之间选举出新的主路由设备来承担虚拟路由设备的路由转发功能，由此实现了简单路由冗余。

图 1-1



功能部属

- 路由设备 A、B 以及 C 均使用以太网口与局域网连接。
- 路由设备 A、B 以及 C 在与局域网连接的以太网接口上设置了 VRRP。
- 路由设备 A、B 以及 C 在与局域网连接的以太网接口上处于同一个 VRRP 组并且该 VRRP 组的虚拟 IP 地址为 192.168.12.1。
- 局域网内的主机 1、2 以及 3 以虚拟路由设备的 IP 地址 192.168.12.1 作为网关。

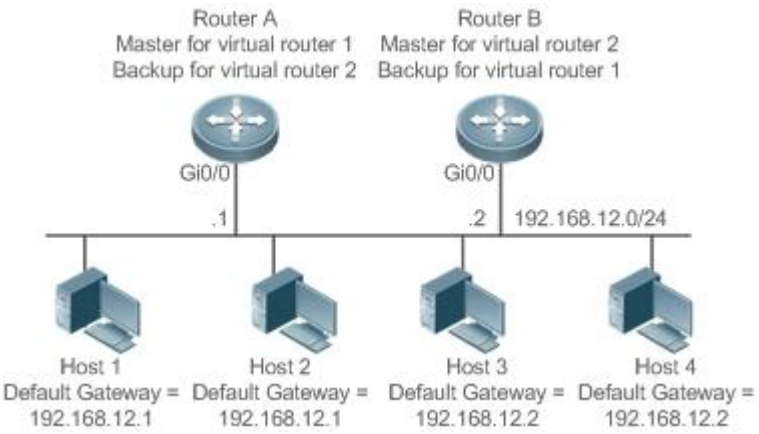
1.2.2 负载均衡

应用场景

在连接局域网的路由设备上配置多个备份组，局域网中的主机分别以各备份组的虚拟 IP 作为网关，路由设备互相作为主路由设备和备份路由设备。

- 以虚拟路由器 1 的虚拟IP地址作为默认网关的主机 1 和 2 发往其它网络的数据包将由主路由设备(在 图 1-2 中是路由设备 A)进行路由转发。
- 以虚拟路由器 2 的虚拟IP地址作为默认网关的主机 3 和 4 发往其它网络的数据包将由主路由设备(在 图 1-2 中是路由设备 B)进行路由转发。
- 路由设备 A 和 B 实现了路由冗余，并同时分担了来自局域网的流量即实现了负载平衡。

图 1-2



功能部属

- 路由设备 A 和 B 均使用以太网口与局域网连接。
- 路由设备 A 和 B 在与局域网连接的以太网接口上设置了两个虚拟路由设备。
- 设置了两个虚拟路由设备。对于虚拟路由设备 1，路由设备 A 使用以太网口 Gi0/0 的 IP 地址 192.168.12.1 作为虚拟路由设备的 IP 地址，这样路由设备 A 就成为主路由设备，而路由设备 B 成为备份路由设备。
- 对于虚拟路由设备 2，路由设备 B 使用以太网口 Gi0/0 的 IP 地址 192.168.12.2 作为虚拟路由设备的 IP 地址，这样路由设备 B 就成为主路由设备，而路由设备 A 成为备份路由设备。
- 在局域网内，主机 1 和主机 2 使用虚拟路由设备 1 的 IP 地址 192.168.12.1 作为默认网关，主机 3 和主机 4 使用虚拟路由设备 2 的 IP 地址 192.168.12.2 作为默认网关。

1.3 功能详解

基本概念

↘ 虚拟路由器

又称 VRRP 备份组，被当作一个共享局域网内主机的缺省网关。 包括一个虚拟路由器标识符和一组虚拟 IP 地址。

↘ 虚拟 IP 地址

虚拟路由器的 IP 地址，一个虚拟路由器可以配置有一个或多个虚拟 IP 地址。

↘ IP 地址拥有者

如果 VRRP 组的虚拟 IP 地址与所在以太网接口上的 IP 一致，那么就认为该 VRRP 组占用(Own)了以太网接口实际 IP 地址，认为该设备是 IP 地址拥有者，此时该 VRRP 组的优先级为 255，如果对应的以太网接口可用，那么该 VRRP 组将自动处于 Master 状态。IP 地址拥有者接收处理目的 IP 地址为虚拟路由器的 IP 地址的报文。

↘ 虚拟 MAC 地址

VRRP 的虚拟 MAC 地址就是协议规定的、由国际标准统一分配的：00-00-5E-00-01-{VRID}，其中前五个字节固定，最后一个字节是备份组的组号。当虚拟路由器回应 ARP 请求时，使用虚拟 MAC 地址，而不是接口的实 MAC 地址。

Master 路由器

在一个 VRRP 备份组中，只有 Master 路由器负责 ARP 响应和转发 IP 数据包。如果该设备是 IP 地址拥有者，通常它将成为 Master 路由器。

Backup 路由器

在一个 VRRP 备份组中，Backup 路由器不承担 ARP 响应和转发 IP 数据包的任务，只负责监听 Master 路由器的状态。当 Master 路由器出现故障时，它们将有机会通过选举成为新的 Master 路由器。

抢占模式

如果 VRRP 组工作在抢占模式，一旦它发现自己的优先级高于当前 Master 的优先级，它将抢占成为该 VRRP 组的主路由设备。

功能特性

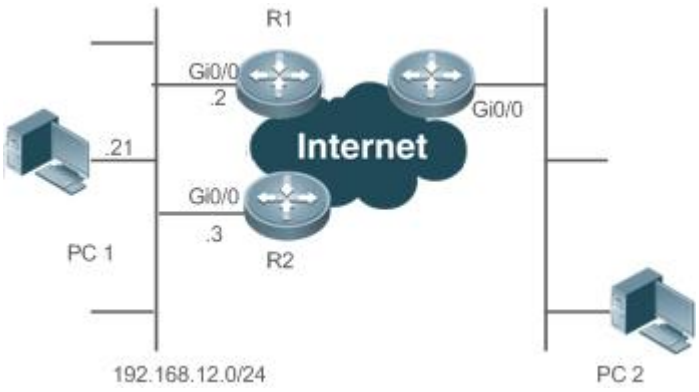
功能特性	作用
VRRP	通过启动 VRRP 功能，VRRP 对共享多存取访问介质（如以太网）上终端设备的默认网关进行冗余备份，从而在其中一台路由设备宕机时，备份路由设备及时接管转发工作，向用户提供透明的切换，提高了网络服务质量。

1.3.1 VRRP

通过启动 VRRP 功能，当主路由设备发生故障时，备份路由设备可以在不影响内外数据通信的前提下进行功能切换，且不需要再修改内部网络的参数。

工作原理

图 1-3 VRRP 工作原理



VRRP 的运作方式

RFC 2338、RFC3768、RFC5798 中定义了 VRRP 类型的 IP 报文格式及其运作机制，VRRP 报文是一类指定目的地址的组播报文，该报文由主路由设备定时发出来标志其运行正常同时该报文也用于选举主路由设备。VRRP 允许为 IP 局域网承担路由转发功能的路由设备失效后，局域网中另外一个路由设备将自动接管失效的路由设备，从而实现 IP 路由的热备份与容错，同时也保证了局域网内主机通讯的连续性和可靠性。一个 VRRP 应用组通过多台路由设备来实现冗余，但是任何时候只有一台路由设备作为主路由设备来承担路由转发功能，其他的为备份路由设备，VRRP 应用组中不同路由设备间的切换对局域网内的主机则是完全透明的。

↘ 路由设备的切换规则

RFC 规定了路由设备的切换规则：

- VRRP 协议采用简单竞选的方法选择主路由设备。首先比较同一个 VRRP 组内的各台路由设备对应接口上设置的 VRRP 优先级的大小，优先级最大的为主路由设备，它的状态变为 Master。若路由设备的优先级相同，则比较对应网络接口的主 IP 地址大小，主 IP 地址大的就成为主路由设备，由它提供实际的路由转发服务。
- 主路由设备选出后，其它路由设备作为备份路由设备(状态变为 Backup)，并通过主路由设备定时发出的 VRRP 报文监测主路由设备的状态。当正常工作时，主路由设备会每隔一段时间发送一个 VRRP 组播报文，称为通告报文，以通知备份路由设备：主路由设备处于正常工作状态。如果组内的备份路由设备在设定的时间段没有接收到来自主路由设备的报文，则将自己状态转为 Master。当组内有多台状态为 Master 路由设备时，重复 1)的竞选过程。通过这样一个过程就会将优先级最大的路由设备选成新的主路由设备，从而实现 VRRP 的备份功能。

一旦在一个 VRRP 备份组选举出它的主路由设备，局域网内的主机将通过主路由设备进行路由转发。

↘ 通讯过程

通讯过程可以由上图来说明。在图中，路由设备 R1 和 R2 均通过以太网口 Gi0/0 与局域网 192.168.12.0/24 连接，路由设备 R1 与 R2 的 Gi 0/0 接口上设置了 VRRP，局域网内的主机都以该 VRRP 组的虚拟路由设备 IP 地址作为默认网关。对于局域网内的主机而言，它们只能感受到由 VRRP 组的虚拟路由设备，而实际承担路由转发功能的 VRRP 组的主路由设备对它们而言则是透明的。譬如，局域网内的主机 PC 1 如果要与其它网络内的主机 PC 2 通讯，PC 1 会以虚拟路由设备为默认网关来发送通向 PC 2 的网络数据包，VRRP 组中的主路由设备在接收到该数据包后会将该数据包转发给 PC 2。在这个通讯过程中，PC 1 只能感受到虚拟路由设备而不知道扮演虚拟路由设备角色的主路由设备究竟是 R1 还是 R2，在这个 VRRP 组中的主路由设备是在 R1 与 R2 之间选举产生的，一旦主路由设备失效，那么另外一台将自动成为主路由设备。

相关配置

↘ 配置启动 VRRP 功能

缺省情况下，接口上 VRRP 功能关闭。

在接口模式下，使用 **vrrp** *group* **ip** *ipaddress* [**secondary**] 或者 **vrrp** *group* **ipv6** *ipv6-address* 命令设置备份组号和虚拟 IP 地址来启用 VRRP 功能。

必须在接口上配置启动 VRRP 功能，才能参与 VRRP 协议工作。

↘ 设置 IPv4 VRRP 的验证字符串

缺省状态下，VRRP 处于无验证模式。

使用 **vrrp group authentication** *string* 命令可以设置 IPv4 VRRP 的验证字符串的同时也设定该 VRRP 组处于明文密码验证模式。在明文密码验证模式下，明文密码长度不能超过 8 个字节。

VRRP 备份组成员必须处于相同的验证模式下才可能正常通讯。明文密码验证模式下，在同一个 VRRP 组中的路由设备必须设置相同的验证口令。明文验证口令不能保证安全性，它只是用来防止/提示错误的 VRRP 配置。

↘ 设置 VRRP 备份组的通告发送间隔

缺省状态下，系统默认主路由设备的 VRRP 通告发送间隔为 1 秒。

使用 **vrrp** [**ipv6**] *group* **timers advertise** { *advertise-interval* | **csec** *centisecond-interval* }可以调整 VRRP 备份组的通告发送间隔。

在没有设置 VRRP 定时设备学习功能的时候，同一个 VRRP 备份组要设置相同的 VRRP 通告发送间隔，否则处于备份状态的路由设备将会丢弃接收到的 VRRP 通告。

↘ 设置路由设备在 VRRP 备份组中的抢占模式

缺省情况下，VRRP 组工作在抢占模式下。

使用 **vrrp** [**ipv6**] *group* **preempt** [**delay** *seconds*] 设置 VRRP 组工作在抢占模式下，可选参数 **delay** *seconds 缺省为 0 秒*。

如果 VRRP 组工作在抢占模式下，一旦它发现自己的优先级高于当前 Master 的优先级，它将抢占成为该 VRRP 组的主路由设备。如果 VRRP 组工作在非抢占模式下，即便它发现自己的优先级高于当前 Master 的优先级，它也不会抢占成为该 VRRP 组的主路由设备。VRRP 组使用以太网接口 IP 地址情况下，抢占模式是否设置意义不大，因为此时该 VRRP 组具有最大优先级，它自动成为该 VRRP 组中的主路由设备。可选参数 Delay Seconds 定义了处于备份状态的 VRRP 路由设备准备宣告自己拥有 Master 身份之前的延迟。

↘ 设置 IPv6 VRRP 虚拟路由器的 Accept_Mode 模式

缺省状态下，IPv6 VRRP 组没有配置 Accept_Mode 模式。

使用 **vrrp ipv6** *group* **accept_mode** 命令可以设置 IPv6 VRRP 组处于 Accept_Mode 模式。

如果配置了 Accept_Mode 模式，则表示 Master 状态的 IPv6 VRRP 虚拟路由器需接收处理任何目的 IP 为虚拟路由器的 IP 地址的报文，如果未配置 Accept_Mode 模式，则表示 Master 状态的 IPv6 VRRP 虚拟路由器需丢弃处理任何目的 IP 为虚拟路由器的 IP 地址的报文，但不丢弃 NA 和 NS 报文。另外，Owner 状态的 IPv6 VRRP Master 状态虚拟路由器，不管有没有配置 Accept_Mode 模式，都会接收处理任何目的 IP 为虚拟路由器的 IP 地址的报文。

↘ 设置路由设备在 VRRP 备份组中的优先级

缺省状态下，VRRP 组默认其优先级为 100。

使用 **vrrp** [**ipv6**] *group* **priority** *level* 可以调整 VRRP 组的优先级。

工作在抢占模式下具有最高优先级并且已获得虚拟 IP 地址的路由设备将成为该备份组的活动的(或主)路由设备，同一个备份组中低于该路由设备优先级的其它路由设备将成为备份的(或监听的)路由设备。

↘ 设置 VRRP 备份组监视的接口

缺省状态下，没有设置 VRRP 备份组监视的接口。

vrrp *group* **track** *interface-type interface-numbe* [*priority*] 或者 **vrrp ipv6** *group* **track** *interface-type interface-numbe* [*priority*]命令可以设置监视接口。

配置了 VRRP 备份组监视的接口后，系统将根据所监视接口的状态动态地调整本路由设备的优先级。一旦所监视的接口状态变为不可用就按照设置的数值减少本路由设备在 VRRP 备份组中的优先级，而此时同一个备份组中接口状态更稳定并且优先级更高的其它路由设备就可以成为该 VRRP 备份组的活动的(或主)路由设备。

设置 VRRP 备份组监视地址

缺省状态下，没有设置 VRRP 备份组监视的 IP 地址。

使用 **vrrp** *group* **track** *ip-address* [**interval** *interval-value*] [**timeout** *timeout-value*] [**retry** *retry-value*] [*priority*]或者 **vrrp** ipv6 *group* **track** *ipv6-address* [**interval** *interval-value*] [**timeout** *timeout-value*] [**retry** *retry-value*] [*priority*] 命令可以设置监视 IP/IPv6 地址。

配置了 VRRP 备份组监视的 IP 地址后，系统将根据所监视的地址是否可达来动态地调整本设备的优先级。一旦所监视的 IP 地址变为不可达，即 ping 不通，就按照设置的数值减少本设备在 VRRP 备份组中的优先级，而此时同一个备份组中优先级更高的其它路由设备就可以成为该 VRRP 备份组的活动的(或主)路由设备。

设置 VRRP 通告定时设备学习功能

缺省状态下，系统没有为 VRRP 组设置定时设备学习功能。

使用 **vrrp** [**ipv6**] *group* **timers learn** 命令设置 VRRP 组启用定时设备学习功能。

一旦启用了定时设备学习功能，如果当前路由设备是 VRRP 备份路由设备，在设置了定时设备学习功能后，它会从主路由设备的 VRRP 通告中学习 VRRP 通告发送间隔，并由此来计算 Master 路由设备失效判断间隔，而不是使用自己本地设置的 VRRP 通告发送间隔来计算。本命令可以实现 Backup 路由设备与 Master 路由设备的 VRRP 通告发送定时设备同步。

设置路由设备在 VRRP 备份组的描述字符串

缺省状态下，系统没有设置 VRRP 组描述符。

使用 **vrrp** [**ipv6**] *group* **description** *text* 命令可以设置 VRRP 组描述符。

为 VRRP 组设置描述符，可以便于区分 VRRP 组。当设置的描述符超过 80 个字节，提示配置错误。

设置 VRRP 备份组延迟启动

缺省状态下，系统没有设置 VRRP 备份组延迟启动。

使用 **vrrp delay** { **minimum** *min-seconds* | **reload** *reload-seconds* }可以设置 VRRP 备份组延迟启动，两种 VRRP 备份组延迟启动时间的取值范围均为 0~60 秒。

本命令配置某个接口上 VRRP 备份组的延迟启动时间；延迟时间有两种：系统启动时的延迟时间，与接口状态变为活动时的延迟时间，可以分别配置，也可同时配置。配置本命令后，当系统启动，或者接口状态变为活动时，该接口上的 VRRP 备份组不会立即启动；而是等待相应的延迟时间后再启动 VRRP 备份组，保证非抢占配置不会失效。如果在延迟启动 VRRP 时该接口上接收到 VRRP 报文，则会取消延迟，立即启动 VRRP 协议。

配置此命令将对接口的 IPv4 VRRP 和 IPv6 VRRP 备份组同时生效。

设置 IPv4 VRRP 的 VRRP 报文发送标准

缺省状态下，IPv4 VRRP 的 VRRP 报文使用 VRRPv2 标准。

使用 **vrrp** *group* **version** { **2 | 3** }命令设置 IPv4 VRRP 的 VRRP 报文发送标准。

参数配置为 2，则 IPv4 VRRP 的 VRRP 报文使用 VRRPv2 标准；参数配置为 3，则 IPv4 VRRP 的 VRRP 报文使用 VRRPv3 标准。

1.4 产品说明



NRB108G-P、NBR800G、NBR950G、NBR1000G-C、NBR1000G-E、NBR6120-E 不支持 VRRP； NBR1500G、NBR2000G、NBR2000G-C、NBR3000G-S、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 VRRP。

NRB108G-P、NBR800G、NBR950G、NBR1000G-C、NBR1000G-E、NBR6120-E 不支持 VRRP 的 ipv6 功能；NBR1500G、NBR2000G、NBR2000G-C、NBR3000G-S、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 VRRP 的 ipv6 功能。

1.5 配置详解

配置项	配置建议 & 相关命令	
配置 IPv4 VRRP	⚠ 必须配置。用于启动 IPV4 VRRP 备份功能。	
	vrrp *group* **ip** *ipaddress* [**secondary**]	启用 IPv4 VRRP
	⚠ 可选配置。用于配置 IPV4 VRRP 备份组参数。	
	vrrp *group* **authentication** *string*	设置 IPv4 VRRP 的验证字符串
	vrrp *group* **timers advertise** { *advertise-interval* | **csec** *centisecond-interval* }	设置 IPv4 VRRP 主路由设备 VRRP 通告间隔
	vrrp *group* **preempt** [**delay** *seconds*]	设置 Ipv4 VRRP 备份组处于抢占模式
	vrrp *group* **priority** *level*	设置 IPv4 VRRPVRRP 备份组的优先级
配置 IPv6 VRRP	⚠ 必须配置。用于启动 IPV6 VRRP 备份功能。	
	ipv6 vrrp enable	全局启用 IPv6 VRRP
	vrrp *group* **ipv6** *ipv6-address*	接口启用 IPv6 VRRP
	⚠ 可选配置。用于配置 IPV6 VRRP 备份组参数。	
	vrrp ipv6 *group* **timers advertise** { *advertise-interval* | **csec** *centisecond-interval* } [**multiplier** *interval*]	设置 IPv6 VRRP 主路由设备 VRRP 通告间隔和超时倍数
	vrrp ipv6 *group* **preempt** [**delay** *seconds*]	设置 IPv6 VRRP 备份组处于抢占模式

	vrrp ipv6 *group* **accept_mode**	设置 IPv6 VRRP 备份组的 Accept_Mode 模式
	vrrp ipv6 *group* **priority** *level*	设置 IPv6 VRRPVRRP 备份组的优先级
	vrrp ipv6 *group* **track** *interface-type interface-number* [**link**] [*interface–priority*]	设置 IPv6 VRRP 备份组监视的接口
	vrrp ipv6 *group* **track** { *ipv6-global-address* | { *ipv6-linklocal-address interface-type interface-number* } } [**interval** *interval-value*] [**timeout** *timeout-value*] [**retry** *retry-value*] [*priority*]	设置 IPv6 VRRP 备份组监视的 IP 地址
	vrrp ipv6 *group* **timers learn**	设置 IPv6 VRRP 定时设备学习功能
	vrrp ipv6 *group* **description** *text*	设置者 IPv6 VRRP 组描述字符串
	vrrp delay { **minimum** *min-seconds* | **reload** *reload-seconds* }	设置接口上 VRRP 备份组延迟启动时间
配置 VRRP+MSTP	VRRP 的基本配置跟 IPv4VRRP 配置一样。	

1.5.1 配置IPv4 VRRP

配置效果

- 配置单备份组时，通过设置备份组号和虚拟 IP 地址，可以在指定的局域网段上添加一个备份组，从而启动对应接口的 VRRP 单备份功能。
- 配置多备份组时，在同一个以太网接口上配置多个 VRRP 备份组，可以实现负载均衡同时通过互相备份来提供更稳定可靠的网络服务。
- 通过设置监视接口，动态的调整备份组的优先级，实现动态故障监测，实现备份组的状态切换。

注意事项

- 同一个 VRRP 备份组内路由设备上 VRRP 需要配置相同的虚拟 IPv4 地址。
- 实现 IPv4 VRRP 多备份组相互备份，需要通过在接口上配置多个相同的 IPv4 VRRP 备份组，且通过配置不同优先级等形式形成互为主备关系，从而实现 IPv4 VRRP 多备份组功能。
- 启动 VRRP 需要在三层口上配置。

配置方法

↘ 启用 IPv4 VRRP

- 默认接口上没有启用 IPv4 VRRP，如果接口要启用 IPv4 VRRP 备份功能则必须配置。

设置 IPv4 VRRP 的验证字符串

- 默认 VRRP 处于无验证模式，如果需要 VRRP 处于明文密码验证模式则配置。

设置 IPv4 VRRP 主路由设备 VRRP 通告间隔

- 默认 VRRP 的主路由设备 VRRP 通告间隔为 1 秒，如果需要手动设置则配置。

设置 Ipv4 VRRP 备份组处于抢占模式

- 默认 VRRP 处于抢占模式，抢占延迟时间缺省为 0 秒。

设置 IPv4 VRRP 备份组的优先级

- 默认 VRRP 组优先级为 100，如果需要手动设置则配置。

设置 IPv4 VRRP 备份组监视的接口

- 默认 IPv4 VRRP 组未配置监视接口，缺省优先级改变值为 10，如果需要通过监视接口来实现故障检测则配置。

设置 IPv4 VRRP 定时设备学习功能

- 默认 VRRP 组未开启定时设备学习功能，如果备份路由设备需要学习主路由设备的 VRRP 通告间隔则配置。

设置 IPv4 VRRP 组描述字符串

- 默认 VRRP 组未配置描述字符串，如果需要便于区分 VRRP 组则配置。

设置接口上 VRRP 备份组延迟启动时间

- 默认 VRRP 组未配置延迟启动时间，如果为了保证非抢占模式不失效则配置。

设置 IPv4 VRRP 的 VRRP 报文标准

- 默认 IPv4 VRRP 使用 VRRPv2 标准，如果需要手动设置则配置。

检验方法

- **show vrrp** 命令显示配置是否生效

相关命令

启用 IPv4 VRRP

【命令格式】 **vrrp** *group* **ip** *ipaddress* [**secondary**]

【参数说明】 *group*：VRRP 组号，不同产品型号取值范围不同。

Ipaddress：虚拟设备的 IP 地址。

secondary：标明是该虚拟设备的次 IP 地址。

【命令模式】 接口模式

【使用指导】 如果不指定虚拟 IP 地址，路由设备就不会参与 VRRP 备份组。如果不使用 Secondary 参数，那么设置的 IP

地址将成为虚拟路由设备的主 IP 地址。

设置 IPv4 VRRP 的验证字符串

【命令格式】 **vrrp** *group* **authentication** *string*

【参数说明】 *group*：VRRP 组号。

string：用于 VRRP 组验证的字符串(不能超过 8 个字节，这里的验证口令是明文口令)。

【命令模式】 接口模式

【使用指导】 在同一个 VRRP 组中的设备必须设置相同的验证口令。明文验证口令不能保证安全性，它只是用来防止/提示错误的 VRRP 配置。

此命令只对 VRRPv2 报文适用，对于 VRRPv3 不适用。

VRRPv3（IPv4 VRRP 和 IPv6 VRRP）已经废除了认证功能，如果用户在 IPv4 VRRP 选择的是 VRRPv2，则对 VRRPv2 生效，如果选择的是 VRRPv3，则对 VRRPv3 不生效。

设置 IPv4 VRRP 主路由设备 VRRP 通告间隔

【命令格式】 **vrrp** *group* **timers advertise** { *advertise-interval* | **csec** *centisecond-interval* }

【参数说明】 *group*：VRRP 组号。

advertise-interval：VRRP 通告发送间隔(以秒为单位)。

csec *centisecond-interval*：备份组中 Master 发送 VRRP 报文的时间间隔。整数形式，取值范围是 50～99。单位是厘秒。无缺省值。

如果 VRRPv2 配置了此命令，则取默认的主设备的通告发送间隔，即 1 秒。

【命令模式】 接口模式

【使用指导】 如果当前设备成为 VRRP 组中的主设备，它将以设定的间隔发送 VRRP 通告来通告自己的 VRRP 状态、优先级以及其它信息。

设置 IPv4 VRRP 备份组处于抢占模式

【命令格式】 **vrrp** *group* **preempt** [**delay** *seconds*]

【参数说明】 *group*：VRRP 组号。

delay *seconds*：准备宣告自己拥有 Master 身份之前的延迟。缺省值为 0 秒。

【命令模式】 接口模式

【使用指导】 如果 VRRP 组工作在抢占模式下，一旦它发现自己的优先级高于当前 Master 的优先级，它将抢占成为该 VRRP 组的主设备。如果 VRRP 组工作在非抢占模式下，即便它发现自己的优先级高于当前 Master 的优先级，它也不会抢占成为该 VRRP 组的主设备。VRRP 组使用以太网接口 IP 地址情况下，抢占模式是否设置意义不大，因为此时该 VRRP 组具有最大优先级，它自动成为该 VRRP 组中的主设备。

设置 IPv4 VRRP 备份组的优先级

【命令格式】 **vrrp** *group* **priority** *level*

【参数说明】 *group*：VRRP 组号。

level：VRRP 组的优先级。

【命令模式】 接口模式

【使用指导】 该命令将手动设置 VRRP 组的优先级。

设置 IPv4 VRRP 备份组监视的接口

【命令格式】 **vrrp** *group* **track** *interface-type interface-number* [*priority*]

【参数说明】 *group*：VRRP 组号。

interface-type interface-number：被监视的接口。

priority：被监视的接口状态改变时其 VRRP 优先级改变的尺度。缺省值为 10。

【命令模式】 接口模式

【使用指导】 被监视的接口只允许是三层可路由的逻辑接口(如 Routed Port、SVI、Loopback 等等)。

如果 VRRP 组占用(Own)了以太网接口实际 IP 地址，此时该 VRRP 组的优先级为 255，不能配置监视接口。

设置 IPv4 VRRP 备份组监视的 IP 地址

【命令格式】 **vrrp** *group* **track** *ipv4-address* [**interval** *interval-value*] [**timeout** *timeout-value*] [**retry** *retry-value*] [*priority*]

【参数说明】 *group*：VRRP 组号。

ipv4-addres：被监视的 IPv4 地址。

interval *interval-value*：发送探测报文的时间间隔。单位为秒。如果不设定，系统缺省值为 3 秒。

timeout *timeout-value*：发送探测报文后等待应答的超时时间。如果超时时间到了，没有收到应答，则认为不可达。单位为秒。如果不设定，系统缺省值为 1 秒。

retry *retry-value*：确认不可达的次数，如果在连续 *retry-value* 次都没有收到应答，则认为不可达。单位为次数，如果不设定，系统缺省值为 3 次。

priority：被监视的接口状态改变时其 VRRP 优先级改变的尺度。缺省值为 10。

【命令模式】 接口模式

【使用指导】 如果是监视主机，对于 IPv4 虚拟路由器，指定主机的 IPv4 地址。

如果 VRRP 组占用(Own)了以太网接口实际 IP 地址，此时该 VRRP 组的优先级为 255，不能配置监视 IP 地址。

设置 IPv4 VRRP 定时设备学习功能

【命令格式】 **vrrp** *group* **timers learn**

【参数说明】 *group*：VRRP 组号。

【命令模式】 接口模式

【使用指导】 一旦启用了定时器学习功能，如果当前设备是 VRRP 备份设备，在设置了定时器学习功能后，它会从主设备的 VRRP 通告中学习 VRRP 通告发送间隔，并由此来计算 Master 设备失效间隔，而不是使用自己本地设置的 VRRP 通告发送间隔来计算。本命令可以实现与 Master 设备的 VRRP 通告发送定时器同步。

设置 IPv4 VRRP 组描述字符串

【命令格式】 **vrrp** *group* **description** *text*

【参数说明】 *group*：VRRP 组号。

text：VRRP 组描述符。

【命令模式】 接口模式

【使用指导】 为 VRRP 组设置描述符，可以便于区分 VRRP 组。当设置的描述符超过 80 个字节，提示配置错误。

设置接口上 VRRP 备份组延迟启动时间

【命令格式】 **vrrp delay** { **minimum** *min-seconds* | **reload** *reload-seconds* }

【参数说明】 **minimum** *min-seconds*：接口状态变为活动时的延迟时间。

reload *reload-seconds*：系统启动时的延迟时间。

【命令模式】 接口模式

【使用指导】 配置本命令后，当系统启动，或者接口状态变为活动时，该接口上的 VRRP 备份组不会立即启动；而是等待相应的延迟时间后再启动 VRRP 备份组，保证非抢占配置不会失效。如果在延迟启动 VRRP 时该接口上接收到 VRRP 报文，则会取消延迟，立即启动 VRRP 协议。两种 VRRP 备份组延迟启动时间的取值范围均为 0~60 秒。

配置此命令将对接口的 IPv4 VRRP 和 IPv6 VRRP 备份组同时生效。

设置 IPv4 VRRP 的 VRRP 报文标准

【命令格式】 **vrrp** *group* **version** { **2** | **3** }

【参数说明】 **2**：使用 VRRPv2 报文发送标准。

3：使用 VRRPv3 报文发送标准。

【命令模式】 接口模式

【使用指导】 对于 IPv4 VRRP 考虑到 VRRPv2 和 VRRPv3 的兼容性问题，用户可以根据网络实际环境选择 VRRP 报文的发送标准。VRRPv2 基于 RFC3768，VRRPv3 基于 RFC 5798。

此命令只适用于 IPv4 VRRP。

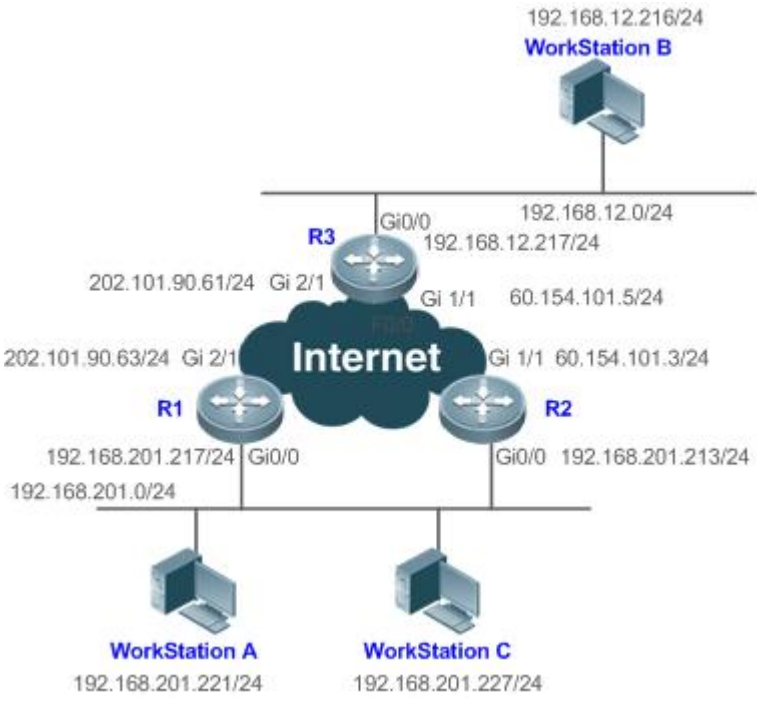
配置举例

以下配置举例，仅介绍与 VRRP 相关的配置。

在 IPv4 的 VRRP 单备份组和监视接口

【网络环境】

图 1-4



【配置方法】
- 用户工作站群(192.168.201.0/24)使用路由设备 R1 与 R2 组成的备份组，并将其网关指向该备份组设置的虚拟路由设备的 IP 地址 192.168.201.1，经由虚拟路由设备 192.168.201.1 访问远程用户工作站群(其工作网络为 192.168.12.0 /24)。
- 路由设备 R1 中设置了 VRRP 监视接口 GigabitEthernet 2/1。
- 路由设备 R3 上没有配置 VRRP 而只是配置了普通路由功能。

R3

```
R3#configure terminal
R3(config)#interface GigabitEthernet 0/0
// “no switchport"命令只有在交换机上才需要
R3(config-if-GigabitEthernet 0/0)#no switchport
R3(config-if-GigabitEthernet 0/0)#ip address 192.168.12.217 255.255.255.0
R3(config-if-GigabitEthernet 0/0)#exit
R3(config)#interface GigabitEthernet 1/1
// “no switchport"命令只有在交换机上才需要
R3(config-if-GigabitEthernet 1/1)#no switchport
R3(config-if-GigabitEthernet 1/1)#ip address 60.154.101.5 255.255.255.0
R3(config-if-GigabitEthernet 1/1)#exit
R3(config)#interface GigabitEthernet 2/1
// “no switchport"命令只有在交换机上才需要
R3(config-if-GigabitEthernet 2/1)#no switchport
R3(config-if-GigabitEthernet 2/1)#ip address 202.101.90.61 255.255.255.0
R3(config-if-GigabitEthernet 2/1)#exit
R3(config)#router ospf
R3(config-router)#network 202.101.90.0 0.0.0.255 area 10
R3(config-router)#network 192.168.12.0 0.0.0.255 area 10
R3(config-router)#network 60.154.101.0 0.0.0.255 area 10
```

R1

```
R1#configure terminal
R1(config)#interface GigabitEthernet 0/0
R1(config-if-GigabitEthernet 0/0)#ip address 192.168.201.217 255.255.255.0
R1(config-if-GigabitEthernet 0/0)#vrrp 1 priority 120
R1(config-if-GigabitEthernet 0/0)#vrrp 1 timers advertise 3
R1(config-if-GigabitEthernet 0/0)#vrrp 1 ip 192.168.201.1
R1(config-if-GigabitEthernet 0/0)#vrrp 1 track GigabitEthernet 2/1 30
R1(config-if-GigabitEthernet 0/0)#exit
R1(config)#interface GigabitEthernet 2/1
R1(config-if-GigabitEthernet 2/1)#ip address 202.101.90.63 255.255.255.0
R1(config-if-GigabitEthernet 2/1)#exit
R1(config)#router ospf
R1(config-router)#network 202.101.90.0 0.0.0.255 area 10
R1(config-router)#network 192.168.201.0 0.0.0.255 area 10
```

R2

```
R2#configure terminal
```

```
R2(config)#interface GigabitEthernet 0/0
R2(config-if-GigabitEthernet 0/0)#ip address 192.168.201.213 255.255.255.0
R2(config-if-GigabitEthernet 0/0)#vrrp 1 ip 192.168.201.1
R2(config-if-GigabitEthernet 0/0)#vrrp 1 timers advertise 3
R2(config-if-GigabitEthernet 0/0)#exit
R2(config)#interface GigabitEthernet 1/1
// “no switchport"命令只有在交换机上才需要
R2(config-if-GigabitEthernet 1/1)#no switchport
R2(config-if-GigabitEthernet 1/1)#ip address 60.154.101.3 255.255.255.0
R2(config-if-GigabitEthernet 1/1)#exit
R2(config)#router ospf
R2(config-router)#network 60.154.101.0 0.0.0.255 area 10
R2(config-router)#network 192.168.201.0 0.0.0.255 area 10
```

【检验方法】 通过 **show vrrp** 命令显示验证。

- 检查当路由设备 R1 在作为 Master 路由设备状态下发现与广域网的接口 GigabitEthernet 2/1 不可用，路由设备 R1 是否降低自己的 VRRP 备份组优先级 30 而成为 90，这样路由设备 R2 就会成为 Master 路由设备。
- 检查当路由设备 R1 发现自己的与广域网的接口 GigabitEthernet 2/1 恢复可用，是否增加自己的 VRRP 备份组优先级 30 而恢复到 120，这样路由设备 R1 将再次成为主路由设备。

R1

```
R1#show vrrp
GigabitEthernet 0/0 - Group 1
  State is Master
  Virtual IP address is 192.168.201.1 configured
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 3 sec
  Preemption is enabled
    min delay is 0 sec
  Priority is 120
  Master Router is 192.168.201.217 (local), priority is 120
  Master Down interval is 10.59 sec
  Tracking state of 1 interface, 1 up:
    up   GigabitEthernet 2/1 priority decrement=30
```

R2

```
R2#show vrrp
GigabitEthernet 0/0 - Group 1
  State is Backup
  Virtual IP address is 192.168.201.1 configured
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 3 sec
  Preemption is enabled
    min delay is 0 sec
```

```
Priority is 100
Master Router is 192.168.201.217 , priority is 120
Master Advertisement interval is 3 sec
Master Down interval is 10.82 sec
```

常见错误

- 同一个 VRRP 备份组内路由设备上 VRRP 的虚拟 IP 地址不一致导致同一个 VRRP 备份组内出现多个 Master 路由设备。
- 同一个 VRRP 备份组内路由设备上 VRRP 的通告发送间隔不一致 ,并且未设置定时设备学习功能导致同一个 VRRP 备份组内出现多个 Master 路由设备。
- 同一个 VRRP 备份组内路由设备上 VRRP 协议报文版本不一致导致同一个 VRRP 备份组内出现多个 Master 路由设备。
- 对于 VRRPv2，同一 VRRP 备份组内各路由设备以太网接口上 VRRP 组验证模式相同均为明文密码模式，但是验证字符串不一致导致同一个 VRRP 备份组内出现多个 Master 路由设备。

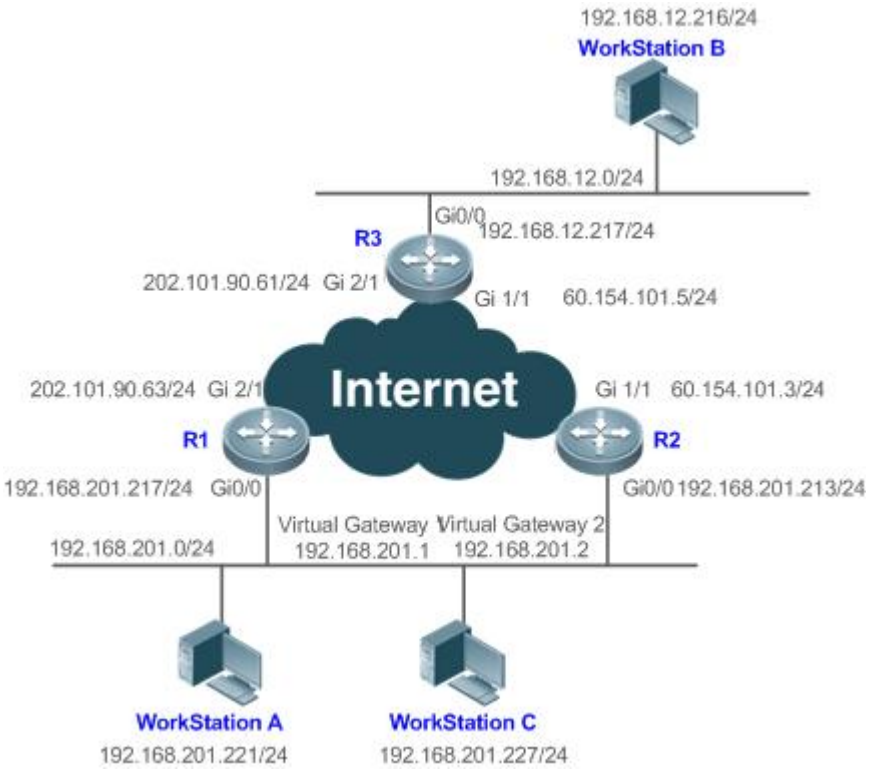
配置举例

以下配置举例，仅介绍与 VRRP 相关的配置。

在 IPv4 的 VRRP 多备份组

【网络环境】

图 1-5



【配置方法】

- 用户工作站群(192.168.201.0/24)使用路由设备 R1 与 R2 组成的备份组 ,其中部分用户工作站(如 A)将其

网关指向备份组 1 的虚拟 IP 地址 192.168.201.1，部分用户工作站(如 C)则将其网关指向备份组 2 的虚拟 IP 地址 192.168.201.2。在所有路由器上启动 IPv4 组播路由功能。

- 路由设备 R1 在备份组 2 中作为主路由设备，在备份组 1 中作为备份路由设备。
- 路由设备 R2 在备份组 2 中作为备份路由设备，在备份组 1 中作为主路由设备。

R3

```
R3#configure terminal
R3(config)#interface GigabitEthernet 0/0
// “no switchport"命令只有在交换机上才需要
R3(config-if-GigabitEthernet 0/0)#no switchport
R3(config-if-GigabitEthernet 0/0)#ip address 192.168.12.217 255.255.255.0
R3(config-if-GigabitEthernet 0/0)#exit
R3(config)#interface GigabitEthernet 1/1
// “no switchport"命令只有在交换机上才需要
R3(config-if-GigabitEthernet 1/1)#no switchport
R3(config-if-GigabitEthernet 1/1)#ip address 60.154.101.5 255.255.255.0
R3(config-if-GigabitEthernet 1/1)#exit
R3(config)#interface GigabitEthernet 2/1
// “no switchport"命令只有在交换机上才需要
R3(config-if-GigabitEthernet 2/1)#no switchport
R3(config-if-GigabitEthernet 2/1)#ip address 202.101.90.61 255.255.255.0
R3(config-if-GigabitEthernet 2/1)#exit
R3(config)#router ospf
R3(config-router)#network 202.101.90.0 0.0.0.255 area 10
R3(config-router)#network 192.168.12.0 0.0.0.255 area 10
R3(config-router)#network 60.154.101.0 0.0.0.255 area 10
```

R1

```
R1#configure terminal
R1(config)#interface GigabitEthernet 0/0
R1(config-if-GigabitEthernet 0/0)#ip address 192.168.201.217 255.255.255.0
R1(config-if-GigabitEthernet 0/0)#vrrp 1 timers advertise 3
R1(config-if-GigabitEthernet 0/0)#vrrp 1 ip 192.168.201.1
R1(config-if-GigabitEthernet 0/0)#vrrp 2 priority 120
R1(config-if-GigabitEthernet 0/0)#vrrp 2 timers advertise 3
R1(config-if-GigabitEthernet 0/0)#vrrp 2 ip 192.168.201.2
R1(config-if-GigabitEthernet 0/0)#vrrp 2 track GigabitEthernet 2/1 30
R1(config-if-GigabitEthernet 0/0)#exit
R1(config)#interface GigabitEthernet 2/1
R1(config-if-GigabitEthernet 2/1)#ip address 202.101.90.63 255.255.255.0
R1(config-if-GigabitEthernet 2/1)#exit
R1(config)#router ospf
R1(config-router)#network 202.101.90.0 0.0.0.255 area 10
R1(config-router)#network 192.168.201.0 0.0.0.255 area 10
```

R2

```
R2#configure terminal
R2(config)#interface GigabitEthernet 0/0
R2(config-if-GigabitEthernet 0/0)#ip address 192.168.201.213 255.255.255.0
R2(config-if-GigabitEthernet 0/0)#vrrp 1 ip 192.168.201.1
R2(config-if-GigabitEthernet 0/0)#vrrp 1 timers advertise 3
R2(config-if-GigabitEthernet 0/0)#vrrp 1 priority 120
R2(config-if-GigabitEthernet 0/0)#vrrp 2 ip 192.168.201.2
R2(config-if-GigabitEthernet 0/0)#vrrp 2 timers advertise 3
R2(config-if-GigabitEthernet 0/0)#exit
R2(config)#interface GigabitEthernet 1/1
R2(config-if-GigabitEthernet 1/1)#ip address 60.154.101.3 255.255.255.0
R2(config-if-GigabitEthernet 1/1)#exit
R2(config)#router ospf
R2(config-router)#network 60.154.101.0 0.0.0.255 area 10
R2(config-router)#network 192.168.201.0 0.0.0.255 area 10
```

【检验方法】 通过 **show vrrp** 命令显示验证。

- 检查当路由设备 R1 在 VRRP 组 2 中作为 Master 路由设备状态下发现与广域网的接口 GigabitEthernet 2/1 不可用，路由设备 R1 是否降低自己的 VRRP 备份组优先级 30 而成为 90，这样 VRRP 组 2 中路由设备 R2 就会成为 Master 路由设备。
- 检查当路由设备 R1 发现自己的与广域网的接口 GigabitEthernet 2/1 恢复可用，是否增加自己的 VRRP 备份组优先级 30 而恢复到 120，这样路由设备 R1 将再次成为 VRRP 组 2 主路由设备。

R1

```
R1#show vrrp
GigabitEthernet 0/0 - Group 1
  State is Backup
  Virtual IP address is 192.168.201.1 configured
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 3 sec
  Preemption is enabled
    min delay is 0 sec
  Priority is 100
  Master Router is 192.168.201.213 , priority is 120
  Master Advertisement interval is 3 sec
  Master Down interval is 10.82 sec
GigabitEthernet 0/0 - Group 2
  State is Master
  Virtual IP address is 192.168.201.2 configured
  Virtual MAC address is 0000.5e00.0102
  Advertisement interval is 3 sec
  Preemption is enabled
    min delay is 0 sec
```

```
  Priority is 120
  Master Router is 192.168.201.217 (local), priority is 120
  Master Advertisement interval is 3 sec
  Master Down interval is 10.59 sec
  Tracking state of 1 interface, 1 up:
    up   GigabitEthernet 2/1 priority decrement=30
```

R2

```
R2#show vrrp
GigabitEthernet 0/0 - Group 1
  State is Master
  Virtual IP address is 192.168.201.1 configured
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 3 sec
  Preemption is enabled
    min delay is 0 sec
  Priority is 120
  Master Router is 192.168.201.213 (local), priority is 120
  Master Advertisement interval is 3 sec
  Master Down interval is 10.59 sec
GigabitEthernet 0/0 - Group 2
  State is Backup
  Virtual IP address is 192.168.201.2 configured
  Virtual MAC address is 0000.5e00.0102
  Advertisement interval is 3 sec
  Preemption is enabled
    min delay is 0 sec
  Priority is 100
  Master Router is 192.168.201.217 , priority is 120
  Master Advertisement interval is 3 sec
  Master Down interval is 10.82 sec
```

常见错误

- 同一个 VRRP 备份组内路由设备上 VRRP 的虚拟 IP 地址不一致导致同一个 VRRP 备份组内出现多个 Master 路由设备。
- 同一个 VRRP 备份组内路由设备上 VRRP 的通告发送间隔不一致 ,并且未设置定时设备学习功能导致同一个 VRRP 备份组内出现多个 Master 路由设备。
- 同一个 VRRP 备份组内路由设备上 VRRP 协议报文版本不一致导致同一个 VRRP 备份组内出现多个 Master 路由设备。
- 对于 VRRPv2，同一 VRRP 备份组内各路由设备以太网接口上 VRRP 组验证模式相同均为明文密码模式，但是验证字符串不一致导致同一个 VRRP 备份组内出现多个 Master 路由设备。

1.5.2 配置IPv6 VRRP

配置效果

- 配置 IPv6 VRRP 单备份组，通过设置备份组号和虚拟 IPv6 地址，可以在指定的局域网段上添加一个备份组，从而启动对应接口的 VRRP 单备份功能。
- 配置 IPv6 VRRP 多备份组，在同一个以太网接口上配置多个 IPv6 VRRP 备份组，可以实现负载均衡同时通过互相备份来提供更稳定可靠的网络服务。
- 通过设置监视接口，动态的调整备份组的优先级，实现动态故障监测，实现备份组的状态切换。

注意事项

- 同一个 VRRP 备份组内路由设备上 VRRP 需要配置相同的虚拟 IPv6 地址。
- 实现 IPv6 VRRP 多备份组相互备份，需要通过在接口上配置多个相同的 IPV6 VRRP 备份组，且通过配置不同优先级等形式形成互为主备关系，从而实现 IPv6 VRRP 多备份组功能。
- 启动 VRRP 需要在三层口上配置。
- 在插入 CB 线卡的 N18K 设备上，如果要使用 IPv6 VRRP，必须先在全局模式下开启 IPv6 VRRP 功能。

配置方法

全局启用 IPv6 VRRP

- 在插入 CB 线卡的 N18K 设备上才支持全局开启、关闭 IPv6 VRRP。默认全局没有启用 IPv6 VRRP ,如果全局要启用 IPv6 VRRP 备份功能则必须配置。

接口启用 IPv6 VRRP

- 默认接口上没有启用 IPv6 VRRP，如果接口要启用 IPv6 VRRP 备份功能则必须配置。

设置 IPv6 VRRP 主路由设备 VRRP 通告间隔

- 默认 VRRP 的主路由设备 VRRP 通告间隔为 1 秒，如果需要手动设置则配置。

设置 IPv6 VRRP 备份组处于抢占模式

- 默认 VRRP 处于抢占模式，抢占延迟时间缺省为 0 秒。

设置 IPv6 VRRP 备份组的 Accept_Mode 模式

- 默认 IPv6 VRRP 未配置 Accept_Mode 模式，如果要求处于 Master 状态的 IPv6 VRRP 虚拟路由器接收处理目的 IP 地址为虚拟路由器的 IP 地址的报文，则配置 Accept_Mode 模式。

设置 IPv6 VRRP 备份组的优先级

- 默认 VRRP 组优先级为 100，如果需要手动设置则配置。

设置 IPv6 VRRP 备份组监视的接口

- 默认 IPv6 VRRP 组未配置监视接口，缺省优先级改变值为 10，如果需要通过监视接口来实现故障检测则配置。

设置 IPv6 VRRP 备份组监视的 IP 地址

- 默认 IPv6 VRRP 组未配置监视 IP 地址，缺省优先级改变值为 10，如果需要通过监视接 IP 地址来实现故障检测则配置。

设置 IPv6 VRRP 定时设备学习功能

- 默认 VRRP 组未开启定时设备学习功能，如果备份路由设备需要学习主路由设备的 VRRP 通告间隔则配置。

设置 IPv6 VRRP 组描述字符串

- 默认 VRRP 组未配置描述字符串，如果需要便于区分 VRRP 组则配置。

设置接口上 VRRP 备份组延迟启动时间

- 默认 VRRP 组未配置延迟启动时间，如果为了保证非抢占模式不失效则配置。

检验方法

- **show ipv6 vrrp** 命令显示配置是否生效

相关命令

全局启用 IPv6 VRRP

【命令格式】 **ipv6 vrrp enable**
【参数说明】 无
【命令模式】 全局模式
【使用指导】 在插入 CB 线卡的 N18K 设备上才支持该命令。
若要关闭 IPv6 VRRP 功能，使用 **no ipv6 vrrp enable 命令**

接口启用 IPv6 VRRP

【命令格式】 **vrrp** *group* **ipv6** *ipv6-address*
【参数说明】 *group*：VRRP 组号，不同产品型号取值范围不同。
ipv6-address：虚拟设备的 IPv6 地址。
【命令模式】 接口模式
【使用指导】 IPv6 的 VRRP 与 IPv4 的 VRRP 共用 1～255 的组号。同一个接口一个相同的 VRRP 组号可以同时适用于 IPv4 VRRP 和 IPv6 VRRP。第一个配置的地址必须是链路本地地址，链路本地地址必须在其它虚拟地址删除后才能删除。

设置 IPv6 VRRP 主路由设备 VRRP 通告间隔

【命令格式】 **vrrp ipv6** *group* **timers advertise** { *advertise-interval* | **csec** *centisecond-interval* } [**multiplier** *interval*]

【参数说明】 *group*：VRRP 组号。

advertise-interval：VRRP 通告发送间隔(以秒为单位)。

csec *centisecond-interval*：备份组中 Master 发送 VRRP 报文的时间间隔。整数形式，取值范围是 50～99。单位是厘秒。无缺省值。只对 VRRPv3 生效，如果 VRRPv2 配置了此命令，则取默认的主设备的通告发送间隔，即 1 秒。

multiplier *interval*：超时倍数，缺省是 3

【命令模式】 接口模式

【使用指导】 如果当前设备成为 VRRP 组中的主设备，它将以设定的间隔发送 VRRP 通告来通告自己的 VRRP 状态、优先级以及其它信息。

根据 RFC 标准，组播报文发送标准为 VRRPv3 的 IPv6 VRRP 备份组，其组播报文中最大的报文通告间隔为 40 秒，所以如果配置的报文通告间隔超过 40 秒，则取最大的通告间隔 40 秒，但该通告间隔配置是生效的。

设置 IPv6 VRRP 备份组处于抢占模式

【命令格式】 **vrrp ipv6** *group* **preempt** [**delay** *seconds*]

【参数说明】 *group*：VRRP 组号。

delay *seconds*：准备宣告自己拥有 Master 身份之前的延迟。缺省值为 0 秒。

【命令模式】 接口模式

【使用指导】 如果 VRRP 组工作在抢占模式下，一旦它发现自己的优先级高于当前 Master 的优先级，它将抢占成为该 VRRP 组的主设备。如果 VRRP 组工作在非抢占模式下，即便它发现自己的优先级高于当前 Master 的优先级，它也不会抢占成为该 VRRP 组的主设备。VRRP 组使用以太网接口 IP 地址情况下，抢占模式是否设置意义不大，因为此时该 VRRP 组具有最大优先级，它自动成为该 VRRP 组中的主设备。

设置 IPv6 VRRP 备份组的 Accept_Mode 模式

【命令格式】 **vrrp ipv6** *group* **accept_mode**

【参数说明】 *group*：VRRP 组号。

【命令模式】 接口模式

【使用指导】 缺省情况下，Master 状态的 IPv6 VRRP 是不允许接收目的 IPv6 地址为虚拟路由器的 IPv6 地址的报文的。但是 NA 和 NS 报文不管是否配置 Accept_Mode 都必须接收。另外，Owner 状态的 IPv6 VRRP Master 状态虚拟路由器，不管有没有配置 Accept_Mode 模式，都会接收处理任何目的 IPv6 为虚拟路由器的 IPv6 地址的报文。

设置 IPv6 VRRP 备份组的优先级

【命令格式】 **vrrp ipv6** *group* **priority** *level*

【参数说明】 *group*：VRRP 组号。

level：VRRP 组的优先级。

【命令模式】 接口模式

【使用指导】 该命令将手动设置 VRRP 组的优先级。

设置 IPv6 VRRP 备份组监视的接口

【命令格式】 **vrrp ipv6** *group* **track** *interface-type interface-numbe* [**link**] [*priority*]

【参数说明】 *group*：VRRP 组号。

interface-type interface-number：被监视的接口。

priority：被监视的接口状态改变时其 VRRP 优先级改变的尺度。缺省值为 10。

【命令模式】 接口模式

【使用指导】 被监视的接口只允许是三层可路由的逻辑接口(如 Routed Port、SVI、Loopback、Tunnel 等等)。

如果 VRRP 组占用(Own)了以太网接口实际 IP 地址，此时该 VRRP 组的优先级为 255，不能配置监视接口。

设置 IPv6 VRRP 备份组监视的 IP 地址

【命令格式】 **vrrp ipv6** *group* **track** [**interval** *interval-value*] [**timeout** *timeout-value*] [**retry** *retry-value*] [*priority*]

【参数说明】 *group*：VRRP 组号。

interval *interval-value*：发送探测报文的时间间隔。单位为秒。如果不设定，系统缺省值为 3 秒。

timeout *timeout-value*：发送探测报文后等待应答的超时时间。如果超时时间到了，没有收到应答，则认为不可达。单位为秒。如果不设定，系统缺省值为 1 秒。

retry *retry-value*：确认不可达的次数，如果在连续 *retry-value* 次都没有收到应答，则认为不可达。单位为次数，如果不设定，系统缺省值为 3 次。

priority：被监视的接口状态改变时其 VRRP 优先级改变的尺度。缺省值为 10。

【命令模式】 接口模式

【使用指导】 如果是监视主机，对于 IPv6 虚拟路由器，指定主机的 IPv6 地址。

如果被跟踪的主机地址是链路本地地址，必须指定网络接口。

如果 VRRP 组占用(Own)了以太网接口实际 IP 地址，此时该 VRRP 组的优先级为 255，不能配置监视 IP 地址。

设置 IPv6 VRRP 定时设备学习功能

【命令格式】 **vrrp ipv6** *group* **timers learn**

【参数说明】 *group*：VRRP 组号。

【命令模式】 接口模式

【使用指导】 一旦启用了定时器学习功能，如果当前设备是 VRRP 备份设备，在设置了定时器学习功能后，它会从主设备的 VRRP 通告中学习 VRRP 通告发送间隔，并由此来计算 Master 设备失效间隔，而不是使用自己本地设置的 VRRP 通告发送间隔来计算。本命令可以实现与 Master 设备的 VRRP 通告发送定时器同步。

设置 IPv6 VRRP 组描述字符串

【命令格式】 **vrrp ipv6** *group* **description** *text*

【参数说明】 *group*：VRRP 组号。

text：VRRP 组描述符。

【命令模式】 接口模式

【使用指导】 为 VRRP 组设置描述符，可以便于区分 VRRP 组。当设置的描述符超过 80 个字节，提示配置错误。

设置接口上 VRRP 备份组延迟启动时间

【命令格式】 **vrrp delay** { **minimum** *min-seconds* | **reload** *reload-seconds* }

【参数说明】 **minimum** *min-seconds*：接口状态变为活动时的延迟时间。

reload *reload-seconds*：系统启动时的延迟时间。

【命令模式】 接口模式

【使用指导】 配置本命令后，当系统启动，或者接口状态变为活动时，该接口上的 VRRP 备份组不会立即启动；而是等待相应的延迟时间后再启动 VRRP 备份组，保证非抢占配置不会失效。如果在延迟启动 VRRP 时该接口上接收到 VRRP 报文，则会取消延迟，立即启动 VRRP 协议。两种 VRRP 备份组延迟启动时间的取值范围均为 0~60 秒。配置此命令将对接口的 IPv4 VRRP 和 IPv6 VRRP 备份组同时生效。

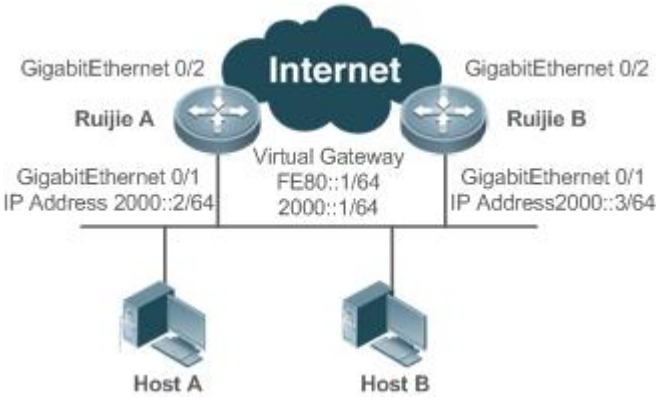
配置举例

以下配置举例，仅介绍与 VRRP 相关的配置。

在 IPv6 的 VRRP 单备份组和监视接口

【网络环境】

图 1-6



【配置方法】

- Host A Host B 需要通过网关访问 Internet 上的资源，它们的缺省网关为 2000::1/64。
- Ruijie A 和 Ruijie B 属于虚拟 IPv6 路由器的备份组 1，其虚拟地址为 2000::1/64 和 FE80::1。
- Ruijie A 监视与 Internet 链接的接口 GigabitEthernet 0/2 ,当 GigabitEthernet 0/2 不可用时 ,Ruijie A Ruijie 的 VRRP 1 降低自己的优先级，由 Ruijie B 执行网关功能。

RuijieA

```
RuijieA#configure terminal
RuijieA(config)#ipv6 vrrp enable
RuijieA(config)#interface GigabitEthernet 0/1
RuijieA(config-if-GigabitEthernet 0/1)#no switchport
RuijieA(config-if-GigabitEthernet 0/1)#ipv6 address 2000::2/64
RuijieA(config-if-GigabitEthernet 0/1)#vrrp 1 ipv6 FE80::1
RuijieA(config-if-GigabitEthernet 0/1)#vrrp 1 ipv6 2000::1
RuijieA(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 priority 120
RuijieA(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 timers advertise 3
RuijieA(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 track GigabitEthernet 0/2 50
RuijieA(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 accept_mode
```

RuijieB

```
RuijieB#configure terminal
RuijieA(config)#ipv6 vrrp enable
RuijieB(config)#interface GigabitEthernet 0/1
RuijieB(config-if-GigabitEthernet 0/1)#no switchport
```

```
RuijieB(config-if-GigabitEthernet 0/1)#ipv6 address 2000::3/64
RuijieB(config-if-GigabitEthernet 0/1)#vrrp 1 ipv6 FE80::1
RuijieB(config-if-GigabitEthernet 0/1)#vrrp 1 ipv6 2000::1
RuijieB(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 priority 100
RuijieB(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 timers advertise 3
RuijieB(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 accept_mode
```

【检验方法】 通过 **show ipv6 vrrp** 命令显示验证。

- 检查当路由设备 Ruijie A 作为 Master 路由设备状态下发现与广域网的接口 GigabitEthernet 0/2 不可用，路由设备 Ruijie A 是否降低自己的 VRRP 备份组优先级 50 而成为 70，这样 VRRP 中路由设备 Ruijie B 就会成为 Master 路由设备。
- 检查当路由设备 Ruijie A 发现自己的与广域网的接口 GigabitEthernet 0/2 恢复可用，是否增加自己的 VRRP 备份组优先级 50 而恢复到 120，这样路由设备 Ruijie A 将再次成为主路由设备。

RuijieA

```
RuijieA#show ipv6 vrrp 1
GigabitEthernet 0/1 - Group 1
  State is Master
  Virtual IPv6 address is as follows:
    FE80::1
    2000::1
  Virtual MAC address is 0000.5e00.0201
  Advertisement interval is 3 sec
  Accept_Mode is enabled
  Preemption is enabled
    min delay is 0 sec
  Priority is 120
  Master Router is FE80::1234 (local), priority is 120
  Master Advertisement interval is 3 sec
  Master Down interval is 10.59 sec
  Tracking state of 1 interface, 1 up:
    up GigabitEthernet 0/2 priority decrement=50
```

RuijieB

```
RuijieB#show ipv6 vrrp 1
GigabitEthernet 0/1 - Group 1
  State is Backup
  Virtual IPv6 address is as follow:
    FE80::1
    2000::1
  Virtual MAC address is 0000.5e00.0201
  Advertisement interval is 3 sec
  Accept_Mode is enabled
  Preemption is enabled
    min delay is 0 sec
```

```
Priority is 100
Master Router is FE80::1234, priority is 120
Master Advertisement interval is 3 sec
Master Down interval is 10.82 sec
```

常见错误

- 同一个VRRP备份组内路由设备上VRRP的虚拟IPv6地址不一致导致同一个VRRP备份组内出现多个Master路由设备。
- 同一个 VRRP 备份组内路由设备上 VRRP 的通告发送间隔不一致 ,并且未设置定时设备学习功能导致同一个 VRRP 备份组内出现多个 Master 路由设备。

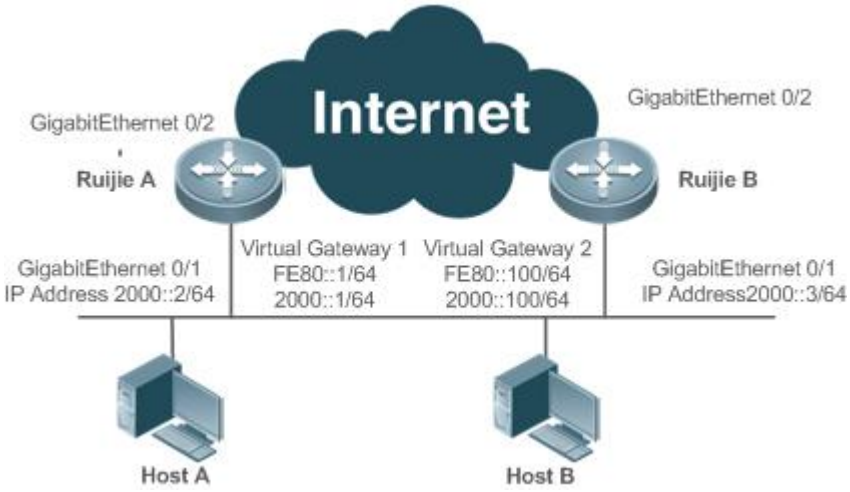
配置举例

以下配置举例，仅介绍与 VRRP 相关的配置。

在 IPv6 的 VRRP 多备份组

【网络环境】

图 1-7



【配置方法】

- Host A Host B 需要通过网关访问 Internet 上的资源，它们的缺省网关分别为 2000::1/64 和 2000::100/64。
- Ruijie A 和 Ruijie B 属于虚拟 IPv6 路由器的备份组 1，其虚拟地址为 2000::1/64 和 FE80::1。
- Ruijie A 和 Ruijie B 也属于虚拟 IPv6 路由器的备份组 2，其虚拟地址为 2000::100/64 和 FE80::100。
- Ruijie A 和 Ruijie B 同时作为网关转发流量，同时作为另外一台设备的备份。

RuijieA

```
RuijieA#configure terminal
RuijieA(config)#ipv6 vrrp enable
RuijieA(config)#interface GigabitEthernet 0/1
RuijieA(config-if-GigabitEthernet 0/1)#no switchport
RuijieA(config-if-GigabitEthernet 0/1)#ipv6 address 2000::2/64
RuijieA(config-if-GigabitEthernet 0/1)#vrrp 1 ipv6 FE80::1
```

```
RuijieA(config-if-GigabitEthernet 0/1)#vrrp 1 ipv6 2000::1
RuijieA(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 priority 120
RuijieA(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 timers advertise 3
RuijieA(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 accept_mode
RuijieA(config-if-GigabitEthernet 0/1)#vrrp 2 ipv6 FE80::100
RuijieA(config-if-GigabitEthernet 0/1)# vrrp 2 ipv6 2000::100
RuijieA(config-if-GigabitEthernet 0/1)#vrrp ipv6 2 priority 100
RuijieA(config-if-GigabitEthernet 0/1)#vrrp ipv6 2 timers advertise 3
RuijieA(config-if-GigabitEthernet 0/1)#vrrp ipv6 2 accept_mode
```

RuijieB

```
RuijieB#configure terminal
RuijieA(config)#ipv6 vrrp enable
RuijieB(config)#interface GigabitEthernet 0/1
RuijieB(config-if-GigabitEthernet 0/1)#no switchport
RuijieB(config-if-GigabitEthernet 0/1)#ipv6 address 2000::3/64
RuijieB(config-if-GigabitEthernet 0/1)#vrrp 1 ipv6 FE80::1
RuijieB(config-if-GigabitEthernet 0/1)#vrrp 1 ipv6 2000::1
RuijieB(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 priority 100
RuijieB(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 timers advertise 3
RuijieB(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 accept_mode
RuijieB(config-if-GigabitEthernet 0/1)#vrrp 2 ipv6 FE80::100
RuijieB(config-if-GigabitEthernet 0/1)# vrrp 2 ipv6 2000::100
RuijieB(config-if-GigabitEthernet 0/1)#vrrp ipv6 2 priority 120
RuijieB(config-if-GigabitEthernet 0/1)#vrrp ipv6 2 timers advertise 3
RuijieB(config-if-GigabitEthernet 0/1)#vrrp ipv6 2 accept_mode
```

【检验方法】 通过 **show ipv6 vrrp** 命令显示验证。

RuijieA

```
RuijieA#show ipv6 vrrp
GigabitEthernet 0/1 - Group 1
  State is Master
  Virtual IPv6 address is as follows:
    FE80::1
    2000::1
  Virtual MAC address is 0000.5e00.0201
  Advertisement interval is 3 sec
  Accept_Mode is enabled
  Preemption is enabled
    min delay is 0 sec
  Priority is 120
  Master Router is FE80::1234 (local), priority is 120
  Master Advertisement interval is 3 sec
  Master Down interval is 10.59 sec
```

```
GigabitEthernet 0/1 - Group 2
  State is Backup
  Virtual IPv6 address is as follows:
    FE80::100
    2000::100
  Virtual MAC address is 0000.5e00.0202
  Advertisement interval is 3 sec
  Accept_Mode is enabled
  Preemption is enabled
    min delay is 0 sec
  Priority is 100
  Master Router is FE80::5678, priority is 120
  Master Advertisement interval is 3 sec
  Master Down interval is 10.82 sec
```

RuijieB

```
RuijieB#show ipv6 vrrp
GigabitEthernet 0/1 - Group 1
  State is Backup
  Virtual IPv6 address is as follow:
    FE80::1
    2000::1
  Virtual MAC address is 0000.5e00.0201
  Advertisement interval is 3 sec
  Accept_Mode is enabled
  Preemption is enabled
    min delay is 0 sec
  Priority is 100
  Master Router is FE80::1234, priority is 120
  Master Advertisement interval is 3 sec
  Master Down interval is 10.82 sec
GigabitEthernet 0/1 - Group 2
  State is Master
  Virtual IPv6 address is as follows:
    FE80::100
    2000::100
  Virtual MAC address is 0000.5e00.0202
  Advertisement interval is 3 sec
  Accept_Mode is enabled
  Preemption is enabled
    min delay is 0 sec
  Priority is 120
  Master Router is FE80::5678(local), priority is 120
```

```
Master Advertisement interval is 3 sec
Master Down interval is 10.59 sec
```

常见错误

- 同一个VRRP备份组内路由设备上VRRP的虚拟IPv6地址不一致导致同一个VRRP备份组内出现多个Master路由设备。
- 同一个 VRRP 备份组内路由设备上 VRRP 的通告发送间隔不一致 ,并且未设置定时设备学习功能导致同一个 VRRP 备份组内出现多个 Master 路由设备。

1.5.3 配置VRRP+MSTP

配置效果

- MTSP 和 VRRP 同时使用可以达到链路级备份和网关级备份，极大提高网络健壮性。

注意事项

- 同一个 VRRP 备份组内路由设备上 VRRP 需要配置相同的虚拟 IPv4 地址。
- 启动 VRRP 需要在三层口上配置。

配置方法

↘ 启用 IPv4 VRRP

- 默认接口上没有启用 IPv4 VRRP，如果接口要启用 IPv4 VRRP 备份功能则必须配置。

↘ 设置 IPv4 VRRP 的验证字符串

- 默认 VRRP 处于无验证模式，如果需要 VRRP 处于明文密码验证模式则配置。

↘ 设置 IPv4 VRRP 主路由设备 VRRP 通告间隔

- 默认 VRRP 的主路由设备 VRRP 通告间隔为 1 秒，如果需要手动设置则配置。

↘ 设置 Ipv4 VRRP 备份组处于抢占模式

- 默认 VRRP 处于抢占模式，抢占延迟时间缺省为 0 秒。

↘ 设置 IPv4 VRRP 备份组的优先级

- 默认 VRRP 组优先级为 100，如果需要手动设置则配置。

↘ 设置 IPv4 VRRP 备份组监视的接口

- 默认 IPv4 VRRP 组未配置监视接口，缺省优先级改变值为 10，如果需要通过监视接口来实现故障检测则配置。

设置 IPv4 VRRP 定时设备学习功能

- 默认 VRRP 组未开启定时设备学习功能，如果备份路由设备需要学习主路由设备的 VRRP 通告间隔则配置。

设置 IPv4 VRRP 组描述字符串

- 默认 VRRP 组未配置描述字符串，如果需要便于区分 VRRP 组则配置。

设置接口上 VRRP 备份组延迟启动时间

- 默认 VRRP 组未配置延迟启动时间，如果为了保证非抢占模式不失效则配置。

设置 IPv4 VRRP 的 VRRP 报文标准

- 默认 IPv4 VRRP 使用 VRRPv2 标准，如果需要手动设置则配置。

检验方法

- **show vrrp** 命令显示配置是否生效

相关命令

启用 IPv4 VRRP

【命令格式】 **vrrp** *group* **ip** *ipaddress* [**secondary**]

【参数说明】 *group*：VRRP 组号，不同产品型号取值范围不同。

Ipaddress：虚拟设备的 IP 地址。

secondary：标明是该虚拟设备的次 IP 地址。

【命令模式】 接口模式

【使用指导】 如果不指定虚拟 IP 地址，路由设备就不会参与 VRRP 备份组。如果不使用 Secondary 参数，那么设置的 IP 地址将成为虚拟路由设备的主 IP 地址。

设置 IPv4 VRRP 的验证字符串

【命令格式】 **vrrp** *group* **authentication** *string*

【参数说明】 *group*：VRRP 组号。

string：用于 VRRP 组验证的字符串(不能超过 8 个字节，这里的验证口令是明文口令)。

【命令模式】 接口模式

【使用指导】 在同一个 VRRP 组中的设备必须设置相同的验证口令。明文验证口令不能保证安全性，它只是用来防止/提示错误的 VRRP 配置。

此命令只对 VRRPv2 报文适用

设置 IPv4 VRRP 主路由设备 VRRP 通告间隔

【命令格式】 **vrrp** *group* **timers advertise** { *advertise-interval* | **csec** *centisecond-interval* }

【参数说明】 *group*：VRRP 组号。

advertise-interval：VRRP 通告发送间隔(以秒为单位)。

csec *centisecond-interval*：备份组中 Master 发送 VRRP 报文的时间间隔。整数形式，取值范围是 50～99。单位是厘秒。无缺省值。

如果 VRRPv2 配置了此命令，则取默认的主设备的通告发送间隔，即 1 秒。

【命令模式】 接口模式

【使用指导】 如果当前设备成为 VRRP 组中的主设备，它将以设定的间隔发送 VRRP 通告来通告自己的 VRRP 状态、优先级以及其它信息。

设置 IPv4 VRRP 备份组处于抢占模式

【命令格式】 **vrrp** *group* **preempt** [**delay** *seconds*]

【参数说明】 *group*：VRRP 组号。

delay *seconds*：准备宣告自己拥有 Master 身份之前的延迟。缺省值为 0 秒。

【命令模式】 接口模式

【使用指导】 如果 VRRP 组工作在抢占模式下，一旦它发现自己的优先级高于当前 Master 的优先级，它将抢占成为该 VRRP 组的主设备。如果 VRRP 组工作在非抢占模式下，即便它发现自己的优先级高于当前 Master 的优先级，它也不会抢占成为该 VRRP 组的主设备。VRRP 组使用以太网接口 IP 地址情况下，抢占模式是否设置意义不大，因为此时该 VRRP 组具有最大优先级，它自动成为该 VRRP 组中的主设备。

设置 IPv4 VRRP 备份组的优先级

【命令格式】 **vrrp** *group* **priority** *level*

【参数说明】 *group*：VRRP 组号。

level：VRRP 组的优先级。

【命令模式】 接口模式

【使用指导】 该命令将手动设置 VRRP 组的优先级。

设置 IPv4 VRRP 备份组监视的接口

【命令格式】 **vrrp** *group* **track** *interface-type interface-number* [*priority*]

【参数说明】 *group*：VRRP 组号。

interface-type interface-number：被监视的接口。

priority：被监视的接口状态改变时其 VRRP 优先级改变的尺度。缺省值为 10。

【命令模式】 接口模式

【使用指导】 被监视的接口只允许是三层可路由的逻辑接口(如 Routed Port、SVI、Loopback 等等)。

如果 VRRP 组占用(Own)了以太网接口实际 IP 地址，此时该 VRRP 组的优先级为 255，不能配置监视接口。

设置 IPv4 VRRP 备份组监视的 IP 地址

【命令格式】 **vrrp** *group* **track** *ipv4-address* [**interval** *interval-value*] [**timeout** *timeout-value*] [**retry** *retry-value*] [*priority*]

【参数说明】 *group*：VRRP 组号。

ipv4-addres：被监视的 IPv4 地址。

interval *interval-value*：发送探测报文的时间间隔。单位为秒。如果不设定，系统缺省值为 3 秒。

timeout *timeout-value*：发送探测报文后等待应答的超时时间。如果超时时间到了，没有收到应答，则认为不

可达。单位为秒。如果不设定，系统缺省值为 1 秒。

retry *retry-value*：确认不可达的次数，如果在连续 *retry-value* 次都没有收到应答，则认为不可达。单位为次数，如果不设定，系统缺省值为 3 次。

priority：被监视的接口状态改变时其 VRRP 优先级改变的尺度。缺省值为 10。

【命令模式】 接口模式

【使用指导】 如果是监视主机，对于 IPv4 虚拟路由器，指定主机的 IPv4 地址。

如果 VRRP 组占用(Own)了以太网接口实际 IP 地址，此时该 VRRP 组的优先级为 255，不能配置监视 IP 地址。

设置 IPv4 VRRP 定时设备学习功能

【命令格式】 **vrrp** *group* **timers learn**

【参数说明】 *group*：VRRP 组号。

【命令模式】 接口模式

【使用指导】 一旦启用了定时器学习功能，如果当前设备是 VRRP 备份设备，在设置了定时器学习功能后，它会从主设备的 VRRP 通告中学习 VRRP 通告发送间隔，并由此来计算 Master 设备失效间隔，而不是使用自己本地设置的 VRRP 通告发送间隔来计算。本命令可以实现与 Master 设备的 VRRP 通告发送定时器同步。

设置 IPv4 VRRP 组描述字符串

【命令格式】 **vrrp** *group* **description** *text*

【参数说明】 *group*：VRRP 组号。

text：VRRP 组描述符。

【命令模式】 接口模式

【使用指导】 为 VRRP 组设置描述符，可以便于区分 VRRP 组。当设置的描述符超过 80 个字节，提示配置错误。

设置接口上 VRRP 备份组延迟启动时间

【命令格式】 **vrrp delay** { **minimum** *min-seconds* | **reload** *reload-seconds* }

【参数说明】 **minimum** *min-seconds*：接口状态变为活动时的延迟时间。

reload *reload-seconds*：系统启动时的延迟时间。

【命令模式】 接口模式

【使用指导】 配置本命令后，当系统启动，或者接口状态变为活动时，该接口上的 VRRP 备份组不会立即启动；而是等待相应的延迟时间后再启动 VRRP 备份组，保证非抢占配置不会失效。如果在延迟启动 VRRP 时该接口上接收到 VRRP 报文，则会取消延迟，立即启动 VRRP 协议。两种 VRRP 备份组延迟启动时间的取值范围均为 0~60 秒。

配置此命令将对接口的 IPv4 VRRP 和 IPv6 VRRP 备份组同时生效。

设置 IPv4 VRRP 的 VRRP 报文标准

【命令格式】 **vrrp** *group* **version** { **2** | **3** }

【参数说明】 **2**：使用 VRRPv2 报文发送标准。

3：使用 VRRPv3 报文发送标准。

【命令模式】 接口模式

【使用指导】 对于 IPv4 VRRP 考虑到 VRRPv2 和 VRRPv3 的兼容性问题，用户可以根据网络实际环境选择 VRRP 报文的

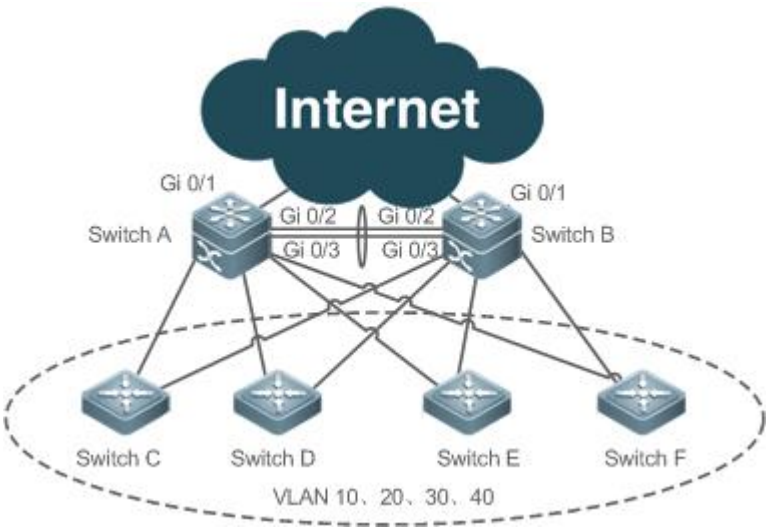
发送标准。VRRPv2 基于 RFC3768，VRRPv3 基于 RFC 5798。
此命令只适用于 IPv4 VRRP。

配置举例

以下配置举例，仅介绍与 VRRP 相关的配置。

配置 VRRP+MSTP

【网络环境】
图 1-8



【配置方法】

- 在设备上（本例为 Switch A、B、C、D、E、F）使能 MSTP 功能，配置 VLAN-Instance 之间的实例映射（本例将 VLAN 10、20 对应 Instance 1，VLAN 30、40 对应 Instance 2，其余 VLAN 对应 Instance 0），并设置网关设备（本例为 Switch A 和 Switch B）为对应实例的根桥。
- 将各 VLAN 的 SVI 加入相应的 VRRP 备份组，并设置网关设备为对应备份组的 Master 路由设备和 Backup 路由设备。本例具体配置如下表所示：

网关设备	VLAN ID	SVI	备份组	虚拟 IP 地址	状态
Switch A	10	192.168.10.2	VRRP 10	192.168.10.1	Master
Switch B		192.168.10.3			Backup
Switch A	20	192.168.20.2	VRRP 20	192.168.20.1	Master
Switch B		192.168.20.3			Backup
Switch A	30	192.168.30.2	VRRP 30	192.168.30.1	Backup
Switch B		192.168.30.3			Master
Switch A	40	192.168.40.2	VRRP 40	192.168.40.1	Backup
Switch B		192.168.40.3			Master

- 将对应备份组的 Master 路由设备的上链口（本例为 Switch A 和 Switch B 的端口 Gi 0/1）设置为 Master 路由设备的监视接口。

- 第一步，在设备上创建 VLAN，在 Switch A、B 上创建 VLAN 10、20、30、40
- 第二步 ,配置 MST 域 ,在 Switch A、B 上配置 VLAN 10、20 对应 Instance 1 ,VLAN 20、30 对应 Instance 2，其余 VLAN 对应 Instance 0。
- 第三步，配置 Switch A 为 MST 0 和 MST 1 的根桥，Switch B 为 MST 2 的根桥。
- 第四步，使能 MSTP。
- 第五步，配置各 VLAN 的 SVI，并加入对应的备份组，同时设置备份组的虚拟 IP 地址。对应配置参见上表。
- 第六步，配置各备份组对应的 Master 路由设备和 Backup 路由设备。
- 第七步，将备份组的 Master 路由设备的上链口配置为 VRRP 组的监视接口。注意：监视接口必须为三层接口。

第八步，配置双核心设备的互联端口为 AP 口。

SwitchA

```
//在 Switch A 上创建 VLAN 10、20、30、40
SwitchA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)#vlan range 10,20,30,40
SwitchA(config-vlan-range)#exit
//配置 VLAN 10、20 对应 Instance 1，VLAN 30、40 对应 Instance 2，其余 VLAN 对应 Instance 0。
SwitchA(config)#spanning-tree mst configuration
SwitchA(config-mst)#instance 1 vlan 10,20
%Warning:you must create vlans before configuring instance-vlan relationship
SwitchA(config-mst)#instance 2 vlan 30,40
%Warning:you must create vlans before configuring instance-vlan relationship
SwitchA(config-mst)#exit
//在 Switch A 上设置 MST 0 和 MST 1 的优先级为 4096，MST 2 的优先级为 8192。
SwitchA(config)#spanning-tree mst 0 priority 4096
SwitchA(config)#spanning-tree mst 1 priority 4096
SwitchA(config)#spanning-tree mst 2 priority 8192
//开启 MSTP
SwitchA(config)#spanning-tree
Enable spanning-tree.
//配置各 VLAN 的 SVI，并加入对应的备份组，同时设置备份组的虚拟 IP 地址。
SwitchA(config)#interface vlan 10
SwitchA(config-if-VLAN 10)#ip address 192.168.10.2 255.255.255.0
SwitchA(config-if-VLAN 10)#vrrp 10 ip 192.168.10.1
SwitchA(config-if-VLAN 10)#exit
SwitchA(config)#interface vlan 20
SwitchA(config-if-VLAN 20)#ip address 192.168.20.2 255.255.255.0
SwitchA(config-if-VLAN 20)#vrrp 20 ip 192.168.20.1
```

```
SwitchA(config-if-VLAN 20)#exit
SwitchA(config)#interface vlan 30
SwitchA(config-if-VLAN 30)#ip address 192.168.30.2 255.255.255.0
SwitchA(config-if-VLAN 30)#vrrp 30 ip 192.168.30.1
SwitchA(config-if-VLAN 30)#exit
SwitchA(config)#interface vlan 40
SwitchA(config-if-VLAN 40)#ip address 192.168.40.2 255.255.255.0
SwitchA(config-if-VLAN 40)#vrrp 40 ip 192.168.40.1
SwitchA(config-if-VLAN 40)#exit
//将 Switch A 的备份组 10、20 的优先级调高为 120
SwitchA(config)#interface vlan 10
SwitchA(config-if-VLAN 10)#vrrp 10 priority 120
SwitchA(config-if-VLAN 10)#exit
SwitchA(config)#interface vlan 20
SwitchA(config-if-VLAN 20)#vrrp 20 priority 120
SwitchA(config-if-VLAN 20)#exit
//配置 Switch A 的端口 Gi 0/1 为 Route Port，并设置 IP 地址为 10.10.1.1/24
SwitchA(config)#interface gigabitEthernet 0/1
SwitchA(config-if-GigabitEthernet 0/1)#no switchport
SwitchA(config-if-GigabitEthernet 0/1)#ip address 10.10.1.1 255.255.255.0
SwitchA(config-if-GigabitEthernet 0/1)#exit
//将 Switch A 的端口 Gi 0/1 配置为备份组 10、20 的监视接口，并设置 Priority decrement 为 30。
SwitchA(config)#interface vlan 10
SwitchA(config-if-VLAN 10)#vrrp 10 track gigabitEthernet 0/1 30
SwitchA(config-if-VLAN 10)#exit
SwitchA(config)#interface vlan 20
SwitchA(config-if-VLAN 20)#vrrp 20 track gigabitEthernet 0/1 30
SwitchA(config-if-VLAN 20)#exit
//配置端口 Gi 0/2 和 Gi 0/3 属于 AP 口，并设置 AP 口为 trunk 口。
SwitchA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)#interface range gigabitEthernet 0/2-3
SwitchA(config-if-range)#port-group 1
SwitchA(config)#interface aggregateport 1
SwitchA(config-if-AggregatePort 1)#switchport mode trunk
```

SwitchB

```
//在 Switch B 上创建 VLAN 10、20、30、40
SwitchB#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchB(config)#vlan range 10,20,30,40
SwitchB(config-vlan-range)#exit
//配置 VLAN 10、20 对应 Instance 1，VLAN 30、40 对应 Instance 2，其余 VLAN 对应 Instance 0。
```

```
SwitchB(config)#spanning-tree mst configuration
SwitchB(config-mst)#instance 1 vlan 10,20
%Warning:you must create vlans before configuring instance-vlan relationship
SwitchB(config-mst)#instance 2 vlan 30,40
%Warning:you must create vlans before configuring instance-vlan relationship
SwitchB(config-mst)#exit
//在 Switch B 上设置 MST 2 的优先级为 4096，MST 0 和 MST 1 的优先级为 8192
SwitchB(config)#spanning-tree mst 2 priority 4096
SwitchB(config)#spanning-tree mst 0 priority 8192
SwitchB(config)#spanning-tree mst 1 priority 8192
//开启 MSTP
SwitchB(config)#spanning-tree
Enable spanning-tree.
//配置各 VLAN 的 SVI，并加入对应的备份组，同时设置备份组的虚拟 IP 地址。
SwitchB(config)#interface vlan 10
SwitchB(config-if-VLAN 10)#ip address 192.168.10.3 255.255.255.0
SwitchB(config-if-VLAN 10)#vrrp 10 ip 192.168.10.1
SwitchB(config-if-VLAN 10)#exit
SwitchB(config)#interface vlan 20
SwitchB(config-if-VLAN 20)#ip address 192.168.20.3 255.255.255.0
SwitchB(config-if-VLAN 20)#vrrp 20 ip 192.168.20.1
SwitchB(config-if-VLAN 20)#exit
SwitchB(config)#interface vlan 30
SwitchB(config-if-VLAN 30)#ip address 192.168.30.3 255.255.255.0
SwitchB(config-if-VLAN 30)#vrrp 30 ip 192.168.30.1
SwitchB(config-if-VLAN 30)#exit
SwitchB(config)#interface vlan 40
SwitchB(config-if-VLAN 40)#ip address 192.168.40.3 255.255.255.0
SwitchB(config-if-VLAN 40)#vrrp 40 ip 192.168.40.1
SwitchB(config-if-VLAN 40)#exit
//将 Switch B 的 VRRP 30、40 的优先级调高为 120。
SwitchB(config)#interface vlan 30
SwitchB(config-if-VLAN 30)#vrrp 30 priority 120
SwitchB(config-if-VLAN 30)#exit
SwitchB(config)#interface vlan 40
SwitchB(config-if-VLAN 40)#vrrp 40 priority 120
SwitchB(config-if-VLAN 40)#exit
//配置 Switch B 的端口 Gi 0/1 为 Route Port，并设置 IP 地址为 10.10.2.1/24
SwitchB(config)#interface gigabitEthernet 0/1
SwitchB(config-if-GigabitEthernet 0/1)#no switchport
SwitchB(config-if-GigabitEthernet 0/1)#ip address 10.10.2.1 255.255.255.0
```

```
SwitchB(config-if-GigabitEthernet 0/1)#exit
//将 Switch B 的端口 Gi 0/1 配置为备份组 30、40 的监视接口，并设置 Interface -Priority 为 30。
SwitchB(config)#interface vlan 30
SwitchB(config-if-VLAN 30)#vrrp 30 track gigabitEthernet 0/1 30
SwitchB(config-if-VLAN 30)#exit
SwitchB(config)#interface vlan 40
SwitchB(config-if-VLAN 40)#vrrp 40 track gigabitEthernet 0/1 30
SwitchB(config-if-VLAN 40)#exit
//配置端口 Gi 0/2 和 Gi 0/3 属于 AP 口，并设置 AP 口为 trunk 口。
SwitchB #configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchB (config)#interface range gigabitEthernet 0/2-3
SwitchB (config-if-range)#port-group 1
SwitchB (config)#interface aggregateport 1
SwitchB (config-if-AggregatePort 1)#switchport mode trunk
```

【检验方法】

SwitchA

```
//查看设备的配置信息。
SwitchA#show running-config
!
vlan 10
!
vlan 20
!
vlan 30
!
vlan 40
!
spanning-tree
spanning-tree mst configuration
 instance 0 vlan 1-9, 11-19, 21-29, 31-39, 41-4094
 instance 1 vlan 10, 20
 instance 2 vlan 30, 40
spanning-tree mst 0 priority 4096
spanning-tree mst 1 priority 4096
spanning-tree mst 2 priority 8192
interface GigabitEthernet 0/1
 no switchport
 no ip proxy-arp
 ip address 10.10.1.1 255.255.255.0
!
interface GigabitEthernet 0/2
```

```
 port-group 1
!
interface GigabitEthernet 0/3
 port-group 1
!
interface AggregatePort 1
 switchport mode trunk
!
interface VLAN 10
 no ip proxy-arp
 ip address 192.168.10.2 255.255.255.0
 vrrp 10 priority 120
 vrrp 10 ip 192.168.10.1
 vrrp 10 track GigabitEthernet 0/1 30
!
interface VLAN 20
 no ip proxy-arp
 ip address 192.168.20.2 255.255.255.0
 vrrp 20 priority 120
 vrrp 20 ip 192.168.20.1
 vrrp 20 track GigabitEthernet 0/1 30
!
interface VLAN 30
 no ip proxy-arp
 ip address 192.168.30.2 255.255.255.0
 vrrp 30 ip 192.168.30.1
!
interface VLAN 40
 no ip proxy-arp
 ip address 192.168.40.2 255.255.255.0
 vrrp 40 ip 192.168.40.1
//查看设备的 VRRP 状态
SwitchA#show vrrp brief
Interface  Grp  Pri  timer  Own  Pre  State   Master addr   Group addr
VLAN 10    10   120  3      -    P    Master  192.168.10.2  192.168.10.1
VLAN 20    20   120  3      -    P    Master  192.168.20.2  192.168.20.1
VLAN 30    30   100  3      -    P    Backup  192.168.30.3  192.168.30.1
VLAN 40    40   100  3      -    P    Backup  192.168.40.3  192.168.40.1
//断开 Switch A 的上行链路，查看设备的 VRRP 状态
SwitchA#show vrrp brief
Interface  Grp  Pri  timer  Own  Pre  State   Master addr   Group addr
```

```
VLAN 10     10    90    3       -     P     Backup   192.168.10.3   192.168.10.1
VLAN 20     20    90    3       -     P     Backup   192.168.20.3   192.168.20.1
VLAN 30     30    100   3       -     P     Backup   192.168.30.3   192.168.30.1
VLAN 40     40    100   3       -     P     Backup   192.168.40.3   192.168.40.1
```

SwitchB

```
//查看设备的配置信息。
SwitchB#show running-config
!
vlan 10
!
vlan 20
!
vlan 30
!
vlan 40
!
spanning-tree
spanning-tree mst configuration
 instance 0 vlan 1-9, 11-19, 21-29, 31-39, 41-4094
 instance 1 vlan 10, 20
 instance 2 vlan 30, 40
spanning-tree mst 0 priority 8192
spanning-tree mst 1 priority 8192
spanning-tree mst 2 priority 4096
interface GigabitEthernet 0/1
 no switchport
 no ip proxy-arp
 ip address 10.10.2.1 255.255.255.0
!
interface GigabitEthernet 0/2
 port-group 1!
interface GigabitEthernet 0/3
 port-group 1
!
interface AggregatePort 1
 switchport mode trunk
!
interface VLAN 10
 no ip proxy-arp
 ip address 192.168.10.3 255.255.255.0
```

```
 vrrp 10 ip 192.168.10.1
!
interface VLAN 20
 no ip proxy-arp
 ip address 192.168.20.3 255.255.255.0
 vrrp 20 ip 192.168.20.1
!
interface VLAN 30
 no ip proxy-arp
 ip address 192.168.30.3 255.255.255.0
 vrrp 30 priority 120
 vrrp 30 ip 192.168.30.1
 vrrp 30 track GigabitEthernet 0/1 30
!
interface VLAN 40
 no ip proxy-arp
 ip address 192.168.40.3 255.255.255.0
 vrrp 40 priority 120
 vrrp 40 ip 192.168.40.1
 vrrp 40 track GigabitEthernet 0/1 30
//查看设备的 VRRP 状态
SwitchB#show vrrp brief
Interface  Grp  Pri  timer  Own  Pre  State   Master addr   Group addr
VLAN 10    10   100  3      -    P    Backup  192.168.10.2  192.168.10.1
VLAN 20    20   100  3      -    P    Backup  192.168.20.2  192.168.20.1
VLAN 30    30   120  3      -    P    Master  192.168.30.3  192.168.30.1
VLAN 40    40   120  3      -    P    Master  192.168.40.3  192.168.40.1
//断开 Switch B 的上行链路，查看设备的 VRRP 状态如下
SwitchB#show vrrp brief
Interface  Grp  Pri  timer  Own  Pre  State   Master addr   Group addr
VLAN 10    10   100  3      -    P    Master  192.168.10.3  192.168.10.1
VLAN 20    20   100  3      -    P    Master  192.168.20.3  192.168.20.1
VLAN 30    30   120  3      -    P    Master  192.168.30.3  192.168.30.1
VLAN 40    40   120  3      -    P    Master  192.168.40.3  192.168.40.1
```

常见错误

- 同一 VRRP 备份组内各路由设备以太网接口上 VRRP 组验证模式不同导致同一个 VRRP 备份组内出现多个 Master 路由设备。

- 对于 VRRPv2，同一 VRRP 备份组内各路由设备以太网接口上 VRRP 组验证模式相同均为明文密码模式，但是验证字符串不一致导致同一个 VRRP 备份组内出现多个 Master 路由设备。
- 同一个 VRRP 备份组内路由设备上 VRRP 的通告发送间隔不一致，并且未设置定时设备学习功能导致同一个 VRRP 备份组内出现多个 Master 路由设备。
- 同一个 VRRP 备份组内路由设备上 VRRP 的虚拟 IP 地址不一致导致同一个 VRRP 备份组内出现多个 Master 路由设备。

1.6 监视与维护

清楚各类信息

无

查看运行情况

作用	命令
查看 IPv4 VRRP 或者 IPv6 VRRP 的概况或者细节。	**show** [**ipv6**] **vrrp** [**brief** | *group*]
查看指定接口上的 IPv4 VRRP 组或者 IPv6 VRRP 组的情况。	**show** [**ipv6**] **vrrp interface** *type number* [**brief**]
查看 VRRP 报文收发的统计信息。	**show vrrp packet statistics** [*interface-type interface-number*]

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 VRRP 出错提示、VRRP 事件、VRRP 报文以及状态调试开关。	**debug** [**ipv6**] **vrrp**
打开 VRRP 出错提示调试开关。	**debug** [**ipv6**] **vrrp errors**
打开 VRRP 事件提示调试开关。	**debug** [**ipv6**] **vrrp events**
打开 VRRP 数据包调试开关。	**debug vrrp packets** [**acl** *acl-id* **|** [**icmp | protocol**] **interface** *type number* [*group*]] **debug ipv6 vrrp packets** [**acl** *acl-name* **|** [**icmp | protocol**] **interface** *type number* [*group*]]
打开 VRRP 状态调试开关。	**debug** [**ipv6**] **vrrp state**

2 RNS

2.1 概述

RNS 是 Reliable Network Service 的缩写，RNS 通过探测对端设备提供的特定服务，来监控服务的可用性，端到端连接的完整性和服务的质量。利用 RNS 探测结果，用户可以：

- 及时了解网络的性能状况，针对不同的网络性能进行相应处理。
- 对网络故障进行诊断和定位。

下文仅介绍 RNS 的相关内容。

协议规范

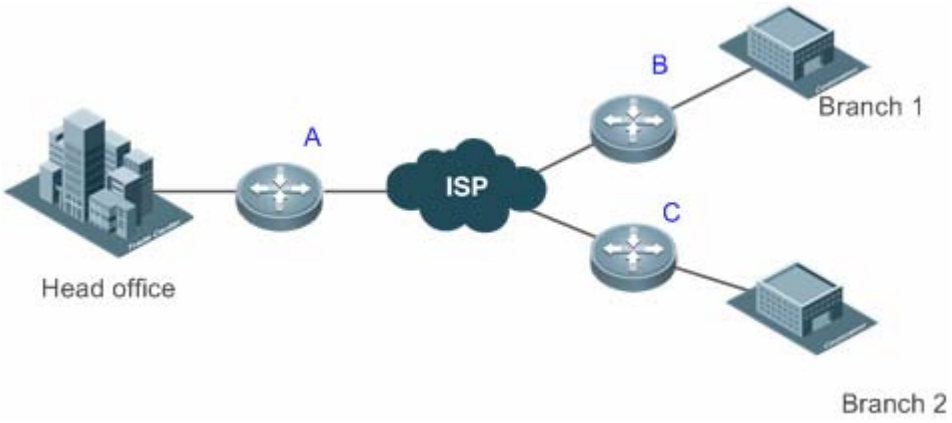
无

2.2 典型应用

2.2.1 对业务性能进行探测评估

应用场景

如下图，某公司打算在总部和分支结构之间部署视频会议系统，并已经进行了相关的 Qos 配置。在正式部署之前，要先检测在公司现有的业务压力下，该新业务是否能正常的运作。由于视频会议系统对于网络的UDP 延迟和UDP 传输抖动性能比较敏感，传统的 ping 工具仅仅能检测 ICMP 的性能，对于 UDP 传输性能没法有效的衡量，而且也无法满足抖动性能的测量。



【注释】 A,B,C 均为交换机设备

功能部署

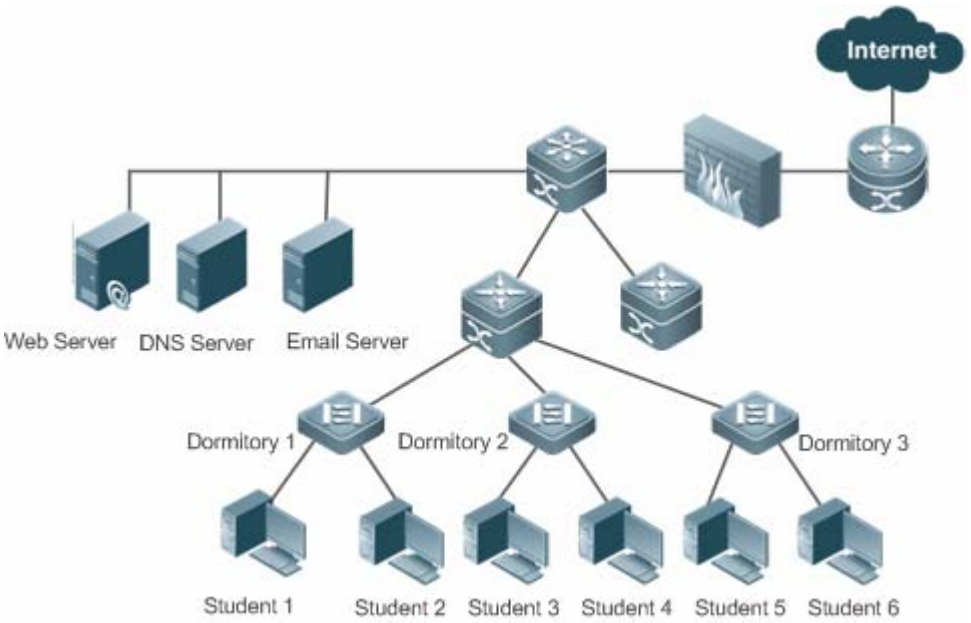
- 在分支机构的出口交换设备/交换机上配置 RNS 探测，能进行 UDP 抖动检测，UDP 延迟检测；
- 用户只需要在交换机 A 上指定好总部的出口交换设备/交换机的 IP 地址，UDP 端口，就能主动发送 UDP 报文，总部的出口交换设备/交换机能通过配置，自动应答该 UDP 报文，通过在分支机构的出口交换设备/交换机上对发送和接收报文的处理，计算 UDP 抖动值。为了了解在各个时段的情况，RNS 探测还应开启定时启动/停止，重复运行等时间调度功能。

2.2.2 定位网络故障

应用场景

如下园区中，学生 1 报告无法访问 Web 服务器，学生 3 报告无法访问 Internet，学生 6 报告邮件无法正常收发。

图 2-1



功能部署

- 管理员直接在该学生宿舍的接入交换机上开启 DNS 功能的探测，检测是否是域名服务器解析问题；若 DNS 探测失败，则自动触发 ICMP-Echo 探测以检测 Web 服务器网络是否可达。
- 当出现故障时，仅需要启动一个探测，后续的都能自动触发，然后查看结果就可以分析大致的问题点，大大简化管理员的工作。

2.3 功能详解

基本概念

RNS 探测实例

RNS探测实例，可看作是一个RNS进程。进行RNS探测前，需要创建RNS探测实例。在RNS探测实例中配置RNS探测的参数，如探测类型，探测目的地址，探测频率等。探测实例ID全局唯一。

功能特性	作用
RNS 探测	主要用于监控网络的连通性，服务的可用性，端到端连接的完整性和服务的质量。
track 联动功能	Track 可跟踪探测结果，并将结果通告给相应的模块。

2.3.1 RNS探测

主要用于监控网络的连通性，服务的可用性，端到端连接的完整性和服务的质量，如探测该设备 DNS 功能是否正常，目前 RNS 支持的探测类型包括 ICMP-Echo，DNS 和 TCP 类型的探测。

工作原理

ICMP-Echo 探测

ICMP-Echo 探测是 RNS 最基本的功能，遵循 RFC 2925 来实现。其实现原理是通过发送 ICMP 报文来判断目的地的可达性、计算网络响应时间及丢包率。

ICMP-Echo 探测根据设置的探测时间及频率向探测的目的 IP 地址发 ICMP 回显请求报文，目的地址收到 ICMP 回显请求报文后，回复 ICMP 回显应答报文。ICMP-Echo 探测根据 ICMP 回显应答报文的接收情况，如接收时间和报文个数，计算出到目的 IP 地址的响应时间及丢包率，从而反映当前的网络性能及网络情况。ICMP-Echo 探测的结果和历史记录将被记录，可以通过命令行来查看。

⚠ ICMP-Echo 探测成功的前提条件是目的设备要能够正确响应 ICMP 回显请求报文。

DNS 探测

DNS 探测通过模拟 DNS 客户端向指定的 DNS 服务器发送域名解析请求，根据域名解析是否成功及域名解析需要的时间，来判断 DNS 服务器是否可用，及域名解析速度。DNS 探测只是模拟域名解析的过程，不保存解析的域名与 IP 地址的对应关系。DNS 探测的结果和历史记录将被记录，可以通过命令行来查看。

RNS 探测的配置过程

1. 创建特定类型的探测实例，根据探测类型进行相应探测参数的配置。
2. 启动 RNS 探测实例。
3. RNS 探测实例构造指定探测类型的报文，并发送给对端。
4. 对端收到探测报文后，回复相应类型的应答报文。

5. RNS 探测实例根据是否收到应答报文，以及接收应答报文的时间，计算报文丢失率、往返时间等。

6. 通过显示命令或调试命令查看探测结果。

以上配置过程介绍的是 RNS 实例探测通用的流程，不同类型的探测具体配置步骤，参看下文配置详解。

相关配置

配置探测的重复时间间隔

缺省情况下，探测的重复时间间隔为 60 秒。

在 RNS 探测类型对应的模式下，使用 **frequency** *millisecond* 命令可以配置探测重复时间间隔。

配置 **frequency** 应当满足下面的公式，以保证探测的计算正确。

(**frequency** *milliseconds*) > (**timeout** *milliseconds*) >= (**threshold** *milliseconds*)

配置探测超时时间

不同探测类型的缺省超时时间不同，可以通过 **show ip rns configuration** 查看

在 RNS 探测类型对应的模式下，使用 **timeout** *millisecond* 命令可以配置探测实例超时时间间隔。

配置 **timeout** 应当满足一定的计算关系，请参见 **frequency** 的使用指导。

配置探测的时间阈值

缺省情况下，探测的时间阈值为 5000ms。

在 RNS 探测类型对应的模式下，使用 **threshold** *milliseconds* 命令可以配置实例探测的时间阈值。

配置 **threshold** 应当满足一定的计算关系，请参见 **frequency** 的使用指导。

探测设置一个标签

无缺省配置

在 RNS 探测类型对应的模式下，使用 **tag** *text* 命令可以配置探测标签。

tag 可以为探测指定一个标签，通常用于标识这个探测的作用。

配置探测实例的协议载荷大小

不同探测类型的缺省值不同，默认为对应探测类型协议报文必须的最小值或适合值。

在对应 RNS 探测类型配置模式下，使用 **request-data-size** *bytes* 命令可以配置协议载荷大小。

配置探测的报文的 TOS 字段

缺省配置为 0。

在 RNS 探测类型对应的模式下，使用 **tos** number 命令配置 RNS 探测报文中 IPv4 首部 TOS 字段。

2.3.2 track联动功能

track 支持跟踪的对象类型包括：跟踪一个 RNS 探测结果、跟踪一个 RNS 列表的状态、跟踪一个接口的链路状态以及跟踪一个 track 列表的状态。同时当 track 的状态发生变化时，可以触发其他模块进行联动。

工作原理

以 track 跟踪 RNS 探测结果为例，说明 track 的工作原理。

- 配置一个 track 对象，用来跟踪一个 RNS 探测结果。
- 当 RNS 探测结果发生变化时，RNS 模块发送状态变化的消息给 track 模块。
- track 模块接收到 RNS 探测结果的消息，经过设置的延迟时间后，若该 RNS 探测结果未发生变化，则修改该 track 对象的状态，通告关注该 track 对象的模块。若在这段时间内，该 RNS 探测结果又恢复原有状态，则不修改 track 状态和通告相应的模块。

相关配置

↘ 配置用于跟踪接口链路状态的 track 对象

缺省情况下，跟踪接口的链路状态功能不生效。

使用 **track interface line-protocol** 命令可以配置一个 track 对象，用于跟踪一个接口的链路状态。

该接口的链路状态为 up，则 track 对象的状态为 up；该接口的链路状态为 down，则 track 对象的状态为 down。

↘ 配置用于跟踪 RNS 探测结果的 track 对象

缺省情况下，跟踪 RNS 探测结果功能不生效。

使用 **track rns** 命令可以配置一个 track 对象，用于跟踪一个 RNS 探测结果。其中，RNS 探测编号范围为 1-500。

若该 RNS 探测结果为成功，则 track 对象的状态为 up；若该 RNS 探测结果为失败，则 track 对象的状态为 down。

↘ 配置用于跟踪 track 列表状态的 track 对象

缺省情况下，跟踪 track 列表状态的功能不生效。

使用 **track list** 命令可以配置一个 track 对象，用于跟踪一个 track 列表的状态，其结果可以是所有成员状态取“与”或者“或”的结果。

配置 track 对象的结果取所有成员状态“与”的结果，则当所有成员的状态“与”的结果为 up 时，该 track 对象的状态为 up；当所有成员的状态“与”的结果为 down 时，该 track 对象的状态为 down。“或”情况类似。

↘ 配置 track 列表成员

缺省情况下，track 列表成员为空。

使用 **object** 命令可以配置一个 track 列表成员，该列表成员的状态可配置为与对应 track 对象相同或相反。

↘ 调整 track 的延迟通告时间

缺省情况下，track 的延迟通告时间为 0，即无通告延迟。

使用 **delay** 命令可以调整 track 的延迟通告时间，包括 track 状态由 up 变为 down 的延迟通告时间和由 down 变为 up 的延迟通告时间，取值范围是 0-180，单位为秒。

track 延迟通告的时间越大，则需要等待越长的时间，才会将该状态通告给关注该 track 对象的模块。track 延迟通告的时间越小，则需要等待越短的时间，便会将该状态通告给关注该 track 对象的模块。

2.4 配置详解

配置项	配置建议 & 相关命令	
配置 RNS 基本功能	⚠ 必选配置，用于设置 RNS 基本功能参数。	
	ip rns	支持详细配置与简洁配置。其中， 详细配置：定义一个 RNS 操作对象。用于后续具体探测及参数的配置标识 简洁配置：无需进行后续配置，可以一步启动探测。目前支持 ICMP-Echo、DNS、TCP 类型的 RNS 探测一步启动。
	ip rns reaction-configuration	配置 RNS 探测实例的主动阈值监控和触发机制。
	ip rns reaction-trigger	配置一个 RNS 探测实例在发生监控阈值超过预期时，触发另一个处于 pending 状态的 RNS 探测实例激活探测。
	ip rns schedule	配置 RNS 探测实例的调度方法、启动时间、生存时间。
	ip rns restart	重新启动一个 RNS 探测实例。
	ip rns reset	清除所有 ip rns 的配置。
配置 icmp-echo 探测	⚠ 可选配置，用于实现 ICMP-Echo 类型的 RNS 探测。	
	icmp-echo	创建一个 ICMP-Echo 类型的 RNS 探测实例。
	request-data-size	配置探测的协议载荷大小。
	frequency	设置探测的重复时间间隔。
	tag	设置标签。
	threshold	配置探测的时间阈值。
	timeout	配置探测的超时时间。
	tos	配置探测报文的 IPv4 首部 TOS 字段。
配置 dns 探测	⚠ 可选配置，用于实现 DNS 类型的 RNS 探测。	
	dns	创建一个 DNS 类型的 RNS 探测实例。
	frequency	设置探测的重复时间间隔。
	tag	设置标签。
	threshold	配置探测的时间阈值。
	timeout	配置探测的超时时间。
	tos	配置探测报文 IPv4 首部的 TOS 字段。

配置 track 联动功能	⚠ 可选配置，用于与其他模块进行联动。	
	track rns	配置 track 对象，跟踪一个 RNS 探测的探测结果。
	track interface line-protocol	配置 track 对象，跟踪一个接口的链路状态。
	track list	配置 track 对象，跟踪一个 track 列表的状态。
	object	设置一个 track 跟踪的 list 对象的成员对象。
	delay	设置 track 状态变化的通告延迟时间。

2.4.1 配置RNS基本功能

配置效果

- 详细配置：配置 RNS 探测实例，完成 RNS 探测实例基本配置。
- 简洁配置：一步配置并启动具体的 RNS 探测实例（可选）。

注意事项

- 详细配置下，在通过命令进入 IP-RNS 模式后，若没有进一步配置探测类型，那么这个 RNS 探测实例不会被创建。
- 详细配置下，在配置完一个 RNS 探测实例后，应当通过 **ip rns schedule** 命令配置它的启动策略，否则该探测不会被执行。

配置方法

↘ 定义 RNS 操作对象

- 必须配置。
- 若无特殊要求，应在每台交换设备上定义 RNS 操作对象。
- 简洁配置属于可选配置项。

↘ 配置 RNS 探测实例的主动阈值监控和触发机制

- 如果要求配置探测的主动阈值监控和触发机制，则必须配置。
- 若无特殊要求，应在每台交换设备上配置探测的主动阈值监控和触发机制。

↘ 配置一个 RNS 探测实例触发另一个 RNS 探测实例

- 如果要求一个 RNS 探测实例在发生监控阈值超过预期时，触发另一个处于 pending 状态的 RNS 探测实例开始运行，则必须配置。
- 如果被触发运行的 RNS 探测实例未配置调度参数，则以默认的调度参数运行。
- 若无特殊要求，应在每台交换设备上配置一个 RNS 探测实例触发另一个 RNS 探测实例。

配置 RNS 探测实例的调度参数

- 若无特殊要求，应在每台交换设备上配置 RNS 探测的调度参数。
- 简洁配置下，已使用默认参数自动配置了该命令，无需手动配置。

配置 ip rns restart 重新启动一个 RNS 探测实例

- 如果要求重新启动一个调度处于 pending 状态的探测实例，则可以使用该命令（或者直接配置调度启动 ip rns schedule X start-time now）。

配置 ip rns reset 清空 RNS 探测配置

- 如果要求清除所有配置实例的探测（如配置了大量探测实例，发现配置有误时），则可以使用该命令。

检验方法

- 通过命令 **show ip rns configuration** 查看 RNS 探测实例配置。

相关命令

定义 ip rns 操作对象

【命令格式】 **ip rns** *operation-number*

【参数说明】 *operation-number*：RNS 探测实例编号，取值范围<1-500>。

【命令模式】 全局模式

【使用指导】 目前 RNS 探测仅支持 IPv4 的相关探测，暂不支持 IPv6。目前最多支持配置的探测数量为 500 个。根据不同设备的性能情况，可能无法达到该最大值。由于探测功能只是一个增值功能，当配置了大量的探测，导致消耗掉系统过多的资源时，探测功能会被暂时的禁止，以保证核心业务（如路由转发等）的正常运行。

详细配置（执行 ip rns operation-number 必选项）：执行该命令后，进入 IP-RNS 配置模式。在这个模式内可以定义各种探测类型，若没有进一步配置探测类型，那么这个 RNS 探测不会被创建；在配置完一个 RNS 探测后，还应当通过 **ip rns schedule** 命令配置它的调度参数，否则该探测不会被执行。

一个 RNS 探测配置完探测类型后，下一次再通过 **ip rns** 命令将直接进入对应探测类型的模式，如果要修改一个 RNS 探测实例的探测类型，应当先删除该 RNS 探测实例（通过全局模式下输入 **no ip rns** 命令），再重新进行配置。

配置探测的主动阈值监控和触发机制

【命令格式】 **ip rns reaction-configuration** *operation-number* **react** *monitored-element* [**action-type** *option*] [**threshold-type** { **average** [*number-of-measurements*] | **consecutive** [*occurrences*] | **immediate** | **never** | **xofy** [*x-value y-value*] }] [**threshold-value** *upper-threshold lower-threshold*]

【参数说明】 *operation-number*：RNS 探测实例编号，取值范围<1-500>。

monitored-element：指定被监视的探测信息元素。

action-type *option*：触发后联动的动作。

average [*number-of-measurements*]：被监视元素以 *number-of-measurements* 次数的平均值超出阈值则触发。

consecutive [*occurrences*] :被监视元素连续 *occurrences* 次超出阈值范围则触发 ,*occurrences* 缺省值为 5，可选范围 1-16。

immediate：被监视元素一超出阈值范围就触发。

never：从不触发。

xofy [*x-value y-value*]：在最后 Y 次探测中，有 X 次探测结果超出阈值范围，x 和 y 默认值均为 5，可选范围 1-16。

threshold-value *upper-threshold lower-threshold*：该参数用于配置阈值上下限，具体含义如下：

- 当 *monitored-element* 为 rtt 时，解释为时间，默认值参见“使用指导”。可选范围均为 0-60000ms。
- 需要注意的是：当 react 类型为 timeout 时，threshold-vaule 值无需配置。

【命令模式】 全局模式

【使用指导】 对于同一个 RNS 探测，可以配置多个阈值监控，每一个监控不同的元素。不同的探测类型，支持的监控对象对应关系见下表：

monitored-element	icmp-echo	dns
timeout	✓	✓
rtt	✓	✓

各监控元素的默认阈值如下表:

Monitored Element	Upper Threshold	Lower Threshold
timeout	-	-
rtt	5000ms	0ms

配置一个 RNS 探测实例触发另一个 RNS 探测实例

【命令格式】 **ip rns reaction-trigger** *operation-number target-operation*

【参数说明】 *operation-number*：触发动作的源 RNS 探测实例编号，取值范围<1-500>。。

target-operation：被触发的目的 RNS 探测实例编号，取值范围<1-500>。

【命令模式】 全局模式

【使用指导】 trigger 功能通常用在网络故障诊断场景，普通场景下不需要配置 trigger 功能。

配置 RNS 探测实例的调度参数

【命令格式】 **ip rns schedule** operation-number [**life** { **forever** | seconds }] [**start-time** { hh:mm [:ss] [month day | day month] | **pending** | **now** | **after** hh:mm:ss }] [**recurring**]

【参数说明】 operation-number：RNS 操作索引，取值范围<1-500>。

life forever：RNS 探测实例启动后一直运行。

life seconds：RNS 探测实例的运行时间秒数。

hh:mm [:ss]：RNS 探测实例启动时刻，24 小时制。

month：RNS 探测实例启动的月份，默认是本月。

day：RNS 探测实例启动的日期，默认是当日。

pending：RNS 探测实例启动时间未定，默认值。

now：RNS 探测实例立即启动。

after hh:mm:ss：RNS 探测实例延迟 hh:mm:ss 的时间后启动。

recurring：RNS 探测实例是否在每天的相同时间启动。

【命令模式】 全局模式

【使用指导】 已经通过 **ip rns schedule** 命令配置了调度参数的 RNS 探测实例，其配置参数在运行期间无法进行修改，如果要修改该配置，应当先通过 **no ip rns schedule** 命令删除调度参数，然后再进行修改。

life { *seconds* } 是指 RNS 探测运行时间，即在启动探测后，经过 seconds 时间后将停止探测。

配置 ip rns restart 重新启动一个 RNS 探测

【命令格式】 **ip rns restart** *operation-number*

【参数说明】 *operation-number*：RNS 探测实例编号，取值范围<1-500>。

【命令模式】 全局模式

【使用指导】 该命令将一个已经配置了调度，并调度已停止后(调度状态为 pending)的 RNS 探测重新启动。对于未配置调度的 RNS 探测，该命令无效。

配置 ip rns reset 清空 RNS 探测配置

【命令格式】 **ip rns reset**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 该命令清除所有 ip rns 的所有配置信息。只有在极端情况下，才需要使用该命令（例如配置了大量 RNS 探测实例，但发现配置有误）。

配置举例

配置 RNS 基本功能

【网络环境】

图 2-2



【配置方法】

- 在交换机 A 上配置探测实例 1
- 配置探测实例 1 的探测的调度方法、启动时间、生存时间
- 配置探测实例 1 的主动阈值监控和触发机制
- 配置探测实例 1 在发生监控阈值超过预期时，触发另一个处于 pending 状态的探测实例 2 探测

Swtich A

```
A# configure terminal
A(config)# ip rns 1
A(config-ip-rns)#icmp-echo 10.1.1.1
A(config-ip-rns-icmp-echo)#exit
A(config)ip rns schedule 1 start-time now life forever
A(config)ip rns reaction-configuration 1 react timeout threshold-type immediate action-type trigger
A(config)ip rns reaction-trigger 1 2
```

【检验方法】 通过 **show ip rns configureation** 命令显示实例配置信息

```
Router#show ip rns configuration 1
```

```
Entry number: 1
Tag: ruijie555
Type of operation to perform: icmp-echo
Operation timeout (milliseconds): 5000
Operation frequency (milliseconds): 60000
Threshold (milliseconds): 5000
Recurring (Starting Everyday): FALSE
Life (seconds): 3500
Next Scheduled Start Time:Start Time already passed
Target address/Source address: 2.2.2.3/0.0.0.0
Request size (ARR data portion): 36
```

常见错误

无

2.4.2 配置icmp-echo探测

配置效果

创建一个 ICMP-Echo 类型的 RNS 探测实例。

注意事项

- 必须先配置 RNS 基本功能。

配置方法

↘ 创建 ICMP-Echo 类型的 RNS 探测实例

- 必须配置。
- 若无特殊要求，应在每台交换设备上创建 ICMP-Echo 类型的 RNS 探测实例。

↘ 配置探测通用可选参数

- 如果要求改变探测通用可选参数（重复时间间隔、标签、时间阈值、超时时间、TOS 字段等），则必须配置。
- 若无特殊要求，应在每台交换设备上配置探测通用可选参数。

↘ 配置探测的协议载荷大小

- 如果要求改变探测的协议载荷大小，则必须配置。

- 若无特殊要求，应在每台交换设备上配置探测的协议载荷大小。

检验方法

- 通过 **show ip rns configuration** 命令查看。

相关命令

创建一个 ICMP-Echo 类型的 RNS 探测实例

【命令格式】 **icmp-echo** | { { *destination-ip-address* | *destination-hostname* [**name-server** *ip-address*] } [**source-ipaddr** *ip-address*] [[**af-direct**] **out-interface** *type num* [**next-hop** *ip-address*]] }

【参数说明】 *destination-ip-address*：目的 IP。

destination-hostname：目的主机名。

name-server *ip-address*：配置目的主机名时，指定域名服务器，默认使用设备上通过 ip name-server 配置的域名服务器进行解析。

source-ipaddr *ip-address*：源 ip 地址。

out-interface *type num*：指定探测报文的出接口。

af-direct : 配置 RNS 探测不经过协议栈收发报文。

next-hop *A.B.C.D*：下一跳 ip 地址

【命令模式】 IP RNS 配置模式(config-ip-rns)

【使用指导】 ICMP-Echo 类型的 RNS 探测启动后将发送 ICMP 回显请求报文以探测本机到目标主机网络是否连通。创建 ICMP-Echo 类型的 RNS 探测后将进入 IP RNS ICMP-Echo 模式。默认 ICMP 回显请求报文的协议载荷大小是 36 字节。通过 **request-data-size** 命令，可以修改报文大小。应当先配置 RNS 探测的类型（如 icmp-echo 探测，dns 探测），然后再配置该探测类型的具体参数。如果要修改一个 RNS 探测实例的探测类型，必须先删除该 RNS 探测（通过全局模式下输入 **no ip rns** 命令），再重新进行配置。

配置 RNS 探测实例的协议载荷大小

【命令格式】 **request-data-size** *bytes*

【参数说明】 *bytes*：探测报文的字节数，不同探测类型的最小/最大字节数不同，依据对应探测类型配置模式下的命令提示进行配置。

【命令模式】 IP RNS ICMP-Echo 配置模式（config-ip-rns-icmp- echo)

【使用指导】 该命令主要用来在探测数据包中填充一些字节，以进行较大数据包的探测。

配置探测的重复时间间隔

【命令格式】 **frequency** *milliseconds*

【参数说明】 *milliseconds*：报文的发送时间间隔（毫秒），默认值 60000 毫秒，范围<10-604800000>，最长一周时间。

【命令模式】 IP RNS DNS 配置模式（config-ip-rns-dns)

IP RNS ICMP-Echo 配置模式（config-ip-rns-icmp-echo)

【使用指导】 在一个 RNS 探测实例启动后，会进行周期性的探测。通过配置 **frequency** 命令，可以指定该重复间隔。配置 **frequency** 应当满足下面的公式，以保证探测的计算正确。

(**frequency** *milliseconds*) > (**timeout** *milliseconds*) >= (**threshold** *milliseconds*)

为 RNS 探测实例设置一个标签

【命令格式】 **tag** *text*

【参数说明】 *text*：设置探测的标签，tag 由可打印字符组成，最长允许输入 79 个字符。

【命令模式】 IP RNS DNS 配置模式 (config-ip-rns-dns)

IP RNS ICMP-Echo 配置模式 (config-ip-rns-icmp-echo)

【使用指导】 tag 可以为探测指定一个标签，通常用于标识这个探测的作用。

配置 RNS 探测实例的时间阈值

【命令格式】 **threshold** *milliseconds*

【参数说明】 *milliseconds*：探测的时间阈值，取值范围为 0-60000，单位 ms，默认值 5000。

【命令模式】 IP RNS DNS 配置模式 (config-ip-rns-dns)

IP RNS ICMP-Echo 配置模式 (config-ip-rns-icmp-echo)

【使用指导】 配置 **threshold** 应当满足下面的公式，以保证探测的计算正确。

(**frequency** *milliseconds*) > (**timeout** *milliseconds*) >= (**threshold** *milliseconds*)

配置 RNS 探测实例的超时时间

【命令格式】 **timeout** *millisecond*

【参数说明】 *millisecond*：探测超时时间，取值范围为 10-604800000，单位 ms，不同探测类型，其超时默认值不同。

【命令模式】 IP RNS DNS 配置模式 (config-ip-rns-dns)

IP RNS ICMP-Echo 配置模式 (config-ip-rns-icmp-echo)

【使用指导】 配置 **timeout** 应当满足下面的公式，以保证探测的计算正确。

(**frequency** *milliseconds*) > (**timeout** *milliseconds*) >= (**threshold** *milliseconds*)

配置 RNS 探测的 IPv4 报文 TOS 字段

【命令格式】 **tos** *number*

【参数说明】 *number*：设置探测报文 IPv4 头部的 TOS 字段，取值范围 0-255。默认为 0。

【命令模式】 IP RNS DNS 配置模式 (config-ip-rns-dns)

IP RNS ICMP-Echo 配置模式 (config-ip-rns-icmp-echo)

【使用指导】 TOS 是 IPv4 报文首部中的一个 8bit 字段。通过设置 TOS，可以控制探测报文的优先级。不同的 TOS，中间路由器的处理优先程度不同。

配置举例

以下配置举例，仅介绍与 icmp-echo 相关的配置。

【网络环境】

图 2-3



【配置方法】 在 switch A 上配置 RNS 探测实例 1 及相应参数

Switch A

```
A# configure terminal
A(config)# ip rns 1
A(config-ip-rns)#icmp-echo 10.2.2.2
A(config-ip-rns-icmp-echo)#exit
A(config)#ip rns schedule 1 start-time now life forever
```

【检验方法】 通过 **show ip rns configuration** 命令显示实例配置信息

Switch A

```
A#show ip rns configuration 1
Entry number: 1
Tag:
Type of operation to perform: icmp-echo
Operation timeout (milliseconds): 5000
Operation frequency (milliseconds): 60000
Threshold (milliseconds): 5000
Recurring (Starting Everyday): FALSE
Life (seconds): foerver
Next Scheduled Start Time:Start Time already passed
Target address/Source address: 10.2.2.2/0.0.0.0
Request size (ARR data portion): 36
```

常见错误

无

2.4.3 配置dns探测

配置效果

创建一个 DNS 类型的 RNS 探测实例，进行 dns 探测。

注意事项

- 必须先配置 RNS 基本功能。

配置方法

↘ 创建 DNS 类型的 RNS 探测实例

- 必须配置。
- 若无特殊要求，应在每台交换设备上创建 DNS 类型的 RNS 探测实例。

↘ 配置探测通用可选参数

- 如果要求改变探测通用可选参数（重复时间间隔、标签、时间阈值、超时时间、TOS 字段等），则必须配置。
- 若无特殊要求，应在每台交换设备上配置探测通用可选参数。

检验方法

- 通过 **show ip rns configuration** 命令查看

相关命令

↘ 创建一个 DNS 类型的 RNS 探测实例

【命令格式】 **dns** { *destination-hostname* **name-server** *ip-address* [**source-ipaddr** *ip-address*] [[**af-direct**] **out-interface** *type num* [**next-hop** *ip-address*]] }

【参数说明】 *destination-hostname*：目的主机域名。

name-server *ip-address*：DNS 服务器 IP 地址。

source-ipaddr *ip-address*：源 IP 地址。

out-interface type *num*：指定探测报文的出接口。

af-direct：配置 RNS 探测不经过协议栈收发报文。

next-hop *ip-address*：指定出接口时，下一跳 ip 地址。

【命令模式】 IP RNS 配置模式(config-ip-rns)

【使用指导】 DNS 类型的 RNS 探测启动后将发送 DNS 解析请求报文以探测本机到目标主机网络是否连通。创建 DNS 类型的 RNS 探测后将进入 IP RNS DNS 模式。

您必须先配置 RNS 探测的类型，然后再配置该探测类型的具体参数。如果要修改一个 RNS 探测的探测类型，必须先删除该 RNS 探测（通过全局模式下输入 **no ip rns** 命令），再重新进行配置。

↘ 配置探测的重复时间间隔

【命令格式】 **frequency** *milliseconds*

【参数说明】 *milliseconds*：报文的发送时间间隔（毫秒），默认值 60000 毫秒，范围<10-604800000>，最长一周时间。

【命令模式】 IP RNS DNS 配置模式 (config-ip-rns-dns)

IP RNS ICMP-Echo 配置模式 (config-ip-rns-icmp-echo)

【使用指导】 在一个 RNS 探测实例启动后，会进行周期性的探测。通过配置 **frequency** 命令，可以指定该重复间隔。配置 **frequency** 应当满足下面的公式，以保证探测的计算正确。

(**frequency** *milliseconds*) > (**timeout** *milliseconds*) >= (**threshold** *milliseconds*)

↘ 为 RNS 探测实例设置一个标签

【命令格式】 **tag** *text*

【参数说明】 *text*：设置探测的标签，tag 由可打印字符组成，最长允许输入 79 个字符。

【命令模式】 IP RNS DNS 配置模式 (config-ip-rns-dns)

IP RNS ICMP-Echo 配置模式 (config-ip-rns-icmp-echo)

【使用指导】 tag 可以为探测指定一个标签，通常用于标识这个探测的作用。

配置 RNS 探测实例的时间阈值

【命令格式】 **threshold** *milliseconds*

【参数说明】 *milliseconds*：探测的时间阈值，取值范围为 0-60000，单位 ms，默认值 5000。

【命令模式】 IP RNS DNS 配置模式 (config-ip-rns-dns)

IP RNS ICMP-Echo 配置模式 (config-ip-rns-icmp-echo)

【使用指导】 配置 **threshold** 应当满足下面的公式，以保证探测的计算正确。

(**frequency** *milliseconds*) > (**timeout** *milliseconds*) >= (**threshold** *milliseconds*)

配置 RNS 探测实例的超时时间

【命令格式】 **timeout** *millisecond*

【参数说明】 *millisecond*：探测超时时间，取值范围为 10-604800000，单位 ms，不同探测类型，其超时默认值不同。

【命令模式】 IP RNS DNS 配置模式 (config-ip-rns-dns)

IP RNS ICMP-Echo 配置模式 (config-ip-rns-icmp-echo)

【使用指导】 配置 **timeout** 应当满足下面的公式，以保证探测的计算正确。

(**frequency** *milliseconds*) > (**timeout** *milliseconds*) >= (**threshold** *milliseconds*)

配置 RNS 探测的 IPv4 报文 TOS 字段

【命令格式】 **tos** *number*

【参数说明】 *number*：设置探测报文 IPv4 首部的 TOS 字段，取值范围 0-255。默认为 0。

【命令模式】 IP RNS DNS 配置模式 (config-ip-rns-dns)

IP RNS ICMP-Echo 配置模式 (config-ip-rns-icmp-echo)

【使用指导】 TOS 是 IPv4 报文首部中的一个 8bit 字段。通过设置 TOS，可以控制探测报文的优先级。不同的 TOS，中间路由器的处理优先程度不同。

配置举例

以下配置举例，仅介绍与 dns 相关的配置。

【网络环境】 图 2-4



【配置方法】 在 switch A 上配置 RNS 探测实例 1 及相应参数

Switch A

```
A# configure terminal
A(config)# ip rns 1
A(config-ip-rns)# dns www.ruijie.com.cn name-server 10.2.2.2
A(config-ip-rns-dns)#exit
A(config)ip rns schedule 1 start-time now life forever
```

【检验方法】 通过 **show ip rns configuration** 命令显示实例配置信息

Switch A

```
A#show ip rns configuration 1
Entry number: 1
Tag:
Type of operation to perform: dns
Operation timeout (milliseconds): 5000
Operation frequency (milliseconds): 60000
Threshold (milliseconds): 5000
Recurring (Starting Everyday): FALSE
Life (seconds): foerver
Next Scheduled Start Time:Start Time already passed
Target host name: www.ruijie.com.cn
Name Server: 10.2.2.2
```

常见错误

- 域名解析服务器 IP 地址错误

2.4.4 配置track联动功能

配置效果

- 配置 track 与 rns 联动，track 能跟踪一个 RNS 探测的探测结果。
- 配置 track 跟踪一个接口的链路状态。
- 配置 track 跟踪一个 track 列表的状态。
- 跟踪一个 RNS 探测列表的状态。

注意事项

- 如果配置 track 跟踪一个 RNS 探测的探测结果，则需要配置相应的 RNS 探测。
- 如果配置 track 跟踪一个接口的链路状态，则需要配置相应的接口。
- 如果配置 track 跟踪一个 track 列表的状态，则需要配置相应的 track 列表成员。
- 如果配置 track 跟踪一个 RNS 探测列表的状态，则需要配置相应的 RNS 探测列表成员。

配置方法

↘ 配置 track 对象

- 如果要求创建 track 对象，则必须配置。

- 配置 track 对象的四种方法 :配置跟踪 RNS 探测的探测结果 ,配置跟踪接口的链路状态 ,配置跟踪一个 track 列表的状态，配置跟踪一个 RNS 探测列表的状态。
- 配置跟踪 RNS 探测的探测结果：若无特殊要求，应在每台交换设备上配置跟踪 RNS 探测的探测结果的 track 对象。
- 配置跟踪接口的链路状态：若无特殊要求，应在每台交换设备上配置跟踪接口的链路状态的 track 对象。
- 配置跟踪 track 列表的状态：若无特殊要求，应在每台交换设备上配置跟踪 track 列表状态的 track 对象。
- 配置跟踪 RNS 探测列表的状态：若无特殊要求，应在每台交换设备上配置跟踪 RNS 探测列表状态的 track 对象。

配置 track 对象的延迟通告时间

- 若需要延迟通告 track 对象的状态，则必须设置 track 的延迟通告时间。。
- track 状态的延迟通告时间包括两种：track 状态由 up 变为 down 的延迟通告时间、track 状态由 down 变为 up 的延迟通告时间。可设置其中一种，也可两者都进行设置。
- 若无特殊要求，应在每台交换设备上配置 track 对象的延迟通告时间。

配置 track 成员

- 如果配置 track 对象用于跟踪一个 track 列表的状态，必须配置。
- 配置 track 成员，可配置其满足条件时的状态为 up 或 down。
- 若无特殊要求，应在每台交换设备上配置 track 成员。

检验方法

使 track 跟踪的对象（如 RNS 探测的探测结果、接口的链路状态、track 列表的状态）状态发生变化，观察相应的 track 对象的状态。

- 经过设置的延迟时间后，通过 **show track** 命令查看当前 track 的状态是否发生变化。

相关命令

配置跟踪接口链路状态的 track 对象

【命令格式】 **track** *object-number* **interface** *interface-type interface-number* **line-protocol**

【参数说明】 *object-number*：track 对象的编号，取值范围为 1-700。

Interface-type interface-number：接口类型及接口编号。

【命令模式】 全局模式

【使用指导】 使用该命令配置一个 track 对象，用来跟踪一个接口的链路状态。当接口链路状态为 up 时，相应的 track 对象状态为 up。

配置跟踪 RNS 探测的探测结果的 track 对象

【命令格式】 **track** *object-number* **rns** *entry-number*

【参数说明】 *object-number*：track 对象的编号，取值范围为 1-700。

entry-number：RNS 探测实例编号，取值范围为 1-500。

【命令模式】 全局模式

【使用指导】 使用该命令配置一个 track 对象，用来跟踪一个 RNS 探测的探测结果。当 RNS 探测的探测结果成功时，则相应的 track 对象状态为 up。

配置跟踪 track 列表状态的 track 对象

【命令格式】 **track** *object-number* **list boolean** { **and** | **or** }

【参数说明】 *object-number*：track 对象的编号，取值范围为 1-700。

【命令模式】 全局模式

【使用指导】 该命令配置一个 track 对象，用来跟踪一个 track 列表的状态。其结果可以是所有成员状态取“与”或者“或”的结果。

配置 track 成员

【命令格式】 **object** *object-number* [**not**]

【参数说明】 *object-number*：track 对象的编号，取值范围为 1-700。

【命令模式】 track 配置模式

【使用指导】 该命令配置一个 track 跟踪的 list 对象的成员对象，可以配置的对象个数仅受 track 对象容量的限制。

配置 track 的延迟时间

【命令格式】 **delay** { **up** *seconds* [**down** *seconds*] **|** [**up** *seconds*] **down** *seconds* }

【参数说明】 **up** *seconds*：指定 track 状态由 down 变为 up 的延迟时间，取值范围为 0-180，单位为秒。缺省为 0。
down *seconds*：指定 track 状态由 up 变为 down 的延迟时间，取值范围为 0-180，单位为秒。缺省为 0。

【命令模式】 track 配置模式

【使用指导】 当 track 对象的状态不停的震荡，会使得使用该 track 对象的客户端状态也跟着不停变化。
使用该命令可以延迟通告 track 对象状态的变化。比如某一个 track 对象的状态由 up 变为 down，如果用户配置了 delay **down 10**，则 track 对象的 down 状态在 10 秒后才会通告。如果在这段时间内，track 对象的状态又变为 up，那就不会通告。在使用该 track 对象的客户端看来，track 对象的状态一直是 up 的。

显示 track 的统计信息

【命令格式】 **show track** [*object-number*]

【参数说明】 *object-number*：指定 track 对象的编号，取值范围 1-700。缺省为所有 track 对象。

【命令模式】 特权模式

【使用指导】 使用该命令可以查看 track 对象的统计信息。

配置举例

配置 track 对象(编号为 3)，跟踪一个接口（FastEthernet 1/0）的链路状态。

【配置方法】
- 配置 track 对象，跟踪一个接口的链路状态。
- 配置状态由 up 变为 down 的延迟时间。

```
Ruijie# configure terminal
Ruijie(config)# track 3 interface FastEthernet 1/0 line-protocol
Ruijie(config-track)# delay down 10
Ruijie(config-track)# exit
```

【检验方法】 使接口 FastEthernet 1/0 的链路状态变为 down。

- 立即检查 track 的状态，确认仍旧为 up。
- 过 10s 后，再次检查 track 的状态，确认 track 的状态变为 down

```
Ruijie# show track 3

Track 3

  Interface FastEthernet 1/0

  The state is Up, delayed Down (5 secs remaining)

    1 change, current state last: 300 secs

  Delay up 0 secs, down 10 secs
```

↘ 配置一个 track 对象编号 3，当 track 对象 1 为 up，2 为 down 同时满足时，track 对象 3 为 up。

【配置方法】

- 配置 track 1 和 track 2；
- 配置 track 3，其成员为 track 1 和 track 2。

```
Ruijie # config
Ruijie(config)#track 1 interface gigabitEthernet 0/0 line-protocol
Ruijie(config-track)#delay up 20 down 40
Ruijie(config-track)#exit
Ruijie(config)#
Ruijie(config)#track 2 interface gigabitEthernet 0/1 line-protocol
Ruijie(config-track)#delay down 30
Ruijie(config-track)#exit
Ruijie(config)# track 3 list Boolean and
Ruijie(config-track)#object 1
Ruijie(config-track)#object 2 not
Ruijie(config-track)# exit
```

【检验方法】 使 track 1 和 track 2 的状态发生变化，查看 track 3 的状态。

- track 1 的状态由 down 变为 up，track 2 状态保持 down 不变，确认 track 3 的状态由 down 变为 up。
- track 1 的状态保持 up 不变，track 2 状态由 down 变为 up，确认 track 3 的状态由 up 变为 down。

```
Ruijie# show track 3


Track 3
  List boolean and
  Object 1
```

【配置方法】
- 配置 track 1 和 track 2；
- 配置 track 3，其成员为 track 1 和 track 2。

```
Ruijie # config
Ruijie(config)#track 1 interface gigabitEthernet 0/0 line-protocol
Ruijie(config-track)#delay up 20 down 40
Ruijie(config-track)#exit
Ruijie(config)#
Ruijie(config)#track 2 interface gigabitEthernet 0/1 line-protocol
Ruijie(config-track)#delay down 30
Ruijie(config-track)#exit
Ruijie(config)# track 3 list Boolean and
Ruijie(config-track)#object 1
Ruijie(config-track)#object 2 not
Ruijie(config-track)# exit
```

【检验方法】 使 track 1 和 track 2 的状态发生变化，查看 track 3 的状态。
- track 1 的状态由 down 变为 up，track 2 状态保持 down 不变，确认 track 3 的状态由 down 变为 up。
- track 1 的状态保持 up 不变，track 2 状态由 down 变为 up，确认 track 3 的状态由 up 变为 down。

```
 Object 2 not
 The state is Down
   1 change,current state last:10 secs
 Delay up 0 secs,down 0 secs
```

↘ 配置 track 对象(编号为 5)，跟踪一个 RNS 探测（编号为 7）的探测结果。

【配置方法】
- 配置一个 RNS 探测
- 配置 track 对象，跟踪一个 RNS 探测的探测结果。
- 配置探测结果由 up 变为 down、由 down 变为 up 的延迟通告时间。

```
Ruijie# configure terminal
Ruijie (config)#ip rns 7
Ruijie (config-ip-rns)#icmp-echo 2.2.2.2
Ruijie (config-ip-rns-icmp-echo)#exit
Ruijie (config)#ip rns schedule 7 start-time now life forever
Ruijie(config)# track 5 rns 7
Ruijie (config-track)# delay up 20 down 30
Ruijie (config-track)# exit
```

【检验方法】 使编号为 7 的 RNS 探测结果由成功变为失败。
- 探测结果变为失败时立即检查 track 的状态，确认仍旧为 up。
- 过 30s 后，再次检查 track 的状态，确认 track 的状态变为 down。

```
Ruijie# show track 5

Track 5
```

【配置方法】
- 配置一个 RNS 探测
- 配置 track 对象，跟踪一个 RNS 探测的探测结果。
- 配置探测结果由 up 变为 down、由 down 变为 up 的延迟通告时间。

```
Ruijie# configure terminal
Ruijie (config)#ip rns 7
Ruijie (config-ip-rns)#icmp-echo 2.2.2.2
Ruijie (config-ip-rns-icmp-echo)#exit
Ruijie (config)#ip rns schedule 7 start-time now life forever
Ruijie(config)# track 5 rns 7
Ruijie (config-track)# delay up 20 down 30
Ruijie (config-track)# exit
```

【检验方法】 使编号为 7 的 RNS 探测结果由成功变为失败。
- 探测结果变为失败时立即检查 track 的状态，确认仍旧为 up。
- 过 30s 后，再次检查 track 的状态，确认 track 的状态变为 down。

```
 Reliable Network Service 7

 The state is Down

   2 change, current state last: 10 secs

 Delay up 20 secs, down 30 secs
```

配置 track 对象(编号为 5)，跟踪一个 RNS 探测列表（编号分别为 1,2-5,8）的探测结果。

【配置方法】
- 配置并启动 RNS 探测（参见 RNS 配置）
- 配置 track 对象，跟踪一个 RNS 探测列表的探测结果。
- 配置探测结果由 up 变为 down、由 down 变为 up 的延迟通告时间。

```
Ruijie(config)# track 5 rns-list 1,2-5,8 and
Ruijie (config-track)# delay up 20 down 30
Ruijie (config-track)# exit
```

【检验方法】 使编号为 1,2,-5,8 的 RNS 探测中的一个结果由成功变为失败。
- 探测结果变为失败时立即检查 track 的状态，确认仍旧为 up。

过 30s 后，再次检查 track 的状态，确认 track 的状态变为 down。

```
Ruijie# show track 5

Track 5

 rns-list 1,2-5,8 and

 The state is Down

   2 change, current state last: 10 secs
   Delay up 20 secs, down 30 secs
```

常见配置错误

- 配置了跟踪 RNS 探测的 track，但未配置相应的 RNS 探测。
- 配置了跟踪接口链路状态的 track，但未配置相应的接口。
- 配置了跟踪 track 列表的 track 对象，但未配置相应的 track 成员。
- 配置了跟踪 RNS 探测列表的 track，但未配置相应的 RNS 探测。

2.5 监视与维护

查看运行情况

作用	命令
查看 rns 对象的配置信息。	**show ip rns configuration** [*operation-number*]
查看 rns 对象探测的详细统计信息。	**show ip rns collection-statistics** [*operation-number*]
查看 rns 对象探测的当前状态信息。	**show ip rns operational-state** [*operation-number*]
查看 rns 对象探测的主动阈值监控信息。	**show ip rns reaction-configuration** [*operation-number*]
查看 rns 对象探测的触发探测信息。	**show ip rns reaction-trigger** [*operation-number*]
查看 rns 对象的简单统计信息。	**show ip rns statistics** [*operation-number*]
查看 track 对象的统计信息。	**show track** [*object-number*]
查看 track 客户端的统计信息。	**show track client**

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 track 模块相关的调试开关。	**debug track** { **all** | **proc-event** | **rdnd-event** | **client** }
打开 rns 模块相关的调试开关。	**debug rns** { **all** | **interface** | **lib** | **rdnd-event** | **restart** | **rns_id** [**0, 500**] }

配置指南-设备管理

本分册介绍设备管理相关内容，包括以下章节：

1. DEV-AUDIT
2. USB
3. USER-TASK
4. SERVICE-MANAGER

1 DEV-AUDIT

1.1 概述

DEV-AUDIT（Divice Audit，设备审计）是用于监控设备运行情况。工作原理是定期记录设备 CPU、内存、磁盘空间使用情况。用户通过查看记录，可监控一段时间内设备系统的运行情况。

DEV-AUDIT 审计信息记录在 sata 硬盘或 USB 等内部存储的数据库中，对于没有内部存储的设备，可支持发送日志。

协议规范

- 无

1.2 典型应用

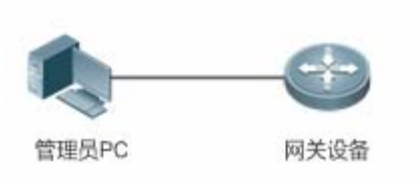
典型应用	场景描述
开启设备审计功能	网络管理员想要了解设备运行情况

1.2.1 开启设备审计功能

应用场景

开启设备审计功能后，设备自动定期记录 cpu、内存、磁盘等使用情况。设备管理员登录设备后，查看记录可监控设备近期的运行情况。

图 1-1





【注释】 管理员通过登录设备的 web，查看设备审计记录

功能部属

- 直接开启即可使用

1.3 功能详解

基本概念

↘ CPU 利用率、内存使用率、磁盘使用情况

开启设备审计后，每 5 分钟读取系统 CPU 使用情况；每 5 分钟读取系统总内存和可用内存，计算内存使用率；每 1 小时读取 flash 和 sata 硬盘的总空间及可用空间。在硬盘中保存近 90 天的记录数据。

功能特性

功能特性	作用
开启设备审计	开启设备审计功能

1.3.1 开启设备审计

开启设备审计后，定期记录设备运行相关数据，用于监控设备运行情况。

工作原理

开启设备审计后，每 5 分钟读取系统 CPU 使用情况；每 5 分钟读取系统总内存和可用内存，计算内存使用率；每 1 小时读取 flash 和 sata 硬盘的总空间及可用空间。在硬盘中保存近 90 天的记录数据。

相关配置

↘ 开启设备审计功能

缺省情况下，功能开启。

1.4 产品说明



NBR108G-P 不支持设备审计功能；NBR2500D-E、NBR3000D-E、NBR3000D-UE 带硬盘设备支持审计记录在本地；NBR800G、NBR950G、NBR1500G、NBR2000G、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1000G-E、

NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E 不支持本地记录 ;NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 带硬盘时支持审计记录在本地，默认不带硬盘时不支持。

1.5 配置详解

配置项	配置建议 & 相关命令	
开启设备审计功能	必须配置。	
	dev-audit enable	开启设备审计功能
配置设备审计告警水线	可选配置	

1.5.1 开启设备审计功能

配置效果

- 记录设备 cpu、内存、磁盘空间使用情况。

注意事项

- 带 sata 硬盘的设备才有记录。

配置方法

↘ 开启设备审计功能

- 必须配置。
- 在本机上配置开启。

检验方法

- 查看审计记录。

相关命令

↘ 开启设备审计功能

【命令格式】 **dev-audit enable**
【参数说明】 -
【命令模式】 全局配置模式

【使用指导】 -

配置举例

【配置方法】
- 开启设备审计功能

```
Ruijie# configure terminal
Ruijie(config)# dev-audit enable
```

【检验方法】 10 分钟后查看审计记录。

```
Ruijie# show dev-audit cpu from 2013 9 2 12:00:00
Date & Time             CPU
2013-09-02 12:03:11     2%
2013-09-02 12:08:11     2%
```

常见错误

- 无

1.5.2 配置设备审计告警水线

配置效果

- 当 buffer 使用率过高时，打印告警 log。
- 当接口 1 分钟内 no buffer 数增长过快，打印告警 log。
- 当流表连接数使用率过高，打印告警 log。
- 当 flash 或硬盘空间使用率过高，打印告警 log。

注意事项

- 无。

配置方法

↘ 开启设备审计告警水线

- 可选配置。
- 在本机上配置开启。

检验方法

- 查看配置结果。

相关命令

配置 buffer 使用率过高告警水线

【命令格式】 **dev-audit buffer high-watermark set up** *buffer-usage* **down** *buffer-usage*

【参数说明】 **up** *buffer-usage*： buffer 使用率上限，恢复到该值打印取消告警 log。可配置范围<1-99>，默认 75

down *buffer-usage*： buffer 使用率下限，达到该值打印告警 log。可配置范围<1-99>，默认 60

【命令模式】 全局配置模式

【使用指导】 buffer 使用率达到水线上限，打印告警 log。恢复到水线下限以下，打印取消告警 log。

可用 buffer 数不足，将影响内网用户上网。可用 buffer 数不足，可能是设备受到攻击导致。

配置接口 1 分钟内 no buffer 增长过快告警水线

【命令格式】 **dev-audit nobuffer high-watermark set up** *buffer-count* **down** *buffer-count*

【参数说明】 **up** *buffer-count*：接口 1 分钟内新增的 no buffer 数上限，达到该值打印告警 log。可配置范围<1-1000000>，默认 50000

down *buffer-count*：接口 1 分钟内新增的 no buffer 数下限，恢复到该值打印取消告警 log。可配置范围<1-1000000>，默认 500

【命令模式】 全局配置模式

【使用指导】 接口 1 分钟内 no buffer 数增长达到水线上限时，打印告警 log。恢复到水线下限以下后，打印取消告警 log。

接口 no buffer 数增长过快，将影响内网用户上网。接口 no buffer 数新增数过高，可能是设备受到攻击导致。

配置流表连接数使用率过高告警水线

【命令格式】 **dev-audit flow high-watermark set up** *unilization* **down** *unilization*

【参数说明】 **up** *unilization*：流表连接数使用率上限，使用率达到该值打印告警 log。可配置范围<1-99>，单位为：%，默认 90

down *unilization* 流表连接数使用率下限 ,使用率恢复到该值打印取消告警 log。可配置范围 1-99> ,单位为 :%，默认 75

【命令模式】 全局配置模式

【使用指导】 流表连接数使用率达到水线上限时，打印告警 log。恢复到水线下限以下后，打印取消告警 log。

流表连接数不足，将影响内网用户上网。流表连接数使用率过高，可能是设备受攻击导致。

配置 flash 或硬盘使用率过高告警水线

【命令格式】 **dev-audit flash high-watermark set up** *unilization* **down** *unilization*

【参数说明】 **up** *unilization*：flash 和硬盘使用率上限，使用率达到该值打印告警 log。可配置范围<1-99>，单位为：%，默认 90

down *unilization*：flash 和硬盘使用率下限，使用率恢复到该值打印取消告警 log。可配置范围 1-99>，单位为：%，默认 75

【命令模式】 全局配置模式

【使用指导】 flash 或硬盘使用率达到水线上限时，打印告警 log。恢复到水线下限以下后，打印取消告警 log。

flash 或硬盘空间不足，将影响一些功能使用，如升级、各种审计的记录。

配置举例

【配置方法】

- 配置 flash 告警水线为 90%，取消告警为 75%

```
Ruijie# configure terminal
Ruijie(config)# dev-audit flash high-watermark set up 90 down 75
Set flash high-watermark up 90% down 75%
```

【检验方法】 show run 查看配置。

```
Ruijie# show run
dev-audit flash high-watermark set up 90 down 75
```

常见错误

- 无

1.6 监视与维护

清除各类信息

无

查看记录

作用	命令
查看设备审计信息。	**show dev-audit** { **cpu** | **memory** | **flash** } **from** *year* [*month* [*mday* [*hh:mm:ss*]]] [**to** *year* [*month* [*mday* [*hh:mm:ss*]]]]

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
打开设备审计的调试开关。	**debug dev-audit errors**

2 USB

2.1 概述

USB（Universal Serial Bus，通用串行总线）是一种外部总线标准，这里指的是遵循 USB 标准的外围设备，如 U 盘。

USB 是一种热拔插产品，用户可以使用它，将通信设备内的文件（例如配置文件、日志文件等）数据方便地拷贝复制出来，也可以将外部的数据（例如系统升级文件）拷贝至设备内部存储器。

USB 的具体应用场景请参见不同功能的配置指南，这里只介绍 USB 产品的识别、查看、使用、卸载等。

2.2 典型应用

典型应用	场景描述
利用 USB 升级设备	U 盘中存放着升级文件，设备上电后，检测到 U 盘，执行升级命令，从中加载升级文件，加载成功后，设备复位，运行升级的新版本。

2.2.1 利用USB升级设备

应用场景

U 盘中存放着升级文件，设备上电后，检测到 U 盘，执行升级命令，从中加载升级文件，加载成功后，设备复位，运行升级的新版本。如：

upgrade usb0:/s12k-ppc_11.0(1B2)_20131025_main_install.bin。

执行上面的命令，若文件有效，命令执行成功，设备会自动复位，运行新的版本。

功能部属

- 用 usb0:/ 前缀，访问 USB 0 设备，**show usb** 可以看到 id 为 0 的设备相关信息。
- **upgrade** 命令是升级功能相关命令。

2.3 功能详解

↘ USB 的使用

将 USB 产品插入 USB 插槽 ,系统会自动查找 USB 产品，找到后驱动模块会自动对它进行驱动初始化，成功初始化 USB 产品之后，自动加载里面的文件系统，后面就可以读写这个 USB 产品了。

- 系统找到 USB 产品并加载驱动成功的话，会打印出如下的提示信息：

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

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

USB 的卸载

使用 CLI 命令先将 USB 产品进行移除，以防系统正在使用设备，导致出错。

- 如果 USB 产品移除成功，会打印如下提示信息：

```
OK, now you can pull out the device 0.
```

在打印出如上面的提示信息后，方可拔出 USB 产品。

2.4 产品说明

NBR1500G、NBR2000G 不支持 USB 接口；NBR108G-P 、NBR800G、NBR950G、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 USB 接口。

2.5 配置详解

配置项	配置建议 & 相关命令	
使用 USB	必须配置。	
	无	
卸载 USB	必须配置。卸载 USB 产品。	
	usb remove	移除 USB 产品

2.5.1 使用USB

配置效果

USB 产品加载到系统后，可以直接使用文件系统的命令（**dir，copy，del** 等）对 USB 产品进行操作。

注意事项

- RGOS 系统只能使用支持标准 SCSI 指令的产品（一般通用的 U 盘），非标准 SCSI 指令的产品在系统中无法使用（比如 USB 上网卡附带的 U 盘，附带虚拟 USB 光驱的 U 盘），另外有些产品配置了 USB 转串口功能。
- USB 产品仅支持 FAT 文件系统，其他文件系统的 USB 产品需要在 PC 上格式成 FAT 文件系统后，才能在设备上使用。
- RGOS 系统支持 HUB ,U 盘接在 HUB 端口时 ,设备访问的路径不同。U 盘直接插入设备 USB 端口 ,设备访问路径是 usbX:/ ，其中 X 表示 device id ,show usb 可以查看到 ;U 盘插在 HUB 端口 ,HUB 插在设备 USB 端口 ,设备访问路径是 usbX-Y:/ ，其中 X 表示 device id, Y 表示 HUB 端口号，比如 usb0-3:/ 表示设备 0 号 USB 端口上的 HUB 所属的 3 号端口。

配置方法

识别 USB

USB 产品的插入无需命令行操作，直接将其插入 USB 插槽即可。

使用 USB

如下操作是将 USB 产品中的文件复制到 flash 中。

- 使用 **cd** 命令进入 USB 产品分区
- 使用 **copy** 命令将 USB 产品中的文件复制到设备的 flash 中。
- 使用 **dir** 命令查看文件是否已添加在设备中。

当 USB 产品上有多个分区的时候，在设备上仅能访问第一个 FAT 分区。

USB 产品的路径不存在上层目录的概念。通过“cd usbX:\”进入 USB 产品后，通过“cd flash:\”返回 flash 文件系统。

检验方法

使用 **show usb** 命令查看已插入的 USB 产品的信息。

相关命令

无

配置举例

使用 USB

【网络环境】 单机环境

【配置方法】
- 将 U 盘插入设备 USB 插槽。
- 在设备控制台执行 **show usb** 命令。
- 将 U 盘里的 config.txt 文件拷贝至设备 flash。

```
Ruijie#show usb
```

```
Device: Mass Storage
ID: 0
URL prefix: usb0
Disk Partitions:
usb0(type:vfat)
Size:15789711360B(15789.7MB)
Available size:15789686784B(15789.6MB)
Ruijie#
Ruijie#dir usb0:/
Directory of usb0:/
   1 -rwx             4  Tue Jan  1 00:00:00 1980  fac_test
   2 -rwx             1  Mon Sep 30 13:15:48 2013  config.txt
2 files, 0 directories
15,789,711,360 bytes total (15,789,686,784 bytes free)
Ruijie#
Ruijie#
Ruijie#copy usb0:/config.txt flash:/
Copying: !
Accessing usb0:/config.txt finished, 1 bytes prepared
Flushing data to flash:/config.txt...
Flush data done
Ruijie#
```

【检验方法】

- 查看 flash 中是否有 config.txt 文件

```
Ruijie#
Ruijie#dir flash:/
Directory of flash:/
   1 drw-           160  Wed Mar 31 08:40:01 2010  at
   2 drwx           160  Thu Jan  1 00:00:11 1970  dm
   3 drwx           160  Thu Jan  1 00:00:05 1970  rep
   4 drwx           160  Mon Apr 26 03:42:00 2010  scc
   5 drwx           160  Wed Mar 31 08:39:52 2010  ssh
   6 drwx           224  Thu Jan  1 00:00:06 1970  var
   7 d---           288  Sat May 29 06:07:45 2010  web
   8 drwx           160  Thu Jan  1 00:00:11 1970  addr
```

```
  9 drwx            160  Sat May 29 06:07:44 2010  cwmp
 10 drwx            784  Sat May 29 06:07:47 2010  sync
 11 --w-             92  Tue Feb  2 01:06:55 2010  config_vsu.dat
 12 -rw-            244  Sat Apr  3 04:56:52 2010  config.text
 13 -rwx              1  Thu Jan  1 00:00:30 1970  .issu_state
 14 -rw-              0  Tue Feb  2 01:07:03 2010  ss_ds_debug.txt
 15 -rw-           8448  Thu Jan  1 00:01:41 1970  .shadow
 16 -rwx            268  Thu Jan  1 00:01:41 1970  .pswdinfo
 17 -rw-              4  Tue May 25 09:12:01 2010  reload
 18 drwx            232  Wed Mar 31 08:40:00 2010  snpv4
 19 drwx           6104  Sat May 29 06:10:45 2010  .config
 20 ----              1  Thu Jan  1 00:04:51 1970  config.txt
 21 d---            160  Thu Jan  1 00:00:12 1970  syslog
 22 drwx            160  Tue May 25 03:05:01 2010  upgrade_ram
 23 drwx            160  Tue Feb  2 01:06:54 2010  dm_vdu
 24 -rwx             16  Thu Jan  1 00:01:41 1970  .username.data
9 files, 15 directories
5,095,424 bytes total (4,960,256 bytes free)
Ruijie#
```

常见错误

- 使用了非标准 SCSI 指令的产品插入设备中。
- USB 产品为非 FAT 文件系统，则系统无法识别。

2.5.2 卸载USB

配置效果

卸载 USB 产品，并使 USB 产品及设备保持完好。

注意事项

- 一定要先执行移除命令移除设备后再拔出，以免系统出现错误。

配置方法

↘ 移除 USB

- 必须配置。

- 应在每次卸载 USB 产品时先对其执行移除命令。

拔出 USB

在成功执行移除命令后，直接将 USB 产品拔出即可。

检验方法

使用 **show usb** 命令查看已插入的 USB 设备的信息。

相关命令

移除 USB 产品

【命令格式】 **usb remove** *device-id*

【参数说明】 *device-id*：设备上 USB 接口号，它是 USB 显示信息中的 ID 号。该号可以通过 **show usb** 来获取。

【命令模式】 特权模式

【使用指导】 在拔出 USB 产品之前，需要用命令移除该产品，以防系统正在使用而导致错误。若移除成功，系统会打印出提示，此时方可拔出设备。如果移除失败，说明系统正在使用该 USB 产品，请在系统未使用 USB 产品时再执行移除操作。

配置举例

卸载 USB

【网络环境】 单机环境

【配置方法】
- 执行 **show usb** 命令查看 USB 设备的 ID 信息。
- 执行 **usb remove** 命令卸载 USB 设备。

```
Ruijie#show usb
Device: Mass Storage
ID: 0
URL prefix: usb0
Disk Partitions:
usb0(type:vfat)
Size:15789711360B(15789.7MB)
Available size:15789686784B(15789.6MB)
Ruijie#
Ruijie#
Ruijie#usb remove 0

OK, now you can pull out the device 0.
```

【检验方法】

- 再次执行 **show usb** 命令，查看 USB 设备是否已经卸载。**show usb** 命令不显示 id 为 0 的设备。

```
Ruijie#show usb
Ruijie#
```

常见错误

无

2.6 监视与维护

查看运行情况

作用	命令
查看已插入的 USB 设备信息。	**show usb**

3 USER-TASK

3.1 概述

USER-TASK（User Task，用户任务）是用于定时在设备上执行指定的 CLI 命令。工作原理是通过配置添加需要执行的 CLI 命令，到达配置的执行时间后，设备自动地执行该命令，达到无人值守的目的。

3.2 典型应用

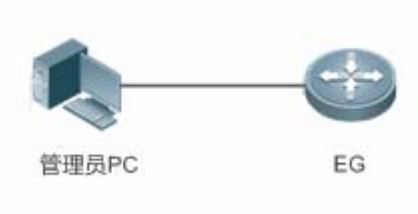
典型应用	场景描述
定时重启	网络管理员想要在每周的固定时间重启设备
设备信息收集	网络管理员、故障支持人员想要定时执行 show 命令搜集想要的信息

3.2.1 定时重启

应用场景

网络管理员想要在每周日凌晨两点维护网络的时候重启网关设备。

图 3-1



【注释】 网络管理员通过登录设备的 WEB 页面，进行相应的功能配置。

功能部署

开启用户任务功能

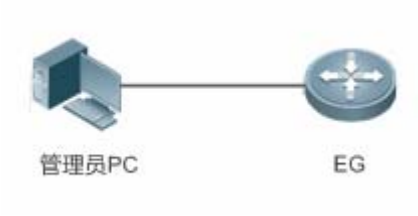
配置每周日凌晨两点重启设备

3.2.2 设备信息收集

应用场景

网络管理员/故障支持人员想要在设备上定时执行一些 show 命令并登录设备查看执行结果，以防通过 telnet 执行脚本的时候发生网络中断、tty 超时等意外导致没能及时收集信息。

图 3-2



【注释】 网络管理员通过登录设备的 WEB 页面，进行相应的功能配置。

功能部署

开启用户任务功能

开启用户任务日志功能

配置想要执行的 show 命令

登录设备查看执行结果

3.3 功能详解

基本概念

↘ 用户任务日志

启用了用户日志功能后，所有的任务执行命令后，如果有结果输出（无论执行成功还是失败），均会记录该结果以及该任务的计划时间与执行时间等相关信息，方便用户查看。

↘ 命令模式

命令模式分为特权模式与全局配置模式，配置为特权模式的时候执行权限为特权模式权限（即登录设备后的 Ruijie#，通常用于执行 show 命令）；全局配置模式则是执行权限为配置模式权限（即输入 config 后进入的 Ruijie(config)#，通常用于配置一些命令）。

↘ 命令序列

有些命令需要在多级模式下配置，比如应用识别的自定义应用组添加删除应用，需要按顺序执行如下命令：

```
Ruijie(config)#identify-application custom-group test_group
Ruijie(config-custom-group)#app-add 即时通讯软件
```

这些需要按顺序执行的命令即为命令序列。在 CLI 中添加任务执行命令序列时，各条命令之间要按顺序以“@”符号间隔。

功能特性

功能特性	作用
配置用户任务	开启并配置用户任务，定时执行任务中的 CLI 命令

3.3.1 配置用户任务

开启用户任务功能后，通过配置用户任务，可以定时执行 CLI 命令。

工作原理

配置用户任务后，会往任务数据库中记录所配置的任务信息，当用户任务功能启用时，每分钟会读取任务数据库，调出其中计划时间已经到期的任务，逐个执行其中的 CLI 命令。若同时开启用户任务日志功能，则会记录 CLI 命令的执行结果。

相关配置

↘ 启动用户任务功能

缺省情况下，用户任务功能打开。

使用 **user-task enable** 命令可以启动或关闭用户任务功能。

关闭用户任务功能后，依然能够新增/修改/删除用户任务，只是不再执行任务数据库中的任务。

↘ 启动用户任务日志功能

缺省情况下，用户任务日志功能关闭。

使用 **user-task log enable** 命令可以启动或关闭用户任务日志功能。

关闭用户任务日志功能后，不再记录任务执行结果，但能查看之前的日志。

3.4 产品说明

NBR1500G、NBR2000G、NBR108G-P 、NBR800G、NBR950G、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR1000G-C、NBR2000G-C、NBR3000G-S 不支持用户任务； NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持用户任务。

3.5 配置详解

配置项	配置建议 & 相关命令
配置用户任务	必须配置。用于添加/删除/修改任务。

	user-task enable	启动用户任务功能
	user-task	配置用户任务
配置用户任务日志	可选配置。用于配置用户任务日志功能。	
	user-task log	启动用户任务日志功能

3.5.1 配置用户任务

配置效果

- 添加用户任务，可以指定一个时间执行想要的 CLI 命令。

注意事项

- 必须打开用户任务功能后所配置的用户任务才能够被调度。
- 最多允许同时存在 1000 条任务。

配置方法

↘ 启动用户任务功能

- 必须配置。

↘ 配置用户任务

- 必须配置
- 在设备上添加/删除/修改用户任务

检验方法

- 查看用户任务库

相关命令

↘ 启动用户任务功能

【命令格式】 **user-task enable**
【参数说明】 **-**
【命令模式】 全局配置模式
【使用指导】 -

↘ 添加用户任务

【命令格式】 **user-task add** *task-name* **command** *cli-string* **mode** { **exec** | **config** } [**date** *YYYY MM DD*] **time** *hh:mm* [**every** { *mmm* | *hhh:mm* }]

【参数说明】 *task-name*：任务名。

command *cli-string*：待执行的 CLI 命令或命令序列。

exec：特权模式。

config：全局配置模式。

date *YYYY MM DD*：任务执行日期。

time *hh:mm*：任务执行时间。

every { *mmm* | *hhh:mm* }：任务循环时间

【命令模式】 特权模式

【使用指导】 此命令用来添加用户任务。

CLI 命令如果有空格必须在两端用双引号包含，如果是序列则必须以“@”符号间隔，如果命令中带有“@”符号，必须使用“\@”代替，以便和分隔符区分。

如果任务未指定日期，则默认为当天，但如果任务时间比当前时间早，则日期为第二天。

若未配置循环时间，则任务为一次性任务，不会循环。

上述均可通过 modify 命令修改。

注意：若配置的日期+时间早于当前的日期+时间，则任务会立即被执行，包括重启命令！

删除用户任务

【命令格式】 **user-task delete** *task-name*

【参数说明】 *task-name*：任务名。

【命令模式】 特权模式

【使用指导】 -

修改用户任务

【命令格式】 **user-task modify** *task-name* { **mode** { **exec** | **config** } | **date** *YYYY MM DD* | **time** *hh:mm* | **every** { *mmm* | *hhh:mm* } }

【参数说明】 *task-name*：任务名。

exec：特权模式。

config：全局配置模式。

date *YYYY MM DD*：任务执行日期。

time *hh:mm*：任务执行时间。

every { *mmm* | *hhh:mm* }：任务循环时间

【命令模式】 特权模式

【使用指导】 此命令用来修改指定任务的属性。

如果要修改多项属性（比如时间+循环时间），则必须分次修改。

查看用户任务库

【命令格式】 **show user-task**

【参数说明】 **-**

【命令模式】 特权模式、全局模式、接口模式

【使用指导】 查看是否成功添加/删除/修改任务。

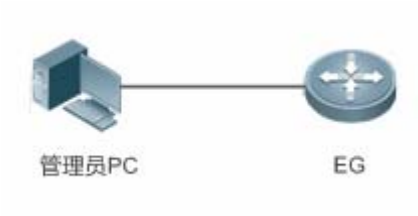
查看用户任务功能与用户任务日志功能的开关情况。

配置举例

配置定时重启

【网络环境】

图 3-3



【配置方法】

- 启动用户任务功能，在设备上添加一个任务，指定每周日凌晨两点进行重启设备操作（reload 命令需要再次输入 yes 进行确认重启，因此需要命令序列）。

```
Ruijie# configure terminal
Ruijie(config)# user-task enable
Ruijie(config)# exit
Ruijie# user-task add 重启任务 command “reload@y” mode exec date 2014 9 21 time 2:00 every 168
```

【检验方法】

- 查看用户任务库。
- 到时间后执行 show version 查看起机时间看是否重启。

```
Ruijie# show user-task
User-task: enable
User-task log: unable
Time              Name             Mode    Loop    Command-sequence
2014-09-21 02:00 重启任务          exec    168h    reload
                                                   y
```

常见错误

- CLI 命令没有加引号
- CLI 命令序列没有用“@”符号间隔
- 任务名过长
- 任务名重复
- 删除/修改不存在的任务

- 修改任务时间/日期时，如果输入的时间日期早于当前时间日期则修改失败。
- 设备无硬盘，导致数据库错误。

3.5.2 配置用户任务日志

配置效果

- 任务执行时会记录执行结果

注意事项

- 必须配置用户任务
- 最多保存 30 天日志
- 所有日志容量上限为 20MB，超过则自动按时间顺序清除

配置方法

- 启动用户任务日志功能

检验方法

- 查看用户任务日志

相关命令

↘ 启动用户任务日志

【命令格式】 **user-task log enable**
【参数说明】 **-**
【命令模式】 全局配置模式
【使用指导】 -

↘ 查看用户任务日志

【命令格式】 **show user-task log**
【参数说明】 **-**
【配置模式】 特权模式、全局模式、接口模式
【使用指导】 -

配置举例

↘ 启用并查看用户任务日志

【配置方法】

- 配置用户任务。略
- 启用用户任务日志，并查看任务日志。

```
Ruijie# configure terminal
Ruijie(config)# user-task log enable
Ruijie(config)# exit
Ruijie# show user-task log


--------------------
Task name: vvvv
Task time: 2014-09-19 16:09
Execute time: 2014-09-19 15:09
Execute mode: exec
Command: #wri
Result:  #
Building configuration...

[OK]


--------------------
Task name: 自定义应用组
Task time: 2014-09-18 19:03
Execute time: 2014-09-19 15:14
Execute mode: config
Command: #identify-application custom-group test-group
Command: #app-add  普通网页浏览
Command: #app-add 即时通讯软件
```

【检验方法】 -

常见配置错误

-

3.6 监视与维护

清除各类信息

作用	命令
清除用户任务日志。	**clear user-task**

查看运行情况

作用	命令
查看用户任务库	**show user-task**
查看用户任务日志	**show user-task log**

查看调试信息

4 SERVICE-MANAGER

4.1 概述

服务管理（Service Manager）允许用户按需开启设备提供的业务功能。

用户使用设备的各项功能是与其实际场景相关的，往往都有一部分功能不需要使用。这部分未用到的功能在启机阶段默认加载，也会消耗设备部分资源，WEB 上不使用的功能页面也会干扰用户使用常见功能，降低了易用性。通过服务管理配置，用户可以控制业务功能组件的按需加载，未配置的不运行，节约内存、不消耗 CPU，不想要的不在 web 呈现。

协议规范

- 无

4.2 典型应用

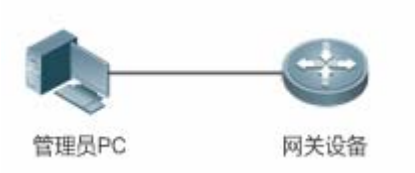
典型应用	场景描述
启动或关闭服务	用户希望按需加载想要的业务功能

4.2.1 启动或关闭服务

应用场景

用户根据实际场景中需要用到的功能对网关设备进行配置。对于不需要使用的功能，可以在服务管理中关闭，以释放设备部分资源占用，同时简化 WEB 页面上的菜单呈现，不想要的功能不在 WEB 上显示。

图 4-1



功能部属

- 确定需要开启或关闭的业务
- 配置服务的开启或关闭状态

4.3 功能详解

基本概念

开启服务、关闭服务

开启或关闭服务，是通过加卸载业务模块的进程，并同步控制业务模块是否启机加载、同步显示或屏蔽 WEB 指定页面的方式工作的。

功能特性

功能特性	作用
开启或关闭服务	开启或关闭指定服务。

4.3.1 开启或关闭服务

可按需加载服务，关闭的服务可以释放设备部分资源占用，并简化 WEB 页面上的菜单项。

部分业务的加卸载要求重启设备才能生效。

业务功能关闭后，模块被卸载，相关模块的 CLI 不可用。

需注意开启过多业务是否会造成设备内存使用率高。

工作原理

开启或关闭服务，是通过加卸载业务模块的进程，并同步控制业务模块是否启机加载、同步显示或屏蔽 WEB 指定页面的方式工作的。

相关配置

开启指定服务

指定服务名称开启服务。

关闭指定服务

指定服务名称关闭服务。

4.4 产品说明



NBR800G、NBR950G、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持按需开启和关闭业务功能；NBR108G-P、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1500G、NBR2000G 不支持按需开启和关闭业务功能。

4.5 配置详解

配置项	配置建议 & 相关命令	
开启或关闭服务	⚠ 可选配置。	
	servctl service *name* { **on** | **off** }	开启或关闭服务
	no servctl service *name*	恢复服务默认状态

4.5.1 开启或关闭服务

配置效果

- 指定服务名称开启服务。
- 指定服务名称关闭服务。
- 恢复指定服务为默认状态。

注意事项

- 部分业务的加卸载要求重启设备才能生效。
- 业务功能关闭后，模块被卸载，相关模块的 CLI 不可用。
- 需注意开启过多业务是否会造成设备内存使用率高。

配置方法

↘ 开启或关闭服务

- 可选配置。不配置的话，服务是否启机运行是按照版本自带的默认设定。
- 对于不需要的功能，可关闭对应的服务。

【命令格式】 **servctl service** *name* { **on** | **off** }

【参数说明】 *name*：指定服务名称。可通过 show 命令查看。

on：设置服务状态为运行。

off：设置服务状态为停止。

【缺省配置】 -

【命令模式】 全局配置模式

【使用指导】 -

检验方法

- 使用 show 命令查看服务状态。

【命令格式】 **show servctl** { **all | service** *name* }

【参数说明】 **all**：显示所有服务状态。

serervice *name*：显示指定服务状态。

【命令模式】 特权模式、全局模式

【使用指导】 查看支持服务管理控制的服务，以及服务状态。

【命令展示】

```
Ruijie#show servctl service was
service             controllable startup   running
------------------- ------------ --------- ---------
was                 true         true      true
```

关于 show 信息的详细解释请参看对应功能的命令手册。

配置举例

↘ 启动服务 was 的功能，允许启机自动运行

【网络环境】

图 4-2



【配置方法】

- 指定启动 was 服务。
- 加卸载 was 服务要求重启设备。重启设备让服务生效。

```
Ruijie(config)#servctl service was on
You must reload the system to enable service was.
Ruijie(config)#exit
Ruijie#write
Ruijie#reload
Reload system?(Y/N)
```

【检验方法】

- 使用 show 命令查看服务状态

```
Ruijie#show servctl service was
service             controllable startup   running
------------------- ------------ --------- ---------

was                 true         true      true
```

常见错误

- 指定的服务名错误或不支持控制。

4.6 监视与维护

清除各类信息

无

查看运行情况

作用	命令
查看支持服务管理控制的服务 ,以及服务状态。	**show servctl** { **all** | **service** *name* }

查看调试信息

无

配置指南-网络管理

本分册介绍网络管理相关内容，包括以下章节：

1. RLOG
2. POLICE-LOG
3. LOG-POLICY
4. SNMP
5. CM-APM
6. ANTI-SNIPER
7. IPMAC-SNIFF

1 RLOG

1.1 概述

RLOG 为日志上传模块。当设备需要上传日志到服务器时（如 ELOG，SNC），使用到本模块。

设备负责日志的采集，并通过 RLOG 将日志传给服务器。经过服务器端程序日志的解析后写入数据库。RLOG 可以用来上传设备运行信息，用户上网信息，系统安全信息等多种日志，在服务器端可以方便的查询到指定的记录。

下文仅介绍 RLOG 的相关内容。

协议规范

- 无

1.2 典型应用

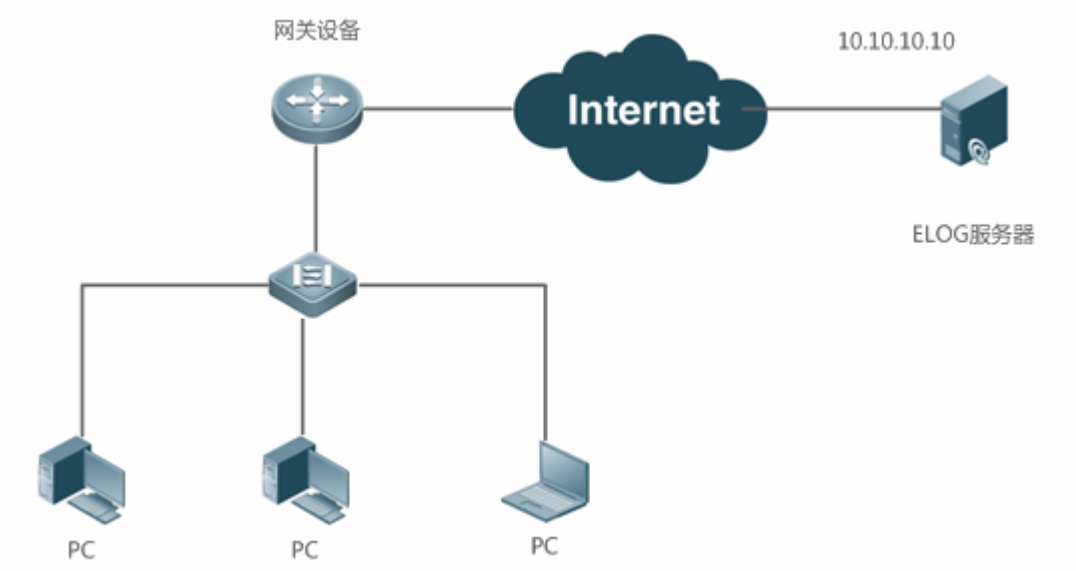
典型应用	场景描述
上传流日志	打开 NAT 日志 ,RLOG 将流日志上传到服务器 ,然后在服务器可以查询到每条数据流的详细记录。

1.2.1 上传流日志

应用场景

网关设备打开 RLOG 日志功能，打开 NAT 日志记录功能，当用户通过网关上网时，就会有 NAT 日志产生。流消亡时，流日志通过 RLOG 上传给 ELOG 服务器。

图 1-1



【注释】

功能部属

- 网关设备中开启 NAT 日志记录，开启 RLOG，并配置服务器。
- RLOG 服务器接收并解析日志，提供查询统计的服务。

1.3 功能详解

基本概念

无。

功能特性

功能特性	作用
上传日志	将网关设备的日志上传到服务器。
每种日志单独配置服务器	每类日志，可以单独配置上传的服务器

1.3.1 上传日志

将设备日志上传到服务器。

工作原理

设备的功能模块，如流日志，设备审计，流量审计，内容审计等，生成对应的日志，通过 RLOG 接口，发送给服务器。服务器接收，解析，展现这些日志信息。

相关配置

↘ 开启模块功能

各个模块的缺省情况下，并不一定在工作，需要打开。

比如流量审计，开启命令为：flow-audit enable

↘ 配置日志发送功能

缺省情况下，未配置服务器和日志发送功能。

配置一台服务器：rlog server 192.168.1.100 port 20000

配置日志发往服务器：rlog type 25 server 192.168.1.100 priority 1

其中，日志类型 25 表示接口流量日志。

1.3.2 每种日志单独配置服务器

将设备不同的日志上传到不同的服务器。

工作原理

RLOG 模块在接收到功能模块的日志发送请求，根据配置，对不同类型的日志区分对待。

相关配置

↘ 开启模块功能

各个模块的缺省情况下，并不一定在工作，需要打开。

比如流量审计，开启命令为：flow-audit enable

↘ 配置日志发送功能

缺省情况下，未配置服务器和日志发送功能。

配置两台服务器：rlog server 192.168.1.100 port 20000

rlog server 192.168.1.101 port20000

配置流日志发往服务器：rlog type 16 server 192.168.1.100 priority 1

配置接口流量日志发往服务器：rlog type 25 server 192.168.1.101 priority 1

其中，日志类型 16 表示流日志。

1.4 产品说明



NBR108G-P、NBR1500G、NBR2000G、NBR1000G-C、NBR2000G-C、NBR3000G-S 不支持 RLOG 功能 ;NBR800G、NBR950G、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 RLOG 功能。

NBR1500G、NBR2000G、NBR1000G-C、NBR2000G-C、NBR3000G-S 不支持流日志功能 ;NBR800G、NBR950G、NBR1000G-E 、 NBR6120-E 、 NBR1300G-E 、 NBR1700G-E 、 NBR2100G-E 、 NBR2500D-E 、 NBR3000D-E 、 NBR3000D-UE、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持流日志功能。

NBR2500D-E 、 NBR3000D-E 、 NBR3000D-UE 带硬盘设备支持日志记录在本地 ； NBR800G 、 NBR950G 、 NBR1000G-E 、 NBR6120-E 、 NBR1300G-E 、 NBR1700G-E 、 NBR2100G-E 不支持本地记录 ； NBR6205-E 、 NBR6135-E、NBR6210-E、NBR6215-E 带硬盘时支持本地记录，默认不带硬盘时不支持。

1.5 配置详解

配置项	配置建议&相关命令
配置日志发送	⚠ 必须配置。用于指定服务器地址端口。

1.5.1 配置日志发送

配置效果

- 配置 RLOG 服务器。
- 配置某一种日志发往指定的服务器。

注意事项

- 无。

配置方法

↘ 配置 RLOG 服务器

- 必须配置。
- 若无特殊要求，可以配置一个服务器。

↘ 配置日志发送

- 必须配置。

- 一般需要哪种日志就配哪种日志。

检验方法

设备正常发送配置的日志

- 检查 RLOG 服务器能否成功接收每个日志报文。

相关命令

配置日志服务器

【命令格式】 **rlog server** *ip-address* [**port***port-num*]

【参数说明】 *Ip-address*：服务器 ip

port-num：服务器端口

【命令模式】 配置模式

【使用指导】 配置日志服务器命令只是打开日志服务，输出日志内容并没有开启，单独打开该命令不会有日志内容输出。例如流日志开关是 **ip session log-on**，需要单独打开。

若要取消服务器配置，则可以执行：**no rlog server***ip-address*

配置日志发送

【命令格式】 **rlog type** *n***server** *server-ip* **priority** *prio*

rlogtype *n* **file**

【参数说明】 *n*：RLOG 日志类型

server-ip：已配置的服务器 IP

prio：日志发送优先级，取值 0~7，取值越小优先级越高

rlog type n file 表示日志直接生成文件，由 rlog-file 负责发送

【命令模式】 配置模式

【使用指导】 要取消发送某个日志，执行：**no rlog type***n***server***srever-ip*

目前支持的日志类型包括：

[16] RLOG_TYPE_FLOW, /* 流日志 */

[17] RLOG_TYPE_CPU_MEM, /* CPU 使用率，内存使用率日志 */

[18] RLOG_TYPE_DISC, /* 硬盘使用情况 */

[19] RLOG_TYPE_DEV_LOG, /* 设备审计的日志 */

[20] RLOG_TYPE_URL_AUDIT, /* URL 审计 */

[21] RLOG_TYPE_SESSION, /* 在线 ip 数，在线会话数日志 */

[22] RLOG_TYPE_IP_APP, /* 某个 IP,应用的流量 */

[23] RLOG_TYPE_IP, /* 某个 IP 的会话数 */

[24] RLOG_TYPE_CHANNEL, /* 某个通道的流量 */

[25] RLOG_TYPE_INTERFACE, /* 某个接口的流量 */

[26] RLOG_TYPE_IP_OFFLINE, /* IP 下线通告 */

[27] RLOG_TYPE_MAIL_AUDIT, /* 邮件审计 */

```
[28] RLOG_TYPE_TELNET_AUDIT,            /*  telnet 审计  */
[29] RLOG_TYPE_WEB_SEARCH_AUDIT,     /*    搜索审计  */
[30] RLOG_TYPE_WEB_BBS_AUDIT,          /*  web_bbs 审计  */
[31] RLOG_TYPE_IM_AUDIT,                /* IM 审计  */
[32] RLOG_TYPE_FTP_AUDIT,               /* FTP 审计  */
[33] RLOG_TYPE_WEB_AUDIT,               /* web 审计  */
[34] RLOG_TYPE_APP_AUDIT,               /*  应用控制审计  */
[35] RLOG_TYPE_FLOOD,                   /*  发现洪水攻击日志*/
[36] RLOG_TYPE_FLOOD_CEASEm,        /*       洪水攻击停止日志*/
[37] RLOG_TYPE_SCAN,                    /*  发现扫描日志*/
[38] RLOG_TYPE_SCAN_CEASE,          /*       扫描停止日志*/
[39] RLOG_TYPE_ATTACK_FRAG,           /*发现 IP 分片攻击*/
```

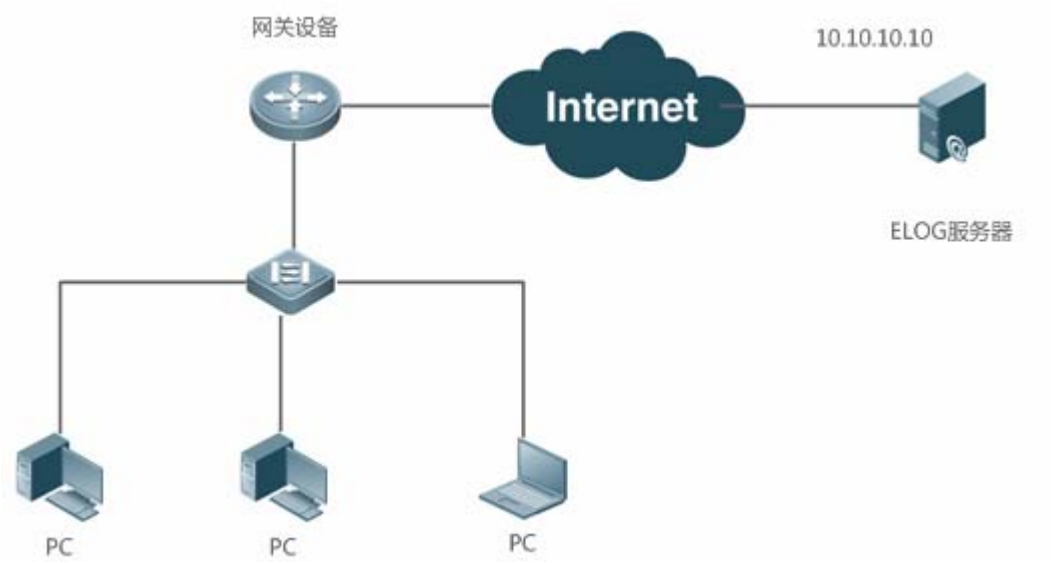
配置举例

以下配置举例，仅介绍与 RLOG 相关的配置。

配置流日志发送到服务器 10.10.10.10

【网络环境】

图 1-2



【配置方法】

- 在网关设备上配置 RLOG 服务器的 ip 和端口
- 在网关设备上配置流日志发送往服务器 10.10.10.10。
- 在网关设备上打开流日志。

A

```
A#configure terminal
A(config)#rlog server 10.10.10.10 port 20000
A(config)# rlog type 16 server 10.10.10.10 priority 1
A(config)#ip session log-on
```

【检验方法】 检查 A 是否发送日志报文到 RLOG 服务器，也可以检查 RLOG 模块的日志发送计数是否增加。

- 检查 RLOG 模块的日志生成计数是否增加
- 检查 RLOG 日志发送计数是否增加

A

```
A# show rlog-status log
local rlog message:

remote rlog message:
[16]RLOG_TYPE_FLOW                : 0
[17]RLOG_TYPE_CPU_MEM             : 0
[18]RLOG_TYPE_DISC                : 0
[19]RLOG_TYPE_DEV_LOG             : 0
[20]RLOG_TYPE_URL_AUDIT           : 0
[21]RLOG_TYPE_SESSION             : 0
[22]RLOG_TYPE_IP_APP              : 0
[23]RLOG_TYPE_IP                  : 0
[24]RLOG_TYPE_CHANNEL             : 0
[25]RLOG_TYPE_INTERFACE           : 0
[26]RLOG_TYPE_IP_OFFLINE          : 0
[27]RLOG_TYPE_MAIL_AUDIT          : 0
[28]RLOG_TYPE_TELNET_AUDIT        : 0
[29]RLOG_TYPE_WEB_SEARCH_AUDIT    : 0
[30]RLOG_TYPE_WEB_BBS_AUDIT       : 0
[31]RLOG_TYPE_IM_AUDIT            : 0
[32]RLOG_TYPE_FTP_AUDIT           : 0
[33]RLOG_TYPE_WEB_AUDIT           : 0
[34]RLOG_TYPE_APP_AUDIT           : 0
[35]RLOG_TYPE_FLOOD               : 0
[36]RLOG_TYPE_FLOOD_CEASEm        : 0
[37]RLOG_TYPE_SCAN                : 0
[38]RLOG_TYPE_SCAN_CEASE          : 0
[39]RLOG_TYPE_ATTACK_FRAG         : 0
```

如果日志有生成，那么 RLOG_TYPE_FLOW 的日志计数会增加。

A

```
A# show rlog
rlog server is enable
 port 20000  server 192.168.1.100
 port 20000  server 10.10.10.10
rlog dev-ip 0.0.0.0
rlog export-rate 10000 rlog queue remain 10000
send log count : 0 error count : 0 errorno : 0
```

```
recv buf: 0 poll buf err: 0 push buf: 0 local buf: 0
recv err cnt: 0 depatch err cnt: 0

enable log combination: 0
```

如果发送成功，则 `send log count` 的值会增加。

常见错误

- 配置了 RLOG 服务器，没有指定日志发送到该服务器。
- 配置了 RLOG 日志和服务器，但是产生日志的开关没有打开。

1.5.2 配置日志发送参数

配置效果

- 使得 RLOG 工作得更加健康。

注意事项

- 必须了解每项参数配置的作用，和参数取值的意义之后再配置，否则可能导致 RLOG 不能正常工作。

配置方法

- 根据环境，有需要此项配置时才进行配置。

检验方法

- RLOG 发送日志正常，服务器能正常接收到日志。

相关命令

↘ 配置日志发送速率

【命令格式】 **rlog export-rate** *val*

【参数说明】 *Val*：每秒发送的日志条数上限值。

【命令模式】 配置模式

【使用指导】 配置取值必须考虑本设备的性能，RLOG 服务器的性能，以及设备的日志产生量。配置太小，容易造成日志发送丢失。配置过大，可能导致 CPU 持续偏高。

↘ 配置日志合并发送

【命令格式】 **rlog set log-com**

【参数说明】 -

【配置模式】 配置模式

【使用指导】 配置该命令后，多条日志会被拼接在一条报文中发送。需要 RLOG 服务器支持，配置时要先弄清楚服务器是否支持该功能。

配置设备 ip

【命令格式】 **rlog dev-ip** *ip*

【参数说明】 *ip*：指定设备 ip。

【配置模式】 配置模式

【使用指导】 部分日志需要取得本设备的 ip，该 ip 由本命令指定。有需要的时候才配置。

配置日志过滤条件

【命令格式】 **rlog filter***acl_id*

【参数说明】 access-list id

【配置模式】 配置模式

【使用指导】 当前版本不对该命令进行处理

配置流日志带有 sn 和 mac 信息

【命令格式】 **rlog sn-mac-on**

【参数说明】 -

【配置模式】 配置模式

【使用指导】 仅在确认服务器支持模式时选择开启

配置举例

指定本设备 IP 为 10.10.10.1，日志发送速率为 10000，不合并日志。

【配置方法】

```
Ruijie#configure terminal
Ruijie(config)# rlog dev-ip 10.10.10.1
Ruijie(config)# rlog export-rate 10000
Ruijie(config)# end
```

【检验方法】 查看配置是否生效，服务器日志是否正常接收

```
Ruijie# show rlog
rlog server is enable
 port 20000  server 192.168.1.100
 port 20000  server 10.10.10.10
rlog dev-ip 10.10.10.1
rlog export-rate 10000 rlog queue remain 10000
send log count : 0 error count : 0 errorno : 0
```

```
recv buf: 0 poll buf err: 0 push buf: 0 local buf: 0
recv err cnt: 0 depatch err cnt: 0
```

常见配置错误

- 日志发送速率配置过小，导致日志丢失。

1.5.3 配置文件日志发送

配置效果

- 配置 RLOG 文件服务器。
- 配置某一种日志发往指定的服务器。

注意事项

- 无。

配置方法

配置 RLOG 文件服务器

- 必须配置。
- 只能配置一个文件服务器。

配置日志发送

- 必须配置。
- 一般需要哪种日志就配哪种日志。

检验方法

设备正常发送配置的日志

- 检查 RLOG 服务器能否成功接收每个日志文件。

相关命令

配置日志文件服务器

【命令格式】 **rlog-file server***protocalip-address* [**port***port-num*] [**path***server-path-string*] [**username***username-string***passwd***passwd-string*]

【参数说明】 protocal:HTTP 或者 FTP

ip-address：指定的 RLOG 文件服务器 ip 地址

port-num：指定 RLOG 文件服务器服务端口，仅适用于 HTTP 服务器，默认 80

server-path-string：服务器目录，默认目录为 ‘/’

username-string：用户名，默认为 “ruijie”

passwd-string：密码，默认为 “ruijie”

【命令模式】 配置模式

【使用指导】 配置日志服务器命令只是打开日志文件服务 ,输出日志内容并没有开启 ,单独打开该命令不会有日志内容输出。

若要取消服务器配置，则可以执行：**no rlog-file server***ip-address*

配置日志发送

【命令格式】 **rlog-file type** *type-num*

【参数说明】 *type-num：日志类型*

【命令模式】 配置模式

【使用指导】 要取消发送某个日志，执行：**no rlog-file type***n*

目前支持的日志类型包括：

[16] RLOG_TYPE_FLOW, /* 流日志 */

[17] RLOG_TYPE_CPU_MEM, /* CPU 使用率，内存使用率日志 */

[18] RLOG_TYPE_DISC, /* 硬盘使用情况 */

[19] RLOG_TYPE_DEV_LOG, /* 设备审计的日志 */

[20] RLOG_TYPE_URL_AUDIT, /* URL 审计 */

[21] RLOG_TYPE_SESSION, /* 在线 ip 数，在线会话数日志 */

[22] RLOG_TYPE_IP_APP, /* 某个 IP,应用的流量 */

[23] RLOG_TYPE_IP, /* 某个 IP 的会话数 */

[24] RLOG_TYPE_CHANNEL, /* 某个通道的流量 */

[25] RLOG_TYPE_INTERFACE, /* 某个接口的流量 */

[26] RLOG_TYPE_IP_OFFLINE, /* IP 下线通告 */

[27] RLOG_TYPE_MAIL_AUDIT, /* 邮件审计 */

[28] RLOG_TYPE_TELNET_AUDIT, /* telnet 审计 */

[29] RLOG_TYPE_WEB_SEARCH_AUDIT, /* 搜索审计 */

[30] RLOG_TYPE_WEB_BBS_AUDIT, /* web_bbs 审计 */

[31] RLOG_TYPE_IM_AUDIT, /* IM 审计 */

[32] RLOG_TYPE_FTP_AUDIT, /* FTP 审计 */

[33] RLOG_TYPE_WEB_AUDIT, /* web 审计 */

[34] RLOG_TYPE_APP_AUDIT, /* 应用控制审计 */

[35] RLOG_TYPE_FLOOD, /* 发现洪水攻击日志*/

[36] RLOG_TYPE_FLOOD_CEASEm, /* 洪水攻击停止日志*/

[37] RLOG_TYPE_SCAN, /* 发现扫描日志*/

[38] RLOG_TYPE_SCAN_CEASE, /* 扫描停止日志*/

[39] RLOG_TYPE_ATTACK_FRAG, /*发现 IP 分片攻击*/

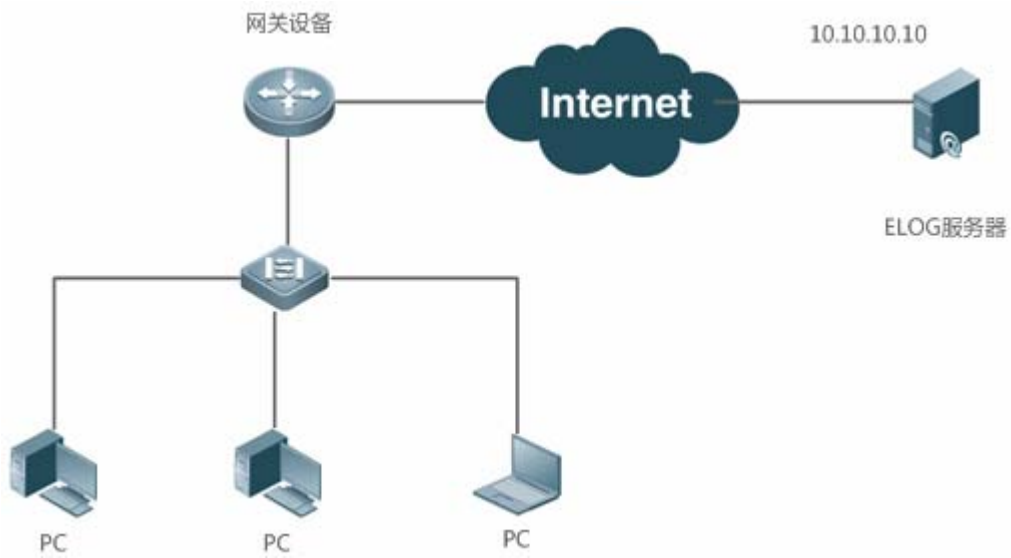
配置举例

以下配置举例，仅介绍与 RLOG 相关的配置。

配置流日志发送到服务器 10.10.10.10

【网络环境】

图 1-3



【配置方法】

- 在网关设备上配置 RLOG 文件服务器的 ip 和端口
- 在网关设备上配置邮件审计日志和流日志以 ftp 方式发送往服务器 10.10.10.10。
- 在网关设备上打开邮件审计。

A

```
A#configure terminal
A(config)#rlog-file server 10.10.10.10 username test passwd test
A(config)# rlog-file send protocol http
A(config)# rlog-file type 48
A(config)#rlog type 16 file
```

【检验方法】 检查 A 是否发送日志报文到 RLOG 文件服务器，也可以检查 RLOG 模块的日志文件发送计数是否增加。

- 检查 RLOG 模块的日志文件发送计数是否增加

A

```
A# show rlog-file info

Ruijie#showrlog-fileinfo

rlog file server: http

    ip      :172.18.8.97, port:8080

    source  :0.0.0.0
```

```
    path    : /ELCService/upload/PullLogFile
    username:; passwd:;
local path    : /mnt/usb0/rlog_file
local storage : 524288 K
send time-rage: from 0 to 24
send compress : zip
send format   : ELOG
client count  : 3

LOG        : total[2771]; tar[2771|0]; send[2771|0],lasterr[0]
MAIL_BODY  : total[2]; tar[2|0]; send[2|0],lasterr[0]
MAIL_ATTACH: total[1]; tar[1|0]; send[1|0],lasterr[0]
WEBMAIL    : total[0]; tar[0|0]; send[0|0],lasterr[0]
BSS_BODY   : total[7]; tar[7|0]; send[7|0],lasterr[0]
MACC       : total[0]; tar[0|0]; send[0|0],lasterr[0]

type
RLOG_FILE_TYPE_MAIL_AUDIT      48
RLOG_FILE_TYPE_WEBMAIL_AUDIT   49
RLOG_FILE_TYPE_WEB_BBS_AUDIT   50
RLOG_FILE_TYPE_IP_APP          51
```

如果日志有生成，那么 RLOG_FILE_TYPE_MAIL_AUDIT 的日志计数会增加。

常见错误

- 配置了 RLOG 文件服务器，没有指定日志发送到该服务器。

配置了 RLOG 文件服务器，没有配置用户名密码，传输方式，压缩方式，文件格式等信息。

1.5.4 配置本地日志

配置效果

- 配置本地日志开关。

注意事项

- 需要记录本地日志的时候，进行此配置。

配置方法

- 在需要记录本地日志的设备上直接配置。

检验方法

- 使用 **show nat-log** 命令查看是否有本地日志记录。

相关命令

↘ 打开本地日志

【命令格式】 **nat-log enable**
【参数说明】 --
【命令模式】 配置模式
【使用指导】 打开本地日志功能，本地日志将被记录到本地磁盘中。取消使用命令：**no nat-log enable**

↘ 设置本地日志保存天数

【命令格式】 **nat-log data-store** *days*
【参数说明】 **-**
【配置模式】 配置模式
【使用指导】 配置该命令，可以设置本地日志保存的天数。可选的天数范围为 10~90.

↘ 只记录 NAT 日志

【命令格式】 **ip nat-log on**
【参数说明】 **-**
【配置模式】 配置模式
【使用指导】 配置该命令，则本地日志只记录 NAT 日志。关闭使用命令：**no ip nat-log on**。关闭后，记录所有流日志。

配置举例

↘ 打开本地日志，只记录 NAT 日志，设置本地日志保存 14 天

【配置方法】

```
Ruijie#configure terminal
Ruijie(config)# ip nat-log on
Ruijie(config)#nat-log enable
Ruijie(config)# nat-log data-store 14
Ruijie(config)# end
```

【检验方法】 在有流产生和消亡的前提上，查看是否有记录日志（假设日期是 2014-4-16 ）。如果有记录，则会显示出来。

```
Ruijie# show nat-log time-interval 2014 4 16 0 to 2014 4 16 23
count:0
Pr  SrcAddr                          DstAddr                          UserName
SrcPort      DstPort      Vrf        SendBytes  RecvBytes  time
```

网关产品不支持 VRF，配置举例仅作为配置参考，实际请以具体设备配置为准。

常见配置错误

- 想要查看本地日志，却未打开本地日志功能

1.6 监视与维护

清除各类信息

无

查看运行情况

作用	命令
查看 RLOG 运行、配置情况	**show rlog**
查看 RLOG 支持的日志类型	**show rlog-type**
查看 RLOG 服务器状态	**show rlog-status** [**server***ip*]
查看连接 RLOG 的功能模块个数	**show rlog-status client**
查看 RLOG 每种日志产生的日志个数	**show rlog-status log**
查询时间段内的流/NAT 日志信息，可以根据用户名，协议，源 ip，源端口，目的 ip，目的端口过滤	**Show nat-log**[**username***user_name*] [**ip-protocol** *ip-protocol*] [**source-ip***source-ip*] [**dst-ip***dst-ip*] [**src-port** *src-port*] [**dst-port***dst-port*] **time-interval***begin-year begin-mon begin-day begin-hour* **to** *end-year end-mon end-day end-hour*

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 RLOG debug 开关	**debug rlog info**
打开 RLOG 库的 debug 开关	**debug rlog lib**
打开 NAT LOG 的 debug 开关	**debug nat-log**

2 POLICE-LOG

2.1 概述

POLICE-LOG 是公共场所无线上网安全的管理程序，用于让网关设备与 MACC/ELOG，或者第三方平台对接，发送指定要求的日志。

在部署 MACC/ELOG 的公共上网场景下，MACC/ELOG 需要与第三方的公共场所无线上网安全管理平台对接，此时需要开启 POLICE-LOG 与 MACC/ELOG 对接，后续的描述 MACC 均代指 MACC/ELOG 服务器。

协议规范

为了保障公共无线上网的安全，需要对其进行审计；为了保障各厂商的产品能够更好的对接第三方的公共场所无线上网安全管理系统，以下标准得以提出：

《GAWA3011.1-2015 公共场所无线上网安全管理系统无线接入场所端功能要求.docx》

《GAWA3011.2-2015 公共场所无线上网安全管理系统管理后台功能要求（秘密）.docx》

《GAWA3011.3-2015 公共场所无线上网安全管理系统 前端数据和基础数据交换格式.docx》

《GAWA3011.4-2015 公共场所无线上网安全管理系统 数据传输交换规范.docx》

《GAWA3011.5-2015 公共场所无线上网安全管理系统 统一 XML Schema 接口规范.docx》

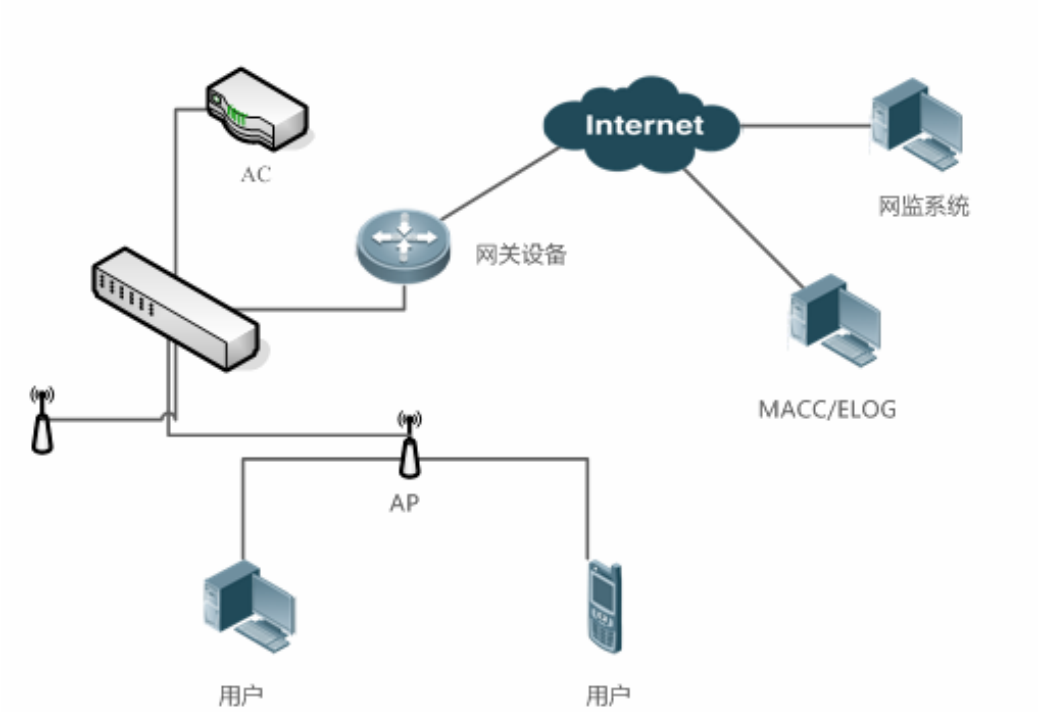
2.2 典型应用

典型应用	场景描述
第三方日志审计	该场景为通用的公共上网安全标准的场景

2.2.1 第三方日志审计

对接 ELOG 场景

- 网关设备作为 NAT 网关出口
- MACC/ELOG 可以管理网关设备，包括远程升级，状态监控，以及下发配置等。
- 公共场所无线上网安全管理系统可以收到 MACC/ELOG 的审计日志

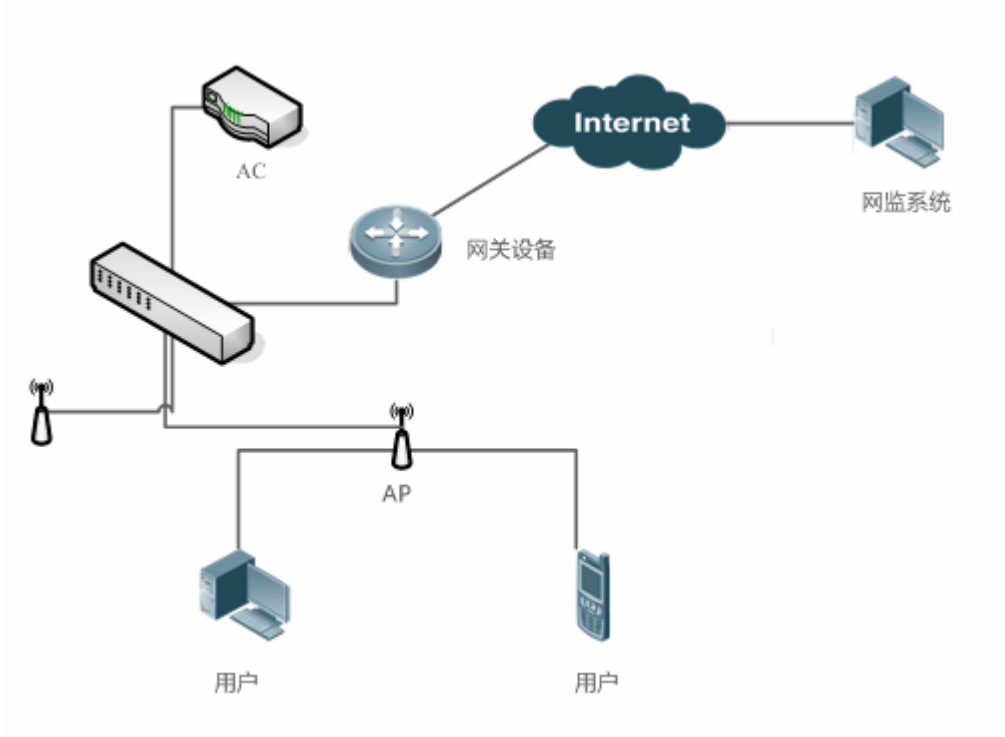


功能部属

- 网关上开启 POLICE-LOG 组件
- 网关上开启 NAT-LOG 组件
- 网关上开启通用日志组件

对接任子行场景

- 网关设备作为 NAT 网关出口，或者旁路部署
- 任子行系统可以收到网关设备的审计日志



功能部属

- 网关上开启 POLICE-LOG 组件
- 网关上开启 NAT-LOG 组件
- 网关上开启通用日志组件

2.3 功能详解

基本概念

↘ 认证日志

无线用户上网时，需要实名认证，其中实名可以是用户的身份证件号，或者手机号。该日志将发送到公共场所无线上网安全管理平台，以便追溯实名用户的上网行为。

↘ NAT 流日志

由于网关设备是作为 NAT 网关，为了审计具体用户的上网行为，需要审计 NAT 流的详细五元组信息（源地址，源端口，目的地址，目的端口，协议类型），以及用户上网的详细行为。

↘ 通用日志

网关设备作为出口设备 ,具备内容审计的功能 ,可审计具体用户的上网行为 ,输出虚拟身份、http 访问、mail、webbbs、websearch 等日志，细查到用户的上网行为，以上日志统称为通用日志。

功能特性

功能特性	作用
MACC 对接	MACC 需要识别对接设备，以及检测其状态
认证日志	用户认证上网，该认证日志需要上报到 MACC，以便网综平台可以跟踪该用户
NAT 流上网日志	用户上网日志，网综平台用来分析用户的上网行为
通用上网行为日志	用户上网行为识别，提供给网综平台分析、记录用户上网行为
直接对接第三方系统	按照第三方系统对接规范，将日志直接发送给第三方系统

2.3.1 MACC对接

MACC 需要识别对接设备，以及检测其状态

工作原理

网关设备上的 police_log 程序启动时，会根据 cli 配置的 MACC 对接地址，向其获取当前设备的场所信息，如果获取成功，那么定时上报网关设备的状态。如果该设备未注册到 MACC 上 ,那么 MACC 会保存该设备的注册信息 ,在 MACC 的设备管理中通过。

用户通过网关设备的认证时，需要将认证的记录上报给 MACC

2.3.2 认证日志

工作原理

认证时由 APP-AUTH 负责认证通过，或者用户下线，app-auth 发送该事件给 police_log, police_log 将改事件格式化成指定格式上报给 MACC，MACC 入库，并在指定的 WEB 界面展示。

2.3.3 NAT流上网日志

用户上网的 NAT 流信息需要上报给 MACC，在 MACC 与第三方的公共场所无线上网安全管理平台对接时，第三方的公共场所无线上网安全管理平台可以通过日志分析来提取所关心的用户行为。

工作原理

NAT-LOG 模块注册流平台，在流创建时，获取流信息发送到 police_log, police_log 转换为指定的记录格式，上报给 MACC，MACC 入库并展示。

2.3.4 通用上网行为日志

用户上网行为识别需要上报给 MACC，在 MACC 与第三方的公共场所无线上网安全管理平台对接时，第三方的公共场所无线上网安全管理平台可以通过日志分析来提取所关心的用户行为。

工作原理

通用日志中的上网行为识别，如虚拟身份审计、mail 审计、http 访问审计、webbbs 审计、websearch 审计，这五种审计日志的识别需要由内容审计模块完成，之后传递给第三方日志 police_log 模块，police_log 转换为指定的记录格式，上报给 MACC，MACC 入库并展示。

其中虚拟身份审计又包括 im 聊天和 vid 两种审计内容，mail 包括终端 mail 和 webmail 两种审计内容，均需要单独开启

2.3.5 直接对接第三方系统

按照第三方系统对接规范，将日志直接发送给第三方系统。

工作原理

将认证日志、NAT 流上网日志、通用上网日志（虚拟身份审计、mail 审计、http 访问审计、webbbs 审计、websearch 审计）按照规范转换为第三方系统的日志格式，上报给第三方系统，第三方系统收到日志并处理。

2.4 产品说明



NBR108G-P、NBR3000G-S 、NBR1500G、NBR2000G、NBR1000G-C、NBR2000G-C、NBR800G、NBR950G 不支持第三方日志功能，NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持第三方日志功能。

NBR108G-P、NBR800G、NBR950G 不支持第三方日志服务器，NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E 、NBR2100G-E 、NBR2500D-E 、NBR3000D-E 、NBR3000D-UE 、NBR1500G 、NBR2000G 、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持第三方日志服务器（包括：任子行、美亚柏科、全国部标、湖南部标、新网程、以太网科、优码创达、芝立软件、中新网安、重庆爱思、锐安（宝鸡）、山东兆物、网博、上海派博、网际星辰、武汉宏旭、佰安、安徽中新、锐安（北京）、博艺、烽火）。

2.5 配置详解

配置项	配置建议 & 相关命令	
配置 POLICE-LOG 基本功能	⚠ 必须配置。	
	police-log enable	启动 POLICE-LOG 模块
	police-log set url *url*	配置 MACC/ELOG 地址
开启 NAT-LOG 功能	⚠ 必须配置	
	nat-log police	配置第三方上网流审计日志
开启通用日志发送第三方日志模块功能	**content-audit write-plog *im***	配置开启 IM 聊天审计
	content-audit write-plog *vid*	配置开启 vid 身份审计
	content-audit write-plog *mail*	配置开启客户端 mail 审计
	content-audit write-plog *webmail*	配置开启 webmail 审计
	content-audit write-plog *url*	配置开启 http 访问审计
	content-audit write-plog *webbbs*	配置开启论坛审计
	content-audit write-plog *websearch*	配置开启搜索审计
配置对接平台	**police-log set platform { elog | { *platform-type* [name *plat-name*] } }**	配置对接平台
配置场所信息	**police-log-netsite** *index*	配置场所信息
配置 AP 信息	**police-log-ap** *index*	配置 AP 信息

2.5.1 配置POLICE-LOG基本功能

配置效果

- 与 MACC/ELOG 对接，MACC/ELOG 可以管理当前设备。

注意事项

- MACC/ELOG 的地址应该是完整的 URL 地址。

配置方法

↘ 启动 POLICE-LOG 功能

【命令格式】 **police-log enable**
【参数说明】 -
【缺省配置】 关闭
【命令模式】 全局模式

【使用指导】 该命令用户开启第三方日志模块功能，与 MACC/ELOG 对接，发送相应的日志

设置 MACC 地址

【命令格式】 **police-log set url** *url* **source** [**interface** *interface-name* | *addr*]

【参数说明】 url： 为 MACC 的完整 url 地址

interface-name： 本地接口名称

addr： 本地 IP 地址

【缺省配置】 地址为空

【命令模式】 全局模式

【使用指导】 该命令是用来配置 MACC 服务器的 url，请注意，是完整的 MACC 服务主机地址，有些主机上会部署多套的 WEB 服务

检验方法

- 使用 **show police-log** 命令可以确认 police-log 是否开启。

【命令格式】 **show police-log config**

【参数说明】 无

【命令模式】 特权模式、全局模式

【使用指导】 用来查看第三方日志模块的运行情况，是否开启，是否与 MACC 连接成功等

【配置举例】 1：查看第三方日志模块运行状态

```
Ruijie#show police-log config

police log configuration

    >police log: enable

    >server url: https://192.168.25.184:443/specification

    >auth type: define (1021999)

    >file compress: enable
```

字段解释：

字段	说明
police-log	第三方日志模块是否开启 ,enable 表示开启 ,disable 表示关闭
server url	MACC/ELOG 服务器地址
auth type	认证类型配置
file compress	文件压缩开关：enable 压缩，disable 不压缩

【提示信息】 -

配置举例

1：缺省配置，MACC 的对接地址：https://172.18.124.35/specification/。

```
Ruijie# configure
Ruijie(config)# police-log set url https://172.18.124.35/specification/
Ruijie(config)# exit
Ruijie# wr
```

2：源接口配置，MACC 的对接地址：https://172.18.124.35/specification/，接口为 Loopback 0

```
Ruijie# configure
Ruijie(config)# police-log set url https://172.18.124.35/specification/ source interface Loopback 0
Ruijie(config)# exit
Ruijie# wr
```

常见错误

无

2.5.2 开启NAT-LOG功能

配置效果

- 网关设备可以审计到 NAT 数据流，以便 MACC 获得上网流信息。

注意事项

- -

配置方法

↘ 启动 NAT-LOG 功能

【命令格式】 **nat-log police**
【参数说明】 -
【缺省配置】 关闭
【命令模式】 全局模式
【使用指导】 无

检验方法

- 使用 **show nat-log status** 命令可以确认 nat-log police 是否开启。

【命令格式】 **show nat-log status**

【参数说明】 无

【命令模式】 特权模式、全局模式

【使用指导】 用来确认 nat-log 的 police 参数是否设置成功

【配置举例】 1：查看 nat-log police 选项是否开启

```
Ruijie#show nat-log status
nat-log status:0
ip nat-log on: 0
nat-log police on: enable
nat-log police snd sus: 4953, fail: 0
```

字段解释：

字段	说明
nat-log police on	enable 开启了 nat-log 发送第三方日志模块；disable 关闭
其他信息	可不用关注

【提示信息】 -

配置举例

无

常见错误

无

2.5.3 开启通用日志发送第三方日志模块功能

配置效果

- 网关设备可以审计到通用上网行为数据，发送 macc 展示并发送公共场所无线上网安全管理系统。

注意事项

- -

配置方法

启动通用日志发送第三方日志模块功能

【命令格式】 **content-audit write-plog {**im | mail | url | vid | web-bbs | web-mail | web-search**}**

【参数说明】

参数	描述
-im	开启 im 聊天日志发送第三方日志模块
-mail	开启客户端 mail 日志发送第三方日志模块
-url	开启 http 日志发送第三方日志模块
-vid	开启虚拟身份审计发送第三方日志模块
-web-bbs	开启论坛日志发送第三方日志模块
-web-mail	开启 web 端 mail 日志发送第三方日志模块
-web-search	开启搜索日志发送第三方日志模块

【缺省配置】 关闭

【命令模式】 全局模式

【使用指导】 无

检验方法

- **使用 show content-audit plog config 命令可以确认通用日志发送**第三方日志模块**是否开启。**

【命令格式】 **show content-audit plog config**

【参数说明】 无

【命令模式】 特权模式、全局模式

【使用指导】 用来确认 nat-log 的 police 参数是否设置成功

【配置举例】 1：查看 nat-log police 选项是否开启

```
Ruijie#show content-audit plog config
content-audit log send to police-log
-----------------------------------
    >im:            enable
    >vid:           enable
    >url:           enable
    >web search :   enable
    >web bbs :      enable
    >web mail:      enable
    >mail:          enable
```

字段解释：

字段	说明
im	enable 开启 im 聊天日志；disable 关闭
vid	enable 开启 vid 日志；disable 关闭
url	enable 开启 http 访问日志；disable 关闭
web search	enable 开启搜索日志；disable 关闭
web bbs	enable 开启论坛日志；disable 关闭
web mail	enable 开启 web mail 日志；disable 关闭
mail	enable 开启 mail 客户端日志；disable 关闭

【提示信息】 -

配置举例

无

常见错误

无

2.5.4 配置对接平台

配置效果

- 配置第三方日志对接的后台服务器。

注意事项

- -

配置方法

↘ 配置对接的第三方日志平台

【命令格式】 **police-log set platform { elog | {** *platform-type* [**name** *plat-name*] } }

【参数说明】 elog 表示对接的是 elog 服务器，如果是 elog，则无需在配置其他参数。elog 与第三方日志平台是互斥的，两者只能选其一，如果没有配置，则默认为 elog。

platform-type：第三方日志平台类型，取值范围查看 **show plog platform**，如 surfilter 表示任子行，myp 表示对接美亚柏科。

plat-name：第三方日志名称，如果没有配置，则默认跟 *platform-type* 一样。

【缺省配置】 如果没有配置该命令，则默认对接 elog；如果 *plat-name* 没有配置，则 *plat-name* 默认等于 *platform-type*。

【命令模式】 全局模式

【使用指导】 配置完该命令，进入一个新的命令模式（config-plog-platform）

↘ 配置第三方日志平台的参数

【命令格式】 { **data-gather | send-para** } *key-string value*

【参数说明】 **data-gather**：配置数据采集相关参数

send-para：配置日志发送相关参数

key-string：表示参数名，分别通过下面两条命令获取参数名：

show plog para-list data-gather *plat-name*

show plog para-list send-para *palt-name*

value：参数对应的值。

【缺省配置】 无

【命令模式】 config-plog-platform 模式

【使用指导】 如果配置的参数名不在列表范围内，则会提示错误。

检验方法

- **使用 show plog config platform 命令可以查看配置的第三方日志列表。**

【命令格式】 **show plog config platform**

【参数说明】 *无*

【命令模式】 特权模式、全局模式

【使用指导】 无

【配置举例】

```
Ruijie#sh plog config platform
{"code":0,"msg":"","list":[{"platform-type":"surfilter","platform-name":"surfilter"}]}
```

【提示信息】 -

- **使用 show plog config { data-gather | send-para } platform plat-name 命令可以查看第三方日志平台的配置信息。**

【命令格式】 **show plog config { data-gather | send-para } platform** *plat-name*

【参数说明】 *plat-name* 第三方日志的名称

【命令模式】 特权模式、全局模式

【使用指导】 不管参数有没有配置，都会罗列出来。

【配置举例】

```
Ruijie#sh plog config data-gather platform surfilter
{ "code": 0, "msg": "", "list": [ { "org-name": "123", "security-org-code": "123123123",
"collection-type": "123", "source-wacode": "123123", "destination-wacode": "123123" } ] }
Ruijie#sh plog config send-para platform surfilter
{ "code": 0, "msg": "", "list": [ { "server": "1.1.1.1", "ftp-server-port": "21", "username": "1",
"password": "1" } ] }
```

【提示信息】 -

配置举例

无

2.5.5 配置场所信息

配置效果

- 网关设备可以获取场所资料并发送给第三方系统。

注意事项

- -

配置方法

↘ 配置场所

【命令格式】 **police-log-netsite** *index*
【参数说明】 index 表示场所索引
【缺省配置】 无
【命令模式】 全局模式
【使用指导】 配置完成后，进入 config-plog-netsite 命令模式

↘ 配置场所所属的第三方日志平台

【命令格式】 **set platform** *plat-name*
【参数说明】 *plat-name*：所属的第三方日志平台
【缺省配置】 无

【命令模式】 config-plog-netsite

【使用指导】 该命令同一个场所下最多允许配置 3 次。并且要求 3 个第三方日志平台都属于同一个第三方日志类型，否则会提示出错。

配置场所的参数

【命令格式】 *set key-string value*

【参数说明】 key-string：场所参数名，通过 **show plog para-list netsite** *palt-name* 获取参数

value：参数值

【缺省配置】 无

【命令模式】 config-plog-netsite

【使用指导】 如果配置的参数名非法，则会提示错误。

检验方法

- 使用 show plog config netsite [netsite-id | platform plat-name]命令可以查看指定第三方日志平台的配置信息。

【命令格式】 **show plog config netsite [** *netsite-id* **|** **platform** *plat-name* **]**

【参数说明】 netsite-id 场所的 id

plat-name 第三方日志的名称

【命令模式】 特权模式、全局模式

【使用指导】

1. 如果不跟参数，则显示所有已经配置归属第三方日志平台的上网服务场所列表；
2. 如果有跟 netsite-id，则只显示指定的场所信息；
3. 如果有跟 plat-name，则显示归属该第三方日志的场所信息；

【配置举例】

```
Ruijie#sh plog config netsite 1
{ "code": 0, "msg": 0, "total": 1, "max": 100, "list": [ { "platform-name": [ "surfilter" ],
"platform-type": "surfilter", "service-code": "11112222333344", "service-name": "qwe",
"principal-name": "qwe", "principal-cert-type": "1021133", "principal-cert-code": "123",
"person-name": "qwe", "person-phone": "", "cap-type": "2", "service-type": "1", "business-nature":
"2", "status": "1", "address": "123", "create-time": "2018-12-13", "province-code": "122212",
"city-code": "111112", "area-code": "111113", "police-code": "22223333", "longitude": "123.050000",
"latitude": "023.050000", "start-time": "09:00", "end-time": "18:00", "producer-code": "1",
"producer-type": "1", "id": "1" } ] }
```

【提示信息】 -

配置举例

无

常见错误

无

2.5.6 配置AP信息

配置效果

- 网关设备可以根据配置的 AP 信息生成 AP 设备资料，并日志发送给第三方日志系统。

注意事项

- -

配置方法

配置 AP 设备

【命令格式】 **police-log-ap** *index*
【参数说明】 index：表示 ap 设备索引
【缺省配置】 无
【命令模式】 全局模式
【使用指导】 配置完成后，进入 config-plog-ap 命令模式

配置 AP 所属的场所

【命令格式】 **set service-code** *code-value* **platform** *plat-name*
【参数说明】 code-value：上网服务场所编码
plat-name：第三方日志平台名称
【缺省配置】 无
【命令模式】 config-plog-ap
【使用指导】 该命令必须先配置，然后才能配置其他参数，否则会提示错误。一个 AP 只能属于一个场所。

配置场所的参数

【命令格式】 *set key-string value*
【参数说明】 key-string：AP 设备参数名，通过 **show plog para-list ap { platform** *plat-name* | **netsite** *id* } *获取参数*
value：参数值
【缺省配置】 无
【命令模式】 config-plog-ap

【使用指导】 必须先配置 AP 设备所属的场所 service-code，否则会提示异常。

检验方法

- 使用 **show plog config ap [** *ap-id* **| netsite** *netsite-id* **start** *sid* **limit** *num* **| platform** *plat-name* **start** *sid* **limit** *num* | **start** *sid* **limit** *num* **]**命令可以查看 AP 设备配置信息。

【命令格式】 **show plog config ap [** *ap-id* **| netsite** *netsite-id* **start** *sid* **limit** *num* **| platform** *plat-name* **start** *sid* **limit** *num* | **start** *sid* **limit** *num* **]**

【参数说明】 ap-id：AP 设备的 id
netsite-id：场所 id
plat-name 第三方日志的名称
sid：起始输出的 ap id
num：最大输出的 ap 个数

【命令模式】 特权模式、全局模式

【使用指导】
1. 如果不跟参数，则显示所有 AP 设备信息；
2. 如果有跟 ap-id，则显示指定的 AP 设备信息；
3. 如果有跟 netsite-id，则显示指定场所的 AP 设备信息；
4. 如果有跟 plat-name，则显示指定第三方日志的 AP 设备信息；

【配置举例】

```
Ruijie#sh plog config ap start 0 limit 2
{"code": 0, "msg": 0, "total": 34, "max": 500, "list": [{"id": "1", "platform-name": ["surfilter"], "platform-type": "surfilter", "service-code": "35021200001003", "mac": "AA-AA-AA-AA-03-78", "apname": "AP 名称", "aptype": "0", "apfloor": "30", "create-time": "2018-12-07", "service-name": "上网服务场所名称" }, { "id": "2", "platform-name": [ "surfilter" ], "platform-type": "surfilter", "service-code": "35021200001003", "mac": "AA-AA-AA-AA-03-79", "apname": "AP 名称", "aptype": "0", "apfloor": "30", "create-time": "2018-12-07", "service-name": "上网服务场所名称" } ] }
```

【提示信息】 -

配置举例

无

常见错误

无

2.6 监视与维护

查看运行情况

作用	命令
查看运行情况	**show police-log status**
查看支持的第三方日志平台	**show plog platform**
查看指定网监平台支持的参数	**show plog para-list**
查看网监当前的配置	**show plog config**

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 POLICE-LOG 的调试开关。	**debug police-log**

3 LOG-POLICY

3.1 概述

日志策略能够提供精细化的日志控制，之前产品对所有用户产生的日志都是一样，且产生的日志可能不是客户所需要的。日志策略能够对用户、单 ip、ip 段指定特定的日志类型。

3.2 典型应用

典型应用	场景描述
日志策略	描述日志策略的基本场景及功能

3.2.1 日志策略典型应用场景

应用场景

日志策略：指定用户上报的日志类型。

功能部属

用户可以按照如下方式定制日志策略：

- 用户可以基于用户名，ip，ip 段配置日志策略。

3.3 功能详解

3.3.1 日志策略

主要设置用户或者 ip 用户的日志上报类型

工作原理

日志策略的工作原理是通过规则限定用户或者 ip 的日志类型

相关配置

使用 log-policy 命令可以创建策略。

使用 log-policy-relate 设置策略关联的对象

配置规则的参数决定上报哪种日志类型。

调换日志策略的优先级

3.4 产品说明



NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E 支持日志策略功能；NBR108G-P、NBR800G、NBR950G、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1500G、NBR2000G 不支持日志策略功能。

3.5 配置详解

3.5.1 配置日志策略

配置效果

- 建立日志策略对象。

注意事项

- 先配置的策略先生效

配置方法

↘ 配置日志策略

- 必须配置。

检验方法

使用 show log-policy 命令可以查看配置状态。

相关命令

↘ 配置日志策略

【命令格式】 **log-policy** *policy-name* { **netlog | 82log | none** }

【参数说明】 *policy-name*：日志策略名称。

【命令模式】 全局模式

【使用指导】 生成日志策略。

1：不能配置同名的日志策略

2：删除日志策略，可以在全局配置模式下执行 **no log-policy** *policy-name*

配置举例

↘ 配置日志策略

【配置方法】 ●

```
Ruijie# configure terminal
Ruijie(config)# log-policy auth 82log
Ruijie(config)# end
```

【检验方法】 ● 使用 show log-policy 命令可以查看配置状态。

```
Ruijie# show log-policy
log-policy auth 82log
```

常见错误

- 正则表达式不满足语法要求。
- 策略容量超过 1000 条限制。
- 策略名称长度超过最大 64 字节的限制。

3.5.2 设置策略关联对象

配置效果

- 设置策略关联对象。

注意事项

- 基于 ip 的策略，一条策略只能关联一个对象。
- 基于用户的策略，一条策略最多只能关联 10 个用户对象。
- 基于绑定 mac 的用户配置的日志策略只能在二层环境中使用。
- 基于绑定 mac 的用户的日志策略不支持 sam/smp/ess 场景下的认证日志。

配置方法

↘ 配置日志策略

- 必须配置。

检验方法

使用 show log-policy 命令可以查看配置状态。

相关命令

↘ 配置日志策略

【命令格式】 **log-policy-relate relate policyname** policy-name { **ip-host** *ip-address* **| ip-subnet** *subnet-address subnet-mask* **| ip-range** *ip-address-begin ip-address-end* | **subscriber** *user-name* | **auth-subscribe** *user-name* }

【参数说明】 *policy-name*：日志策略名称。

ip-address: ip 地址。

subnet-address: 子网地址。

subnet-mask: 子网掩码。

ip-address-begin: 起始地址。

ip-address-end: 结束地址。

user-name: 用户名称

【命令模式】 全局模式

【使用指导】 策略关联对象。

1：关联的策略必须存在

2： 删除日志策略，可以在全局配置模式下执行 **no log-policy-relate relate policyname** *policy-name* { **ip-host** *ip-address* | **ip-subnet** *subnet-address subnet-mask* **| ip-range** *ip-address-start ip-address-end* | **subscriber** *user-name* | **auth-subscribe** *user-name* }

基于绑定 mac 的用户的日志策略只能在二层环境中使用，基于绑定 mac 的用户的日志策略不支持 sam/smp/ess 认证场景下的认证日志。

用户管理模块或营销认证模块重启时，这期间将无认证日志

配置举例

↘ 配置日志策略

【配置方法】

- 配置举例

```
Ruijie# configure terminal
Ruijie(config)# log-policy-relate relate policyname subnet ip-subnet 192.168.5.0 255.255.255.0
Ruijie(config)# log-policy-relate relate policyname range ip-range 192.168.3.1 192.168.5.1
Ruijie(config)# log-policy-relate relate policyname ip ip-host 192.168.3.11
```

```
Ruijie(config)# log-policy-relate relate policyname sub-any subscriber any
Ruijie(config)# log-policy-relate relate policyname auth auth-subscribe any
Ruijie(config)# end
```

【检验方法】

- 使用 show log-policy 命令可以查看配置状态。

```
Ruijie# show log-policy
  log-policy subnet none
      log-policy-relate relate policyname subnet ip-subnet 192.168.5.0 255.255.255.0
  log-policy range 82log
      log-policy-relate relate policyname range ip-range 192.168.3.1 192.168.5.1
  log-policy ip none
      log-policy-relate relate policyname ip ip-host 192.168.3.11
  log-policy auth netlog
      log-policy-relate relate policyname auth auth-subscribe any
  log-policy sub-any netlog
      log-policy-relate relate policyname sub-any subscriber any
```

常见错误

- 正则表达式不满足语法要求。
- 策略名称长度超过最大 64 字节的限制。
- 用户名长度超过最大 128 字节的限制
- 基于 ip 范围配置时，起始地址大于结束地址
- 用户或者 ip 参数已被使用

3.5.3 日志策略优先级调换

配置效果

- 调换两条策略的顺序

注意事项

- 两条日志策略必须是前后关系

配置方法

↘ 日志策略调换顺序

- 必须配置。

检验方法

使用 show log-policy 命令可以查看配置状态。

相关命令

日志策略调换顺序

【命令格式】 **log-policy-config priority-swap** *policy-name1 policy-name2*

【参数说明】 *policy-name1*：日志策略名称。

policy-name2：日志策略名称

【命令模式】 全局模式

【使用指导】 策略优先级调换。

1：两条日志策略必须存在

2：两条策略必须是前后关系

配置举例

日志策略调换顺序

【配置方法】

- 配置举例

```
Ruijie#show log-policy
  log-policy subnet none
      log-policy-relate relate policyname subnet ip-subnet 192.168.5.0 255.255.255.0
  log-policy range 82log
      log-policy-relate relate policyname range ip-range 192.168.3.1 192.168.5.1
  log-policy ip none
      log-policy-relate relate policyname ip ip-host 192.168.3.11
  log-policy auth netlog
      log-policy-relate relate policyname auth auth-subscribe any
  log-policy sub-any netlog
      log-policy-relate relate policyname sub-any subscriber any
Ruijie(config)# log-policy-config priority-swap subnet range
Ruijie(config)# end
```

【检验方法】

- 使用 show log-policy 命令可以查看配置状态。

```
Ruijie#show log-policy
  log-policy range 82log
      log-policy-relate relate policyname range ip-range 192.168.3.1 192.168.5.1
  log-policy subnet none
```

```
    log-policy-relate relate policyname subnet ip-subnet 192.168.5.0 255.255.255.0
log-policy ip none
    log-policy-relate relate policyname ip ip-host 192.168.3.11
log-policy auth netlog
    log-policy-relate relate policyname auth auth-subscribe any
log-policy sub-any netlog
  log-policy-relate relate policyname sub-any subscriber any
```

常见错误

- 正则表达式不满足语法要求。
- 日志策略不存在
- 两条日志策略不是前后关系

3.6 监视与维护

清除各类信息

作用	命令
删除所有的日志策略	**clear log-policy**

查看运行情况

作用	命令
策略日志策略信息	**show log-policy** [**policyname** *policy-name*]

4 SNMP

4.1 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

4.2 典型应用

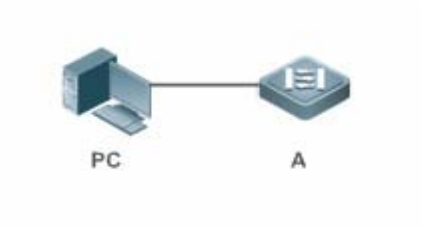
典型应用	场景描述
通过 SNMP 管理网络设备	通过 SNMP 网络管理器对网络设备进行管理和监控。

4.2.1 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 4-1



【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。

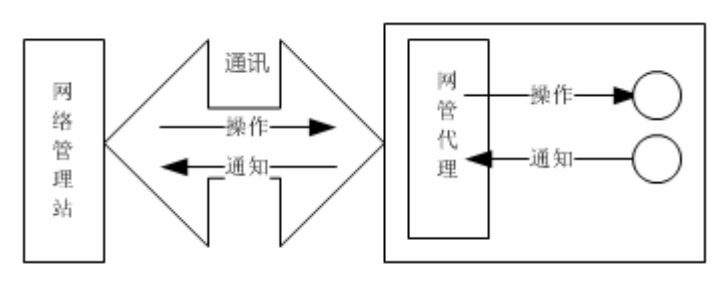
4.3 功能详解

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 4-2 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的系统，也称为 NMS (Network Management System)。

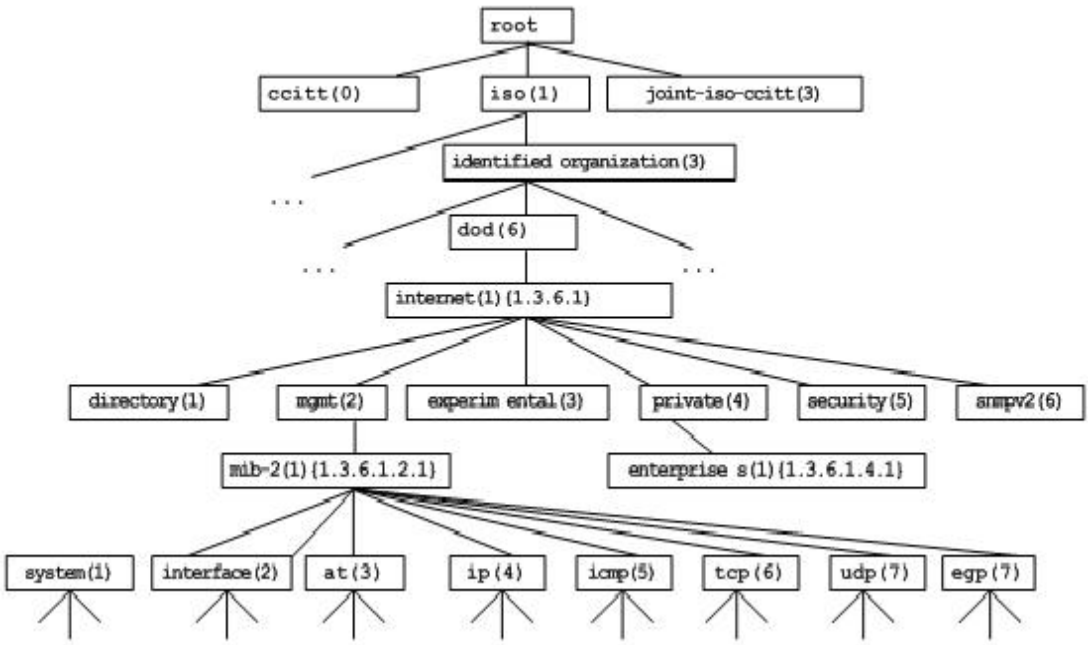
SNMP 代理

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 4-3 MIB 树形层次结构



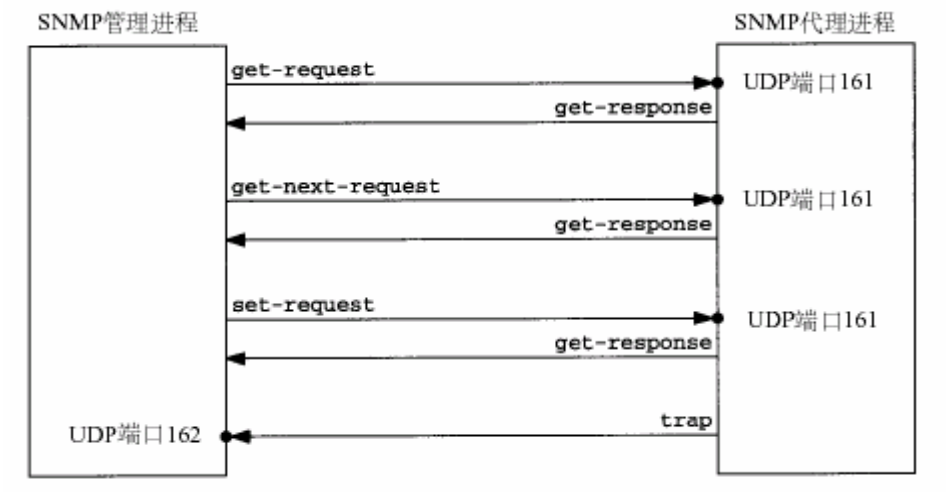
操作类型

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 4-4 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。

4.3.1 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 4-4 SN MP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、系统位置和设备的网元信息为空；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 net-id** 命令配置或删除设备的网元信息。

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；Trap 消息缺省不带私有字段。

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 trap-format private** 命令设置或关闭发送 Trap 消息时携带私有字段的功能。

使用 **snmp-server system-shutdown** 命令打开或关闭发送系统重启 Trap 功能。

↘ 设置 SNMP 攻击防护检测功能

缺省情况下，没有打开 SNMP 攻击防护检测功能。

使用 **snmp-server authentication attempt** *times* **exceed** { **lock** | **lock-time** *minutes* | **unlock** }命令设置打开攻击防护检测功能。

↘ 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，该命令需要与全局配置命令 **password policy** 一起使用。

↘ 设置 SNMP 日志功能记录 NMS 对 SNMP Agent 的 GET、GET-NEXT 和 SET 操作

缺省情况下，SNMP 日志开关处于关闭状态。

使用 **snmp-server logging** { **get-operation** | **set-operation** }命令打开记录 get、set 操作的功能，get 开关控制 GET、GET-NEXT 操作记录，set 开关控制 SET 操作记录

4.3.2 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。

4.3.3 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 SnmpEngineID。

引擎标识为一个 OCTET STRING，长度为 5～32 字节长。在 RFC3411 中定义了引擎标识的格式：

- 前 4 个字节标识厂商的私有企业号（由 IANA 分配），用 HEX 表示。
- 第 5 个字节表示剩下的字节如何标识：
- 0：保留
- 1：后面 4 个字节是一个 Ipv4 地址。
- 2：后面 16 个字节是一个 Ipv6 地址。
- 3：后面 6 个字节是一个 MAC 地址。
- 4：文本，最长 27 个字节，由厂商自行定义。
- 5：16 进制值，最长 27 个字节，由厂商自行定义。
- 6-127：保留。
- 128-255：由厂商特定的格式。

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。

4.4 产品说明



NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE 支持 SNMP IPV6 功能；NBR800G、NBR950G、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR108G-P、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1500G、NBR2000G 不支持 SNMP IPV6 功能。

4.5 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。	
	enable service snmp-agent	启动 Agent 功能。
	snmp-server community	配置认证名和访问权限。
	snmp-server user	配置 SNMP 用户信息。
	snmp-server view	配置 SNMP 视图。
	snmp-server group	配置 SNMP 用户组。
	snmp-server authentication	配置 SNMP 攻击防护检测功能
	snmp-server enable secret-dectionaty-check	配置对 community 和 user 进密码字典令检查。
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。
	snmp-server trap-format private	发送 Trap 消息时携带私有字段
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 logging	设置日志功能
	snmp-server chassis-id	设置设备序列码。
	snmp-server net-id	设置设备的网元信息。
	snmp-server packetsize	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。

4.5.1 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。

设置 SNMP 日志功能，记录 NMS 对 SNMP Agent 的 GET、GET-NEXT 和 SET 操作

- 可选配置。
- SNMP 日志功能将记录 NMS 对 SNMP Agent 的 GET、GET-NEXT 和 SET 操作。当进行 GET 和 GET-NEXT 操作时，Agent 会记录 NMS 用户的 IP 地址、操作类型、操作节点的 OID。当进行 SET 操作时，Agent 会记录 NMS 用户的 IP 地址、操作类型、操作的节点的 OID、设置的值。这些日志将被发送到设备的信息中心，级别为 informational，即作为设备的一般提示信息。

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** { **ipv6** *ipv6-aclname* | *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。

ipv6-aclname：ipv6 访问列表名称，关联指定的访问列表，指定能访问 MIB 的 ipv6 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*]] [**ipv6** *ipv6-aclname*] [*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。

ipv6-aclname：ipv6 访问列表名称，关联指定的访问列表，指定能访问 MIB 的 ipv6 NMS 地址范围。

【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** { **ipv6** *ipv6-aclname* | *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。

ipv6-aclname：ipv6 访问列表名称，关联指定的访问列表，指定能访问 MIB 的 ipv6 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】 特权用户模式

【使用指导】 该命令用于启动设备的 SNMP 代理功能。

启动 SNMP 攻击防护检测功能

【命令格式】 **snmp-server authentication attempt** *times* **exceed** { **lock** | **lock-time** *minutes* | **unlock** }

【参数说明】 *times*：连续认证失败的尝试次数。

lock：连续认证失败后，永久禁止该源 IP 地址重新进行认证访问，需要管理员手工解除。

lock-time *minutes*：连续认证失败后，禁止该源 IP 地址一段时间，超过限定时间后可以重新进行论证访问。

unlock：连续认证失败后，允许该源 IP 地址继续进行访问，相关于没有配置 SNMP 的攻击防护检测功能。

【命令模式】 全局配置模式

【使用指导】 配置 SNMP 攻击防护检测功能，以使在连续认证失败后做出对应的处理策略。

对于被永久禁止的源 IP 地址，只有管理员进行手动解除后，该源 IP 地址才能重新访问认证。

对于被禁止一段时间内认证的源 IP 地址，当设置的禁止时间超时或者管理员手工解除后该源 IP 地址才能重新访问认证。

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。

设置 SNMP 日志功能记录 NMS 对 SNMP Agent 的 GET、GET-NEXT 和 SET 操作

【命令格式】 **snmp-server logging** { **get-operation | set-operation** }

【参数说明】 **get-operation**：记录 GET、GET-NEXT 操作的开关

set-operation：记录 SET 操作的开关

【命令模式】 全局配置模式

【使用指导】 使用此命令将记录 NMS 对 SNMP Agent 的 GET、GET-NEXT、SET 操作。当进行 GET 和 GET-NEXT 操作时，Agent 会记录 NMS 用户的 IP 地址，操作类型以及操作的节点 OID。当进行 SET 操作时，Agent 会记录 NMS 用户的 IP 地址，操作类型，操作的节点 OID 和设置的值。

⚠ 大量的日志记录会影响设备的性能，正常情况下，建议关闭 SNMP 日志功能。

显示 SNMP 的状态信息

【命令格式】 **show snmp** [**mib** | **user** | **view** | **group| host | locked-ip | 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。

locked-ip：snmp 连续认证失败后被锁定的源 IP 地址信息。

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

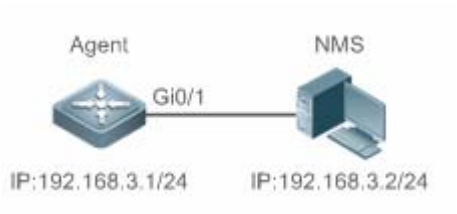
【使用指导】 -

配置举例

SNMPv3 配置举例

【网络环境】

图 4-5



- 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
```

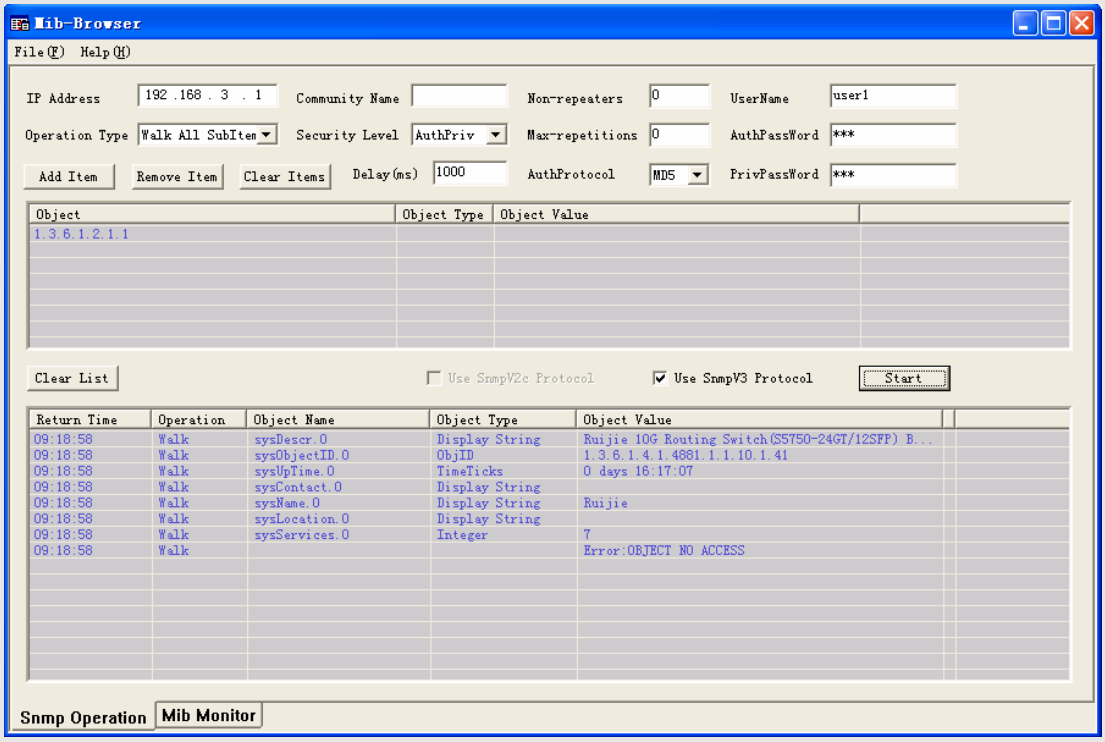
```
Ruijie#show snmp view
view1(include) 1.3.6.1.2.1.1
view2(include) 1.3.6.1.2.1.1.4.0
default(include) 1.3.6.1
```

```
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

-

4.5.2 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。

发送 Trap 消息时携带私有字段

- 可选配置。
- 当需要 Trap 消息携带私有字段时，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** [**oob**] { *host-addr* | **ipv6** *ipv6-addr* } [**traps | inrorms**] [**version** { **1** | **2c** | **3** { **auth** | **noauth** | **priv** }] *community-string* [**udp-port** *port-num*] [*notification-type*]

【参数说明】 **oob：**将告警服务器指定为带外通信（一般指通过 MGMT 口发往告警服务器）

host-addr：SNMP 主机地址。

ipv6-addr：SNMP 主机地址（ipv6 ）。

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，对于相同主机（相同端口 ），最后的一次配置会和前面的配置合并，即如要给相同主机发送不同 Trap 消息，可以分别配置不同 Trap 类型，最终这些配置会合并到一起。

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；

ospf: 启动 OSPF 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。

配置发送 Trap 消息时携带私有字段

【命令格式】 **snmp-server trap-format private**

【参数说明】 -

【配置模式】 全局配置模式

【使用指导】 使用该命令可配置发送 Trap 消息携带私有格式字段，包含的字段目前支持的有告警发生时间，各个字段的具体数据类型和数据范围可参见 RUIJIE-TRAP-FORMAT-MIB.mib 文件说明。

配置举例

配置启用 trap 功能

【网络环境】

图 4-6



- 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

-

4.5.3 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

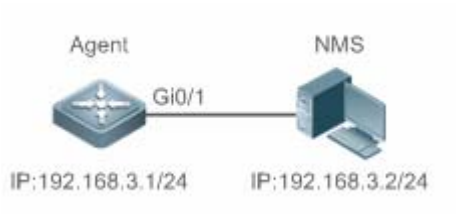
【使用指导】 关闭 SNMP 服务开关，但不会屏蔽 SNMP 代理参数。

配置举例

配置启用 snmp 服务功能

【网络环境】

图 4-7



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

-

4.5.4 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。

配置设备的网元信息

- 可选配置。
- 当需要修改网元编码信息时，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。

配置设备的网元信息

【命令格式】 **snmp-server net-id** *text*

【参数说明】 *text*：设置设备网元编码 text，text 是长度为 1~255 的字符串，区分大小写，可包含空格。
【配置模式】 全局模式
【使用指导】 配置设备网元编码信息。

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

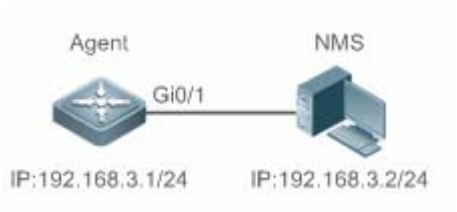
【命令格式】 **snmp-server flow-control pps** [*count*]
【参数说明】 *count*：每秒处理的 SNMP 请求报文数量，范围<50-65535>。
【命令模式】 全局配置模式
【使用指导】 如果 SNMP 的请求报文太多导致 SNMP 任务的 CPU 占用比较高，可以配置 SNMP 流控，限制 SNMP 任务每秒处理的请求报文个数，从而控制 SNMP 任务的 CPU 占用情况。

配置举例

设置 SNMP 的控制参数

【网络环境】

图 4-8



- 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 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 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

-

4.6 监视与维护

清除各类信息

作用	命令
清除 SNMP 连续认证失败后被锁定的源 IP 地址表	**clear snmp locked-ip** [**ipv4** *ipv4-address* | **ipv6** *ipv6-address*]

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**]

5 CM-APM

5.1 概述

CM（Centralized Management，集中管理），APM（Application Performance Management，应用性能管理，也称业务性能管理），是锐捷网关设备集中管理以及性能监控的功能简称，需要配合锐捷 RAC（Remote Auto-management Center，远程运维中心）网管软件一起使用。

它们能实现网关设备的集中管理，并基于全局进行设备性能、VPN、流量、业务情况的监控，大大提高网管的工作效率。

锐捷 CM-APM 通常应用于总分型企业、连锁酒店，普教城域网等需要同时管理多台网关设备的场景。

下文仅介绍 CM-APM 的相关内容。

协议规范

- 无

5.2 典型应用

典型应用	场景描述
总分型企业实现全网网关集中管理、性能监控	在典型的总分型企业拓扑中，WEB、ERP 等办公软件的服务器、数据中心等都部署在企业总部。企业总部以及各分支机构的网络出口都有部署网关（如 EG 网关）。

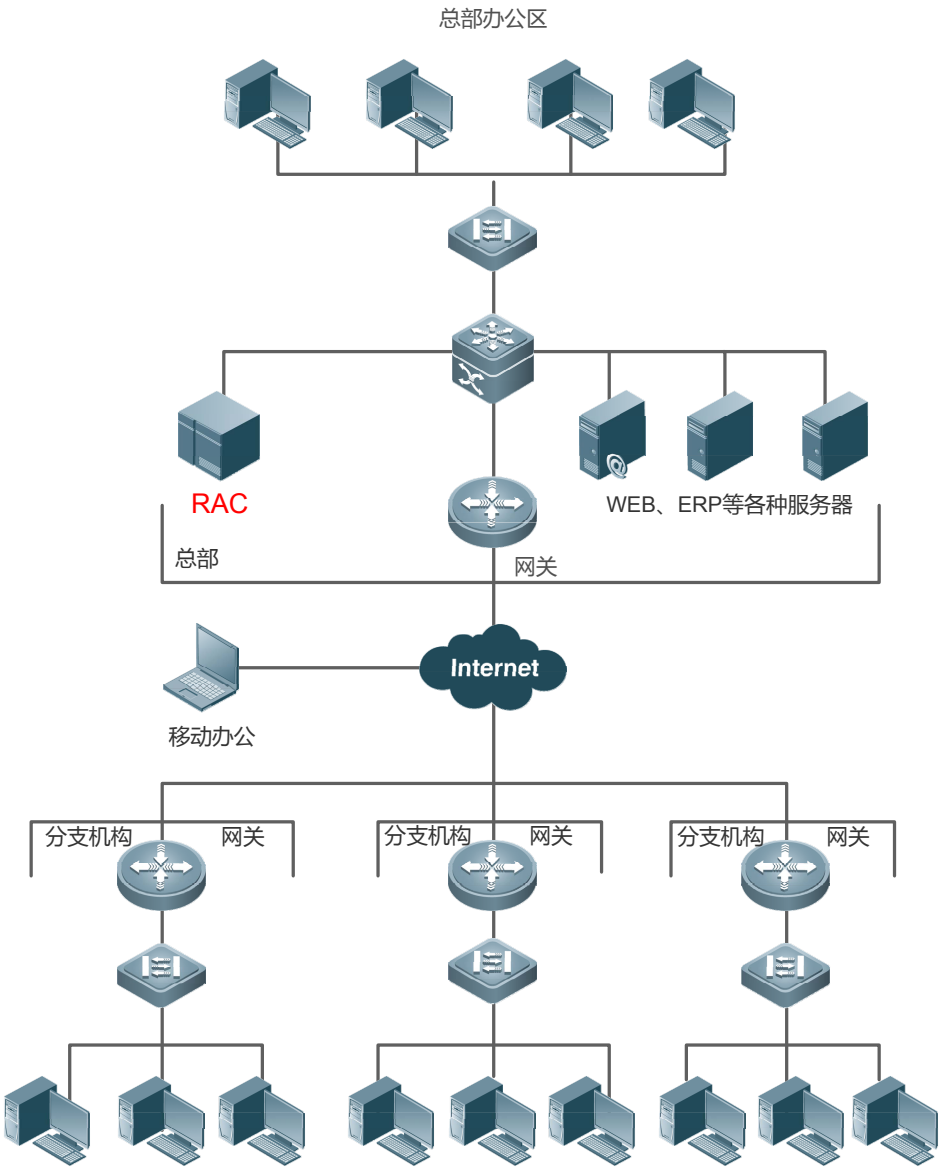
5.2.1 总分型企业实现全网网关集中管理、性能监控

应用场景

在典型的总分型企业拓扑中，WEB、ERP 等办公软件的服务器、数据中心等都部署在企业总部。企业总部以及各分支机构的网络出口都有部署网关（如 EG 网关）。总分型企业的带宽特点是：一般总部（一般通过光纤联网）的带宽会比较大，而且通常不只一个线路。而各分支机构（一般通过 ADSL 联网）的带宽都比较小。总部 WEB、ERP 系统通常是由总部信息资源部运维的，他们负责业务服务器的维护工作。在这个场景中，企业员工访问 WEB、ERP 等业务系统，通常有三种情况：

- 在总部内网直接访问业务系统，此种情况，由于直接走内网，网速很快，只要业务服务器本身没有问题，一般用户体验会很好。
- 在分支机构办公的员工访问业务系统，此种情况，业务系统的体验可能更容易受到网络等因素的制约而变得不好。
- 移动办公的员工通过其他网络以 VPN 的方式访问业务系统。此种情况同样可能受到网络等因素的影响。

图 5-1



【注释】 网关为出口网关设备。
RAC 为锐捷网管软件

功能部属

- 开启全网网关应用识别、二三层识别、流量审计等功能。
- 开启全网网关设备状态（CPU、内存、硬盘）。
- 开启分支机构网关设备 VPN 状态监控。
- 开启分支设备网关设备流量带宽监控。
- 监控分支机构访问总部内网首页的加载耗时。

5.3 功能详解

基本概念

时延

时延是指一个报文或分组从一个网络的一端传送到另一个端所需要的时间。

HTTP GET

HTTP（hypertext transport protocol，超文本传送协议）是一种详细规定了浏览器和万维网服务器之间互相通信的规则，通过因特网传送万维网文档的数据传送协议。HTTP GET 是 HTTP 请求的一种，通常我们浏览网页都是通过 GET 请求获取网页的。

功能特性

功能特性	作用
设备状态监控	RAC 统一监控所有网关设备的 CPU、内存、硬盘使用情况，易于及时发现问题。
VPN 状态监控	对于总分型企业等典型场景，分支机构一般通过 VPN 与总部实现虚拟专网相连，分支机构访问总部的办公系统，都承载于 VPN 线路之上。可以说，VPN 线路质量的好坏，直接影响到分支机构的办公效率。RAC 对分支机构网关设备的 VPN 状态进行监控，可以及时发现问题，避免影响办公。
带宽状态监控	RAC 统一监控所有网关设备的带宽流量使用情况，易于及时发现问题。
业务数据加载速率	RAC 统一监控所有网关设备的特定业务的流量速率，将各网关设备的业务数据流量速率直观化，有助于及时发现业务慢等问题。
PING 检测	PING 通常用于检测网络是否正常，RAC 统一监控所有设备的 PING 检测结果，有助于及时发现网络异常。
行为报表 URL-TOPN	某些情况下，我们可能希望知道哪些 URL 是大家访问最多的，根据用户的行为进行工作效率的分析，又或者作为广告投放的依据。
网页加载耗时监控	我们经常会收到用户打开网页慢的抱怨，甚至是投诉。这种情况下，我们希望能够将网页打开快慢速度量化的表示出来，从而判断是否的确打开慢，还是只是部分人的主观感觉。
视频会议质量监控	RAC 对整网视频会议质量进行监控，有助于及时发现问题。

5.3.1 设备状态监控

RAC 统一监控所有网关设备的 CPU、内存、硬盘使用情况，易于及时发现问题。

工作原理

设备状态监控是指设备定期采样自身的 CPU 利用率、内存利用率以及硬盘利用率，并将采样数据发送给 RAC 进行统一监控。

相关配置

↘ 启动设备状态监控功能

缺省情况下，该功能是关闭的。

可以使用全局开关命令 **apm sample enable** 启动该功能。

如果在开启全局开关的情况下希望单独关闭该功能，则可以通过命令 **apm sample cpu-mem disable 和 apm sample sata-flash disable** 来单独关闭。

↘ 调整设备状态监控采样的周期

缺省情况下，设备状态采样周期为 5 分钟。

使用 **apm sample default interval** *second* 全局调整采样的周期，取值范围是 10~3600 秒；

也可以通过 **apm sample cpu-mem interval** *second 和* **apm sample sata-flash interval** *second* 来单独调整采样周期。

采样周期越小，则 RAC 上显示的信息会越实时，但是过小的采样周期可能使得设备以及 RAC 服务器的处理负担加重。

5.3.2 VPN状态监控

对于总分型企业等典型场景，分支机构一般通过 VPN 与总部实现虚拟专网相连，分支机构访问总部的办公系统，都承载于 VPN 线路之上。可以说，VPN 线路质量的好坏，直接影响到分支机构的办公效率。RAC 对分支机构网关设备的 VPN 状态进行监控，可以及时发现问题，避免影响办公。

工作原理

VPN 状态监控是通过设备定期采样自身的 VPN 通断情况以及流量情况，并将采样数据发送给 RAC 进行统一监控。

相关配置

↘ 启动 VPN 状态监控功能

缺省情况下，该功能是关闭的。

可以使用全局开关命令 **apm sample enable** 启动该功能。

如果在开启全局开关的情况下希望单独关闭该功能，则可以通过命令 **apm sample vpn disable 和 apm sample vpn-detail disable** 来单独关闭。

↘ 调整 VPN 状态监控采样的周期

缺省情况下，设备状态采样周期为 5 分钟。

使用 **apm sample default interval** *second* 全局调整采样的周期，取值范围是 10~3600 秒；

也可以通过 **apm sample vpn interval** *second 和* **apm sample vpn-detail interval** *second* 来单独调整采样周期。

采样周期越小，则 RAC 上显示的信息会越实时，但是过小的采样周期可能使得设备以及 RAC 服务器的处理负担加重。

5.3.3 带宽状态监控

RAC 统一监控所有网关设备的带宽流量使用情况，易于及时发现问题。

工作原理

带宽状态监控是通过设备定期采样流量审计的整机 IP/会话数，接口流量、应用流量、应用类型流量、用户流量等信息，并将采样数据发送给 RAC 进行统一监控。

相关配置

↘ 启动带宽状态监控功能

缺省情况下，该功能是关闭的。

可以使用全局开关命令 **apm sample enable** 启动该功能。

如果在开启全局开关的情况下希望单独关闭该功能，则可以通过命令 **apm sample ip-session disable** 、 **apm sample intf-flowrate disable** 、 **apm sample app-type-flowrate disable** 、 **apm sample app-flowrate disable** 和 **apm sample user-flowrate disable** 来单独关闭。

↘ 调整带宽状态监控采样的周期

缺省情况下，设备状态采样周期为 5 分钟。

使用 **apm sample default interval** *second* 全局调整采样的周期，取值范围是 10~3600 秒；

也可以通过 **apm sample ip-session interval** *second* 、 **apm sample intf-flowrate interval** *second* 、 **apm sample app-type-flowrate interval** *second* 、 **apm sample app-flowrate interval** *second* 和 **apm sample user-flowrate interval** *second* 来单独调整采样周期。

采样周期越小，则 RAC 上显示的信息会越实时，但是过小的采样周期可能使得设备以及 RAC 服务器的处理负担加重。

5.3.4 业务数据加载速率监控

RAC 统一监控所有网关设备的特定业务的流量速率，将各网关设备的业务数据流量速率直观化，有助于及时发现业务慢等问题。

工作原理

业务数据加载速率监控是通过设备定期采样特定业务的数据加载速率，并将采样数据发送给 RAC 进行统一监控。

相关配置

↘ 启动业务数据加载速率监控功能

缺省情况下，该功能是关闭的。

可以使用全局开关命令 **apm sample enable** 启动采样功能，同时通过 **apm sample business application** *app-name* 添加需要监控的业务（应用）名，其中 app-name 为应用名。

如果在开启全局开关的情况下希望单独关闭该功能 ,则可以通过命令 **apm sample ip-session business disable** 来单独关闭；也可以通过 **no apm sample business application all** 删除所有需要监控的业务来关闭。

↘ 调整业务数据加载速率监控的周期

缺省情况下，设备状态采样周期为 5 分钟。

使用 **apm sample default interval** *second* 全局调整采样的周期，取值范围是 10~3600 秒；

也可以通过 **apm sample business interval** *second* 来单独调整采样周期。

采样周期越小，则 RAC 上显示的信息会越实时，但是过小的采样周期可能使得设备以及 RAC 服务器的处理负担加重。

5.3.5 PING检测

PING 通常用于检测网络是否正常，RAC 统一监控所有设备的 PING 检测结果，有助于及时发现网络异常。

工作原理

PING 检测是设备定期主动去 PING 指定的服务器，并将 PING 检测的结果发送给 RAC 进行统一监控。

相关配置

↘ 启动 PING 检测功能

缺省情况下，该功能是关闭的。

可以使用全局开关命令 **apm sample enable** 启动采样功能，同时通过 **apm sample ping-detect serve** 命令添加需要检测的服务器地址。

如果在开启全局开关的情况下希望单独关闭该功能，则可以通过命令 **apm sample ping-detect disable** 来单独关闭；也可以通过 **no apm sample ping-detect server all** 删除所有 PING 服务器来关闭。

↘ 调整 PING 检测参数

缺省情况下，设备状态采样周期为 5 分钟。

使用 **apm sample default interval** *second* 全局调整采样的周期，取值范围是 10~3600 秒；

也可以通过 **apm sample ping-detect interval** *second* 来单独调整采样周期。

采样周期越小，则 RAC 上显示的信息会越实时，但是过小的采样周期可能使得设备以及 RAC 服务器的处理负担加重。

5.3.6 行为报表URL-TOPN

某些情况下，我们可能希望知道哪些 URL 是大家访问最多的，根据用户的行为进行工作效率的分析，又或者作为广告投放的依据。

工作原理

行为报表 URL-TOPN 依托于网关设备的 URL 审计功能，每天定期对访问最多的站点进行统计汇总，并将统计结果发送给 RAC 进行统一监控。

相关配置

↘ 启动 URL-TOPN 功能

缺省情况下，该功能是关闭的。

可以使用全局开关命令 **apm sample enable** 启动采样功能。

如果在开启全局开关的情况下希望单独关闭该功能，则可以通过命令 **apm sample url-topn disable** 来单独关闭。

↘ 调整 URL-TOPN 的参数

缺省情况下，开启全局采样功能后，默认统计汇总访问最多的前 50 个站点，可以通过 **apm sample url-topn top** *num* 来调整统计发送 TOP 几，取值范围是 1~100；

缺省情况下，URL-TOPN 是在每天凌晨 1 点统计前一天的数据并进行发送的，可以通过 **apm sample url-topn send-time** *hour* 来调整时间点。

通常情况下，将时间设置为设备比较空闲的时候，避免统计处理影响设备正常业务的运行。

5.3.7 网页加载耗时监控

我们经常会收到用户打开网页慢的抱怨，甚至是投诉。这种情况下，我们希望能够将网页打开快慢速度量化的表示出来，从而判断是否的确打开慢，还是只是部分人的主观感觉。

工作原理

设备通过实时监控用户的 HTTP GET 请求，并对 HTTP 请求到回应的整个过程进行监控记录，最终得出网页加载耗时，然后将监控数据发送给 RAC 进行统一监控。

相关配置

↘ 启动网页加载耗时监控功能

缺省情况下，该功能是关闭的。

可以通过 **apm webpage url** *string* 来添加需要监控的 URL，添加完成后，就自动开启了网页加载耗时监控功能。
可以通过 **no apm webpage url all** 来关闭整个功能。
如果希望在不删除 URL 表项的前提下关闭功能，则可以通过命令 **no apm webpage enable** 来关闭。

5.3.8 视频会议质量监控

RAC 对整网视频会议质量进行监控，有助于及时发现问题。

工作原理

设备通过实时监控用户的视频会议数据流，对时延、丢包、乱序等进行检测，并根据这些性能数据推算出视频会议的质量。最终将结果发送给 RAC 进行统一监控。

相关配置

↘ 启动视频会议质量监控功能

缺省情况下，该功能是关闭的。

可以通过 **apm conference-system** { **application** *app-name* } | { **access-list** *acl_id* **alias** *alias-name* } 来添加需要监控的数据流。添加完成后，就自动开启了视频会议质量监控功能。
可以通过 **no apm conference-system application all** 和 **no apm conference-system access-list all** 来关闭整个功能。
如果希望在不删除应用以及 ACL 的前提下暂时关闭该功能，则可以通过命令 **no apm conference-system enable** 来关闭。

5.4 产品说明

NBR108G-P、NBR3000G-S 、NBR1500G、NBR2000G、NBR1000G-C、NBR2000G-C、NBR800G、NBR950G 不支持集中管理功能， NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持集中管理功能。

5.5 配置详解

配置项	配置建议 & 相关命令	
配置 APM 日志服务器	⚠ 必须配置。用于发送 APM 信息	
	apm server	设置 APM 日志服务器
	apm log-type	设置 APM 日志往哪个服务器发送
	apm export-rate	设置 APM 日志的发送速率
	apm export-length	设置 APM 日志报文有效数据的最大长度
	apm template send-period	设置 APM 日志模板发送周期

配置 APM 监控信息	⚠ 必须配置。用于设置需要开启哪些 APM 监控	
	apm sample enable	开启全局 APM 采样监控
	apm sample disable	关闭指定的 APM 监控
	apm sample interval	设定 APM 采样周期
	apm sample ping-detect	设置 PING 检测相关参数
	apm sample url-topn	设置 URL-TOPN 的相关参数
	apm webpage	设置网页加载耗时监控
	apm conference-system	设置视频会议质量监控

5.5.1 配置APM日志服务器

配置效果

- 配置 APM 日志发送服务器的信息，包括 IP、端口、协议等。
- 配置各 APM 日志发送给哪个日志服务器。

注意事项

- 配置完 APM 日志服务器的相关信息后，还需要指定日志类型需要发给哪个服务器。

配置方法

↘ 设置 APM 日志服务器

- 必须配置。
- 若无特殊要求，只需要设置一个默认的日志服务器即可。

↘ 设置 apm 日志往哪个服务器发送

- 必须配置。
- 若无特殊要求，只需要设置将所有信息都发往默认服务器即可。

↘ 设置 APM 日志发送速率

- 可选配置。
- 若无特殊要求，按默认配置即可。如果 APM 日志发送速率设置过大，在 APM 信息很大的情况下，可能造成设备 CPU 偏高。

↘ 设置日志报文有效数据的最大长度

- 可选配置

- 若无特殊要求，按默认配置即可。

设置 APM 模板发送周期

- 可选配置。
- 若无特殊要求，按默认配置即可。

检验方法

结合下文“配置 APM 监控信息”开启监控功能，并正确设置 APM 日志服务器以及对应的日志类型。

- 检查 RAC 服务器是否有收到对应的报文。
- 通过 show apm server log-count 检查日志发送情况。

相关命令

设置 APM 日志服务器

【命令格式】 **apm server** *name* { *ip-address* } [source *ip-address*] [*port*] [**tcp** | **udp**] [**oob**]

【参数说明】 *name*：APM 日志服务器的名字

ip-address：APM 日志服务器的 IP 地址 source：Apm 绑定的本地源 ip

port：APM 日志服务器的端口号

【命令模式】 全局模式

【使用指导】 可以通过 tcp 和 udp 来指定 APM 日志发送采用的协议，默认是 tcp 协议；为了保证信息的可靠性，建议使用 tcp 协议进行信息发送。

Source 配置用于创建 socket 时绑定源 ip，可以解决 vpn 等场景问题，如果配置有 source，则配置的 source 会生效；如果未配置 source，并且该 server 未配置，则认为 source 为 0，如果该 server 已经配置，则 source 保留原有的，其余根据新的配置进行更新。

如果是通过管理口来发送日志信息，则指定 oob 关键字。

要删除一个服务器，使用 **no apm server** *name* 命令。

设置 APM 日志往哪个服务器发送

【命令格式】 **apm log-type** { *type* | **default** } **priority** *prio* **server** *name*

【参数说明】 *type*：apm 消息类型，通过 show apm log-type 查看每个数值代表的消息类型。

prio：配置的消息类型对应的优先级，取值 0-2，其中 0 的优先级最高

【命令模式】 全局模式

【使用指导】 设置消息优先级以及发往哪个 apm 服务器，一个消息只能往一个服务器发送。default 表示特殊配置的除外，其余所有日志都往该服务器发。一般情况下，我们只需要配置一个 default 的即可。

删除所有消息类型，使用命令 **no apm log-type all**

删除 default 的所有消息类型，使用命令 **no apm log-type default**

删除某一个消息类型，使用命令 **no apm log-type** *type*。其中该 type 指的是已经被单独配置过服务器的消息类型。

设置 APM 日志发送速率

【命令格式】 **apm export-rate** *rate*

【参数说明】 *rate*：每秒发送多少个 apm 信息，取值范围 10~100000 之间。

【命令模式】 全局模式

【使用指导】 默认值为 1000 个/秒。无特别需求，建议使用默认值即可。过高的配置可能导致 CPU 偏高。过低的配置可能导致日志信息丢失。

设置日志报文有效数据的最大长度

【命令格式】 **apm export-length** *value*

【参数说明】 *value*：ipfix 报文有效数据的长度，从从 TCP 或 UDP 有效数据算起，单位为字节，取值范围为 300~1400。

【命令模式】 全局模式

【使用指导】 默认值为 1400，通常情况下，此项无需配置，取默认值即可。该值越大，传输同样信息量的情况下，带宽消耗越小。

设置 APM 模板发送周期

【命令格式】 **apm template send-period** *seconds*

【参数说明】 *seconds*：定时发送模板时长，单位为秒，取值范围为 60~3600。

【命令模式】 全局模式

【使用指导】 模板发送周期，默认为 5min。APM 日志服务器（也就是 RAC 服务器）是根据模板来进行日志格式提取解析的，定期发送模板给服务器，可以避免服务器模板数据丢失时（如重启或刚上线）无法进行消息解析。

配置举例

本章节配置举例并入下一章节“配置 APM 监控信息”

常见错误

- 只配置了 APM 日志服务器，没有指定消息类型发往该日志服务器，导致 RAC 服务器都没有收到相关的 APM 信息。

5.5.2 配置APM监控信息

配置效果

- 开启全局 APM 采样监控，设备会采集 CPU、内存、硬盘状态、VPN 状态、带宽状态、业务数据加载速率、PING 检测、行为报表 URL-TOPN 等信息，并发送给 RAC 服务器。
- 开启网页加载耗时监控，并配置相应的监控 URL，则设备会监控该网页的加载耗时，并发送给 RAC 服务器。
- 开启视频会议质量监控，并配置需要监控的应用或者 ACL，则设备会评估该视频会议的质量，并发送给 RAC 服务器。

注意事项

- 设备状态、VPN 状态、带宽状态、业务数据加载速率、PING 检测、行为报表 URL-TOPN，开启这几个功能，都必须先通过 apm sample enable 开启全局的采样功能。而这几个功能在开启全局采样功能的情况下，可以单独关闭。
- 有硬盘的设备才支持行为报表 URL-TOPN。

配置方法

开启全局 APM 采样监控

- 必须配置。
- 开启设备状态、VPN 状态、带宽状态、业务数据加载速率、PING 检测、行为报表 URL-TOPN 这几个功能，必须先开启全局采样开关。

关闭指定类型的 APM 监控

- 可选配置。
- 在开启了全局的 APM 采样后，如果不需要某些 APM 监控功能，可以单独关闭。

设置 APM 采样周期

- 可选配置。
- 若无特殊要求，按默认配置即可。
- 采样周期越小，则数据越实时，但也会消耗更多的系统资源。
- 行为报表 URL-TOPN 固定为每天发一次，只能设置统计发送的时间点，不可设置采样周期。

设置 PING 检测的参数

- 必须配置。
- 根据需要设置需要检测哪些服务器。

设置 URL-TOPN 的参数

- 可选配置
- 可以根据需要修改 URL-TOPN 的参数配置，如无特殊要求，使用默认值即可。

设置网页加载耗时监控

- 必须配置。
- 根据需要配置需要监控的 URL，这里的 URL 是精确匹配。通常情况下，我们监控首页的加载耗时即可。

设置视频会议质量监控

- 必须配置。

- 根据需要配置哪些视频会议需要监控。这里有两种指定方式，一种是指定应用名（依赖于应用识别），一种是指定 ACL（通常用于只知道视频服务器 IP 地址的场景）

检验方法

开启所有的 APM 监控功能，配置 APM 日志服务器以及对应的日志类型。

- 检查 RAC 服务器是否有收到对应的报文。
- 通过 show apm server log-count 检查日志发送情况。

相关命令

开启全局 APM 采样监控

【命令格式】 **apm sample enable**

【参数说明】 无

【命令模式】 全局模式

【使用指导】 开启设备状态、VPN 状态、带宽状态、业务数据加载速率、PING 检测、行为报表 URL-TOPN 这几个功能，必须先开启全局采样开关

设置全局 APM 采样周期

【命令格式】 **apm sample default interval** *num*

【参数说明】 *num*：默认采样的周期，单位为秒，取值范围为 10~3600。

【命令模式】 全局模式

【使用指导】 默认采样周期为 5min，无特殊配置的都按此来。可以通过 **no apm sample default interval** 来恢复默认值。

单独设置各 APM 信息的采样周期

【命令格式】 **apm sample** { **cpu-mem** | **sata-flash** | **vpn** | **vpn-detail | ip-session | intf-flowrate | app-type-flowrate | app-flowrate** | **user-flowrate | ping-detect** | **business** } **interval** *second*

【参数说明】 *second*：采样周期，单位为秒，取值范围为 10~3600。

【命令模式】 全局模式

【使用指导】 单独设置各 APM 信息的采样周期，无特殊需求，无需此项配置。可以通过 no 命令来删除单独的特殊配置，恢复使用全局默认的采样周期。

cpu-mem 表示 CPU 和内存使用率；

sata-flash 表示硬盘以及 flash 使用情况；

vpn 表示 VPN 通断情况；

vpn-detail 表示 VPN 线路应用流量明细；

ip-session 表示 IP 和会话数；

intf-flowrate 表示接口流量；

app-type-flowrate 表示应用类型流量；

app-flowrate 表示应用流量；

user-flowrate 表示用户流量；

ping-detect 表示 PING 检测；
business 表示业务数据加载速率。

单独关闭某些 APM 信息采样

【命令格式】 **apm sample** { **cpu-mem** | **sata-flash** | **vpn | vpn-detail | ip-session | intf-flowrate | app-type-flowrate | app-flowrate | user-flowrate | ping-detect | business** } **disable**

【参数说明】 无

【命令模式】 全局模式

【使用指导】 开启全局 APM 采样功能后，如果不需要某些 APM 信息，则可以通过此命令进行关闭。可以通过 no 命令来重新开启（在全局采样功能是开启的情况下）。也可以通过 **apm sample del-all-disable** 来开启所有的 APM 采样（在全局采样功能是开启的情况下）。
cpu-mem 等字段含义同上文，这里不再累述。

设置哪些业务（应用）需要监控数据加载速率

【命令格式】 **apm sample business application** *app-name*

【参数说明】 *app-name*：应用名称，具体参考应用识别

【命令模式】 全局模式

【使用指导】 设置哪些业务（应用）需要监控数据加载速率，通过应用来指定，因此依赖于应用识别模块识别的准确性。目前最多允许配置 50 个监控应用。

设置 PING 检测服务器

【命令格式】 **apm sample ping-detect server** [*ip-address* | *host*] [**ntimes** *times*] [**length** *len*] [**source** { **lan** | *so-ip-address* | *interface-name* }]

【参数说明】 *ip-address*：PING 的 IP 地址
host：PING 的域名
times：每次 PING 的包数，取值范围 1~10
len：PING 包的长度，取值范围 64~1400
so-ip-address：PING 检测包的源 IP
interface-name：接口名

【命令模式】 全局模式

【使用指导】 通常情况下，只需要设置 IP 地址或域名即可，其余的参数不用配置，使用默认值即可。如果 PING 检测的服务器是通过 IPSECVPN 访问的，则需要加上 **source lan** 的参数，这样才能保证会进入 IPSEC 隧道。其他情况可以不用配置 source 参数。

设置需要收集 TOP 几的 URL 站点

【命令格式】 **apm sample url-topn top** *num*

【参数说明】 *num*：收集 url 访问量 top 多少的值，取值范围是 1~100。

【命令模式】 全局模式

【使用指导】 设置发送 top 几的 url 信息

设置行为报表 URL-TOPN 信息的发送时间

【命令格式】 **apm sample url-topn send-time** *hour*

【参数说明】 *hour*：URL-TOPN 发送的时间。取值范围 0~23

【命令模式】 全局模式

【使用指导】 默认时间为凌晨 1 点，通常设置在设备比较空闲的时段。

设置网页加载耗时需要监控的网址

【命令格式】 **apm webpage url** *string*

【参数说明】 string 为需要监控的网址，不含 http://，不能为'all'关键字。最多只能配置 50 条，每条最长 200 字节。

【命令模式】 全局模式

【使用指导】 配置一条需要监控的网址。可以通过 **no apm webpage url** *string* 来删除指定的网址，也可以通过 **no apm webpage url all** 来删除所有的配置。

设置网页加载耗时功能开关

【命令格式】 **apm webpage enable**

【参数说明】 无

【命令模式】 全局模式

【使用指导】 该开关默认是开启的，可以通过 **no apm webpage enable** 在不删除监控网址的情况下暂时关闭该功能。

设置视频会议质量监控的数据流（通过应用名）

【命令格式】 **apm conference-system application** *app-name*

【参数说明】 *app-name*：应用名称，不能为 all。

【命令模式】 全局模式

【使用指导】 配置需要监控的视频会议，通过应用来指定，要删除某一个应用的配置，可以在全局配置模式下执行 no **apm conference-system application** *app-name*， 删除所有应用的配置，在全局配置模式下执行 no **apm conference-system application all**

设置视频会议质量监控的数据流（通过 ACL）

【命令格式】 **apm conference-system access-list** *acl_id* **alias** *alias-name*

【参数说明】 *acl_id*：acl 的 id，取值范围 1~199。

alias-name: 这些数据流的别名

【命令模式】 全局配置模式

【使用指导】 配置需要监控的视频会议，通过 ACL 来指定，要删除某一个 ACL 规则，可以在全局配置模式下执行 no **apm conference-system access-list** *acl_id*，删除所有 ACL 的规则，在全局配置模式下执行 no **apm conference-system access-list all**

配置视频会议质量的监控粒度周期

【命令格式】 **apm conference-system measure-period** *period-time*

【参数说明】 *period-time*: 粒度大小，单位为秒，范围为 30~120

【命令模式】 全局模式

【使用指导】 配置视频会议质量的监控粒度周期，即多长时间作为一个周期进行质量监控评估，默认为 60 秒，要恢复默认配置 ,可以在全局配置模式下执行 no **apm conference-system measure-period。**通常情况下无需配置该项。

开启视频会议监控功能

【命令格式】 **apm conference-system enable**

【参数说明】 无

【命令模式】 全局模式

【使用指导】 该开关默认是开启的，可以通过 **no apm conference-system enable** 在不删除监控指定应用与 ACL 的情况下暂时关闭该功能。

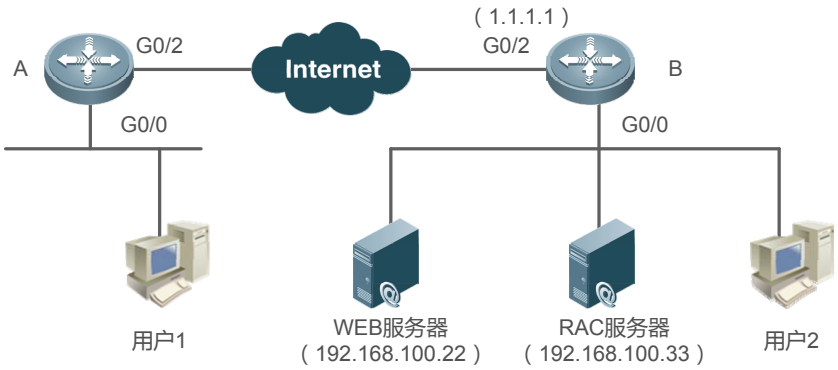
配置举例

以下配置举例，仅介绍与 CM-APM 相关的配置。

开启整网的 APM 性能监控，需要监控的视频会议有“红杉树会议系统”，需要监控的网页有 www.ietf.org，需要 PING 检测的服务器为 192.168.100.22（分支机构通过 IPSEC VPN 进行访问）

【网络环境】

图 5-2



【配置方法】

- 在网关 B 上将 RAC 相关信息映射到公网 IP 上。
- 网关 A 和 B 上设置 APM 日志服务器相关信息。
- 网关 A 和 B 上设置所有消息都发往指定的服务器。
- 网关 A 和 B 上开启全局采样监控功能。
- 网关 A 和 B 上开启 PING 检测，地址为 192.168.100.22
- 网关 A 和 B 上设置需要监控的视频会议为“红杉树会议系统”。
- 网关 A 和 B 上设置需要监控网页加载耗时的网址为 www.ietf.org

A

```
A# configure terminal
A(config)# apm sample enable
A(config)# apm sample default interval 300
A(config)# apm sample ping-detect server 192.168.100.22 ntimes 5 length 100 source lan
A(config)# apm webpage url www.ietf.org/
A(config)# apm conference-system application 红杉树会议系统
A(config)# apm server rac 1.1.1.1 30000 tcp
A(config)# apm log-type default priority 1 server rac
```

B

```
B# configure terminal
B(config)# ip nat inside source static tcp 192.168.100.33 30000 interface gigabitEthernet 0/2 30000
permit-inside
B(config)# apm sample enable
B(config)# apm sample default interval 300
B(config)# apm sample ping-detect server 192.168.100.22 ntimes 5 length 100
B(config)# apm webpage url www.ietf.org/
B(config)# apm conference-system application 红杉树会议系统
B(config)# apm server rac 192.168.100.33 30000 tcp
B(config)# apm log-type default priority 1 server rac
```

【检验方法】

- 用户 1 与用户 2 使用红杉树会议系统进行视频会议，RAC 服务器上有收到网关 A 和 B 的监控信息。
- 用户 1 访问 www.ietf.org，RAC 服务器有收到网关 A 的监控信息。
- RAC 服务器定期都会收到网关 A 和 B 的 PING 检测的监控信息。
- RAC 服务器定期都会收到网关 A 和 B 的其他 APM 监控信息。

A

```
A# show apm server log-count
```

B

```
B# show apm server log-count
```

常见错误

- 视频会议质量监控配置的应用名，设备不能识别 或 应用名为 all。
- 配置的网址包含了 http:// 协议头，导致不能正确识别。
- 配置的网址不是指定网页且不以”/”结尾，如”www.itef.org/”写成 www.ietf.org
- PING 检测的服务器不需要经过 IPSEC 隧道，但是却配置了 source lan 的参数。

5.6 监视与维护

清除各类信息

作用	命令
清除 APM 日志发送统计	**clear apm server log-count**

查看运行情况

作用	命令
查看 APM 日志服务器的设置	**show apm server info**
查看 APM 日志发送情况	**show apm server log-count**
查看各类采样业务的周期	**show apm sample log-sends**
查看用户配置的 PING 或 URL-TOPN 信息	**show apm sample ping-detect info**

查看用户配置的 URL-TOPN 信息	**show apm sample url-topn info**
查看配置了哪些业务(应用)需要监控数据加载速率	**show apm sample business info**
查看当前需要监控的网址	**show apm webpage url**
查看当前网页加载耗时监控情况	**show apm webpage statistics**
查看当前视频会议监控的 UDP 流情况	**show apm udp-measure info**
查看当前视频会议监控的 TCP 流情况	**show apm tcp-measure info**

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
打开网页加载耗时的调试开关	**debug apm webpage info**

6 ANTI-SNIPER

6.1 概述

网络尖兵可以自动检测出网络中私自架设的代理服务器系统或非法路由器，并对通过非法代理服务器的 IP 包以及流向非法路由器的 IP 包进行控制。通过这种控制，避免用户恶意偷逃上网费用的情况发生，目前中国电信、网通等运营商用它来限制用户共享上网。防网络尖兵就是为了防止共享上网的行为被运营商识别出来。

协议规范

无

6.2 典型应用

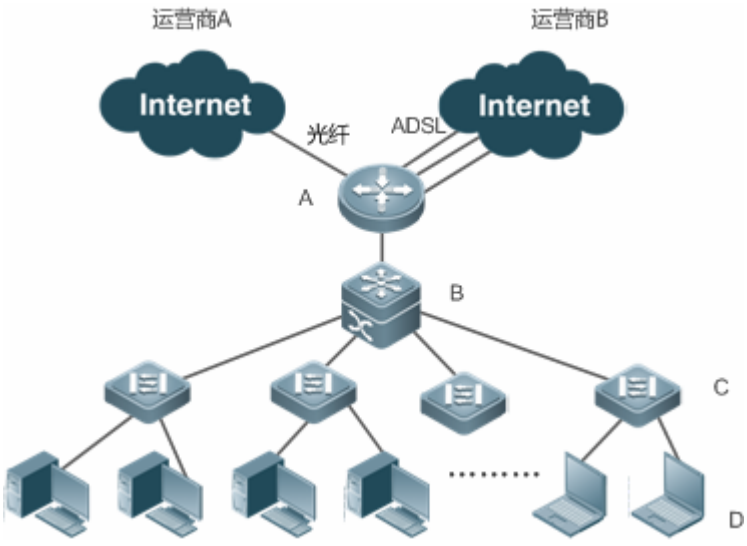
典型应用	场景描述
出口网关部署	出口网关设备部署防网络尖兵

6.2.1 出口网关部署

应用场景

防网络尖兵一般布署在拨号口，以下罗列网吧用户的典型拓扑。

图 6-1 出口网吧用户典型的应用场景



【注释】 A 为出口网关设备
B 为核心交换机。
C 为接入交换机。
D 为内网用户 PC。

功能部属

- 基本 NAT 上网功能：完成基本的 NAT 地址转换，保障用户正常上网。
- 应用识别功能：完成转发流量的应用识别。
- 应用路由功能（包括应用代理功能）：以应用识别为基础，实现大流量应用或者重点应用的流量能够走指定的出口。
- 流量控制功能：和应用识别结合，实现对重点应用流量的保障等功能。
- 二三层识别功能：完成转发流量的用户、用户组识别。
- 多链路负载均衡功能：完成数据流在多条链路的合理分配，确保多条链路的带宽利用合理。
- 流量审计功能：流量审计即是对流经网关设备的各种流量进行统计，有基于用户的流量统计，也有基于应用的流量统计等等，从而使得网络的流量可视化。
- 防网络尖兵： 能够防止运营商的网络尖兵识别出共享网络上网

6.3 功能详解

基本概念

无

功能特性

功能特性	作用
防网络尖兵	开启防网络尖兵

6.3.1 防网络尖兵

防网络尖兵就是防止运营商的网络尖兵识别出共享网络上网，从而被限制上网

工作原理

防网络尖兵基本原理是通过修改报文里的字段值，包括 TTL，IPID，TCP 端口，window size，时间戳等，伪装成是同一用户的行为，同时会拆分 HTTP 报文，使其增加运营商网络尖兵的审查难度，以达到防止被检测出共享上网。

6.4 产品说明



NBR108G-P 不支持启用防封杀功能 ;NBR800G、NBR950G、NBR1500G、NBR2000G、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持启用防封杀功能。

6.5 配置详解

配置项	配置建议 & 相关命令	
开启防网络尖兵功能	⚠ 必须配置。打开流量审计功能。	
	anti-sniper interface *intf-name*	开启流量监控审计。
配置 IP 报文的 TTL 值	⚠ 可选配置。配置修改 IP 报文的 TTL。	
	ip-ttl off	关闭修改 IP 报文 TTL 值的功能
	ip-ttl *num*	配置修改 TLL 的值。
配置 IP 报文的 IPID 修改方式	⚠ 可选配置。配置修改 IP 报文的 IPID。	
	ip-id off	关闭修改 IP 报文 ipid 值的功能
	ip-id random	设置 ipid 的值为随机
配置修改 tcp 端口的功能	⚠ 可选配置。配置修改 TCP 的端口。	
	tcp-port	打开或关闭修改 tcp 端口的功能
	tcp-port continuous	设置修改 tcp 端口的方式，递增方式
	tcp-port range *min-port max-port*	设置可用的 tcp 端口范围
配置修改 tcp 窗口大小的功能	⚠ 可选配置。配置修改 tcp 端口大小的功能。	
	tcp-win-size off	关闭修改 tcp 窗口大小的功能
	tcp-win-size *value*	设置 tcp 窗口的大小
配置抹掉时间戳选项的功能	⚠ 可选配置。配置打开去掉报文中时间戳选项的功能。	
	tcp-timestamp off	关闭抹掉时间戳选项的功能
配置拆分 HTTP 报文的功能	⚠ 可选配置。配置拆分 HTTP 报文的功能。	
	http-modify off	关闭拆分 HTTP 报文的功能
	http-modify mode *value*	设置拆分 HTTP 报文的方式

6.5.1 开启防网络尖兵

配置效果

- 打开防网络尖兵功能，能够防止共享上网的行为被运营商识别出来。

注意事项

- 防网络尖兵功能关闭的情况下，功能失效。

配置方法

↘ 开启某个接口的防网络尖兵

- 缺省情况下，防网络尖兵的功能是关闭。
- 在全局配置模式中，使用 **anti-sniper interface** *intf-name* 命令在某个接口上开启防网络尖兵功能。
- 在全局配置模式中，使用 **no anti-sniper interface***intf-name* 命令可以在某个接口上关闭防网络尖兵功能。

【命令格式】 **anti-sniper interface**
【参数说明】 -
【命令模式】 全局模式
【使用指导】 -

检验方法

- 检查防网络尖兵的配置信息。

配置举例

↘ 开启防网络尖兵

【配置方法】 在出口网关设备上的 GI0/5 口上开启防网络尖兵。

```
Ruijie# configure terminal
Ruijie(config)# anti-sniper interface gigabitEthernet 0/5
```

【检验方法】
- 查看防网络尖兵的状态。

```
Ruijie#show anti-sniper policy
[GigabitEthernet 0/5]
```

常见错误

无

6.5.2 配置IP报文的TTL值

配置效果

- 配置修改 IP 报文 TTL 值的功能，设置 TTL 的值

注意事项

- 默认功能是打开，TTL 的默认值为 128，取值范围为 1~255

配置方法

↘ 打开修改 TTL 值的功能

- 可选配置。
- 缺省情况下，修改 IP 报文的 TTL 值功能是打开，默认值为 128
- 在防网络尖兵模式下，使用 **ip-ttl off** 关闭修改 IP 报文的 TTL 值功能。使用 **no ip-ttl off** 打开修改 IP 报文的 TTL 值功能。

【命令格式】 **no ip-tll off**
【参数说明】 -
【命令模式】 防网络尖兵模式
【使用指导】 关闭此功能 ip-tll off

↘ 修改 TTL 值

- 在防网络尖兵模式下，使用 **ip-ttl value** *num* 来修改 IP 报文的 TTL 值，取值范围为 1~255.
- 使用 **no ip-ttl value** 来恢复 IP 报文的 TTL 值

【命令格式】 **ip-ttl value** *num*
【参数说明】 *num*：设置 TTL 的值，取值范围为 1~255。
【命令模式】 防网络尖兵模式
【使用指导】 如果 ip-tll 的开关为 OFF，则此配置无效。

检验方法

- 检查功能开关状态及 TTL 值

配置举例

↘ 打开修改 IP 报文的 TTL 值功能，且 TTL 值为 129

【配置方法】 在出口网关设备上配置。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# anti-sniper interface gigabitEthernet 0/5
Ruijie(config-anti-sniper)#no ip-tll off
Ruijie(config-anti-sniper)#ip-ttl value 129
```

【检验方法】

- 查看配置的信息。

```
Ruijie(config)#show anti-sniper policy
[GigabitEthernet 0/5]
ip-ttl                  : ON
ip-ttl value            : 129
```

常见错误

无

6.5.3 配置IP报文的IPID修改方式

配置效果

- 配置修订 IP 报文的 IPID 值的方式

注意事项

-

配置方法

↘ 打开修订 IPID 的功能

- 缺省情况下，修改 IP 报文的 ipid 值功能是打开，ipid 的值为递增的方式。
- 在防网络尖兵模式下，使用 **ip-id off** 来关闭修改 ipid 的功能，使用 **no ip-id off** 打开此功能。

【命令格式】 **no ip-id off**
【参数说明】 -
【命令模式】 防网络尖兵模式
【使用指导】 -

↘ 设置 IPID 值为随机的

- 在防网络尖兵模式下， 使用 ip-id random 改变 ipid 的值为随机方式，使用 no ip-id random 恢复递增方式。

【命令格式】 **ip-id random**
【参数说明】 -
【命令模式】 防网络尖兵模式
【使用指导】 -

检验方法

- 检查功能开关状态及方式

配置举例

↘ 打开修订 IPID 的功能，并设置 IPID 的值为递增

【配置方法】 在出口网关设备上配置。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# anti-sniper interface gigabitEthernet 0/5
Ruijie(config-anti-sniper)#no ip-id off
Ruijie(config-anti-sniper)# no ip-id random
```

【检验方法】
- 查看配置信息。

```
Ruijie(config)#show anti-sniper policy
[GigabitEthernet 0/5]
ip-ttl                  : ON
ip-ttl value            : 129
ip-id                   : ON
ip-id random            : FALSE
```

常见错误

无

6.5.4 配置修改tcp端口的功能

配置效果

- 配置修改 tcp 端口的功能，指定端口的范围及修改方式

注意事项

-

配置方法

打开修改 tcp 端口功能

- 缺省情况下，修改 tcp 端口功能是关闭的，端口的值默认为奇偶交替，端口范围默认为 1054-9000。
- 在防网络尖兵模式下，使用 **tcp-port off** 来关闭修改 tcp 端口的功能，用 **no tcp-port off** 打开此功能。

【命令格式】 **no tcp-port off**
【参数说明】 -
【命令模式】 防网络尖兵模式
【使用指导】 -

设定 tcp 端口值为连续的

- 在防网络尖兵模式下，使用 no tcp-port continuous 采取端口连续递增的方式， 用 tcp-port continuous 恢复默认配置。

【命令格式】 **tcp-port continuous**
【参数说明】 -
【命令模式】 防网络尖兵模式
【使用指导】 使用 no tcp-port continuous 采取端口连续递增的方式

设定 tcp 端口值的范围

- 在防网络尖兵模式下，使用 **tcp-port range** *port1 port2* 配置端口的范围，用 **no tcp-port range** 恢复默认配置。

【命令格式】 **tcp-port range** *min-port max-port*
【参数说明】 *min-port*：端口范围的最小值，范围为 1-65535，默认值为 1054
max-port：端口范围的最大值，范围为 1-65535，默认值为 9000
【命令模式】 防网络尖兵模式
【使用指导】 -

检验方法

- 检查配置信息

配置举例

打开修改 TCP 端口功能，端口值为连续，范围为 2000~8000

【配置方法】 在出口网关设备上配置。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# anti-sniper interface gigabitEthernet 0/5
Ruijie(config-anti-sniper)#no tcp-port off
Ruijie(config-anti-sniper)#tcp-port continuous
Ruijie(config-anti-sniper)# tcp-port range 2000 8000
```

【检验方法】

- 查看配置。

```
Ruijie(config-anti-sniper)#show anti-sniper policy
[GigabitEthernet 0/5]
ip-ttl                  : ON
ip-ttl value            : 128
ip-id                   : ON
ip-id random            : TRUE
tcp-port                : ON
tcp-port continuous     : TRUE
tcp-port range          : 2000-8000
```

常见错误

无

6.5.5 配置修改tcp窗口大小的功能

配置效果

- 配置修改 TCP 窗口大小的功能，并设定窗口值的大小

注意事项

- 缺省情况下，此功能是打开，窗口大小为 65535

配置方法

↘ 打开修改窗口大小功能

- 缺省情况下，修改 TCP 窗口大小的功能是打开的，默认窗口值为 65535。
- 在防网络尖兵模式下，使用 **tcp-win-size off** 关闭此功能，用 **no tcp-win-size off** 打开此功能

【命令格式】 **no tcp-win-size off**

【参数说明】 -

【命令模式】 防网络尖兵模式

【使用指导】 -

↘ 设定窗口大小的值

- 在防网络尖兵模式下，使用 **tcp-win-size value** *num* 来配置窗口的值，范围为 1~65535， 用 **no tcp-win-size value** 恢复配置。

【命令格式】 **tcp-win-size value** *num*

【参数说明】 *num*：窗口值的大小，范围为 1~65535，默认值为 65535

【命令模式】 防网络尖兵模式

【使用指导】 -

检验方法

- 检查配置信息

配置举例

↘ 打开修改窗口大小功能，并设定其值为 65535

【配置方法】 在出口网关设备上配置。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# anti-sniper interface gigabitEthernet 0/5
Ruijie(config-anti-sniper)#no tcp-win-size off
Ruijie(config-anti-sniper)# tcp-win-size value 65535
```

【检验方法】

- 查看配置。

```
Ruijie(config-anti-sniper)#show anti-sniper policy
[GigabitEthernet 0/5]
ip-ttl                  : ON
ip-ttl value            : 128
ip-id                   : ON
ip-id random            : TRUE
tcp-port                : ON
tcp-port continuous     : TRUE
tcp-port range          : 2000-8000
tcp-win-size            : ON
tcp-win-size value      : 65535
```

常见错误

无

6.5.6 配置抹掉时间戳选项的功能

配置效果

- 配置去掉报文中时间戳选项的功能

注意事项

- 缺省情况下，此功能是打开

配置方法

↘ 打开此功能

- 缺省情况下，抹掉报文中带时间戳选项的功能
- 在反网络尖兵模式下，使用 **tcp-timestamp off** 来关掉此功能，用 **no tcp-timestamp off** 来恢复功能。

【命令格式】 **no tcp-timestamp off**
【参数说明】 -
【命令模式】 防网络尖兵模式
【使用指导】 -

检验方法

- 检查配置信息。

配置举例

↘ 打开去掉报文中时间戳选项的功能

【配置方法】 在出口网关设备上配置。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# anti-sniper interface gigabitEthernet 0/5
Ruijie(config-anti-sniper)#no tcp-timestamp off
```

【检验方法】
- 查看配置。

```
Ruijie(config-anti-sniper)#show anti-sniper policy
[GigabitEthernet 0/5]
ip-ttl                  : ON
ip-ttl value            : 128
ip-id                   : ON
ip-id random            : TRUE
tcp-port                : ON
tcp-port continuous     : TRUE
tcp-port range          : 2000-8000
tcp-win-size            : ON
tcp-win-size value      : 65535
tcp-timestamp           : ON
```

常见错误

无

6.5.7 配置拆分HTTP报文的功能

配置效果

- 配置拆分 HTTP 报文的功能，设置其拆分的方式

注意事项

- 默认功能是打开，拆分方式默认为 1

配置方法

↘ 打开拆分 HTTP 报文功能

- 可选配置。
- 缺省情况下，拆分 HTTP 报文的功能是打开，默认采用模式 1 方式拆分。
- 在防网络尖兵模式下，使用 **http-modify off** 来关闭此功能，使用 **no http-modify off** 打开此功能。

【命令格式】 **no http-modify off**
【参数说明】 -
【命令模式】 防网络尖兵模式
【使用指导】 -

↘ 设定拆分 HTTP 报文的方式

- 在防网络尖兵模式下，使用 **http-modify mode** *num* 来改变拆分模式，使用 **no http-modify mode** 恢复默认配置。

【命令格式】 **http-modify mode** *num*

【参数说明】 *num*：设定 HTTP 报文拆分方式，取值范围为 1~4，默认为 1

【命令模式】 防网络尖兵模式

【使用指导】 如果 http-modify 的开关为 OFF，此配置无效

检验方法

- 检查配置信息。

配置举例

↘ 打开 HTTP 报文拆分功能，且拆分方式为 1

【配置方法】 在出口网关设备上配置。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# anti-sniper interface gigabitEthernet 0/5
Ruijie(config-anti-sniper)#no http-modify off
Ruijie(config-anti-sniper)# http-modify mode 1
```

【检验方法】

- 查看配置的信息。

```
Ruijie(config-anti-sniper)#show anti-sniper policy
[GigabitEthernet 0/5]
ip-ttl                  : ON
ip-ttl value            : 128
ip-id                   : ON
ip-id random            : TRUE
tcp-port                : ON
tcp-port continuous     : TRUE
tcp-port range          : 2000-8000
tcp-win-size            : ON
tcp-win-size value      : 65535
tcp-timestamp           : ON
http-modify             : ON
http-modify mode        : 1
```

常见错误

无

6.6 监视与维护

清除各类信息

无

查看运行情况

作用	命令
查看当前的配置信息	**show anti-sniper policy**

查看调试信息

输出调试信息。

作用	命令
查看内核配置是否同步	**show anti-sniper ef-policy**
查看内核运行情况	**show anti-sniper stat**

7 IPMAC-SNIFF

7.1 概述

IPMAC-SNIFF 是用于嗅探 ip 对应的 mac，并进行绑定，通告给有需要的模块。

主要功能是将终端 ip 地址及 mac 地址进行绑定，通告给相应的模块。ip 地址区分 v4 和 v6

协议规范

无

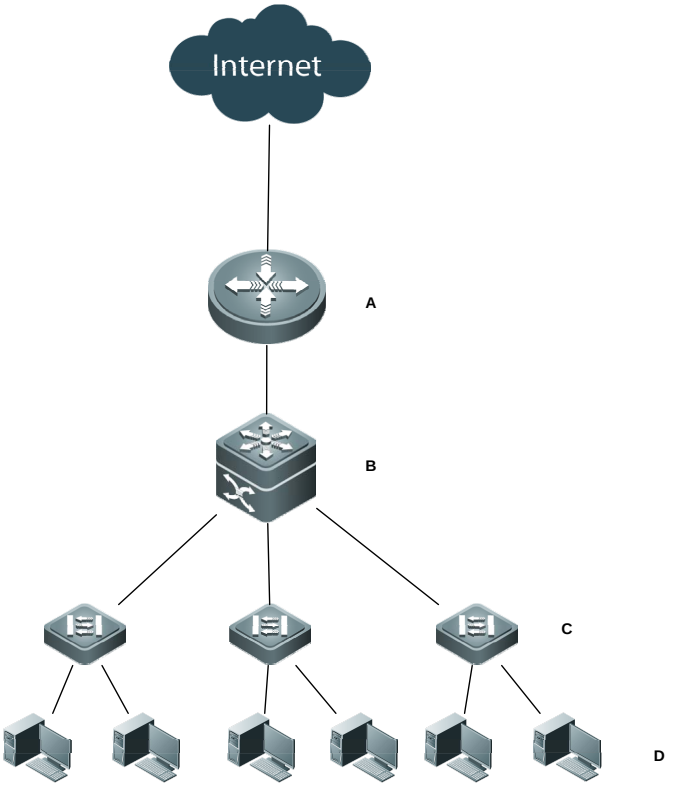
7.2 典型应用

典型应用	场景描述
出口网关部署	出口网关设备部署 ipmac 嗅探功能

7.2.1 出口网关部署

应用场景

通过报文，提取 ip 及 mac 的绑定信息，吐给相关模块。



【注释】

A 为出口网关设备

B 为核心交换机。

C 为接入交换机。

D 为内网用户 PC。

功能部属

- 在网关上开启 ipmac 的嗅探功能

7.3 功能详解

基本概念

↘ Ipmac 嗅探

根据报文信息，将 ip 报文提取 ip 地址和 mac 进行绑定，IP 区分 v4 和 v6。

功能特性

功能特性	作用

Ipmac 嗅探	获取 ip 对应的 mac 地址，并绑定二者关系

7.3.1 Ipmac嗅探

获取 ip 对应的 mac 地址，并绑定二者关系

工作原理

快转层面直接处理所有报文，将 ip 地址及 mac 进行绑定，并通告给相关模块。
作为转发面的一个业务，目前嗅探需要做的事很简单，只需要提取 MAC+IP 数据即可，基本处理步骤如下：
1） 收到报文
2） 获取源 MAC
3） 获取源 IP 地址
4） 生成 MAC+IP 节点

7.4 产品说明



NBR1500G、NBR2000G、NBR108G-P 、NBR800G、NBR950G、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR1000G-C、NBR2000G-C、NBR3000G-S 不支持 IPMAC 嗅探； NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 IPMAC 嗅探。

7.5 配置详解

配置项	配置建议 & 相关命令	
开启 ipmac 嗅探功能	⚠ 必须配置。用于建立组播服务。	
	ipmac-sniff enable	启动嗅探功能总开关
	ipmac-sniff ipv6 enable	开启 ipv6-mac 嗅探
	ipmac-sniff ipv4 enable	开启 ipv4-mac 嗅探
设置 ipmac 老化参数	**ipmac-sniff flow-detect**	设置 ipmac 节点老化参数

7.5.1 开启ipmac嗅探功能

配置效果

生成 ip+mac 节点，并通告相关模块

注意事项

开启 ip+mac 嗅探功能要先开启嗅探功能的总开关

配置方法

开启嗅探功能总开关

【命令格式】 **ipmac-sniff enable**
【参数说明】 -
【缺省配置】 关闭
【命令模式】 全局模式
【使用指导】 该命令用于开启 ipmac 嗅探功能总开关

开启 ipv6-mac 嗅探功能

【命令格式】 **ipmac-sniff ipv6 enable**
【参数说明】 -
【缺省配置】 开启
【命令模式】 全局模式
【使用指导】 该命令用于开启 ipv6-mac 嗅探功能开关

开启 ipv4-mac 嗅探功能

【命令格式】 **ipmac-sniff ipv4 enable**
【参数说明】 -
【缺省配置】 开启
【命令模式】 全局模式
【使用指导】 该命令用于开启 ipv4-mac 嗅探功能开关

检验方法

开启功能后，可以查看到 ip 及 mac 的绑定信息

【命令格式】 show ipmac-sniff { ipv6 | ipv4 }
【参数说明】 -
【命令模式】 特权模式、全局模式
【使用指导】 用来查看嗅探功能是否开启，及开启功能后，ipv6、ipv4 及 mac 的表项信息
【命令展示】

```
Ruijie# show ipmac-sniff ipv6

ipv6-mac-cnt: 2

ipv6                                            mac               update-time
```

```
================================================================================
2001:0000:3238:DFE1:0063:0000:0000:FEFB     AABB.CCDD.EEF0     2018-11-20 18:00:00
2002:0000:3238:DFE1:0063:0000:0000:FEFB     AABB.CCDD.EEF1     2018-11-20 18:00:01
```

关于 show 信息的详细解释请参看对应功能的命令手册。

配置举例

1：缺省配置

```
Ruijie# show ipmac-sniff stat
ipmac-sniff           : unable
ipv4-mac              : enable
ipv6-mac              : enable
flow-detect flow(bps) : 0
flow-detect time(min) : 15
```

2：开启嗅探功能总开关

```
Ruijie(config)# ipmac-sniff enable
```

3：开启 ipv6 嗅探功能

```
Ruijie(config)# ipmac-sniff ipv6 enable
Ruijie# show ipmac-sniff ipv6
ipv6-mac-cnt: 2
ipv6                                        mac               update-time
================================================================================
2001:0000:3238:DFE1:0063:0000:0000:FEFB           AABB.CCDD.EEF0     2018-11-20 18:00:00
2002:0000:3238:DFE1:0063:0000:0000:FEFB           AABB.CCDD.EEF1     2018-11-20 18:00:01
```

4：开启 ipv4 嗅探功能

```
Ruijie(config)# ipmac-sniff ipv4 enable
Ruijie# show ipmac-sniff ipv4
ipv4-mac-cnt: 2
ipv4                mac               update-time
=======================================================
192.168.1.2         AABB.CCDD.EEF0     2018-11-20 18:00:00
192.168.1.3         AABB.CCDD.EEF1     2018-11-20 18:00:01
```

常见错误

总开关未开启

7.5.2 设置ipmac老化参数

配置效果

设置 ip+mac 节点老化参数

注意事项

无

配置方法

↘ 设置 ipmac 节点老化时间

【命令格式】 **ipmac-sniff flow-detect time-interval** *time-val*
【参数说明】 -
【缺省配置】 15
【命令模式】 全局模式
【使用指导】 该命令用于设置 ipmac 节点老化时间

↘ 设置 ipmac 节点老化流量阀值

【命令格式】 **ipmac-sniff flow-detect flowrate** *flow-val*
【参数说明】 -
【缺省配置】 0
【命令模式】 全局模式
【使用指导】 该命令用于设置 ipmac 节点老化的流量阀值

检验方法

开启功能后，可以查看到 ip 及 mac 的绑定信息

【命令格式】 show ipmac-sniff stat
【参数说明】 -
【命令模式】 特权模式、全局模式
【使用指导】 用来查看嗅探功能的基本配置信息
【命令展示】

```
Ruijie# show ipmac-sniff stat
```

```
ipmac-sniff:enable

Ipv6-mac:enable

ipv4-mac:enable

flow-detect flow:0 byte

flow-detect time:15 min
```

关于 show 信息的详细解释请参看对应功能的命令手册。

配置举例

1：配置 ipmac 节点老化流量阀值为 1K，老化时间为 20 分钟

```
Ruijie(config)# ipmac-sniff flow-detect flowrate 1024

Ruijie(config)# ipmac-sniff flow-detect time-interval 20
```

常见错误

无

7.6 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 ipmac 表项	clear ipmac-sniff all

查看运行情况

作用	命令
查看 ipmac 表项	show ipmac-sniff { ipv6 | ipv4 }
查看嗅探功能配置信息	show ipmac-sniff stat

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
-	-

配置指南-IPV6

本分册介绍 IPV6 相关内容，包括以下章节：

1. IPV6

1 IPv6

1.1 概述

随着Internet的迅速增长以及IPv4地址空间的逐渐耗尽，IPv4的局限性就越来越明显。对新一代互联网络协议(Internet Protocol Next Generation - IPng ）的研究和实践已经成为热点，Internet 工程任务工作小组(IETF)的 IPng 工作组确定了 IPng 的协议规范，并称之为"IP 版本 6"（ IPv6 ），该协议的规范在 RFC2460 中有详细的描述。

IPv6 的主要特点

更大的地址空间

地址长度由 IPv4 的 32 位扩展到 128 位，约有 2^128 个地址，IPv6 采用分级地址模式，支持从 Internet 核心主干网到企业内部子网等多级子网地址分配方式。

简化了报头格式

新 IPv6 报文头的设计原则是力图将报文头开销降到最低，因此将一些非关键性字段和可选字段从报文头中移出，放到扩展的报文头中，虽然 IPv6 地址长度是 IPv4 的四倍，但报头仅为基本 IPv4 首部的两倍。改进的 IPv6 报文头在设备转发时拥有更高的效率，例如 IPv6 报文头中没有校验和，IPv6 设备在转发中不需要去处理分片(分片由发起者完成)。

高效的层次寻址及路由结构

IPv6 采用聚合机制，定义非常灵活的层次寻址及路由结构，同一层次上的多个网络在上层设备中表示为一个统一的网络前缀，这样可以显著减少设备必须维护的路由表项，这也大大降低了设备的选路和存储开销。

简单的管理：即插即用

通过实现一系列的自动发现和自动配置功能，简化网络节点的管理和维护。比如邻接节点发现（ Neighbor Discovery ）、最大传输单元发现（ MTU Discovery ）、路由器通告（ Router Advertisement ）、路由器请求（ Router Solicitation ）、节点自动配置（ Auto-configuration ）等技术就为即插即用提供了相关的服务。特别要提到的是 IPv6 支持全状态和无状态两种地址配置方式，在 IPv4 中，动态主机配置协议 DHCP 实现了主机 IP 地址及其相关配置的自动设置，IPv6 承继 IPv4 的这种自动配置服务，并将其称为全状态自动配置(Stateful Autoconfiguration)（参见 DHCPv6 ）。除了全状态自动配置，IPv6 还采用了一种被称为无状态自动配置（ Stateless Autoconfiguration ）的自动配置服务。在无状态自动配置过程中，主机自动获得链路本地地址、本地设备的地址前缀以及其它一些相关的配置信息。

安全性

IPSec 是 IPv4 的一个可选扩展协议，但是在 IPv6 中它是 IPv6 的一个组成部分，用于提供 IPv6 的安全性。目前，IPv6 实现了认证头（ Authentication Header，AH ）和封装安全载荷（ Encapsulated Security Payload，ESP ）两种机制。前者实现数据的完整性及对 IP 包来源的认证，保证分组确实来自源地址所标记的节点；后者提供数据加密功能，实现端到端的加密。

更好的 QoS 支持

IPv6 包头的新字段定义了数据流如何识别和处理。IPv6 包头中的流标识（Flow Label）字段用于识别数据流身份，利用该字段，IPv6 允许用户对通信质量提出要求。设备可以根据该字段标识出同属于某一特定数据流的所有包，并按需对这些包提供特定的处理。

↘ 用于邻居节点交互的新协议

IPv6 的邻居发现协议（Neighbor Discovery Protocol）使用一系列 IPv6 控制信息报文（ICMPv6）来实现相邻节点（同一链路上的节点）的交互管理。邻居发现协议以及高效的组播和单播邻居发现报文替代了以往基于广播的地址解析协议 ARP、ICMPv4 路由器发现等报文。

↘ 可扩展性

IPv6 特性具有很强的可扩展性，新特性可以添加在 IPv6 包头之后的扩展包头中。不像 IPv4，包头最多只能支持 40 字节的可选项，IPv6 扩展包头的大小仅受到整个 IPv6 包最大字节数的限制。

协议规范

- RFC4291 - IPVersion6AddressingArchitecture.
- RFC2460 - Internet Protocol, Version 6 (IPv6) Specification
- RFC4443 - Internet Control Message Protocol (ICMPv6)for the Internet Protocol Version 6 (IPv6) Specification
- RFC4861 - Neighbor Discovery for IP version 6 (IPv6)
- RFC4862 - IPv6 Stateless Address Autoconfiguration
- RFC5059 - Deprecation of Type 0 Routing Headers in IPv6

1.2 典型应用

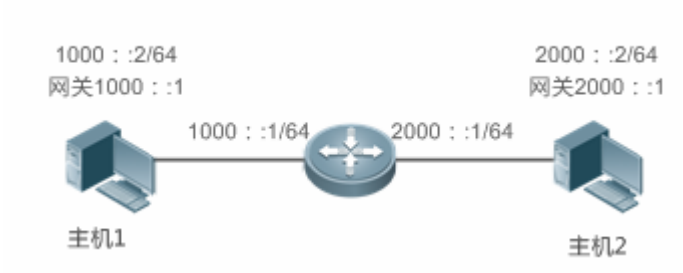
典型应用	场景描述
IPv6 地址通讯	两台 PC 使用 IPv6 地址进行通信

1.2.1 IPv6 地址通讯

应用场景

如下图所示，主机 1 和主机 2 可以通过 IPv6 地址进行通信。

图 1-1



功能部属

主机可以使用无状态地址自动配置也可以使用 DHCPv6 分配地址，配置完地址后，即可以使用 IPv6 地址进行通讯。

1.3 功能详解

功能特性

功能特性	作用
IPv6 地址格式	IPv6 的地址格式使其具有更大的地址空间，及灵活的表示方法。
IPv6 地址类型	IPv6 通过地址标识来区分其网络应用。
IPv6 包头结构	IPv6 通过简化固定报头、扩展选项报头，提高了设备处理数据包的速度，也提高了其转发性能。
IPv6 路径 MTU 发现	主机动态的发现并调整发送数据路径上的 MTU 的大小，节省了路由器的资源，提高了 IPv6 网络的效率。
IPv6 邻居发现	完成路由器发现、前缀发现、参数发现、地址自动配置、地址解析（相当于 ARP）、确定下一跳、邻居不可达检测、地址冲突检测和重定向。
IPv6 源路由	用来指定报文经过哪些中间节点到达目的地址，类似于 IPv4 的宽松源路由选项和宽松记录路。
IPv6 防 ND 拒绝服务攻击	防止无效 IPv6 邻居发现表项占满设备 IPv6 邻居发现表，而导致无法进行正常的邻居发现。
控制 ICMPv6 差错报文的发送速率	防止拒绝服务攻击。
IPv6 HOP-LIMIT	防止无用的单播报文在网络上无限传播下去，浪费网络带宽
抑制往认证 vlan 发送广播 NS 报文	网关认证模式下，设备抑制往认证 VLAN 发送广播 NS 请求的功能
MGMT 口支持缺省网关	给 MGMT 口配置缺省网关，为 MGMT 口生成一条默认路由

1.3.1 IPv6 地址格式

IPv6 地址格式 IPv6 地址的基本表达方式是 X：X：X：X：X：X：X：X，其中 X 是一个 4 位十六进制整数(16 位)。每一个数字包含 4 个比特，每个整数包含 4 个十六进制数字，每个地址包括 8 个整数，一共 128 位。下面是一些合法的 IPv6 地址：

2001:ABCD:1234:5678:AAAA:BBBB:1200:2100

800 : 0 : 0 :0 : 0 : 0 : 0 : 1

1080 : 0 : 0 : 0 : 8 : 800 : 200C : 417A

这些整数是十六进制整数，其中 A 到 F 表示的是 10 到 15。地址中的每个整数都必须表示出来，但起始的 0 可以不必表示。某些 IPv6 地址中可能包含一长串的 0 (就像上面的第二和第三个例子一样)。当出现这种情况时，允许用“ : :”来表示这一长串的 0。即地址 800 : 0 : 0 : 0 : 0 : 0 : 0 : 1 可以被表示为：800 :: 1

这两个冒号表示该地址可以扩展到一个完整的 128 位地址。在这种方法中，只有当 16 位组全部为 0 时才会被两个冒号取代，且两个冒号在地址中只能出现一次。

在 IPv4 和 IPv6 的混合环境中还有一种混合的表示方法。IPv6 地址中的最低 32 位可以用于表示 IPv4 地址，该地址可以按照一种混合方式表达，即 X : X : X : X : X : X : d . d . d . d，其中 X 表示一个 1 6 位整数，而 d 表示一个 8 位的十进制整数。例如，地址 0 : 0 : 0 : 0 : 0 : 0 : 192 .168 . 20 .1 就是一个合法的 IPv6 地址。使用简写的表达方式后，该地址也可以表示为 :: : 192 .168 . 20 . 1。典型代表是 IPv4 兼容 IPv6 地址和 IPv4 映射 IPv6 地址，IPv4 兼容 IPv6 地址前 96 比特是 0，表示法为“**::**A.B.C.D”，例如“**::**1.1.1.1”，目前 IPv4 兼容地址已被废除；IPv4 映射 IPv6 地址表示法为“**::**FFFF:A.B.C.D”，用于把 IPv4 地址表示为 IPv6 地址，如把 IPv4 地址“1.1.1.1”映射到 IPv6 地址“**::**FFFF:1.1.1.1”。

由于 IPv6 地址被分成两个部分：子网前缀和接口标识符，因此可以按照类似 CIDR 地址的方式被表示为一个带额外数值的地址，其中该数值指出了地址中有多少位是代表网络部分(网络前缀)，即 IPv6 节点地址中指出了前缀长度，该长度与 IPv6 地址间以斜杠区分，例如：12AB::CD30:0:0:0:0/60，这个地址中用于选路的前缀长度为 60 位。

相关配置

配置 IPv6 地址

- 缺省情况接口没有配置 IPv6 地址。
- 可通过 **ipv6 address** 命令配置接口 IPv6 地址。
- 配置后根据冲突检测即可使用该 IPv6 地址进行通信。
- 可通过 **ipv6 unnumbered** 命令配置接口借用其他接口的 IPv6 单播地址。该借用地址可用于本地发包报文的源地址。

1.3.2 IPv6 地址类型

RFC4291 定义了三种 IPv6 地址类型：

- 单播(Unicast)：单个接口的标识符。送往一个单播地址的包将被传送至该地址标识的接口上。
- 组播(Multicast)：一组接口(一般属于不同节点)的标识符。送往一个组播地址的包将被传送至加入该组播地址的所有接口上。
- 泛播(Anycast)：一组接口的标识符。送往一个泛播地址的包将被传送至该地址标识的接口之一(根据选路协议选择“最近”的一个)。

⚠ 在 IPv6 中已经没有定义广播地址。

下面逐一介绍这几类地址：

↘ 单播地址（Unicast Addresses）

单播地址分为未指定地址、环回地址、链路本地地址、站点本地地址和全球单播地址。目前，站点本地地址被废除了，除了未指定地址、环回地址和链路本地地址以外的单播地址，都是全球单播地址。

- 未指定地址

未指定地址是 0:0:0:0:0:0:0:0，通常简写为**::**，常见的两个用途是：

1. 若主机启动时没有单播地址，则以未指定地址作为源地址，发送路由器请求，从网关获取前缀信息，从而自动生成单播地址。
2. 给主机配置 IPv6 地址时，检测地址是否和同网段其它主机的地址冲突，则以未指定地址作为源地址发送邻居请求（相当于免费 ARP）。

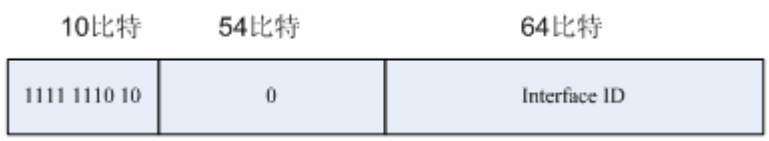
- 环回地址

环回地址是 0:0:0:0:0:0:0:1，通常简写为**::**1，相当于 IPv4 地址 127.0.0.1，一般在节点给自身发报文时使用。

- 链路本地地址

链路本地地址的格式如下：

图 1-2

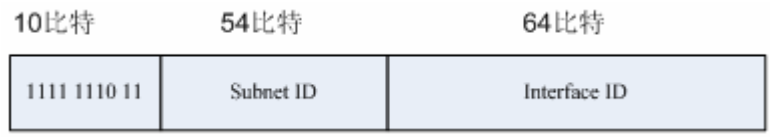


链路本地地址用于单个网络链路上给主机编号。前缀的前 10 位标识的地址即链路本地地址。设备永远不会转发源地址或者目的地址带有链路本地地址的报文。该地址的中间 54 位置成 0。后 64 位表示接口标识符，地址空间的这部分允许单个网络连接多达（2 的 64 次方减 1）个主机。

- 站点本地地址

站点本地地址的格式如下：

图 1-3



站点本地地址可以用在站点内传送数据，设备不会将源地址或者目的地址带有站点本地地址的报文转发到 Internet 上，即这样的包只能在站点内转发，而不能把包转发到站点外去。站点可以理解为一个公司的局域网，这种地址类似于 IPv4 的私有地址，如 192.168.0.0/16。RFC3879 已经废除了站点本地地址。对于新的实现，不再支持该前缀，统一视为全球单播地址；对于已经实现和部署的，可以继续用这个前缀。

- 全球单播地址

全球单播地址格式如下：

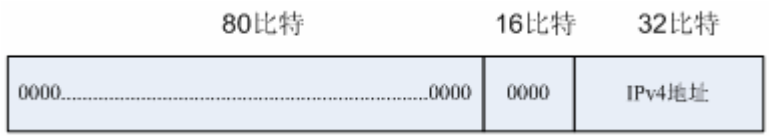
图 1-4



全球单播地址中有一类地址是嵌入 IPv4 地址的 IPv6 地址，用于 IPv4 节点和 IPv6 节点互通，分为 IPv4 兼容 IPv6 地址和 IPv4 映射 IPv6 地址两种。

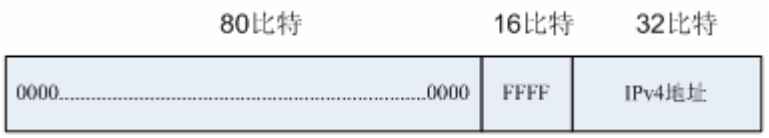
IPv4 兼容 IPv6 地址格式（IPv4-compatible IPv6 address）

图 1-5



IPv4 映射 IPv6 地址格式（IPv4-mapped IPv6 address）

图 1-6



IPv4 兼容 IPv6 地址主要是用在自动隧道上，这类节点既支持 IPv4 也支持 IPv6，IPv4 兼容 IPv6 地址通过 IPv4 设备以隧道方式传送 IPv6 报文，目前 IPv4 兼容 IPv6 地址已被废除。而 IPv4 映射 IPv6 地址则被 IP6 节点用于访问只支持 IPv4 的节点，例如当一个 IPv4/IPv6 主机的 IPv6 应用程序请求解析一个主机名字(该主机只支持 IPv4)时，那么名字服务器内部将动态生成 IPv4 映射的 IPv6 地址返回给 IPv6 应用程序。

↘ 组播地址（Multicast Addresses）

IPv6 组播的地址格式如下：

```
|   8       |   4 |   4  |                    112       bits                    |
+--------+----+----+-------------------------------------------+
|11111111|flgs|scop|                          group ID                          |
+--------+----+----+-------------------------------------------+
```

地址格式中的第 1 个字节为全“1”代表是一个组播地址。

- 标志字段：

由 4 个比特位组成。目前只指定了第 4 位，该位用来表示该地址是由 Internet 编号机构指定的知名的组播地址，还是特定场合使用的临时组播地址。如果该标志位为“0”，表示该地址为知名组播地址；如果该位为“1”，表示该地址为临时地址。其他 3 个标志位保留将来用。

- 范围字段：

由 4 个比特位组成，用来表示组播的范围。即组播组是包括本地节点、本地链路、本地站点，还包括 IPv6 全球地址空间中任何位置的节点。

- 组标识符字段：

长 112 位，用于标识组播组。根据组播地址是临时的还是知名的以及地址的范围，同一个组播标识符可以表示不同的组。

IPv6 的组播地址是以 FF00::/8 为前缀的这类地址。一个 IPv6 的组播地址通常标识一系列不同节点的接口。当一个报文发送到一个组播地址上时，那么该报文将分发到标识有该组播地址的每个节点的接口上。一个节点(主机或者设备)必须加入下列的组播：

3. 本地链路所有节点组播地址 FF02::1

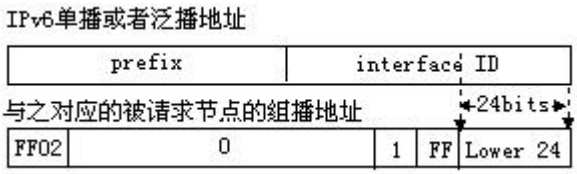
4. 被请求节点的组播地址，前缀为 FF02:0:0:0:0:1:FF00:0000/104

如果是设备那么还必须加入本地链路所有设备的组播地址 FF02::2。

被请求节点的组播地址是对应于 IPv6 单播(unicast)和泛播(anycast)地址的，IPv6 节点必须为配置的每个单播地址和泛播地址加入其相应的被请求节点的组播地址。被请求节点的组播地址的前缀为 FF02:0:0:0:0:1:FF00:0000/104，另外 24 位由单播地址或者泛播地址的低 24 比特组成，例如对应于单播地址 FE80::2AA:FF:FE21:1234 的被请求节点的组播地址是 FF02::1:FF21:1234 ，

被请求节点组播地址通常用于邻居请求(NS)报文中，被请求节点组播地址的格式如下：

图 1-7



泛播地址（Anycast Addresses）

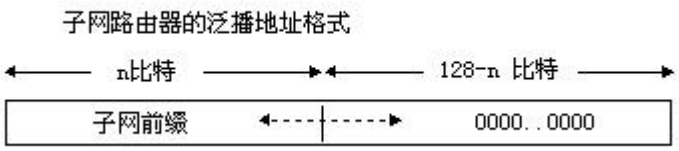
泛播地址与组播地址类似，同样是多个节点共享一个泛播地址，不同的是只有一个节点期待接收给泛播地址的数据包而组播地址成员的所有节点均期待着接收发给该地址的所有包。泛播地址被分配在正常的 IPv6 单播地址空间，因此泛播地址在形式上与单播地址无法区分开，一个泛播地址的每个成员，必须显式地加以配置，以便识别是泛播地址。

泛播地址只能分配给设备，不能分配给主机，并且泛播地址不能作为报文的源地址。

在 RFC2373 中预定义了一个泛播地址，称之为子网路由器的泛播地址。下图显示了子网路由器的泛播地址格式，这类地址由子网前缀后面跟着一系列的 0(作为接口标识符)组成。

其中子网前缀标识了一个指定的链路(子网)，送给子网路由器泛播地址的报文将被分发到在该子网上的一个设备。子网路由器的泛播地址通常是被用于一个节点上的应用程序需要和远程子网的一个设备通信而使用。

图 1-8



相关配置

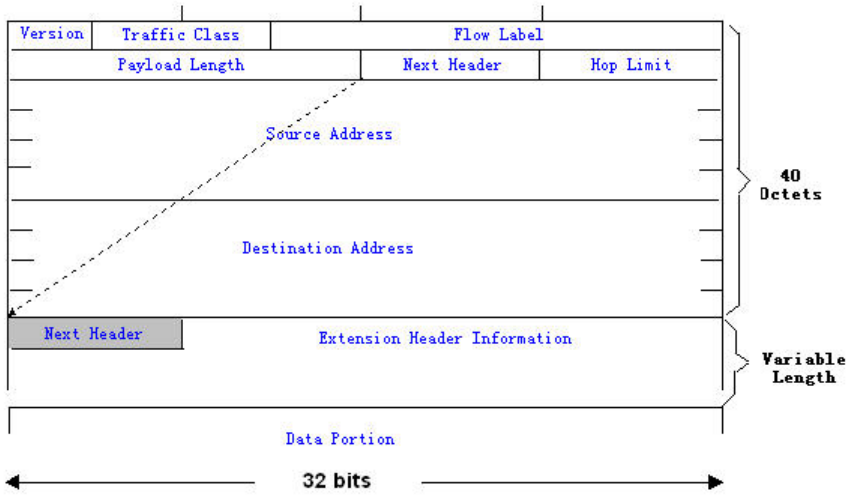
↘ 配置 IPv6 地址

- 缺省情况接口没有配置 IPv6 地址。
- 可通过 **ipv6 address** 命令配置接口 IPv6 单播地址和泛播地址。
- 接口 up 之后将会自动加入相应的组播组。

1.3.3 IPv6 包头结构

IPv6 包头格式如下图：

图 1-9



在 IPv4 中，所有包头以 4 字节为单位。在 IPv6 中，包头以 8 字节为单位，包头的总长度是 40 字节。IPv6 包头定义了以下字段：

- 版本(Version)：

长度为 4 位，对于 IPv6 该字段必须为 6。

- 类别(Traffic Class)：

长度为 8 位，指明为该包提供了某种服务，相当于 IPv4 中的“TOS”。

- 流标签(Flow Label)：

长度为 20 位，用于标识属于同一业务流的包，一个节点可以同时作为多个业务流的发送源，流标签和源节点地址唯一标识了一个业务流。

- 净荷长度(Payload Length)：

长度为 16 位，其中包括包净荷的字节长度，同时也包含了各个 IPv6 扩展选项的长度(如果存在)，换句话说就是包含了除 IPv6 头本身外的 IPv6 包的长度。

- 下一个头(Next Header)：

这个字段指出了 IPv6 头后所跟的头字段中的协议类型。与 IPv4 协议字段类似，下一个头字段可以用来指出高层是 TCP 还是 UDP，它也可以用来指明 IPv6 扩展头的存在。

- 跳数(Hop Limit)：

长度为 8 位。每当设备对包进行一次转发之后，这个字段就会被减 1，如果该字段达到 0，这个包就将被丢弃。它与 IPv4 包头中的生存期字段类似。

- 源地址(Source Address)：

长度为 128 位，指出了 IPv6 包的发送方地址。

- 目的地址(Destination Address)：

长度为 128 位，指出了 IPv6 包的接收方地址。

IPv6 的扩展头，目前 IPv6 定义了下列的扩展头：

- 逐跳选项头(Hop-by-Hop Options)：

此扩展头必须紧随在 IPv6 头之后，它包含包所经过的路径上的每个节点都必须检查的选项数据。

- 路由选项头（Routing （Type 0））：

此扩展头指明包在到达目的地途中将经过哪些节点，它包含包沿途经过的各节点的地址列表。IPv6 头的最初目的地址是选路头的一系列地址中的第一个地址，而不是包的最终目的地址。IPv6 头部目的地址对应的节点接收到该包之后，对 IPv6 头和选路头进行处理，并把包发送到选路头列表中的第二个地址，如此继续，直到包到达其最终目的地。

- 分片头（Fragment）：

此扩展头用于源节点对长度超出源节点和目的节点路径 MTU 的包进行分片。

- 目的地选项头（Destination Options）：

此扩展头代替了 IPv4 选项字段，目前唯一定义的目的地选项是在需要时把选项填充为 6 4 位（8 字节）的整数倍，此扩展头可以用来携带由目的地节点检查的信息。

- 上层扩展头(Upper-layer header)：

指明了上层传输数据的协议，如 TCP(6)、UDP(17)。

此外还有身份验证头(Authentication)和封装安全性净荷(Encapsulating Security Payload)的扩展头，这将放到 IPSec 章节描述。

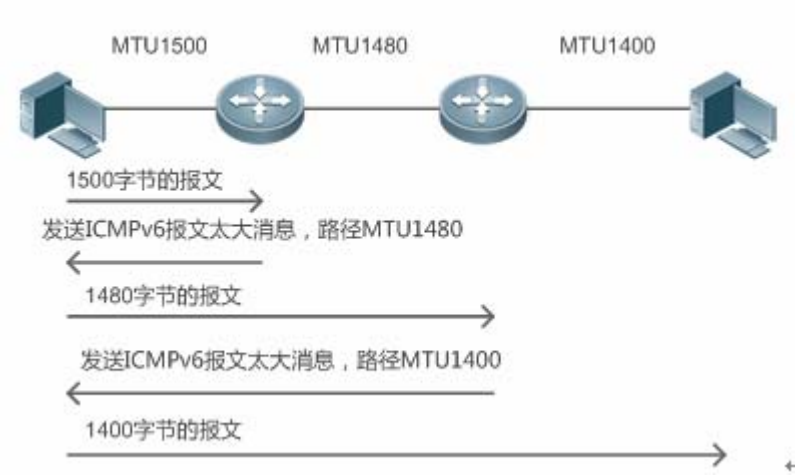
相关配置

无

1.3.4 IPv6 路径MTU发现

和 IPv4 的路径 MTU 发现类似，IPv6 的路径 MTU 发现允许一台主机动态的发现并调整发送数据路径上的 MTU 的大小。另外，当主机要发送的数据包的大小如果比发送数据路径上的 MTU 大时，那么将由主机自行负责分片。这种由主机分片的行为使得设备无需处理分片从而节省了 IPv6 设备的资源，同时也提高了 IPv6 网络的效率。

图 1-10



如上图，当主机要发送的报文的长度比路径 MTU 大时，路由器丢弃报文，并且向主机发送一个 ICMPv6 报文太大消息，把 MTU 告诉主机，然后主机根据新的路径 MTU 对报文进行分片。这种由主机分片的行为使得路由器不需要对报文进行分片从而节省了路由器的资源，同时也提高了 IPv6 网络的效率。

相关配置

配置接口 IPv6 MTU

- 以太网接口的默认 IPv6 MTU 是 1500。
- 可通过 **ipv6 mtu** 命令修改接口的 IPv6 MTU 值。

配置静态路径 MTU

- 可通过 **ipv6path-mtu** 配置静态路径 MTU。

配置动态路径 MTU 的老化时间

- 默认老化时间是 10 分钟。
- 可通过 **ipv6path-mtu age** 配置动态路径 MTU 的老化时间。

1.3.5 IPv6 邻居发现

邻居发现协议是 IPv6 协议的一个基本的组成部分，它的主要功能有路由器发现、前缀发现、参数发现、地址自动配置、地址解析（相当于 ARP）、确定下一跳、邻居不可达检测、地址冲突检测和重定向。邻居发现定义了 5 种 ICMP 报文："路由器请求， ICMP 类型为 133；路由器公告， ICMP 类型为 134；邻居请求，相当于 ARP 请求，ICMP 类型为 135；邻居公告，相当于 ARP 应答，ICMP 类型为 136；ICMP 重定向报文，ICMP 类型为 137"。

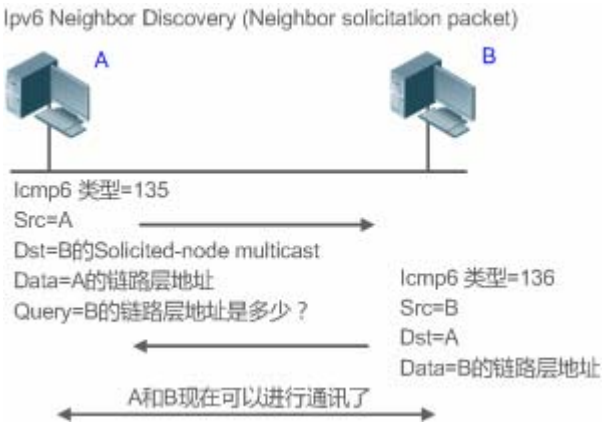
上述五种 ICMP 报文都会携带一个或者多个的选项，这些选项在某些情况下是可选，事实上，有些情况下选项实际上就是报文的全部意义所在，邻居发现主要定义五种选项："源链路层地址选项"，类型=1；"目标链路层地址选项"，类型=2；"前缀信息选项"，类型=3；"重定向的首部选项"，类型=4；"MTU 选项" 类型=5；

地址解析

当一个节点要与另外一个节点通信时，那么该节点必须获取对方的链路层地址，此时就要向该节点发送邻居请求(NS)报文,报文的目的地址是对应于目的节点的 IPv6 地址的被请求多播地址，发送的 NS 报文同时也包含了自身的链路层地址。当对应的节点收到该邻居请求后发回一个响应的报文称之为邻居公告报文(NA)，其目的地址是邻居请求的源地址，内容为被请求的节点的链路层的地址。当源节点收到该应答报文后就可以和目的节点进行通讯了。

下图是地址解析的过程：

图 1-11



邻居不可达检测

当一个邻居被认为可到达的时间到期以后，如果有 IPv6 单播报文需要发送给这个邻居，将执行邻居不可达检测（Neighbor Unreachability Detection)。

邻居不可达检测和向邻居发送 IPv6 报文可以同时进行，在检测过程中，继续向该邻居转发 IPv6 报文。

地址冲突检测

当给主机配置 IPv6 地址以后，想知道这个 IPv6 地址在链路上是不是唯一的，需要执行地址冲突检测，发送源 IPv6 地址是未指定地址的邻居请求。

如果设备检测到地址冲突，该地址将被设置为冲突状态，设备将不能接收目的地址为该地址的 ipv6 报文，同时设备会为该冲突的地址起一个定时器，定时进行地址冲突检测，如果重新检测没有冲突，该地址将可以正常使用。

路由器，前缀和参数发现

路由器公告报文(RA)在设备上是定期被发往链路本地所有节点的。

路由器公告报文发送如下图：

图 1-12



路由器公告报文中通常包含如下内容：

- 一个或者多个 IPv6 地址前缀（用于 on-link 确定，或无状态地址自动配置）
- IPv6 地址前缀的有效期。
- 主机自动配置使用的方式(有状态还是无状态)。
- 作为缺省设备的信息(即决定本设备是否要作为缺省设备，如果是那么还宣布自己充当缺省设备的时间)。
- 提供给主机配置的一些其它信息如跳数限制、MTU、邻居请求重传间隔时间等。

路由器公告报文同时也用来应答主机发出的路由器请求(RS)报文，路由器请求报文允许主机一旦启动后可以立即获得自动配置的信息而无需等待设备发出的路由器公告报文(RA)。当主机刚启动时如果没有单播地址，那么主机发出的路由器请求报文将使用未指定地址(0:0:0:0:0:0:0:0)作为请求报文的源地址，否则使用已有的单播地址作为源地址，路由器请求报文使用本地链路所有设备组播地址(FF02::2)作为目的地址。作为应答路由器请求(RS)报文的路由器公告(RA)报文将使用请求报文的源地址作为目的地址(如果源地址是未指定地址那么将使用本地链路所有节点组播地址 FF02::1)。

在路由器公告报文中下列参数是可以被配置的：

- Ra-interval 路由器公告报文的发送间隔。
- Ra-lifetime 路由器生存期，即设备是否充当本地链路的缺省路由器以及充当该角色的时间。
- Prefix 本地链路的 IPv6 地址前缀，用于 on-link 确定，或无状态地址自动配置，包括前缀的其它参数配置。
- Ns-initerval 邻居请求报文重传的时间间隔。

- Reachabletime 检测到邻居可到达事件后认为邻居是可到达的所维持的时间。
- Ra-hoplimit 路由器公告(RA)报文跳数的值，用于设置主机发送单播报文的 hop-limit
- Ra-mtu 路由器公告(RA)报文的 MTU 字段的值
- Maneged-config-flag 决定了收到该路由器公告的主机是否要使用全状态自动配置来获取地址
- Other-config-flag 决定了收到该路由器公告的主机是否将使用 dhcpv6 来获取除 IPv6 地址以外的其他信息进行自动配置。

以上这些参数在 IPv6 接口属性中进行配置。

重定向

当路由器收到 IPv6 报文以后，发现存在更优的下一跳，就发送 ICMP 重定向报文把更优的下一跳告诉主机，下一次主机直接把 IPv6 报文发给更优的下一跳。

未解析的邻居表项的最大数量

- 为防止恶意扫描网段，生成大量的未解析邻居表项，占用过多的内存，可配置限制未解析的邻居表项的最大数量

处理 ND 选项最大数量

- 为防止伪造 ND 报文携带无穷的 ND 选项，设备处理占用过多的 CPU，可配置限制 ND 选项最大数量

接口邻居学习表项数量

- 为防止邻居学习攻击，占用设备邻居表项，占用内存且影响转发性能，可配置限制接口邻居学习表项数量

相关配置

配置 IPv6 重定向

- 缺省情况 IPV6 的接口上允许发送 ICMPv6 重定向报文
- 可以使用接口配置模式命令“**no ipv6 redirects**”禁止接口发送重定向报文

配置 IPv6 地址冲突检测

- 缺省情况接口上为 IPV6 地址执行地址冲突检测时会发送的 1 个邻居请求(NS)报文
- 可以使用接口配置模式命令“**ipv6 nd dad attempts** *value*”配置 DAD 连续发送的 NS 报文个数，0 表示阻止为该接口上的 Ipv6 地址启动地址冲突检测
- 使用“**no ipv6 nd dad attempts**”恢复默认配置
- 缺省情况设备对已经冲突 IPv6 地址会定时执行地址冲突检测，时间间隔为 60s
- 可以使用全局配置模式命令“**ipv6 nd dad retry** value”配置重复地址冲突检测的时间间隔，0 表示关闭设备进行重复冲突地址检测功能。
- 使用“**no ipv6 nd dad retry**”恢复默认配置

配置邻居可达时间

- 缺省情况 IPv6 邻居默认可达时间为 30s
- 可以使用接口配置模式命令“**ipv6 nd reachable-time***milliseconds*”修改可达时间

配置邻居 stale 状态时间

- 缺省情况 IPv6 邻居默认 stale 状态持续时间 1h，到期后将进行邻居不可达检测
- 可以使用接口配置模式命令“**ipv6 nd stale-time***seconds*”修改 stale 状态持续时间

配置前缀信息

- 缺省情况 RA 公告的前缀是在该接口上通过 **ipv6 address** 命令配置的前缀
- 可以使用接口配置模式命令“**ipv6 nd prefix**”添加或删除可公告的前缀及前缀参数
- 使用接口模块式下命令”**peer default ipv6 pool**”从前缀池分配前缀来进行公告

配置 RA 抑制功能

- 缺省情况 IPv6 的接口上不会发送路由器公告报文
- 可以使用接口配置模式命令“**no ipv6 nd suppress-ra**”关闭 RA 抑制功能

配置未解析的邻居表项的最大数量

- 默认值为 0，表示不限制，即受限于设备支持的 ND 表项容量
- 使用全局配置模式下命令 **ipv6 nd unresolved** *number* 限制未解析邻居数量，表项超过该限制后，将不为后续报文进行主动解析

配置处理 ND 选项最大数量

- 使用全局配置模式下命令 **ipv6 nd max-opt** *value* 限制处理邻居选项个数，默认值为 10

配置接口可学习邻居表项的数量

- 使用接口配置模式下命令 **ipv6 nd cache interface-limit***value* 限制接口可学习的邻居数量，默认值为 0，表示不限制

1.3.6 IPv6 防ND拒绝服务攻击

工作原理

IPv6 防 ND 拒绝服务攻击，通过设置一定的触发条件，保证系统的 IPv6 邻居表项资源不被耗尽，进而保证 IPv6 邻居发现功能正常运行。

所谓邻居表项，是指一个 MAC 地址和 IPv6 地址的配对，用于指明特定 IPv6 地址对应的 MAC 地址。一个 IPv6 用户，其 MAC 地址只能有一个，而对应的 IPv6 地址却可以有多个，这样一个用户可以对应着多个 IPv6 邻居表项。当外界向设备发送

一个 NS 报文，而该 NS 报文内部所包含的 MAC 地址是虚构的，则系统会基于此 NS 报文的虚构的 MAC 地址生成一个邻居表项。

与此同时，邻居表项有一个自身的状态维护机制，通过特定的状态机推动邻居表项的老化。这里的老化需要一定的时间，比如 1 个小时。当外部不断向设备发送基于虚假 MAC 地址的 NS 请求报文时，设备会生成对应的 IPv6 邻居表项。又由于对应的 IPv6 邻居表项的老化需要时间，使得表项的生成速度大于老化速度，使得 IPv6 邻居表被占满，无法再进行正常的 IPv6 邻居发现，进而系统的功能受到影响。这就是 ND 拒绝服务攻击。

IPv6 防 ND 拒绝服务攻击功能在发现系统学习到的 IPv6 邻居表项与 IPv6 邻居表上限之比已经达到了预先设定的某一阈值时，则加速当前处于 STALE 状态的邻居表项进行老化。另外，在任意一个 MAC 地址对应的 IPv6 邻居表项数量超出预先设定的阈值时，则针对该 MAC 地址处于 STALE 状态的 IPv6 邻居表项进行老化。

最后，IPv6 防 ND 拒绝服务攻击功能在加速处于 STALE 状态的 IPv6 邻居进行老化的同时，依然能正常地执行 IPv6 邻居表项的学习。

相关配置

配置整机执行防 ND 拒绝服务攻击的邻居容量占比阈值

- 全局模式，使用 **ipv6 nd threshold***percent_value* 设置
- 缺省情况下，对应的 *percent_value* 为 70

配置单个用户执行防 ND 拒绝服务攻击的邻居表项数量

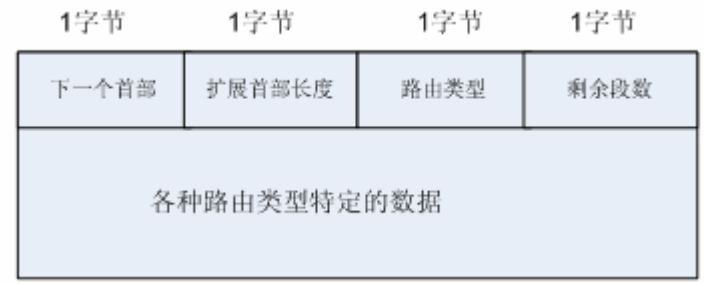
- 全局模式，**ipv6 nd thresholdper-mac** *value* 设置
- 缺省情况下，对应的 *value* 为 16，取值范围是 4- 256

1.3.7 IPv6 源路由

工作原理

IPv6 报文通过路由首部被发送者用来指定报文经过哪些中间节点到达目的地址，类似于 IPv4 的宽松源路由选项和宽松记录路由选项，格式为：

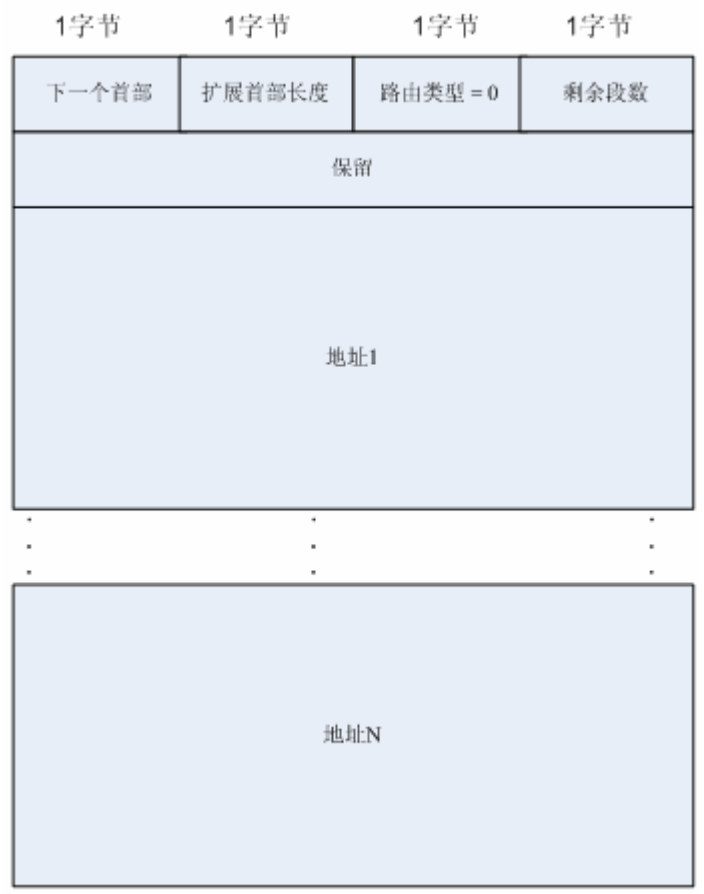
图 1-13



其中剩余段数用来指明报文从当前节点到最终目的地址，还需要经过多少个路由首部指明的中间节点，不包括路由首部没有列出的中间节点。

目前定义了两种路由类型：0 和 2。类型 2 路由首部用于移动通信。RFC2460 定义了类型 0 路由首部（类似于 IPv4 的宽松源路由选项），格式如下图所示。

图 1-14



下面举例说明类型 0 路由首部的应用，如 图 1-15 所示。

图 1-15



主机 1 发报文给主机 2，指明要经过路由器 2 和 3，转发过程中报文 IPv6 首部和路由首部的相关字段变化如下表所示：

传输节点	IPv6 首部的相关字段	类型 0 路由首部的相关字段
主机 1	源地址=1000::2 目的地址=1001::1（路由器 2 的地址）	剩余段数=2 地址 1=1002::1（路由器 3 的地址）

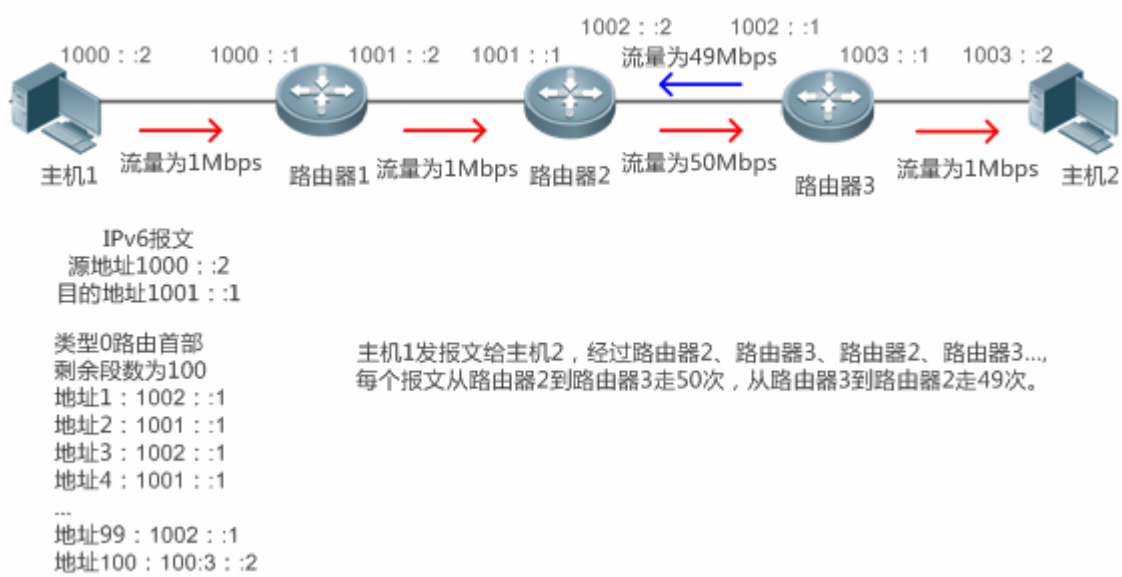
		地址 2=1003::2（主机 2 的地址）
路由器 1	无变化	
路由器 2	源地址=1000::2 目的地址=1002::1（路由器 3 的地址）	剩余段数=1 地址 1=1001::1（路由器 2 的地址） 地址 2=1003::2（主机 2 的地址）
路由器 3	源地址=1000::2 目的地址=1003::2（主机 2 的地址）	剩余段数=0 地址 1=1001::1（路由器 2 的地址） 地址 2=1002::1（路由器 3 的地址）
主机 2	无变化	

具体过程如下：

5. 主机 1 发出报文，目的地址是路由器 2 的地址 1001::1，在类型 0 路由首部中填上路由器 3 的地址 1002::1 和主机 2 的地址 1003::2，剩余段数是 2。
6. 路由器 1 只是简单地把报文转发给路由器 2。
7. 路由器 2 把 IPv6 首部的目的地址和路由首部的地址 1 交换，即现在目的地址是路由器 3 的地址 1002::1，路由首部的地址 1 是路由器 2 的地址 1001::1，剩余段数是 1。修改完以后，路由器 2 把报文转发给路由器 3。
8. 路由器 3 把 IPv6 首部的目的地址和路由首部的地址 2 交换，即现在目的地址是主机 2 的地址 1003::2，路由首部的地址 2 是路由器 3 的地址 1002::1，剩余段数是 0。修改完以后，路由器 3 把报文转发给主机 2。

类型 0 路由首部有可能被利用进行拒绝服务攻击，如下图所示，主机 1 以 1Mbps 的速度向主机 2 发报文，故意构造一个路由首部，使报文在路由器 2 和路由器 3 之间多次往返，从路由器 2 到路由器 3 走 50 次，从路由器 3 到路由器 2 走 49 次，这时路由首部产生流量放大效应：“路由器 2 到路由器 3 方向的流量为 50Mbps，路由器 3 到路由器 2 方向的流量为 49Mbps”。由于存在这个安全问题，RFC5095 废除了类型 0 路由首部。

图 1-16



相关配置

↘ 配置 IPv6 源路由

- 缺省情况不支持类型 0 路由首部
- 可以使用全局配置模式命令“**ipv6 source-route**”打开这项功能

1.3.8 控制ICMPv6 差错报文的发送速率

工作原理

ICMPv6 差错报文是由目标节点或者中间路由器发送，用于报告在转发和传送 IPv6 数据包过程中出现的错误。主要包括下面四种类型的差错报文：目标不可达（Destination unreachable）、报文太大（Packet too big）、超时（Time exceeded）、参数问题（Parameter problem）。

往设备发送非法 IPv6 报文，设备会丢弃这些报文，并向源 IPv6 地址发送相应的 ICMPv6 差错报文。如果受到 IPv6 非法报文攻击，可能出现设备一直在应答 ICMPv6 差错报文而耗尽设备资源，这样设备将不能正常提供服务，针对这种攻击，可以对 ICMPv6 差错报文的发送速率进行限制。

如果转发的 IPv6 报文的长度超过出口的 IPv6 MTU ,路由器会丢弃 IPv6 报文 ,并且向源 IPv6 地址发送 ICMPv6 报文太大消息，这种 ICMPv6 差错报文的主要用途是 IPv6 路径 MTU 发现。为了防止其它 ICMPv6 差错报文太多而将 ICMPv6 报文太大消息限速过滤掉，从而导致 IPv6 路径 MTU 发现功能失效，对 ICMPv6 报文太大消息和其它 ICMPv6 差错报文分别限速。

ICMPv6 重定向报文不属于 ICMPv6 差错报文，我司把 ICMPv6 重定向报文和其它 ICMPv6 差错报一起限速。

相关配置

↘ 配置 ICMPv6 报文太大消息的发送速率

- 缺省速率是 100 毫秒 10 个。
- 可通过 **ipv6icmp error-interval too-big** 配置发送速率。

↘ 配置其它 ICMPv6 差错报文的发送速率

- 缺省速率是 100 毫秒 10 个。
- 可通过 **ipv6icmp error-interval** 配置发送速率。

1.3.9 IPv6 HOP-LIMIT

工作原理

IPv6 数据包从源地址向目的地址经过路由器间传播，设置一个 hop-limit 数值，每过一个路由器 hop-limit 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。其功能类似于 IPv4 的 TTL。

相关配置

↘ 设置 IPv6 hop-limit

- 缺省情况设备 IPv6 HOP-LIMIT 为 64。
- 可通过 **ipv6 hop-limit** 设置设备的 IPv6 HOP-LIMIT 值。

1.3.10 抑制往认证vlan发送广播邻居请求（NS）报文

工作原理

在网关认证模式下，SuperVLAN 下的所有子 VLAN 默认都是认证 VLAN，认证 VLAN 下的认证用户需要在认证后才能上网。用户认证后会在设备上生成静态 ND 表项，因此设备访问认证用户时，不需要往认证 VLAN 发送 NS 请求。若设备需要访问免认证 VLAN 下的用户时，只需要往免认证 VLAN 发送 ARP 请求。

在网关认证模式下，设备默认开启了抑制往认证 VLAN 发送 NS 请求的功能。如果设备需要访问认证 VLAN 下的非认证用户，需要关闭该功能。

相关配置

↘ 设置抑制往认证 vlan 发送广播 NS 报文

- 接口模式下，使用命令 **ipv6 nd suppress-auth-vlan-ns** 开启抑制往认证 VLAN 发送 NS 请求功能。
- 缺省情况下开启抑制往认证 VLAN 发送 NS 请求功能。
- 只支持在 SVI 接口上配置，且只有网关认证模式下才生效

1.3.11 MGMT接口支持缺省网关

工作原理

给 MGMT 口配置缺省网关，为 MGMT 口生成一条默认路由。

相关配置

↘ 设置 MGMT 口的缺省网关

- 接口模式下，使用命令 **ipv6 gateway** *ipv6-address* 配置 MGMT 口的缺省网关。
- 缺省情况下，MGMT 口没有配置缺省网关

1.3.12 IPv6 ND为不同的用户分配不同的前缀

工作原理

接口配置特定的前缀池，使得设备为该接口下的每个用户分配不同的 IPv6 前缀。

相关配置

↘ 配置接口绑定的前缀

- 全局模式下，使用 **ipv6 local pool** *pool-nameipv6-prefix/prefix-length prefix-length* 配置可以分配的前缀池。
- 接口模式下，使用 **ipv6 nd prefix pool** *pool-name*，配置接口绑定的前缀池名称。

1.4 产品说明



NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE 支持 IPV6 功能；NBR800G、NBR950G、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR108G-P、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1500G、NBR2000G 不支持 IPV6 功能。

1.5 配置详解

配置项	配置建议&相关命令	
配置 IPv6 地址	⚠ 必须配置，用于配置 ipv6 地址，启用 IPv6 协议。	
	ipv6 enable	打开接口的 IPv6 协议
	ipv6 address	配置接口 IPv6 的单播地址
	⚠ 可选配置，用于 ipv6 地址借用。	
	ipv6 unnumbered	配置接口借用其他接口的单播地址
配置 IPv6 邻居发现	⚠ 可选配置，用于限制接口 IPv6 重定向功能。	
	ipv6 redirects	打开该接口的 IPv6 重定向功能
	⚠ 可选配置，用于设置 DAD 检测。	

	ipv6 nd dad attempts	配置冲突检测时要连续发送的邻居请求(NS)报文的数量。
	⚠ 可选配置，用于设置邻居发现的各种参数。	
	ipv6 nd reachable-time	设置邻居被认为可到达的时间
	ipv6 nd prefix	设置路由器公告(RA)报文中所要公告的地址前缀
	peer default ipv6 pool	设置路由器公告(RA)从前缀池分配前缀公告
	ipv6 nd suppress-ra	设置是否在该接口上阻止路由器公告（RA）报文发送
	⚠ 可选配置，用于设置未解析邻居的最大数量。	
	ipv6 nd unresolved	设置未解析邻居的最大数量
	⚠ 可选配置，用于设置处理 ND 报文的选项最大数量	
	ipv6 nd max-opt	设置处理 ND 选项最大数量
	⚠ 可选配置，用于限制接口可学习的邻居数量	
	ipv6 nd cache interface-limit	设置接口可学习邻居数量
配置接口 IPv6 防 ND 拒绝服务攻击	⚠ 可选配置，配置整机执行防 ND 拒绝服务攻击的邻居容量占比阈值	
	ipv6 nd threshold	配置整机执行防 ND 拒绝服务攻击的邻居容量占比阈值
	⚠ 可选配置，配置单个用户执行防 ND 拒绝服务攻击的邻居表项数量	
	ipv6 nd threshold per-mac	配置单个用户执行防 ND 拒绝服务攻击的邻居表项数量
配置路径 MTU 发现	⚠ 可选配置，用于限制接口发送 IPv6 报文的 mtu。	
	ipv6 mtu	设置 IPv6 MTU 值
配置 IPv6 源路由	⚠ 可选配置，用于开启支持 IPv6 源路由功能。	
	ipv6 source-route	配置设备转发带有路由首部的 IPv6 报文。
配置 ICMPv6 差错报文的发送速率	⚠ 可选配置。	
	ipv6 icmp error-interval too-big	配置 ICMPv6 报文太大消息的发送速率。
	ipv6 icmp error-interval	配置其它 ICMPv6 差错报文和 ICMPv6 重定向报文的发送速率。
配置设备 IPv6 HOP-LIMIT	⚠ 可选配置，用于限制接口发送 IPv6 单播报文的可转发跳数。	
	ipv6hop-limit	设置 IPv6 HOP-LIMIT 值。
配置抑制往认证 vlan 发送广播 NS 报文	⚠ 可选配置，用于网关认证模式下，抑制往免认证 vlan 发送广播 ns 报文。	
	ipv6 nd suppress-auth-vlan-ns	设置抑制往免认证 vlan 发送广播 ns 报文。
配置 MGMT 口缺省网关	⚠ 可选配置，用于给 mgmt 口配置缺省网关。	

	ipv6 gateway *ipv6-address*	设置 mgmt 口的缺省网关。
配置 IPV6 为不同用户分配不通前缀	⚠ 可选配置，使得设备为接口下的每个用户分配不同的 IPv6 前缀。	
	ipv6 nd prefix pool *pool-name*	为接口绑定前缀地址池。

1.5.1 配置IPv6 地址

配置效果

通过配置接口 IPv6 地址实现 IPv6 网络通信。

注意事项

无

配置方法

↘ 打开接口的 IPv6 协议

- 可选配置，若不想通过配置 IPv6 地址来开启接口 IPv6 协议，则必须配置 **ipv6 enable** 来开启接口 IPv6 功能。

↘ 配置接口 IPv6 的单播地址

- 必须配置。

↘ 配置接口借用其他接口的 IPv6 单播地址

- 通过 **ipv6 unnumbered** 配置接口借用 IPv6 地址。
- 可选配置，只支持 ppp 口。

检验方法

通过 **show ipv6 interface** 可以看到配置的地址生效

相关命令

↘ 打开接口的 IPv6 协议

【命令格式】 **ipv6 enable**
【参数说明】 -
【命令模式】 接口模式

【使用指导】 有 2 种方式可以打开接口上的 IPv6 功能，一是在接口下配置 **ipv6 enable** 命令，二是直接在接口下配置了 IPv6 地址。

> 如果接口已经被绑定到没有配置 IPv6 地址族的多协议 VRF，那么不允许在接口上打开 IPv6 功能，必须先给多协议 VRF 配置 IPv6 地址族，然后才能在接口上打开 IPv6 功能。

如果在接口上配置了 IPv6 地址那么接口的 IPv6 功能就会自动打开，即使使用 **no ipv6 enable** 也不能关闭 IPV6 功能。

配置接口 IPv6 的单播地址

【命令格式】 **ipv6 address***ipv6-address*/*prefix-length*

ipv6 address*ipv6-prefix*/*prefix-length***eui-64**

ipv6 address*prefix-name sub-bits*/*prefix-length* [**eui-64**]

【参数说明】 *ipv6-address*：IPV6 地址，必须遵循 RFC4291 定义的地址形式，每个地址域之间用冒号隔开，每个域占 16 比特，用十六进制数表示.

ipv6-prefix：IPV6 地址前缀，必须遵循 RFC4291 定义的地址形式，每个地址域之间用冒号隔开，每个域占 16 比特，用十六进制数表示.

prefix-length：IPV6 前缀的长度即 IPV6 地址中代表网络的部分。

prefix-name：通用前缀的名字。使用这个指定的通用前缀生成接口地址。

sub-bits：子前缀比特与主机比特的值。这个值与通用前缀中的前缀合并生成接口地址。这个值的表示法要遵循 RFC4291 描述的冒号表示法。

eui-64：表示生成的 IPV6 地址由配置的地址前缀和 64 比特的接口 ID 标识符组成。

【命令模式】 接口模式

【使用指导】

> 如果接口已经被绑定到没有配置 IPv6 地址族的多协议 VRF，那么不允许给接口配置 IPv6 地址，必须先给多协议 VRF 配置 IPv6 地址族，然后才能给接口配置 IPv6 地址。

当一个 IPV6 接口被创建并且链路状态为 UP 时那么系统将为该接口自动生成链路本地地址。

接口的 IPv6 地址也可以使用通用前缀机制生成。其机制就是 IPv6 地址=“通用前缀”+“子前缀”+“主机比特”。通用前缀可以使用 **ipv6 general-prefix** 命令配置，也可能通过 DHCPv6 客户端的 PD(前缀发现)功能学习到(参见 DHCPv6 配置指南)。“子前缀”+“主机比特”就是使用本命令的 *sub-bits/prefix-length* 参数配置。

使用 **no ipv6 address** 如果不指定删除具体的地址，那么将删除所有手工配置的地址。

使用 **no ipv6 address***ipv6-prefix/prefix-length***eui-64** 可以删除使用命令 **ipv6 address***ipv6-prefix/prefix-length***eui-64** 配置的地址。

配置接口借用其他接口的 IPv6 单播地址

【命令格式】 **ipv6 unnumbered** *interface-id*

【参数说明】 -

【命令模式】 接口模式

【使用指导】 借用其他接口的地址可以节省 IPv6 地址，只支持 ppp 口。

> 如果接口已经被绑定到没有配置 IPv6 地址族的多协议 VRF，那么不允许在接口上配置 IPv6 unnumbered

功能，必须先给多协议 VRF 配置 IPv6 地址族，然后才能在接口上配置 IPv6 unnumbered 功能。

如果在接口上配置了 ipv6 unnumbered 那么接口的 IPv6 功能就会自动打开，即使使用 **no ipv6 enable** 也不能关闭 IPV6 功能。

配置举例

↘ 给接口配置 IPv6 地址

【配置方法】 在接口 GigabitEthernet 0/0 开启 IPv6 协议，并添加 ipv6 地址 2000::1

```
Ruijie(config)#interface gigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 enable
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 address 2000::1/64
```

【检验方法】 使用 **show ipv6 interface** 可以看到接口 GigabitEthernet 0/0 添加地址成功

```
Ruijie(config-if-GigabitEthernet 0/0)#show ipv6 interface gigabitEthernet 0/0

interface GigabitEthernet 0/0 is Down, ifindex: 1, vrf_id 0
  address(es):
    Mac Address: 00:00:00:00:00:00
    INET6: FE80::200:FF:FE00:1 [ TENTATIVE ], subnet is FE80::/64
    INET6: 2000::1 [ TENTATIVE ], subnet is 2000::/64
  Joined group address(es):
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND retransmit interval is 1000 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds<160--240>
  ND router advertisements live for 1800 seconds
```

常见错误

无

1.5.2 配置IPv6 邻居发现

配置效果

配置 ND 协议相关属性，比如配置 ipv6 重定向功能，配置 DAD 检测等。

注意事项

接口默认是抑制发送 RA 报文，要设备能够发送 RA 报文必须在接口模式下配置 no ipv6 nd suppress-ra。

配置方法

打开该接口的 IPv6 重定向功能

- 可选配置，缺省已开启。
- 当需要关闭接口 IPv6 重定向功能时，使用“**no ipv6 redirects**”。

配置冲突检测时要连续发送的邻居请求(NS)报文的数量

- 可选配置。
- 如果需要阻止为该接口上的 Ipv6 地址启动地址冲突检测或者修订 DAD 连续发送邻居请求(NS)报文个数，可使用该配置。

设置邻居被认为可到达的时间

- 可选配置。
- 如果需要修改邻接可达时间，可使用该配置。

设置路由器公告(RA)报文中所要公告的地址前缀

- 缺省情况 RA 公告的前缀是在该接口上通过 ipv6 address 命令配置的前缀
- 可选配置，可使用“**ipv6 nd prefix**”手工添加或删除可公告的前缀及前缀参数，或者使用“**peer default ipv6 pool**”从前缀池分配前缀来进行公告

设置是否在该接口上阻止路由器公告（RA）报文发送

- 可选配置。
- 如果需要设备能发送路由器公告，可使用该命令来配置。

配置未解析的邻居表项的最大数量

- 可选配置。
- 如果设备受到扫描攻击而创建大量未解析邻居表项，消耗表项资源，可以使用该命令限制未解析邻居的数量。

配置处理 ND 选项最大数量

- 可选配置
- 如果环境要求设备能够处理更多的选项内容，可使用该命令来配置。

配置接口可学习邻居表项的数量

- 可选配置
- 如果环境中 IPv6 主机数可控制，可以使用该功能限制接口的学习邻居个数，防止网络中进行 ND 学习攻击，使得设备学习表项占用内存影响性能。

检验方法

通过以下命令查看配置是否正确：

- **show ipv6 interface** *interface-type interface-num* 可查看接口重定向功能，邻居可达时间、邻居请求发送间隔等信息是否配置生效
- **show ipv6 interface** *interface-type interface-num* **ra-inifo** 可查看路由器公告配置的前缀及其他信息是否正确
- **show run**

相关命令

打开该接口的 IPv6 重定向功能

【命令格式】 **ipv6 redirects**

【参数说明】 -

【命令模式】 接口模式

【使用指导】 所有 ICMPv6 的错误报文的数据包传输速率是有限制的，缺省每秒钟最多可以发送 10 个错误 ICMPv6 错误报文(10pps)。

配置冲突检测时要连续发送的邻居请求(NS)报文的数量

【命令格式】 **ipv6 nd dad attempts** *value*

【参数说明】 *value*：邻居请求(NS)报文的数量

【命令模式】 接口模式

【使用指导】 当在接口上配置一个新的 IPV6 地址前要为它启动地址冲突检测，此时该地址处于”tentative”（试验）的状态。地址冲突过程执行完了，如果没有检测到冲突，那么该地址就可以被正确使用，如果检测到冲突了，并且该地址所使用的接口标识符是使用 EUI-64 的标识符，那么表明在该链路上存在链路层地址出现重复，那么此时系统会自动关闭该接口（即阻止在该接口上进行 IPV6 的相关操作），此时必须手工去修改并配置新的地址，并通过再次 down/up 接口重新启动地址冲突检测。任何情况下当一个接口从 down 状态变为 up 状态时都会为该接口上的地址重新启动地址冲突检测。

设置邻居被认为可到达的时间

【命令格式】 **ipv6 nd reachable-time***milliseconds*

【参数说明】 *milliseconds*：邻居被认为可到达的时间，以毫秒为单位，范围： 0-3600000。缺省为 30 秒。

【命令模式】 接口模式

【使用指导】 设备通过该配置的时间来检测不可用的邻居，所设置的时间越短意味着可以更快的检测到邻居失效，但是将浪费更多的网络带宽、消耗设备更多的资源。因此不建议将该时间配置的过小。

配置的值将在路由器公告报文(RA)中被发布出去，同时该值也被设备自身使用。如果设置的值为 0 表示设备

未指定该时间，即使用缺省值。

设置路由器公告(RA)报文中所要公告的地址前缀

【命令格式】 **ipv6 nd prefix {***ipv6-prefix/prefix-length* | **default**} [[*valid-lifetime* {**infinite** | *preferred-lifetime* }] | [**at** *valid-datepreferred-date*] | [**infinite**{**infinite** | *preferred-lifetime*}]] [**no-advertise**] | [[**off-link**] [**no-autoconfig**]]

【参数说明】 *ipv6-prefix*：IPV6 的网络号，必须遵循 RFC4291 的地址表示形式。

prefix-length：IPV6 前缀的长度，注意前面必须加上’ /’ 。

valid-lifetime：主机收到路由器公告的前缀后认为有效的时间，取值范围 0-4294967295。缺省 30 天。

preferred-lifetime：主机收到路由器公告的前缀后认为首选有效的时间，取值范围 0-4294967295，缺省 7 天。

at*valid-date preferred-date*：设置公告前缀有效和首选有效的截止时间，截止时间是以日、月、年、小时、分钟表示的。

infinite：表示永远都有效。

default：设置要使用的缺省参数配置。

no-advertise：表示该前缀不被路由器公告。

off-link：主机在发送 IPV6 报文时如果目的地址的前缀匹配前缀那么认为该目的地是在同一链路(on-link)上是可直接到达的。设置了该选项表示该前缀不用来做 on-link 的判断。

no-autoconfig：该选项指示主机收到该路由器公告中的前缀不能用于地址自动配置。

【命令模式】 接口模式

【使用指导】 通过该命令可以分别配置每一个前缀的各个参数，包括是否要公告该前缀，缺省情况下路由器公告报文中(RA)公告的前缀是在该接口上通过 **ipv6 address** 命令配置的前缀 如果要增加其它前缀可以使用该命令进行配置。**ipv6 nd prefix default** 设置该接口上使用的缺省配置参数，即新增加一个前缀时，如果没有指定任何参数，那么将使用 **ipv6 nd prefix default** 所设置的参数做为配置的前缀的参数。注意一旦为该前缀指定了某个参数以后将不再认为使用缺省参数配置。即以后使用 **ipv6 nd prefix default** 改变缺省参数配置时不会去修改该前缀的配置，而只修改完全使用缺省参数配置的前缀。

at *valid-datepreferred-date* 前缀的有效时间有 2 种指定方式：一种是在公告报文中每个前缀指定一个固定的时间；另外一种是指定截止时间，使用该方式那么每次发出去的公告报文中的前缀的有效时间将采用递减的方式，直到值为 0。

设置是否在该接口上阻止路由器公告（RA）报文发送

【命令格式】 **ipv6 nd suppress-ra**

【参数说明】 -

【命令模式】 接口模式

【使用指导】 当要在一个接口上抑制路由器公告报文发送时可以使用 ipv6 suppress-ra 命令

设置未解析的邻居表项的最大数量

【命令格式】 **ipv6 nd unresolved** *number*

【参数说明】 *number*：表示未解析邻居表项限制数

【命令模式】 全局模式

【使用指导】 为了防止恶意扫描攻击导致生成大量未解析的 ND 表项，占用表项资源，可以通过配置限制未解析的 ND 表项的个数。

设置可处理 ND 选项数量

【命令格式】 **ipv6 nd max-opt***value*

【参数说明】 *value*：支持的选项个数

【命令模式】 全局模式

【使用指导】 配置设备处理 ND 选项数量限制，比如链路层地址选项，MTU 选项，重定向选项，前缀选项。

设置接口可学习邻居表项数量

【命令格式】 **ipv6 nd cache interface-limit***value*

【参数说明】 value：接口所能学习的邻居最大限制

【命令模式】 接口模式

【使用指导】 限制接口的邻居学习数量，可防止恶意的邻居攻击，让设备生成大量的邻居表项，占用过多的内存。配置的值必须不小于当前接口已经学习到的邻居数，否则配置不生效。该限制受限于设备支持 ND 容量。

配置举例

打开接口的 IPv6 重定向功能

【配置方法】 开启接口 IPv6 重定向功能。

```
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 redirects
```

【检验方法】 通过 **show ipv6 interface** 查看配置是否生效。

```
Ruijie#show ipv6 interface gigabitEthernet 0/0


interface GigabitEthernet 0/0 is Down, ifindex: 1, vrf_id 0
  address(es):
    Mac Address: 00:00:00:00:00:00
    INET6: FE80::200:FF:FE00:1 [ TENTATIVE ], subnet is FE80::/64
  Joined group address(es):
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND retransmit interval is 1000 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds<160--240>
  ND router advertisements live for 1800 seconds
```

配置 IPv6 地址冲突检测

【配置方法】 配置 DAD 检测要连续发送 3 个 NS 报文。

```
Ruijie(config-if-GigabitEthernet 0/0)# ipv6 nd dad attempts 3
```

【检验方法】 通过 **show ipv6 interface** 查看配置是否生效。

```
Ruijie#show ipv6 interface gigabitEthernet 0/0


interface GigabitEthernet 0/0 is Down, ifindex: 1, vrf_id 0
  address(es):
    Mac Address: 00:00:00:00:00:00
    INET6: FE80::200:FF:FE00:1 [ TENTATIVE ], subnet is FE80::/64
  Joined group address(es):
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 3
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND retransmit interval is 1000 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds<160--240>
  ND router advertisements live for 1800 seconds
Ruijie(config-if-GigabitEthernet 0/0)#
```

↘ 手工配置路由器公告的前缀信息

【配置方法】 为接口添加一个前缀 1234::/64。

```
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 nd prefix 1234::/6
```

【检验方法】 通过 **show ipv6 interface** 查看配置是否生效。

```
Ruijie#show ipv6 interface gigabitEthernet 0/0 ra-info


GigabitEthernet 0/0: DOWN (RA is suppressed)
  RA timer is stopped
  waits: 0, initcount: 0
  statistics: RA(out/in/inconsistent): 0/0/0, RS(input): 0
  Link-layer address: 00:00:00:00:00:00
  Physical MTU: 1500
  ND router advertisements live for 1800 seconds
  ND router advertisements are sent every 200 seconds<160--240>
  Flags: !M!O, Adv MTU: 1500
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit time is 0 milliseconds
  ND advertised CurHopLimit is 64
  Prefixes: <total: 1>
    1234::/64(Def, CFG, vltime: 2592000, pltime: 604800, flags: LA)
```

配置路由器公告的前缀从前缀池获取

【配置方法】 配置路由器公告的前缀从前缀池“ra-pool”获取

```
Ruijie(config-if-GigabitEthernet 0/0)#peel default ipv6 pool ra-pool
```

【检验方法】 通过 **show run** 查看配置是否生效。

```
Ruijie(config-if-GigabitEthernet 0/0)#show run interface gigabitEthernet 0/0

Building configuration...
Current configuration : 125 bytes

interface GigabitEthernet 0/0
 ipv6 enable
 no ipv6 nd suppress-ra
 peel default ipv6 pool ra-pool
!
```

配置关闭路由器公告抑制功能

【配置方法】 关闭接口抑制路由器公告功能

```
Ruijie(config-if-GigabitEthernet 0/0)# no ipv6 nd suppress-ra
```

【检验方法】 通过 **show run** 查看配置是否生效。

```
Ruijie(config-if-GigabitEthernet 0/0)#show run interface gigabitEthernet 0/0

Building configuration...
Current configuration : 125 bytes

interface GigabitEthernet 0/0
 ipv6 enable
 no ipv6 nd suppress-ra
!
```

配置未解析的邻居表项的最大数量

【配置方法】 配置未解析的邻居表项的最大数量为 200

```
Ruijie(config)# ipv6 nd unresolved 200
```

【检验方法】 通过 **show run** 查看配置是否生效。

```
Ruijie#show run

ipv6 nd unresolved 200
!
```

配置可处理 ND 选项数量

【配置方法】 配置可处理 ND 选项数量为 20

```
Ruijie(config)# ipv6 nd max-opt20
```

【检验方法】 通过 **show run** 查看配置是否生效。

```
Ruijie#show run

ipv6 nd max-opt20
!
```

↘ 配置接口可学习邻居表项数量

【配置方法】 配置接口可学习邻居表项数量 100

```
Ruijie(config-if-GigabitEthernet 0/1)# ipv6nd cache interface-limit 100
```

【检验方法】 通过 **show run** 查看配置是否生效。

```
Ruijie#show run
!
interface GigabitEthernet 0/1
 ipv6nd cache interface-limit 100
!
```

常见配置错误

无

1.5.3 配置IPv6 防ND拒绝服务攻击

配置效果

依据配置启动设备的防 ND 拒绝服务攻击功能

注意事项

无

配置方法

↘ 配置启动防 ND 拒绝服务攻击的整机邻居表项容量占比阈值

- 可选配置

↘ 配置启动防 ND 拒绝服务攻击的单个用户的邻居表项数量

- 可选配置

检验方法

- 通过 **show running-config** 命令查看配置是否正确。

相关命令

配置启动防 ND 拒绝服务攻击的整机邻居表项容量占比阈值

【命令格式】 **ipv6 nd threshold***percent_value*

【参数说明】 *percent_value*：当设备 ND 表项数与设备 ND 表项容量之比超出这一数值时，启动 IPv6 防 ND 拒绝服务攻击

【命令模式】 全局模式

【使用指导】 这里的 *percent_value* 是指当前 ND 表项数与设备所能支持的 ND 表项数之比。在系统 IPv6 邻居总表项占比已经达到命令设置的阈指时，则对系统中处于 stale 状态的邻居表项进行可达性探测，但邻居发现功能不受影响，依旧可以继续学习新的邻居表项。

配置启动防 ND 拒绝服务攻击的单个用户的邻居表项数量

【命令格式】 **ipv6 nd thresholdper-mac** *value*

【参数说明】 *value*：单个用户的 IPv6 邻居表项数超出这一数值时，启动针对该用户的 IPv6 防 ND 拒绝服务攻击

【命令模式】 全局模式

【使用指导】 这里是针对单个用户启动防 ND 拒绝服务攻击，当任意的一个用户对应的 IPv6 邻居表项数达到了该命令指定的数值时，则对应用户的相关 stale 状态的 IPv6 邻居表项执行可达性探测。其他 IPv6 邻居表项没有达到该命令指定的数值的用户不受影响。该命令同样不会影响到邻居发现功能的运行，可以继续学习到对应用户的新的邻居表项。

配置举例

配置启动防 ND 拒绝服务攻击的整机邻居表项容量占比阈值

【配置方法】 配置启动防 ND 拒绝服务攻击的整机邻居表项容量占比阈值为 80%

```
Ruijie(config)# ipv6nd threshold 80
```

【检验方法】 通过 **show running-config** 查看配置是否生效。

配置启动防 ND 拒绝服务攻击的单个用户的邻居表项数量

【配置方法】 配置启动防 ND 拒绝服务攻击的单个用户的邻居表项数量为 100

```
Ruijie(config)# ipv6nd threshold per-mac 100
```

【检验方法】 通过 **show running-config** 查看配置是否生效。

常见配置错误

无

1.5.4 配置路径MTU发现

配置效果

本地发送 IPv6 报文时根据路径 MTU 分片。

注意事项

接口 IPv6 MTU 的配置范围受接口 MTU 限制，最大值是接口 MTU。

配置方法

设置接口 IPv6 MTU 值

- 可选配置。

配置静态路径 MTU

- 可选配置。

配置动态路径 MTU 的老化时间

- 可选配置。

检验方法

- 通过 **show run** 命令查看配置是否正确。
- 通过 **show ipv6 interface** 命令查看接口 IPv6 MTU 配置是否正确。
- 通过 **show ipv6 path-mtu** 命令查看路径 MTU。
- 本地发送长度超过路径 MTU 的 IPv6 报文，抓包可以看到 IPv6 报文根据路径 MTU 进行分片。

相关命令

设置接口 IPv6 MTU 值

【命令格式】 **ipv6 mtu** *bytes*

【参数说明】 *bytes*：IPv6 包最大传输单元，以字节为单位，范围 1280~1500。

【命令模式】 接口模式

【使用指导】 -

配置静态路径 MTU

【命令格式】 **ipv6 path-mtu** [**vrf** *vrf-name*]*ipv6-address value*

ipv6 path-mtu *ipv6-address value*

【参数说明】 **vrf** *vrf-name*：VRF 实例的名称，如果不输入该参数，表示公网。

ipv6-address：IPv6 地址，可以是单播地址或者组播地址。

value：路径 MTU 的值，单位是字节，取值范围是 1280 到 65575。

【命令模式】 全局模式

【使用指导】 本地发送 IPv6 报文时，将比较出口的 IPv6 MTU 和路径 MTU，如果报文长度大于两者的最小值，采用最小值对报文进行分片。

IPv6 组播报文可能通过多条路径到达多个不同的节点，所以组播地址的路径 MTU 是在所有路径的路径 MTU 中取最小值。

在 VRF 名称和 IPv6 地址都相同的情况下，静态路径 MTU 覆盖动态路径 MTU，动态路径 MTU 不可以覆盖静态路径 MTU。

用户可以执行命令“**no ipv6 path-mtu all**”删除所有静态路径 MTU。

用户可以执行命令“**show ipv6 path-mtu statistics**”查看静态路径 MTU 的容量和当前数量。

设置动态路径 MTU 的老化时间

【命令格式】 **ipv6 path-mtu age**{*age-time* | **infinity**}

【参数说明】 *age-time*：老化时间，单位是分钟，范围是 10 到（30 * 24 * 60），默认值是 10 分钟。

infinity：老化时间无穷大，即永远不老化。

【命令模式】 全局模式

【使用指导】 学习到动态路径 MTU，在老化以前，路径 MTU 的值只能减小，不能增大。

在实际应用中，网络拓扑可能变化，路由可能变化，导致路径变化，已经学习到的路径 MTU 比实际的路径 MTU 小，所以需要定期老化路径 MTU，然后重新学习。

当动态路径 MTU 的老化时间到期时，将删除动态路径 MTU，在重新学习到路径 MTU 前，发送长的 IPv6 报文，在转发过程中可能被路由器丢弃。如果局域网通过一条小 MTU 链路连接到因特网，可以确定这条链路的 MTU 在所有路径中是最小的 ,那么不应该忍受每隔 10 分钟丢包 ,应该增大老化时间 ,可以配置为永远不老化。

配置举例

配置接口 IPv6 MTU

【配置方法】 修改接口 IPv6 MTU 为 1300。

```
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 mtu 1300
```

【检验方法】 通过 **show ipv6 interface** 查看配置是否生效。

```
Ruijie(config-if-GigabitEthernet 0/0)#show ipv6 interface


interface GigabitEthernet 0/ is Down, ifindex: 1, vrf_id 0
  address(es):
    Mac Address: 00:d0:f8:22:33:47
    INET6: FE80::2D0:F8FF:FE22:3347 [ TENTATIVE ], subnet is FE80::/64
    INET6: 1020::1 [ TENTATIVE ], subnet is 1020::/64
    INET6: 1023::1 [ TENTATIVE ], subnet is 1023::/64
  Joined group address(es):
  MTU is 1300 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND retransmit interval is 1000 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds<160--240>
  ND router advertisements live for 1800 seconds
```

配置静态路径 MTU

【配置方法】 配置 IPv6 地址 A000::1 的路径 MTU 为 1400 字节。

```
Ruijie(config)#ipv6path-mtu A000::1 1400
```

【检验方法】 通过 **show ipv6 path-mtu** 查看配置是否生效。

```
Ruijie#show ipv6 path-mtu
IPv6 Address    MTU    Age    Type
A000::1         1400   --     Static
A000::2         1300   1      Dynamic
```

Age 是老化时间，即学习到动态路径 MTU 到现在的时间长度，单位是分钟，如果是静态路径 MTU，显示为“--”。

Type 是路径 MTU 的类型：动态或者静态。

配置动态路径 MTU 的老化时间

【配置方法】 配置动态路径 MTU 的老化时间为 30 分钟。

```
Ruijie(config)#ipv6path-mtu age 30
```

【检验方法】 通过 **show run** 查看配置是否生效。

```
Ruijie#show run | include ipv6 path-mtu age
ipv6path-mtu age 30
```

常见配置错误

无

1.5.5 配置IPv6 源路由

配置效果

RFC5095 废除了类型 0 路由首部。锐捷的解决方法是缺省情况不支持类型 0 路由首部 ,管理员可以使用全局配置模式命令“ipv6 source-route” 打开这项功能。

注意事项

无

配置方法

↘ 配置设备转发带有路由首部的 IPv6 报文

- 可选配置。
- 如果需要开启 IPv6 源路由功能，可使用该配置。

检验方法

向设备发送带有 0 路由首部的报文，设备能够正常转发。

相关命令

↘ 配置设备转发带有路由首部的 IPv6 报文

【命令格式】 **ipv6 source-route**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 因为类型 0 路由首部有安全隐患：使设备很容易遭受拒绝服务攻击，所以在缺省情况下禁止转发带有路由首部的 IPv6 报文，但是仍然处理最终目的地址是本机的带有类型 0 路由首部的 IPv6 报文。

配置举例

↘ 配置支持 IPv6 类型 0 路由。

【配置方法】 开启支持 IPv6 类型 0 路由功能。

```
Ruijie(config)#ipv6 source-route
```

【检验方法】 使用 **show run** 查看配置是否生效。

```
Ruijie#show run | inc ipv6 source-route
ipv6 source-route
```

常见配置错误

无

1.5.6 配置ICMPv6 差错报文的发送速率

配置效果

配置 ICMPv6 差错报文的发送速率。

注意事项

-

配置方法

配置 ICMPv6 报文太大消息的发送速率

- 可选配置。
- 如果设备收到大量 IPv6 报文的长度超过出口的 IPv6 MTU，并因发送 ICMPv6 报文太大消息而消耗较大 CPU 的情况，可以使用该配置限制该差错报文的发送。

配置其它 ICMPv6 差错报文的发送速率

- 可选配置。
- 如果设备收到大量非法 IPv6 报文，并因此而产生大量 ICMPv6 差错报文时，可以使用该配置限制差错报文发送速率（该命令不会影响 ICMPv6 报文太大差错报文的发送速率）

检验方法

执行 **show running-config** 可以看到配置生效。

相关命令

配置 ICMPv6 报文太大消息的发送速率

【命令格式】 **ipv6 icmp error-interval too-big** *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 ICMPv6 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 ICMPv6 差错报文的发送速率进行限制，采用令牌桶算法。

如果转发的 IPv6 报文的长度超过出口的 IPv6 MTU ,路由器会丢弃 IPv6 报文 ,并且向源 IPv6 地址发送 ICMPv6 报文太大消息，这种 ICMPv6 差错报文的主要用途是 IPv6 路径 MTU 发现。为了防止其它 ICMPv6 差错报文太多导致发不出 ICMPv6 报文太大消息，从而导致 IPv6 路径 MTU 发现功能失效，对 ICMPv6 报文太大消息和其它 ICMPv6 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 ICMPv6 差错报文的发送速率

【命令格式】 **ipv6 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 ICMPv6 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 ICMPv6 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 ICMPv6 差错报文的发送速率

【配置方法】 配置 ICMPv6 报文太大消息的发送速率为 1 秒 100 个，配置其它 ICMPv6 差错报文的发送速率为 1 秒 10 个。

```
Ruijie(config)#ipv6 icmp error-interval too-big 1000 100
Ruijie(config)#ipv6 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 ipv6 icmp error-interval
ipv6 icmp error-interval 1000 10
ipv6 icmp error-interval too-big 1000 100
```

常见配置错误

无

1.5.7 配置IPv6 HOP-LIMIT

配置效果

配置发送单播报文的跳数，避免报文在网络上无限传播下去。

注意事项

-

配置方法

↘ 设置 IPv6 HOP-LIMIT 值

- 可选配置
- 如果需要修订单播报文的转发跳数，可以使用该配置

检验方法

- 通过 **show running-config** 命令查看配置是否正确。
- 本地发送 ipv6 单播报文，抓包可以看到 ipv6 首部的 hop-limit 字段值与配置的一致。

相关命令

↘ 设置 IPv6 HOP-LIMIT 值

【命令格式】 **ipv6 hop-limit value**
【参数说明】 *value*：设备发送单播报文的跳数值，范围 1~255。
【命令模式】 全局模式
【使用指导】 -

配置举例

↘ 配置 IPv6 HOP-LIMIT

【配置方法】 修改设备 IPv6 HOP-LIMIT 为 250。

```
Ruijie(config)#ipv6 hop-limit 250
```

【检验方法】 通过 **show running-config** 查看配置是否生效。

```
Ruijie#show running-config
ipv6 hop-limit 254
```

常见配置错误

无

1.5.8 配置抑制往认证vlan发送广播邻居请求（NS）报文

配置效果

抑制在 SVI 口上往认证 vlan 发送广播邻居请求（NS）报文。

注意事项

只支持 SVI 口配置，且在网络认证模式下才生效。

配置方法

↘ 配置抑制往免认证 vlan 发送广播 NS 报文

- 可选配置
- 网关认证模式下，如果希望设备能往认证 vlan 发送广播 NS 报文，可使用该配置

检验方法

- 通过 **show running-config** 命令查看配置是否正确。

相关命令

↘ 设置抑制往免认证 vlan 发送广播 NS 报文

【命令格式】 **ipv6 nd suppress-auth-vlan-ns**

【参数说明】 -

【命令模式】 接口模式

【使用指导】 使用改命令的 no 形式，可以关闭该功能。

配置举例

配置关闭抑制往免认证 vlan 发送广播 NS 报文

【配置方法】 配置关闭抑制往免认证 vlan 发送广播 ns 报文。

```
Ruijie(config-if-VLAN 2)#no ipv6 nd suppress-auth-vlan-ns
```

【检验方法】 通过 **show running-configinterface vlan 2** 查看配置是否生效。

```
Ruijie#show running-config interface vlan 2
no ipv6 nd suppress-auth-vlan-ns
```

常见配置错误

无

1.5.9 配置MGMT口缺省网关

配置效果

配置 mgmt 口缺省网关，生成一条默认路由出口是 mgmt 口，下一跳是配置的网关。

注意事项

MGMT 口才支持。

配置方法

配置 MGMT 口缺省网关

- 可选配置
- 如果需要为 MGMT 配置一条默认路由并指定下一跳，可以使用该配置

检验方法

- 通过 **show running-config** 命令查看配置是否正确。

相关命令

设置 MGMT 口缺省网关

【命令格式】 **ipv6 gataway** *ipv6-address*

【参数说明】 -

【命令模式】 接口模式

【使用指导】 只在 MGMT 口支持

配置举例

配置 MGMT 口缺省网关为 2000::1

【配置方法】 配置 MGMT 口缺省网关为 2000::1。

```
Ruijie(config)# interface mgmt 0

Ruijie(config-mgmt)# ipv6gateway 2000::1
```

【检验方法】 通过 **show running-configinterface vlan 2** 查看配置是否生效。

```
Ruijie#show running-config interface mgmt 0
Ipv6 gateway 2000::1
```

常见配置错误

无

1.5.10 配置IPv6 ND为不同的用户分配不同的前缀

配置效果

接口配置特定的前缀池，使得设备为该接口下的每个用户分配不同的 IPv6 前缀。

注意事项

无

配置方法

配置接口绑定的前缀

- 可选配置
- 全局模式下，使用 **ipv6 local pool** *pool-nameipv6-prefix/prefix-length prefix-length* 配置可以分配的前缀池。
- 接口模式下，使用 **ipv6 nd prefix pool** *pool-name*，配置接口绑定的前缀池名称。

检验方法

- 通过 **show running-config** 命令查看配置是否正确。

相关命令

配置接口绑定的前缀

【命令格式】 **ipv6 local pool** *pool-nameipv6-prefix/prefix-length prefix-length*

【参数说明】 -

【命令模式】 接口模式

【使用指导】 pool-name 为使用 **ipv6 local pool** *pool-nameipv6-prefix/prefix-length prefix-length* 配置的前缀池。

配置举例

配置接口绑定的前缀

【配置方法】 配置 GigabitEthernet 0/1 口的接口绑定前缀为 ruijie，使得设备为 GigabitEthernet 0/1 下的用户分配不同的基于 ruijie 前缀的地址前缀。

```
Ruijie(config)# ipv6 local pool ruijie 2409:88A0:8205::/48 64
Ruijie(config)# interfaceGigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ipv6 nd prefix pool ruijie
```

【检验方法】 通过 **show running-configinterface** GigabitEthernet 0/1 查看配置是否生效。

```
Ruijie#show running-config interface GigabitEthernet 0/1
ipv6 nd prefix pool ruijie
```

常见配置错误

无

1.6 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
清除动态学习到的邻居。	**clrear ipv6 neighbors** [**vrf***vrf-name*] [**oob**] [*interface-id*] **clrear ipv6 neighbors** [**vrf***vrf-name*] [*interface-id*] **clrear ipv6 neighbors** [*interface-id*]

清除动态路径 MTU	**clear ipv6 path-mtu** [**vrf***vrf-name*][*ipv6-address*] **clear ipv6 path-mtu**[*ipv6-address*] **clear ipv6 path-mtu all** 表示清除公网和所有 VRF 的动态路径 MTU

查看运行情况

作用	命令
显示接口上关于 IPv6 的信息	**show ipv6 interface**[[*interface-id*] [ra-info]] [brief [*interface-id*]]
显示邻居的信息	**show ipv6 neighbors[vrf***vrf-name*] [**verbose**][*interface-id*] [*ipv6-address*] [static] [oob] **show ipv6 neighbors[vrf***vrf-name*] [**verbose**][*interface-id*] [*ipv6-address*] [static] **show ipv6 neighbors** [**verbose**][*interface-id*] [*ipv6-address*] [static]
显示每个 MAC 地址的邻居表项的数量。	**showipv6 neighbor statistics per-mac** [*interface-name*] [*mac-address*]
显示路径 MTU	**show ipv6 path-mtu** [**vrf***vrf-name*][*ipv6-address* | **dynamic** | **static**] **show ipv6 path-mtu** [*ipv6-address* | **dynamic** | **static**]
显示路径 MTU 的统计信息	**show ipv6 path-mtu 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 ND 学习情况	**debug ipv6 nd**

配置指南-应用加速

本分册介绍应用加速相关内容，包括以下章节：

1. HTTP-AD
2. APP-CACHE

1 HTTP-AD

1.1 概述

HTTP-AD 是一种针对手机网页浏览的广告插入功能，对基于 http 协议的 html 类型网页源文件插入指定的广告脚本，达到运营目的。

协议规范

- 无

1.2 典型应用

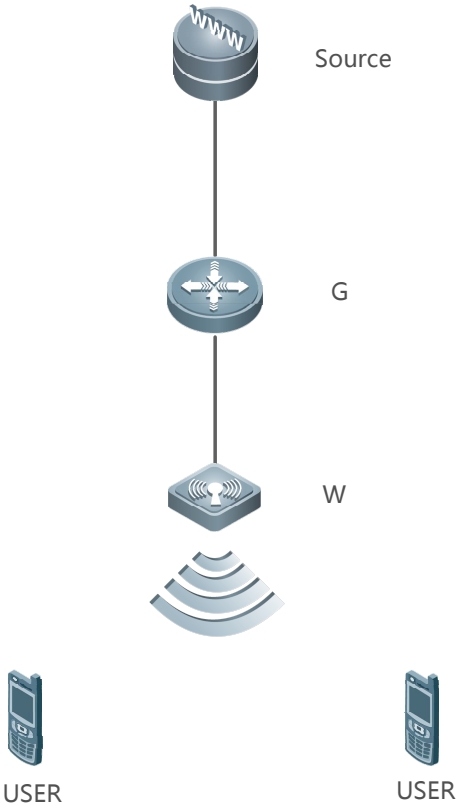
典型应用	场景描述
HTTP-AD 的典型应用场景	手机通过网关设备访问 html 网页

1.2.1 HTTP-AD典型应用场景

应用场景

手机通过网关设备访问 html 网页。

以下图 1-1 为例，手机连接无线设备，再通过网关设备访问 html 网页，网关设备对 HTTP 报文进行代理并插入广告脚本。最终在手机上弹出广告。



【注释】 G 为出口网关设备。
W 为无线设备，提供给用户手机连接。
Source 为 http 服务器。

功能部属

- 在网关设备开启加速功能
- 在网关设备上开启悬浮广告功能

1.3 功能详解

基本概念

↘ 基于端口的 TCP 代理

对特定的 TCP 流进行代理，在悬浮广告缓存场景中，对 http 协议流进行代理。http 协议默认端口为 80

↘ 插入广告脚本

对手机用户浏览的网页进行广告插入，使用户看到运营商的定制广告。

功能特性

功能特性	作用
悬浮广告	在手机访问的 html 网页中弹出广告
对 HTTP 协议报文进行代理	对特定的 TCP 流进行代理

1.3.1 悬浮广告

工作原理

手机用户通过 HTTP 协议浏览网页，对于 HTML 类型的页面，可以通过对报文的代理，在其应答报文中插入特定的广告脚本，达到在手机浏览器中显示特定广告的目的。

⚠ 广告脚本本身内容决定了广告显示的效果。另外，对于非 html 格式的页面无效，对于非 HTTP 协议（比如 HTTPS）不插入广告脚本。

相关配置

↘ 配置使能开关

缺省情况无配置。

配置 was 启用: **was enable**

配置悬浮广告启用: **was http ad enable**

↘ 配置使能开关

配置广告脚本链接：**was http ad url** *stirng*

1.3.2 对HTTP协议报文进行代理

工作原理

通过 TCP 代理功能，把报文送到用户空间，进行处理后再转发报文。通过配置特定端口，对此端口的流进行代理。http 协议的默认端口为 80

相关配置

↘ 配置 tcp 代理规则

缺省情况无配置。

1.4 配置详解

配置项	配置建议 & 相关命令	
配置悬浮广告开启	⚠ 必须配置。全局功能开启	
	was enable	全局开启 was 模块功能
	was http ad enable	开启悬浮广告功能
配置对 HTTP 协议进行代理	⚠ 必须配置。HTTP 协议报文进行代理	
	in-path rule auto-discovery dstport port 80 accelerate http rulenum start	配置 TCP 代理规则 ,针对 HTTP 协议主要配置 80 端口

1.4.1 配置悬浮广告开启

配置效果

- 全局启用 was 功能模块
- 全局启用 http-ad 功能
- 配置广告脚本 URL

注意事项

- 开启 was 时，因为涉及流表的修改操作，会提示重启设备

配置方法

1. 全局开启 was 功能模块

- 必须配置。未启动 was 功能模块，则悬浮广告无法工作。

【命令格式】 **was enable**
【参数说明】 -
【缺省配置】 was 模块关闭
【命令模式】 全局模式
【使用指导】 必须先启动 was 模块功能，才能启动悬浮广告功能。

2. 开启悬浮广告功能

- 必须配置。未启动悬浮广告功能，则悬浮广告无法工作。

【命令格式】 **was http ad enable**

【参数说明】 -

【缺省配置】 悬浮广告关闭

【命令模式】 全局模式

【使用指导】 此命令用来启动悬浮广告功能。

检验方法

- 使用 **show was status** 命令检查 was 模块是否开启

【命令格式】 **show was status**

【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 was 模块是否开启

【命令展示】

```
Ruijie(config)#show was status
was:on
```

- 使用 **show was http ad config** 命令查看悬浮广告的配置信息

【命令格式】 **show was http ad config**

【参数说明】 -

【命令模式】 特权模式、全局模式、接口模式

【使用指导】 查看悬浮广告模块的配置信息

【命令展示】

```
Ruijie(config)#show was http ad config
ad   status : on
ad   url    : http://rujie.com.cn/ad.js
```

配置举例

启用 HTTP-AD 功能

【配置方法】

- 在网关设备上开启 HTTP-AD 功能

```
Ruijie# configure terminal
Ruijie(config)# was enable
Ruijie(config)# was http ad enable
Ruijie(config)# was http ad url http://rujie.com.cn/ad.js
```

【检验方法】

- show was http ad config 查看功能是否开启命令

```
Ruijie# svr(config)#sh was status
was: on
Ruijie#show was http ad config
ad   status : on

ad   url    : http://rujie.com.cn/ad.js

```

常见错误

- 无

1.4.2 配置对HTTP协议进行代理

配置效果

- 基于 80 端口的 HTTP 流量会被代理

注意事项

-

配置方法

3. 配置基于 80 端口的 TCP 代理规则

- 必须配置，未配置 TCP 代理，则悬浮广告无法正常工作。

【命令格式】 **in-path rule auto-discovery dstport port 80 accelerate http rulenum start**
【参数说明】 **-**
【缺省配置】 无 TCP 代理
【命令模式】 全局模式
【使用指导】 使用此命令配置 TCP 代理

检验方法

- 使用 **show in-path rules** 命令检查是否配置基于 80 端口的 TCP 代理

【命令格式】 **show in-path rules**
【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 was 模块是否开启
【命令展示】

```
Ruijie#show in-path rules
Rule   Type O VLAN   App   Source Addr/Mask   Source port   Dest Addr/Mask   Dest port   description
1      auto N all    http  all                port:all      all              port:80
def    pass N all    none  all                port:all      all              port:all    any

(O) Optimization Policy:    F=Full D=DRE-only C=Compression-only M=DRE-M N=None
```

配置举例

↘ 配置代理 HTTP 协议流量

【配置方法】

- 配置基于 80 端口的 TCP 代理规则

```
Ruijie# configure terminal
Ruijie(config)# in-path rule auto-discovery dstport port 80 description http80  accelerate http
```

【检验方法】

- 查看 TCP 代理规则

```
Ruijie# show in-path rule
Rule   Type O VLAN   App    Source Addr/Mask   Source port    Dest Addr/Mask   Dest port
description
1      pass N all    none   all                port:all       all              name:Secure
Secure(bypass)
2      pass N all    none   all                port:all       all              name:Interactive
Interactive(bypass)
3      auto N all    http   all                port:all       all              port:all
http
4      auto N all    http   all                port:all       all              port:80
http80
def    pass N all    none   all                port:all       all              port:all
any
```

常见配置错误

1.5 监视与维护

清除各类信息

无

查看运行情况

作用	命令
查看悬浮广告的配置	**show was http ad config**
查看悬浮广告的当前状态	**show was http ad status**
查看 TCP 代理规则	**show in-path rule**

查看调试信息

无

2 APP-CACHE

2.1 概述

APP-CACHE 是一种针对手机应用下载的缓存功能 ,可以缓存所有安卓和苹果的应用文件 ,也可以只缓存指定厂家的应用文件。

协议规范

- 无

2.2 典型应用

典型应用	场景描述
APP-CACHE 的典型应用场景	手机通过网关设备到文件服务器中下载文件

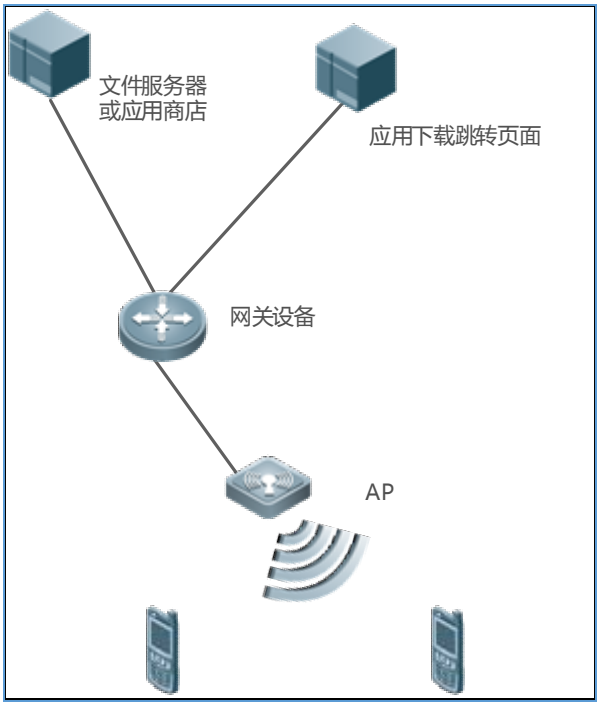
2.2.1 APP-CACHE典型应用场景

应用场景

如下图 2-1 所示，在商业 WIFI 场景中，经常需要手机用户下载指定的 APP 才能进行 WIFI 的应用认证， 在网关设备，对手机下载 app 安装文件进行缓存。使客户下载 APP 速度大大提高，提升了用户体验。

原始应用文件存储于文件服务器中，在有手机用户下载安装后，接下来的其它用户直接从设备上获取文件。

手机用户访问下载页面， 再跳转到文件服务器下载，通过此特性，可以对指定的应用进行缓存。



【注释】 -

功能部属

- 在网关设备开启加速功能
- 在网关设备上开启应用缓存功能
- 配置文件服务器或应用商店域名
- 配置应用下载跳转页面链接 URL

2.3 功能详解

基本概念

↘ 基于域名的 TCP 代理

对应用文件存储 TCP 流进行代理，在应用缓存场景中，特定服务器的 http 协议流进行代理。根据配置的域名及 URL，解析出服务器地址，代理访问服务器的 HTTP 会话。

↘ 应用缓存

对手机用户下载的应用软件安装包进行缓存，目前流行的手机系统是 Android 的 apk 文件和 Apple 的 ipa 文件，通过缓存，在用户发起重复下载时可以直接从本地网关设备上获取。

↘ 指定应用缓存

在免费 wifi 等应用场景中，使设备只对客户指定的应用文件进行缓存，不加速其它的应用下载。

功能特性

功能特性	作用
基于域名的 TCP 代理	对特定的 TCP 流进行代理
应用缓存	缓存 app 文件
缓存指定应用	只缓存指定的 app 文件

2.3.1 基于域名的TCP代理

工作原理

通过 TCP 代理功能，把报文送到用户空间，进行处理后再转发报文。通过配置应用文件存储服务器域名或 ip，针对性地对访问此服务器的流进行代理。

相关配置

↘ 配置域名

缺省情况无配置。

代理指定服务器的域名: **was http inpath domain** *string*

2.3.2 应用缓存

工作原理

手机用户通过 HTTP 协议下载应用安装文件，在第一次下载时，应用缓存模块识别出 URL 中含有 apk 或 ipa 的下载链接，则对应答的报文进行缓存，在第二次有用户下载同样的应用文件时，缓存命中，就在网关设备上构造应答报文并传给手机。

相关配置

↘ 配置使能开关

缺省情况无配置。

配置 was 启用: **was enable**

配置应用缓存启用: **was http app-cache enable**

2.3.3 缓存指定应用

工作原理

手机用户下载应用时，通常是先访问应用提供商的一个跳转（比如 portal 页）页面，然后点击对应的手机系统跳转到文件服务器或者应用商店进行下载。根据此操作规律，设定了 10 分钟的窗口时间，如果用户访问了指定应用的 url，就把其手机的 ip 记录，在 10 分钟内此 ip 发起的 ipa 或 apk 文件进行缓存功能处理，超过 10 分钟则不处理。

⚠ 基于对用户行为的预判，如果用户行为不符合，则可能缓存到其它应用或者不缓存，此情况下，只是缓存功能不生效，不影响用户的实际使用。

相关配置

↘ 缓存指定应用

缺省情况无配置。无配置情况下，会缓存所有的应用

配置应用下载页面链接: **was http app-cache url** *string*

2.4 产品说明

NBR108G-P、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR800G、NBR950G、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1500G、NBR2000G 不支持资源缓存下载命中， NBR1000G-E、NBR6120-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持资源缓存下载命中。

NBR108G-P、NBR800G、NBR950G、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1500G、NBR2000G 不支持支持浮窗功能， NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR1000G-E、NBR6120-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持支持浮窗功能。

NBR108G-P、NBR800G、NBR950G、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1500G、NBR2000G 不支持支持应用缓存（苹果，安卓）， NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR1000G-E、NBR6120-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持应用缓存（苹果，安卓）。

NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持本机缓存文件下载以及应用缓存（windows 补丁、360 卫士补丁、电脑管家补丁）; NBR108G-P、NBR800G、NBR950G、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1500G、NBR2000G 不支持本机缓存文件下载以及应用缓存（windows 补丁、360 卫士补丁、电脑管家补丁）。

2.5 配置详解

配置项	配置建议 & 相关命令	
配置 app-cache 开启	⚠ 必须配置。全局功能开启	
	was enable	全局开启 was 模块功能
	was http app-cache enable	开启 app 缓存功能
配置文件下载服务器域名或 ip	⚠ 必须配置。指定文件服务器,对目的服务器的报文进行 tcp 代理	
	was http inpath domain *string*	配置文件服务器域名
配置应用文件匹配规则	⚠ 可选配置。修改缓存匹配规则	
	was http app-cache rule type *string*	配置匹配的文件类型
	was http app-cache rule key *string*	配置 url 匹配算法
配置缓存指定应用	⚠ 可选配置。配置只缓存指定应用	
	was http app-cache url *string*	配置应用下载页面的 url

2.5.1 配置app-cache开启

配置效果

- 全局启用 was 功能模块
- 全局启用 app-cache 功能

注意事项

- 开启 was 时，因为涉及流表的修改操作，会提示重启设备

配置方法

- 必须配置

检验方法

- TCP 流被成功代理到 was 模块

相关命令

↘ **配置 was 功能**

【命令格式】 **was enable**
【参数说明】 -
【命令模式】 全局配置模式
【使用指导】

配置 app-cache 功能

【命令格式】 **was http app-cache enable**
【参数说明】 -
【命令模式】 全局配置模式
【使用指导】 开启 app-cache 缓存功能

配置举例

开启 APP-CACHE 功能

【配置方法】
- 在网关上开启 APP-CACHE 功能

```
Ruijie# configure terminal
Ruijie(config)# was enable
Ruijie(config)# was http app-cache enable
```

【检验方法】
- show was http app-cache config 查看功能是否开启命令

```
Ruijie# svr(config)#sh was status
was: on
Ruijie (config)#show was http app-cache config
app-cache : on
```

常见错误

- 无

2.5.2 配置文件下载服务器域名或ip

配置效果

- 访问下载服务器的 http 流量会被代理

注意事项

- 如果配置域名，需保证 dns 服务器正确配置

配置方法

- 必须配置

检验方法

- 访问指定域名的 HTTP 流被代理

相关命令

配置文件下载服务器域名或 ip

【命令格式】 **was http inpath domain** *string*

【参数说明】 *string*：域名或 ip

【命令模式】 全局配置模式

【使用指导】 配置 app-cache 的下载服务器

配置举例

配置域名作为文件下载服务器

【配置方法】 1.根据域名配置文件服务器

```
Ruijie# configure terminal
Ruijie(config)# was http inpath domain itunes.apple.com
```

【检验方法】 1. 从 apple 应用商店下载应用 http://www.ruijie.com 上下载 apk/文件(ipa)可以被缓存

```
Ruijie#show was http inpath domain
inpath domain: www.ruijie.com
        70.39.84.230
```

配置 ip 做为文件服务器

【配置方法】 1.根据 ip 配置文件服务器

```
Ruijie# configure terminal
Ruijie(config)# was http inpath domain 10.0.0.10
```

【检验方法】 1. 从 10.0.10 上使用 http 下载应用 http://www.ruijie.com 上下载 apk/文件(ipa 或 apk)可以被缓存

```
Ruijie#show was http inpath domain
inpath domain: 10.0.0.10
        10.0.0.10
```

常见配置错误

-

2.5.3 配置应用文件类型匹配规则

配置效果

- 通过配置匹配规则决定缓存文件的类型或者 URL 的匹配算法

注意事项

-

配置方法

- 可选配置
- 根据用户指定的规则进行文件缓存

检验方法

- 配置规则对应用文件缓存生效

相关命令

↘ 配置文件类型

【命令格式】 **was http app-cache rule type** *string*
【参数说明】 *string*: 文件类型
【命令模式】 全局配置模式
【使用指导】 根据需要缓存的文件类型进行配置

↘ 配置认证 URL

【命令格式】 **was http app-cache rule key** *string*
【参数说明】 *string*: 匹配算法
【配置模式】 全局配置模式
【使用指导】 $host, $path, $name, $args 可进行组合，分别对应 url 中的几个元素

配置举例

↘ 配置缓存 exe 文件

【配置方法】 1.配置支持 exe 类型文件的缓存功能

```
Ruijie# configure terminal
Ruijie(config)# was http app-cache rule type exe
Ruijie(config)# end
```

【检验方法】 下载 exe 格式文件，可被缓存

↘ 配置 URL 匹配算法，只匹配特定的 host 及文件名

【配置方法】 1.配置特定的 host 和文件名

```
Ruijie# configure terminal
Ruijie(config)# was http app-cache rule key $host$name
```

【检验方法】 只有特定 host 中的文件被缓存

2.5.4 配置缓存指定应用-时间窗

配置效果

- 只缓存特定的应用，并不缓存其它应用

注意事项

算法基于对用户行为的预测，并非百分百严谨

配置方法

- 可选配置
- 通过配置应用提供者的下载跳转页面来指定应用

检验方法

- 访问过跳转页面后 10 分钟内下载的应用才被缓存

相关命令

↘ 设置应用下载页面的 url

【命令格式】 **was http app-cache url** *string*

【参数说明】 *string:* 应用下载页面的 url

【命令模式】 全局配置模式

【使用指导】 -

配置举例

↘ 设置无需认证用户 IP 范围

【配置方法】

- 设置应用下载页面的 url

```
Ruijie (config)# was http app-cache url http://rujie.com.cn/appdownload.html
```

【检验方法】

- show was http app-cache config 查看

```
Ruijie#show was http app-cache config
app-cache url num 1:
    0      http://rujie.com.cn/appdownload.html
```

- 模拟下载应用操作，观察缓存情况

2.5.5 配置缓存指定应用-url特征

配置效果

- 只缓存特定的应用，并不缓存其它应用

注意事项

-

配置方法

- 可选配置
- 通过配置 url 特征字符串来指定应用

检验方法

- 下载指定 url 可缓存，其它则不缓存

相关命令

↘ 设置应用下载页面的 url

【命令格式】 **was http app-cache match url** *string*
【参数说明】 *string*：*文件* url 中的特征字符串
【命令模式】 全局配置模式
【使用指导】 -

配置举例

↘ 设置无需认证用户 IP 范围

【配置方法】
- 设置应用下载页面的 url 特征字符

```
Ruijie (config)# was http app-cache match url ruijie
```

【检验方法】
- show was http app-cache config 查看
- 模拟下载应用操作，观察缓存情况

2.5.6 配置缓存指定应用-应用名

配置效果

- 只缓存特定的应用，其它则不缓存

注意事项

-

配置方法

- 可选配置
- 通过配置应用名指定缓存应用

检验方法

- 下载指定应用名的资源可缓存，其它则不缓存

相关命令

↘ 设置应用下载页面的 url

【命令格式】 **was http app-cache app-name** *string*
【参数说明】 *string*：应用名

【命令模式】 全局配置模式
【使用指导】 -

配置举例

↘ 设置无需认证用户 IP 范围

【配置方法】
- 设置应用下载页面的 url

```
Ruijie (config)# was http app-cache match app-name testapp
```

【检验方法】
- show was http app-cache config 查看

```
Ruijie#show was http app-cache config
```

- 模拟下载应用操作，观察缓存情况

2.6 监视与维护

清除各类信息

无

查看运行情况

作用	命令
查看配置	**show was http app-cache config**
查看当前状态	**show was http app-cache status**
查看多线程下载的状态	**Show was http app-cache muldownload status**
查看缓存文件数据库	**show was http app-cache database**
查看域名配置	**show was http inpath domain**

查看调试信息

无

WLAN 基础配置

本分册介绍 WLAN 基础配置相关内容，包括以下章节：

1. APMG
2. STAMG
3. CAPWAP
4. WBS
5. ETH-MNG
6. DATA-PLANE
7. WLOG

1 APMG

1.1 概述

APMG（AP Management）主要针对集中管理型无线网络架构，负责对 AP 的集中管理与配置。

WLAN（Wireless Local Area Network，无线局域网）是通过无线通信技术将计算机设备互联起来，构成可以互相通信和实现资源共享的网络体系。无线局域网本质的特点是不再使用通信电缆将计算机与网络连接起来，而是通过无线的方式连接，从而使网络的构建和终端的移动更加灵活。

传统无线局域网采用胖 AP 的网络架构，各个 AP 独立工作。一方面需要对网络中每个 AP 进行独立的配置与管理，增加了无线网络管理的复杂度与运维工作量；另一方面由于 AP 间难以进行有效的协作，导致 AP 间的射频干扰、无线用户漫游等问题难以得到有效解决方案。针对这些问题，出现了由 AC 与瘦 AP 组成的集中管理型无线网络架构（也称为瘦 AP 网络架构），AP 通过 CAPWAP 隧道与 AC 建立连接，由 AC 对 AP 进行集中管理控制。

协议规范

- RFC5415：Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification
- RFC5416：Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11

1.2 典型应用

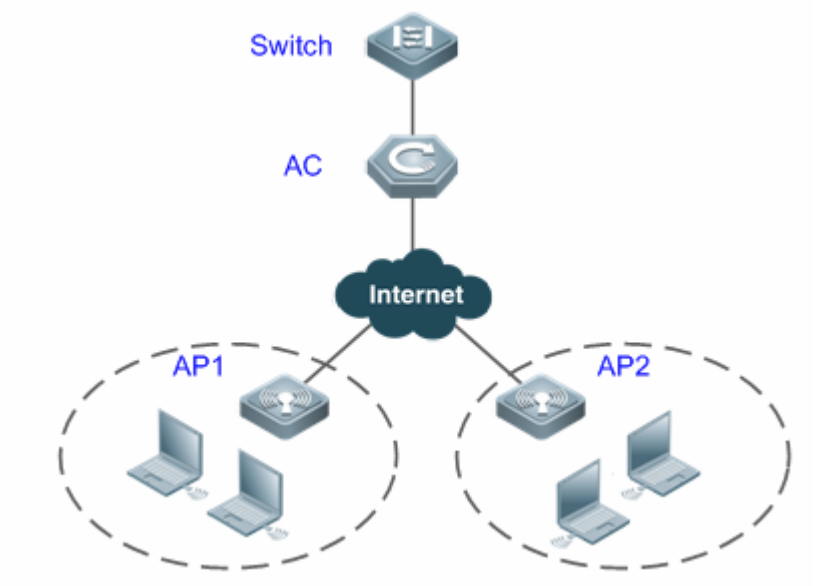
典型应用	场景描述
瘦 AP 网络架构	采用有线交换机+无线控制器（Access Controller，AC）+瘦 AP 的组网方式

1.2.1 瘦AP网络架构

应用场景

瘦 AP 无线技术是采用有线交换机+无线控制器（Access Controller，AC）+瘦 AP 的组网方式，即 AP 作为简单的无线接入点，不具备管理控制功能，而通过无线控制器（AC）统一管理所有 AP，向指定 AP 下发控制策略，无需在各 AP 上单独配置。如下图所示，AC 通过 CAPWAP 隧道与多个 AP 相连，用户只需在 AC 上对所关联的 AP 进行配置管理。

图 1-1 简单瘦 AP 组网拓扑



【注释】 Switch 为交换机设备。
AC 为 AC 设备。
AP1、AP2 为瘦 AP 模式的 AP 设备。

功能部署

- 为 AP 配置具有指示性的名称，之后便可以通过名称对 AP 进行配置。
- 创建 WLAN，配置 WLAN 相关属性。
- 创建 AP 组，将 AP 加入指定 AP 组，之后便可以通过 AP 组对该 AP 组内所有 AP 进行统一配置。
- 通过 AP 组配置，将 WLAN 部署到 AP 组内所有 AP 上，之后 AP 便可以对外提供 WLAN 接入服务，无线终端用户可以接入 WLAN，使用无线网络。

1.3 功能详解

基本概念

AP

AP（Access Point）：无线终端访问有线网络的接入点，相当于无线终端与有线网络通信的桥梁。

AC

AC（Access Control）：无线控制器通过有线网络与 AP 相连，用于集中管理控制 AP。

AC 集群功能

AC 集群功能，又称为 AC 冗余功能，是指通过为 AP 指定多个具有优先级的 AC，当 AP 到高优先级 AC 的连接不通的时候，AP 就可以使用低优先级的 AC（(备用 AC)），当高优先级 AC 的连接恢复时，断开与低优先级 AC 的 CAPWAP 隧道，重新与高优先级 AC 建立 CAPWAP 隧道。

功能特性

功能特性	作用
AC 参数的配置	对 AC 的名称、发送 trap 信息的开关等进行配置
AP 参数的配置	对 AP 的名称、Telnet 用户名密码、定期报告统计信息的时间间隔等参数进行配置
AP 行为的配置	配置 AP 每天定时重启、恢复出厂配置、AP 复位等
AP 组管理	通过 AP 组对 AP 进行管理，减少逐个 AP 配置的配置工作量
AP 数限制	限制本 AC 允许接入的最大 AP 数
AP 合规性检查	基于 MAC 绑定的 AP 接入控制功能
AP 接入认证	实现对 AP 接入的认证
AP 优先级功能	基于优先级的 AP 接入控制功能
AC 集群功能	通过 AC 集群实现 AC 冗余，降低 AC 单点故障风险，提高无线网络可用性
配置 WLAN	配置创建 WLAN，并将 WLAN 部署到 AP 上，为无线用户提供网络服务
AP 备份功能	配置 AP 备份功能，提高无线网络可用性

1.3.1 AC参数的配置

AC 参数的配置包括 AC 的名称、AC 发送 trap 信息的开关、AC 的接入地编号等。

工作原理

AC 的参数配置不涉及工作原理。

1.3.2 AP参数的配置

AP 的参数配置包括 AP 的名称、Telnet 用户名密码、定期报告统计信息的时间间隔等。

工作原理

AC 设备上对 AP 的参数配置主要通过 CAPWAP 报文向 AP 下发。

1.3.3 AP行为的配置

AP 行为的配置包括 AP 每天定时重启、AP 恢复出厂配置、AP 复位。

工作原理

AP 行为的配置主要通过 CAPWAP 报文向 AP 下发，由 AP 根据 AC 下发的配置执行相应的行为。

1.3.4 AP组管理

通过 AP 组对 AP 进行管理，可以实现通过 AP 组向该 AP 组内所有 AP 进行配置，从而减少配置工作量。AP 组的配置对组内所有 AP 生效。对于同一配置，如果同时存在基于 AP 的配置和基于 AP 组的配置，则基于 AP 的配置优先生效。

工作原理

系统自动创建一个默认的 AP 组，名称为 default 组。AP 缺省加入 default 组。可以根据创建 AP 组，将 AP 加入 AP 组，对 AP 进行分组管理。

1.3.5 AP数限制

AP 数限制功能是指可以通过配置 AC 允许接入的最大 AP 数，来限制接入 AP 的最大数，控制 AC 的最大 AP 负载，避免 AC 的负载过高。

工作原理

当 AC 的接入 AP 数达到最大值时，不再允许新的 AP 接入。

我司的 WALL-AP 系列产品在接入数限制上被当作半台设备处理，即该型号的 AP 的接入上限是系统 AP 支持能力的两倍。

1.3.6 AP合规性检查

AP 合规性检查，也称为“基于 MAC 地址绑定的 AP 接入控制”。开启 AP 合规性检查，可以实现只允许某些指定 MAC 地址的 AP 接入，从而避免计划外 AP 的接入，增加无线网络安全性。

工作原理

在 AP 接入时，只有在本 AC 上有该 AP 的 MAC 地址绑定的 AP 配置存在时，才允许该 AP 接入。否则，不允许其接入。为避免对大量 AP 配置 MAC 地址绑定，在 AP 合规性检查开启时，将自动对所有当前在线的 AP 进行 MAC 地址绑定。同时，也支持对指定 AP 配置 MAC 地址绑定。

1.3.7 AP接入认证

AP 接入认证支持基于系列号的接入认证、基于密钥的接入认证和基于证书的接入认证。通过 AP 接入认证可以实现只有得到授权的 AP 才能接入。

工作原理

在 AP 请求接入时，上传认证信息，AC 对其认证信息进行认证校验，只允许认证通过的 AP 接入。

1.3.8 AP优先级功能

AP 优先级功能属于 AP 数限制功能高级版本。AP 优先级功能可以实现在 AC 当前 AP 数达到上限时，如果有高优先级的 AP 请求接入时，通过 AC 主动对低优先级的 AP 做下线处理，实现高优先级 AP 的接入。

工作原理

在 AP 请求接入时，如果当前 AP 数达到上限且 AP 优先级功能开启，则进行优先级的比对，如果存在在线 AP 优先级低于当前请求 AP，则对低优先级 AP 做下线处理，允许高优先级 AP 接入。

1.3.9 AC集群功能

集群功能一方面通过 AC 冗余来增强 AC 集群的可靠性，另一方面通过优先级来控制稳定情况下 AP 所归属的 AC，便于 AP 的管理。

工作原理

参见 CAPWAP 标准（RFC5415）。

1.3.10 配置WLAN

配置 WLAN 的创建并部署到 AP 上，实现 AP 对外提供 WLAN 接入服务。

工作原理

AC 上创建的 WLAN 主要用于对 WLAN 的参数的配置。WLAN 部署信息和参数的下发主要通过 CAPWAP 标准定义的报文下发。

1.3.11 AP备份功能

AP 备份功能，是在物理部署上位置相近、覆盖范围存在重叠、放出不同无线新信号的 AP 之间的备份，备份内容是放出的无线信号。当放出重要无线信号的 AP 出现故障时，一个或者多个备份 AP 放出故障 AP 的无线信号，接替故障 AP 继续工作，保证我司无线信号的稳定性。该功能一般使用在比较特殊的场景，如医疗行业零漫游场景下，覆盖范围广的 AP4210 是一个重要的 AP，其下联的 APD-M 作为备份 AP。

工作原理

AC 上创建 AP 备份组 ,并选定主 AP ,其余的为备份 AP ,当主 AP 出现故障而掉线时 ,向组内所有备份 AP 下发主 AP 的 WLAN 配置，使备份 AP 放出主 AP 的无线信号。

1.4 产品说明



NBR800G、NBR950G、NBR1500G、NBR2000G 不支持无线集成 AC 功能 ;NBR108G-P、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持无线集成 AC 功能。

1.5 配置详解

配置项	配置建议 & 相关命令	
配置 AC 的名称	可选配置，可以将 AC 名称配置为具有指示性的名称，便于管理。	
	ac-name	配置本 AC 的名称
配置 AC 发送 trap 信息的开关	可选配置，可以通过该命令开启 trap 信息发送，通过接收 trap 信息实现网络运维管理。	
	acctrl-trap	配置本 AC 是否发送指定 trap 信息
配置 AC 接入地编号	可选配置，缺省为 AC MAC 地址点分形式字符串	
	nas-id	AC 配置模式，配置本 AC 接入地编号
创建 AP 配置	可选配置，通过创建对应名称的 AP 配置，对指定 AP 进行配置	
	ap-config	添加 AP 配置/进入 AP 配置模式
创建 AP 组	可选配置，AP 组配置模式下命令对该 AP 组下所有在线 AP 有效。	
	ap-group	添加 AP 组配置/进入 AP 组配置模式
配置 AP 所属的 AP 组	可选配置，在 AP 配置模式下配置，可以对指定 AP 进行所属 AP 组的配置，缺省属于 default 组。	
	ap-group	配置 AP 所属的 AP 组

配置 AP 的名称	可选配置，可以根据需要为 AP 配置新的名称。	
	ap-name	配置 AP 的名称
配置 AP 的 MAC 地址绑定	可选配置，配置 MAC 地址绑定可实现 AP 配置强制在对应 MAC 地址的 AP 上生效。	
	ap-mac	配置指定 AP 配置的 MAC 地址绑定
配置 AP 的用户名和密码	可选配置，可以根据需要修改 AP 的 Telent 用户名和密码。	
	credential	配置 AP 的用户名和密码
配置 AP 定期报告统计信息的时间间隔	可选配置，标准规定该时间间隔默认值为 120 秒，可根据需要配置。	
	statistics-timer	配置 AP 定期报告统计信息的时间间隔
配置 AP 每天定时重启的时间	可选配置，通过配置 AP 每天定时重启可以避免 AP 长时间工作。	
	reload at	配置 AP 每天定时重启
配置指定 AP 恢复出厂配置	可选配置，实现 AP 恢复出厂配置。	
	factory-reset	配置指定 AP 恢复出厂配置
配置 AP 复位	可选配置，可触发 AP 复位。	
	reset	配置 AP 复位
配置 AP 数限制	可选配置，可以根据需要配置本 AC 允许接入的最大 AP 数，减少 AC 的最大负荷。	
	wtp-limit	配置本 AC 允许接入的最大 AP 数
配置 AP 合规性检查	可选配置，通过开启 AP 合规性检查功能可以实现只有绑定有 MAC 地址的 AP 才能接入，实现对 AP 接入的有效控制。	
	bind-ap-mac	AC 配置模式，配置开启/关闭 AP 合规性检查功能
配置 AP 接入认证	可选配置，通过配置 AP 接入认证，可以实现只有合法 AP 能够接入，增加无线网络安全性	
	ap-auth enable	AC 配置模式，配置本 AC 的 AP 接入认证功能开启与否
	ap-auth serial-update	AC 配置模式，配置所有在线 AP 更新认证序列号
	ap-auth	AP 配置模式，指定 AP 的接入认证相关配置
配置 AP 优先级功能	可选配置，该命令在 AC 配置模式和 AP 配置模式下均存在。	
	ap-priority	AC 配置模式，配置本 AC 是否开启 AP 接入优先级功能
	priority	AP 配置模式，配置指定 AP 的 Failover 优先级
配置 AP 系统日志信息	可选配置，AP 配置模式下，配置指定 AP 或者所有 AP 的日志信息。	
	logging on	配置系统日志显示开关
	logging server	配置系统日志服务器地址
创建 WLAN	可选配置，配置 WLAN 部署之前，需要先创建 WLAN	

	wlan-config	创建 WLAN 配置/进入 WLAN 配置模式
配置 WLAN 部署	⚠ 可选配置，配置指定 AP 组的 WLAN-VLAN 映射的同时，对于 WLAN 将部署到 AP 组内所有 AP 上	
	interface-mapping	AP 组配置模式，配置指定 AP 组的 WLAN-VLAN 映射
配置 WLAN SSID 广播开关	⚠ 可选配置，缺省情况未开启 SSID 广播，可根据需要关闭	
	enable-broad-ssid	WLAN 配置模式，配置指定 WLAN 开启/关闭 SSID 广播
配置 WLAN 用户接入地编号	⚠ 可选配置，缺省为空字符串	
	nas-id	WLAN 配置模式，配置指定 WLAN 用户接入地编号
配置 WLAN SSID 名字	⚠ 可选配置，可以根据需要为 WLAN 配置新的 SSID 名字	
	ssid	WLAN 配置模式，修改 WLAN 的 SSID 名字
配置 AP 备份功能	⚠ 可选配置，用于提高无线网络的可用性	
	ap-backup group	AC 配置模式下，创建 AP 备份组
	ap-backup-group	绑定 AP 备份组

1.5.1 配置AC的名称

配置效果

- 配置 AC 的名称为指定字符串。

注意事项

- 最多可配置 63 个字符，不能包含空格。

配置方法

- 可选配置，使用 AC 配置模式下 **ac-name** *ac-name* 命令，可以根据需求为 AC 配置新的名称。
- 提供命令 **ac-controller** 进入 AC 配置模式。
- AC 设备上，AC 配置模式下，通过 **ac-name** 命令进行 AC 名称的配置。

【命令格式】 **ac-controller**
【参数说明】 -
【缺省配置】 无
【命令模式】 全局配置模式
【使用指导】 -

【命令格式】 **ac-name** *ac-name*

no ac-name

【缺省配置】 AC 名称的缺省值为 Ruijie_Ac_MAC 地址后六位，例如 AC 的 MAC 地址为 001a.a916.e7b8，则其缺省名称为 Ruijie_Ac_16e7b8

【参数说明】 *ac-name*：配置该 AC 的名称描述符，最多可配置 63 个字符，不能包含空格。

【命令模式】 AC 配置模式

【使用指导】 可以给不同的 AC 配置不同的名称便于管理。

AC 名称的缺省值为 Ruijie_Ac_MAC 地址后六位，例如 AC 的 MAC 地址为 001a.a916.e7b8，则其缺省名称为 Ruijie_Ac_16e7b8

检验方法

- 通过 **show ac-config** 命令查看当前 AC 名称，确认是否配置成功。

配置举例

配置 AC 的名称为 Ruijie-AC1

【配置方法】
- 进入 AC 配置模式
- 配置 AC 的名称
- 通过 no 命令可以恢复 AC 名称为缺省值

AC

```
Ruijie(config)#ac-controller
Ruijie(config-ac)#
Ruijie(config-ac)#ac-name Ruijie-AC1
Ruijie(config)#ac-controller
Ruijie(config-ac)#no ac-name
```

【检验方法】 通过 **show ac-config** 命令可以查看当前 AC 名称。

AC

```
Ruijie#show ac-config

ac_name          :Ruijie-AC1
```

常见错误

- 无。

1.5.2 配置AC发送trap信息的开关

配置效果

- AC 对外发送的 trap 信息包括：CAPWAP 隧道 up/down 信息、AP 加入 AC 失败信息、CAPWAP 隧道报文解密失败信息、AP 升级失败信息、时间同步失败信息、STA 上下线信息。
- 缺省情况下，上述所有 trap 信息的发送都是关闭的，通过 AC 配置模式下 **acctrl-trap** 命令打开，则相应的 trap 信息发送将开启。

注意事项

- 无。

配置方法

- 可选配置。AC 设备上，进入 AC 配置模式，通过 **acctrl-trap** 命令进行配置。
- AC 对外发送的 trap 信息包括：CAPWAP 隧道 up/down 信息、AP 加入 AC 失败信息、CAPWAP 隧道报文解密失败信息、AP 升级失败信息、时间同步失败信息、STA 上下线信息。

【命令格式】 **acctrl-trap** [**acap-updown-ctrl** | **acap-joinfail-ctrl** | **acap-decryeroreport-ctrl** | **acap-imageupdt-ctrl** | **acap-timestamp-ctrl** | **acsta-oper-ctrl**]

【参数说明】 **acap-updown-ctrl**：用来控制 CAPWAP 隧道 up/down 的 trap 消息的发送
acap-joinfail-ctrl：用来控制 AP 加入 AC 失败的 trap 消息的发送
acap-decryeroreport-ctrl：用来控制 CAPWAP 隧道报文解密失败的 trap 消息的发送
acap-imageupdt-ctrl：用来控制 AP 的 bin 文件升级的 trap 信息的发送
acap-timestamp-ctrl：用来控制时间同步的 trap 信息的发送
acsta-oper-ctrl：用来控制 STA 上下线的 trap 信息的发送

【缺省配置】 缺省情况下，所有 trap 的控制开关是关闭的，可以通过 AC 配置模式下 **acctrl-trap** 命令打开

【命令模式】 AC 配置模式

【使用指导】 用来控制 AC 上相关 trap 的开关。

检验方法

- 通过 **show ac-config** 命令查看当前各种类型 trap 的开关状态。

配置举例

↘ 配置 AC 开启 AP 加入 AC 失败的 trap 消息的发送.

【配置方法】
- 进入 AC 配置模式
- 配置 AC 开启 AP 加入 AC 失败的 trap 消息的发送
- 通过 no 命令可以恢复缺省值

AC

```
Ruijie(config)#ac-controller
Ruijie(config-ac)#acctrl-trap acap-joinfail-ctrl
Ruijie(config)#ac-controller
```

```
Ruijie(config-ac)#no acctrl-trap acap-joinfail-ctrl
```

【检验方法】 通过 **show ac-config** 命令可以查看当前各种类型 trap 的开关状态。

AC

```
Ruijie#show ac-config
acctrl-trap acap-updown-ctrl            :Disable
acctrl-trap acap-joinfail-ctrl          :Enable
acctrl-trap acap-decryeroreport-ctrl    :Disable
acctrl-trap acap-imageupdt-ctrl         :Disable
acctrl-trap acap-timestamp-ctrl         :Disable
acctrl-trap acsta-oper-ctrl             :Disable
```

常见错误

- 无。

1.5.3 配置AC接入地编号

配置效果

- 在 WLAN 网络中，AC 接入地编号（NAS-ID）可用于区分不同的热点区域。缺省情况下 AC 接入地编号为 AC MAC 地址点分形式字符串。

注意事项

- 无。

配置方法

- 可选配置。
- AC 设备上，进入 AC 配置模式，通过 **nas-id** 命令进行配置。

【命令格式】 **nas-id** *ac-nas-id*

no nas-id

【参数说明】 -

【缺省配置】 AC MAC 地址点分形式字符串

【命令模式】 AC 配置模式

【使用指导】 无。

检验方法

- 通过 **show running** 查看 AC 配置。

配置举例

↘ 配置 AC 接入地编号为 123456789

【配置方法】
- 进入 AC 配置模式
- 配置 AC 接入地编号

AC

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# nas-id 123456789
```

【检验方法】 通过 **show running** 可查看 AC 配置

AC

```
Ruijie#show running
!
ac-controller
 nas-id 123456789
!
```

常见错误

- 无。

1.5.4 创建AP配置

配置效果

- 创建指定名称的 AP 配置后，进入 AP 配置模式。
- 如果该名称对应的 AP 配置已经存在，则直接进入 AP 配置模式。
- **ap-config** 携带的参数 *ap-name* 称为 AP 配置名称。AP 上线时，通过 AP 上传的自身名称与 AP 配置名称匹配，来决定 AP 设备与 AP 配置的一一对应关系。

注意事项

- 无。

配置方法

- 可选配置。
- AC 设备上，在全局配置模式，通过 **ap-config** *ap-name* 命令创建 AP 配置

【命令格式】 **ap-config** *ap-name*

【参数说明】 *ap-name*：AP 配置名称

【缺省配置】 无 AP 配置

【命令模式】 全局配置模式

【使用指导】 1.用户可以通过命令 **ap-config all** 命令进入所有 AP 的配置模式，在该模式下的配置将会对与本 AC 关联的所有 AP 生效。指定 AP 配置模式下的配置优先级高于所有 AP 配置模式下配置。如果 **ap-config** *ap-name* 配置模式下存在配置（即，非默认配置），则优先使用该配置；否则，将继承 **ap-config all** 配置模式下的配置。

2.用户可以通过 **no ap-config** *ap-name* 命令删除指定 AP 配置，如果该配置对应 AP 已经在线，则删除配置将触发该 AP 下线后上线。

3.用户可以通过命令 **no ap-config all** 命令删除本 AC 上所有离线 AP 配置。

检验方法

- 通过 **show ap-config running** *ap-name* 命令可以查看该 AP 配置。

配置举例

创建名称为 Ruijie_AP 的 AP 配置

【配置方法】
- 创建名称为 Ruijie_AP 的 AP 配置

AC

```
Ruijie(config)#ap-config Ruijie_AP
You are going to config AP(Ruijie_AP), which is not on line now.
Ruijie(config-ap)#
```

【检验方法】 通过 **show ap-config running** 命令可以查看该 AP 配置。

AC

```
Ruijie#show ap-config running Ruijie_AP
!
ap-config Ruijie_AP
!
```

常见错误

- 无。

1.5.5 创建AP组

配置效果

- 通过 AP 组对 AP 进行管理，可以实现通过 AP 组向该 AP 组内所有 AP 进行配置，从而减少配置工作量。AP 组的配置对组内所有 AP 生效。

注意事项

- default 组为系统自动创建，不可删除。
- 删除 AP 组时，属于该 AP 组的 AP 将自动切换到 default 组。
- 对于在 ap-config 和 ap-name 配置模式，ap-config all 配置模式和 ap-group 配置模式下均存在的配置，按照“ap-config ap-name 高于 ap-group，ap-group 高于 ap-config all”的优先级生效。

配置方法

- 可选配置。
- AC 设备上，通过全局配置模式下 **ap-group** *ap-group-name* 命令可以创建 AP 组

【命令格式】 **ap-group** *ap-group-name*

no ap-group *ap-group-name*

【参数说明】 *ap-group-name*：AP 组名。

【缺省配置】 缺省情况下，系统启动后会自动创建一个默认 AP 组（组名为：default），该组不可创建、不可删除

【命令模式】 全局配置模式

【使用指导】 通过 **no** 前缀删除 AP 组时，属于该 AP 组的 AP 将自动切换到 default 组。

检验方法

- 通过 **show running** 命令可查看所有 AP 组配置。

配置举例

↘ 创建名称为 APG-1 的 AP 组

【配置方法】
- 全局配置模式下，通过 ap-group 命令创建 AP 组

AC

```
Ruijie(config)#ap-group APG-1
Ruijie(config-ap-group)#
```

【检验方法】 通过 **show running** 命令可以看到 AP 组 APG-1

AC

```
Ruijie#show running
!
ap-group APG-1
!
```

常见错误

- 无。

1.5.6 配置AP所属的AP组

配置效果

- 配置 AP 属于某个指定的 AP 组，要求该 AP 组已经存在。
- 缺省情况下，AP 属于默认 AP 组（默认 AP 组的名称为 default）。
- AP 将继承所属 AP 组的配置。如果同一配置在指定 AP 配置（**ap-config** *ap-name*）、所有 AP 配置（**ap-config all**）和 AP 组配置中都存在，则按照“指定 AP 配置 > AP 组配置 > 所有 AP 配置”的优先级生效。因此，配置 AP 所属的 AP 组变化将可能导致该 AP 继承自 AP 组的配置发生变化。

注意事项

- 无。

配置方法

- 可选配置。
- 通过 **ap-config** 命令创建 AP 配置/进入 AP 配置模式。
- AC 设备上，进入 AP 配置模式，通过 **ap-group** 命令进行配置。

【命令格式】 **ap-config** *ap-name*
【参数说明】 *ap-name*：AP 配置名称
【缺省配置】 无
【命令模式】 全局配置模式
【使用指导】 无

【命令格式】 **ap-group** *ap-group-name*
no ap-group
【参数说明】 *ap-group-name*：AP 组名称
【缺省配置】 缺省情况下，AP 自动加入 default 组
【命令模式】 AP 配置模式
【使用指导】 删除 AP 组时，属于该 AP 组的 AP 将自动切换到 default 组。

检验方法

- 通过 **show ap-config running** 命令查看当前 AP 的配置。

配置举例

↘ 配置 Ruijie-AP1 属于 AP 组

【配置方法】
- 创建 AP 组 apg-1
- 进入 AP 配置模式
- 通过 no 命令可以恢复缺省 AP 组（default 组）

AC

```
Ruijie(config)#ap-group apg1
Ruijie(config-ap-group)#
Ruijie(config)#ap-config Ruijie-AP1
Ruijie(config-ap)#
Ruijie(config-ap)#ap-group apg-1
Ruijie(config)#ap-config Ruijie-AP1
Ruijie(config-ac)#no ap-group
```

【检验方法】 通过 **show ap-config running** 命令可以查看当前 AP 配置。

AC

```
Ruijie(config)#show ap-config running Ruijie-AP1
!
ap-config Ruijie-AP1
ap-group apg-1
!
```

常见错误

- 无。

1.5.7 配置AP的名称

配置效果

- **AC 设备上配置 AP 的名称：**

如果对应的 AP 在线，则 AP 名称的配置将即时生效，同时，AP 配置模式的名称（即 **ap-config** 后面的字符串）也将即时被新的名称替换。

如果对应的 AP 离线，则 AP 名称的配置将在对应 AP 上线时生效，而 AP 配置模式的名称将保持原名称直到对应 AP 上线该配置生效后。

配置 AP 名称后，无需退出 AP 配置模式即可继续对该 AP 进行配置。

如果对应的 AP 在线，不支持 **no** 命令。

如果对应的 AP 离线，则 **no** 命令将清除未生效的 AP 名称配置。

如果新的名称已经被使用，则配置不成功。

- **AP 设备上配置 AP 名称：**

如果 AP 还没有建立 CAPWAP 连接，则直接配置 AP 的名称。

如果 AP 已经建立了 CAPWAP 连接，先配置 AP 的名称，然后断开 CAPWAP 连接，重建隧道，如果 AC 上名称有配置或者有离线配置，那么还是以 AC 上的 AP 名称为准。

注意事项

- 最多可配置 64 个字符，不能包含空格
- 不能配置 AP 名称为“all”和“AP”。
- 应当在配置上避免对不同的离线 AP，配置相同的新名称。如果对不同的离线 AP 配置了相同的新名称，则最先上线的 AP 将以新的名称生效，后续上线的 AP 将保留原名称，无法使用新的名称。
- AP 设备上配置 AP 名称，只在瘦 AP 模式下生效。

配置方法

- 可选配置，可以根据需要通过 AP 配置模式下 **ap-name** *ap-name* 命令配置 AP 的名称，建议为 AP 配置具有指示性的名称，便于管理。
- AC 设备上，进入 AP 配置模式，通过 **ap-name** 命令进行配置。

【命令格式】 **ap-name** *name*
【参数说明】 *name*：配置 AP 的名称描述符，不能带空格。
【缺省配置】 AC 以 AP 上传的名称作为 AP 的名称。AP 的出厂配置一般采用 MAC 地址作为名称。
【命令模式】 AP 的配置模式
【使用指导】 1、请勿将 AP 命名为“all”和“AP”。
2、该命令执行后，在线 AP 的命令模式即为具有新 AP 名称的 AP 的命令模式，无需退出即可继续配置其他属性。离线 AP 的命令模式不变。

- AP 设备上，进入全局配置模式，通过 **ap-name** 命令进行配置。

【命令格式】 **ap-name** *name*
【参数说明】 *name*：配置 AP 的名称描述符，不能带空格。
【缺省配置】 AP 上默认”AP”作为 AP 的名称。
【命令模式】 AP 的全局配置模式
【使用指导】 1、请勿将 AP 命名为“all”。
2、该命令执行后， AP 重建 CAPWAP 隧道。

检验方法

- AC 设备通过 **show ap-config running** 命令查看当前 AP 配置情况。
- AC 设备通过 **show ap-config summary** 命令可以查看在线 AP 的名称是否为配置的新名称。
- AP 设备通过 show running-config 命令查看当前 AP 配置情况。

配置举例

配置在线 AP Ruijie-AC1 的名称为 Ruijie-AC2

【配置方法】
- 进入 AP 配置模式
- 配置 AP 的名称

AC

```
Ruijie(config)#ap-config Ruijie-AC1
Ruijie(config-ap)#ap-name Ruijie-AC2
```

【检验方法】
- 通过 show ap-config running 命令可以查看当前 AP 配置。
- 通过 show ap-config summary 命令查询在线 AP 当前名称。

AC

```
Ruijie#show ap-config running
!
ap-config Ruijie-AC2
!
Ruijie#show ap-config summary
========= show ap status =========
Radio: Radio ID or Band: 2.4G = 1#, 5G = 2#
       E = enabled, D = disabled, N = Not exist
       Current Sta number/Max Sta number supported
       Channel: * = Global
       Power Level = Percent

Online AP number: 0
Offline AP number: 1

AP Name                                IP Address       Mac Address     Radio 1             Radio
2             Up/Off time    State
---------------------------------------- --------------- --------------- --------------------
------------------- ------------- -----
ap1                                    10.0.20.15       00d0.f822.33b0 N    -/-      -      - N
-/-      -      -     0:00:16:03 Quit
```

配置离线 AP Ruijie-AC1 的名称为 Ruijie-AC2

【配置方法】
- 进入 AP 配置模式
- 配置 AP 的名称

AC

```
Ruijie(config)#ap-config Ruijie-AC1
Ruijie(config-ap)#ap-name Ruijie-AC2
```

【检验方法】 通过 **show ap-config running** 命令可以查看当前 AP 配置。

AC

```
Ruijie#show ap-config running
```

```
!
ap-config Ruijie-AC1
  ap-name Ruijie-AC2
!
```

配置清除离线 AP Ruijie-AC1 的名称配置

【配置方法】
- 进入 AP 配置模式
- 配置 AP 的名称

AC

```
Ruijie(config)#ap-config Ruijie-AC1
Ruijie(config-ap)#no ap-name
```

【检验方法】 通过 **show ap-config running** 命令可以查看当前 AP 配置。

AC

```
Ruijie#show ap-config running
!
ap-config Ruijie-AC1
!
```

配置 AP 设备的 AP 名称为 Ruijie-AP1

【配置方法】
- 进入 AP 全局配置模式
- 配置 AP 的名称

AP

```
Ruijie(config)#ap-name Ruijie-AP1
```

【检验方法】
- 通过 show running-config 命令可以查看当前 AP 配置。

AP

```
Ruijie#show running-config

Building configuration...
Current configuration: 1592 bytes

version 11.1(5)B0
privilege exec all level 1 debug
privilege exec all level 1 show
privilege exec all level 1 terminal
privilege exec all level 1 undebug
ap-name Ruijie-AP1
fair-schedule
!
```

常见错误

- 无。

1.5.8 配置AP MAC地址绑定

配置效果

- 在 AP 配置模式下通过 **ap-mac** 命令为该 AP 配置绑定 MAC 地址，可实现该 AP 配置只对所绑定 MAC 地址的 AP 生效。
- 一般情况下，AP 上线通过 AP 名称与 AP 配置名称的匹配来决定 AP 使用哪个配置。而 MAC 地址绑定是比名称匹配更强的绑定关系，其优先级高于名称匹配。因此，只要 AP 配置所绑定的 MAC 地址与 AP 的 MAC 地址一致，则 AP 上线时使用该配置。
- MAC 地址自动绑定：如果对应的 AP 配置没有配置 MAC 地址绑定，在对应的 AP 上线时，将自动进行 MAC 地址绑定，，该绑定关系在 AP 下线时仍然有效，即 AP 上线后将自动生成该配置。
- MAC 地址绑定还用于 AP 接入控制的 **bind-ap-mac** 接入控制功能，具体参见 **bind-ap-mac** 配置说明。
- 只能对离线 AP 的配置进行指定 MAC 地址绑定。如果对应的 AP 已经在线，则无法对其进行指定 MAC 地址绑定的配置。

注意事项

- 只能对离线 AP 的配置进行指定 MAC 地址绑定。如果对应的 AP 已经在线，则无法对其进行指定 MAC 地址绑定的配置。

配置方法

- 可选配置。。
- AC 设备上，进入 AP 配置模式，通过 **ap-mac** 命令进行配置。

【命令格式】 **ap-mac** *ap-mac-address*

no ap-mac

【参数说明】 *ap-mac-address*：配置所绑定的 MAC 地址

【缺省配置】 AP 配置没有 MAC 地址绑定。在需要强制指定该 AP 配置应用于某个指定 MAC 地址的 AP 时，可以配置该 AP 配置的 MAC 地址绑定

【命令模式】 AP 的配置模式

【使用指导】
- ap-mac ap-mac-address 命令适用于对离线 AP 配置 ,用户可以通过该命令指定离线 AP 的 MAC 地址，使得 AP 上线之后直接通过 MAC 地址找到该配置信息。
- no ap-mac 命令适用于所有 AP 配置。

检验方法

- 通过 **show ap-config running** 命令查看当前 AP 的 ap-mac 配置。

配置举例

↘ **配置离线 Ruijie-AP1 绑定 001a.a979.1234**

【配置方法】
- 进入 AP 配置模式
- 通过 no 命令可以清除 MAC 地址绑定

AC

```
Ruijie(config)#ap-config Ruijie-AP1
Ruijie(config-ap)#ap-mac 001a.a979.1234
Ruijie(config)#ap-config Ruijie-AP1
Ruijie(config-ac)#no ap-mac
```

【检验方法】 通过 **show ap-config running** 命令可以查看当前 AP 配置。

AC

```
Ruijie(config)#show ap-config running Ruijie-AP1
!
ap-config Ruijie-AP1
  ap-mac 001a.a979.1234
!
```

常见错误

- 无。

1.5.9 配置AP的用户名和密码

配置效果

- 为避免非法用户通过 Telnet 直接登录到 AP 上对其实施配置控制，影响正常 WLAN 网络运行，用户可以配置指定 AP 的 Telnet 用户名和密码
- **credential** 配置同时支持 **ap-config** *ap-name* 配置模式、**ap-group** 配置模式和 **ap-config all** 配置模式。上述配置模式下命令生效遵循优先级生效规则：优先级 **ap-config** *ap-name* > **ap-group** > **ap-config all**。

注意事项

- 无。

配置方法

- 可选配置，可以根据需要通过 AP 配置模式下 **credential** *user-name password* 命令对 AP 配置新的 Telent 用户名密码，增加安全性。
- AC 设备上，进入 AP 配置模式/AP 组配置模式，通过 **credential** 命令进行配置。

【命令格式】 **credential** *user-name password*

no credential

【参数说明】 *user-name*：用户名，不允许带空格。

password：密码，不允许带空格。

【缺省配置】 AC 设备不对 AP 的 Telent 用户名密码做配置，AP 的 Telent 用户名密码为出厂配置的用户名密码。用户可以根据需要，对 AP 配置新的用户名密码，便于管理

【命令模式】 AP 的配置模式/AP 组配置模式

【使用指导】 -

检验方法

- 通过 **show ap-config running** / **show running** 命令查看配置。

配置举例

配置 Ruijie-AP1 的用户名和密码

【配置方法】
- 配置 Ruijie-AP1 的用户名和密码
- 通过 no 命令删除 AP 用户名和密码的配置（AP 上获取缺省用户名和密码）

AC

```
Ruijie(config)#ap-config Ruijie-AP1
Ruijie(config-ap)#credential user pass
Ruijie(config)#ap-config Ruijie-AP1
Ruijie(config-ac)#no credential
```

【检验方法】 通过 **show ap-config running** 命令可以查看当前 AP 配置。

AC

```
Ruijie(config)#show ap-config running Ruijie-AP1
!
ap-config Ruijie-AP1
  credential user pass
!
```

常见错误

- 无。

1.5.10 配置AP定期报告统计信息的时间间隔

配置效果

- 通过 **statistics-timer** 命令可以配置 AP 定期报告统计信息的时间间隔

注意事项

- 无。

配置方法

- 可选配置，用户可以根据统计信息的精度需求，结合 AC 和 AP 设备负载，调整该时间间隔。。
- AC 设备上，进入 AP 配置模式/AP 组配置模式，通过 **statistics-timer** 命令进行配置。

【命令格式】 **statistics-timer** *timer-interval*

no statistics-timer

【参数说明】 *timer-interval*：定期报告的时间间隔，单位为秒，默认值为 120。

【缺省配置】 120 秒

【命令模式】 AP 的配置模式/AP 组配置模式

【使用指导】 -

检验方法

- 通过 **show ap-config running** 命令查看配置。

配置举例

配置 Ruijie-AP1 的定期报告统计信息的时间间隔为 300 秒

【配置方法】
- 配置 Ruijie-AP1 定期报告统计信息的时间间隔为 300 秒
- 通过 no 命令恢复 Ruijie-AP1 定期报告统计信息的默认时间间隔

AC

```
Ruijie(config)#ap-config Ruijie-AP1
Ruijie(config-ap)#statistics-timer 300
Ruijie(config)#ap-config Ruijie-AP1
Ruijie(config-ac)#no statistics-timer
```

【检验方法】 通过 **show ap-config running** 命令可以查看当前 AP 配置。

AC

```
Ruijie(config)#show ap-config running Ruijie-AP1
!
ap-config Ruijie-AP1
  statistics-timer 300
!
```

常见错误

- 无。

1.5.11 配置AP系统日志信息

配置效果

- 控制 AP 系统日志显示，设置记录 AP 系统日志信息的服务器地址。

注意事项

- 无。

配置方法

- 可选配置。
- 通过命令 **logging on** 配置指定 AP 系统日志显示开关
- 提供命令 **logging server** *ip-address* **[udp-port** *num***]**配置指定 AP 系统日志服务器地址

【命令格式】 **logging on**
no logging on
【参数说明】 -
【缺省配置】 允许显示系统日志
【命令模式】 AP 配置模式或所有 AP 配置模式
【使用指导】 -

【命令格式】 **logging server** *ip-address* **[udp-port** *num***]**
no logging server *ip-address*
【参数说明】 *ip-address*：接收日志信息的主机 IP 地址。
num：接收日志信息的主机的端口号(可选参数)。
【缺省配置】 无
【命令模式】 AP 配置模式或所有 AP 配置模式
【使用指导】 用户最多可以配置 5 个日志服务器地址，日志信息将同时发送给配置的所有日志服务器

检验方法

- 通过 **show ap-config running** 命令查看配置。

配置举例

↘ 配置 Ruijie-AP1 关闭系统日志显示

【配置方法】
- 进入 AP 配置模式

- 配置关闭系统日志显示

AC

```
Ruijie(config)#ap-config Ruijie-AP1
Ruijie(config-ap)#no logging on
```

【检验方法】 通过 **show ap-config running** 命令可以查看当前 AP 配置。

AC

```
Ruijie(config)#show ap-config running Ruijie-AP1
!
ap-config Ruijie-AP1
  no logging on
!
```

↘ 配置 Ruijie-AP1 日志服务器地址

【配置方法】

- 进入 AP 配置模式
- 配置日志服务器地址为 1.1.1.1

AC

```
Ruijie(config)#ap-config Ruijie-AP1
Ruijie(config-ap)#logging server 1.1.1.1
```

【检验方法】 通过 **show ap-config running** 命令可以查看当前 AP 配置。

AC

```
Ruijie(config)#show ap-config running Ruijie-AP1
!
ap-config Ruijie-AP1
  logging server 1.1.1.1
!
```

常见错误

- 无。

1.5.12 配置AP每天定时重启的时间

配置效果

- 为避免因 AP 长时间工作导致负荷过重，影响用户上网质量，可以配置 AP 每天定时重启，能够使用户每天的上网质量得到保证。

注意事项

- 无。

配置方法

- 可选配置。用户可根据 AP 负载情况下，配置开启该功能。
- 通过配置 AP 每天定时重启，可以避免 AP 长时间工作，增强可用性。

【命令格式】 **reload at** *time*

no reload at

【参数说明】 *time*：以 hh:mm:ss 形式定义的每天定时重启的时间点

【缺省配置】 AP 不存在每天定时重启的行为

【命令模式】 AP 的配置模式

【使用指导】 -

检验方法

- 通过 **show ap-config running** 命令查看配置。

配置举例

↘ 配置 Ruijie-AP1 在每天 1:00:00 定时重启

【配置方法】
- 配置 Ruijie-AP1 在每天的 1:00:00 定时重启
- 通过 no 命令取消定时重启配置

AC

```
Ruijie(config)#ap-config Ruijie-AP1
Ruijie(config-ap)#reload at 1:00:00
Ruijie(config)#ap-config Ruijie-AP1
Ruijie(config-ac)#no reload at
```

【检验方法】 通过 **show ap-config running** 命令可以查看当前 AP 配置。

AC

```
Ruijie(config)#show ap-config running Ruijie-AP1
!
ap-config Ruijie-AP1
  reload at 1:00:00
!
```

常见错误

- 无。

1.5.13 配置指定AP恢复出厂配置

配置效果

- 配置指定 AP 恢复出厂配置。

- 该配置只对在线 AP 有效。

注意事项

- 该操作会引起该 AP 下线与复位。

配置方法

- 可选配置，用户可根据需求配置指定 AP 恢复出厂配置。
- AP 恢复出厂配置属于 AP 的即时行为，在 AC 上配置 AP 恢复出厂配置可以实现 AP 恢复出厂配置，该配置将触发 AP 复位。

【命令格式】 **factory-reset** *ap-name*
【参数说明】 *ap-name*：指定某个 AP 名称。
【缺省配置】 无
【命令模式】 AC 配置模式
【使用指导】 配置将指定的 AP 恢复出厂设置，该操作会引起该 AP 复位。

检验方法

- 对在线 AP 配置后，该 AP 将下线，重新上线后，通过 **show ap-config running** 可以查看该 AP 为出厂配置。

配置举例

配置在线 AP Ruijie-AP1 恢复出厂配置

【配置方法】
- 进入 AC 配置模式
- 配置 Ruijie-AP1 恢复出厂配置

AC

```
Ruijie(config)#ac-controller
Ruijie(config-ac)#factory-reset Ruijie-AP1
```

【检验方法】 对在线 AP 配置后，该 AP 将下线，重新上线后，通过 **show ap-config running** 可以查看该 AP 为出厂配置(空配置)

常见错误

- 无。

1.5.14 配置AP复位

配置效果

- 配置指定在线 AP 复位。
- 配置所有在线 AP 复位。

注意事项

- 无。

配置方法

- 可选配置，用户可根据需要配置 AP 复位。
- 在 AC 上配置 AP 复位，对应的 AP 将复位。可以配置指定 AP 复位，也可以配置所有在线 AP 复位。

【命令格式】 **reset** { **all** | **single** *ap-name* }

【参数说明】 **all**：复位所有的在线 AP。

single *ap-name*：复位指定的 AP

【缺省配置】 无

【命令模式】 AC 配置模式

【使用指导】 -

检验方法

- 配置完成后，AC 上可以看到对应 AP 下线的 SYSLOG，对应 AP 设备将复位。

配置举例

↘ 配置 Ruijie-AP1 复位

【配置方法】
- 进入 AC 配置模式
- 配置 Ruijie-AP1 复位

AC

```
Ruijie(config)#ac-controller
Ruijie(config-ac)#
Ruijie(config-ac)#reset Ruijie-AP1
```

【检验方法】 Ruijie-AP1 将复位，AC 上可以看到如下 AP 下线的 SYSLOG

AC

```
%APMG-6-RX_CTRL_MSG: AP(AP_20#3F_S:001a.a912.3456) leave AC.
```

常见错误

- 无。

1.5.15 配置AP数限制

配置效果

- AC 的在线 AP 数量将不会超过配置的允许接入的最大 AP 数

注意事项

- 不同型号的 AP 占用的权重不一样(如 WALL-AP 两个 AP 占用一个 AP 数)，AC 在 AP 接入时会根据权重系数计算实际的权重 AP 数。

配置方法

- 可选配置，用户可根据需要，在容量范围内设置 AP 数限制。

【命令格式】 **wtp-limit** *max-num*
【参数说明】 *max-num*：可连接的最大 AP 数。
【缺省配置】 缺省情况下，该数值等于各型号 AC 的支持的 AP 数
【命令模式】 AC 配置模式
【使用指导】 配置 AP 上支持的最大 AP 数量。该数量不能超过 AC 支持的最大值。

检验方法

- 通过 **show ac-config** 命令查看当前 AC 名称，确认是否配置成功。

配置举例

↘ 配置 AC 可连接的最大 AP 数为 512.

【配置方法】
- 进入 AC 配置模式
- 配置 AC 的可连接的最大 AP 数为 512
- 通过 no 命令可以恢复缺省值

AC

```
Ruijie(config)#ac-controller
Ruijie(config-ac)#wtp-limit 512
Ruijie(config)#ac-controller
Ruijie(config-ac)#no wtp-limit
```

【检验方法】 通过 **show ac-config** 命令可以查看配置的 AC 可连接的最大 AP 数。

AC

```
Ruijie#show ac-config
......
max_wtp          :512
......
```

常见错误

- 无。

1.5.16 配置AP合规性检查

配置效果

- AP 合规性检查功能又称为“基于 MAC 绑定的接入控制”，也称为“bind-ap-mac 功能”。开启 AP 合规性检查，则只允许存在离线配置且离线配置中绑定有其 MAC 地址的 AP 关联该 AC。

注意事项

- 无。

配置方法

- 可选配置，用户通过开启 AP 合规性检查来限制只允许指定 MAC 地址的 AP 上线，对 AP 的接入进行严格的控制。
- 在 AP 合规性检查开启时，将自动对所有当前在线的 AP 进行 MAC 地址绑定。因此，一般在网络部署阶段建议关闭该功能，在所有计划内 AP 上线后，开启该功能。
- **bind-ap-mac** 功能开启时，所有在线 AP 的自动绑定的 MAC 地址将全部转换为正式的 MAC 地址绑定，在 AP 下线时，不会自动清除。
- 也可在 AC 设备上通过 AP 配置模式下 **ap-mac** *X.Y.Z* 命令，配置单个 AP 配置的 MAC 地址绑定。

【命令格式】 **bind-ap-mac**

no bind-ap-mac

【参数说明】 -

【缺省配置】 AP 合规性检查关闭。

【命令模式】 AC 配置模式

【使用指导】 配置开启 AP 合规性检查

【命令格式】 **ap-mac** *ap-mac-address*
no ap-mac
【参数说明】 *ap-mac-address*：配置所绑定的 MAC 地址
【缺省配置】 无
【命令模式】 AP 的配置模式
【使用指导】 **ap-mac** *ap-mac-address* 命令适用于对离线 AP 配置，用户可以通过该命令指定离线 AP 的 MAC 地址，使得 AP 上线之后直接通过 MAC 地址找到该配置信息。

检验方法

- 通过 **show running** 命令可以查看 **bind-ap-mac** 命令是否开启
- 通过 **show ap-config running** 命令可以查看 AP 配置的 MAC 地址绑定

配置举例

配置 AC 开启 bind-ap-mac 功能

【配置方法】
- 在所有合法 AP 上线之后，通过 AC 配置模式下 bind-ap-mac 命令配置开启 bind-ap-mac 功能

AC

```
Ruijie(config)#ac-controller
Ruijie(config-ac)#bind-ap-mac
```

【检验方法】 通过 **show running** 查看 **bind-ap-mac** 功能是否开启

AC

```
Ruijie#show running
!
ac-controller
  bind-ap-mac
!
```

常见错误

- 无。

1.5.17 配置AP接入认证

配置效果

- AP 接入认证支持：基于系列号的接入认证、基于密码的接入认证和基于证书的接入认证。

注意事项

- AC 配置模式下配置接入认证开启 **ap-auth** { **serial** | **password** | **certificate** } **enable** 的情况下，如果 AP 配置模式下没有配置相应的认证参数 **ap-auth** { **serial** *serial-string* | **password** *password* | **ac-cert** *ac-cert-name* | **ap-cert** *ap-cert-name* } **,** 则对应 AP 的接入认证将失败，AP 将无法接入上线。

配置方法

- 可选配置。
- 提供 **ap-auth serial-update** 命令配置所有在线 AP 更新认证序列号。
- 通过 AC 配置模式下 **ap-auth enable** 命令开启指定类型的 AP 接入认证。
- 通过 **ap-auth** { **serial** *serial-string* | **password** *password* | **ac-cert** *ac-cert-name* | **ap-cert** *ap-cert-name* }命令进行相应的 AP 接入认证配置。

【命令格式】 **ap-auth serial-update**
【参数说明】 -
【缺省配置】 缺省为不配置
【命令模式】 AC 配置模式
【使用指导】 所有在线 AP 将以当前 AP 的序列号作为认证的序列号配置

【命令格式】 **ap-auth** { **serial** | **password** | **certificate** } **enable**
【参数说明】 **serial**：基于 AP 接入序列号的认证功能
password：基于 AP 接入密码的认证功能
certificate: 基于 AP 证书的认证功能
【缺省配置】 缺省为不开启
【命令模式】 AC 配置模式
【使用指导】 -

【命令格式】 **ap-auth** { **serial** *serial-string* | **password** *password* | **ac-cert** *ac-cert-name* | **ap-cert** *ap-cert-name* }
【参数说明】 *serial-string*：指定 AP 接入的序列号
password：指定 AP 接入的密码
ac-cert-name：指定 AC 的证书文件名
ap-cert-name：指定 AP 的证书文件名
【缺省配置】 缺省为不配置
【命令模式】 AP 的配置模式。
【使用指导】 AP 接入认证配置，只在 AP 接入时有效，如果 AP 已在线，则配置在下次 AP 上线时生效。
ap-auth serial 不支持 all 模式下配置，因为每台 AP 的序列号是不同的。
通过 **ap-auth ap-cert** 下发的证书文件，在 AP 上会保存为 cert.crt，文件名不可变。

检验方法

- 通过 **show ap-config running** 命令查看配置是否成功。

配置举例

配置 AP 基于序列号的接入认证

【配置方法】
- 在合法 AP 均上线之后，配置所有在线 AP 更新认证序列号
- 配置开启基于序列号的 AP 接入认证
- 配置指定 AP 的认证序列号

AC

```
Ruijie(config)#ac-controller
Ruijie(config-ac)#ap-auth serial-update
Ruijie(config)#ac-controller
Ruijie(config-ac)#ap-auth serial enable
Ruijie(config)#ap-config Ruijie-AP1
Ruijie(config-ap)#ap-auth serial G1GD10U000456
```

【检验方法】 通过 **show running** / **show ap-config running** 命令可以查看 AP 接入认证配置。

AC

```
Ruijie(config)#show run
!
ac-controller
  ap-auth serial enable
!
Ruijie(config)#show ap-config running Ruijie-AP1
!
ap-config Ruijie-AP1
  ap-auth serial G1GD10U000456
!
```

配置 AP 更新接入认证证书

【配置方法】
- 配置更新接入认证证书

AC

```
Ruijie(config)#ap-config Ruijie-AP1
Ruijie(config-ap)#ap-auth ap-cret ap1_cret.crt
```

【检验方法】 通过 **show ap-config running** 命令可以查看当前 AC 名称。如果对应 AP 在线，则 ap1_cret.crt 证书将即时更新到 AP 上；否则，在对应 AP 上线后，更新到 AP 上。

AC

```
Ruijie(config)#show ap-config running Ruijie-AP1
!
ap-config Ruijie-AP1
  ap-auth ap-cret ap1_cret.crt
!
```

常见错误

- 无。

1.5.18 配置AP优先级功能

配置效果

- 缺省情况下，AC 是按照 AP 关联请求到达的顺序提供其接入的。通过设置 AP 的 Failover 优先级，并在 AC 上开启对 AP 的 Failover 优先级的支持，使得 AC 可以按照 AP 的优先级顺序来接受 AP 的接入。AP 的优先级为 1-4，其中 1 为最低优先级。

注意事项

- 无。

配置方法

- 可选配置，用户可根据需要开启，并为指定 AP 配置优先级。
- AC 设备上，AC 配置模式下，通过 **ap-priority** { **enable** | **disable** }命令进行配置 AP 优先级功能开启与否。
- AC 设备上，AP 配置模式下，通过 **priority** *priority-value* 命令对指定 AP 进行优先级配置。

【命令格式】 **ap-priority** { **enable** | **disable** }
【参数说明】 **enable**：开启对 AP 的 Failover 优先级的支持
disable：关闭对 AP 的 Failover 优先级的支持
【缺省配置】 缺省关闭
【命令模式】 AC 配置模式
【使用指导】 -

【命令格式】 **priority** *priority-value*
【参数说明】 priority-value：AP 优先级 1-4，1 为最低优先级，缺省值为 1。
【缺省配置】 AP 的缺省优先级为 1，可配置优先级为 1~4，其中 1 为最低优先级，4 为最高优先级。通过 AP 配置模式下 **priority** 命令进行 AP 优先级的配置
【命令模式】 AP 配置模式
【使用指导】 -

检验方法

- 通过 **show running** / **show ap-config running** 查看配置。

配置举例

↘ 配置 Ruijie-AP1 的优先级为 2，并开启 AP 优先级功能

【配置方法】
- 进入 AP 配置模式
- 配置 AP 优先级
- 进入 AC 配置模式
- 配置开启 AP 优先级功能

AC

```
Ruijie(config)#ap-config Ruijie-AP1
Ruijie(config-ap)#priority 2
Ruijie(config)#ac-controller
Ruijie(config-ac)#ap-priority enable
```

【检验方法】 通过 **show running** 命令可以查看 AC 配置模式下 **ap-priority enable** 命令是否配置。
通过 **show ap-config running** 命令查询 AP 配置。

AC

```
Ruijie(config)#show running
!
ac-controller
  ap-priority enable
!
Ruijie#show ap-config running
!
ap-config Ruijie-AP1
  priority 2
!
```

常见错误

- 无。

1.5.19 创建WLAN

配置效果

- 用户可以在 AC 上创建多个 WLAN，并进入指定 WLAN 的配置模式，根据实际网络需要配置该 WLAN 的相关功能属性。
- 基于以下配置最终形成特定的 WLAN 服务模板，必须将 WLAN\应用到指定的 AP 组方可生效，无线用户通过接入对应的 AP 实现 WLAN 的用户接入。
- 在无线网络中，用户可以通过创建 WLAN 将网络划分成多个 WLAN 子网，并在 WLAN 配置模式下配置指定 WLAN 的功能属性，实现为无线用户提供不同的网络服务。
- 在创建 WLAN 的同时必须关联一个 SSID，SSID 仅是一个网络服务域的名称，一个 SSID 可以对应一个或多个 WLAN。

注意事项

- 无。

配置方法

- 可选配置，缺省情况下，无 WLAN 配置。在部署 WLAN 之前，需要先创建 WLAN 配置。
- 通**过 wlan-config** 命令创建 WLAN，通**过 no** 命令删除 WLAN。

【命令格式】 **wlan-config** *wlan-id* [*profile –string*] [*ssid-string*]
no wlan-config *wlan-id*

【参数说明】 *wlan-id*：指定 WLAN 的 ID 号，取值范围 1~4094；
profile -string：该 WLAN 的描述符，可省略，最大长度为 32 字节；
ssid-string：SSID 标识符，最大长度为 32 字节。创建 WLAN 时，必须指定该 WLAN 关联的 SSID。
使用 no 命令删除指定 WLAN。

【缺省配置】 不存在 WLAN

【命令模式】 全局配置模式

【使用指导】 一个 SSID 可以对应多个 WLAN，但一个 WLAN 不能同时关联多个 SSID。

检验方法

- 通过 **show running** 可以查看 WLAN 配置

↘

配置举例

↘ 创建 WLAN 举例

【配置方法】
- 配置创建 WLAN 1，SSID 为 ruijie-wireless

AC

```
Ruijie(config)#wlan-config 1 ruijie-wireless
Ruijie(config-wlan)#
```

【检验方法】 通过 **show running** 命令可以查看 WLAN 配置。

AC

```
Ruijie#show running
!
wlan-config 1 ruijie-wireless
!
```

常见错误

- 无。

1.5.20 配置WLAN部署

配置效果

- 必须将 WLAN\应用到指定的 AP 组方可生效，无线用户通过接入对应的 AP 实现 WLAN 的用户接入。通过 AP 组配置模式下的 **interface-mapping** 命令可以配置将 WLAN 应用（或称为部署）到指定 AP 组。该命令同时配置了该 WLAN 与 VLAN/VLAN-Group 的映射，从而指定该 WLAN 对应的有线网络的 VLAN。

注意事项

- 当 WLAN 的转发模式为本地转发时，该命令配置的 vlan-id 或 vlan-group 模式下为 STA 分配的 vlan-id 与 ap-vlan 命令指定的 vlan-id 相同时，STA 的真正 VLAN 将由 AP 的接入交换机决定而非该命令配置的 VLAN 或 vlan-group 模式分配的 VLAN。特别的，由于 ap-vlan 的默认 vlan-id 为 1，即未配置 ap-vlan 时，如果该命令配置的 vlan-id 为 1，则本地转发下 STA 的 VLAN 将由接入交换机决定。

配置方法

- 可选配置，需要通过 AP 组配置模式下 **interface-mapping** 命令配置 WLAN 部署到该 AP 组的所有 AP 上。
- AC 设备上，进入 AP 组配置模式，通过 **interface-mapping** 命令进行配置。

【命令格式】 **interface-mapping** *wlan-id* { *vlan-id* | **group** *vlan-group-id* } [**radio** {*radio-id* | [*802.11b* | *802.11a*]}] [**ap-wlan-id** *ap-wlan-id*]

【参数说明】 *wlan-id*：指定的 WLAN，该 WLAN 必须已经创建，取值范围为 1~4094。
vlan-id：指定的 VLAN，取值范围为 1~4094。
vlan-group-id：指定的 vlan-group，取值范围为 1~128。
r*adio-id*：指定 AP 的 Radio，若不指定 radio-id 参数，会应用到该 AP 组内的所有 AP 的所有 radio 上。
802.11b：该 mapping 会被应用到该 AP 组内的所有 AP 的 2.4G 的 radio 上。
802.11a：该 mapping 会被应用到该 AP 组内的所有 AP 的 5.8G 的 radio 上。
ap-wlan-id：指定 interface-mapping 中 wlan-id 在 AP 上使用的 wlan-id，取值范围为：1~64

【缺省配置】 缺省情况不会部署到任何 AP 上

【命令模式】 AP 组配置模式

【使用指导】 若不指定 ap-wlan-id 参数，则该 mapping 自动选择空闲的一个 ap-wlan-id 来使用。

检验方法

- 通过 **show running** 命令查看 AP 组配置。

↘

配置举例

配置 WLAN 部署到指定 AP 组上

【配置方法】

Ruijie-AP1 属于 AP 组 APG-1，创建 WLAN 并部署到 Ruijie-AP1 上。

- 创建 WLAN 1，SSID 为 ruijie-wireless
- 创建 VLAN 1
- 在 AP 组配置模式下配置 WLAN-VLAN 映射

AC

```
Ruijie(config)#wlan-config 1 ruijie-wireless
Ruijie(config-wlan)#exit
Ruijie(config)#vlan 1
Ruijie(config-vlan)#exit
Ruijie(config)#ap-group APG-1
Ruijie(config-ap-group)#interface-mapping 1 1
```

【检验方法】 通过 **show running** 查看 ap-group 配置

```
Ruijie#show running
!
wlan-config 1 ruijie-wireless
!
!
ap-group APG-1
  interface-mapping 1 1
!
```

常见错误

- 无。

1.5.21 配置WLAN SSID广播开关

配置效果

- 在 WLAN 网络中，AP 会定期广播 SSID 信息，向外通告无线网络的存在，无线用户使用无线网卡搜索 SSID 发现网络。为避免无线网络被非法用户通过 SSID 广播搜索到，并建立非法连接，可以将 SSID 广播禁用。

注意事项

- 无。

配置方法

- 可选配置。缺省情况下，WLAN 的 SSID 广播开启。在需要对 WLAN 的 SSID 进行隐藏，避免非法无线用户通过 SSID 广播搜索并接入该 WLAN 时，可以配置 WLAN 的 SSID 广播关闭。
- AC 设备上，进入 WLAN 配置模式，通过 **enable-broad-ssid** 命令进行配置

【命令格式】 **enable-broad-ssid**
no enable-broad-ssid
【参数说明】 -
【缺省配置】 缺省情况下，为 enable
【命令模式】 WLAN 配置模式
【使用指导】 缺省情况下打开 SSID 广播，通过 **no** 命令可关闭 SSID 广播。
WLAN 此配置变化将导致该 WLAN 下关联的用户下线。

检验方法

- 通过 **show running** 查看 WLAN 配置。

配置举例

↘ 配置 WLAN 1 关闭 SSID 广播

【配置方法】
- 进入 WLAN 配置模式
- 配置 SSID 广播禁用

AC
```
Ruijie(config)#wlan-config 1
Ruijie(config-wlan)#no enable-broad-ssid
```

【检验方法】 通过 **show running** 可查看 WLAN 配置

AC
```
Ruijie#show running
!
wlan-config 1 ruijie-wireless
  no enable-broad-ssid
!
```

常见错误

- 无。

1.5.22 配置WLAN用户接入地编号

配置效果

- 在 WLAN 网络中，WLAN 用户接入地编号（NAS-ID）可用于区分不同的热点区域。缺省情况下 WLAN 用户接入地编号为空字符串。

注意事项

- 无。

配置方法

- 可选配置。
- AC 设备上，进入 WLAN 配置模式，通过 **nas-id** 命令进行配置。

【命令格式】 **nas-id** *wlan-nas-id*

no nas-id

【参数说明】 -

【缺省配置】 空字符串

【命令模式】 WLAN 配置模式

【使用指导】 无。

检验方法

- 通过 **show running** 查看 WLAN 配置。

配置举例

配置 WLAN 1 关闭 SSID 广播

【配置方法】
- 进入 WLAN 配置模式
- 配置 WLAN 接入用户地编号

AC

```
Ruijie(config)#wlan-config 1
Ruijie(config-wlan)# nas-id 0000059159100460
```

【检验方法】 通过 **show running** 可查看 WLAN 配置

AC

```
Ruijie#show running
!
wlan-config 1 ruijie-wireless
  nas-id 0000059159100460
!
```

常见错误

- 无。

1.5.23 配置WLAN SSID名字

配置效果

- 配置 WLAN 的 SSID 新名字。如果该 WLAN 已经部署，那么关联在该 WLAN 下的用户将会下线。

注意事项

- 无。

配置方法

- 可选配置。
- AC 设备上，进入 WLAN 配置模式，通过 **ssid** 命令进行配置。

【命令格式】 **ssid** *ssid-string*
【参数说明】 -
【缺省配置】 无
【命令模式】 WLAN 配置模式
【使用指导】 无。

检验方法

- 通过 **show running 可以**查看 WLAN 配置。

配置举例

↘ 配置 WLAN 1 的 SSID 新名字为 ruijie

【配置方法】
- 进入 WLAN 配置模式
- 配置 SSID 新名字为 ruijie

AC

```
Ruijie(config)#wlan-config 1
Ruijie(config-wlan)#ssid ruijie
```

【检验方法】 通过 **show running** 可查看 WLAN 配置

AC

```
Ruijie#show running
!
wlan-config 1 ruijie
!
```

常见错误

- 无。

1.5.24 配置AP备份功能

配置效果

- AP 备份组中的主 AP 发生故障而掉线时，组里的其它备份 AP 接收到主 AP 的 WLAN 配置，放出主 AP 的无线信号。

注意事项

- AP 备份组中，如果没有选定主 AP，则该 AP 备份功能不生效。

配置方法

↘ 配置 AP 备份组

- 可选配置，当某个 AP 的无线网络需要备份时进行配置创建 AP 备份组。
- 配置 AP 备份组：AC 配置模式下 ap-backup group 命令创建 AP 备份组。

【命令格式】 **ap-backup group** *backup-group*
【参数说明】 *backup-group*：AP 备份组的名称
【缺省配置】 缺省配置，AC 上仅存在名为 default 的 AP 备份组，该备份组的备份功能不生效。
【命令模式】 AC 配置模式
【使用指导】
- -

↘ 配置 AP 加入备份组

- 可选配置，当某个 AP 的无线网络需要由其它 AP 进行备份时，将备份 AP 和被备份 AP 均加入 AP 备份组，并指定被备份 AP 为主 AP。
- 需要通过 AP 配置模式下 **ap-backup-group** 命令配置到该 AP 备份组里，加入 AP 备份组时，可指定该 AP 是否为主 AP 角色。

【命令格式】 **ap-backup-group** *backup-group* **[master]**
【参数说明】 *backup-group*：AP 备份组名字
【缺省配置】 缺省情况下，AP 不加入 default 组，该备份组的备份功能不生效。
【命令模式】 AP 配置模式
【使用指导】

该命令不支持 ap-config all 模式

可选关键字 master 指定 AP 为本组的主 AP，不带该关键字则为备份 AP，一个组最多只有一个主 AP，

备份 AP 可以有多个

当 AP 备份组开始工作，即备份 AP 已继承主 AP 的 WLAN 信号后，需要注意：1、修改备份 AP 所在的 ap-group 的 WLAN 配置；2、修改主 AP 所在的 ap-group 的 WLAN 配置；3 备份 AP 切换 ap-group；4、主 AP 切换 ap-group；这些操作改变了备份 AP 实际应该生效的 WLAN 配置，其继承而来的 WLAN 信号将重新生效，如果已有用户关联，则用户会下线。

检验方法

- 通过 **show ap-config running 和 show ac-config ap-backup-group** 查看配置。

配置举例

创建名称为 APBACK-APG-1 的 AP 备份组

【配置方法】 ● 在 AC 配置模式下通过 ap-backup group 命令创建 AP 备份组

AC

```
Ruijie(ac-config)# ap-backup group APBACK-APG-1
```

【检验方法】 ● 通过 show ac-config ap-backup-group 命令查看。

AC

```
Ruijie#show ac-config ap-backup-group
Cnt    Group-Name                  Master-AP cnt   Standby-AP cnt   Master-AP-Name     Working
------ ----------------------------- ------------ ------------ -------------  ------------
1      APBACK-APG-1                1               2                AP4210-1            false
```

把 ap4210-1 加入到名为 APBACK-APG-1 的 AP 备份组中，并设置为该组的主 AP

【配置方法】 ● 在 AP 配置模式下通过 backup-group 命令把 AP 加入到 AP 备份组

AC

```
Ruijie(ap-config)# ap-backup-group APBACK-APG-1 master
```

【检验方法】 ● 通过 show ac-config ap-backup-group 命令查看。

AC

```
Ruijie#show ac-config ap-backup-group APBACK-APG-1
Cnt     Ap-Name                  Ap-Mac              Online    Is-Master   Inherit-Wlan Cnt
------- ------------------------ ------------------- -------- ------------ ------------------
1       AP4210-1                 8832.0000.1111      true       Yes        0
```

常见错误

- 无。

1.6 监视与维护

清除各类信息

- 无。

查看运行情况

作用	命令
查看本 AC 的基本配置信息	**show ac-config**
查看 AP 备份组信息	**show ac-config ap-backup-group**
查看所有 AP 的 BSSID 列表	**show ap-config bssid**
查看 AP 的状态信息	**show ap-config cb**
查看 AP 继承的 WLAN 信息	**show ap-config inherit-wlan**
查看 AP 产品统计列表	**show ap-config product**
查看所有 AP 的当前状态	**show ap-config summary**
查看所有 AP 的认证相关信息	**show ap-config summary ap-auth**
查看尝试关联但是被 AC 拒绝的 AP 列表	**show ap-config summary deny-ap**
查看指定 AP 组的 AP 列表	**show ap-group aps**
查看所有 AP 组的 AP 列表	**show ap-group aps summary**
查看指定 AP 的基本信息	**show ap-group cb**
显示指定 AP 组的 WLAN-VLAN 映射	**show ap-group intf-wlan-map**
查看所有 AP 列表	**show ap-group summary**
查看指定 WLAN 的基本信息	**show wlan-config cb**
查看 AC 上的 WLAN 配置列表	**show wlan-config summary**

查看调试信息

- 无。

2 STAMG

2.1 概述

STAMG（Sta Manage，无线用户管理）是对无线用户进行管理的功能，主要包含 STA 接入控制的管理以及 STA 的事件通告，事件通告主要服务于其他模块。STAMG 功能适用于：

- 动态黑名单适用于对安全性要求较高的网络中，避免用户攻击。
- STA 数量限制适用于用户数超过 AP 容量的情况下。
- 负载均衡适用于用户需要均衡的分布到多台 AP 上的场景。
- 关联控制适用于电子书包场景中。

协议规范

- 无。

2.2 典型应用

典型应用	场景描述
瘦 AP 组网	使用瘦 AP 组网，至少包括一台 AC、一台 AP
大会议室场景	使用瘦 AP 组网，至少包括一台 AC、两台 AP
电子书包场景	使用瘦 AP 组网，至少包括一台 AC、两台 AP

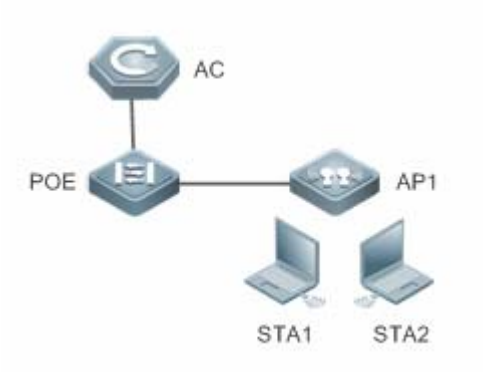
2.2.1 瘦AP组网

应用场景

在无线网络中，部署一台 AC 设备，在 AC 上开启动态黑名单、STA 数量限制。

以下图为例，在 AC 设备上开启动态黑名单、STA 数量限制。

图 2-1



【注释】 AC：无线控制器设备。
POE：交换机设备，作为 AP 的网关。
AP：无线接入设备。
STA1、STA2：用户设备，作为 STA 来使用。

功能部属

- 在 AC 设备上开启动态黑名单、STA 数量限制。

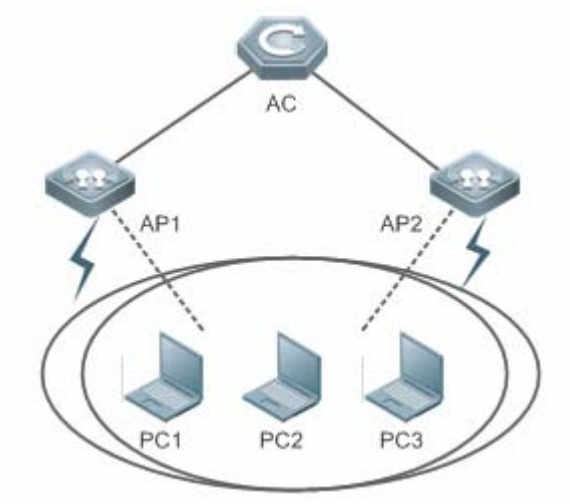
2.2.2 大会议室场景

应用场景

在大会议室中，通常用户众多，需要将用户均衡的分布到几台 AP 上，避免某些 AP 关联太多的用户，导致无线网速变慢，影响用户体验。

以下图为例，在会议室中部署两台 AP：AP1 和 AP2，使得 STA 能够均衡的分布到两台 AP 上。

图 2-2



【注释】 AC：无线控制器设备。
AP1、AP2：无线接入设备。
PC1、PC2、PC3：用户设备，作为 STA 来使用。

功能部属

- 在 AC 设备上开启负载均衡，将 AP1 和 AP2 加入到负载均衡组中。

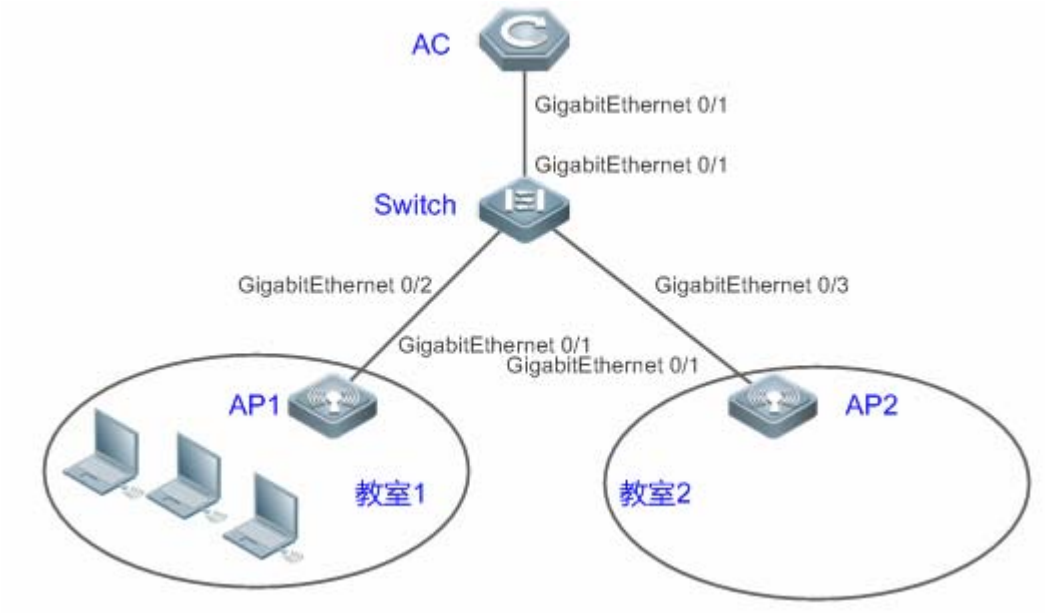
2.2.3 电子书包场景

应用场景

在无线网络中，部署一台 AC 设备，多台 AP 设备分别部署到多个教室。当教师 STA 关联到一台 AP 之后，要求学生 STA 也关联到同一组 AP 中，这样可以保证网络传输速度。

以下图为例，AP1 属于教室 1，AP2 属于教室 2。当教师 STA 关联到 AP1 时，学生的 STA 只能关联到 AP1 上面，不能关联到 AP2，这样发完同一个教室的流量只会发给 AP1，不会发给 AP2，避免影响到 AP2 上的用户。

图 2-3



【注释】 AC：无线控制器设备。
POE：交换机设备，作为 AP 的网关。
AP1、AP2：无线接入设备。

在电子书包应用场景中，如果教师机使用的是有线，为了达到关联控制的目的，也必须将终端包中的某台 STA 配置为主 STA，至于由谁来使用这台主 STA 由用户自己决定，比如可以将终端包中的主 STA 交给班长，由班长来使用；或者将主 STA 交给老师来控制，使得从 STA 可以做正确关联，从 STA 正确关联之后，教师就可以将该主 STA 放在一边，实际授课时再使用有线。

功能部属

- 在 AC 设备上开启关联控制功能，将 AP 加入到指定的关联控制域中。

2.3 功能详解

基本概念

无。

功能特性

功能特性	作用
动态黑名单	能够针对非法用户的关联进行检测。
STA 数量限制	对 STA 的数量进行限制。
负载均衡	能够让 STA 均衡的分布在多台 AP 上。

radio 间负载均衡	能够让 STA 均衡地分布在同一 AP 的各 radio 间。
关联控制	能够让从 STA 跟着主 STA 关联到同一组 AP 上。
STA 管理	对于一些没有流量的 STA 也要能够将其踢下线，从而回收资源。
STA 日常 syslog 抑制	STA 日常 syslog 的输出速率进行抑制

2.3.1 动态黑名单

动态黑名单，对于某些恶意、非法的 STA，AC 要能够对这些 STA 进行惩罚，让在一段时间内不能够上线，同时还需要具备将这些 STA 踢下线的功能。

工作原理

统计一段时间内，STA 关联失败的次数，包括用户名密码错误。当关联失败的次数超过一定阈值时，会将 STA 加入黑名单中。在黑名单中的 STA 在一段时间内不允许关联上线。

2.3.2 STA数量限制

STA 数量限制是为了根据各个 AP 不同的负载能力，对所能关联的 STA 数量进行限制，从而避免 AP 过载照成资源不够用的风险。

工作原理

当 STA 上线的时候，判断当前关联的 STA 数目是否超过阈值，如果超过阈值，则不允许 STA 上线。

2.3.3 负载均衡

负载均衡是为了让 AC 下所管理的 AP 能够比较均衡的承受负载，这里的负载可以认为是流量，也可以认为是关联的 STA 个数，其目的就是为了避免有些 AP 出现过载，而有些 AP 处于空闲的状态。

工作原理

在 STA 上线过程中，若 STA 关联的 AP 上的负载超过配置的启动门限值，则判断该 AP 对应的负载均衡组中的所有 AP 之间的负载差值是否超过阈值。如果超过阈值，则不允许 STA 在该 AP 上线。此负载差值可以配置为用户数量，也可以是流量。

为了避免 STA 只能收到一个 AP 的信号时，由于负载均衡而无法关联上线，可以配置负载均衡次数限制功能，当连续 2 次由于负载均衡关联失败之后，第 3 次就不再进行均衡，允许用户关联上线。

2.3.4 Radio间负载均衡

Radio 间负载均衡是对 AP 内各个 radio 之间的负载进行的均衡，目的是避免单一 radio 的负载过大。同样，这里的负载可以是流量，也可以是关联的 STA 个数。

工作原理

Radio 间负载均衡的原理与均衡组负载均衡基本相同，但用户可以分别配置同频 radio (同为 2.4G 或 5G) 和不同频 radio 的负载均衡启动门限值和阈值。若 AP 的所有 radio 属于同频，则同频配置生效，反之则不同频配置生效。

2.3.5 关联控制

关联控制，是控制无线 STA 关联行为的一种方法。通过对 STA 进行分组，定义其中一台 STA 为主 STA，其他 STA 为从 STA，控制从 STA 只能跟随主 STA 的方式，使得从 STA 关联的无线网络必须与主 STA 关联的无线网络相同，从而达到控制。

工作原理

将无线网络需要覆盖的范围划分成若干个关联控制域，在每个关联控制域中部署一台或多台 AP，再对无线终端进行分组，严格控制终端能关联的控制域。比如，学校的电子书包应用，一个学校有很多个教室，每个教室里都安装有无线 AP，无线信号是在空间中传播的，当两个相邻的教室都在用电子书包上课时，理想的状况是，教师机和学生机都关联到本教室的 AP 上，这样，每个教室各上各的课，互不干扰。这就要求一个教室就是一个关联控制域，这个教室里的所有学生机和教师机都关联到本教室的无线 AP 上。

关联控制的目的是为了防止终端在有多个无线网络选择的情况下进行胡乱关联 ,对于网络配置是有一定前提的。主要包括如下：

- AC 会根据预先配置的关联控制域和终端包信息，将所有终端包中的主 STA 信息都下发到所有关联控制域的 AP 上，并将这些 AP 上生成该主 STA 的白名单信息。
- 由于所有终端包的主 STA 信息已经在 AP 的白名单列表中，应用关联控制功能时，需要主 STA 首先与指定控制域对应的 SSID 进行关联；主 STA 完成关联后，AC 会根据该主 STA 所在的终端包配置，将对应的所有从 STA 下发到该关联控制域的所有 AP 上并生成白名单列表，从而允许从 STA 关联到本控制域中来。
- 当主 STA 解关联下线后，所有对应的从 STA 也都会跟着下线，并从关联控制域的 AP 上的白名单列表中删除。
- 上述的过程可以简单地概括为从 STA 跟着主 STA 走，主 STA 关联到哪个关联控制域的 AP 上，从 STA 也必须跟着关联到这个控制域的某个 AP 上，因为只有在这个关联控制域的 AP 上才有对应从 STA 的白名单列表，其他关联控制域的 AP 上没有，这样就可以保证 STA 不会胡乱关联。

2.3.6 STA管理

STA 管理，是用来管理 STA 的上下线逻辑处理。

工作原理

正常情况下，STA 下线时会发解关联报文通告 AC STA 下线。当 STA 无故下线（例如用户将网卡拔出），使得 STA 不会发送解关联报文给 AC，使得 AC 无法获知 STA 下线消息。这样，AC 通过检测 STA 的流量，发现一段时间内 STA 无流量，则认为 STA 已经下线，将 STA 进行下线处理。

2.3.7 STA日常syslog抑制

STA 日常 syslog 抑制是为了防止 STA 上下线频繁时，syslog 输出过多导致 CPU 偏高。

工作原理

对每秒输出的 syslog 条数进行统计，当这一秒内输出的 syslog 条数达到配置的上限时，这一秒内将不再输出 syslog，达到抑制的效果，下一秒将重新统计。

2.4 产品说明

NBR800G、NBR950G、NBR1500G、NBR2000G 不支持无线集成 AC 功能；NBR108G-P、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持无线集成 AC 功能。

2.5 配置详解

配置项	配置建议 & 相关命令	
动态黑名单	必须配置。用于开启动态黑名单功能。	
	sta-blacklist enable	开启动态黑名单功能
	可选配置。用于配置动态黑名单参数。	
	sta-blacklist lifetime	配置动态黑名单老化时间
	sta-blacklist detect-time	配置动态黑名单检测时间
	sta-blacklist fail-limit	配置关联失败次数上限
STA 数量限制	可选配置。用于配置最大允许的用户数。	
	sta-limit	配置最大用户数
	sta-limit radio	配置 AP 的 radio 下允许的最大用户数
负载均衡	必须配置。用于配置负载均衡基本信息。	
	num-balance-group create	创建数量负载均衡组
	num-balance-group add	将 AP 加入数量负载均衡组
	num-balance-group del	将 AP 从数量负载均衡组中删除
	flow-balance-group create	创建流量负载均衡组

	flow-balance-group add	将 AP 加入流量负载均衡组
	flow-balance-group del	将 AP 从流量负载均衡组中删除
	可选配置。用于配置负载均衡参数。	
	num-balance-group num	配置数量负载均衡组的阈值
	num-balance-group mode	配置数量负载均衡组的工作模式
	flow-balance-group flow	配置流量负载均衡组的阈值
	flow-balance-group radio-flow	指定流量负载均衡组使用 AP 上传的流量信息
Radio 间负载均衡	必须配置。用于开启 radio 间负载均衡功能。	
	inter-radio-balance flow-balance enable	开启 radio 间流量负载均衡功能
	inter-radio-balance num-balance enable	开启 radio 间数量负载均衡功能
	可选配置。用于配置负载均衡参数。	
	inter-radio-balance flow-balance dual-band	配置不同频 radio 间流量负载均衡参数
	inter-radio-balance flow-balance same-band	配置同频 radio 间流量负载均衡参数
	inter-radio-balance num-balance dual-band	配置不同频 radio 间数量负载均衡参数
	inter-radio-balance num-balance same-band	配置同频 radio 间数量负载均衡参数
关联控制	必须配置。用于开启关联控制功能。	
	package	配置终端包
	primary-sta	配置终端包中的主 STA
	secondary-sta	配置终端包中的从 STA
	control-zone	配置关联控制域
	ap	配置 AP 信息
	assoc-control	开启关联控制
STA 管理	可选配置。用于配置 STA 无流量下线时间。	
	sta-idle-timeout	配置 STA 无流量下线时间
STA 日常 syslog 抑制	可选配置。用于设置 STA 日常 syslog 的最大输出速率。	
	sta-logging rate-limit	配置 STA 日常 syslog 抑制的速率值

2.5.1 动态黑名单

配置效果

- 当检测到某个 STA 在指定时间内关联失败达到一定次数，则将此 STA 加入黑名单中禁止其继续关联。

注意事项

- 时间并不是固定的，会在 detect-time 秒～（detect-time + 5）秒之间。在实际配置时需要考虑到这个因素。
- 对于存在多种认证方式的场景，只要有其中一种认证方式失败，STA 的关联失败次数就会加 1。多种认证方式组合举例：psk+web，psk+mab+web，psk+mab，mab+web，1x+web。

配置方法

↘ 开启动态黑名单功能

- 在 AC 或者胖 AP 上配置，必须配置。

【命令格式】 **sta-blacklist enable**
【参数说明】 -
【缺省配置】 黑名单功能默认关闭
【命令模式】 AC 配置模式
【使用指导】 -

↘ 调整动态黑名单参数

- 在 AC 或者胖 AP 上配置，可选配置。
- 配置黑名单老化时间：如果觉得黑名单表项老化时间不合适，可以进行调整。
- 使用 **sta-blacklist lifetime** 命令可以配置动态黑名单老化时间。老化时间越长，加入黑名单的 STA 不允许关联上线的时间越长。
- 使用 **sta-blacklist detect-time** 命令可以配置检测时间，检测时间越短，对于非法 STA 检测越灵敏，误报也越多。
- 使用 **sta-blacklist fail-limit** 命令可以动态黑名单关联失败上限，如果实际环境中关联失败次数不合适，可以进行调整。关联失败上限越大，STA 允许尝试的次数越多。

【命令格式】 **sta-blacklist lifetime** *seconds*
【参数说明】 *seconds*：配置黑名单中 STA 的老化时间，范围在 60～1200 秒。
【缺省配置】 300s
【命令模式】 AC 配置模式
【使用指导】 -

【命令格式】 **sta-blacklist detect-time** *seconds*
【参数说明】 *seconds*：STA 的检测时间，配置范围在 5-60 秒。
【缺省配置】 60s
【命令模式】 AC 配置模式
【使用指导】 配置 STA 的检测时间，STA 在第一次失败时就被列为可疑的攻击端，如果在检测时间内 STA 关联失败次数达到次数上限（即 fail-limit）则把该 STA 加入黑名单。

【命令格式】 **sta-blacklist fail-limit** *number*
【参数说明】 *number*：关联失败次数上限。配置范围为 1-100

【缺省配置】 动态黑名单关联失败上限为 5 次

【命令模式】 AC 配置模式

【使用指导】 -

检验方法

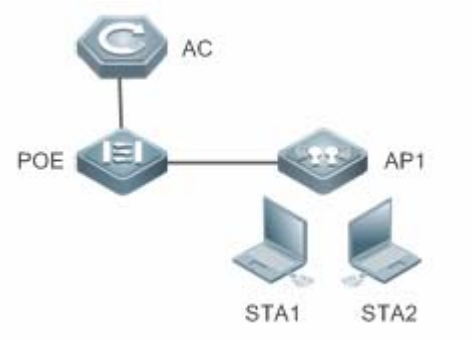
- 用 **show sta-blacklist** 查看当前在黑名单中的 STA。

配置举例

↘ 配置动态黑名单功能

【网络环境】

图 2-4



【配置方法】 ● 配置动态黑名单功能。

AC

```
AC# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
AC(config)# ac-controller
AC(config-ac)# sta-blacklist enable
```

【检验方法】 ● AP 与 AC 建立 CAPWAP 连接之后，输入多次错误的密码，验证能够加入到黑名单中。

AC

```
AC# show sta-blacklist
Num        STA MAC        Add time
---------- -------------- -------------------
1          0080.1111.1111 2013-07-02 13:56:22
2          0090.2222.3333 2013-07-02 13:56:35
3          0070.1111.2233 2013-07-02 13:57:08
```

常见错误

- 无。

2.5.2 STA数量限制

配置效果

- 在无线网络中，可以限制一台 AC、一个 WLAN、一台 AP 或者一台 AP 的 radio 最大用户数。

注意事项

- AC、WLAN、AP 和 AP 的 radio 下的 STA 数量限制是同时生效的，也就是说，需要同时满足的情况下，STA 才能上线。
- AC 上 STA 数量限制受 license 影响。

配置方法

↘ 配置 STA 数量限制

- 在 AC 或者胖 AP 上，可选配置。
- 如果无线网络中 STA 数目比较多，可以打开 STA 数量限制，可以使得更多的 STA 上线，但是总体带宽就会变小。
- 使用 **sta-limit** 命令可以配置 STA 数量限制，STA 数量限制越大，可以关联的 STA 数目越多。
- 基于 AC 的 STA 数量限制，缺省为 32*最大支持 AP 数；基于 WLAN 的 STA 数量限制，缺省不限制；基于 AP 的 STA 数量限制，对于离线 AP 或批量配置，缺省为 64；对于在线 AP，缺省值依型号而定。
- 使用 **sta-limit radio** 命令可以配置基于 AP 的 radio 的 STA 数量限制，STA 数量限制越大，可以关联的 STA 数目越多。缺省不限制。注意基于 radio 的配置与基于 AP 的配置相互独立，不能认为各 radio 限制之和为整机限制。
- 使用 **sta-limit per-ap** 命令可以配置某个 WLAN 下每台 AP 的 STA 数量限制，缺省不限制。若配置值超过 AP 的能力，以 AP 实际支持能力为准。

【命令格式】 **sta-limit** *max-num*

【参数说明】 *max-num*：最大用户数，取值范围因配置模式和设备而异。

【缺省配置】 在 AC 配置模式下：缺省值为 32 乘以 AC 可支持的 AP 数量（受 license 限制）。
在 AP 组配置模式下：缺省值为 64。
在 AP 配置模式下：离线 AP 或 ap-config all 的缺省值为 64，在线 AP 的缺省值根据 AP 的型号决定。
在 WLAN 配置模式下：缺省不做限制。

【命令模式】 AC 配置模式、WLAN 配置模式、AP 配置模式、AP 组配置模式

【使用指导】 若对于离线AP配置的最大用户数超过AP实际能力，AP上线后，将自动调整为实际支持的最大值。

【命令格式】 **sta-limit** *max-num* **radio** *radio-id*

【参数说明】 *max-num*：可支持的最大用户数，取值范围：1~156，缺省不做限制。
radio-id：配置的 radio 标识符，取值范围：1-32。

【缺省配置】 缺省不做限制

【命令模式】 AP 配置模式

AP 组配置模式

【使用指导】 若对于离线AP配置的最大用户数超过AP上该radio的实际能力，AP上线后，将自动调整为实际支持的最大值。注意AP整机用户数限制独立于本命令，不能认为各radio限制之和为整机限制。

【命令格式】 **sta-limit per-ap** *max-num*

【参数说明】 *max-num*：可支持的最大用户数，取值范围：1~1536，缺省不做限制。

【缺省配置】 缺省不做限制

【命令模式】 WLAN 配置模式

【使用指导】 -

检验方法

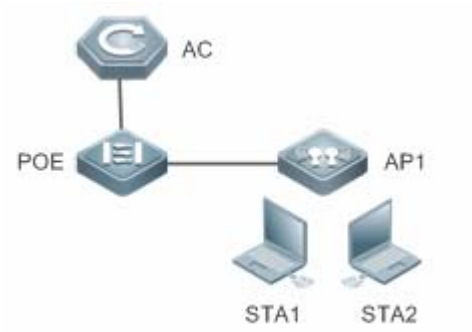
- 确认 STA 用户数的确收到限制。

配置举例

配置 STA 数量限制

【网络环境】

图 2-5



【配置方法】

- 配置 STA 数量限制。

AC

```
AC# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
AC(config)# ap-config ap1
AC(config-ap)# sta-limit 128
```

【检验方法】

- AP 与 AC 建立 CAPWAP 连接之后，查看配置信息：

AC

```
AC# show ap-config running
ap-config ap1
 sta-limit 128
!
```

常见错误

- 无。

2.5.3 负载均衡

配置效果

- 可以让一个负载均衡组的多台 AP 上用户均衡。

注意事项

- 负载均衡只对 STA 上线过程进行处理，对于 STA 下线过程不进行处理，因此 STA 下线之后，会存在 AP 间的流量差值或者 STA 数量差值超过阈值的情况。
- 负载均衡只在同类型(2.4G 或 5G)的 radio 之间进行，若 radio 类型不同，则仅当 AP 上报 STA 能力为双频时，才进行负载均衡。否则，仅支持 2.4G 的用户可能会在 5G 的 radio 没有用户的情况下，无法关联到 2.4G 的 radio。
- 配置流量负载均衡组使用 AP 上传的流量信息后，由于流量只在 AP 上，AC 上需要 AP 定时上传到 AC 上，因此在两次 AP 上传的间隔时间内，AC 上的流量是不会发生变化的，如果此时 AP 之间流量不均衡，则 STA 会一直关联不上流量多的 AP，需要等到 AP 将新流量上传为止。

配置方法

↘ 配置数量负载均衡组

- 在 AC 上配置，必须配置。
- 创建负载均衡组之后，才能将 AP 加入负载均衡组，并进行负载均衡的配置。

【命令格式】 **num-balance-group create** *group-name*
【参数说明】 *group-name*：均衡组名称
【缺省配置】 没有创建数量负载均衡组
【命令模式】 AC 配置模式
【使用指导】 -

↘ 将 AP 加入数量负载均衡组

- 在 AC 上配置，必须配置。
- 只有将 AP 加入到负载均衡组中，才能对该 AP 进行负载均衡。

【命令格式】 **num-balance-group add** *group-name ap-name*
【参数说明】 *group-name*：均衡组名称
ap-name：AP 名字

【缺省配置】 没有 AP 加入数量负载均衡组
【命令模式】 AC 配置模式
【使用指导】 -

配置流量负载均衡组

- 在 AC 上配置，必须配置。
- 创建负载均衡组之后，才能将 AP 加入负载均衡组，并进行负载均衡的配置。

【命令格式】 **flow-balance-group create** *group-name*
【参数说明】 *group-name*：均衡组名称
【缺省配置】 没有创建流量负载均衡组
【命令模式】 AC 配置模式
【使用指导】 -

将 AP 加入流量负载均衡组

- 在 AC 上配置，必须配置。
- 只有将 AP 加入到负载均衡组中，才能对该 AP 进行负载均衡。

【命令格式】 **flow-balance-group add** *group-name ap-name*
【参数说明】 *group-name*：均衡组名称
ap-name：AP 名字
【缺省配置】 没有 AP 加入流量负载均衡组
【命令模式】 AC 配置模式
【使用指导】 -

调整负载均衡组参数

- 在 AC 上配置，可选配置。
- 使用 **num-balance-group num** 命令可以配置数量负载均衡的阈值。负载均衡阈值越高，两台 AP 上关联的 STA 数量差值越大，越不均衡。
- 使用 **num-balance-group mode** 命令配置基于 radio 的数量负载均衡，开启基于 radio 的数量负载均衡，控制较精确，AP 间的均衡性会差些。
- 使用 **num-balance-group enable** 命令配置数量负载均衡组的启动门限值，较高的启动门限值意味着负载均衡仅在当前 AP 负载较高时才启动。
- 使用 **num-balance-group del** 命令可以从数量负载均衡组中移除一个 AP。
- 使用 **flow-balance-group flow** 命令可以配置流量负载均衡的阈值，负载均衡阈值越高，两台 AP 上流量差值越大，越不均衡。
- 使用 **flow-balance-group radio-flow** 命令可以配置流量负载均衡组使用 AP 上报的流量信息，在本地转发下，由于数据报文不经过 AC，AC 上无法获取到流量信息，必须使用 AP 上报的流量信息来进行负载均衡判断。
- 使用 **flow-balance-group enable** 命令配置流量负载均衡组的启动门限值，较高的启动门限值意味着负载均衡仅在当前 AP 负载较高时才启动。

- 使用 **flow-balance-group del** 命令可以从流量负载均衡组中移除一个 AP。
- 使用 **flow-balance-group base** 命令可以配置流量负载均衡的基准值，这是全局配置，不针对特定均衡组。
- 使用 **sta-balance num-limit enable** 命令可以开启负载均衡次数限制功能。

【命令格式】 **num-balance-group num** *group-name number*
【参数说明】 group-name：均衡组名称
number：负载阈值，默认 3，范围 0-20，其中 0 表示该均衡组不开启数量均衡功能。
【缺省配置】 缺省阈值为 3
【命令模式】 AC 配置模式
【使用指导】 -

【命令格式】 **num-balance-group mode** *group-name* { **radio-mode** | **ap-mode** }
【参数说明】 *group-name*：均衡组名称
【缺省配置】 基于 AP 的数量负载均衡
【命令模式】 AC 配置模式
【使用指导】 -

【命令格式】 **num-balance-group enable** *group-name number*
【参数说明】 *group-name*：均衡组名称
number：启动门限值，默认 3，范围 0-10，其中 0 表示该均衡组不开启数量均衡功能。
【缺省配置】 3
【命令模式】 AC 配置模式
【使用指导】 -

【命令格式】 **num-balance-group del** *group-name ap-name*
【参数说明】 *group-name*：均衡组名称
ap-name：AP 名字
【缺省配置】 无
【命令模式】 AC 配置模式
【使用指导】 -

【命令格式】 **flow-balance-group flow** *group-name number*
【参数说明】 *group-name*：均衡组名称
number：负载阈值，单位%，默认 5%，范围 0-1000，其中 0 表示该均衡组不开启流量均衡功能。其中百分比的基准默认为 10Mbps。
【缺省配置】 5%
【命令模式】 AC 配置模式
【使用指导】 -

【命令格式】 **flow-balance-group radio-flow** *group-name*
【参数说明】 配置指定流量负载均衡组使用 AP 上传的流量信息。
【缺省配置】 使用 AC 上 CAPWAP 数据通道的流量信息
【命令模式】 AC 配置模式
【使用指导】 用户可以配置流量负载均衡组使用 AP 上传的流量信息，这样该流量负载均衡组就接收 AP 定时发送来的流量信息来进行负载均衡。

【命令格式】 **flow-balance-group enable** *group-name number*
【参数说明】 *group-name*：均衡组名称
number：启动门限值，单位%，默认 5%，范围 0-500，其中 0 表示该均衡组不开启流量均衡功能。其中百分比的基准默认为 10Mbps。
【缺省配置】 默认 5%
【命令模式】 AC 配置模式
【使用指导】 -

【命令格式】 **flow-balance-group del** *group-name ap-name*
【参数说明】 *group-name*：均衡组名称
ap-name：AP 名字
【缺省配置】 无
【命令模式】 AC 配置模式
【使用指导】 -

【命令格式】 **flow-balance-group base** *number*
【参数说明】 *number*：流量基准值，默认 10Mbps，范围 1-100。
【缺省配置】 默认 10Mbps
【命令模式】 AC 配置模式
【使用指导】 -

【命令格式】 **sta-balance num-limit enable**
【参数说明】 无
【缺省配置】 缺省情况下，该功能关闭
【命令模式】 AC 配置模式
【使用指导】 -

检验方法

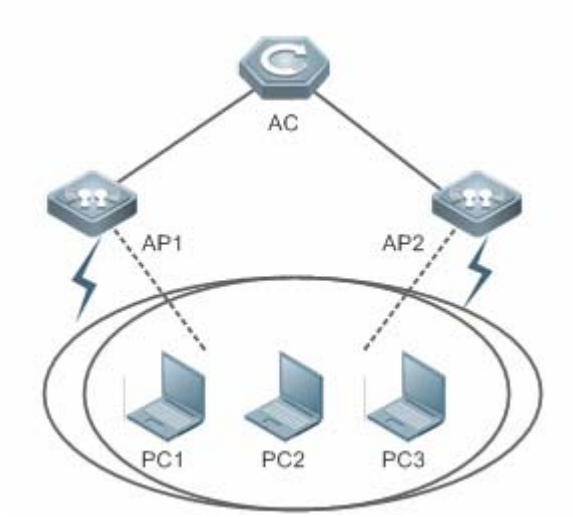
- 数量负载均衡：查看负载均衡组内的 AP 下 STA 数的差值是否在阈值范围内。
- 流量负载均衡：查看负载均衡组内的 AP 的流量差值是否在阈值范围内。

配置举例

↘ 配置基于流量的负载均衡

【网络环境】

图 2-6



【配置方法】

- 创建一个负载均衡组。
- 配置该负载均衡组的负载阈值为 1000kbps。
- 配置 AP1、AP2 加入负载均衡组 test-group（配置为同一个负载均衡组的 AP 即认为该组所服务的 PC 都能搜索到该组的所有 AP 的射频信号）。

AC

```
AC# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
AC(config)#ac-controller
AC(config-ac)# flow-balance-group create test-group
AC(config-ac)# flow-balance-group flow test-group 10
AC(config-ac)# flow-balance-group add test-group AP1
AC(config-ac)# flow-balance-group add test-group AP2
```

【检验方法】

- 查看负载均衡组的配置情况：

AC

```
AC# show ac-config flow-balance summary
Group           State Enable         Threshold Base mode       AP NAME
--------------- ----- -------------- --------- ---- ----------
-----------------------------------------------------------------------
test-group         UP      5*100kbps        10%   10 ap-mode(0) AP1, AP2
```

常见错误

- 无。

2.5.4 Radio间负载均衡

配置效果

- 开启 Radio 间负载均衡的 AP 上，各 radio 之间的负载将尽可能均衡。

注意事项

- 智分场景不适用此功能。由于不同 radio 的信号覆盖不同空间范围，STA 可能只能收到一个或几个 radio 的信号，此时不能开启 radio 间负载均衡功能。
- 负载均衡只对 STA 上线过程进行处理，对于 STA 下线过程不进行处理，因此 STA 下线之后，会存在 AP 间的流量差值或者 STA 数量差值超过阈值的情况。
- 若 STA 意图关联的 radio 与最低负载 radio 类型不同，则仅当 AP 上报 STA 能力为双频时，才进行负载均衡。否则，仅支持 2.4G 的用户可能会在 5G 的 radio 没有用户的情况下，无法关联到 2.4G 的 radio。
- 配置流量负载均衡组使用 AP 上传的流量信息后，由于流量只在 AP 上，AC 上需要 AP 定时上传到 AC 上，因此在两次 AP 上传的间隔时间内，AC 上的流量是不会发生变化的，如果此时 AP 之间流量不均衡，则 STA 会一直关联不上流量多的 AP，需要等到 AP 将新流量上传为止。
- 负载均衡参数的配置区分同频 radio 和不同频 radio，在 AP 上线时将检查 AP 的类型。若 AP 拥有不同频 radio，则不同频配置生效，反之则同频配置生效。
- 对于某个特定 AP 而言，只要 ap-config、ap-group、ap-config all 三种模式中的一种开启了负载均衡，该 AP 就开启了负载均衡。若三种模式下配置的负载均衡参数不同，则按照 ap-config > ap-group > ap-config all 的优先顺序生效。
- radio 间负载均衡在 5min 内对同一 STA 最多只会连续拒绝关联 2 次，若 STA 第 3 次仍关联到负载较高的 radio，将允许关联。因此，radio 间负载均衡的实际效果与 STA 的具体行为有关。

配置方法

↘ 开启 radio 间流量负载均衡

- 在 AC 上配置，必须配置。开启后同一 AP 的不同 radio 之间将尽可能保持流量均衡。
- 可以针对单个 AP 开启，也可以对某个 AP 组下的所有 AP 开启，或开启全部 AP（ap-config all 模式下配置）。

【命令格式】 **inter-radio-balance flow-balance enable**
【参数说明】 -
【缺省配置】 没有开启 radio 间流量负载均衡
【命令模式】 AP 配置模式，AP 组配置模式
【使用指导】 -

↘ 开启 radio 间数量负载均衡

- 在 AC 上配置，必须配置。开启后同一 AP 的不同 radio 之间将尽可能保持用户数均衡。

- 可以针对单个 AP 开启，也可以对某个 AP 组下的所有 AP 开启，或开启全部 AP（ap-config all 模式下配置）。

【命令格式】 **inter-radio-balance num-balance enable**
【参数说明】 -
【缺省配置】 没有开启 radio 间数量负载均衡
【命令模式】 AP 配置模式，AP 组配置模式
【使用指导】 -

↘ 调整 radio 间负载均衡参数

- 在 AC 上配置，可选配置。进行网络优化时可以按实际需求调整各参数。
- 使用 **inter-radio-balance flow-balance dual-band enable-load** *en-num* **threshold** *thrs-num* 配置不同频 radio 流量负载均衡的启动门限值和阈值。门限值越低则负载均衡越容易启动，阈值越低则越均衡。
- 使用 **inter-radio-balance flow-balance same-band enable-load** *en-num* **threshold** *thrs-num* 配置同频 radio 流量负载均衡的启动门限值和阈值。门限值越低则负载均衡越容易启动，阈值越低则越均衡。
- 使用 **inter-radio-balance num-balance dual-band enable-load** *en-num* **threshold** *thrs-num* 配置不同频 radio 数量负载均衡的启动门限值和阈值。门限值越低则负载均衡越容易启动，阈值越低则越均衡。
- 使用 **inter-radio-balance num-balance same-band enable-load** *en-num* **threshold** *thrs-num* 配置同频 radio 数量负载均衡的启动门限值和阈值。门限值越低则负载均衡越容易启动，阈值越低则越均衡。

【命令格式】 **inter-radio-balance flow-balance dual-band enable-load** *en-num* **threshold** *thrs-num*
【参数说明】 en-num：启动门限值，单位 100Kbps，默认 10，范围 1-1000。
thrs-num：负载阈值，单位 100Kbps，默认 10，范围 1-1000。
【缺省配置】 缺省启动门限值为 10，负载阈值为 10
【命令模式】 AP 配置模式，AP 组配置模式
【使用指导】 -

【命令格式】 **inter-radio-balance flow-balance same-band enable-load** *en-num* **threshold** *thrs-num*
【参数说明】 en-num：启动门限值，单位 100Kbps，默认 5，范围 1-1000。
thrs-num：负载阈值，单位 100Kbps，默认 5，范围 1-1000。
【缺省配置】 缺省启动门限值为 5，负载阈值为 5
【命令模式】 AP 配置模式，AP 组配置模式
【使用指导】 -

【命令格式】 **inter-radio-balance num-balance dual-band enable-load** *en-num* **threshold** *thrs-num*
【参数说明】 en-num：启动门限值，默认 8，范围 1-20。
thrs-num：负载阈值，默认 8，范围 1-20。
【缺省配置】 缺省启动门限值为 8，负载阈值为 8
【命令模式】 AP 配置模式，AP 组配置模式
【使用指导】 -

【命令格式】 **inter-radio-balance num-balance same-band enable-load** *en-num* **threshold** *thrs-num*

【参数说明】 en-num：启动门限值，默认 10，范围 1-1000。

thrs-num：负载阈值，默认 10，范围 1-1000。

【缺省配置】 缺省启动门限值为 10，负载阈值为 10

【命令模式】 AP 配置模式，AP 组配置模式

【使用指导】 -

检验方法

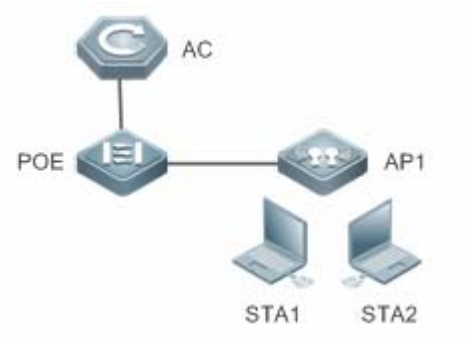
- 数量负载均衡：**show ap-config summary** 查看开启均衡的 AP 下各 radio 的 STA 数的差值是否在阈值范围内。
- 流量负载均衡：**show ac-config client** 查看开启均衡的 AP 下各 radio 的流量差值是否在阈值范围内。

配置举例

↘ 为默认 AP 组内的所有 AP 开启 radio 间数量负载均衡

【网络环境】

图 2-7



【配置方法】

- 进入默认 AP 组配置。
- 开启数量负载均衡。

AC

```
AC# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
AC(config)#ap-group default
AC(config-group)# inter-radio-balance num-balance enable
```

【检验方法】

- 查看 show run 中的配置：

AC

```
AC# show run | begin ap-group default
ap-group default
 inter-radio-balance num-balance enable
```

常见错误

- 无。

2.5.5 关联控制

配置效果

- 从 STA 上线受主 STA 上线影响，跟着主 STA 关联到同一组的 AP 中。

注意事项

- 删除终端包时，所有与该终端包相关的配置都将被清除，而且如果这个时候该终端包中有 STA 在线，则会造成所有这些 STA 下线。
- 一部终端包对应只能配置一个主 STA，如果多次配置不同的主 STA 信息，则以最后一次的配置为准。
- 从一个终端包中删除主 STA 时，则可能会造成该 STA 下线，同时也会造成所有从 STA 下线。
- 从一个终端包中删除一个从 STA 时，可能会造成该 STA 下线。
- 关联控制域不能重名，否则将得出到一个错误提示。另外，删除关联控制域时，所有与该控制域相关的配置将被清除，而且可能会导致关联到该控制域中的终端包对应的 STA 下线。
- 删除一个关联控制域中的 AP 信息时，可能会导致关联在该 AP 上的终端包对应的 STA 下线。

配置方法

↘ 配置终端包

- 在 AC 或者胖 AP 上配置，必须配置。
- 配置终端包之后，才能配置主从 STA 信息。

【命令格式】 **package** *pkg-name*
【参数说明】 *pkg-name*：终端包名称，长度：1-32。
【缺省配置】 无配置终端包
【命令模式】 全局配置模式
【使用指导】 -

↘ 配置终端包中的主从 STA

- 在 AC 或者胖 AP 上配置，必须配置。
- 使用 **primary-sta** 命令配置主 STA。只能配置一台主 STA，从 STA 会跟随主 STA 关联到同一组 AP 上。
- 使用 **secondary-sta 命**令配置从 STA。配置了从 STA，从 STA 会跟随主 STA 关联到同一组 AP 上。

【命令格式】 **primary-sta** *mac-address*
【参数说明】 *mac-address*：STA 的 MAC 地址。
【缺省配置】 没有配置主 STA
【命令模式】 终端包配置

【使用指导】 -

【命令格式】 **secondary-sta** *mac-address*
【参数说明】 *mac-address*：STA 的 MAC 地址。
【缺省配置】 没有配置从 STA
【命令模式】 终端包配置
【使用指导】 -

配置关联控制域

- 在 AC 或者胖 AP 上配置，必须配置。
- 配置管理控制域。
- 只有配置了关联控制域之后，才能将 AP 加入到关联控制域中。

【命令格式】 **control-zone** *czone-name*
【参数说明】 *czone-name*：关联控制域名称，长度：1-64。
【缺省配置】 无关联控制域配置
【命令模式】 全局配置模式
【使用指导】 -

将 AP 加入关联控制域中

- 在 AC 或者胖 AP 上配置，必须配置。
- 将 AP 加入到关联控制域中。
- 只有加入到关联控制域中的 AP，才能进行关联控制。

【命令格式】 **ap** *WORD*
【参数说明】 *WORD*：AP 名称，长度：1-64。
【缺省配置】 没有 AP 加入到关联控制域中
【命令模式】 关联控制域配置模式
【使用指导】 -

开启关联控制功能

- 在 AC 或者胖 AP 上配置，必须配置。只有使用 **assoc-control** 这个命令才能开启关联控制功能。
- 开启关联控制功能。

【命令格式】 **assoc-control**
【参数说明】 -
【缺省配置】 关联控制功能关闭
【命令模式】 全局配置模式
【使用指导】 -

检验方法

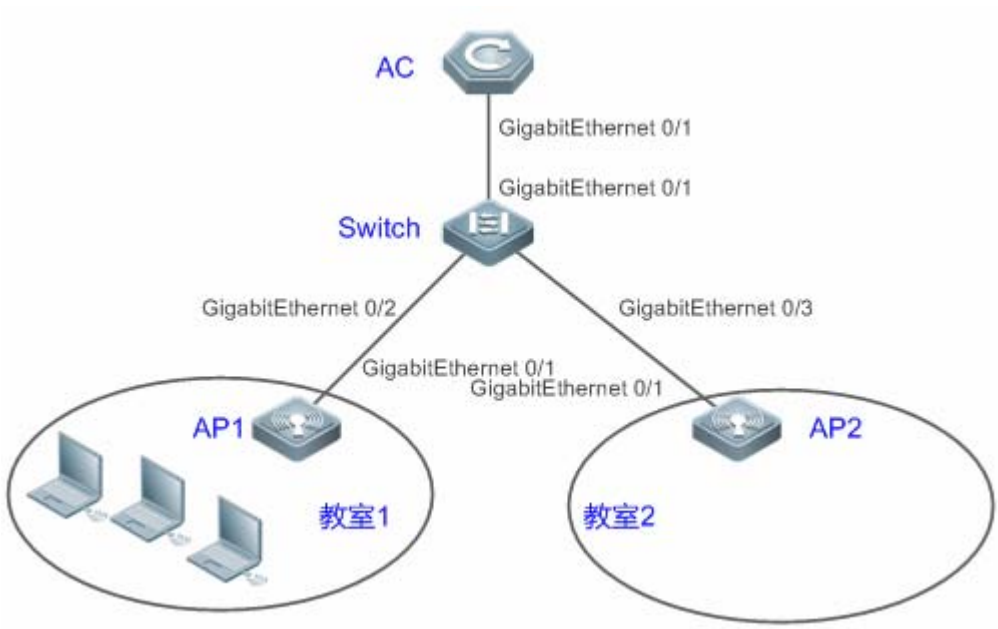
- 确认从 STA 能够跟着主 STA 关联到同一组 AP 上。

配置举例

配置瘦 AP 架构电子书包

【网络环境】

图 2-8



【配置方法】

- 配置终端包以及对应的主 STA 和从 STA。
- 配置关联控制域以及对应的 AP 信息。
- 开启关联控制功能。

AC

```
AC# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
AC(config)# package 推车 1
AC(config-package)# primary-sta 00d0.f800.0001
AC(config-package)# secondary-sta 00d0.f800.0002
AC(config-package)# secondary-sta 00d0.f800.0003
AC(config-package)# exit
AC(config)# control-zone 教室 1
AC(config-czone)# ap AP1
AC(config-czone)# exit
AC(config)# control-zone 教室 2
AC(config-czone)# ap AP2
AC(config-czone)# exit
AC(config)#assoc-control
```

【检验方法】

- 显示验证关联控制运行状态。

- 显示验证终端包配置。
- 显示验证关联控制域配置

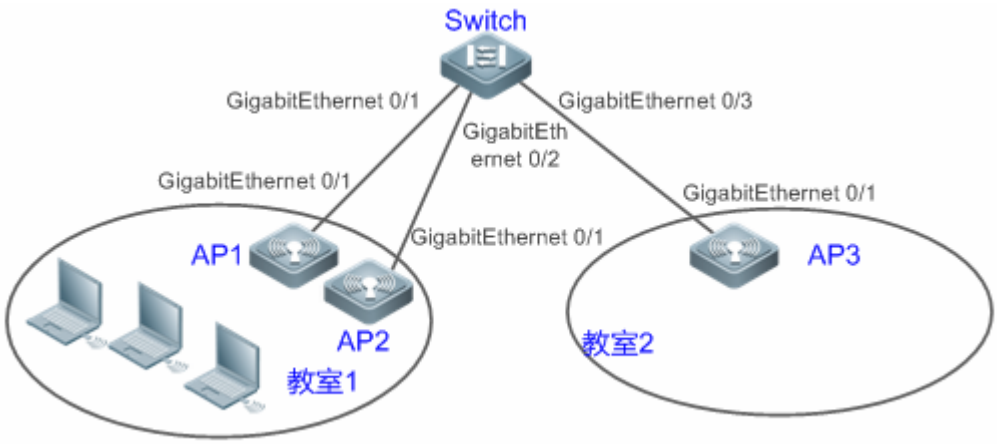
AC

```
AC# show assoc-control
Association control is enabled.
AC# show package
total package num : 1
========= 推车 1 =========
primary STA : 00d0.f800.0001
secondary STA num : 2
00d0.f800.0002
00d0.f800.0003
AC# show control-zone
control zone num : 2
control-zone AP
-------------       ------------------------
教室 1                AP1   00d0.f800.889e
教室 2                AP2   00d0.f800.889f
```

配置胖 AP 架构电子书包

【网络环境】

图 2-9



【配置方法】

- 配置终端包以及对应的主 STA 和从 STA。
- 配置关联控制域以及对应的 AP 信息。
- 开启关联控制功能。

AP1

```
AP1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
AP1(config)# package 推车 1
AP1(config-package)# primary-sta 00d0.f800.0001
AP1(config-package)# secondary-sta 00d0.f800.0002
AP1(config-package)# secondary-sta 00d0.f800.0003
```

```
AP1(config-package)# exit
AP1(config)# control-zone 教室 1
AP1(config-czone)# ap AP1
AP1(config-czone)# exit
AP1(config)# assoc-control
```

AP3

```
AP3# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
AP3(config)# package 推车 1
AP3(config-package)# primary-sta 00d0.f800.0001
AP3(config-package)# secondary-sta 00d0.f800.0002
AP3(config-package)# secondary-sta 00d0.f800.0003
AP3(config-package)# exit
AP3(config)# control-zone 教室 2
AP3(config-czone)# ap AP3
AP3(config-czone)# exit
AP3(config)# assoc-control
```

【检验方法】

- 显示验证关联控制运行状态。
- 显示验证终端包配置。
- 显示验证关联控制域配置

AP1

```
AP1# show assoc-control
Association control is enabled.
AP1# show package
total package num : 1
========= 推车 1 =========
primary STA : 00d0.f800.0001
secondary STA num : 2
00d0.f800.0002
00d0.f800.0003
AP1# show control-zone
control zone num : 1
control-zone AP
-------------      ------------------------
教室 1                AP1   00d0.f800.889e
```

AP3

```
AP3# show assoc-control
Association control is enabled.
AP3# show package
========= 推车 1 =========
primary STA : 00d0.f800.0001
secondary STA num : 2
00d0.f800.0002
```

```
00d0.f800.0003
AP3# show assoc-control
control zone num : 1
control-zone AP
-------------      ------------------------
教室 1                AP3   00d0.f800.889f
```

常见错误

- 无。

2.5.6 STA管理

配置效果

- STA 可以在规定的时间内无流量下线。

注意事项

- 无。

配置方法

↘ 配置无线用户老化时间

- 在 AC 或者胖 AP 上配置，可选配置。
- 配置时间越短，无流量的用户越快被检测到，越快下线。

【命令格式】 **sta-idle-timeout** *value*
【参数说明】 *value*：老化时间值，单位秒，取值范围：60~86400，缺省值为 300 秒。
【缺省配置】 缺省情况下，该定时器为 300s
【命令模式】 AP 配置模式
【使用指导】 -

检验方法

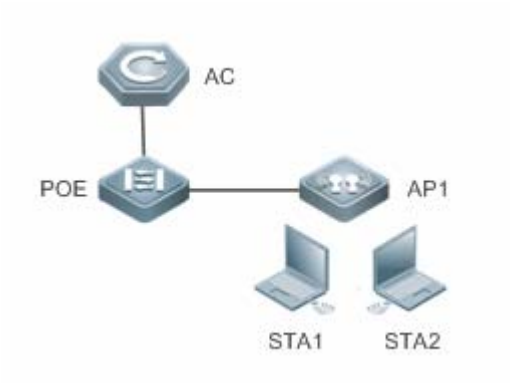
- 检查该配置是否配置成功。

配置举例

↘ 配置无线用户老化时间

【网络环境】

图 2-10



【配置方法】

- 配置无线用户老化时间。

AC

```
AC# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
AC(config)# ap-config ap1
AC(config-ap)# sta-idle-timeout 15
```

【检验方法】

- AP 与 AC 建立 CAPWAP 连接之后，查看配置信息：

AC

```
AC# show ap-config running
ap-config ap1
 sta-idle-timeout 15
!
```

常见错误

- 无。

2.5.7 STA日常syslog抑制

配置效果

- 即使 STA 上下线频繁，每秒输出的日常 syslog 条数不超过一定数量。

注意事项

- 无。

配置方法

配置 syslog 抑制的速率值

- 在 AC 上配置，可选配置。
- 配置 syslog 抑制的速率值：配置速率值越大，每秒允许输出的 syslog 条数越多。

【命令格式】 **sta-logging rate-limit** *limit-num*
【参数说明】 *limit-num*：速率值，单位条每秒，取值范围：0~10000，缺省值为 5 条每秒。
【缺省配置】 syslog 每秒输出不超过 5 条，即上限为 5 条/秒
【命令模式】 AC 配置模式
【使用指导】 -

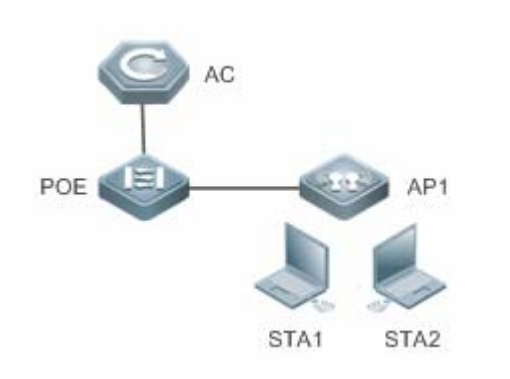
检验方法

- 通过 show running 检查该配置是否配置成功。

配置举例

配置 STA 日常 syslog 抑制

【网络环境】
图 2-11



【配置方法】 ● 配置 syslog 抑制。

AC

```
AC# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
AC(config)# ac-controller
AC(config-ac)# sta-logging rate-limit 50
```

【检验方法】 ● AP 与 AC 建立 CAPWAP 连接之后，查看配置信息：

AC

```
AC# show running
ac-controller
 sta-logging rate-limit 50
!
```

常见错误

- 无。

2.6 监视与维护

清除各类信息

无。

查看运行情况

作用	命令
查看本 AC 上所有连接的 STA 的信息	**show ac-config client** [**by-ap-name | 802.11a | 802.11b | 802.11n | 802.11g** | **802.11ac | other**]
查看指定无线用户的详细信息	**show ac-config client detail** *mac-address*
查看所有无线用户的统计信息。	**show ac-config client statistic**
查看基于流量的负载均衡组的详细配置信息	**show ac-config flow-balance summary**
查看基于数量的负载均衡组的详细配置信息	**show ac-config num-balance summary**
查看当前的关联控制功能开启情况	**show assoc-control**
查看关联控制域配置	**show control-zone** [**summary** | *czone-name*]
查看终端包配置	**show package** [*pkt-name*]
查看当前在黑名单中的 STA	**show sta-blacklist**

查看调试信息

无。

3 CAPWAP

3.1 概述

CAPWAP（Control And Provisioning of Wireless Access Points，无线接入点控制和规定）是为了解决 WLAN 大规模 AP 部署的问题而提出的协议。

在瘦 AP 网络框架中，无线控制器（AC）通过 CAPWAP 统一管理所有 AP，向指定 AP 下发控制策略，无需在各 AP 上单独配置。CAPWAP 协议在 AP 和 AC 之间建立控制通道和数据通道，其中控制通道用于 AC 配置 AP 以及 AP 向 AC 发送事件通告，数据通道用于 AP 和 AC 之间发送数据报文。

协议规范

- RFC5415：Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification
- RFC5416：Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11
- RFC5417：Control And Provisioning of Wireless Access Points (CAPWAP) Access Controller DHCP Option

3.2 典型应用

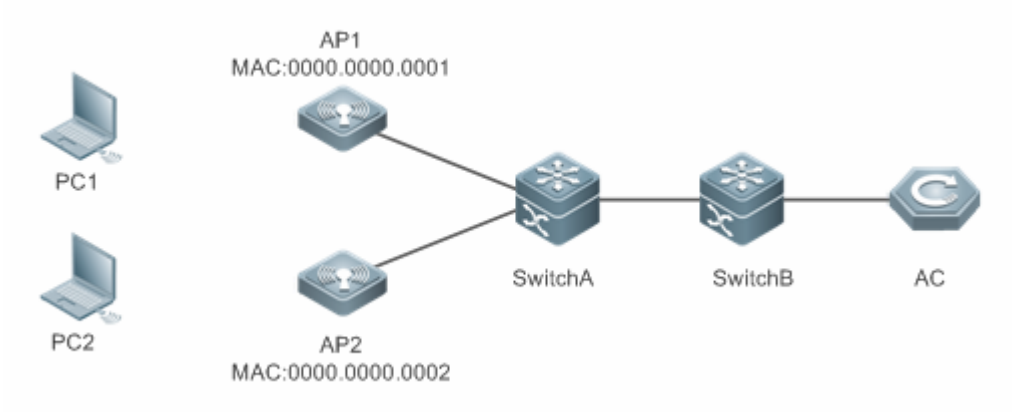
典型应用	场景描述
动态建立 CAPWAP 隧道	AP 通过交换机接入 AC，在 AP 上联的交换机上搭建 DHCP Server。AP 通过 DHCP 方式动态获取 AC 地址，和 AC 建立 CAPWAP 隧道。
静态建立 CAPWAP 隧道	AP 通过交换机接入 AC。在 AP 上配置静态 ACIP，AP 通过配置的静态 ACIP 和 AC 建立 CAPWAP 隧道。
升级 AP	AP 和 AC 间建立 CAPWAP 隧道后，AC 通过 CAPWAP 对 AP 大规模进行升级。

3.2.1 动态建立CAPWAP隧道

应用场景

AP 通过交换机接入 AC，在 AP 上联的交换机上搭建 DHCP Server。DHCP Server 配置 DHCP 地址池、下发 Option138 选项，option138 为 AC 的 IP 地址。AP 获取到 AC 地址，和 AC 建立 CAPWAP 隧道。以下图为例，无线控制器（AC）、交换机（Switch A 和 Switch B）、无线接入点（AP1 和 AP2）之间通过 Trunk Port 相连；PC1 接入 AP1，PC2 接入 AP2。

图 3-1



【注释】 Switch：交换机。
AC：无线控制器。

功能部署

- 对于瘦 AP 网络，无需单独对 AP 进行配置。当 AP 上电时，首先要获取 IP 地址。因此，需要在网络中部署 DHCP Server。没有 DHCP server 则使用 AC 自带的 DHCP 功能实现 DHCP Server。
- AC 与 AP 之间跨三层通信，需要 DHCP Server 下发 Option 138 选项，option138 为 AC 的 IP 地址，AP 获取到 AC 的 IP 地址后会与 AC 建立 CAPWAP 通信隧道。
- 在 AC 上配置 loopback 接口地址或配置 **capwap ctrl-ip** *ip-address* 作为建立 CAPWAP 的源地址。
- 配置路由连接实现 AC 与 AP 获得的 IP 地址互通。

3.2.2 静态建立CAPWAP隧道

应用场景

AP 通过配置的静态 ACIP 和 AC 建立 CAPWAP 隧道，AP 通过交换机接入 AC，拓扑图同上图。

功能部署

- 静态配置 AC 的 IP 地址，AP 将向这些静态 IP 地址发送发现请求报文探测 AC 的有效性，然后选择一台 AC 加入。
- 在 AC 上配置 loopback 接口地址作为建立 CAPWAP 的源地址。
- 配置路由连接实现与 AP 获得的 IP 地址互通。

3.2.3 升级AP

应用场景

AP 通过静态配置 AC 地址或者的动态方式获取 AC 地址 ,和 AC 建立 CAPWAP 隧道。AP 通过交换机接入 AC ,拓扑图如上图。

功能部署

- 在 AC 上配置地址作为建立 CAPWAP 的源地址。
- 配置路由连接实现与 AP 获得的 IP 地址互通。
- 在 AC 上激活本地存放的 AP 软件。

3.3 功能详解

基本概念

STA、AP、AC

STA：无线工作站，带有无线网卡的设备，如笔记本、手机等。

AP：无线接入点，提供无线信号使得 STA 能够接入。

AC：无线控制器，提供无线连接及相关服务的功能。

控制通道、数据通道

控制通道：用于 AC 配置 AP 以及 AP 向 AC 发送事件通告。

数据通道：用于 AP 和 AC 之间发送数据报文。

AC 发现

AC 发现阶段：AP 可以通过广播、组播、DHCP、DNS、静态配置等方式发送“发现请求消息”来发现 AC，然后从一个或者多个 AC 中选择最佳的 AC 开始建立 CAPWAP 会话。

DTLS

CAPWAP 控制通道利用 DTLS 协议进行密钥协商和加密。

Option 选项

DHCP 的 Option 选项中可以携带 AC 的 IPv4 地址，AP 通过获取 DHCP 服务器下发的 Option 信息来获取 AC 的地址。

AP 支持通过 option 138 和 option 43 两种方式获取 AC 的 IP 地址。在配置 AP 的 DHCP Server 时，需要配置对应的 option 选项设置 AC 的 IP 地址，否则 AP 将无法通过 DHCP 发现的方式发现 AC。

这里 option 138 和 option 52 是 RFC5417 定义的标准格式，option 43 的格式由厂商自定义，目前支持解析如下 option 43 的格式：

格式一：以指定 AC 的 IP 地址为 1.1.1.1 为例，对应的配置为 option 43 hex f10401010101

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

+-+

```
|  o ption-code   | option-length | Sub-opt Type   |  S ub-opt Len   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                              Server   Address                                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

option-code：option 选项，这里为 43（十进制）

option-length：option 选项数据长度，不包括 option-code 和 option-length

Sub-opt Type：子选项类型，这里为 0xF1，即十进制 241

Sub-opt Len：子选项的载荷长度，即地址数量*4

Server Address：服务器的地址

格式二：以指定 AC 的 IP 地址为 1.1.1.1 为例，对应的配置为 option 43 hex 800700000101010101

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  o ption-code   | option-length | Sub-opt Type   |  S ub-opt Len   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            PXE Server Type             | PXE Server Num|                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
          PXE Server   Address                                |       ...           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

option-code：option 选项，这里为 43（十进制）

option-length：option 选项数据长度，不包括 option-code 和 option-length

Sub-opt Type：子选项类型，这里为 0x80，即十进制 128

Sub-opt Len：子选项的载荷长度，即地址数量*4+3

Server Type:服务器类型，取值为 0x0000

Server Num: 服务器地址数量

Server Address：服务器的地址

格式三：以指定 AC 的 IP 地址为 1.1.1.1 为例，对应的配置为 option 43 hex 01010101

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   option-code   | option-length |            Server   Address            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Server   Address              |                .....                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

option-code：option 选项，这里为 43（十进制）

option-length：option 选项数据长度，不包括 option-code 和 option-length

Server Address：服务器的地址

功能特性

功能特性	作用
AP 发现 AC	AP 发现潜在的 AC。
AP 加入 AC	AP 从一个或者多个 AC 中选择最佳 AC 加入，建立 CAPWAP 隧道。
AP 升级	AP 和 AC 建立 CAPWAP 隧道后，AC 可以对大规模 AP 进行版本升级。
隧道数据转发	AP 和 AC 建立 CAPWAP 隧道，通过数据通道发送数据报文。

3.3.1 AP发现AC

AP 通过发送发现请求消息，发现潜在的 AC。

工作原理

AP 被连接到网络时即进入发现 AC 的过程。AP 使用广播、组播或单播方式发送“发现请求”消息，当使用单播方式时，需首先通过 DHCP 或 DNS、静态配置 AC 方式获得 AC 的 IP 地址列表。

3.3.2 AP加入AC

AP 从周围潜在的 AC 中选择一个最佳 AC 加入，建立 CAPWAP 隧道。

工作原理

AP 发送“发现请求”报文后，收到发现请求报文的 AC 返回“发送应答”给 AP，AP 在应答的 AC 中，选择一个最佳 AC 建立 DTLS 连接。DTLS 连接建立成功后，AP 发送“加入请求”，AC 回复“加入应答”确认 AP 加入该 AC 的管理范围，并向该 AP 提供服务。

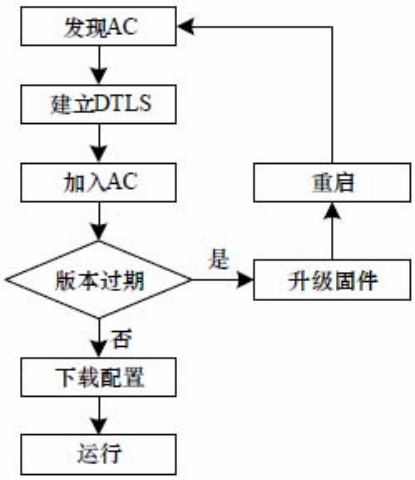
3.3.3 AP升级

AP 和 AC 建立 CAPWAP 隧道后，AC 可以对大规模 AP 进行版本升级。

工作原理

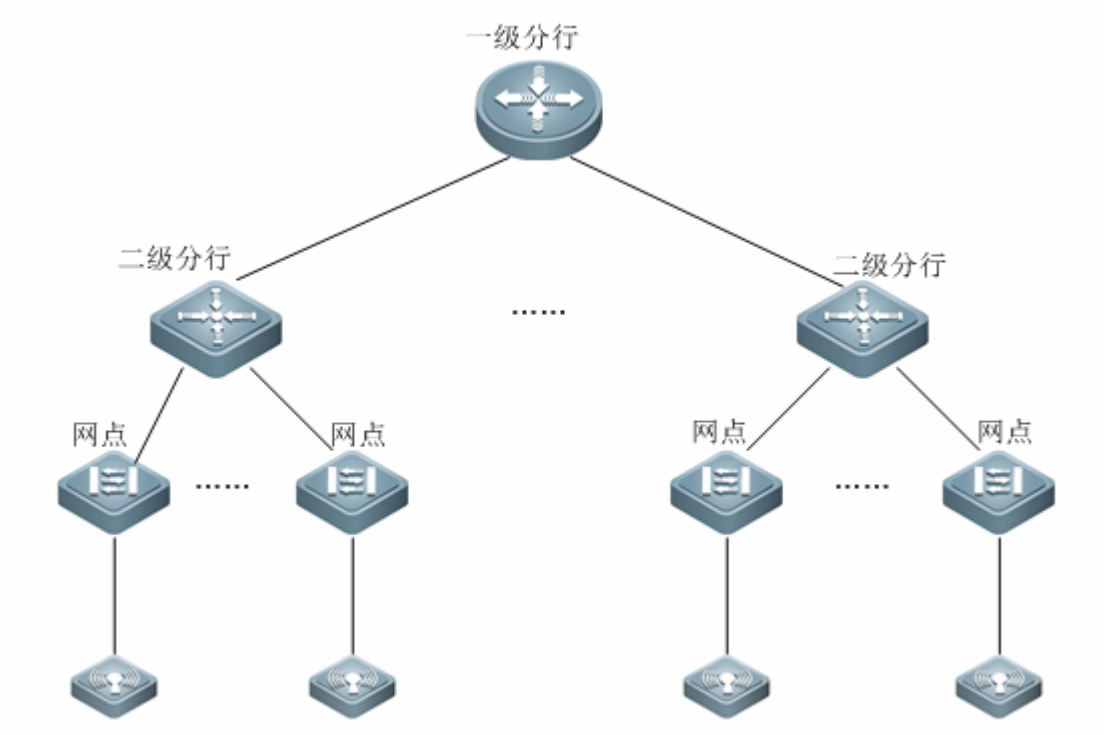
AP 加入 AC 后，若 AP 的固件版本过期，则进入升级固件过程，AP 从 AC 下载最新版本的固件，升级成功以后重启，重新进入发现过程；若 AP 固件为最新版本，则从 AC 下载配置参数，随后进入运行阶段。下图为工作原理示意图。

图 3-2



带宽限制升级应用的典型场景如下图。

图 1-3



以银行 AP 升级为例，说明配置方法。假设银行包含一个一级分行和多个二级分行，每个分行下有数百个网点，一个网点部署 1 个 AP，AC 放置在一级分行。一级分行与二级分行之间的带宽为 20Mbps，二级分行与网点之间的带宽为 2Mbps，为了不影响银行正常业务，AP 升级所占用的带宽不能超过可用带宽的 50%。假设二级分行的个数为 8，AC 上配置 8 个升级组，每个二级分行下网点的 AP 加入到对应的升级组中，对于每个 AP 来说，其最大可用带宽为 1Mpbs，所以对所有 AP 配置带宽 128(1Mbps 转 KB 单位)。每个二级分行下允许并发集中升级的 AP 个数为 10 个(10M/1M)。同时建议配置 AC 集中升级最大并发数为升级组数与升级组下最大并发数的乘积，即 80.

3.3.4 隧道数据转发

AP 和 AC 间建立 CAPWAP 隧道后，通过其中的数据通道可以实现数据报文的转发。

工作原理

CAPWAP 协议在 AP 和 AC 之间建立控制通道和数据通道。其中控制通道用于 AC 配置 AP 以及 AP 向 AC 发送事件通告，该通道必须加密。数据通道用于 AP 和 AC 之间发送 802.11 帧或 802.3 帧。运行在 IPV4 协议栈时候，CAPWAP 使用 UDP 进行数据传输。

3.4 产品说明

NBR800G、NBR950G、NBR1500G、NBR2000G 不支持无线集成 AC 功能；NBR108G-P、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持无线集成 AC 功能。

3.5 配置详解

配置项	配置建议&相关命令	
配置 AC 位置	可选配置，配置 AC 的位置信息。	
	location	配置 AC 的位置信息，以便查看 AC 的物理位置。
配置定制版本号	可选配置，配置定制版本号。	
	set-version	配置定制版本号
配置 AP 位置	可选配置，配置 AP 的位置信息。	
	location	配置 AP 的位置信息，以便查看 AP 的物理位置。
配置 AP 时间同步	可选配置，配置 AP 同步 AC 的时间。	
	timestamp	配置 AP 同步 AC 的时间。
配置 AP 的缺省 VLAN	可选配置，指定 AP 的 Native VLAN	
	ap-vlan	配置 AP 的缺省 VLAN
配置 AP 有线用户的 VLAN	可选配置，在提供以太网接口用于有线用户接入的 AP 中，指定用户所在的 VLAN。	
	wired-vlan	配置有线网络接口使用的 VLAN。
配置 AP 关闭有线网络接口	可选配置，在提供以太网接口用于有线用户接入的 AP 中，关闭有线口。	
	wired-interface	配置 AP 关闭有线网络接口

配置 AP 的 WAN 口子接口	⚠ 可选配置，配置 AP 的 WAN 口子接口	
	ap-subif	配置 AP 的 WAN 口子接口
配置 AP 加入 AC	⚠ 可选配置，在 AC 上配置 AP，用于 CAPWAP 隧道建立。	
	ac-domain-name	配置 AP 的 DNS 域名，用于获取 AC 的地址。
	acip ipv4	配置 AP 接入 AC 的静态 IP 地址。
	ip address	配置静态 IP 地址、掩码和网关。
配置 AP 上执行命令	⚠ 可选配置，在 AC 上配置 AP，用于 CAPWAP 隧道建立。	
	exec-cmd	配置 AP 或者 AP 组内所有 ap-config 执行命令
配置瘦 AP	⚠ 可选配置，在 AP 上进行预配置，用于 CAPWAP 隧道建立。	
	acip ipv4	配置 AP 接入 AC 的静态 IP 地址。
	apip	配置静态 IP 地址、掩码和网关。
	apip pppoe	配置 AP 使用 PPPoE 拨号方式获取地址
配置升级 AP	⚠ 可选配置，用于配置 AP 升级。	
	ap-serial	创建 AP 产品系列名称 ,指定哪些 AP 产品型号属于该系列。
	ap-image	AP 配置模式下，配置为指定 AP 升级版本。 AC 配置模式下，配置指定的 AP 产品系列使用指定的 AP 软件版本升级，或者设置自适应升级方式进行升级。
	active-bin-file	激活 AP 软件版本文件。
	capwap upgrade max-concurrent	配置 AC 升级 AP 的最大并发数
	capwap upgrade group	AC 配置模式下，配置带宽控制升级组
	ap-upgrade band-width	AP 配置模式下，配置 AP 集中升级带宽
	ap-upgrade group	AP 配置模式下，AP 加入带宽控制升级组
配置 CAPWAP 的控制地址	⚠ 可选配置，用于配置 CAPWAP 隧道的控制地址，未配置时默认使用 loopback 口的地址作为控制地址。	
	capwap ctrl-ip	配置 CAPWAP 隧道的控制 IP 地址。
配置 CAPWAP 分片	⚠ 可选配置，用于配置 CAPWAP 分片功能。	
	capwap mtu	配置指定 AP 的隧道路径 MTU。
	capwap fragment enable	配置指定 AP 开启 CAPWAP 分片。
配置 CAPWAP 加密	⚠ 可选配置，用于配置 CAPWAP 加密功能。	
	capwap dtls enable	配置 CAPWAP 控制通道加密。
配置 CAPWAP 接入控制	⚠ 可选配置，用于控制 CAPWAP 最大并发数。	

	capwap max-concurrent	配置 CAPWAP 最大并发个数。
配置 CAPWAP 的心跳保活间隔	⚠ 可选配置，用于配置 CAPWAP 隧道的心跳保活间隔。	
	echo-interval	配置 CAPWAP 的心跳保活间隔。
配置 CAPWAP 的报文重传次数	可选配置，用于配置 CAPWAP 报文的最大重传次数。	
	capwap max-retransmit	配置 CAPWAP 的报文最大重传次数。

3.5.1 配置AC位置

配置效果

- 配置 AC 的位置信息，方便用户在 WLAN 网络中查看 AC 的位置。

注意事项

- 最多可配置 255 个字符，不能包含空格。

配置方法

- 可选配置，在网络中存在较多 AC 设备时可配置以便查看 AC 位置。
- 进入 AC 配置模式，通过 **location** 命令在 AC 上进行配置。
- 通过 **no** 命令恢复缺省值。

【命令格式】 **location** *location-string*

【参数说明】 *location-string*：配置该 AC 的位置描述符，最多可配置 255 个字符，不能带空格。

【缺省配置】 AC 的位置信息为 Ruijie_COM

【命令模式】 AC 配置模式。

【使用指导】 缺省情况下，AC 的位置信息为 Ruijie_COM，用户可以根据实际需要，为各 AC 配置位置信息，方便用户在 WLAN 网络中查看 AC 的位置。

检验方法

- 通过 **show ac-config** 命令查看 AC 的位置信息，确认是否配置成功。

配置举例

↘ 配置 AC 的位置信息为 computer-layer2

【配置方法】
- 进入 AC 配置模式。
- 配置 AC 的位置信息。

AC

```
Ruijie(config)#ac-controller
Ruijie(config-ac)# location computer-layer 2
```

- 通过 no 命令可以恢复 AC 的缺省位置信息。

AC

```
Ruijie(config)#ac-controller
Ruijie(config-ac)#no location
```

【检验方法】 通过 **show ac-config** 命令可以查看当前 AC 的位置信息。

AC

```
Ruijie#show ac-config
ac location      :Ac_COM
```

常见错误

- 无。

3.5.2 配置定制版本号

配置效果

- 进行软件版本定制。

注意事项

- 最多可配置 63 个字符。

配置方法

- 可选配置。
- 当需要进行设备的版本定制时，可以通过该命令定制显示的软件版本号。
- 通过 **no** 命令恢复缺省值。

【命令格式】 **set-version** *string*

【参数说明】 *string*：定制的版本号。

【缺省配置】 无

【命令模式】 AC 配置模式。

【使用指导】 该命令将配置 AC 设备的软件版本号，同时会将该版本下发给 AP 进行版本号设置。

检验方法

- 通过 show version 命令进行版本查看。

配置举例

↘ 配置定制软件版本号为 RGOS 10.4(2B17)-SP2

【配置方法】
- 进入 AC 配置模式。
- 配置定制版本号。

AC

```
Ruijie(config)#ac-controller
Ruijie(config-ac)# set-version RGOS 10.4(2B17)-SP2
```

【检验方法】 通过 show version 命令进行版本查看。

AC

```
Ruijie#show version
System software version : RGOS 10.4(2B17)-SP2
```

常见错误

- 无。

3.5.3 配置AP位置

配置效果

- 实现配置 AP 的所在位置。

注意事项

- 最多可配置 255 个字符，不能包含空格。

配置方法

↘ 配置 AP 的位置信息。

- 可选配置。
- 通过命令 **location** 配置 AP 的位置信息。
- 当需要获知 AP 的物理位置时，可以在 AC 上 AP 配置模式下配置位置信息以便查看 AP 的物理位置。

【命令格式】 **location** *location-string*
【参数说明】 *location-string*：AP 的位置信息，最多可配置 255 字符,不能带空格。
【缺省配置】 AP 的位置信息为空
【命令模式】 AP 配置模式。
【使用指导】 -

检验方法

- 通过 **show ap-config running** 命令，查看 AP 位置信息。

配置举例

↘ 配置 AP0001 的位置信息为 AP-company

【配置方法】
- 进入 AC 的 AP 配置模式。
- 配置 AP0001 的位置信息为 AP-company。

AC

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# location AP-company
```

【检验方法】
- 通过 show ap-config running 查看 AP0001 的位置信息。

AC

```
Ruijie#show ap-config running
!
ap-config AP0001
location AP-company
!
```

常见错误

- 无。

3.5.4 配置AP时间同步

配置效果

- 实现指定 AP 或 AP 组内所有 AP 同步本 AC 的时间。

注意事项

- 无。

配置方法

↘ 配置指定 AP 或 AP 组内所有 AP 同步本 AC 的时间。

- 可选配置。

- 当需要设置 AP 的时间和 AC 一致时，可以在 AC 上 AP 配置模式或 AP 组配置模式通过 **timestamp** 命令实现。

【命令格式】 **timestamp**
【参数说明】 -
【缺省配置】 -
【命令模式】 AP 配置模式或 AP 组配置模式.
【使用指导】 -

检验方法

- 通过查看 AC 和 AP 时间是否一致来检验。

配置举例

↘ 配置 AP0001 同步本 AC 的时间

【配置方法】
- 进入 AC 的 AP 配置模式。
- 配置 AP0001 同步 AC 的时间。

AC

```
Ruijie(config)# ap-config AP0001

Ruijie(config-ap)# timestamp
```

- 【检验方法】
  - 通过 show clock 查看 AP0001 时间和 AC 时间

AC

```
Ruijie#show clock
16:41:05 UTC Thu, Oct 17, 2013
```

常见错误

- 无。

3.5.5 配置AP的缺省VLAN

配置效果

- AP 会将带有 Native VLAN 的帧自动剥去 TAG 再进行转发，即本地转发模式下，用户的 VLAN 与 Native VLAN 相同时，该用户的帧将不带 TAG 转发，由接入交换机决定用户所属的 VLAN。

注意事项

- 配置该命令将使已经在线的 AP 断开重建。

- 在 WDS 部署中，ROOT-BRIDGE 和 NONROOT-BRIDGE 设备需要规划相同的 AP-VLAN，否则 NONROOT-BRIDGE 设备将无法同 ROOT-BRIDGE 共享同一个地址池，甚至影响 NONROOT-BRIDGE 设备报文的正常转发。
- 该命令仅在本地转发模式下某个 WLAN 下的 STA 要 AP 一样由接入交换机分配所属的 VLAN ,且另一个 WLAN 在又要求其 STA 属于 VLAN 1 但接入交换机的 Native VLAN 不为 VLAN 1 时才需要进行配置。一般情况下都不需要该配置。
- 如果配置的静态 DHCP 地址池，并且制定了 Client ID 使用 BVI 1 接口了，则配置该命令将导致 AP 的 BVI 接口改变，这样就需要修订 DHCP 服务器的配置了，否则将无法获取到地址。
- 当 AP 使用 PPPoE 拨号来获取地址时，这时 CAPWAP 将选择 dialer 1 作为源接口，STA 的流量将无法带 TAG 转发，该命令也没有意义。

配置方法

配置 AP 的缺省 VLAN

- 可选配置。
- 当需要规划用户的的 Native VLAN 时，可以配置 AP 的缺省 VLAN 和用户的 VLAN 相同，用户的 VLAN 将和 AP 一样由接入交换机决定。

【命令格式】 **ap-vlan** *vlan-id*

【参数说明】 *vlan-id*：指定的 VLAN，取值范围为 1~4094，缺省值为 1。

【缺省配置】 缺省值为 1

【命令模式】 AP 配置模式/所有 AP 配置模式。

【使用指导】 AP 会将带有 Native VLAN 的帧自动剥去 TAG 再进行转发 ,即本地转发模式下 ,用户的 VLAN 与 Native VLAN 相同时，该用户的帧将不带 TAG 转发，由接入交换机决定用户所属的 VLAN。

检验方法

- 通过 **show running/show ap-config running** 命令，查看所有 AP/AP 配置信息。

配置举例

配置 AP1 配置 AP1 的 Native VLAN 的 VLAN ID 为 20

【配置方法】
- 进入 AC 的 AP 配置模式。
- 配置 AP1 的线网络接口使用 VLAN 20。

AC

```
Ruijie(config)# ap-config AP1

Ruijie(config-ap)# ap-vlan 20
```

【检验方法】
- 通过 show ap-config running 查看 AP1 的位置信息。

AC

```
Ruijie#show ap-config running
!
ap-config AP1
ap-vlan 20
!
```

常见错误

假设交换机规划的 Native VLAN 是 20，希望有线或无线用户和 AP 都属于 VLAN 20，这时进行如下错误配置：

AC 上：

```
Ruijie(config)# ap-config AP120
Ruijie(config-ap)# wired-vlan 20
Ruijie(config-ap)# exit
Ruijie(config)#wlan-config 1 ssid
Ruijie(config-wlan)#tunnel local
Ruijie(config-wlan)#exit
Ruijie(config)#ap-group default
Ruijie(config-ap-group)#interface-mapping 1 20 radio 1
```

交换机上：

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# switchport mode trunk
Ruijie(config-if-GigabitEthernet 0/1)# switchport trunk native vlan 20
```

这里错误的原因是用户的 VLAN 和 AP 的 Native VLAN 不同，所以在 AP 的上行报文是需要带 TAG 20 进行转发的，在接入交换机上将透传 VLAN 20 并为用户分配地址。但在下行报文中，由于交换机的 Native VLAN 是 20，所以下行报文将不带 TAG 进行转发，而 AP 的 Native VLAN 默认是 1，所以报文将无法转发给用户，造成有线用户和无线用户都无法获取到地址。

有如下两种方法进行配置修改：

方法一 将 wired-vlan 20 和 interface-mapping 1 20 radio 1 改为 wired-vlan 1 和 interface-mapping 1 1 radio 1 交换机的 Native VLAN 保持不变。

方法二：增加配置 AP 的 native VLAN 配置，其他配置不变

AC 上：

```
Ruijie(config)# ap-config AP120
Ruijie(config-ap)# ap-vlan 20
```

3.5.6 配置AP有线用户的VLAN

配置效果

- 在提供以太网接口用于有线用户接入的 AP 中，指定用户所在的 VLAN。

注意事项

- 该命令对所有 AP 都可配置，但配置只对具有有线网络接口的 AP 型号生效。
- 在无线 AP 模式下(AP 只做无线接入，不为用户分配地址)，当配置有线网络接口使用的 VLAN 与 AP 相同，则有线口的报文所属的 VLAN 将由接入交换机决定，而非本配置指定的 vlan。当有线网络接口的报文需要带 TAG 转发时，接入交换机的 Native VLAN 不能和有线网络接口的 VLAN 相同，否则报文将无法转发到有线网络接口中。
- 在无线路由模式下(AP 可以为用户分配地址)，有线用户将从 AP 上的 DHCP 地址池获取地址，地址池所在的接口对应的 VLAN 与该命令指定的 VLAN 需要相同。
- 当使能有线口配置保存且有线口 VLAN 与 AP 的 Native VLAN 不同时，AP 重启后若无法获取地址，将无法通过有线口进行管理，这时可以长按 AP 的 reset 键来恢复出厂配置。

配置方法

↘ 配置 AP 有线接口的接入 VLAN

- 可选配置。
- 当需要规划有线用户的 VLAN 与 AP 的 VLAN 不同时，可以在 AC 上配置。

【命令格式】 **wired-vlan** *vlan-id* [**port** *port-id*] **auto-save**

【参数说明】 *vlan-id*：指定的 VLAN，取值范围为 1~4094，缺省情况下，有线网络接口使用的 VLAN 与 AP 相同。

port-id : 指定有线网络接口，取值范围为 1~4。

auto-save：在 AP 上保存配置，设备重启后可以恢复配置。

【缺省配置】 缺省未配置，表示有线网络接口使用的 VLAN 与 AP 相同

【命令模式】 AP 配置模式/所有 AP 配置模式/AP 组配置模式

【使用指导】 在无线 AP 模式下(AP 只做无线接入，不为用户分配地址)，当配置有线网络接口使用的 VLAN 与 AP 相同，则有线口的报文所属的 VLAN 将由接入交换机决定 ,而非本配置指定的 vlan。当有线网络接口的报文需要带 TAG 转发时，接入交换机的 Native VLAN 不能和有线网络接口的 VLAN 相同，否则报文将无法转发到有线网络接口中。

在无线路由模式下(AP 可以为用户分配地址)，有线用户将从 AP 上的 DHCP 地址池获取地址，地址池所在的接口对应的 VLAN 与该命令指定的 VLAN 需要相同。

瘦 AP 是零配置启机的，其配置从 AC 下发。可以配置 auto-save 参数让 AP 上自动保存有线口的配置信息。这样当 AP 和 AC 断开时，AP 重启将能恢复有线口的配置，使得用户仍然可以通过有线口接入网络。

检验方法

- 通过 **show running/show ap-config running** 命令，查看所有 AP/AP 配置信息。

配置举例

配置 AP1 的有线网络接口使用 VLAN 20

【配置方法】
- 进入 AC 的 AP 配置模式。
- 配置 AP1 的线网络接口使用 VLAN 20。

AC

```
Ruijie(config)# ap-config AP1
Ruijie(config-ap)# wired-vlan 20
```

【检验方法】
- 通过 show ap-config running 查看 AP1 的配置信息。

AC

```
Ruijie#show ap-config running
!
ap-config AP1
wired-vlan 20
!
```

常见错误

- 无。

3.5.7 配置AP有线接口管理状态

配置效果

- 关闭或开启 AP 的有线网络接口。

注意事项

- 该命令对所有 AP 都可配置，但配置只对具有有线网络接口的 AP 型号生效。
- 当关闭 AP 有线口，AP 重启后，将无法通过有线口进行管理，这时可以长按 AP 的 reset 键来恢复出厂配置。

配置方法

配置 AP 有线接口管理状态

- 可选配置。
- 当需要关闭或开启 AP 的有线接口时，可以在 AC 上配置。

【命令格式】 **wired-interface** [**port** *port-id*] **enable**

【参数说明】 *port-id*：指定有线网络接口，取值范围为 1~4。

enable：指定的有线口开启。

【缺省配置】 缺省配置，有线网络接口都是开启的。

【命令模式】 AP 配置模式/所有 AP 配置模式/AP 组配置模式

【使用指导】 在提供以太网接口用于有线用户接入的 AP 中，当应用场景不需要使用有线网络接入时，或者在网络部署实施阶段，有线网络还未实施完成的情况下，可以关闭 AP 的有线接口。

检验方法

- 通过 **show running/show ap-config running** 命令，查看所有 AP/AP 配置信息。

配置举例

配置 AP1 关闭所有有线网络接口

【配置方法】
- 进入 AC 的 AP 配置模式。
- 配置 AP 关闭所有有线网络接口。

AC

```
Ruijie(config)# ap-config AP1
Ruijie(config-ap)# no wired-interface enable
```

【检验方法】
- 通过 show ap-config running 查看 AP1 的配置信息。

AC

```
Ruijie#show ap-config running
!
ap-config AP1
no wired-interface enable
!
```

常见错误

- 无。

3.5.8 配置AP的WAN口子接口

配置效果

- 无线 AP 设备默认会创建 WAN 口的子接口用于实现 STA 数据流量带 TAG 转发。在无线路由模式下(AP 可以为用户分配地址)，用户的网关在 AP 上，相应的报文都不需要带 TAG 转发，可以使用该命令删除 AP 的 WAN 口子接口，同时也避免用户的网关地址相同造成地址冲突。

注意事项

- 当 AP 是通过 pppoe 拨号获取地址的，则 AP 的 WAN 口子接口将自动删除。该命令在拨号方式下将无法设置 AP 创建 WAN 口的子接口。

配置方法

↘ 配置 AP 的 WAN 口子接口

- 可选配置。
- 在无线路由模式下，删除 WAN 口的子接口，避免用户的网关地址相同时报文经过子接口泛洪出去造成地址冲突。

【命令格式】 **ap-subif enable**
【参数说明】 -
【缺省配置】 默认会创建 WAN 口的子接口
【命令模式】 AP 配置模式/所有 AP 配置模式
【使用指导】 -

检验方法

- 通过 **show running/show ap-config running** 命令，查看所有 AP/AP 配置信息。

配置举例

↘ 配置 AP1 去掉 WAN 口的子接口

【配置方法】
- 进入 AC 的 AP 配置模式。
- 配置 AP1 去掉 WAN 口的子接口。

AC

```
Ruijie(config)# ap-config AP1
Ruijie(config-ap)# no ap-subif enable
```

【检验方法】
- 通过 show ap-config running 查看 AP1 的配置信息。

AC

```
Ruijie#show ap-config running
!
ap-config AP1
 no ap-subif enable
!
```

常见错误

- 无。

3.5.9 配置AP加入AC

配置效果

- 静态配置 AC 地址，AP 将向这些 IP 地址发送发现请求报文探测 AC 的有效性。选择 AC 加入建立 CAPWAP 隧道。

注意事项

- 瘦 AP 一般都是零配置的，可以通过广播、组播、DHCP、DNS 来发现 AC，也可以通过静态配置的 AC 地址加入 AC。
- 设置 AP 的地址为静态地址将关闭 DHCP 功能，这时将无法通过 DHCP 的 OPTION 选项获取 AC 的地址，因此配置该命令前还需要先在 AP 配置模式下配置连接的 AC 地址，以便 AP 和 AC 不在同一个子网时能发现并加入 AC。
- 若 AP 当前的地址与 AC 命令指定的地址不一致，将更新 AP 的静态地址并重建 CAPWAP 隧道。

配置方法

↘ 配置静态 AC 地址

- 可选配置。
- AC 的地址可以通过 DHCP 或者 DNS 方式获知，也可以在 AC 上的 AP 配置模式或者 AP 上配置静态 AC 地址。
- 当采用静态方式获取 AC 地址时，通过命令 **acip ipv4** 配置静态 AC 地址。

【命令格式】 **acip ipv4** *ip-address* [*ip-address*…]
【参数说明】 *ip-address*：静态 IP 地址，最多可以配置 6 个静态地址。
【缺省配置】 没有静态配置 AC IP
【命令模式】 AP 全局配置模式或 AC 的 AP 配置模式。
【使用指导】 -

↘ 配置 AP 发现 AC 的域名

- 可选配置，通过命令 **ac-domain-name** 在 AC 上配置 DNS 域名，AP 可以通过 DNS 域名来发现 AC。
- 当采用动态方式获取 AC 地址时，可以在 AC 上配置 DNS 域名来发现 AC 的地址。
- 一般情况下，只要不配置 DNS 域名，AP 就无法通过 DNS 获取 AC IP 地址。

【命令格式】 **ac-domain-name** *ac-domain-name*
【参数说明】 *ac-domain-name*：AC 域名
【缺省配置】 ac.ruijie.com.cn
【命令模式】 AC 的 AP 配置模式或 AP 组配置模式。
【使用指导】 -

↘ 配置 AP 的静态 IP 地址

- 可选配置。
- 可以在 AP 上配置 AP 的 IPv4 静态地址使 AP 用固定的 IPv4 地址接入 AC。

【命令格式】 **ip address** *ip-address network-mask gateway*

【参数说明】 *ip-address*：AP 的接口地址

network-mask：AP 地址掩码

gateway：AP 的网关

【缺省配置】 -

【命令模式】 AP 配置模式。

【使用指导】 AP 可以通过静态配置和 DHCP 两种方式获取自身的 IP 地址。若 AP 未配置过静态 IP 地址，则以 DHCP 的方式动态获取地址并加入 AC，这时可以通过该命令配置 AP 的静态地址，使得 AP 重启之后的地址保存不变。

检验方法

- 通过 **show ap-config running** 查看配置是否成功。

配置举例

配置 AP 通过静态 IPv4 获取 ACIP 地址接入 AC

【配置方法】
- 进入 AC 的 AP 配置模式。
- 配置 AP 加入 AC 的静态地址列表为 192.168.1.1。
- 配置 AP 的静态地址为 1.1.1.1，24 位掩码，网关为 1.1.1.2

AC

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# acip ipv4 192.168.1.1
Ruijie(config-ap)# ip address 1.1.1.1 255.255.255.0 1.1.1.2
```

【检验方法】
- 查看 AP 的配置情况。

AC

```
Ruijie#show ap-config running
!
ap-config AP0001
acip ipv4 192.168.1.1
ip address 1.1.1.1 255.255.255.0 1.1.1.2
!
```

配置 AP 通过 DNS 方式获取 ACIP 地址接入 AC

【配置方法】
- 进入 AC 的 AP 配置模式。
- 配置 AP 发现 AC 的域名为 ruijie-ac。

AC

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# ac-domain-name ruijie-ac
```

【检验方法】
- 查看 AP 的配置情况。

【配置方法】
- 进入 AC 的 AP 配置模式。
- 配置 AP 发现 AC 的域名为 ruijie-ac。

AC

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# ac-domain-name ruijie-ac
```

【检验方法】
- 查看 AP 的配置情况。

AC

```
Ruijie#show ap-config running
!
ap-config AP0001
 ac-domain-name ruijie.ac
!
```

常见错误

- 无。

3.5.10 配置AP上执行命令

配置效果

- 可选配置，通过 AC 配置 AP 上执行某条命令。
- 可选配置，对 AC 上 AP 组内所有 AP 执行某条配置命令

注意事项

无。

配置方法

↘ 配置 AP 执行某条命令

- 可选配置，进入 AP 配置模式。
- 可以通过 AC 配置在 AP 上执行某条命令。

【命令格式】 **exec-cmd mode** *exec-mode* **cmd** *exec-cmd* **once**

【参数说明】 *exec-mode*：命令在 AP 上执行所在的模式。

exec-cmd:：在 AP 上执行的命令

once: 该命令只执行一次，不进行保存

【缺省配置】 无

【命令模式】 AP 配置模式/所有 AP 配置模式

【使用指导】 某些配置命令目前只有 AP 上支持，AC 上没有对应的配置命令，如果想在 AC 上对 AP 进行这类配置，可以通过 exec-cmd 命令来实现。需要注意的是，如果需要取消或者更改 exec-cmd 中的配置，需要先使用 no exec-cmd 命令删除对应的配置，然后再使用 exec-cmd 命令进行反向或者需要更改的配置。

如果同时对 ap-config all 和单独 ap-config 进行配置，对于在线 AP，后配置的会生效，对于离线配置，AP 上线，则按照优先级 ap-config > ap-config all 的方式生效；

检验方法

- 登陆到 ap 上看配置命令是否生效，ac 上 show run 或者 show ap-config run 查看配置是否生效

配置 AP 组内 AP 执行某条命令

- 可选配置，进入 AP 组配置模式。
- 对 AP 组内的所有 AP 执行某条命令。

【命令格式】 **exec-cmd** *exec-cmd*

【参数说明】 *exec-cmd*:：对 AP 组内所有 AP 上执行的命令

【缺省配置】 无

【命令模式】 AP 组配置模式。

【使用指导】 某些配置命令只有 ap-config 模式下支持，而 ap-group 下没有对应的配置命令，如果需要对某个 AP 组内所有 AP 进行该类命令的配置，可以在该 AP 组下执行 exec-cmd 命令来实现；需要注意的是，该配置在 ap-group 模式下并不保存，只是相当于在当前 AP 组下所有 AP 执行该命令一次。如果原先 ap-config 下有该配置，ap-group 下执行命令将会对原配置进行覆盖；

检验方法

- show ap-config run 查看组内的 ap 配置是否生效

配置举例

配置 AC 上关闭 AP 的 EWEB 功能，配置 AP 组内所有 AP 蓝牙 ibeacon 配置

【配置方法】
- 配置 AC 上关闭 AP 的 EWEB 功能
- 配置 AC 上重新开启 AP 的 EWEB 功能
- 配置 AP 组内所有 AP 蓝牙 ibeacon 配置
- 配置 AP 组内所有 AP 关闭 EWEB 功能

AC

```
Ruijie(config)#ap-config AP1
Ruijie(config-ap)# exec-cmd mode configure cmd "no enable service web-server all"
Ruijie(config-ap)# no exec-cmd mode configure cmd "no enable service web-server all"
Ruijie(config-ap)# exec-cmd mode configure cmd "enable service web-server all"
Ruijie(config)#ap-group default
Ruijie(config-group)#exec-cmd ibeacon uuid ffffffffffffffffffffffffffffffff major ffff minor ffff
Ruijie(config-group)#exec-cmd exec-cmd mode configure cmd "no enable service web-server all"
```

【检验方法】

- 在 AC 上查看配置是否生效。

AC

```
Ruijie#show ap-config running
 ap-config AP1
  exec-cmd mode configure cmd "no enable service web-server all"
  ibeacon uuid ffffffffffffffffffffffffffffffff major ffff minor ffff
```

常见错误

- 更改 exec-cmd 的配置，没有配置 no exec-cmd 删除原来的配置，或者没有重新通过 exec-cmd 进行反向的配置。

3.5.11 配置瘦AP

配置效果

- 在瘦 AP 上配置静态 IP 地址、掩码、下一跳以及 AC 的地址，使得 AP 能够使用静态地址和 AC 进行通讯。

注意事项

- 设置 AP 的地址为静态地址将关闭 DHCP 功能，这时将无法通过 DHCP 的 OPTION 选项获取 AC 的地址，这时需要在瘦 AP 上配置接入 AC 的地址，以便 AP 和 AC 不在同一个子网时能发现并加入 AC。
- 瘦 AP 的配置命令和 AC 上配置 AP 的部分命令等价，当两者配置冲突时，可能会导致 AP 重新接入 AC 并以 AC 的配置为准。
- 瘦 AP 配置的命令将自动保存配置。

配置方法

↘ 配置 AP 的静态 IP 地址。

- 可选配置。
- 当需要在部署前期静态规划 AP 的 IP 地址时，可以在 AP 上进行地址相关配置。
- 可以配置 AP 的 IPv4 静态地址使 AP 用 IPv4 地址接入 AC。

- 通过命令 **apip ipv4** 配置 AP 的静态 IPv4 地址.

【命令格式】 **apip ipv4** *ip-addressnetwork-mask gateway*
【参数说明】 *ip-address*：静态 IP 地址。
network-mask：子网掩码。
gateway：网关地址。
【缺省配置】 -
【命令模式】 AP 的全局配置模式。
【使用指导】 -

配置 AP 接入 AC 的静态地址

- 可选配置。
- 当配置 AP 采用静态的 IP 地址时，需要同时在 AP 上指定接入 AC 的 IP 地址。
- AP 接入 AC 的静态地址类型要和 AP 的静态地址类型一致，保证都使用 IPv4。
- 通过命令 **acip ipv4** 配置 AP 加入指定 IPv4 AC。

【命令格式】 **acip ipv4** *ip-address* [*ip-address*…]
【参数说明】 *ip-address*：静态 IP 地址，最多可以配置 6 个静态地址。
【缺省配置】 -
【命令模式】 AP 全局配置模式或 AC 的 AP 配置模式。
【使用指导】 -

配置 APAP 使用 PPPoE 拨号方式获取地址

- 可选配置。
- 当 AP 需要通过 ADSL 线路，连接到远端 ISP 并获得上网的能力时，可以配置 CAPWAP 使用 PPPoE 方式获取地址。

【命令格式】 **apip pppoe**
【参数说明】 -
【缺省配置】 默认未指定 PPPoE 方式，AP 通过 DHCP 获取地址
【命令模式】 AP 的全局配置模式。
【使用指导】 配置了 AP 使用 PPPoE 拨号方式获取地址仅仅设置了 CAPWAP 选择获取地址的方式。配置了该命令之后还需要进行 PPPoE 配置，同时配置默认路由指向拨号口，这样 AP 才能与 AC 进行通讯。
CAPWAP 只能选择 dialer 1 作为源接口，因此配置 PPPoE 拨号的时候需要使用 dialer 1。

检验方法

- 检查瘦 AP 的配置命令是否存在。
- 检查 AP 是否能与 AC 通讯。

配置举例

配置静态 AP 接入 AC 的静态地址

【配置方法】
- 配置 AP 的静态 IPv4 地址
- 配置 AP 连接 AC 的静态 IPv4 地址

AP

```
Ruijie(config)# apip 192.168.1.2 255.255.255.0 192.168.1.1
Ruijie(config)# acip ipv4 1.1.1.1
```

【检验方法】
- 通过 show running-config 查看配置。

AP

```
!
apip 192.168.1.2 255.255.255.0 192.168.1.1
acip ipv4 1.1.1.1
!
```

配置 AP 使用 PPPoE 拨号的方式获取地址

【配置方法】
- 配置 AP 的选择 PPPoE 的方式获取地址
- 配置 PPPoE
- 配置默认路由
- 配置 AP 连接 AC 的静态 IPv4 地址

AP

```
Ruijie(config)# apip pppoe
Ruijie(config)# interface FastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# pppoe enable
Ruijie(config-if-FastEthernet 0/1)# pppoe-client dial-pool-number 1 no-ddr
Ruijie(config-if-FastEthernet 0/1)# exit
Ruijie(config)# interface dialer 1
Ruijie(config-if-Dialer 1)# ip address negotiate
Ruijie(config-if-Dialer 1)# ppp chap hostname ruijie
Ruijie(config-if-Dialer 1)# ppp chap password ruijie
Ruijie(config-if-Dialer 1)# ppp pap sent-username ruijie password ruijie
Ruijie(config-if-Dialer 1)# dialer pool 1
Ruijie(config-if-Dialer 1)# exit
Ruijie(config)# ip route 0.0.0.0 0.0.0.0 dialer 1
Ruijie(config)# acip ipv4 1.1.1.1
```

【检验方法】
- 通过 show running-config 查看配置。

AP

```
!
apip 192.168.1.2 255.255.255.0 192.168.1.1
acip ipv4 1.1.1.1
!
```

常见错误

- 无。

3.5.12 配置升级AP

配置效果

- AC 实现升级 AP 的软件版本。

注意事项

- 配置激活 AP 软件版本文件，该命令只有在 AP 需要升级的时候，才会加载 bin 到内存中。当没有 AP 需要升级的时候，这部分内容会自动从内存中卸载掉。
- 自适应升级无法使用 rgos10 到 rgos11 的过渡版本对 rgos10 系统的 AP 进行升级。
- 在有带宽限制的场景，使用带宽控制进行升级。

配置方法

↘ 创建 AP 产品系列

- 可选配置，通过 **ap-serial** 命令来实现在 AC 上配置一个 AP 系列。
- 通过 AC 升级 AP 软件版本必须要在 AC 上配置先把 AP 硬件版本、产品型号配置到某个系列中。
- 一个 AP 的软件版本可以适用于一系列的 AP，可以把 AP 硬件版本、产品型号配置到某个系列中，让该软件版本为特定型号的 AP 进行升级。

【命令格式】 **ap-serial** *serial-name ap-pid1 ap-pid2 ... ap-pidn* [**hw-ver** *hardware-version*]

【参数说明】 *serial-name*：要创建的 AP 系列名称。

ap-pid1 ap-pid2 ... ap-pidn：要加入该 AP 系列的产品型号列表。

hardware-version：指定 AP 的硬件版本。

【缺省配置】 没有配置 AP 系列

【命令模式】 AC 配置模式。

【使用指导】 -

↘ 激活 AP 软件版本文件。

- 可选配置，通过 **active-bin-file** 命令在 AC 上激活一个 AP 软件版本。
- 通过 AC 升级 AP 软件版本必须要在 AC 上配置激活 AP 软件版本。
- 只有被激活的 AP 软件版本可以用于升级。

【命令格式】 **active-bin-file** *filename* [**rgos10**]

【参数说明】 *filename*：指定的软件版本名称，可以包含路径前缀，路径前缀包括 **flash:**， **tmp:**， **usb0:**，路径前缀后面为紧跟着真正的文件名，文件名长度最大 64 字节。

rgos10：激活 10.X 到 11.X 系统的中间版本，只适用于 AP 的软件版本

【缺省配置】 未激活版本

【命令模式】 AC 配置模式。

【使用指导】 1.AC 给 AP 下载版本进行升级时需要先激活版本文件。由于 rgos10 系统到 rgos11 系统差异较大，利用发布 rgos10 到 rgos11 的过渡版本进行系统升级时需要增加 rgos10 关键字。

2.只有在 AP 需要升级的时候，才会加载 bin 到内存中。当没有 AP 需要升级的时候，这部分内容会自动从内存中卸载掉。

3. 配置该命令前需要确保 AC 系统文件中已存有该软件版本。

配置为指定 AP 升级版本

- 可选配置，通过 **ap-image** 命令配置 AC 升级使用指定的文件升级指定系列的 AP，该命令会对连接到本 AC 的所有 AP 起作用。
- 通过 AC 升级 AP 软件版本必须要先指定 AP 使用的升级文件。
- 要升级特定产品的 AP，需要激活软件版本，指定 AP 的系列和配置指定的文件升级指定系列的 AP 三个步骤。

【命令格式】 **ap-image** *filename*

【参数说明】 *filename*：指定的软件版本名称。

【缺省配置】 -

【命令模式】 AP 配置模式。

【使用指导】 -

配置自适应升级

- 可选配置，通过 **ap-image auto-upgrade** 命令配置 AC 自动根据 AP 的升级文件识别适用的 AP 产品并对所有适用的 AP 进行升级。
- 自动匹配软件版本适用的 AP 型号并对 AP 进行自适应升级。

【命令格式】 **ap-image** { **auto-upgrade** | *filename serial-name* }

【参数说明】 **auto-upgrade：**自动匹配序列号进行升级

filename：指定的软件版本名称。该文件名与 active-bin-file 命令指定的文件名一致。

serial-name：将要升级的 AP 型号系列。

【缺省配置】 -

【命令模式】 AC 配置模式。

【使用指导】 AP 版本升级可以使用自适应升级选项进行版本自动匹配并升级 AP ,而无需配置 AP 的产品型号和软件版本的对应关系 ,也可以使用指定的文件升级指定系列的 AP。当自动升级和指定系列升级两种升级方式同时存在时，将优选指定系列的配置方式进行升级。配置 AC 为指定的 AP 产品系列升级版本时，创建 AP 产品系列，配置指定的 AP 对应的软件版本和激活软件版本这三个步骤缺一不可。

配置 AC 升级 AP 的最大并发数

- 可选配置。

- 限制同时通过 AC 进行升级的最大 AP 数。

【命令格式】 **capwap upgrade max-concurrent num**
【参数说明】 num：AP 并发升级的最大个数，默认值 15，范围为 1~200
【缺省配置】 AP 并发上线的最大个数默认值为 15
【命令模式】 AC 配置模式。
【使用指导】 -

配置升级组

- 可选配置。
- 创建升级组，AC 通过均衡调度，平均分配集中升级名额到升级组中，达到带宽限制和避免带宽浪费。

【命令格式】 **capwap upgrade group** *group-name* [**max-concurrent** *num*]
【参数说明】 *group-name*：升级组名字，不能配置 default 为升级组名字
num：该组中并发集中升级的最大个数，默认为 5，范围 1~200
【缺省配置】 无升级组，AP 升级不受带宽限制。配置升级组，并发集中升级的最大个数默认值为 5
【命令模式】 AC 配置模式。
【使用指导】 -

配置把 AP 加入到升级组中

- 可选配置。
- 把 AP 加到升级中，通过调度和配置，限制该组中集中升级的 AP 数，以达到以升级组为单位的带宽控制目的。

【命令格式】 **ap-upgrade group** *group-name*
【参数说明】 *group-name*：升级组名字，配置之前需要通过 capwap upgrade group 命令创建组
【缺省配置】 AP 不加入升级组
【命令模式】 AP 配置模式。
【使用指导】 -

配置 AP 升级的带宽

- 可选配置
- 配置 AP 升级的带宽。

【命令格式】 **ap-upgrade band-width** *num*
【参数说明】 *num*：AP 升级的带宽，以 1KB 为单位，配置范围 8~1024，默认无带宽限制
【缺省配置】 无带宽限制
【命令模式】 AP 配置模式。
【使用指导】 配置 AP 升级带宽、配置升级组以及把 AP 加入到升级组三条命令组成带宽控制 AP 升级配置命令

检验方法

- 查看 AP 的版本是否成功升级。
- 查看带宽控制升级组和组内 AP 升级状态。

配置举例

配置升级 AP

【配置方法】
- 在 AC 上进入 AC 配置模式
- 在 AC 上创建 AP 产品系列。
- 在 AC 上配置指定 AP 的升级版本。
- 在 AC 上配置 AP 升级版本。

AC

```
Ruijie(config-ac)# ap-serial serial1 AP220-E AP220-SE AP620-H hw-ver 1.0
Ruijie(config-ac)# active-bin-file ap.bin
Ruijie(config-ac)# ap-image ap.bin serial1
Ruijie(config-ac)# exit
```

【检验方法】
- 在 AC 上显示本 AC 已经激活的文件列表。

AC

```
Ruijie#show ac-config active-file
Cnt    File Name    Version                                Used Cnt   Ready
------ ------------ ---------------------------------- ---------- --------
1      ap.bin        RGOS 10.4(1t7)(1T7), Release(88888)   1       1
```

配置带宽控制的 AP 升级

【配置方法】
- 在 AC 上进入 AC 配置模式
- 在 AC 上创建 AP 升级组。
- 退出 AC 配置模式
- 进入 AP 配置模式
- 在 AC 上配置指定 AP 的升级组。
- 在 AC 上配置 AP 升级带宽。

AC
- Ruijie(config-ac)# capwap upgrade group UPGRADE-GROUP1 max-concurrent 10
- Ruijie(config-ac)# exit
- Ruijie(config)#ap-config 8832.0000.1111
- Ruijie(config-ap)# ap-upgrade group UPGRADE-GROUP1
- Ruijie(config-ap)# ap-upgrade band-width 128
- Ruijie(config-ap)# exit

【检验方法】
- 在 AC 上显示升级组和组内 AP
- 在 AC 上显示 AP 所处的升级组和其带宽

AC

```
Ruijie#show ac-config upgrade-group
Cnt     Group-Name                  Max-Concurrent     Token cnt     Upgrading cnt
------ ---------------------------------- ------------ ----------- ------------
1       UPGRADE-GROUP1                 10                2           1
    Ruijie#show ac-config upgrade-group UPGRADE-GROUP1
    Group have 2 ap , online 1 offline 1
    Cnt      Ap-Name                     Ap-Mac              Online     Upgrade       Band-width
    ------- ------------------------ -------------------- -------- ------------  ---------
    1       ap220e                     8832.0000.1111       true        true          128
    2       ap330                            -              false       false         128
    Ruijie#show ap-config wtp-info 8832.0000.1111
    Ruijie#show ap-config wtp-info ap220e
    Upgrade-banfwidth    : 128
    Upgrade group        : UPGRADE-GROUP1
```

常见错误

- 配置升级 AP 但是 AC 系统文件中没有要升级的软件版本。

3.5.13 配置CAPWAP的控制地址

配置效果

- 配置 AC 用于建立 CAPWAP 隧道的地址。

注意事项

- 修改 AC 的 CAPWAP 隧道 IP 地址，有可能使已经在线的 AP 断开。
- 配置一个在 AC 上不存在的地址，会使得 CAPWAP 隧道无法建立。
- AP 的网关不在 AC 时(即 AC 和 AP 是三层拓扑)，此时 AP 的地址池的 option 选项，应当配置为 **capwap ctrl-ip** 配置的地址(如果有配置)。
- 在 AC 热备环境中，若通过该命令来配置 CAPWAP 隧道的控制地址，则需要对等备份 AC 在热备配置模式下配置该控制地址为对等控制 IP，命令为 **peer-ip** *A.B.C.D*。

配置方法

- 可选配置，当需要使用非 loopback 口地址作为 CAPWAP 的控制地址时配置。
- 配置 AC 与 AP 建立 CAPWAP 隧道的控制 IPv4 地址，可以指定 AC 希望使用 IP 地址与 AP 建立 CAPWAP 隧道。

- 通过 **capwap ctrl-ip** *ip-address* 指定与 AP 建立隧道的 CAPWAP 隧道控制 IP 地址，*ip-address* 需要为 AC 设备的某个接口的 IP 地址。

【命令格式】 **capwap ctrl-ip** *ip-address*

【参数说明】 *ip-address*：配置 AC 用于建立 CAPWAP 隧道的地址，缺省使用 loopback0 的地址。

【缺省配置】 默认情况下 AC 与 AP 建立 CAPWAP 隧道的地址为 AC 设备的第一个 Loopback IPv4 地址

【命令模式】 AC 配置模式。

【使用指导】 AC 默认是通过第一个 Loopback 接口的 IP 地址来建立 CAPWAP 隧道，该命令允许用户手动指定 AC 与 AP 建立 CAPWAP 隧道的 IP 地址。

检验方法

- 通过 **show running-config** 命令确认是否配置成功。

配置举例

↘ 配置 AC 的控制 IP 为 10.0.0.1

【配置方法】
- 进入 AC 配置模式
- 配置 AC 的位置信息

AC

```
Ruijie(config)#ac-controller
Ruijie(config-ac)#capwap ctrl-ip 10.0.0.1
```

【检验方法】 通过 **show running-config** 命令可以查看配置情况。

AC

```
!
ac-controller
capwap ctrl-ip 10.0.0.1
!
```

常见错误

- 无

3.5.14 配置CAPWAP分片

配置效果

- 当数据报文经过 CAPWAP 隧道封装之后，报文长度可能超过 IP MTU，报文会经过 IP 进行 IP 分片。当链路中存在多个节点的 IP MTU 不一致时，报文可能需要进行多次分片和重组，降低了报文转发性能。通过启用 CAPWAP 分片功能，报文将在 CAPWAP 封装时进行分片操作，CAPWAP 报文长度将指定为链路中的最小 IP MTU，从而避免 IP 分片。

注意事项

- MTU 配置过小会产生大量分片报文，影响报文转发性能，甚至导致大报文无法传输，因此请合理规划 MTU 大小。
- 配置的 CAPWAP MTU 需要小于等于设备出口的 IP MTU，否则 CAPWAP 分片之后将再次进行 IP 分片。

配置方法

配置 CAPWAP 隧道的路径 MTU

- 可选配置，进入 AP 配置模式或 AP 组配置模式后，通过 **capwap mtu** 命令来配置 CAPWAP 隧道的路径 MTU。
- 当数据报文经过 CAPWAP 隧道封装之后的报文长度超过 CAPWAP 隧道的路径 MTU 时 ,CAPWAP 将对该数据报文进行分片。在 AC 上配置隧道路径 MTU 时请配置为隧道路径上的最小 IP MTU，以免报文转发过程中再进行 IP 分片重组，降低转发性能。

【命令格式】 **capwap mtu** *num*
【参数说明】 *num*：CAPWAP 路径 MTU 大小，参数范围 68~1500，以字节为单位。
【缺省配置】 默认 MTU 大小为 1500 字节
【命令模式】 AP 配置模式或 AP 组配置模式。
【使用指导】 -

开启 CAPWAP 分片功能

- 可选配置。
- 当传输网络中存在多个 IP MTU 节点时，建议在 AC 上开启 CAPWAP 分片功能并设置 CAPWAP MTU 为路径 MTU。
- 当数据报文经过 CAPWAP 隧道封装之后，报文长度可能超过 IP MTU，报文会经过 IP 进行 IP 分片。当链路中存在多个节点的 IP MTU 不一致时，报文可能需要进行多次分片和重组，降低了报文转发性能。可以通过该命令开启 CAPWAP 分片功能，报文将在 CAPWAP 封装时进行分片操作，CAPWAP 分片的报文长度可以由 **capwap mtu** 命令指定为链路中的最小 MTU，从而避免 IP 分片。

【命令格式】 **capwap fragment enable**
【参数说明】 -
【缺省配置】 默认不开启 CAPWAP 分片功能
【命令模式】 AP 配置模式或 AP 组配置模式。
【使用指导】 -

检验方法

- 通过查看 CAPWAP 隧道的详细信息，获知 CAPWAP 隧道的 MTU 和是否分片使能。
- 或者通过 **show ap-config running** 可以查看是否配置。

配置举例

↘ 配置 AP1 的 MTU 和分片使能

【配置方法】
- 在 AC 上配置 AP1 的路径 MTU 为 1200 字节。
- 在 AC 上配置开启 AP1 的 CAPWAP 分片功能。

AC

```
Ruijie(config)# ap-config AP1
Ruijie(config-ap)# capwap mtu 1200
Ruijie(config-ap)# capwap fragment enable
```

【检验方法】 通过 **show ap-config running** 命令可以查看配置情况。

AC

```
!
capwap fragment enable
capwap mtu 1200
!
```

常见错误

- 无。

3.5.15 配置CAPWAP加密

配置效果

- 配置控制通道不加密，用于网络故障时进行报文分析。

注意事项

- 当改变数据隧道的加密方式时，将触发 CAPWAP 隧道重新建立。

配置方法

↘ 配置 CAPWAP 控制通道加密

- 可选配置。
- 在 AC 上配置控制通道不加密，用于网络故障时进行报文分析，以便网络工程师通过报文分析进行故障定位。

【命令格式】 **capwap dtls enable**
【参数说明】 -
【缺省配置】 默认开启 CAPWAP 控制通道 DTLS 加密功能
【命令模式】 AC 配置模式
【使用指导】 默认情况下，CAPWAP 的控制通道 DTLS 加密功能是开启的，可以保证 AC 跟 AP 之间控制交互的安全。特殊情况下，为了测试的方便，用户可以配置控制通道不加密。

检验方法

- 通过查看 CAPWAP 隧道的详细信息，判断控制通道和数据通道的加密策略。
- 通过 **show running-config** 命令可以查看控制通道是否未加密。

3.5.16 配置CAPWAP接入控制

配置效果

- 配置 AP 并发接入的最大个数。

注意事项

- 当配置的值较小时，会使该 AC 下所有 AP 上线的总时间偏长。

配置方法

↘ 配置 CAPWAP 最大并发个数

- 可选配置。
- 在 AC 上通过该配置规划最大并发 AP 数，避免大量 CAPWAP 控制报文导致 CPU 飙高。

【命令格式】 **capwap max-concurrent** *num*

【参数说明】 *num*：AP 并发上线的最大个数，范围为 1~200

【缺省配置】 AP 并发上线的最大个数默认值为 50

【命令模式】 AC 配置模式

【使用指导】 大量 AP 并发上线时，可能导致 AC 的 CPU 增高，甚至达到 100%，从而导致已经上线的 AP 由于保活失败而隧道断开。使用该命令可以限制 AP 并发上线的最大个数。

检验方法

- 通过 **show running-config** 查看配置。

配置举例

↘ 配置 CAPWAP 最大并发个数

【配置方法】
- 在 AC 上配置允许的最大 AP 并发上线数。

AC

```
Ruijie(config-ac)#capwap max-concurrent 100
```

【检验方法】 ● 在 AC 上通过 show running-config 查看。

AC

```
!
ac-controller
capwap max-concurrent 100
!
```

常见错误

- 无。

3.5.17 配置CAPWAP的心跳保活间隔

配置效果

- 可选配置，配置保活报文发送的时间间隔，即多长时间发送一次。

注意事项

- 无线网络部署时可以根据网络规模调整 CAPWAP 心跳保活间隔以规划网络收敛性能，调整时需确保对网络规模有足够了解并确实需要该收敛性，避免在大规模 AP 部署的无线网络中设置过低的值对网络环境造成冲击。

配置方法

- 可选配置，进入 AP 配置模式或 AP 组配置模式配置。
- 可以通过在 AC 上配置 CAPWAP 的心跳保活间隔来控制 CAPWAP 隧道的存活周期。

【命令格式】 **echo-interval** *seconds*

【参数说明】 *seconds*：CAPWAP 心跳保活间隔，配置范围为 5~255。

【缺省配置】 保活间隔缺省值为 30s

【命令模式】 AP 配置模式或 AP 组配置模式。

【使用指导】 瘦 AP 网络架构中 ,AC 和 AP 通过 CAPWAP 隧道互联。AP 和 AC 之间使用 Echo Request 和 Echo Response 来维护链路的有效性。AP 在没有其他请求报文的情况下，每隔 echo-interval 发送 Echo Request 报文进行保活。若 AP 发送没有收到应答报文，报文将进行重传，重传以初始重传间隔（3 秒与 echo-interval 的一半两者的最小值）开始倍增，且最大重传间隔不能超过 echo-interval 的一半与 60 秒的最小值。当最大最大重传次数仍然没有收到应答报文，则认为隧道断开。即隧道的保活失效时间为保活时间加上重传间隔。该命令仅在隧道 Run 状态下生效。默认 echo-interval 是 30s，默认的最大重传次数是 5，请求报文在第 0s 发送之后，如果未收到应答，重传报文分别在间隔 3s、6s、12s，15s、15s 被重传。配置 echo-interval 和 max-retransmit 为其它值仍按此规则计算报文超时时间。。

检验方法

- 查看 CAPWAP 隧道的详细信息，能看到修改的保活报文发送的时间间隔。

配置举例

配置 CAPWAP 的心跳保活间隔

【配置方法】
- 在 AC 上配置保活报文发送时间间隔 50。

AC
```
Ruijie(config)#ap-config AP0001
Ruijie(config-ap)# echo-interval 50
```

【检验方法】
- 在 AC 上查看 CAPWAP 隧道的详细信息。

AC
```
Ruijie#show capwap 1.1.1.1 detail
Echo interval is 50 secs, Dead interval is 119 secs
```

常见错误

- 无。

3.5.18 配置CAPWAP的报文重传次数

配置效果

- 可选配置，配置重传的最大次数调整隧道的存活时间。

注意事项

无。

配置方法

- 可选配置，进入 AP 配置模式或 AP 组配置模式配置。
- 可以通过配置重传的最大次数调整隧道的存活时间。

【命令格式】 **capwap max-retransmit** *num*

【参数说明】 *num*：CAPWAP 报文的最大重传次数。

【缺省配置】 默认重传次数 5 次

【命令模式】 AP 配置模式或 AP 组配置模式。

【使用指导】 CAPWAP 发送的请求报文若没有收到应答报文，报文将进行重传，重传以初始重传间隔（3 秒与 echo-interval 的一半两者的最小值）开始倍增，且最大重传间隔不能超过 echo-interval 的一半与 60 秒的最小值。当最大最大重传次数仍然没有收到应答报文，则认为隧道断开。可以通过配置重传的最大次数调整隧道的存活时间。该命令仅在隧道 Run 状态下生效。

检验方法

- 查看 CAPWAP 隧道的详细信息，能看到修改的保活报文发送的时间间隔。

配置举例

配置 CAPWAP 的报文最大重传次数

【配置方法】 ● 配置 AP1 的最大重传次数为 20。

AC

```
Ruijie(config)#ap-config AP1
Ruijie(config-ap)# capwap max-retransmit 20
```

【检验方法】 ● 在 AC 上查看 CAPWAP 隧道的详细信息。

AC

```
Ruijie#show capwap 1.1.1.1 detail
 Config maxretransmit 20
```

常见错误

- 无。

3.6 监视与维护

清除各类信息

无。

查看运行情况

作用	命令
显示本 AC 已经激活的文件列表。	**show ac-config active-file**
显示本 AC 配置的 AP 产品系列和产品型号对应关系 ,以及对应的产品系列要使用怎样的文件进行升级。	**show ac-config serial-product**
显示 AC 配置的升级组信息	show ac-config upgrade-group [*group-name*]
显示 AP 的主板数据信息。	**show ap-config board-data** *ap-name*
显示 AC 与 AP 之间的链路状态。	**show ap-config link-latency** { **all** | **single** *ap-name* }
显示 AP 的厂商信息。	**show ap-config inventory** *ap-name*
显示 AP 的重启数据统计。	**show ap-config reboot** *ap-name*
显示 AP 的静态 IP 地址	**show ap-config static-ip** { **all** | **single** *ap-name* }
显示 AP 的位置信息	**show ap-config summary location**

显示 AP 升级状态信息	**show ap-config updating-list**
显示 AP 的状态描述信息。	**show ap-config wtp-descriptor** *ap-name*
显示 AP 的状态信息	**show ap-config wtp-info** *ap-name*
显示 CAPWAP 隧道的详细信息	**show capwap** [index | [ip-address [port]]] **detail**
显示 CAPWAP 隧道的状态信息	**show capwap state**
显示 CAPWAP 隧道的统计信息	**show capwap** [index | [ip-address [port]]] **statistics**
显示 AP 的版本信息	**show version** { **all** | *ap-name* }
收集和显示 AP 上的各种日志信息	**tran-data-start** *ap-name* { **exception** | **memory | tech-support** | **tech-package** } **tran-data-show** *ap-name* { **exception** | **cpuinfo** | **memory** | **syslog** | **tech-support** }

查看调试信息

无。

4 WBS

4.1 概述

WBS 是无线基础服务。在瘦 AP 场景下，用于在 AC 上配置无线相关参数设置。

链路完整性检测功能是 WBS 的一项基础服务，就是在 AP 上检测 AP 的上链有线链路，在链路断开时，暂停 AP 的接入服务，相当于间接强制用户下线；在链路恢复正常后，AP 再继续提供无线接入服务。在瘦 AP 架构，密集部署 AP 时，打开链路完整性检查，有助于减少用户的断网的时间，提升用户的使用体验。

下文仅介绍 WBS 的相关内容。

协议规范

- 802.11n：Enhancements for Higher Throughput

4.2 典型应用

典型应用	场景描述
配置瘦 AP	在 AC 设备上配置命令，指定各瘦 AP 的参数配置。
链路完整性检测	瘦 AP 架构，开启链路完整性检测功能，提高无线接入服务质量。

4.2.1 配置瘦AP

应用场景

配置瘦 AP，方便管理员在 AC 上集中管理瘦 AP 配置。假设网络中存在如下部署要求：

1、 允许在 AC 上监控各智分 AP 的馈线链路状态。

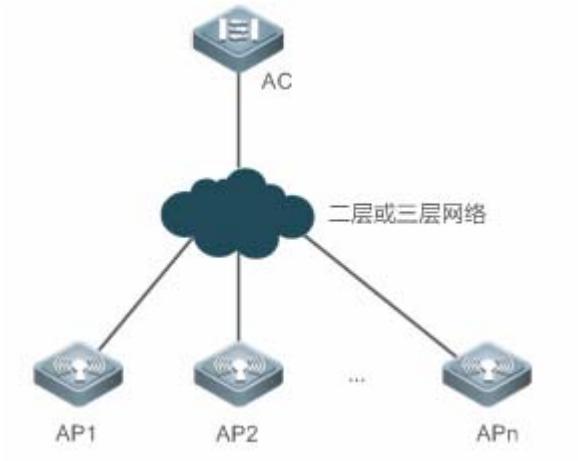
2、 禁止 RSSI 低于 20 的用户接入网络。

3、 开启 20M 带宽下短防护间隔机制。

4、 禁止 1Mbps、2Mbps、5.5Mbps 等低速率使用。

组网环境如下所示：

图 4-1 瘦 AP 场景组网图



功能部属

AC 的配置要点如下：

1、 对所有 AP 配置开启智分天线馈线链路检测功能，设置检测周期为期望值。

2、 对所有 AP 的各 Radio 配置 response-rssi 命令，指定门限为 20db。

3、 对所有 AP 的各 Radio 配置 short-gi enable 命令，指定带宽为 20M。

4、 对 802.11b/g 网络用户，配置禁用 1Mbps、2Mbps、5.5Mbps。

4.2.2 链路完整性检测

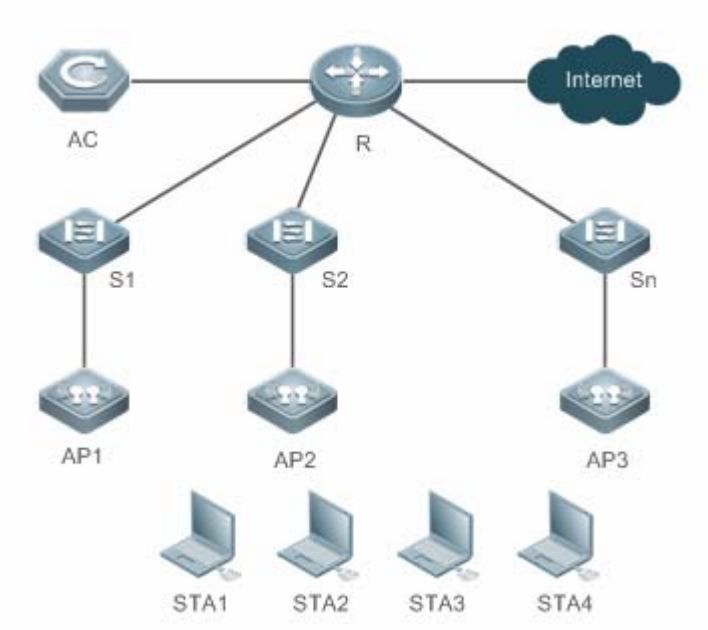
应用场景

瘦 AP 架构无线网络，开启链路完整性检测功能。

以下图为例：

- AC 通过路由器连接 Internet；三个 AP：AP1、AP2 和 AP3，分别通过交换机连接路由器并关联到 AC。
- STA1 关联在 AP1 上；STA2、STA3 关联在 AP2 上；STA4 关联在 AP3 上；它们通过 AC 访问 Internet。

图 4-2



【注释】 R 为网络出口路由器。
S1、S2、S3 为二层交换机，作为 AP 的接入设备。
AP1、AP2、AP3 直接连接到 S1、S2、S3 上。

功能部属

- 二层交换机提供 AP 设备的接入功能。
- 路由器 R 连接 AC 设备和 AP 设备网络；连接 STA 和 Internet。

4.3 功能详解

基本概念

AMPDU

802.11n 标准中采用 A-MPDU 聚合帧格式，即将多个 MPDU 聚合为一个 A-MPDU，只保留一个 PHY 头，删除其余 MPDU 的 PHY 头，减少了传输每个 MPDU 的 PHY 头的附加信息，同时也减少了 ACK 帧的数目，从而降低了协议的负荷，有效的提高网络吞吐量。

MCS

802.11N 物理层支持更快的数据传输速率，同时兼容支持传统的 802.11a/b/g 速率。802.11N 的物理层支持非常广泛的不同的速度，称为调制编码方案（MCS）率。

Beacon

在 WLAN 网络中，AP 会定期向外发送 Beacon（即信标帧），Beacon 包含了该 AP 的相关信息，无线用户通过接收 Beacon 来发现 WLAN 网络。

RSSI

Received Signal Strength Indication 接收信号的强度指示，可以用来表示无线链接质量。

国家码

国家代码是用来识别使用射频所在的国家，不同的国家代码规定的射频频段、信道、功率将有所不同。在配置 AP 前，需要先明确该 AP 所支持的国家代码，如果配置的国家代码发生变化，对应的射频频段、信道、功率值也会有所变化。

频段

支持 2.4GHZ 和 5GHZ 两个频段的射频传输。

信道

无线信道（Channel）是 AP 与无线用户之间传输射频介质的通道。不同的国家以及不同的频段支持的信道也不同。在中国，2.4GHZ 的频段可以配置的信道有 13 个（channel 1、2、3...13），5GHZ 的频段可以配置的信道有 24 个（Channel 36、40、44、48、52、56、60、64、100、104、108、112、116、120、124、128、132、136、140、 149、153、157、161、165）。在 2.4GHZ 的频段中，互相重叠的信道会产生干扰，为避免无线信号冲突，建议将其配置为不重叠的信道（例如 Channel 1、6、11）；而 5GHZ 的频段，这 24 个信道不会互相重叠，也不会产生干扰。

发射功率

发射功率表示 AP 发射射频信号的强弱，如果发射功率大，则 AP 覆盖的无线信号区域更大，反之更小。

时隙类型

在 WLAN 网络中，为避免多个工作站发送数据引起信道竞争，工作站在发送数据之前需要检测信道是否空闲。如果检测到信道处于空闲状态，工作站并不立即发送数据，而是等待一个退避时间（Backoff Time）。退避时间是时隙时间（Slot Time，MAC 协议中的一个操作时间单元）的随机整数倍，则每经过一个时隙时间，系统自动将数值减 1，待数值减为零时，工作站开始发送数据。WLAN 时隙类型分为 20us 和 9us 两种，其中 9us 又称为短时隙。

天线收发类型

天线收发是用于配置射频卡的收发类型，用于选择射频卡上的哪几根天线发送和接收。

短防护间隔

802.11n 提供了缩短防护时间的机制，使能短防护间隔机制，防护时间由 0.8us 降低为 0.4us。

分片阈值

为了提高传输成功率，IEEE 802.11 MAC 协议允许将报文分成若干小片段进行传输。根据分片阈值，对报文进行分片，可降低受干扰机率，且即使重传也可减少所重传浪费的带宽。

RTS

为了避免信道冲突，而导致数据传输失败，IEEE 802.11 MAC 协议提供了一个 RTS/CTS(Request To Send/Clear To Send)握手协议，即请求发送/允许发送协议。假设工作站 A 需要向工作站 B 发送数据，首先会发送一个 RTS 请求帧，如果工作站 B 允许工作站 A 发送 ,就会回复一个 CTS 允许帧 ,工作站 A 收到后便开始发送数据。如果存在多个工作站向同一个工作站发送 RTS 以示请求发送数据，则只有收到 CTS 的工作站可以发送数据，没有收到 CTS 的工作站默认信道冲突，则等待一定时间后再发送 RTS 请求。

↘ PHY 保护模式类型

帧可以用于 greenfield 模式或混合模式，混合模式用于兼容其他 phy 层，gf 模式用于速度较快的物理层标头。应用 HT 混合模式的装置能够应用原来的 802.11a/b/g 模式和新的 802.11n 模式进行传输。具体来说 ,HT 混合模式装置传输一个传统的格式序言，紧跟着一个 HT 格式序言。HT 混合模式装置也必须在传输前发送传统的格式 CTS-to-Self 或 RTS/CTS (Request to Send/Clear to Send)。当通道繁忙时，这些“保护机制”会让 802.11a/b/g 装置，包括哪些没有连接到 HT 混合 AP 的装置感知到繁忙的状态。

↘ 前导码类型

前导码（Preamble）是数据报文头部的一组 Bit 位，用于同步发送端与接收端的传输信号，用户可以配置指定 AP 支持的前导码类型（long 或 short），长前导码的数据帧传输时间长，短前导码的数据帧传输时间短。

↘ U-APSD

U-APSD（Unscheduled Auto Power Save Delivery），非排程自动功率节省发送。为了减小实时性要求高的业务在电源管理过程中的延迟，在 802.11e 中引入 WMM-PS。同时，WMM-PS 使用了 APSD 的技术，通过关闭大多时候的无线信号的发射，延长了电池的使用时间，这是对现在的 802.11 功率节省机制的加强。

功能特性

功能特性	作用
智分天线馈线链路检测	用于检测智分 AP 的馈线链路状态是否正常工作
用户接入控制	实现对某一类无线用户进行接入控制
AP 射频参数设置	实现对 AP 或 Radio 相关射频参数设置
速率控制参数设置	实现对速率控制相关射频参数设置
节电处理参数设置	实现对节电处理相关参数设置
链路完整性检测	实现链路完整性检测功能，提高无线服务质量
电子书包参数设置	在电子书包场景中，经常需要配置一些命令，来达到更好的体验效果。一键配置电子书包网优命令可以用于快速配置。
一键 WLAN 配置	在空配置的设备上，为了实现快速配置，提供一键配置 WLAN 的功能。

4.3.1 智分天线馈线链路检测

工作原理

在整网中可能存在大量智分 AP，而每台 AP 下又有多根馈线。为了方便用户管理，锐捷产品提供了馈线链路检测功能，可以自动检测每台智分 AP 上的每一根馈线是否工作正常。这样任何一台智分 AP 上的任何一根馈线由于接触不良或者人为损坏导致工作不正常的时候，用户都可以检测到，并能及时排除故障。

4.3.2 用户接入控制

工作原理

为了方便对 STA 进行接入管理，锐捷产品提供了对某一类无线用户进行接入控制。

无线用户搜索 AP 的方式主要通过主动扫描或被动扫描。

- 主动扫描：即无线用户发送 Probe Request 帧请求接入 AP，AP 确认后发送 Probe Response 帧响应；
- 被动扫描：即 AP 定期向外广播 Beacon 帧，无线用户侦听到 Beacon 帧试图连接。

为控制 AP 的网络覆盖范围，提高无线信号传输质量，可以通过限制接入的无线用户。首先，可以通过控制 AP 广播 Beacon 帧的范围，减少远距离的无线用户接入；其次，可以通过限制无线用户接入时的 RSSI（接收信号强度指示）的最小值，当接收到无线用户的请求帧的 RSSI 小于这个值，则不允许该无线用户接入；再次，可以通过限制无线用户数据传输时的 RSSI 的最小值，当接收到无线用户的数据帧的 RSSI 小于这个值，则踢掉该无线用户，帮助其漫游到无线信号更好的 AP 上。

4.3.3 AP射频参数设置

实现对 AP 及其 Radio 相关射频参数设置。

工作原理

↘ A-MPDU 聚合

802.11n 标准中采用 A-MPDU 聚合帧格式，即将多个 MPDU 聚合为一个 A-MPDU，只保留一个 PHY 头，删除其余 MPDU 的 PHY 头，减少了传输每个 MPDU 的 PHY 头的附加信息，同时也减少了 ACK 帧的数目，从而降低了协议的负荷，有效的提高网络吞吐量。

↘ MCS

802.11n 射频速率的配置通过 MCS（Modulation and Coding Scheme，调制与编码策略）索引值实现。MCS 调制编码表是 802.11n 为表征 WLAN 的通讯速率而提出的一种表示形式。MCS 将所关注的影响通讯速率的因素作为表的列，将 MCS 索引作为行，形成一张速率表。所以，每一个 MCS 索引其实对应了一组参数下的物理传输速率，全部 MCS 速率表的描述可参见“IEEE P802.11n D2.00”。

↘ 无线信道

无线信道（Channel）是 AP 与无线用户之间传输射频介质的通道。不同的国家以及不同的频段支持的信道也不同。在中国，2.4GHZ 的频段可以配置的信道有 13 个（channel 1、2、3...13），5GHZ 的频段可以配置的信道有 24 个（Channel 36、40、44、48、52、56、60、64、100、104、108、112、116、120、124、128、132、136、140、 149、153、157、161、165）。

在 2.4GHZ 的频段中，互相重叠的信道会产生干扰，为避免无线信号冲突，建议将其配置为不重叠的信道（例如 Channel 1、6、11）；而 5GHZ 的频段，这 24 个信道不会互相重叠，也不会产生干扰。

报文分片

为了提高传输成功率，IEEE 802.11 MAC 协议允许将报文分成若干小片段进行传输。根据分片阈值，对报文进行分片，可降低受干扰机率，且即使重传也可减少所重传浪费的带宽。

RTS/CTS

为了避免信道冲突，而导致数据传输失败，IEEE 802.11 MAC 协议提供了一个 RTS/CTS(Request To Send/Clear To Send)握手协议，即请求发送/允许发送协议。假设工作站 A 需要向工作站 B 发送数据，首先会发送一个 RTS 请求帧，如果工作站 B 允许工作站 A 发送 ,就会回复一个 CTS 允许帧 ,工作站 A 收到后便开始发送数据。如果存在多个工作站向同一个工作站发送 RTS 以示请求发送数据，则只有收到 CTS 的工作站可以发送数据，没有收到 CTS 的工作站默认信道冲突，则等待一定时间后再发送 RTS 请求。

如果每个工作站每次发送数据前都要执行 RTS/CTS 握手，将导致过多的 RTS 帧占用信道带宽，用户可以设置 RTS Threshold 来指定发送数据的帧长度，如果工作站发送数据的帧长度小于 RTS Threshold 设置的门限，将不执行 RST/CTS 握手。。

Beacon

在 WLAN 网络中，AP 会定期向外发送 Beacon（即信标帧），Beacon 包含了该 AP 的相关信息，无线用户通过接收 Beacon 来发现 WLAN 网络。

前导码类型

前导码（Preamble）是数据报文头部的一组 Bit 位，用于同步发送端与接收端的传输信号，用户可以配置指定 AP 支持的前导码类型（long 或 short），长前导码的数据帧传输时间长，短前导码的数据帧传输时间短。

时隙类型

在 WLAN 网络中，为避免多个工作站发送数据引起信道竞争，工作站在发送数据之前需要检测信道是否空闲。如果检测到信道处于空闲状态，工作站并不立即发送数据，而是等待一个退避时间（Backoff Time）。退避时间是时隙时间（Slot Time，MAC 协议中的一个操作时间单元）的随机整数倍，假设随机值为 3，则每经过一个时隙时间，系统自动将数值减 1，待数值减为零时，工作站开始发送数据。因此，降低时隙时间可以减少总体退避时间，从而增加网络的吞吐量。

信道带宽

802.11n 通过将两个 20MHz 的带宽绑定在一起组成一个 40MHz 通讯带宽，在实际工作时可以作为两个 20MHz 的带宽使用（一个为主带宽， 一个为次带宽， 收发数据时既可以以 40MHz 的带宽工作，也可以以单个 20MHz 带宽工作），这样可将速率提高一倍，提高无线网络的吞吐量。

防护间隔

802.11n 提供了缩短防护时间的机制，使能短防护间隔机制，防护时间由 0.8us 降低为 0.4us。

国家代码

国家代码是用来识别使用射频所在的国家，不同的国家代码规定的射频频段、信道、功率将有所不同。在配置 AP 前，需要先明确该 AP 所支持的国家代码，如果配置的国家代码发生变化，对应的射频频段、信道、功率值也会有所变化。

↘ 天线收发类型

AP 发射与接受使用不同数量的天线，可以使得 AP 在 802.11n 模式下采用双空间流模式或者三空间流模式来发射信号，提升 AP 数据传输的性能。

↘ 内置天线与外置天线

内置天线是集成到 AP 设备壳体内的天线。外置天线是可以通过 AP 设备预留的硬件接口进行外接的天线。相同传输功率下，外置天线比内置天线的传输距离更远。

↘ AP 的 radio 与无线传输对端之间允许的最远距离

无线信号以光速在空间传播。AP 的 radio 与无线传输对端之间的距离越远，无线报文在空间传输所需的时间越长；相应地，AP 等待接收 ACK 帧、CTS 帧所需的超时时间就越长。因此，有必要根据 AP 的 radio 与无线传输对端之间的距离长短适当地调整超时时间；否则将无法进行无线数据传输。但是，超时时间也不能过度地加长；否则当 AP 没有接收到 ACK 帧、CTS 帧时，过度的超时时间会造成空口资源浪费。

4.3.4 速率控制参数设置

实现对速率控制相关射频参数设置。

工作原理

802.11 是 IEEE 为无线局域网定义的一个无线网络通信的工业标准，此后这一标准又不断得到补充和完善，形成 802.11X 的标准系列。其中，主要的传输标准为 802.11b\a\g\n，具体说明如下：

1、802.11b

其工作频段为 2.4GHZ，最大数据传输速率可达到 11Mb/s，根据实际需要，传输速率可降低为 5.5、2 或 1Mb/s。

2、802.11a

其工作频段为 5GHZ，最大数据传输速率可达到 54Mb/s，根据实际需要，传输速率可降低为 48，36，24，18，12，9 或 6Mb/s。

3、802.11g

其工作频段为 2.4GHZ，最大数据传输速率可达到 54Mb/s，根据实际需要，传输速率可降低为 48，36，24，18，12，9 或 6Mb/s，支持 802.11g 的设备可向后兼容 802.11b。

4.3.5 节电处理参数设置

工作原理

↘ DTIM 周期

DTIM（Delivery Traffic indication Map，延迟传输指示讯息）是 Beacon 帧内的一个标志位，用来定时 AP 发送广播帧或多播帧的时间间隔。当无线终端处于休眠状态时，AP 会自动为其暂存 DTIM 时间间隔内需要接收的数据。待 DTIM 超时，AP 将这些缓存数据发送给无线终端。

DTIM 是以发送的 Beacon 数为周期，假设设置的 DTIM 周期时间为 3，即每发送 3 个 Beacon 帧后，AP 才会发送广播帧或多播帧。

↘ U-APSD 节电模式

U-APSD 是对原有节电模式的改进。客户端在关联时可以指定某些 AC 具有触发属性，某些 AC 具有发送属性，以及触发后最多允许发送的数据报文数量。触发和发送属性还可以在通过连接准入控制创建流的时候进行更改。客户端休眠后，发往客户端的属于具有发送属性 AC 的数据报文将被缓存在发送缓存队列中，客户端需要发送属于具有触发属性 AC 的报文以获取发送缓存队列中的报文。AP 收到触发报文后，按照接入时确定的发送报文数量，发送属于发送队列的报文。没有发送属性的 AC 仍然使用 802.11 定义的传统方式存储和传送。

4.3.6 链路完整性检测

AP 设备作为无线接入设备，本身的作用相当于物理层和 MAC 的一部分，一般不具备交换功能。从硬件结构看，不管是胖 AP 或者瘦 AP，一般只有单条上链有线链路，这条链路是所有接入用户的数据通道。如果这条上链有线链路由于故障断开，那么所有接入这台 AP 的无线用户都无法连接到外部网络。

问题在于，一旦出现上述问题，无线用户无法立刻感知而采取相应的对策，导致无线用户的网络长时间无法恢复正常连接。

链路完整性检测旨在解决这个问题。

工作原理

链路完整性检测功能，在 AP 上持续检测 AP 上链有线链路；在链路断开时，立刻关闭该 AP 上的射频口，暂停 AP 的接入服务，强制关联此 AP 的无线用户下线，迫使无线用户选择周围其他正常工作的 AP 重新接入网络。

在 AP 上链有线链路恢复正常后，链路完整性检测功能再重新打开 AP 的射频口，恢复 AP 的无线接入服务。

链路完整性检测的必要性在于，当 AP 的唯一上行链路断开后，AP 无法再给无线用户提供接入功能，与其让无线用户继续关联，不如关闭 AP 的射频口，强制无线用户下线，让无线用户选择其他的 AP 重新接入。

4.3.7 电子书包参数设置

实现对 AP 及其 Radio 相关的电子书包参数设置。

工作原理

在电子书包场景中，经常需要配置一些命令，来达到更好的体验效果。一键配置电子书包网优命令可以用于快速配置。

↘ AMPDU

即 A-MPDU 聚合。

LDPC

LDPC 码是一种易实现和系统复杂度低的优秀的线性纠错码。它是一种前向错误修正(Forward Error Correction, FEC)编码技术，可提高编码的可靠性与编码增益。此技术于 1960 年初期开始发展，可在具有大量背景或内容损坏的噪杂频率中传送讯息。在受到严重噪杂干扰的频率中使用此技术，可大幅降低资料遗失的风险，但是存在极少量终端在兼容 LDPC 上具备一定问题，表现为丢包。

STBC

无线通信技术中一种在不同时刻、不同天线上发射数据的多个副本，从而利用时间和空间分集以提高数据传输可靠性的编码，这种 STBC 编码的最大优势在于，采用简单的最大似然译码准则，可以获得完全的天线增益。但是可能存在部分终端无法有效兼容该编码方式。

AMPDU 软件重传次数

配置 AMPDU 软件重传次数作用在于在无线中可能存在子帧丢失情况，因此可以通过软件重传来避免子帧丢失，重传的次数越大，子帧丢失的可能性越低，但是重传次数过多可能造成空口负担增大，造成空气中其他报文的实时性下降，如果需要在子帧丢失概率较大的干扰下确保报文尽可能避免丢失，可以将数值调大。

AMPDU-RTS

AMPDU 的 RTS 保护能够避免因为隐藏节点问题导致 AMPDU 报文在空口碰撞，造成空口资源浪费，但是同时由于 RTS 交互会造成一定的空口消耗，在大多数应用场景中，会对空口造成一定副作用，因此默认情况下处于关闭状态。只有隐藏节点问题造成的空口资源浪费大于 RTS 交互造成的空口资源浪费时，才开启 AMPDU 的 RTS 保护。

以太网单次收包数

配置以太网单次收包数命令，以太网收包数调高能够确保整网性能提升，但是有可能会降低 AP 对关键报文处理的实时性，例如在电子书包等对性能要求不高同时要求多用户并发且对报文实时性要求高的场景下，可以将以太网单次收包数下降，此时的建议值为 25。

4.3.8 一键WLAN配置

在空配置的设备上，为了实现快速配置，提供一键配置 WLAN 的功能。

工作原理

autowifi

在 AC 上配置：

（1）vlan 划分：AC 上使用 vlan 1 作为 AP 的 vlan，vlan 2 作为 STA 的 vlan。

（2）地址池：AC 上使用 192.168.1.0 网段作为 AP 地址池，使用 192.168.2.0 作为 STA 网段；默认 vlan 1、vlan 2 的 IP 分别为 192.168.1.1，192.168.2.1；默认管理 IP 为 88.88.88.88。

（3）wlan 配置：使用 autowifi_XXXX，后面 4 个字符为设备 MAC 的后 4 位；使用 wlan-id 1。

（4）安全：默认使用 WPA2 加密，密码为 autowifi。

（5）wlan-vlan 映射：AC 上在 ap-group default 组里，映射 wlan-id 1 vlan 2。

（6）服务：开启 DHCP 服务。

4.4 产品说明

NBR800G、NBR950G、NBR1500G、NBR2000G 不支持无线集成 AC 功能，NBR108G-P、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持无线集成 AC 功能。

4.5 配置详解

配置项	配置建议&相关命令	
配置智分天线馈线链路检测功能	可选配置，用于设置 AP 开启馈线链路状态检测功能	
	antdetect enable	开启馈线链路状态检测功能
	antdetect interval	配置馈线状态检测时间间隔，单位是分钟。
配置用户接入控制	可选配置，用于设置用户接入控制	
	{802.11a | 802.11b} network {enable | disable}	配置 2.4GHZ 或 5GHZ 网络的开关情况
	11asupport enable	配置指定 AP 指定 radio 在 5G 下支持 11A
	11bsupport enable	配置指定 AP 指定 radio 在 2.4G 下支持 11 B
	11gsupport enable	配置指定 AP 指定 radio 在 2.4G 下支持 11G
	11nasupport enable	配置指定 AP 指定 radio 在 5G 下支持 11N
	11ngsupport enable	配置指定 AP 指定 radio 在 2.4G 下支持 11N
	11acsupport enable	配置指定 AP 指定 radio 支持 11AC
	coverage-area-control	配置 AP 管理帧功率选择
	response-rssi	配置指定 AP 指定 radio 允许接入无线用户的最小信号强度
	assoc-rssi	配置指定 AP 指定 radio 的无线用户保持接入的最小信号强度
配置 AP 射频参数	可选配置，用于设置 AP 射频参数	
	802.11n a-mpdu enable	配置指定 AP 指定 radio 支持 AMPDU
	802.11n mcs support	配置指定 AP 指定 radio 11N 最大支持的 MCS
	802.11ac mcs support	配置指定 AP 指定 radio 11AC 最大支持的 MCS
	antenna	配置指定 AP 指定 radio 的天线收发类型

	external-antenna enable	配置指定 AP 指定 radio 启用外置天线，并禁用内置天线
	beacon dtim-period	配置指定 AP 指定 radio 的 DTIM 周期
	beacon period	配置指定 AP 指定 radio 的 beacon 帧发送周期
	chan-with	配置指定 AP 指定 radio 的带宽
	channel	配置指定 AP 指定 radio 的信道
	country	指定 AC 支持的国家代码集合或 AP Radio 使用的国家码
	enable-radio	设置指定 AP 的 radio 或全部 radio 的使能状态为开启
	fragment-threshold	配置指定 AP 指定 radio 的分片阈值
	green-field enable	配置指定 AP 指定 radio 的保护模式
	power local	配置指定 AP 指定 radio 发射功率
	radio-type	配置指定 AP 指定 radio 的工作频段
	rts-threshold	配置指定 AP 指定 radio 的 RTS 阈值
	short-gi	配置指定 AP 指定 radio 支持 short-gi
	update-key-tsc enable	配置 AP 在进行 1X 重认证的时候更新加密 TSC
	peer-distance	配置 AP 与无线传输对端之间允许的最远距离
	mu-mimo enable	配置 Radio 的多用户多入多出功能
配置速率控制参数	可选配置，用于设置速率控制参数	
	802.11a network rate	配置 802.11a 用户支持的速率集
	802.11b network rate	配置 802.11b 用户支持的速率集
	802.11g network rate	配置 802.11g 用户支持的速率集
	mcast-rate	配置 WLAN 的组播速率
	beacon rate	配置 beacon 帧发送速率
配置节电处理参数	可选配置，用于节电处理参数	
	beacon dtim-period	配置 DTIM 周期
	apsd	配置启用/禁用 U-APSD 节电模式
配置链路完整性检测功能	必须配置。用于开启链路完整性检测功能。	
	link-check enable	打开链路完整性检测功能
配置电子书包参数	可选配置，用于设置电子书包参数	
	ampdu-retries	配置 AMPDU 软件重传次数
	ampdu-rts	配置是否开启 AMPDU 聚合报文的 RTS 保护机制
	eth-schd	配置 AP 以太网单次收包数
	ldpc	配置是否支持低密度奇偶校验编码

	stbc	配置是否使能接收发送空时分组码
	ebag	一键配置电子书包网优
一键 WLAN 配置	⚠ 可选配置，用于一键配置 WLAN	
	autowifi	一键配置 WLAN

4.5.1 配置智分天线馈线链路检测功能

配置效果

- 可以开启智分天线馈线链路检测功能，使得智分 AP 周期检测天线馈线链路状态。当天线馈线链路出现异常时，智分 AP 能将异常天线信息上传到 AC 上，以便网管人员能检测到馈线链路问题，并及时排除故障。

注意事项

- 此功能仅在 AP220-E(M) v3.0 上支持。

配置方法

↘ 开启馈线链路检测功能

- 可选配置。
- 在 AC 设备上面对需要开启馈线链路检测功能的 AP 进行配置。
- 打开该功能后 ,AC 将下发该配置给对应的 AP ,告知 AP 开启智分天线馈线链路检测功能。当 AP 检测到馈线链路异常时，上传链路异常状态给 AC，以便用户查询 AP 馈线链路状态。

【命令格式】 **antdetect enable**
【参数说明】 -
【缺省配置】 馈线链路检测功能是关闭的
【命令模式】 AP 配置模式
【使用指导】 默认情况下，关闭馈线链路状态检测功能。

↘ 配置馈线链路检测时间间隔

- 可选配置。
- 在 AC 设备上面对需要开启馈线链路检测功能的 AP 进行配置，需要开启馈线链路检测功能才能生效。
- 配置该参数后，AC 将下发该参数配置给对应的 AP，告知 AP 馈线链路检测时间间隔，使其以指定的周期进行检测馈线链路状态。

【命令格式】 **antdetect interval** *interval*
【参数说明】 *Interval*：检测时间间隔(单位分钟，范围 1-10000)。
【缺省配置】 1 分钟，表示 1 分钟检测一次

【命令模式】 AP 配置模式

【使用指导】 默认情况下，馈线链路检测时间间隔为 1min。

检验方法

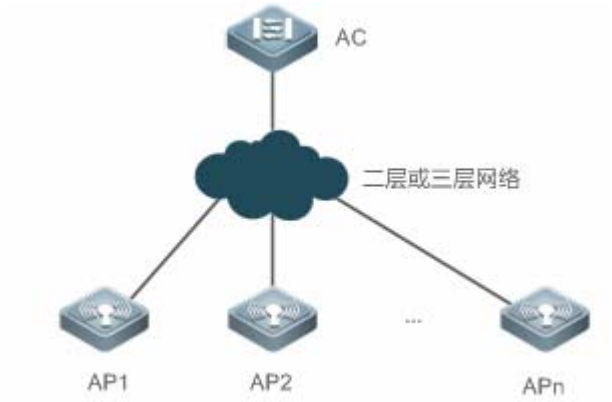
- 通过 **show antenna all** 命令可以查看所有 AP 的天线馈线链路状态。

配置举例

配置馈线链路检测功能

【网络环境】

图 4-3



假设瘦 AP 环境中，如上图所示，在 AC 设备上有以下配置智分天线馈线链路检测功能要求：

1、打开所有 AP 的馈线链路检测功能；

2、设置馈线链路检测周期为 30min 检测一次；

【配置方法】

- 在 AC 设备上面配置智分天线馈线链路检测功能

```
Ruijie# configure terminal
Ruijie(config)# ap-config all
Ruijie(config-ap)# antdetect enable
Ruijie(config-ap)# antdetect interval 30
```

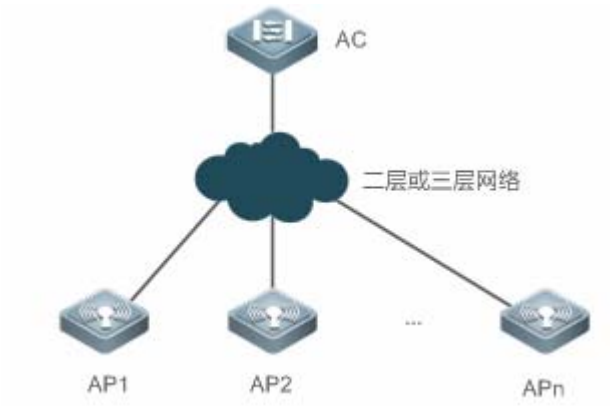
【检验方法】

- 通过 show antenna all 命令可以查看所有 AP 的天线馈线链路状态。

```
Ruijie# show antenna all
ap's antenna state                                                R1        R2        R3
R4        R5        R6
                            ap                                    0 1 2 3   0 1 2 3   0 1 2 3   0
1 2 3   0 1 2 3   0 1 2 3
_______________________________________________________________   _______   _______   _______
_______   _______   _______
```

【网络环境】

图 4-3



假设瘦 AP 环境中，如上图所示，在 AC 设备上有以下配置智分天线馈线链路检测功能要求：

1、打开所有 AP 的馈线链路检测功能；

2、设置馈线链路检测周期为 30min 检测一次；

【配置方法】

- 在 AC 设备上面配置智分天线馈线链路检测功能

```
Ruijie# configure terminal
Ruijie(config)# ap-config all
Ruijie(config-ap)# antdetect enable
Ruijie(config-ap)# antdetect interval 30
```

【检验方法】

- 通过 show antenna all 命令可以查看所有 AP 的天线馈线链路状态。

```
APD-M4                                                    -NN-   -NY-   -NN-   -
NN-   -----   -----
```

常见错误

- 无。

4.5.2 配置用户接入控制

配置效果

- 可以实现对某一类无线用户进行接入控制，方便网管人员进行无线网络用户管理。

注意事项

- 无。

配置方法

配置 2.4GHZ 或 5GHZ 网络的开关情况

- 可选配置。
- 在 AC 设备上面进行配置。
- 配置后，AC 将下发该配置给所有 AP，告知 AP 开启或关闭 2.4GHZ 或 5GHZ 网络。

【命令格式】 { **802.11a** | **802.11b**} **network** { **enable** | **disable** }
【参数说明】 -
【缺省配置】 缺省情况下 2.4GHZ 和 5GHZ 网络都是开启的
【命令模式】 AC 配置模式
【使用指导】 -

配置支持 11A

- 可选配置。
- 该配置仅在 AP 的 Radio 工作于 5G 下生效。
- 在 AC 设备上面对需要是否支持 11A 用户的 AP 进行配置。
- 打开该功能后，AC 将下发该配置给对应的 AP，告知 AP 在 5G 下支持 11A 用户接入。

【命令格式】 **11asupport enable radio** *radio-id*
【参数说明】 *radio-id*：要配置的 radio 的 id，范围为 1-48
【缺省配置】 在 5G 下支持 11A 用户接入
【命令模式】 AP 配置模式
【使用指导】 配置仅在 AP 的 Radio 工作在 5G 下生效。
不支持对所有 AP 进行配置。

配置支持 11B

- 可选配置。
- 该配置仅在 AP 的 Radio 工作于 2.4G 下生效。
- 在 AC 设备上面对需要是否支持 11B 用户的 AP 进行配置。
- 打开该功能后，AC 将下发该配置给对应的 AP，告知 AP 在 2.4G 下支持 11B 用户接入。

【命令格式】 **11bsupport enable radio** *radio-id*
【参数说明】 *radio-id*：要配置的 radio 的 id，范围为 1-48
【缺省配置】 2.4G 下支持 11B 用户接入
【命令模式】 AP 配置模式
【使用指导】 配置仅在 AP 的 Radio 工作在 2.4G 下生效。
不支持对所有 AP 进行配置。

配置支持 11G

- 可选配置。
- 该配置仅在 AP 的 Radio 工作于 2.4G 下生效。

- 在 AC 设备上面对需要是否支持 11G 用户的 AP 进行配置。
- 打开该功能后，AC 将下发该配置给对应的 AP，告知 AP 在 2.4G 下支持 11G 用户接入。

【命令格式】 **11gsupport enable radio** *radio-id*
【参数说明】 *radio-id*：要配置的 radio 的 id，范围为 1-48
【缺省配置】 在 2.4G 下支持 11G 用户接入
【命令模式】 AP 配置模式
【使用指导】 配置仅在 AP 的 Radio 工作在 2.4G 下生效。
不支持对所有 AP 进行配置。

配置支持 11NA

- 可选配置。
- 该配置仅在 AP 的 Radio 工作于 5G 下生效。
- 在 AC 设备上面对需要是否支持 11NA 用户的 AP 进行配置。
- 打开该功能后，AC 将下发该配置给对应的 AP，告知 AP 在 5G 下支持 11N 用户接入。

【命令格式】 **11nasupport enable radio** *radio-id*
【参数说明】 *radio-id*：要配置的 radio 的 id，范围为 1-48
【缺省配置】 在 5G 下支持 11N 用户接入
【命令模式】 AP 配置模式
【使用指导】 配置仅在 AP 的 Radio 工作在 5G 下生效。
不支持对所有 AP 进行配置。

配置支持 11NG

- 可选配置入。
- 该配置仅在 AP 的 Radio 工作于 2.4G 下生效。
- 在 AC 设备上面对需要是否支持 11NG 用户的 AP 进行配置。
- 打开该功能后，AC 将下发该配置给对应的 AP，告知 AP 在 2.4G 下支持 11N 用户接入。

【命令格式】 **11ngsupport enable radio** *radio-id*
【参数说明】 *radio-id*：要配置的 radio 的 id，范围为 1-48
【缺省配置】 在 2.4G 下支持 11N 用户接入
【命令模式】 AP 配置模式
【使用指导】 配置仅在 AP 的 Radio 工作在 2.4G 下生效。
不支持对所有 AP 进行配置。

配置支持 11AC

- 可选配置。
- 在 AC 设备上面对需要是否支持 11AC 用户的 AP 进行配置。
- 打开该功能后，AC 将下发该配置给对应的 AP，告知 AP 支持 11AC 用户接入。

【命令格式】 **11acsupport enable radio** *radio-id*
【参数说明】 *radio-id*：要配置的 radio 的 id，范围为 1-48
【缺省配置】 Radio ID 为奇数的 Radio 不支持 11AC 用户接入，Radio ID 为偶数的 Radio 支持 11AC 用户接入
【命令模式】 AP 配置模式
【使用指导】 -

配置管理帧功率选择

- 可选配置。
- 若无特殊要求，在需要配置 AP 管理帧功率的设备上面配置。
- 在 AC 设备上面对需要配置管理帧功率功能的 AP 进行配置。
- 配置该参数后，AC 将下发该参数配置给对应的 AP，告知 AP 使用指定值作为管理帧发射功率，以控制 AP 的信号覆盖范围以达到限制无线用户接入的目的。

【命令格式】 **coverage-area-control** *power*
【参数说明】 *power*：管理帧功率，单位：dbm，范围 0~32
【缺省配置】 AP 管理帧功率为 0dbm
【命令模式】 AP 配置模式或 AP 组配置模式
【使用指导】 -

配置允许接入无线用户的最小信号强度

- 可选配置。
- 在 AC 设备上面对需要配置允许接入无线用户最小信号强度功能的 AP 进行配置。
- 配置该参数后，AC 将下发该参数配置给对应的 AP，告知 AP 使用指定值作为无线用户接入的信号强度门限。

【命令格式】 **response-rssi** *rssi* **radio** {*radio-id* | *[802.11b* | *802.11a*]}
【参数说明】 *rssi*：允许接入无线用户的最小信号强度，单位：db，范围为 0~100
radio-id：要配置的 radio 的 id，范围为 1-48
802.11b：对所有 2.4G 的 radio 进行配置
802.11a：对所有 5.8G 的 radio 进行配置
【缺省配置】 为 0，即所有信号强度的无线用户都允许接入
【命令模式】 AP 配置模式
【使用指导】 指定了 802.11b 参数将对所有 2.4G 的 radio 进行配置，配置在 AP 第一次上线的时候生效且自动转换为基于 radio 的配置；同样指定的 802.11a 参数将对所有 5.8G 的 radio 进行配置，配置在 AP 第一次上线的时候生效且命令自动转换为基于 radio 的配置。

配置无线用户保持接入的最小信号强度

- 可选配置。
- 在 AC 设备上面对需要配置无线用户保持接入的最小信号强度功能的 AP 进行配置。
- 配置该参数后，AC 将下发该参数配置给对应的 AP，告知 AP 使用指定值作为保持无线用户接入的信号强度门限。

【命令格式】 **assoc-rssi** *rssi* **radio** *radio-id*

【参数说明】 *rssi*：无线用户保持接入的最小信号强度，单位：db，范围为 0~100

radio-id：要配置的 radio 的 id，范围为 1-48

【缺省配置】 为 0，即所有信号强度的无线用户都允许接入

【命令模式】 AP 配置模式

【使用指导】 -

检验方法

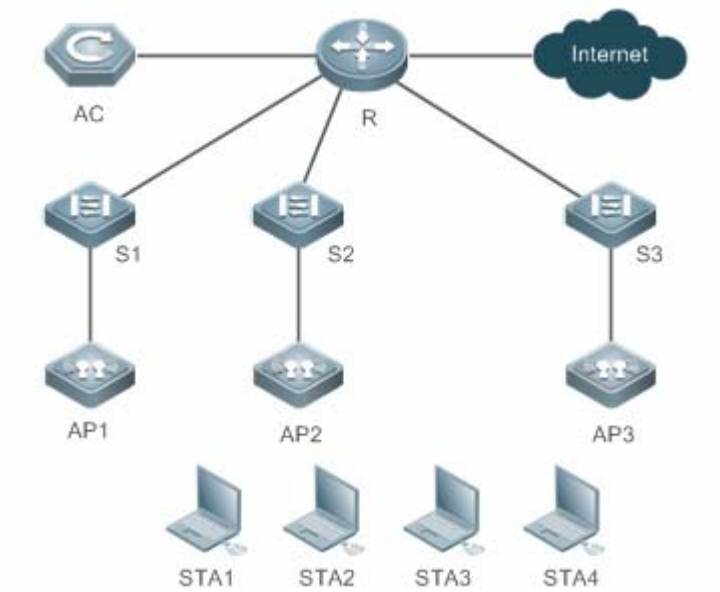
- 通过 **show ap-config running** *ap-name* 命令可以查看设置的用户接入控制参数。

配置举例

配置用户接入控制参数

【网络环境】

图 4-4



假设瘦 AP 环境中，在 AC 设备上对所有 AP 设备有以下用户接入控制参数配置要求：

1、关闭 2.4GHZ 网络；

假设瘦 AP 环境中，在 AC 设备上对 AP1 设备有以下用户接入控制参数配置要求：

1、 5G 下支持 11a、11na 用户接入；

2、 2.4G 下支持 11g、11ng 用户接入，不支持 11b 用户接入；

3、 支持 11ac 用户接入

4、 管理帧功率选择为 20dbm；

5、 允许接入无线用户的最小信号强度为 20db；

6、 无线用户保持接入的最小信号强度为 15db。

【配置方法】

- 在 AC 设备上面配置关闭 2.4GHZ 网络如下

AC

```
Ruijie# configure terminal
Ruijie(config)# ac-controller
Ruijie(config-ac)# 802.11b network disable
```

- 在 AC 设备上面配置 AP1 用户接入控制参数如下

AC

```
Ruijie# configure terminal
Ruijie(config)# ap-config AP1
Ruijie(config-ap)# 11asupport enable radio 2
Ruijie(config-ap)# 11nasupport enable radio 2
Ruijie(config-ap)# 11gsupport enable radio 1
Ruijie(config-ap)# 11ngsupport enable radio 1
Ruijie(config-ap)# 11acsupport enable radio 1
Ruijie(config-ap)# no 11bsupport enable radio 1
Ruijie(config-ap)# coverage-area-control 20
Ruijie(config-ap)# response-rssi 20 radio 1
Ruijie(config-ap)# response-rssi 20 radio 2
Ruijie(config-ap)# assoc-rssi 15 radio 1
Ruijie(config-ap)# assoc-rssi 15 radio 2
```

【检验方法】

- 通过 show running 命令可以查看 2.4GHZ 或 5GHZ 网络的开关情况

AC

```
Ruijie(config)# show running
!
ac-controller
 sta-limit 1024
 no capwap dtls enable
 802.11b network disable
 country CN
 country US
```

- !
- 通过 show ap-config running ap-name 命令可以查看指定 AP 的用户接入控制参数配置。

AC

```
Ruijie(config)# show ap-config running AP1
!
ap-config 220em
  no 11bsupport enable radio 1
  coverage-area-control 20
  response-rssi 20 radio 1
  response-rssi 20 radio 2
  assoc-rssi 15 radio 1
  assoc-rssi 15 radio 2
  radio-type 1 802.11b
  radio-type 2 802.11a
!
```

常见错误

- 无。

4.5.3 配置AP射频参数

配置效果

- 可以实现对各 AP 及其 Radio 相关射频参数设置，方便管理员进行配置管理。

注意事项

- 无。

配置方法

↘ 配置支持 AMPDU

- 可选配置。
- 打开该功能后，AC 将下发该配置给对应的 AP，告知 AP 开启 AMPDU 功能。

【命令格式】 **802.11n a-mpdu enable radio** *radio-id*
【参数说明】 *radio-id*：要配置的 radio 的 id，范围为 1-48
【缺省配置】 支持 AMPDU 功能
【命令模式】 AP 配置模式
【使用指导】 配置仅在 AP 的 Radio 工作在 11N 模式或 11AC 模式下生效。
不支持对所有 AP 进行配置。

↘ 配置 11N 最大支持的 MCS

- 可选配置。
- 配置该功能后，AC 将下发该配置给对应的 AP，告知 AP 11N 最大支持的 MCS。

【命令格式】 **802.11n mcs support** *num* **radio** *radio-id*
【参数说明】 *num*：MCS 序号，范围 0~31
radio-id：要配置的 radio 的 id，范围为 1-48
【缺省配置】 最大支持的 MCS 为 31
【命令模式】 AP 配置模式
【使用指导】 配置仅在 AP 的 Radio 工作在 11N 模式或 11AC 模式下生效。

↘ 配置 11AC 最大支持的 MCS

- 可选配置。
- 配置该功能后，AC 将下发该配置给对应的 AP，告知 AP 11AC 最大支持的 MCS。

【命令格式】 **802.11ac mcs support** *num* **radio** *radio-id*
【参数说明】 *num*：MCS 序号，范围 0~39
radio-id：要配置的 radio 的 id，范围为 1-48
【缺省配置】 最大支持的 MCS 为 39
【命令模式】 AP 配置模式
【使用指导】 配置仅在 AP 的 Radio 工作在 11AC 模式下生效。

配置天线收发类型

- 可选配置。
- 配置该功能后，AC 将下发该配置给对应的 AP，告知 AP 使用指定的天线选择掩码进行收发报文。

【命令格式】 **antenna** { **transmit** | **receive** } *value* **radio** *radio-id*
【参数说明】 **transmit**：配置天线发参数
receive：配置天线收参数
value：天线选择掩码，取值范围为：1~15
radio-id：要配置的 radio 的 id，范围为 1-48
【缺省配置】 AP 配置模式针对不同产品型号、不同天线数目，其缺省天线选择掩码也不同。具体视各产品型号而定
AP 组配置模式缺省无配置
【命令模式】 AP 配置模式或 AP 组配置模式
【使用指导】 配置仅在 AP 的 Radio 工作在 11N 模式或 11AC 模式下生效。

配置 AP 启用外置天线

- 可选配置。
- 配置该功能后，AC 将下发该配置给对应的 AP，告知 AP 启用外置天线，并禁用内置天线。

【命令格式】 **external-antenna enable radio** *radio-id*
【参数说明】 *radio-id*：要配置的 radio 的 id，范围为 1-48
【缺省配置】 缺省情况下启用内置天线，并禁用外置天线
【命令模式】 AP 配置模式
【使用指导】 -

配置 beacon 帧发送周期

- 可选配置。
- 配置该功能后，AC 将下发该配置给对应的 AP，告知 AP 使用指定的值作为 beacon 帧的发送。

【命令格式】 **beacon period** *milliseconds* **radio** *radio-id*
【参数说明】 *milliseconds*：发送 Beacon 帧的周期，单位 ms，范围 20~1000
radio-id：要配置的 radio 的 id，范围为 1-48
【缺省配置】 缺省值为 100ms
【命令模式】 AP 配置模式

【使用指导】 不支持对所有 AP 进行配置。

配置带宽

- 可选配置。
- 配置后，AC 将下发该配置给对应的 AP，告知 AP 使用指定的值作为信道带宽。

【命令格式】 **chan-width** { **20** | **40 | 80|160** } **radio** {*radio-id* | [*802.11b* | *802.11a*]}

【参数说明】 **20**：配置为 20M 带宽

40：配置为 40M 带宽

80：配置为 80M 带宽

160：配置为 160M 带宽

radio-id：要配置的 radio 的 id，范围为 1-48

802.11b：对所有 2.4G 的 radio 进行配置

802.11a：对所有 5.8G 的 radio 进行配置

【缺省配置】 信道带宽为 20M

【命令模式】 AP 配置模式

【使用指导】 指定了 802.11b 参数将对所有 2.4G 的 radio 进行配置，配置在 AP 第一次上线的时候生效且自动转换为基于 radio 的配置；同样指定的 802.11a 参数将对所有 5.8G 的 radio 进行配置，配置在 AP 第一次上线的时候生效且命令自动转换为基于 radio 的配置。带宽配置仅当 AP 工作在 11N 或 11AC 模式下生效。

配置信道

- 可选配置。
- 配置后，AC 将下发该配置给对应的 AP，告知 AP Radio 工作在指定的信道。

【命令格式】 **channel** *channel-id* **radio** *radio-id*

【参数说明】 *channel-id*：AP Radio 的工作信道

radio-id：要配置的 radio 的 id，范围为 1-48

【缺省配置】 由 RRM 自动调整信道，无缺省信道配置

【命令模式】 AP 配置模式

【使用指导】 不支持对所有 AP 进行配置。

配置 AC 支持国家码集合

- 可选配置。
- 只有在 AC 的国家码集合中增加支持指定的国家码后，才能对 AP Radio 配置使用该国家码。

【命令格式】 **country** *country-code*

【参数说明】 *country-code*：国家代码

【缺省配置】 AC 支持国家码集合为{“CN”}

【命令模式】 AP 配置模式

【使用指导】 AC 支持的国家代码“CN”不允许删除。

当前可选支持的国家代码有：

“CN”, “CHINA”,

“US”, “UNITED STATES”,

配置国家码

- 可选配置。
- 该国家码需在 AC 支持的国家码集合当中。配置后，AC 将下发该配置给对应的 AP，告知 AP Radio 工作在指定的国家代码。

【命令格式】 **country** *country-code* **radio** {*radio-id* | [*802.11b* | *802.11a*]}

【参数说明】 *country-code*：国家代码

radio-id：要配置的 radio 的 id，范围为 1-48

802.11b：对所有 2.4G 的 radio 进行配置

802.11a：对所有 5.8G 的 radio 进行配置

【缺省配置】 AP 使用的国家代码为“CN”

【命令模式】 AP 配置模式

【使用指导】

1. AC 支持的国家代码“CN”不允许删除。
2. 不支持对所有 AP 进行配置。
3. 当前支持的国家代码有： “CN”, “CHINA”,“US”, “UNITED STATES”,另外，根据 WLAN 的部署环境，还分为室内（IN）无线和室外（OUT）无线两种。因此，在配置国家代码时可以直接在代码后标记“I”或“O”。例如中国室内使用“CNI”。
4. 在配置 AP 前，需要先 AC 可支持的国家代码集合。如果配置该 AP 所使用的国家代码发生变化，则 AP 对应的射频频段、信道、功率值也会有所变化。
5. 指定了 802.11b 参数将对所有 2.4G 的 radio 进行配置，配置在 AP 第一次上线的时候生效且自动转换为基于 radio 的配置；同样指定的 802.11a 参数将对所有 5.8G 的 radio 进行配置，配置在 AP 第一次上线的时候生效且命令自动转换为基于 radio 的配置。

配置 Radio 使能状态

- 可选配置。
- 配置后，AC 将下发该配置给对应的 AP，告知 AP 开启指定 Radio 的使能状态。

【命令格式】 **enable-radio** { *radio-id* | **all** }

【参数说明】 *radio-id*：要配置的 radio 的 id，范围为 1-48

all：指所有 radio

【缺省配置】 Radio 使能状态是开启的

【命令模式】 AP 配置模式

【使用指导】 该操作会导致连接到指定 radio 上的所有无线用户离线。

不支持对所有 AP 进行配置。

配置分片阈值

- 可选配置。
- 配置后，AC 将下发该配置给对应的 AP，告知 AP Radio 使用指定的分片阈值进行分片逻辑处理。

【命令格式】 **fragment-threshold** *value* **radio** *radio-id*

【参数说明】 *value*：配置的分片阈值，范围为 256~2346 之间的偶数

radio-id：要配置的 radio 的 id，范围为 1-48

【缺省配置】 2346Byte

【命令模式】 AP 配置模式

【使用指导】 不支持对所有 AP 进行配置。

配置保护模式

- 可选配置。
- 配置后，AC 将下发该配置给对应的 AP，告知 AP Radio 开启保护模式。

【命令格式】 **green-field enable radio** *radio-id*

【参数说明】 *radio-id*：要配置的 radio 的 id，范围为 1-48

【缺省配置】 保护模式为 disable

【命令模式】 AP 配置模式

【使用指导】 配置仅在 AP 的 Radio 工作在 2.4G 下生效。

配置发射功率

- 可选配置。
- 配置后，AC 将下发该配置给对应的 AP，告知 AP Radio 使用发射功率。

【命令格式】 **power local** *power***radio** {*radio-id* | [*802.11b* | *802.11a*]}

【参数说明】 *power*：要配置 AP 的发射功率百分比，取值范围为 1~100

radio-id：要配置的 radio 的 id，范围为 1-48

802.11b：对所有 2.4G 的 radio 进行配置

802.11a：对所有 5.8G 的 radio 进行配置

【缺省配置】 由 RRM 自动调整发射功率，无缺省发射功率配置

【命令模式】 AP 配置模式或 AP 组配置模式

【使用指导】 指定了 802.11b 参数将对所有 2.4G 的 radio 进行配置，配置在 AP 第一次上线的时候生效且自动转换为基于 radio 的配置；同样指定的 802.11a 参数将对所有 5.8G 的 radio 进行配置，配置在 AP 第一次上线的时候生效且命令自动转换为基于 radio 的配置。不支持对所有 AP 进行配置。

配置频段

- 可选配置。
- 配置后，该 AP Radio 的工作信道将由 RRM 模块进行全局分析，自动调整，并下发最优信道给对应的 AP，告知 AP Radio 工作在指定的信道。

【命令格式】 **radio-type** *radio-id* { **802.11a** | **802.11b** }

【参数说明】 *radio-id*：要配置的 radio 的 id，范围为 1-48

802.11a：表示 5GHZ 的工作频段

802.11b：表示 2.4GHZ 的工作频段

【缺省配置】 单频 AP（即 Radio 1）支持 2.4GHZ 频段，双频 AP 的 Radio 1 支持 2.4GHZ，Radio 2 支持 5GHZ

【命令模式】 AP 配置模式

【使用指导】 不支持对所有 AP 进行配置。

配置 RTS 阈值

- 可选配置。
- 配置后，AC 将下发该配置给对应的 AP，告知 AP Radio 使用指定配置作为 RTS 阈值。

【命令格式】 **rts-threshold** *value* **radio** *radio-id*

【参数说明】 *value*：RTS 阈值，单位：byte，范围为 257~2347

radio-id：要配置的 radio 的 id，范围为 1-48

【缺省配置】 RTS 阈值为 2347

【命令模式】 AP 配置模式

【使用指导】 -

配置 short-gi

- 可选配置。
- 配置后，AC 将下发该配置给对应的 AP，告知 AP Radio 使用指定的 short-gi 配置。

【命令格式】 **short-gi enable radio** *radio-id* **chan-width** { **20** | **40** | **80** |**160**}

【参数说明】 *radio-id*：要配置的 radio 的 id，范围为 1-48

20：配置为 20M 带宽

40：配置为 40M 带宽

80：配置为 80M 带宽

160：配置为 160M 带宽

【缺省配置】 40M 带宽使能，20M 带宽不使能

【命令模式】 AP 配置模式

【使用指导】 -

配置前导码类型

- 可选配置。
- 配置后，AC 将下发该配置给对应的 AP，告知 AP Radio 工作在指定的前导码类型。

【命令格式】 **preamble** { **long** | **short** } **radio** *radio-id*

【参数说明】 **long**：指定 AP 只传输长前导码的帧

short：指定 AP 可传输短或长前导码的帧

radio-id：要配置的 radio 的 id，范围为 1-48

【缺省配置】 支持短前导码类型

【命令模式】 AP 配置模式

【使用指导】 不支持对所有 AP 进行配置。

配置短时隙

- 可选配置。
- 配置后，AC 将下发该配置给对应的 AP，告知 AP Radio 开启短时隙功能。

【命令格式】 **short-slot-time radio** *radio-id*
【参数说明】 *radio-id*：要配置的 radio 的 id，范围为 1-48
【缺省配置】 使能短时隙功能
【命令模式】 AP 配置模式
【使用指导】 -

配置更新加密 TSC 功能

- 可选配置。
- 配置后，AC 将下发该配置给对应的 AP，告知 AP 使能更新加密 TSC 功能。

【命令格式】 **update-key-tsc enable**
【参数说明】 -
【缺省配置】 更新加密 TSC 功能不使能
【命令模式】 AP 配置模式、AP 组配置模式
【使用指导】 -

配置 AP 与无线传输对端之间允许的最远距离

- 可选配置。
- 配置后，AC 将下发该配置给对应的 AP，告知 AP Radio 使用下发的最远距离参数进行收发报文。

【命令格式】 **peer-distance** *val* **radio** *radio-id*
【参数说明】 *val*：要配置 AP 允许的最远距离，取值范围为 1000~25000，单位：m
radio-id：要配置的 radio 的 id，范围为 1-48
【缺省配置】 1000m
【命令模式】 AP 配置模式
【使用指导】 不支持对所有 AP 进行配置。仅当 AP 与无线传输对端的最远距离大于 1000m 时才需要配置。配置的距离可以偏大但不得小于实际距离。

配置射频的多用户多入多出功能

- 可选配置。
- 配置后，AC 将下发该配置给对应的 AP，告知 AP Radio 开启或关闭 MU-MIMO 功能。

【命令格式】 **mu-mimo enable radio** *radio-id*
【参数说明】 *radio-id*：要配置的 radio 的 id，范围为 1-48
【缺省配置】 缺省情况下，根据 AP 的支持情况而定：比如 radio 不支持，那么 AC 默认就不支持，如果 radio 支持，但默认配置为开启，那么 AC 上的默认值是开启，如果 radio 支持，但默认值是关闭，AC 上的默认值也是关闭。
【命令模式】 AP 配置模式/AP all 配置模式/AP 组配置模式
【使用指导】 -

检验方法

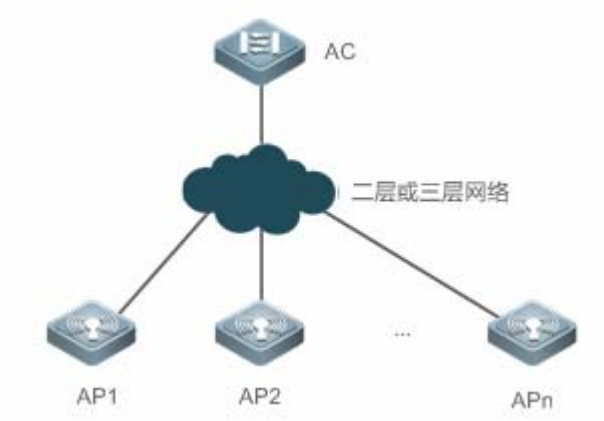
- 通过 **show ap-config running** *ap-name* 命令可以查看设置的 AP 射频参数配置。

配置举例

配置 AP 射频参数

【网络环境】

图 4-5



假设瘦 AP 环境中，在 AC 设备上对 AP1 设备有以下 AP 射频参数配置要求：

1、 在 AC 上配置支持中国国家码；
2、 在 AP1 Radio 1 上配置支持 AMPDU；
3、 在 AP1 Radio 1 上配置 11N 最大支持的 MCS 为 15；
4、 在 AP1 Radio 1 上配置 11AC 最大支持的 MCS 为 19；
5、 在 AP1 Radio 1 上配置天线发类型选择掩码为 7，天线收类型选择掩码为 5；
6、 在 AP1 Radio 1 上配置启用外置天线，并禁用内置天线；
7、 在 AP1 Radio 1 上配置 beacon 帧发送周期为 200ms；
8、 在 AP1 Radio 1 上配置使用国家码为 CN；
9、 在 AP1 Radio 1 上配置信道为 11；
10、 在 AP1 Radio 1 上配置带宽为 20M；
11、 在 AP1 Radio 1 上配置在 20M 带宽下 short-gi 开启；
12、 在 AP1 Radio 1 上配置保护模式开启；
13、 在 AP1 Radio 1 上配置为短前导码类型；
14、 在 AP1 Radio 1 上配置为短时隙；
15、 在 AP1 Radio 2 上配置使用国家码为 CN；
16、 在 AP1 Radio 2 上配置信道为 149；
17、 在 AP1 Radio 2 上配置带宽为 40M；
18、 在 AP1 Radio 2 上配置 Radio 使能状态为 enable；
19、 在 AP1 Radio 2 上配置分片阈值为 2346 Byte；
20、 在 AP1 Radio 2 上配置发射功率为 100%；
21、 在 AP1 Radio 2 上配置 RTS 阈值为 2347Byte；
22、 在 AP1 上配置更新加密 TSC 功能；
23、 在 AP1 Radio 1 上配置 AP 与无线传输对端之间允许的最远距离为 3000m。
24、 在 AP1 Radio 2 上配置 MU-MIMO 开启；

【配置方法】

- 在 AC 设备上面配置 AP1 射频参数如下

```
Ruijie# configure terminal
Ruijie(config)# ac-controller
Ruijie(config-ac)# country CN
Ruijie(config-ac)# exit
Ruijie(config)# ap-config AP1
Ruijie(config-ap)# 802.11n a-mpdu enable radio 1
Ruijie(config-ap)# 802.11n mcs support 15 radio 1
Ruijie(config-ap)# 802.11ac mcs support 19 radio 1
Ruijie(config-ap)# antenna transmit 7 radio 1
Ruijie(config-ap)# antenna receive 5 radio 1
Ruijie(config-ap)# external-antenna enable radio 1
Ruijie(config-ap)# beacon period 200 radio 1
Ruijie(config-ap)# country CN radio 1
Ruijie(config-ap)# channel 11 radio 1
Ruijie(config-ap)# chan-width 20 radio 1
Ruijie(config-ap)# short-gi enable radio 1 chan-width 20
Ruijie(config-ap)# green-field enable radio 1
Ruijie(config-ap)# preamble short radio 1
Ruijie(config-ap)# short-slot-time radio 1
Ruijie(config-ap)# country CN radio 2
Ruijie(config-ap)# channel 149 radio 2
Ruijie(config-ap)# chan-width 40 radio 2
Ruijie(config-ap)# enable-radio 2
Ruijie(config-ap)# fragment-threshold 2346 radio 2
Ruijie(config-ap)# power local 100 radio 2
Ruijie(config-ap)# rts-threshold 2347 radio 2
Ruijie(config-ap)# update-key-tsc enable
Ruijie(config-ap)# peer-distance 3000 radio 1
Ruijie(config-ap)# mu-mimo enable radio 2
```

【检验方法】

- 通过 show ap-config running ap-name 命令可以查看指定 AP 的射频参数配置。

```
Ruijie(config)# show ap-config running AP1
!
ap-config AP1
   802.11n mcs support 15 radio 1
   802.11n mcs support 15 radio 2
   802.11ac mcs support 19 radio 1
   update-key-tsc enable
   short-gi enable radio 1 chan-width 20
```

```
  green-field enable radio 1
  station-role root-ap radio 1
  station-role root-ap radio 2
  chan-width 40 radio 2
  antenna receive 5 radio 1
  external-antenna enable radio 1
  channel 11 radio 1
  channel 149 radio 2
  beacon period 200 radio 1
  power local 100 radio 2
  peer-distance 3000 radio 1
  mu-mimo enable radio 2
!
```

常见错误

- 无。

4.5.4 配置速率控制参数

配置效果

- 可以实现对瘦 AP 速率控制参数集中设置，方便管理员进行配置管理。

注意事项

- 无。

配置方法

↘ 设置 802.11a 用户支持的速率集

- 可选配置。
- 配置后，AC 将下发该配置给所有 AP，告知 AP 对 802.11a 用户使用指定的速率集配置。

【命令格式】 **802.11a network rate** { **6** | **9** | **12** | **18** | **24** | **36** | **48** | **54** } { **disabled** | **mandatory** | **supported** }

【参数说明】 **6**：速率为 6Mbps

9：速率为 9Mbps

12：速率为 12Mbps

18：速率为 18Mbps

24：速率为 24Mbps

36：速率为 36Mbps
48：速率为 48Mbps
54：速率为 54Mbps
disabled：不支持
mandatory：必须支持
supported：可选支持

【缺省配置】 速率 6Mbps、12Mbps、24Mbps 为强制支持，9Mbps、18Mbps、36Mbps、48Mbps、54Mbps 为可选支持
【命令模式】 AC 配置模式、AP 配置模式、AP 组配置模式
【使用指导】 -

设置 802.11b 用户支持的速率集

- 可选配置。
- 配置后，AC 将下发该配置给所有 AP，告知 AP 对 802.11b 用户使用指定的速率集配置。

【命令格式】 **802.11b network rate** { **1** | **2** | **5** | **11** } { **disabled** | **mandatory** | **supported**}
【参数说明】 **1**：速率为 1Mbps
2：速率为 2Mbps
5：速率为 5.5Mbps
11：速率为 11Mbps
disabled：不支持
mandatory：必须支持
supported：可选支持
【缺省配置】 速率 1Mbps、2Mbps、5.5Mbps、11Mbps 为强制支持
【命令模式】 AC 配置模式、AP 配置模式、AP 组配置模式
【使用指导】 -

设置 802.11g 用户支持的速率集

- 可选配置。
- 配置后，AC 将下发该配置给所有 AP，告知 AP 对 802.11g 用户使用指定的速率集配置。

【命令格式】 **802.11g network rate** { **1** | **2** | **5** | **6** | **9** | **11** | **12** | **18** | **24** | **36** | **48** | **54** } { **disabled** | **mandatory** | **supported**}
【参数说明】 **1**：速率为 1Mbps
2：速率为 2Mbps
5：速率为 5.5Mbps
6：速率为 6Mbps
9：速率为 9Mbps
11：速率为 11Mbps
12：速率为 12Mbps
18：速率为 18Mbps
24：速率为 24Mbps
36：速率为 36Mbps
48：速率为 48Mbps

54：速率为 54Mbps
disabled：不支持
mandatory：必须支持
supported：可选支持

【缺省配置】 速率 1Mbps、2Mbps、5.5Mbps、11Mbps 为强制支持，速率 6Mbps、9Mbps、12Mbps、18Mbps、24Mbps、36Mbps、48Mbps、54Mbps 为可选支持

【命令模式】 AC 配置模式、AP 配置模式、AP 组配置模式

【使用指导】 -

设置组播速率

- 可选配置。
- 配置后，AC 将下发该配置给所有应用该 WLAN 的 AP，告知 AP 在指定的 WLAN 下使用指定配置作为组播速率。

【命令格式】 **mcast-rate** *mcas-num*

【参数说明】 *mcast-num*：WLAN 组播速率为 24Mbps，用户可配置的组播速率为 1 Mbps、6 Mbps、11 Mbps、24 Mbps、54 Mbps。

【缺省配置】 组播速率为 24Mbps

【命令模式】 WLAN 配置模式

【使用指导】 -

配置 beacon 帧发送速率

- 可选配置。
- 配置后，AC 将下发该配置给对应的 AP，告知 AP 使用指定配置作为 beacon 帧发送速率。

【命令格式】 **beacon rate** *rate-Mbps* **radio** {*radio-id* | [*802.11b* | *802.11a*]}

【参数说明】 *rate_Mbps*：beacon 帧发送速率
radio-id：要配置的 radio 的 id，范围为 1-48
802.11b：对所有 2.4G 的 radio 进行配置
802.11a：对所有 5.8G 的 radio 进行配置

【缺省配置】 不配置 beacon 帧发送速率

【命令模式】 AP 配置模式

【使用指导】
1、 如果该速率被速率集配置禁用，则不能配置该速率；
2、 由于 5G 频段不支持的速率 1M/2M/5.5M/11M，因此若该 radio 处于 5G 频段，则不能配置以上速率。
3、 指定了 802.11b 参数将对所有 2.4G 的 radio 进行配置，配置在 AP 第一次上线的时候生效且自动转换为基于 radio 的配置；同样指定的 802.11a 参数将对所有 5.8G 的 radio 进行配置，配置在 AP 第一次上线的时候生效且命令自动转换为基于 radio 的配置。

检验方法

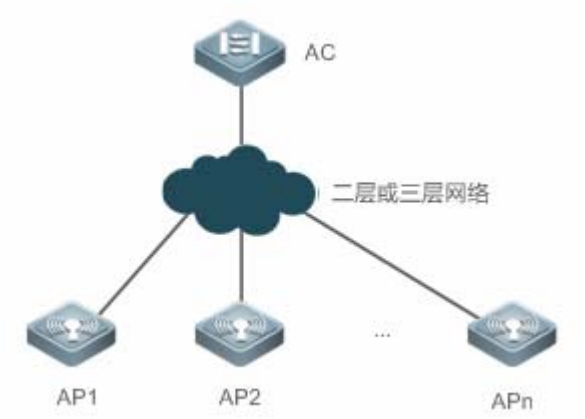
- 通过 **show running** 命令可以查看设置的参数配置。

配置举例

配置速率控制参数

【网络环境】

图 4-6



假设瘦 AP 环境中，在 AC 设备上有以下速率控制参数配置要求：

1、 配置 802.11a 用户禁用 6Mbps 速率；

2、 配置 802.11b 用户禁用 1Mbps、2Mbps、5.5Mbps 速率；

3、 配置 802.11g 用户禁用 1Mbps、2Mbps、5.5Mbps 速率；

4、 配置 WLAN 1 的组播速率为 54Mbps；

假设瘦 AP 环境中，在 AC 设备上对 AP1 设备有以下速率控制参数配置要求：

1、 在 AP1 Radio 1 配置 beacon 帧发送速率；

【配置方法】

- 在 AC 设备上面配置速率控制参数如下

```
Ruijie# configure terminal
Ruijie(config)# ac-controller
Ruijie(config-ac)# 802.11a network rate 6 disabled
Ruijie(config-ac)# 802.11b network rate 1 disabled
Ruijie(config-ac)# 802.11b network rate 2 disabled
Ruijie(config-ac)# 802.11b network rate 5 disabled
Ruijie(config-ac)# 802.11g network rate 1 disabled
Ruijie(config-ac)# 802.11g network rate 2 disabled
Ruijie(config-ac)# 802.11g network rate 5 disabled
Ruijie(config-ac)# exit
Ruijie(config)# wlan-config 1
Ruijie(config-wlan)# mcast-rate 54
```

- 在 AC 设备上配置 AP1 设备的 beacon 帧发送速率如下

```
Ruijie# configure terminal
Ruijie(config)# ap-config AP1
```

```
Ruijie(config-ap)# beacon rate 12.0 radio 1
```

【检验方法】

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

```
Ruijie# show running-config
...
!
wlan-config 1 ss
 enable-broad-ssid
 mcast-rate 54
!
...
!
ac-controller
 country CN
 802.11g network rate 1 disabled
 802.11g network rate 2 disabled
 802.11g network rate 5 disabled
 802.11g network rate 11 mandatory
 802.11g network rate 6 supported
 802.11g network rate 9 supported
 802.11g network rate 12 supported
 802.11g network rate 18 supported
 802.11g network rate 24 supported
 802.11g network rate 36 supported
 802.11g network rate 48 supported
 802.11g network rate 54 supported
 802.11b network rate 1 disabled
 802.11b network rate 2 disabled
 802.11b network rate 5 disabled
 802.11b network rate 11 mandatory
 802.11a network rate 6 disabled
 802.11a network rate 9 supported
 802.11a network rate 12 mandatory
 802.11a network rate 18 supported
 802.11a network rate 24 mandatory
 802.11a network rate 36 supported
 802.11a network rate 48 supported
 802.11a network rate 54 supported
!
...
```

- 通过 show ap-config running ap-name 命令可以查看指定 AP 的 beacon 帧发送速率配置。

```
Ruijie(config)# show ap-config running AP1
!
ap-config AP1
   channel 11 radio 1
   channel 149 radio 2
   beacon period 200 radio 1
   beacon rate 12.0 radio 1
   power local 100 radio 2
!
```

常见错误

- 无。

4.5.5 配置节电处理参数

配置效果

- 可以实现对瘦 AP 节电处理参数集中设置，方便管理员进行配置管理。

注意事项

- 无。

配置方法

↘ 配置 DTIM 周期

- 可选配置。
- DTIM 周期越大，节电效果越好，但是下行的多播报文延时越大。

【命令格式】 **beacon dtim-period** *period-num* **radio** *radio-id*

【参数说明】 *period-num*：指定 DTIM 周期，，单位为 1 个 Beacon 帧周期，取值范围 1~255。

radio-id：指定要配置的 radio 的 id，范围为 1-48

【缺省配置】 DTIM 周期为 1 个 Beacon 帧周期

【命令模式】 AP 配置模式

【使用指导】 -

↘ 配置启用/禁用 U-APSD 节电模式

- 可选配置。

- 启用 U-APSD 节电模式，可以减小实时性要求高的业务在电源管理过程中的延迟，通过关闭大多时候的无线信号的发射，延长了电池的使用时间。

【命令格式】 **apsd** { **enable | disable** } **radio** *radio-id*

【参数说明】 **enable**：指定启用 U-APSD 节电模式。

disable：指定禁用 U-APSD 节电模式。

radio-id：指定要配置的 radio 的 id，范围为 1-48

【缺省配置】 启用 U-APSD 节电模式

【命令模式】 AP 配置模式

【使用指导】 -

检验方法

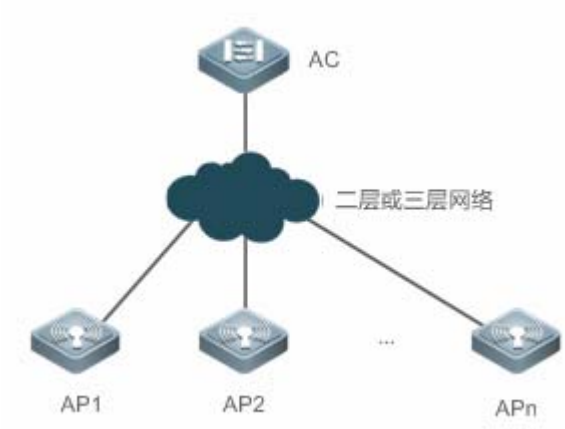
- 通过 **show ap-config running** *ap-name* 命令可以查看设置的参数配置。

配置举例

配置节电处理参数

【网络环境】

图 4-7



【配置方法】

- 在 AC 设备上配置 AP1 Radio 1 的 DTIM 周期为 3。
- 在 AC 设备上配置 AP1 Radio 1 启用 U-APSD。

```
Ruijie#configure terminal
Ruijie(config)#ap-config AP0001
Ruijie(config-ap)#beacon dtim-period 3 radio 1
Ruijie(config-ap)#apsd enable radio 1
```

【检验方法】

- 通过 show ap-config running ap-name 命令可以查看指定 AP 的节电处理参数配置。

```
Ruijie(config)# show ap-config running AP1
!
ap-config AP1
```

```
  802.11n mcs support 15 radio 1
  802.11n mcs support 15 radio 2
  update-key-tsc enable
  short-gi enable radio 1 chan-width 20
  green-field enable radio 1
  station-role root-ap radio 1
  station-role root-ap radio 2
  chan-width 40 radio 2
  antenna receive 5 radio 1
  channel 11 radio 1
  channel 149 radio 2
  beacon period 200 radio 1
  beacon dtim-period 3 radio 1
  power local 100 radio 2
!
```

常见错误

- 无。

4.5.6 配置链路完整性检测功能

配置效果

- 开启链路完整性检测功能。

注意事项

- 无。

配置方法

↘ 开启链路完整性检测功能

- 必须配置，使用 **link-check enable** 命令可以打开链路完整性检测功能。

【命令格式】 **link-check enable**
【参数说明】 -
【缺省配置】 链路完整性检测功能关闭
【命令模式】 全局配置模式
【使用指导】 默认情况下，链路完整性检测功能关闭。

检验方法

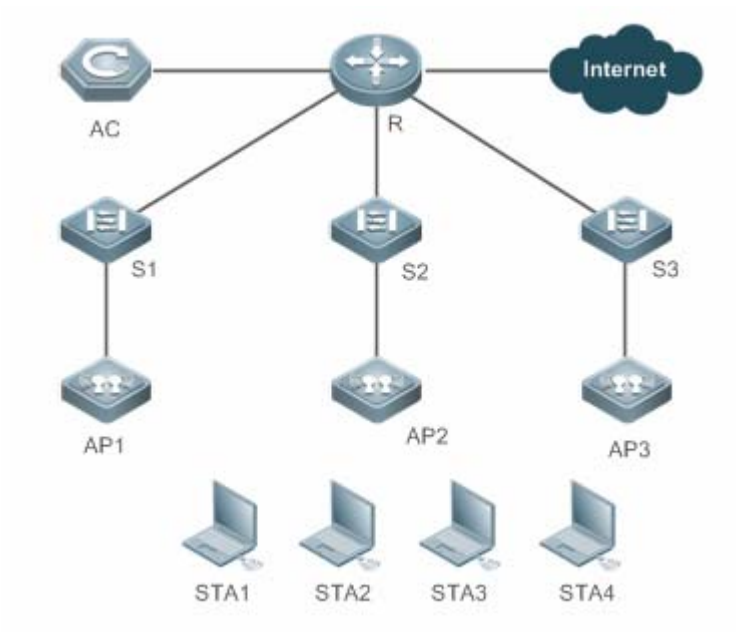
- 通过 **show running-config** 命令可以查看链路完整性检测功能配置状态。

配置举例

配置链路完整性检测功能

【网络环境】

图 4-8



假设如图瘦 AP 环境中，需要打开链路完整性检测功能。

1、打开链路完整性检测功能

【配置方法】

- 在 AC 设备上面配置链路完整性检测功能

```
Ruijie# configure terminal
Ruijie(config)# link-check enable
```

【检验方法】

- 通过 show running-config 命令可以查看。

```
Ruijie(config)# show running-config
.....
link-check enable
.....
```

常见错误

- 无。

4.5.7 配置电子书包参数

配置效果

- 可以实现对各 AP 及其 Radio 相关电子书包参数设置，方便管理员进行配置管理。

注意事项

- 无。

配置方法

↘ 配置 AMPDU 软件重传次数

- 可选配置。
- 打开该功能后，AC 将下发该配置给对应的 AP，告知 AP 使用指定的 AMPDU 软件重传次数发送 AMPDU 聚合报文。
- 重传的次数越大，子帧丢失的可能性越低，但是重传次数过多可能造成空口负担增大，造成空气中其他报文的实时性下降，如果需要在子帧丢失概率较大的干扰下确保报文尽可能避免丢失，可以将数值调大。

【命令格式】 **ampdu-retries** *times* **radio** *radio-id*

【参数说明】 *times*：软件重传次数，取值范围 1-10

radio-id：要配置的 radio 的 id，范围为 1-48

【缺省配置】 缺省情况下 AMPDU 软件重传次数为 10

【命令模式】 AP 配置模式

【使用指导】 配置仅在 AP 的 Radio 工作在 11N 模式或 11AC 模式下生效。

不支持对所有 AP 进行配置。

↘ 配置是否开启 AMPDU 聚合报文的 RTS 保护机制

- 可选配置。
- 配置该功能后，AC 将下发该配置给对应的 AP，告知 AP 发送 AMPDU 聚合报文使用 RTS 保护机制。
- 只有隐藏节点问题造成的空口资源浪费大于 RTS 交互造成的空口资源浪费时，才开启 AMPDU 的 RTS 保护。

【命令格式】 **ampdu-rts radio** {*radio-id* | [*802.11b* | *802.11a*]}

【参数说明】 *radio-id*：要配置的 radio 的 id，范围为 1-48

802.11b：对所有 2.4G 的 radio 进行配置

802.11a：对所有 5.8G 的 radio 进行配置

【缺省配置】 缺省情况下关闭 AMPDU 聚合报文的 RTS 保护机制

【命令模式】 AP 配置模式

【使用指导】 指定了 802.11b 参数将对所有 2.4G 的 radio 进行配置，配置在 AP 第一次上线的时候生效且自动转换为基于 radio 的配置；同样指定的 802.11a 参数将对所有 5.8G 的 radio 进行配置，配置在 AP 第一次上线的时候生效且命令自动转换为基于 radio 的配置。配置仅在 AP 的 Radio 工作在 11N 模式或 11AC 模式下生效。

配置 AP 以太网单次收包数

- 可选配置，缺省情况下所有不同 AP 的取值是不同的。
- 缺省情况下，所有不同 AP 的取值是不同的。
- 配置该功能后，AC 将下发该配置给对应的 AP，告知 AP 以指定的参数限制以太网单次收包数。以太网单次收包数调高能够确保整网性能提升，但是有可能会降低 AP 对关键报文处理的实时性，例如在电子书包等对性能要求不高同时要求多用户并发且对报文实时性要求高的场景下，可以降低以太网单次收包数，此时的建议值为 25。

【命令格式】 **eth-schd** *limit*
【参数说明】 *limit*：以太网单次收包数，范围 1~256
【缺省配置】 缺省情况下，所有不同 AP 的取值是不同的
【命令模式】 AP 配置模式
【使用指导】 -

配置是否支持低密度奇偶校验编码

- 可选配置。
- 配置该功能后，AC 将下发该配置给对应的 AP，告知 AP 使用低密度奇偶校验编码进行收发报文。
- 如果支持低密度奇偶校验编码，可提高编码的可靠性与编码增益。在受到严重噪杂干扰的频率中使用此技术，可大幅降低资料遗失的风险，但是存在极少量终端在兼容 LDPC 上具备一定问题，表现为丢包。

【命令格式】 **ldpc radio** *radio-id*
【参数说明】 *radio-id*：要配置的 radio 的 id，范围为 1-48
【缺省配置】 支持低密度奇偶校验编码
【命令模式】 AP 配置模式
【使用指导】 -

配置是否使能接收发送空时分组码

- 可选配置。
- 配置该功能后，AC 将下发该配置给对应的 AP，告知 AP 使用空时分组码进行收发报文。
- 如果使能接收发送空时分组码，可以提高数据传输的可靠性；但是可能存在部分终端无法有效兼容该编码方式。

【命令格式】 **stbc radio** *radio-id*
【参数说明】 *radio-id*：要配置的 radio 的 id，范围为 1-48
【缺省配置】 使能接收发送空时分组码
【命令模式】 AP 配置模式
【使用指导】 -

一键配置电子书包网优

- 可选配置。
- 在 ap-config 配置模式下使用 **ebag** 命令一键配置电子书包网优，来实现快速配置。
- AP320/AP330/AP3220 等产品的优化项是：

- （1）有线口报文处理优化：eth-schd 25
- （2）无线聚合报文重传优化：ampdu-retries 2
- （3）关闭 wifox
- AP530 的优化项是：
- （1）radio 1、2 使用默认的 sta-idle-time 1800
- （2）radio 1 优化：11b/11g 禁用强制速率 1 2 5M，11g 强制速率 11 24M，开启 ampdu-rts
- 配置后，AC 将下发相应的配置给对应的 AP，告知 AP 使用指定的参数进行收发报文等。

【命令格式】 **ebag**
【参数说明】 **-**
【缺省配置】 没有缺省配置
【命令模式】 AP 配置模式
【使用指导】 一般用于电子书包场景中，其他场景慎用！

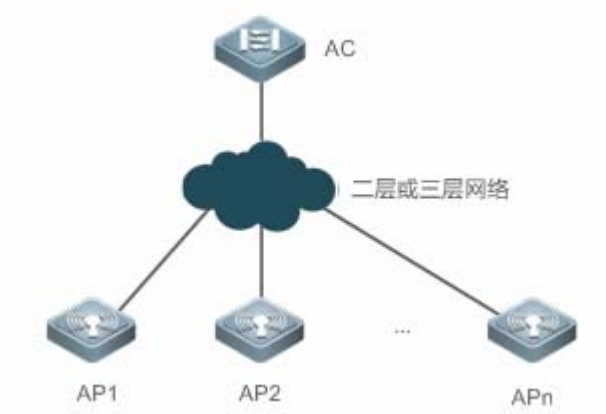
检验方法

- 通过 **show ap-config running** *ap-name* 命令可以查看设置的电子书包参数配置。

配置举例

↘ 配置电子书包参数

【网络环境】
图 4-9



假设瘦 AP 环境中，在 AC 设备上对 AP1 设备有以下电子书包参数配置要求：
1、 在 AP1 Radio 1 上配置 AMPDU 软件重传次数为 3；
2、 在 AP1 Radio 1 上配置开启 AMPDU 聚合报文的 RTS 保护机制；
3、 在 AP1 上配置以太网单次收包数为 100；
4、 在 AP1 Radio 1 上配置不支持低密度奇偶校验编码；
5、 在 AP1 Radio 1 上配置禁用接收发送空时分组码。

【配置方法】

- 在 AC 设备上面配置 AP1 电子书包参数如下

```
Ruijie# configure terminal
Ruijie(config)# ap-config AP1
Ruijie(config-ap)# ampdu-retries 3 radio 1
Ruijie(config-ap)# ampdu-rts radio 1
Ruijie(config-ap)# eth-schd 100
Ruijie(config-ap)# no ldpc radio 1
Ruijie(config-ap)# no stbc radio 1
```

【检验方法】

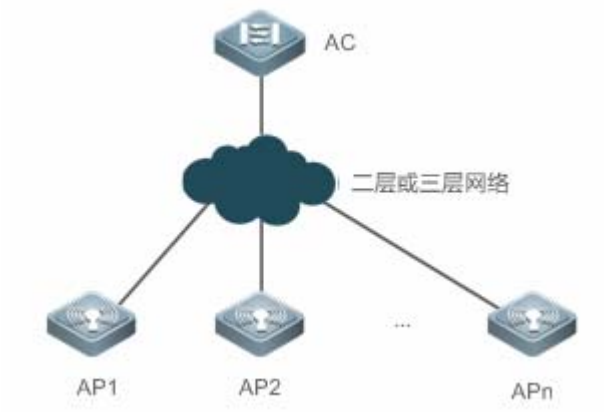
- 通过 show ap-config running ap-name 命令可以查看指定 AP 的电子书包参数配置。

```
Ruijie(config)# show ap-config running AP1
!
ap-config AP1
 ap-mac 00d0.f801.0528
 country US  radio 1
 channel 11 radio 1
 no 11acsupport enable radio 2
 ampdu-retries 3 radio 1
 ampdu-rts radio 1
 no stbc radio 1
 no ldpc radio 1
 eth-schd 100
 wmm edca-radio video aifsn 1 cwmin 3 cwmax 4 txop 90 radio 1
 wmm edca-radio back-ground aifsn 7 cwmin 4 cwmax 10 txop 5 radio 2
!
```

一键配置电子书包网优

【网络环境】

图 4-10



假设瘦 AP 环境中，AP1 设备工作在电子书包场景。在 AC 设备上对 AP1 设备有一键配置电子书包网优的要求。

【配置方法】
- 在 AC 设备上面一键配置 AP1 的电子书包网优参数如下

```
Ruijie# configure terminal
Ruijie(config)# ap-config AP1
Ruijie(config-ap)# ebag
```

【检验方法】
- 通过 show ap-config running ap-name 命令可以查看指定 AP 的电子书包参数配置。

```
Ruijie(config)# show ap-config running AP1
!
ap-config AP1
 ap-mac 00d0.f801.0528
 country US  radio 1
 channel 11 radio 1
 no 11acsupport enable radio 2
 ampdu-retries 2 radio 1
 ampdu-retries 2 radio 2
 eth-schd 25
 ebag
 wmm edca-radio video aifsn 1 cwmin 3 cwmax 4 txop 90 radio 1
 wmm edca-radio back-ground aifsn 7 cwmin 4 cwmax 10 txop 5 radio 2
!
```

常见错误

- 无。

4.5.8 一键WLAN配置

配置效果

- 在空配置的设备上，可以快速配置 WLAN 的功能；方便地勘人员快速配置，提高操作效率；方便渠道快速配置 WLAN 来进行性能测试等。

注意事项

- 无。

配置方法

↘ 一键配置 WLAN

- 可选配置。
- 在 config 配置模式下使用 **autowifi** 命令一键配置 WLAN，来实现快速配置无线网络。一般用于地勘人员快速配置，提高操作效率；方便渠道快速配置 WLAN 来进行性能测试等。

【命令格式】 **autowifi**

【参数说明】 -

【缺省配置】 没有缺省配置

【命令模式】 AC 的全局配置模式

【使用指导】 在空配置的设备上，为了实现快速配置，提供一键配置 WLAN 的功能。

一般用于地勘人员快速配置，提高操作效率；

方便渠道快速配置 WLAN 来进行性能测试等。

检验方法

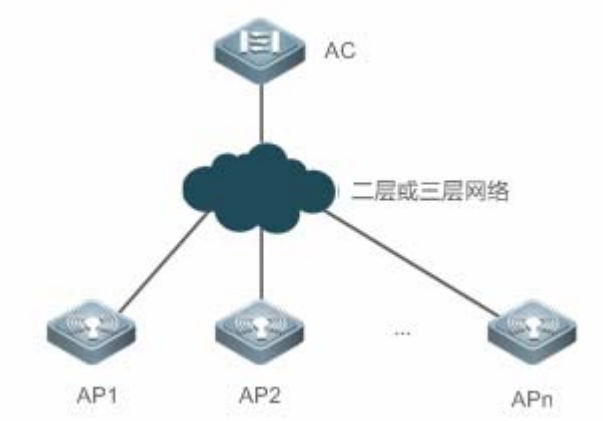
- 通过 **show running** 命令可以查看一键 WLAN 配置。

配置举例

↘ 一键配置 WLAN

【网络环境】

图 4-11



假设瘦 AP 环境中，在 AC 设备上有一键配置 WLAN 的要求。

【配置方法】

- 在 AC 设备上面一键配置 WLAN 如下

```
Ruijie# configure terminal
Ruijie(config)# autowifi
```

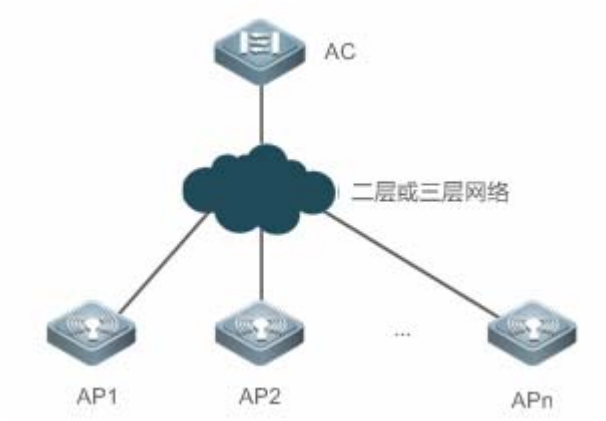
【检验方法】

- 通过 show running 命令可以查看一键 WLAN 配置。

```
Ruijie(config)# show running
!
wlan-config 1 autowifi_1234
```

【网络环境】

图 4-11



假设瘦 AP 环境中，在 AC 设备上有一键配置 WLAN 的要求。

【配置方法】

- 在 AC 设备上面一键配置 WLAN 如下

```
Ruijie# configure terminal
Ruijie(config)# autowifi
```

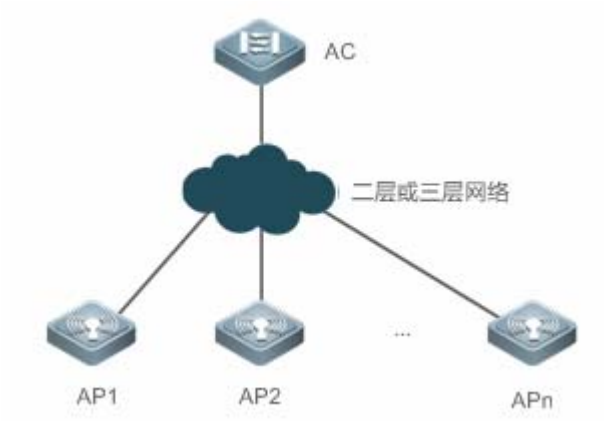
【检验方法】

- 通过 show running 命令可以查看一键 WLAN 配置。

```
!
ap-group default
 interface-mapping 1 2 ap-wlan-id 1
!
ap-config all
 fair-schedule
!
ac-controller
 country CN
 802.11g network rate 1 mandatory
 802.11g network rate 2 mandatory
 802.11g network rate 5 mandatory
 802.11g network rate 6 supported
 802.11g network rate 9 supported
 802.11g network rate 11 mandatory
 802.11g network rate 12 supported
 802.11g network rate 18 supported
 802.11g network rate 24 supported
 802.11g network rate 36 supported
 802.11g network rate 48 supported
 802.11g network rate 54 supported
 802.11b network rate 1 mandatory
 802.11b network rate 2 mandatory
```

【网络环境】

图 4-11



假设瘦 AP 环境中，在 AC 设备上有一键配置 WLAN 的要求。

【配置方法】

- 在 AC 设备上面一键配置 WLAN 如下

```
Ruijie# configure terminal
Ruijie(config)# autowifi
```

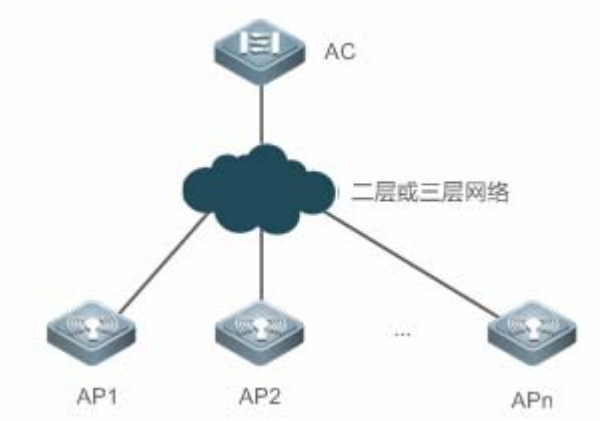
【检验方法】

- 通过 show running 命令可以查看一键 WLAN 配置。

```
 802.11b network rate 5 mandatory
 802.11b network rate 11 mandatory
 802.11a network rate 6 mandatory
 802.11a network rate 9 supported
 802.11a network rate 12 mandatory
 802.11a network rate 18 supported
 802.11a network rate 24 mandatory
 802.11a network rate 36 supported
 802.11a network rate 48 supported
 802.11a network rate 54 supported
!
ip dhcp pool web_ap_pool_1
 option 138 ip 88.88.88.88
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
!
ip dhcp pool web_sta_pool_1
 network 192.168.2.0 255.255.255.0
 dns-server 8.8.8.8
 default-router 192.168.2.1
!
link-check disable
!
```

【网络环境】

图 4-11



假设瘦 AP 环境中，在 AC 设备上有一键配置 WLAN 的要求。

【配置方法】

- 在 AC 设备上面一键配置 WLAN 如下

```
Ruijie# configure terminal
Ruijie(config)# autowifi
```

【检验方法】

- 通过 show running 命令可以查看一键 WLAN 配置。

```
vlan 1
!
vlan 2
!
interface Loopback 0
 ip address 88.88.88.88 255.255.255.255
!
interface VLAN 1
 ip address 192.168.1.1 255.255.255.0
!
interface VLAN 2
 ip address 192.168.2.1 255.255.255.0
!
wlansec 1
 security rsn enable
 security rsn ciphers aes enable
 security rsn akm psk enable
 security rsn akm psk set-key ascii autowifi
!
```

常见错误

- 无。

4.6 监视与维护

清除各类信息

- 无。

查看运行情况

作用	命令
显示无线用户链路信息	**linktest**
显示本 AC 的 802.11a 或 802.11b 网络中的 AP 列表	**show ac-config** { **802.11a** | **802.11b** } **summary**
查看所有 AP 的天线馈线状态	**show antenna all**
查看指定 AP 的天线馈线状态	**show antenna single** *ap-name*
查看所有 AP 的 radio 信息	**show ap-config radio**
查看指定 AP 的 radio 信息	**show ap-config radio ap-name** *ap-name*
查看知道 AP 的 radio 的一些特性配置信息	**show ap-config radio info** *ap-name*
查看指定 AP 指定 radio 的配置信息	**show ap-config radio** *radio-id* **config** *ap-name*
查看 AP 指定 radio 的详细状态信息	**show ap-config radio** *radio-id* **status** *ap-name*
显示 AP 的 radio 列表	**show ap-config radio status** *ap-name*
查看所有 AP 的 radio 详细信息	**show ap-config summary radio**
查看指定 MAC 用户信息	**show client details** *sta-mac*

查看调试信息

- 无。

5 ETH-MNG

5.1 概述

ETH-MNG(Ethernet Manage:以太网管理)是 AP 有线管理服务。用于配置 AP 有线相关参数设置。

LAN 口带宽限制功能是 ETH-MNG 的一项基础服务，就是在 AP 上配置各个 LAN 口的最大带宽，避免在无线、有线用户混用的场景中，有线用户占用大量带宽，导致无线用户上网速度慢。

下文仅介绍 ETH-MNG 的相关内容。

协议规范

- 无

5.2 典型应用

典型应用	场景描述
配置瘦 AP	在 AC 设备上配置命令，指定各瘦 AP 的参数配置。
LAN 口带宽限制配置	瘦 AP 架构，配置 AP 各个 LAN 口的最大带宽。

5.2.1 配置瘦AP

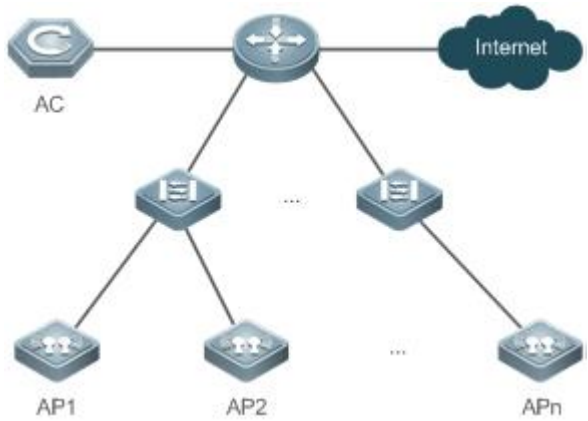
应用场景

配置瘦 AP，方便管理员在 AC 上集中管理瘦 AP 配置。假设网络中存在如下部署要求：

5、 允许在 AC 上配置瘦 AP 的 LAN 口最大带宽。

组网环境如下所示：

图 5-1 瘦 AP 场景组网图



功能部属

AC 的配置要点如下：

5、 对所有 AP 配置 LAN 口的最大带宽。

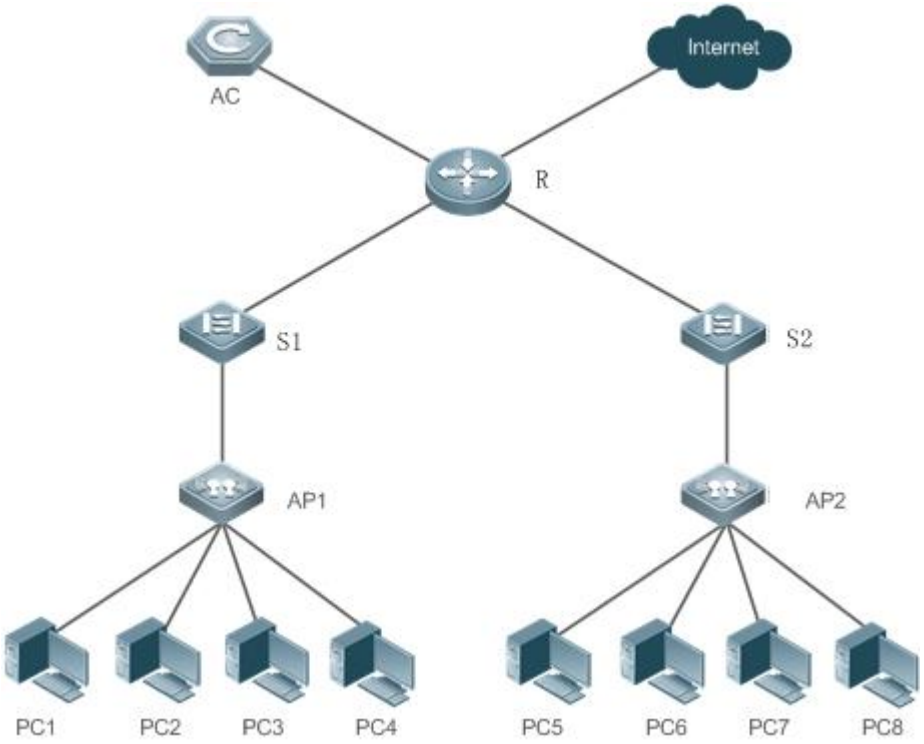
5.2.2 LAN口带宽限制

应用场景

瘦 AP 架构无线网络，配置 LAN 口带宽限制功能。

以下图为例：

- AC 通过路由器连接 Internet；两个 AP：AP1、AP2，分别通过交换机连接路由器并关联到 AC。
- PC1、PC2、PC3、PC4 关联在 AP1 上；PC5、PC6、PC7、PC8 关联在 AP2；它们通过 AC 访问 Internet。



【注释】 R 为网络出口路由器。
S1、S2 为二层交换机，作为 AP 的接入设备。
AP1、AP2 直接连接到 S1、S2 上。

功能部属

- 二层交换机提供 AP 设备的接入功能。
- 路由器 R 连接 AC 设备和 AP 设备网络；连接 PC 和 Internet。
- 通过 AC 配置 AP 的各个 LAN 口带宽限制功能。

5.3 功能详解

基本概念

无

功能特性

功能特性	作用
LAN 口带宽限制	用于配置 AP 的各个 LAN 口的最大带宽，避免在无线、有线用户混用的场景中，有线用户占用大量带宽，导致无线用户上网速度慢

5.3.1 LAN口带宽限制

工作原理

LAN 口带宽限制功能，用于配置 AP 的各个 LAN 口的最大带宽，避免有线用户占用大量带宽，导致无线用户上网速度慢。

5.4 产品说明

NBR800G、NBR950G、NBR1500G、NBR2000G 不支持无线集成 AC 功能，NBR108G-P、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持无线集成 AC 功能。

5.5 配置详解

配置项	配置建议&相关命令	
配置 LAN 口最大带宽	可选配置，用于设置 AP 的 LAN 口最大带宽	
	瘦 AP 配置：wired-rate *value* [**port** *port-id*]	AC 上配置 AP 的各个 LAN 口最大带宽，单位是 Mbps，命令不指定 port 时，表示配置 ap 上的所有 LAN 口速率。
	胖 AP 配置：wired-rate *value*	AP 上配置各个 LAN 口最大带宽，单位是 Mbps。

5.5.1 LAN口带宽限制

配置效果

- 配置各个 LAN 口的最大带宽。

注意事项

- 无。

配置方法

↘ 配置 LAN 口带宽限制功能

- 可选配置。

- 应该在 AC 设备上或胖 AP 设备上配置，命令支持差异详见配置手册。
- 使用 **wired-rate** 命令可以配置 LAN 口的最大带宽。

【命令格式】 **瘦 AP 配置：wired-rate** *value* [**port** *port-id*]

胖 AP 配置：wired-rate *value*

【参数说明】 不指定 port 时，表示配置所有的 port。

【缺省配置】 缺省情况下各个 LAN 口带宽不限制，为各个 LAN 口协商的最大带宽

【命令模式】 瘦 AP 为 AP 配置模式和 AP-GROUP 配置模式，胖 AP 为接口配置模式

【使用指导】 默认情况下，各个 LAN 口带宽不限制。

检验方法

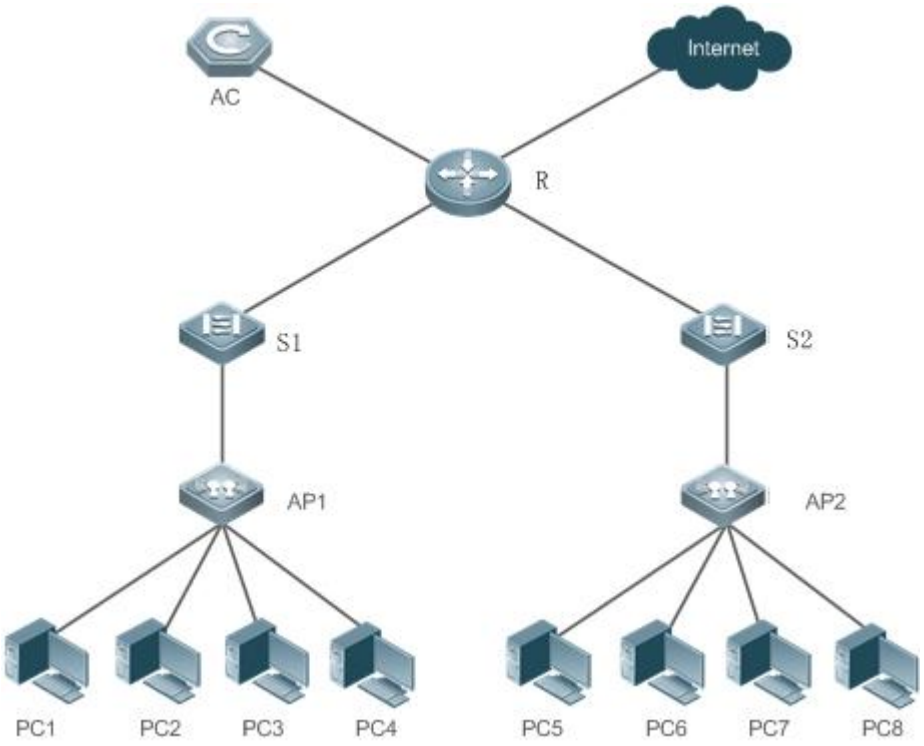
- 通过 **show running-config** 命令可以查看各个 LAN 口带宽限制功能的配置状态。

配置举例

↘ 配置 LAN 口带宽限制

【网络环境】

图 5-2



假设如图瘦 AP 环境中，需要对 LAN 口的带宽做限制。

1、配置各个 LAN 口最大带宽

【配置方法】 ● 在 AC 设备上面配置 AP 的 port 3 的最大带宽为 30Mbps

AC

```
Ruijie(config)# ap-config [ap-name]
Ruijie(config-ap)# wired-rate 30 port 3
```

- 在 AC 设备上面配置组 AP 的 port 3 的最大带宽为 30Mbps

```
Ruijie(config)# ap-group default
Ruijie(config-group)#wired-rate 30 port 3
```

- 在 AC 设备上面配置组 AP 的所有 LAN port 的最大带宽为 30Mbps

```
Ruijie(config)# ap-group default
Ruijie(config-group)#wired-rate 30
```

- 在 AC 设备上面配置所有 AP 的 port 3 的最大带宽为 30Mbps

```
Ruijie(config)# ap-config all
```

- Ruijie(config-ap)# wired-rate 30 port 3

AP120-W

- 在 AP120-W 设备上面配置 interface 0/4 的最大带宽为 40Mbps

```
Ruijie(config)#interface fastEthernet 0/4
Ruijie(config-if-FastEthernet 0/4)#wired-rate 40
```

AP130-W

- 在 AP130-W 设备上面配置 interface 0/4 的最大带宽为 40Mbps

```
Ruijie(config)#interface GigabitEthernet 0/4
```

Ruijie(config-if-GigabitEthernet 0/4)#wired-rate 40

【检验方法】

- 在 AC 上通过 show ap-config running-config 命令可以查看。

AC

```
Ruijie(config)# show ap-config running-config
ap-config ap120w-4
 wired-rate 30 port 3
```

- 在 AC 上通过 show running-config 命令可以查看。

AC

```
Ruijie(config)# show running-config
ap-group default
 wired-rate 30 port 3
```

- 在 AC 上通过 show running-config 命令可以查看。

AC

```
Ruijie(config)# show running-config
ap-group default
 wired-rate 30
```

- 在 AC 上通过 show running-config 命令可以查看。

AC

```
Ruijie(config)# show running-config
ap-config all
 …
 wired-rate 30 port 3
 …
```

- 在 AP 上通过 show running-config 命令可以查看。

AP120-W

```
Ruijie(config)# show running-config
…
interface FastEthernet 0/4
 wired-rate 40
…
```

AP130-W

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

```
...
interface GigabitEthernet 0/4
wired-rate 40
...
```

常见错误

- 无。

5.6 监视与维护

清除各类信息

- 无。

查看运行情况

- 无。

查看调试信息

- 无。

6 DATA-PLANE

6.1 概述

data-plane 是一种对广播转发报文的控制功能，它包括广播转发比重控制，广播无线转发控制。

广播转发比重控制，是限定广播转发中不同类型报文的比重，避免某种类型的报文占用所有资源，而影响用户使用。

广播无线转发控制，是仅将必要的报文转发到无线，以避免一些无用的广播报文占用大量的无线射频资源。

- 广播转发比重控制适用于所有需要广播洪泛的报文。
- 广播无线转发控制适用于所有需要发往无线空口的报文。

协议规范

- 无

6.2 典型应用

典型应用	场景描述
广播转发控制	使用瘦 AP 组网，至少包括一台 AC、一台 AP

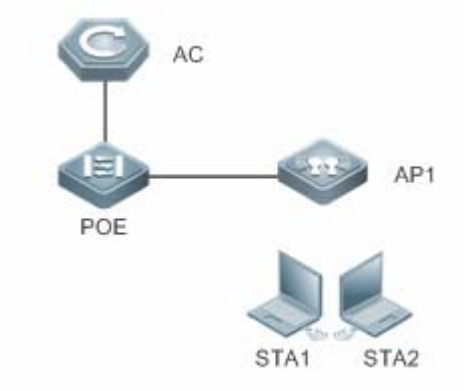
6.2.1 广播转发控制

应用场景

在无线网络中，部署一台 AC 设备，在 AC 上对广播报文发往无线进行控制。

以下图为例，在 AC 设备上对广播报文发往无线进行控制。

图 6-1



【注释】 AC：无线控制器设备。
POE：交换机设备，作为 AP 的网关。
AP：无线接入设备。
STA1、STA2：用户设备，作为 STA 来使用。

功能部属

- 在 AC 设备上开启广播无线转发控制功能。

6.3 功能详解

基本概念

↘ 广播转发比重控制

在网络交换设备中，需要进行广播洪泛的报文可能有广播、组播以及部分单播报文。针对每种类型报文设置广播转发比重，避免某类广播报文将所有广播转发能力耗尽，以提升用户使用网络的体验。

↘ 广播无线转发控制

广播无线转发控制功能只将必需的广播报文转发到无线网络，避免广播报文占用大量的无线空口资源，为 STA 提供更好的网速。

功能特性

功能特性	作用
广播转发比重	限制不同类型报文广播转发中的比重，避免某种类型报文独占广播资源，而影响其他报文的正常转发。
广播无线转发	限制广播报文是否转发到无线网络，避免无用广播报文占用大量无线射频资源。

6.3.1 广播转发比重控制

广播转发比重控制是用来对某种类型的报文进行限制，保证该类型报文在广播转发中不能超过设置的比重。

工作原理

广播转发比重控制先对报文进行分类，大致可分为以下几类：单播报文、组播报文、广播报文、未知名组播、未知名单播。

- 报文分类，大致可分为以下几类：单播报文、组播报文、广播报文、未知名组播、未知名单播。
- 为每个报文类分配一个令牌桶，记录这个时刻可以通过的报文个数。
- 在每个单位周期内，会根据配置的广播转发比重，算出每个单位周期内可以通过的报文个数，来增加令牌桶的大小。
- 当有报文到达时，先判断该报文的类型，并查看相应类型的令牌桶是否令牌，若有令牌，则允许报文通过，并将令牌桶减少；若已无令牌，则将报文进行丢弃。

6.3.2 广播无线转发控制

广播无线转发控制是只将部分影响用户的广播报文转发到无线网络，来避免无用的广播报文占用大量的空口资源。

工作原理

由于无线网络的特殊性，在同一个网络的 STA（包括 AP）共享空口资源，而由于无线和有线网络性能上的差异，空口资源往往成为 STA 性能的瓶颈。而对于广播报文，通常是以低速率来进行发送，因此，广播报文的发送会占用更多的空口时间。

从实际应用来看，有部分的广播报文对无线用户来说是无用的，因此，若将这些广播报文转发到无线，将导致用户可用的空口资源变少，影响用户体验。

为了解决这个问题，对广播报文进行分类控制，只将某些特定的广播报文转到无线网络。

6.4 产品说明



NBR800G、NBR950G、NBR1500G、NBR2000G 不支持无线集成 AC 功能，NBR108G-P、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持无线集成 AC 功能。

6.5 配置详解

配置项	配置建议&相关命令	
广播转发比重控制	⚠ 可选配置。用来设置不同类型广播转发报文的比重。	
	data-plane queue-weight	AC/AP 上，配置不同类型广播转发比重

	data-plane token	AC/AP 上 ,配置广播转发令牌桶的更新周期和倍数
广播无线转发控制	⚠ 可选配置。用来设置广播无线转发。	
	data-plane wireless-broadcast	AC/AP 上，开启或关闭广播无线转发控制

6.5.1 配置广播转发比重

配置效果

- 用户可根据实际网络情况，限制某种报文广播转发的比重，防止由于过分突发流量所引发的网络拥塞。

注意事项

- 无。

配置方法

↘ 配置广播转发比重

- 可选配置。
- 如果用户需要调整广播报文的转发比重时，可进行配置。
- 集中转发场景，在 AC 上的全局模式下进行配置。
- 本地转发场景，在 AC 的 AP 配置模式下进行配置。

【命令格式】 **data-plane queue-weight** *unicast-packet-weight multicast-packet-weight broadcast-packet-weight unknown-multicast-packet-weight unknown-unicast-packet-weight*

【参数说明】 *unicast-packet-weight*：单播报文转发比重，范围为 1-100，缺省值为 16
multicast-packet-weight：组播报文转发比重，范围为 1-50，缺省值为 4
broadcast-packet-weight：广播报文转发比重，范围为 1-50，缺省值为 2
unknown-multicast-packet-weight：未知名组播报文转发比重，范围为 1-25，缺省值为 1
unknown-unicast-packet-weight：未知名单播报文转发比重，范围为 1-25，缺省值为 1

【缺省配置】 使用默认参数

【命令模式】 全局模式

【使用指导】 -

↘ 配置广播转发令牌桶的更新周期和倍数

- 可选配置。
- 如果用户需要调整广播报文的控制粒度，可进行配置。

- 集中转发场景，在 AC 上的全局模式下进行配置。
- 本地转发场景，在 AC 的 AP 配置模式下进行配置。

【命令格式】 **data-plane token** *token-interval token-base-rate*

【参数说明】 *token-interval*：广播转发令牌桶的更新周期，缺省值为 1，单位是 10ms

token-base-rate：广播转发令牌桶的倍数，AC 缺省值为 64，AP 缺省值为 5

【缺省配置】 使用默认参数

【命令模式】 全局模式

【使用指导】 设备每秒钟允许的广播报文速率为：报文比重 × (1 秒 / 令牌桶更新周期) × 令牌桶更新倍数

例如 AC 允许的未知名单播报文速率为：1 × (1 / 0.01) × 64 = 6400pps

检验方法

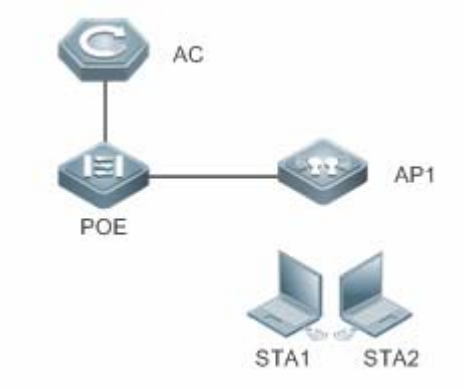
- 使用 **show run** 查看相应的配置。

配置举例

↘ 配置广播转发比重

【网络环境】

图 6-2



【配置方法】 ● 全局配置模式下，配置广播报文类型比重。

AC/AP

```
Ruijie#configure terminal
Ruijie(config)#data-plane queue-weight 100 50 50 25 25
Ruijie(config)#data-plane token 10 10
Ruijie(config)#exit
```

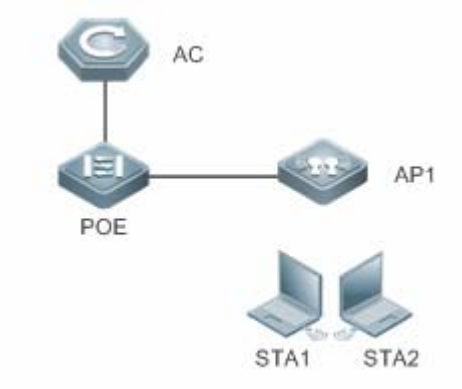
【检验方法】 通过 **show run** 显示配置信息。

AC/AP

```
Ruijie#showrun
...
```

【网络环境】

图 6-2



【配置方法】

AC/AP

- 全局配置模式下，配置广播报文类型比重。

```
Ruijie#configure terminal
Ruijie(config)#data-plane queue-weight 100 50 50 25 25
Ruijie(config)#data-plane token 10 10
Ruijie(config)#exit
```

【检验方法】

通过 **show run** 显示配置信息。

```
!
cwmp
!
data-plane queue-weight 100 50 50 25 25
data-plane token 10 10
!
...
```

常见错误

- 无。

6.5.2 配置广播无线转发

配置效果

- 无用广播报文不会转发向空口。

注意事项

- 无。

配置方法

广播转发功能

- 可选配置。
- 默认配置会限制网络中的广播报文。
- 如果用户希望对网络中的广播报文不作限制，可进行配置。
- 在全局配置模式下通过 **data-plane wireless-broadcast** 命令配置。

【命令格式】 **data-plane wireless-broadcast** { **enable** | **disable** }

【参数说明】 **enable**：允许所有广播报文转发到空口。

disable：禁止所有广播报文转发到空口

【缺省配置】 广播无线转发关闭的，即广播报文不会转发到无线网络。

【命令模式】 全局配置模式

【使用指导】 -

检验方法

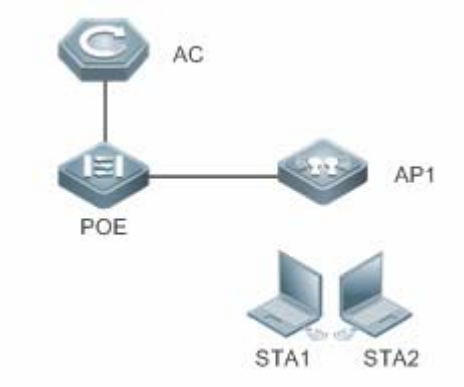
- 使用 **show run** 查看配置信息

配置举例

开启广播无线转发

【网络环境】

图 6-3



【配置方法】 **AC/AP**

- 全局配置模式下，开启广播无线转发功能。

```
Ruijie#configure terminal
```

```
Ruijie(config)#data-plane wireless-broadcast enable
```

【检验方法】 通过 **show running-config** 显示配置信息。

AC/AP

```
Ruijie# show ap-config running
!
cwmp
!
data-plane wireless-broadcast enable
!
```

常见错误

- 无。

6.6 监视与维护

清除各类信息

无。

查看运行情况

无。

查看调试信息

无。

7 WLOG

7.1 概述

WLOG（Wlan Log，无线日志）称为无线网络与终端状况存储与查看功能，主要针对的是对无线网络在过去一段时间内的网络及终端状况信息掌握的需求。通过收集、存储过去 24 小时的无线网络、AP、STA 的信息，然后通过 CLI 命令提供显示给用户，便于用户分析无线网络中出现的状况，定位出现的问题。

因此，WLOG 针对的信息的收集与存储，暂时不支持信息的自动分析、诊断。WLOG 功能致力于让用户通过提供的信息能够对过去 24 小时的无线网络、终端的状况有较为准确的了解，能够对出现的问题进行分析定位。

WLOG 的信息存储包括 AC 上存储和 AP 上存储两种。目前除了“STA 的空间信息”存储在 AP 上，其他信息都存储在 AC 上。

协议规范

- 无。

7.2 典型应用

典型应用	场景描述
瘦 AP 组网	使用瘦 AP 组网，至少包括一台 AC、一台 AP

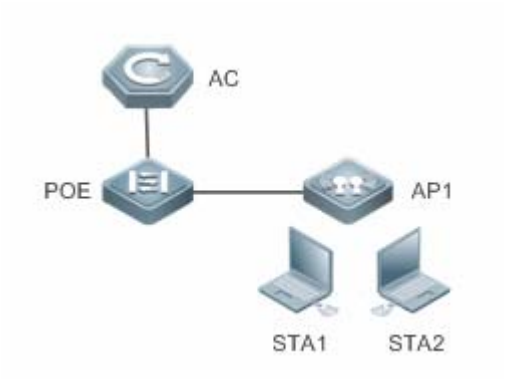
7.2.1 瘦AP组网

应用场景

在无线网络中，部署一台 AC 设备，查询当前 AC 设备上的整网、AP、STA 情况。

以下图为例，在 AC 设备上查看当前设备上的整网、AP、STA 情况。

图 7-1



【注释】 AC：无线控制器设备。
POE：交换机设备，作为 AP 的网关。
AP：无线接入设备。
STA1、STA2：用户设备，作为 STA 来使用。

功能部属

- 在 AC 设备上开启 WLOG 功能。

7.3 功能详解

基本概念

↘ AC 上信息的收集方式有两种：

- 定期收集

整网概况信息、AP 概况信息、STA 概况信息每隔一定的时间周期（1 次/1 小时）定期收集、存储。其中，AP 概况信息、STA 概况信息包括所有在线 AP、在线 STA 的信息。

- 接收通告收集

“AP 的行为类型”中的 AP 行为发生时，由相关模块通告 WLOG 模块进行行为发生现场的信息收集、存储。

“STA 的行为类型”中的 STA 行为发生时，有相关模块通告 WLOG 模块进行现场信息的收集、存储。

AP 上信息的收集只有 STA 的空间信息，针对所有在线 STA，采用定期收集的方式。

↘ 整网概况信息主要包括如下信息：

- AC 的连续运行时间
- 当前在线的 AP 数量
- 预配置但不在线的 AP 数量
- 当前在线的 AP 版本情况（各个版本的 AP 数量）

- 各个 WLAN（SSID）的终端情况如下：

1. 当前 WEB 认证成功在线的终端数
2. 当前 1X 认证成功在线的终端数
3. 当前免认证在线的终端数

AP 概况信息包括：

- AP 名称
- AP MAC 地址
- AP IP 地址
- AP 上线时间
- AP 各个有线端口情况：

1. 最近 5 分钟输入/输出速率(bits/sec)
2. 单播、广播、多播、错帧的输入/输出统计

- 每 radio 概况

1. 工作信道
2. 发射功率(dBm 绝对值)
3. 当前关联成功在线终端数
4. 当前 WEB 认证成功在线终端数
5. 当前 1X 认证成功在线终端数
6. 同频干扰信号强度
7. 收到错帧数量
8. 报文重传次数

终端（STA）的概况信息包括：

1. IP 地址
2. 信号强度
3. 连接速率
4. 当前关联的 AP、radio 以及 SSID

STA 的空间信息

- STA 的空间信息主要包含终端的数据帧、管理帧的统计信息，各类型速率的统计信息，具体如下：

1. 成功发送（AP 发送给终端）的数据帧数量/流量统计
2. 无应答的数据帧数量/流量统计
3. 管理帧数量/流量统计

4. 各个类型常规速率的帧数统计（常规速率分 8 个档次统计）

档次	0	1 2 3			4	5	6	7
包含速率类型（Mbps）	1/2	5.5/11	6/9	12/18	24/36 48/54		预留	预留

5. 各个类型 MIMO 速率的帧数统计（MIMO 速率分 8 个档次统计）

档次	0	1	2	3 4		5	6 7	
包含速率类型	mcs0 mcs1	mcs2 mcs3	mcs4 mcs5	mcs6 mcs7	mcs8 mcs9	mcs10 mcs11	mcs12 mcs13	mcs14 mcs15

空间信息主要用于检查 STA 是否处于低速状态、是否有过高比例的无 ACK 帧、是否收发了太多的管理帧，从而进一步分析定位低速节点、管理帧攻击、环境恶劣等导致的网络问题。STA 的空间信息属于实时变化的信息，目前的采集频率为每 5 分钟一次，由于数据量较大，目前只保存在 AP 上。

↘ AP 的行为类型

AP 的行为类型包括：上线、下线、CAPWAP 连接失败。

↘ STA 的行为类型

STA 的行为类型包括：关联、解关联、漫游、WEB 认证上线、WEB 认证下线、Dot1X 认证上线、Dot1X 认证下线。

功能特性

功能特性	作用
开启 WLOG 功能	开启 WLOG 功能，自动收集 AC、AP、STA 的信息。
STA 上下线信息对接 ELOG 功能	将 STA 的上下线信息与 ELOG 对接。

7.3.1 开启WLOG功能

开启 WLOG 功能之后，AC 或者 AP 会自动收集 AC、AP、STA 的信息，记录在内存中，让用户通过提供的信息能够对过去 24 小时的无线网络、终端的状况有较为准确的了解，能够对出现的问题进行分析定位。

工作原理

开启 WLOG 功能之后，AC 或者 AP 会自动收集 AC、AP、STA 的信息，记录在内存中。同时接收 AP、STA 的上下线通告，也记录到内存中，供用户查看。

7.3.2 STA上下线信息对接ELOG功能

开启 WLOG 功能之后，配置 ELOG 设备的 URL，STA 上下线动作发生的时候，将一些 STA 相关信息发送给 ELOG 设备。

工作原理

开启 WLOG 功能之后，接收 STA 的上下线通告，将 STA 的相关信息按照一定的格式发送给 ELOG。

7.4 产品说明

NBR800G、NBR950G、NBR1500G、NBR2000G 不支持无线集成 AC 功能，NBR108G-P、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持无线集成 AC 功能。

7.5 配置详解

配置项	配置建议 & 相关命令	
配置开启 WLOG 功能	必须配置。开启 WLOG 功能。	
	wlan diag enable	开启 WLOG 功能
配置 STA 上下线信息对接 ELOG 功能	可选配置。STA 上下线信息对接 ELOG 功能。	
	web-server enable api-path assoc-sta url *url*	配置对接的 Elog 服务器地址

7.5.1 配置开启WLOG功能

配置效果

- 打开 WLOG 功能之后，AC 或者 AP 能够自动记录 AC、AP、STA 信息。

注意事项

- 配置 WLOG 功能使能会进行内存的预分配。如果内存不够，则 WLOG 功能将使能失败；WLOG 功能关闭会进行所有存储信息内存与及预分配内存的释放。

配置方法

↘ 开启 WLOG 功能

- 必须配置，使用 wlog diag enable 命令来开启 WLOG 功能。
- 在 AC 设备的配置模式下开启。
- 开启 WLOG 功能之后，会定期收集信息，记录到内存中。

【命令格式】 **wlan diag enable**

【参数说明】 -

【缺省配置】 AC、AP 设备上 WLOG 功能缺省关闭

【命令模式】 全局配置模式

【使用指导】 -

检验方法

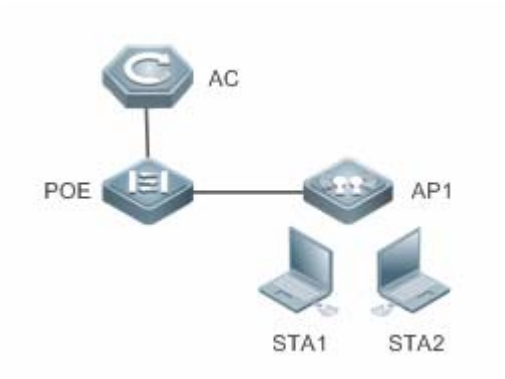
- 通过 **show wlan diag network** 检查确认 AC 上能查看到整网信息。
- 通过 **show wlan diag sta** 检查确认 AP 上能看到 STA 信息。

配置举例

↘ 开启 WLOG 功能

【网络环境】

图 7-2



【配置方法】 ● 在配置模式下开启 WLOG 功能

AC

```
Ruijie# configure terminal
Ruijie(config)# wlan diag enable
```

【检验方法】 通过 **show wlan diag network** 查看 WLOG 状态。

AC

```
Ruijie# show wlan diag network
Time: 2013-10-20 16:44:45
AC uptime: 294 h
Online AP: 1
Offline AP:0
Online AP Version:
PID             HwVer      SwVer                                AP Number
--------------- ---------- ---------------------------------- ---------
AP320-I         1.00       RGOS 10.4(1b19)p2, Release(167368)  1
Wlan information:
```

```
SSID                                Active STA WEB Auth 1X Auth  Open
----------------------------------- ---------- -------- -------- --------
RGWLAN_1T13_wireless                0          0        0        1
RGWLAN_IT13_wireless_1X             0          0        0        0
guest_only                          0          0        0        1
```

常见错误

- 无。

7.5.2 配置STA上下线信息对接ELOG功能

配置效果

- 打开 WLOG 功能和配置 ELOG 的 url 之后，AC 将 STA 的上下线信息发送给 ELOG 服务器。

注意事项

- 需要 STA 的上下线动作触发，在配置这个功能开启前 STA 上下线的信息是不会发送给 ELOG 的。

配置方法

↘ 配置 STA 上下线信息对接的 ELOG 的 url

- url 需要 Elog 服务器的完整地址。

【命令格式】 **web-server enable api-path assoc-sta url** *url*

【参数说明】 *url*：Elog 服务器的完整地址

【缺省配置】 缺省不配置即不与 Elog 服务器对接

【命令模式】 全局配置模式

【使用指导】 要能够顺利发送数据，要 WLOG 使能，并且如果在本地转发的情况下，如果 STA 上线后 AC 上没有 STA 的 IP 地址（show ac-config client 可以查看），在全局配置模式下配置 ip dhcp snooping，确保终端可以获取到 IP 地址。

检验方法

- 通过 **show running** 查看配置。

配置举例

↘ 配置 STA 上下线信息对接的 ELOG 服务器 url

【配置方法】

- 在全局配置模式下配置对接的 url 是 http://172.18.155.14:8080/elog/service/dc/updateSta

AC

```
Ruijie# configure terminal
Ruijie(config)#web-server enable api-path assoc-sta url
http://172.18.155.14:8080/elog/service/dc/updateSta
Ruijie(config)#
```

【检验方法】 通过 **show running-config** 查看。

AC

```
Ruijie# show running-config
!
web-server enable api-path assoc-sta url http://172.18.155.14:8080/elog/service/dc/updateSta
!
```

常见错误

- url 参数只写了一个 IP 地址，不是完整的 url。

7.6 监视与维护

清除各类信息

无。

查看运行情况

作用	命令
查看整网概况记录信息。	**show wlan diag network**
AC 上查看 AP 记录信息的命令	**show wlan diag ap** [**ap-mac** *ap-mac*] [**number** *number*]
在 AC 上查看终端信息	**show wlan diag sta** [**sta-mac** *sta-mac*] [**ip-range** *ip-prefix*] [**action** *action* [**result** *result*]] [**number** *number*]
在 AP 上查看终端信息	**show wlan diag sta** [**sta-mac** *sta-mac*] [**number** *number*]

查看调试信息

无。

WLAN 射频

本分册介绍 WLAN 射频相关内容，包括以下章节：

1. WLAN 优化配置
2. 频谱导航

1 WLAN 优化配置

1.1 概述

OPT（Optimization，无线网络优化）就是调整 WLAN 的某些配置信息，以达到优化无线网络、提升无线用户体验。

通过优化 WLAN 配置可以做到：

- 减少同频干扰、临频干扰，同时保证信号覆盖；
- 增加信道带宽；
- 提高信道利用率；
- 提高无线用户的可用信道带宽；
- 减少网络攻击和多播报文带宽占用；
- 提高 AP 下行吞吐量；
- 减少弱信号终端降低整体无线网络性能；
- 减少节电网卡的影响；
- 限制接入用户数量。

每一项 WLAN 优化手段的应用场合并不完全一样，见下表。

WLAN 优化手段	应用场合
信道规划调整优化	根据实际情况具体确定
功率规划调整优化	根据实际情况具体确定
关闭低速率应用	对于高度部署(学校和楼宇)都可以适用
创建纯 11n 的无线网络	根据实际网络需求设置
调整 Beacon 发送的时间间隔	对于高度部署且 AP 配置众多服务集(SSID)的时候有一定作用
启用无线用户 VLAN 内的二层隔离	对于没有二层互访需求的网络一定配置该功能
启用 RTS/CTS 保护机制	对于室内覆盖的网络适用
提高 AP 发送报文优先级，压制无线客户端发送报文	建议根据实际效果确定是否使用
减少弱信号终端影响	对于高度部署(学校和楼宇)都可以适用
Band Select	对于高度部署且 AP 支持双频可以适用
节电客户端处理优化	对于所有的场景可以普遍适用
11N A-MPDU 聚合帧发送保护	对于所有场景适用
限制 AP 下的 STA 接入数目	对于高度部署(学校和楼宇)且无线用户众多的情景都可以适用

协议规范

- IEEE Std 802.11-2012：Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications

1.2 典型应用

典型应用	场景描述
802.11n	AP 与 STA 都支持 11n 网络。
瘦 AP 架构 WLAN 频谱导航	瘦 AP 架构，由多台双频 AP 组建的 WLAN 开启频谱导航功能。

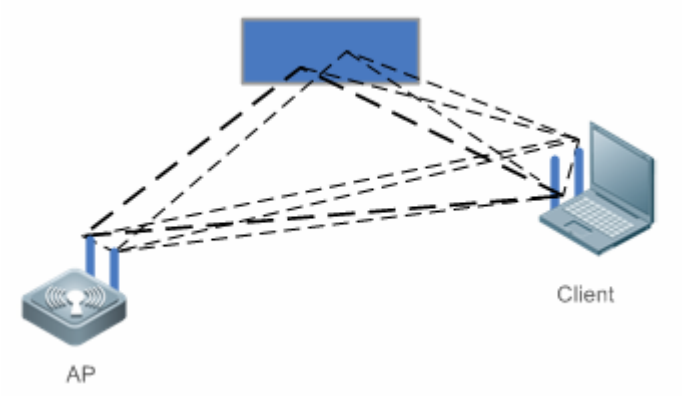
1.2.1 802.11n

应用场景

802.11n 作为 802.11 协议族的一个新协议，支持 2.4GHz 和 5GHz 两个频段，致力于为 WLAN 接入用户提供更高的“接入速率”，802.11n 主要通过 MIMO 技术、增加带宽和提高信道利用率两种方式来提高通信速率。

以下图为例，Client 通过 AP 接入有线网络，Client 与 AP 进行无线通信，Client 与 AP 之间在空间上存在多条传输路径。

图 1-1



【注释】 AP 为无线接入点。
Client 为无线客户端。

功能部属

- 在 AP、Client 中运行 IEEE802.11 协议，实现无线客户端的接入、认证。

1.2.2 瘦AP架构WLAN频谱导航

应用场景

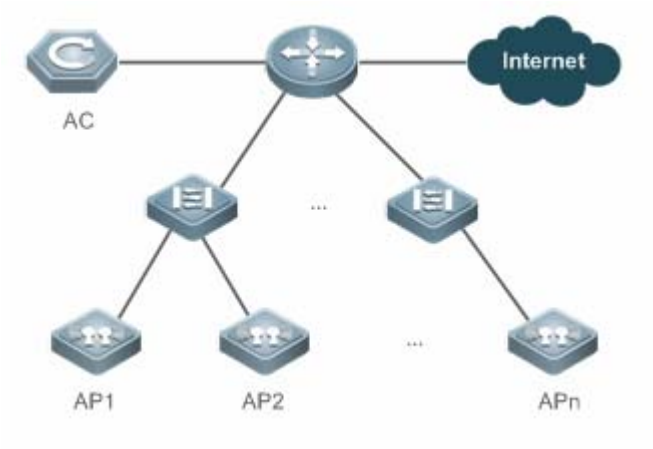
瘦 AP 架构，由多台双频 AP 组建的 WLAN 开启频谱导航功能。

以下图为例，

- 一台 AC 下关联很多双频 AP，AC 和 AP 通过二层交换设备和三层路由设备连接。

- WLAN 映射到所有双频 AP 的两个射频接口上。

图 1-2



【注释】 AC 为无线接入控制器。
AP1、AP2、.....、APn 都是双频 AP。

功能部属

- AC 设备上管理频谱导航功能的工作参数。
- AP 设备上运行频谱导航功能，识别 STA 类型并引导 STA 接入。

1.3 功能详解

基本概念

WLAN

WLAN（Wireless Local Area Network，无线局域网）是通过无线通信技术将计算机设备互联起来，构成可以互相通信和实现资源共享的网络体系。无线局域网本质的特点是不再使用通信电缆将计算机与网络连接起来，而是通过无线的方式连接，从而使网络的构建和终端的移动更加灵活。

AP

AP（Access Point）：无线终端访问有线网络的接入点，相当于无线终端与有线网络通信的桥梁。

STA

无线用户：使用无线终端上网的用户。

RSSI

RSSI（Received Signal Strength Indication，接收信号的强度指示），可以用来表示无线链接质量。

功能特性

功能特性	作用
关闭低速率应用	通过配置速率集关闭低速率应用。
适当增大 Beacon 帧周期	增大 Beacon 帧周期，降低发送 Beacon 帧的频繁程度，减少管理报文的信道占用率，增加无线用户可用的信道带宽。
无线用户 VLAN 内二层隔离	对于没有二层互访需求的网络一定配置该功能，减少网络攻击和多播报文带宽占用。
无线用户限速	为了使有限的网络资源能够更好地发挥效用，更好地为更多的用户服务。
提高抗干扰能力	当同频干扰存在时，适当降低 RTS 阈值，提升抗干扰能力。
提高信道竞争能力	用户可以根据实际需求，调整客户端或 AP 的 EDCA 参数值，使高优先级的 AC 在竞争中可以更早地进行退避过程，从而优先接入信道。
减少弱信号终端	为控制 AP 的网络覆盖范围，提高无线信号传输质量，可以通过限制接入的无线用户。
限制 AP 下的 STA 接入数目	通过限制 AP 下的 STA 接入数目，可以起到一定的负载分担功能，避免 AP 接入用户分配不均。
建立纯 11n 网络	通过配置纯 11n 网络，禁止非 11n 设备接入，使网络的 11n 设备均采用纯 HT 头部传输，减小报文头部尺寸，无线用户可用的信道带宽增加。
频谱导航	Band Select 引导双频 STA 连接到接入容量更高的 5G 频段 ,从而减轻 2.4G 频段的压力，提升用户体验。
一键网优	在无线网络运行一段时间后，可能出现网速慢、信号/干扰问题、认证页面出不来、支持 2.4G/5G 的网卡常关联到 2.4G、存在大量低速报文、组播报文丢包/重传等等问题。这时候，就需要对网络进一步优化。

1.3.1 关闭低速率应用

工作原理

通过配置速率集关闭低速率应用。

1.3.2 适当增大Beacon帧周期

工作原理

增大 Beacon 帧周期，降低发送 Beacon 帧的频繁程度，减少管理报文的信道占用率，增加无线用户可用的信道带宽。

1.3.3 无线用户VLAN内二层隔离

工作原理

对于没有二层互访需求的网络一定配置该功能，减少网络攻击和多播报文带宽占用。

1.3.4 无线用户限速

工作原理

为了使有限的网络资源能够更好地发挥效用，更好地为更多的用户服务，设备需要支持流量限速功能。当数据流量符合承诺速率时，允许数据包通过；数据流量不符合承诺速率时，丢弃数据包。

1.3.5 提高抗干扰能力

工作原理

为了避免信道冲突，而导致数据传输失败，IEEE 802.11 MAC 协议提供了一个 RTS/CTS（Request To Send/Clear To Send，握手协议），即请求发送/允许发送协议。假设工作站 A 需要向工作站 B 发送数据，首先会发送一个 RTS 请求帧，如果工作站 B 允许工作站 A 发送，就会回复一个 CTS 允许帧，工作站 A 收到后便开始发送数据。如果存在多个工作站向同一个工作站发送 RTS 以示请求发送数据，则只有收到 CTS 的工作站可以发送数据，没有收到 CTS 的工作站默认信道冲突，则等待一定时间后再发送 RTS 请求。

如果每个工作站每次发送数据前都要执行 RTS/CTS 握手，将导致过多的 RTS 帧占用信道带宽，用户可以设置 RTS Threshold 来指定发送数据的帧长度，如果工作站发送数据的帧长度小于 RTS Threshold 设置的门限，将不执行 RST/CTS 握手。

1.3.6 提高信道竞争能力

工作原理

EDCA 参数区分了不同优先级的接入信道的能力，每个 AC 均有独立的 EDCA 信道竞争参数。用户可以根据实际需求，调整客户端或 AP 的 EDCA 参数值，使高优先级的 AC 在竞争中可以更早地进行退避过程，从而优先接入信道。

实际配置中可根据应用需求选择配置 Client 端或者 AP 端的 EDCA 参数。配置 Client 端 EDCA 参数影响下行数据流量，配置 AP 使用的 EDCA 参数影响上行数据流量。

1.3.7 减少弱信号终端

工作原理

无线用户搜索 AP 的方式主要通过主动扫描或被动扫描。

- 主动扫描：即无线用户发送 Probe Request 帧请求接入 AP，AP 确认后发送 Probe Response 帧响应。

- 被动扫描：即 AP 定期向外广播 Beacon 帧，无线用户侦听到 Beacon 帧试图连接。

为控制 AP 的网络覆盖范围，提高无线信号传输质量，可以通过限制接入的无线用户。首先，可以通过控制 AP 广播 Beacon 帧的范围，减少远距离的无线用户接入；其次，可以通过限制无线用户的 RSSI（接收信号强度指示）的最小值，当接收到无线用户的请求帧的 RSSI 小于这个值，则不允许该无线用户接入。

1.3.8 限制AP下的STA接入数目

工作原理

在 WLAN 网络中，一台 AP 可接入多个无线用户数，管理员可以配置指定 AP 可连接的最大用户数。通过限制 AP 下的 STA 接入数目，可以起到一定的负载分担功能，避免 AP 接入用户分配不均。

1.3.9 建立纯 11n网络

工作原理

通过配置纯 11n 网络，禁止非 11n 设备接入，使网络的 11n 设备均采用纯 HT 头部传输，减小报文头部尺寸，无线用户可用的信道带宽增加。

1.3.10 频谱导航

工作原理

IEEE802.11 的主要通讯频段分成两段：

- 2.4GHz (2.412 to 2.4835 GHz) (IEEE 802.11b/g operates in this frequency range)
- 5GHz (5.15 to 5.35 and 5.725 to 5.825 GHz) (IEEE 802.11a operates in this frequency range)

双频 STA 同时支持 2.4G 频段和 5G 频段。但是，因为用户本身的专业知识比较薄弱，而且大部分无线接入服务供应商也没有进行有效的引导，再加上 802.11b/g 比 802.11a 的应用更为广泛，最终很多双频 STA 都使用 2.4G 频段，造成 2.4G 频段的拥挤和 5G 频段的浪费。实际上，5G 频段拥有更高的接入容量：2.4G 频段最多只能有 3 个不重叠的通讯信道；而 5G 频段却能提供更多不重叠的通讯信道，在中国有 5 个，而北美更是多达 24 个。

Band Select 引导双频 STA 连接到接入容量更高的 5G 频段，从而减轻 2.4G 频段的压力，提升用户体验。

1.3.11 一键网优

工作原理

在无线网络运行一段时间后，可能出现网速慢、信号/干扰问题、认证页面出不来、支持 2.4G/5G 的网卡常关联到 2.4G、存在大量低速报文、组播报文丢包/重传等等问题。这时候，就需要对网络进一步优化。

（1）网速慢，可能是没有配置限速，使得有的用户下载、看视频等占用大量带宽，导致其他用户网速慢；或是已配置了限速，但速率太高，没达到限速的效果；也可能是配置了限速，速率太低，导致网速慢等。针对这种问题，可选择网优的限速方案：基于 WLAN，对所有用户进行限速，上下行平均速率 256KB，突发速率 300KB。

（2）信号/干扰问题，可能出现信号偏弱、经常漫游、同频/邻频干扰等现象。可选择网优的 RRM 开启功能，让在线 AP 或新加入的 AP 都进行一次信道、功率调整，实现信号覆盖、错开与相邻 AP 的信道。若没有信号弱、同频/邻频干扰的问题，可用网优 RRM 关闭功能，关闭 RRM，提高设备性能。

（3）认证页面出不来，多数是由于配置的会话数太少导致。可选择网优的恢复默认会话数功能，使单个终端有 255 个会话数，单个端口可有 1000 个会话数。

（4）支持 2.4G/5G 的网卡常关联到 2.4G，可开启网优的 5G 优先功能；若环境中只有少量 5G 终端，建议关闭 5G 优先。

（5）环境中存在大量低速报文时，可使用网优的禁用低速功能，禁用 802.11b 802.11g 802.11a 小于 11Mbps 的速率。

（6）组播报文丢包/重传时，可能是设置了较高的组播速率，可用网优的恢复默认组播速率功能来保证用户体验。

1.3.12 智能网优配置

配置命令，智能进行无线网络优化。

工作原理

根据网络实时运行情况，智能进行网络优化。

1.3.13 mcell配置

配置命令，开启密集部署优化。

工作原理

开启密集部署优化。

1.3.14 漫游粘滞配置

工作原理

实时监控整个无线网络中 RSSI 低且体验不好的终端，根据各个 AP 收集到的终端探测信息，评估当前终端是否有更佳的 AP 进行接入，如果发现此类漫游粘滞的终端，AP 通过无线层面解认证的方式对该终端进行引导，帮助其关联到信号质量更佳的 AP 上。

1.3.15 远端关联配置

工作原理

根据终端关联时刻的探测信息，智能识别出终端是否关联到了最佳信号的 AP 上，一旦发现终端关联到了较远的 AP，上报信息通知 WIS 客户端，WIS 客户端根据这一段时间内收集到远端关联信息，智能对这些 AP 进行覆盖调优。

1.3.16 设备信息自动上传配置

工作原理

配置自动上传 AC 和 AP 的软件版本号，硬件版本号信息。

1.4 产品说明



NBR800G、NBR950G、NBR1500G、NBR2000G 不支持无线集成 AC 功能，NBR108G-P、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持无线集成 AC 功能。

1.5 配置详解

配置项	配置建议 & 相关命令	
配置速率集	可选配置。用于关闭低速率应用。	
	802.11a network rate	配置 11a 速率集
	802.11b network rate	配置 11b 速率集
	802.11g network rate	配置 11g 速率集
配置 Beacon 帧周期	可选配置。用于增大 Beacon 帧周期。	
	beacon period	配置 Beacon 帧周期
配置无线用户 VLAN 内的二层隔离	可选配置。用于启用无线用户 VLAN 内的二层隔离。	
	user-isolation ssid_ap enable	配置 AP 下基于 WLAN 的用户隔离
	user-isolation ap enable	配置 AP 下用户隔离

	user-isolation ssid_ac enable	配置 AC 下基于 WLAN 的用户隔离
	user-isolation ac enable	配置 AC 下用户隔离
配置无线用户限速	⚠ 可选配置。用于配置无线用户限速。	
	ap-based	配置基于 AP 的限速
	netuser	配置基于 Client 的限速
	wlan-based	配置基于 WLAN 的限速
配置 RTS/CTS 保护机制	⚠ 可选配置。用于配置 RTS/CTS 保护机制。	
	rts-threshold	配置 RTS 阈值
配置 EDCA 参数	⚠ 可选配置。用于配置 EDCA 参数。	
	wmm edca-client	配置 Client 端的 EDCA 参数
	wmm edca-radio	配置 AP 端的 EDCA 参数
配置允许接入信号强度	⚠ 可选配置。用于配置允许接入信号强度。	
	response-rssi	配置无线用户接入最小 RSSI
	coverage-area-control	配置管理帧发送功率
配置 AP 允许接入用户数	⚠ 可选配置。用于配置 AP 允许接入用户数。	
	sta-limit	配置基于 AP 的 STA 数量限制
配置纯 11n 网络	⚠ 可选配置。用于配置纯 11n 网络。	
	11asupport	配置是否支持 11a
	11bsupport	配置是否支持 11b
	11gsupport	配置是否支持 11g
	11nasupport	配置是否支持 11na
	11ngsupport	配置是否支持 11ng
配置频谱导航	⚠ 必须配置。用于开启 WLAN 的频谱导航功能。	
	band-select enable	开启频谱导航功能
	⚠ 可选配置。用于配置频谱导航功能的工作参数。	
	band-select acceptable-rssi	配置频谱导航可以接受的STA信号强度下限。
	band-select access-denial	配置拒绝双频 STA 接入 2.4G 频段的次数。
	band-select age-out	配置 STA 信息的老化时间。
	band-select probe-count	配置抑制 STA 的探测周期计数值。
	band-select scan-cycle	配置 STA 探测扫描周期门限。
配置一键网优	⚠ 可选配置。用于配置网优选择优化项。	
	wopt choose	配置网优选择优化项
	⚠ 可选配置。用于配置一键网优。	

	wopt enable	配置一键网优
智能网优配置	可选配置。用于配置网优选择优化项。	
	wis enable	开启智能网优
mcell 配置	可选配置。用于配置网优选择优化项。	
	mcell enable	开启密集部署优化
配置漫游粘滞	可选配置。用于配置网优选择优化项。	
	sticky-steering monitor-only	开启漫游粘滞监控
	可选配置。用于配置一键网优。	
	sticky-steering enable	开启漫游粘滞导航
配置远端关联	可选配置。用于配置网优选择优化项。	
	farpoint-steering enable	开启远端关联优化

1.5.1 配置速率集

配置效果

- 通过配置速率集关闭低速率应用，禁止 STA 和 AP 之间使用低速率发送报文，提高信道利用率。

注意事项

- 禁用一个速率，将使这个速率不可用。
- 禁用全部速率，将导致无线用户无法接入。
- 禁用全部 11b 速率，将导致 11b 的无线用户无法接入。

配置方法

↘ 配置 11a 速率集

- 可选配置，使用 802.11a network rate 命令可以配置 11a 速率集。
- 若无特殊要求，应在 AC 设备的 AC 配置模式下配置。
- 禁用一个速率，将使这个速率不可用；禁用全部速率，将导致 11a 的无线用户无法接入。

【命令格式】 **802.11a network rate** { **6** | **9** | **12** | **18** | **24** | **36** | **48** | **54** } { **disable** | **mandatory** | **supported** }

【参数说明】 **6**：速率为 6Mbps

9：速率为 9Mbps

12：速率为 12Mbps
18：速率为 18Mbps
24：速率为 24Mbps
36：速率为 36Mbps
48：速率为 48Mbps
54：速率为 54Mbps
disable：指定禁用速率
mandatory：指定强制速率
supported：指定支持速率

【缺省配置】 速率 6Mbps、12Mbps、24Mbps 为强制支持，9Mbps、18Mbps、36Mbps、48Mbps、54Mbps 为可选支持
【命令模式】 AC 配置模式
【使用指导】 -

配置 11b 速率集

- 可选配置，使用 802.11b network rate 命令可以配置 11b 速率集。
- 若无特殊要求，应在 AC 设备的 AC 配置模式下配置。
- 禁用一个速率，将使这个速率不可用；禁用全部速率，将导致 11b 的无线用户无法接入。

【命令格式】 **802.11b network rate** { **1** | **2** | **5** | **11** } { **disable** | **mandatory** | **supported** }
【参数说明】 **1**：速率为 1Mbps
2：速率为 2Mbps
5：速率为 5.5Mbps
11：速率为 11Mbps
disable：指定禁用速率
mandatory：指定强制速率
supported：指定支持速率
【缺省配置】 速率 1Mbps、2Mbps、5.5Mbps、11Mbps 为强制支持
【命令模式】 AC 配置模式
【使用指导】 -

配置 11g 速率集

- 可选配置，使用 802.11g network rate 命令可以配置 11g 速率集。
- 若无特殊要求，应在 AC 设备的 AC 配置模式下配置。
- 禁用一个速率，将使这个速率不可用；禁用全部速率，将导致 11g 的无线用户无法接入。

【命令格式】 **802.11g network rate** { **1** | **2** | **5** | **6** | **9** | **11** | **12** | **18** | **24** | **36** | **48 | 54** } { **disable** | **mandatory** | **supported** }
【参数说明】 **1**：速率为 1Mbps
2：速率为 2Mbps
5：速率为 5.5Mbps
6：速率为 6Mbps
9：速率为 9Mbps

11：速率为 11Mbps
12：速率为 12Mbps
18：速率为 18Mbps
24：速率为 24Mbps
36：速率为 36Mbps
48：速率为 48Mbps
54：速率为 54Mbps
disable：指定禁用速率
mandatory：指定强制速率
supported：指定支持速率

【缺省配置】 速率 1Mbps、2Mbps、5.5Mbps、11Mbps 为强制支持 ,6Mbps、9Mbps、12Mbps、18Mbps、24Mbps、36Mbps、48Mbps、 54Mbps 为可选支持

【命令模式】 AC 配置模式

【使用指导】 -

检验方法

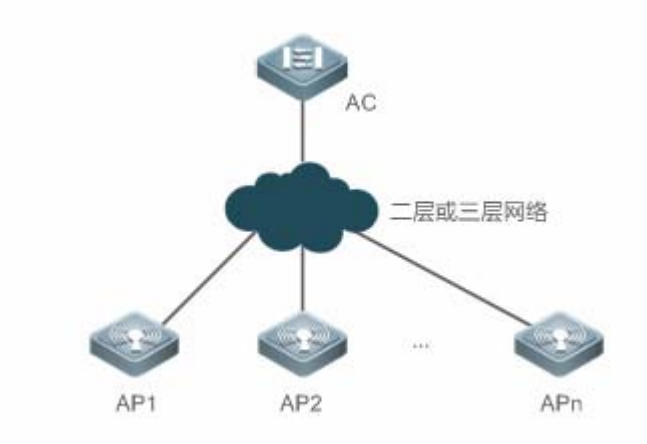
- 通过 **show running** 命令可以查看速率集的配置信息。

配置举例

↘ 配置速率集

【网络环境】

图 1-3



【配置方法】
- 在 AC 设备上配置 802.11a 用户禁用 6Mbps 速率；
- 在 AC 设备上配置 802.11b 用户禁用 1Mbps、2Mbps；
- 在 AC 设备上配置 802.11g 用户禁用 1Mbps、2Mbps、5.5Mbps 速率。

AC

```
Ruijie#configure terminal
Ruijie(config)#ac-controller
Ruijie(config-ac)#802.11a network rate 6 disabled
```

```
Ruijie(config-ac)#802.11b network rate 1 disabled
Ruijie(config-ac)#802.11b network rate 2 disabled
Ruijie(config-ac)#802.11g network rate 1 disabled
Ruijie(config-ac)#802.11g network rate 2 disabled
Ruijie(config-ac)#802.11g network rate 5 disabled
```

【检验方法】 用户配置速率集后，通过显示速率集配置信息进行检验。

- 通过 **show running** 命令可以查看速率集的配置信息。

```
Ruijie#show running
!
ac-controller
 country CN
 country US
 802.11g network rate 1 disabled
 802.11g network rate 2 disabled
 802.11g network rate 5 disabled
 802.11g network rate 11 mandatory
 802.11g network rate 6 supported
 802.11g network rate 9 supported
 802.11g network rate 12 supported
 802.11g network rate 18 supported
 802.11g network rate 24 supported
 802.11g network rate 36 supported
 802.11g network rate 48 supported
 802.11g network rate 54 supported
 802.11b network rate 1 disabled
 802.11b network rate 2 disabled
 802.11b network rate 5 mandatory
 802.11b network rate 11 mandatory
 802.11a network rate 6 disabled
 802.11a network rate 9 supported
 802.11a network rate 12 mandatory
 802.11a network rate 18 supported
 802.11a network rate 24 mandatory
 802.11a network rate 36 supported
 802.11a network rate 48 supported
 802.11a network rate 54 supported
!
```

常见错误

无。

1.5.2 配置Beacon帧周期

配置效果

- 增大 Beacon 帧周期，降低发送 Beacon 帧的频繁程度，减少管理报文的信道占用率，增加无线用户可用的信道带宽。

注意事项

- Beacon 帧周期不能太大，否则可能导致用户频繁掉线或探测。

配置方法

↘ 配置 Beacon 帧周期

- 可选配置，使用 **beacon period** 命令可以配置 Beacon 帧周期。
- 若无特殊要求，应在 AC 设备的 AP 配置模式下配置。
- Beacon 帧周期越小，发送 Beacon 帧越频繁，无线用户搜索到无线网络的速度越快；但是 Beacon 帧越多，即管理报文的信道占用率越多，无线用户可用的信道带宽越少。Beacon 帧周期不能太大，否则可能导致用户频繁掉线或探测。

【命令格式】 **beacon period** *milliseconds* **radio** *radio-id*

【参数说明】 *milliseconds*：指定 Beacon 帧周期，单位毫秒，范围 20~1000

radio-id：指定射频口索引，范围为 1~16

【缺省配置】 100 毫秒

【命令模式】 AP 配置模式

【使用指导】 不支持对所有 AP 进行配置

检验方法

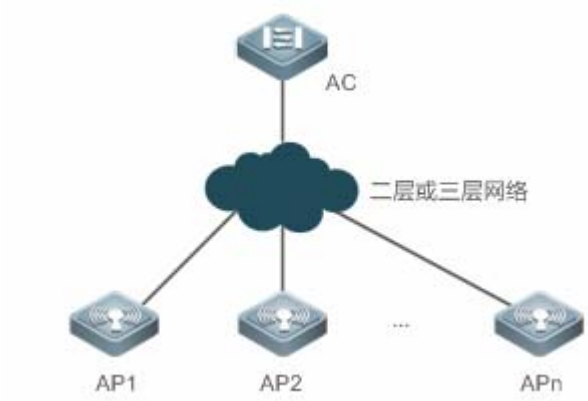
- 通过 **show ap-config running** 命令可以查看 Beacon 帧周期的配置信息。

配置举例

↘ 配置 Beacon 帧周期

【网络环境】

图 1-4



【配置方法】

- 在 AC 设备上配置 AP1 Radio1 的 Beacon 帧周期为 300 毫秒。

AC

```
Ruijie#configure terminal
Ruijie(config)#ap-config AP1
Ruijie(config-ap)#beacon period 300 radio 1
```

【检验方法】

用户配置 Beacon 帧周期后，通过显示 Beacon 帧周期配置信息进行检验。

- 通过 **show ap-config running** 命令可以查看 Beacon 帧周期的配置信息。

```
Ruijie#show ap-config running AP1
!
ap-config AP1
 no 11acsupport enable radio 1
 no 11acsupport enable radio 2
 802.11n mcs support 15 radio 1
 802.11n mcs support 15 radio 2
 antenna receive 3 radio 1
 antenna receive 3 radio 2
 antenna transmit 3 radio 1
 antenna transmit 3 radio 2
 radio-type 1 802.11b
 radio-type 2 802.11a
 beacon period 300 radio 1
 beacon period 100 radio 2
 ap-mac 001a.a9c5.3f49
 no enable-radio 1
 no enable-radio 2
!
```

常见错误

无。

1.5.3 配置无线用户VLAN内的二层隔离

配置效果

- 对于没有二层互访需求的网络一定配置该功能，减少网络攻击和多播报文带宽占用。

注意事项

- 无。

配置方法

↘ 配置 AP 下基于 WLAN 的用户隔离

- 可选配置，使用 user-isolation ssid-ap enable 命令可以配置 AP 下基于 WLAN 的用户隔离。
- 若无特殊要求，应在 AC 设备的 WIDS 配置模式下配置。
- 如果 AP 下基于 WLAN 的用户隔离，则在该 AP 上属于相同 WLAN 的无线用户在二层不能互相访问。

【命令格式】 **user-isolation ssid-ap enable**
【参数说明】 -
【缺省配置】 禁用 AP 下基于 WLAN 的用户隔离
【命令模式】 WIDS 配置模式
【使用指导】 -

↘ 配置 AP 下用户隔离

- 可选配置，使用 **user-isolation ap enable** 命令可以配置 AP 下用户隔离。
- 若无特殊要求，应在 AC 设备的 WIDS 配置模式下配置。
- 如果启用 AP 下用户隔离，则在该 AP 上的无线用户在二层不能互相访问。

【命令格式】 **user-isolation ap enable**
【参数说明】 -
【缺省配置】 禁用 AP 下用户隔离
【命令模式】 WIDS 配置模式
【使用指导】 -

↘ 配置 AC 下基于 WLAN 的用户隔离

- 可选配置，使用 **user-isolation ssid-ac enable** 命令可以配置 AC 下基于 WLAN 的用户隔离。
- 若无特殊要求，应在 AC 设备的 WIDS 配置模式下配置。
- 如果 AC 下基于 WLAN 的用户隔离，则在该 AC 上属于相同 WLAN 的无线用户在二层不能互相访问。

【命令格式】 **user-isolation ssid-ac enable**

【参数说明】 -
【缺省配置】 禁用 AC 下基于 WLAN 的用户隔离
【命令模式】 WIDS 配置模式
【使用指导】 -

配置 AC 下用户隔离

- 可选配置，使用 **user-isolation ac enable** 命令可以配置 AC 下用户隔离。
- 若无特殊要求，应在 AC 设备的 WIDS 配置模式下配置。
- 如果启用 AC 下用户隔离，则在该 AC 上的无线用户在二层不能互相访问。

【命令格式】 **user-isolation ac enable**
【参数说明】 -
【缺省配置】 禁用 AC 下用户隔离
【命令模式】 WIDS 配置模式
【使用指导】 -

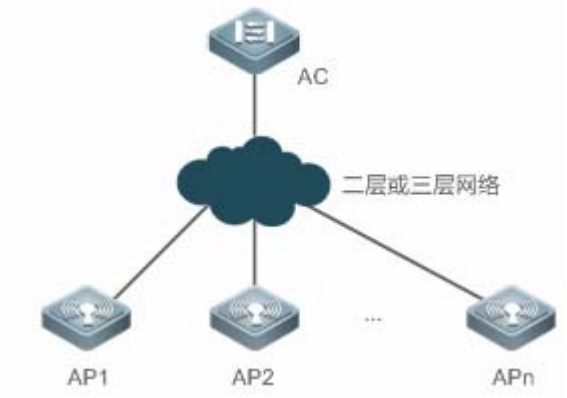
检验方法

- 通过 **show running** 命令可以查看无线用户 VLAN 内的二层隔离的配置信息。

配置举例

配置无线用户 VLAN 内的二层隔离

【网络环境】
图 1-5



【配置方法】
- 在 AC 设备上启用 AP 下基于 WLAN 的用户隔离；
- 在 AC 设备上启用 AP 下用户隔离；
- 在 AC 设备上启用 AC 下基于 WLAN 的用户隔离；
- 在 AC 设备上启用 AC 下用户隔离。

AC

```
Ruijie#configure terminal
Ruijie(config)#wids
Ruijie(config-wids)#user-isolation ssid-ap enable
```

```
Ruijie(config-wids)#user-isolation ap enable
Ruijie(config-wids)#user-isolation ssid-ac enable
Ruijie(config-wids)#user-isolation ac enable
```

【检验方法】 用户配置无线用户 VLAN 内的二层隔离后，通过显示无线用户 VLAN 内的二层隔离配置信息进行检验。

- 通过 **show running** 命令可以查看无线用户 VLAN 内的二层隔离的配置信息。

```
Ruijie#show running
!
wids
 user-isolation ap enable
 user-isolation ac enable
 user-isolation ssid-ac enable
 user-isolation ssid-ap enable
!
```

常见错误

无。

1.5.4 配置无线用户限速

配置效果

- 为了使有限的网络资源能够更好地发挥效用，更好地为更多的用户服务，设备需要支持流量限速功能。当数据流量符合承诺速率时，允许数据包通过；数据流量不符合承诺速率时，丢弃数据包。

注意事项

- 当数据流量不符合承诺速率时，丢弃数据包。

配置方法

↘ 配置基于 AP 的限速

- 可选配置，使用 **ap-based** 命令可以配置基于 AP 的限速。
- 若无特殊要求，应在 AC 设备的 AP 配置模式下配置。
- 速率值越大，无线用户可用的传输速率越大。

【命令格式】 **ap-based { per-user-limit | total-user-limit } { up-streams | down-streams } average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*

【参数说明】 **per-user-limit**：指定对 AP 上的每个用户进行限速。
total-user-limit：指定对整个 AP 进行限速。
up-streams：指定对上行流量进行限速。
down-streams：指定对下行流量进行限速。
average-data-rate：指定平均速率限制，单位为 8Kbps，范围为 8-261120。
burst-data-rate：指定突发速率限制，单位为 8Kbps，范围为 8-261120。

【缺省配置】 禁用基于 AP 的限速

【命令模式】 AP 配置模式

【使用指导】 -

配置基于 Client 的限速

- 可选配置，使用 **netuser** 命令可以配置基于 Client 的限速。
- 若无特殊要求，应在 AC 设备的 AC 配置模式下配置。
- 速率值越大，无线用户可用的传输速率越大。

【命令格式】 **netuser** *mac-address* **{ inbound | outbound } average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*

【参数说明】 *mac-address*：指定用户的 MAC 地址。
inbound：指定对上行流量进行限速。
outbound：指定对下行流量进行限速。
average-data-rate：指定平均速率限制，单位为 8Kbps，范围为 8-261120。
burst-data-rate：指定突发速率限制，单位为 8Kbps，范围为 8-261120。

【缺省配置】 禁用基于 Client 的限速

【命令模式】 AC 配置模式

【使用指导】 -

配置基于 WLAN 的限速

- 可选配置，使用 **wlan-based** 命令可以配置基于 WLAN 的限速。
- 若无特殊要求，应在 AC 设备的 WLAN 配置模式下配置。
- 速率值越大，无线用户可用的传输速率越大。

【命令格式】 **wlan-based { per-user-limit | total-user-limit | per-ap-limit } { up-streams | down-streams } average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*

【参数说明】 **per-user-limit**：指定对 WLAN 上的每个用户进行限速。
total-user-limit：指定对整个 WLAN 进行限速。
per-ap-limit：指定对所有的 AP 各自进行整个 WLAN 的限速。
up-streams：指定对上行流量进行限速。
down-streams：指定对下行流量进行限速。
average-data-rate：指定平均速率限制，单位为 8Kbps，范围为 8-261120。
burst-data-rate：指定突发速率限制，单位为 8Kbps，范围为 8-261120。

【缺省配置】 禁用基于 WLAN 的限速

【命令模式】 WLAN 配置模式

【使用指导】 -

检验方法

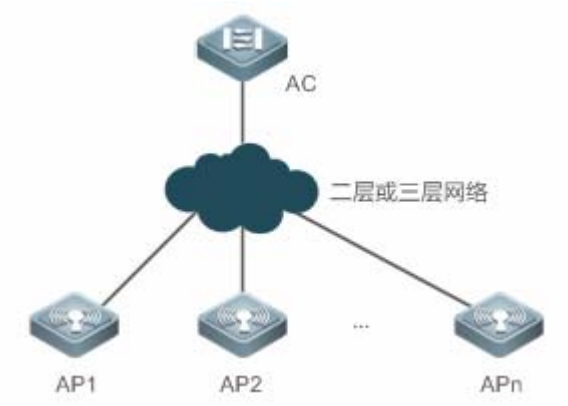
- 通过 **show running** 命令可以查看无线用户限速的配置信息。

配置举例

配置无线用户限速

【网络环境】

图 1-6



【配置方法】

- 在 AC 设备上限制 AP1 上的每个用户的上行最大平均速率为 256Kbps ,上行最大突发速率为 1024Kbps；
- 在 AC 设备上限制 AC 上的无线用户 14cf.920b.bfce 的上行最大平均速率为 256Kbps，上行最大突发速率为 1024Kbps；
- 在 AC 设备上限制 WLAN 12 上的每个用户的上行最大平均速率为 256Kbps，上行最大突发速率为 1024Kbps。

```
Ruijie#configure terminal
Ruijie(config)#ap-config AP1
Ruijie(config-ap)#ap-based per-user-limit up-streams average-data-rate 256 burst-data-rate 1024
Ruijie(config-ap)#end
Ruijie#configure terminal
Ruijie(config)#ac-controller
Ruijie(config-ac)#netuser 14cf.920b.bfce inbound average-data-rate 256 burst-data-rate 1024
Ruijie(config-ap)#end
Ruijie#configure terminal
Ruijie(config)#wlan-config 12
Ruijie(config-wlan)#wlan-based per-user-limit up-streams average-data-rate 256 burst-data-rate
1024
```

【检验方法】 用户配置无线用户限速后，通过显示无线用户限速配置信息进行检验。

- 通过 **show running** 命令可以查看无线用户限速的配置信息。

```
Ruijie#show ap-config running AP1
!
ap-config AP1
 ap-based per-user-limit up-streams average-data-rate 256 burst-data-rate 1024
 no 11acsupport enable radio 1
 no 11acsupport enable radio 2
 802.11n mcs support 15 radio 1
 802.11n mcs support 15 radio 2
 antenna receive 3 radio 1
 antenna receive 3 radio 2
 antenna transmit 3 radio 1
 antenna transmit 3 radio 2
 radio-type 1 802.11b
 radio-type 2 802.11a
 beacon period 300 radio 1
 beacon period 100 radio 2
 ap-mac 001a.a9c5.3f49
 no enable-radio 1
 no enable-radio 2
!
Ruijie#show running
!
wlan-config 12 wlan_opt
 wlan-based per-user-limit up-streams average-data-rate 256 burst-data-rate 1024
 enable-broad-ssid
!
!
ac-controller
 netuser 14cf.920b.bfce inbound average-data-rate 256 burst-data-rate 1024
 country CN
 country US
 802.11g network rate 1 disabled
 802.11g network rate 2 disabled
 802.11g network rate 5 disabled
 802.11g network rate 11 mandatory
 802.11g network rate 6 supported
 802.11g network rate 9 supported
 802.11g network rate 12 supported
 802.11g network rate 18 supported
 802.11g network rate 24 supported
```

```
802.11g network rate 36 supported
802.11g network rate 48 supported
802.11g network rate 54 supported
802.11b network rate 1 disabled
802.11b network rate 2 disabled
802.11b network rate 5 mandatory
802.11b network rate 11 mandatory
802.11a network rate 6 disabled
802.11a network rate 9 supported
802.11a network rate 12 mandatory
802.11a network rate 18 supported
802.11a network rate 24 mandatory
802.11a network rate 36 supported
802.11a network rate 48 supported
802.11a network rate 54 supported
!
```

常见错误

无。

1.5.5 配置RTS/CTS保护机制

配置效果

- 当同频干扰存在时，RTS 阈值越小，抗干扰能力越强；但是 RTS/CTS 报文越多，即控制报文的信道占用率越多，无线用户可用的信道带宽越少 ;用户可以设置 RTS Threshold 来指定发送数据的帧长度 ,如果工作站发送数据的帧长度小于 RTS Threshold 设置的门限，将不执行 RTS/CTS 握手。

注意事项

- 无。

配置方法

↘ 配置 RTS 阈值

- 可选配置，使用 **rts threshold** 命令可以配置 RTS 阈值。
- 若无特殊要求，应在 AC 设备的 AP 配置模式下配置。

- 当同频干扰存在时，RTS 阈值越小，抗干扰能力越强；但是 RTS/CTS 报文越多，即控制报文的信道占用率越多，无线用户可用的信道带宽越少。

【命令格式】 **rts-threshold** *value* **radio** *radio-id*

【参数说明】 *value*：指定 RTS 阈值，单位字节，范围 257~2347

radio-id：指定射频口索引，范围为 1~16

【缺省配置】 2347 字节

【命令模式】 AP 配置模式

【使用指导】 -

检验方法

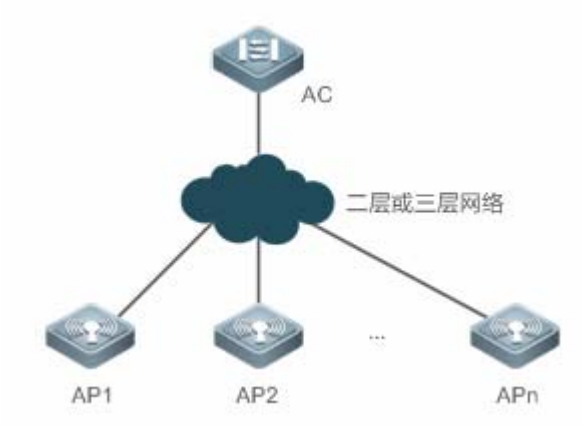
- 通过 **show ap-config running** 命令可以查看 RTS 阈值的配置信息。

配置举例

配置 RTS 阈值

【网络环境】

图 1-7



【配置方法】 ● 在 AC 设备上配置 AP1 Radio1 的 RTS 阈值为 800 字节。

AC

```
Ruijie#configure terminal
Ruijie(config)#ap-config AP1
Ruijie(config-ap)#rts-threshold 800 radio 1
```

【检验方法】 用户配置 RTS 阈值后，通过显示 RTS 阈值配置信息进行检验。

- 通过 show ap-config running 命令可以查看 RTS 阈值的配置信息。

```
Ruijie#show ap-config running AP1
!
ap-config AP1
 ap-based per-user-limit up-streams average-data-rate 256 burst-data-rate 1024
 no 11acsupport enable radio 1
```

```
no 11acsupport enable radio 2
802.11n mcs support 15 radio 1
802.11n mcs support 15 radio 2
rts-threshold 800 radio 1
antenna receive 3 radio 1
antenna receive 3 radio 2
antenna transmit 3 radio 1
antenna transmit 3 radio 2
radio-type 1 802.11b
radio-type 2 802.11a
beacon period 300 radio 1
beacon period 100 radio 2
ap-mac 001a.a9c5.3f49
no enable-radio 1
no enable-radio 2
!
```

常见错误

无。

1.5.6 配置EDCA参数

配置效果

- 实际配置中可根据应用需求选择配置 Client 端或者 AP 端的 EDCA 参数。配置 Client 端 EDCA 参数影响下行数据流量，配置 AP 使用的 EDCA 参数影响上行数据流量。

注意事项

- 无。

配置方法

↘ 配置 Client 端的 EDCA 参数

- 可选配置，使用 **wmm edca-client** 命令可以配置 Client 端的 EDCA 参数。若无特殊要求，应在 AC 设备的 AP 配置模式下配置。

- AIFS 越小，可以越早地进行退避过程，接入信道的能力越强。CWmin 和 Cwmax 越小，由 CWmin 和 CWmax 决定的退避时间越小，可以更早地结束退避过程，接入信道的能力越强。TXOP limit 越大，在竞争到传输机会后使用 SIFS 间隔连续传输的报文越多；增大 TXOP limit 可以在一定程度上降低报文冲突概率和减少空口资源浪费。

【命令格式】 **wmm edca-client** { **back-ground** | **best-effort** | **video** | **voice** } { **aifsn** [*aifsn-value*] **cwmin** [*cwmin-value*] **cwmax** [*cwmax-value*] **txop** [*txop-value*] | **length** [*queue-length*] } **radio** [*radio-id*]

【参数说明】 **back-ground**：表示将设置 back-ground 队列。

best-effort：表示将设置 best-effort 队列。

video：表示将设置 video 队列。

voice：表示将设置 voice 队列。

aifsn-value：表示设置 aifsn 值，范围为 1-15。

cwmin-value：表示设置 cwmin 值，范围为 0-15。

cwmax-value：表示设置 cwmax 值，范围为 0-15。

txop-value：表示设置 txop 值，范围为 0-255，单位为 32 微秒。

queue-length：表示设置 AC 队列长度，范围为 1-768。默认为最大值。

radio-id：表示选择设置客户端 EDCA 参数的 radio，范围为 1~16。

【缺省配置】

AC	AIFS	CWmin	CWmax	TXOP
back-ground	7	4	10	0
best-effort	3	4	10	0
video	2	3	4 94	
voice	2	2	3 47	

【命令模式】 AP 配置模式

【使用指导】 wmm 服务开启时，配置的参数才能生效。

cwmax 值必须大于 cwmin 值，否则提示配置失败。

配置 AP 端的 EDCA 参数

- 可选配置，使用 **wmm edca-radio** 命令可以配置 AP 端的 EDCA 参数。
- 若无特殊要求，应在 AC 设备的 AP 配置模式下配置。
- AIFS 越小，可以越早地进行退避过程，接入信道的能力越强。CWmin 和 Cwmax 越小，由 CWmin 和 CWmax 决定的退避时间越小，可以更早地结束退避过程，接入信道的能力越强。TXOP limit 越大，在竞争到传输机会后使用 SIFS 间隔连续传输的报文越多；增大 TXOP limit 可以在一定程度上降低报文冲突概率和减少空口资源浪费。

【命令格式】 **wmm edca-radio** { **back-ground** | **best-effort** | **video** | **voice** } { **aifsn** [*aifsn-value*] **cwmin** [*cwmin-value*] **cwmax** [*cwmax-value*] **txop** [*txop-value*] | **noack** } **radio** [*radio-id*]

【参数说明】 **back-ground**：表示将设置 back-ground 队列。

best-effort：表示将设置 best-effort 队列。

video：表示将设置 video 队列。

voice：表示将设置 voice 队列。

aifsn-value：表示设置 aifsn 值，范围为 1-15。

cwmin-value：表示设置 cwmin 值，范围为 0-15。

cwmax-value：表示设置 cwmax 值，范围为 0-15。

txop-value：表示设置 txop 值，范围为 0-255，单位为 32 微秒。

noack：表示开启 no ack 策略。默认不开启 no ack 策略。

radio-id：表示选择设置客户端 EDCA 参数的 radio，范围为 1-2。

【缺省配置】

AC	AIFS	CWmin	CWmax	TXOP
back-ground	7	4	10	0
best-effort	3	4	6 0	
video	1	3	4 94	
voice	1	2	3 47	

【命令模式】 AP 配置模式

【使用指导】 wmm 服务开启时，配置的参数才能生效。

cwmax 值必须大于 cwmin 值，否则提示配置失败。

检验方法

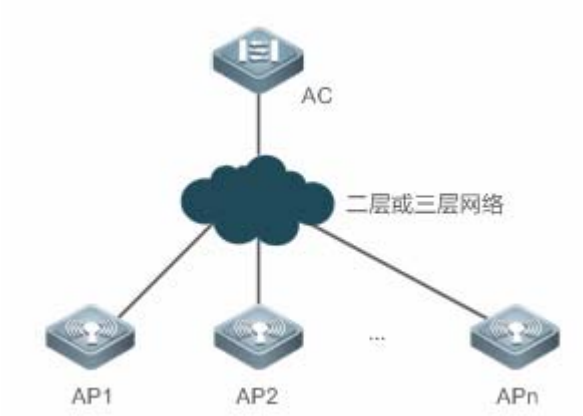
- 通过 **show ap-config running** 命令可以查看 EDCA 参数的配置信息。

配置举例

配置 EDCA 参数

【网络环境】

图 1-8



【配置方法】

- 在 AC 设备上配置 AP1 Radio1 的 Client 端的 EDCA 参数；
- 在 AC 设备上配置 AP1 Radio1 的 AP 端的 EDCA 参数。

AC

```
Ruijie#configure terminal
Ruijie(config)#ap-config AP1
Ruijie(config-ap)#wmm edca-client voice aifsn 2 cwmin 2 cwmax 3 txop 50 radio 1
Ruijie(config-ap)#wmm edca-radio voice aifsn 1 cwmin 1 cwmax 3 txop 50 radio 1
```

【检验方法】 用户配置 EDCA 参数后，通过显示 EDCA 参数配置信息进行检验。

- 通过 **show ap-config running** 命令可以查看 EDCA 参数的配置信息。

```
Ruijie#show ap-config running AP1
!
ap-config AP1
```

```
wmm edca-client voice aifsn 2 cwmin 2 cwmax 3 txop 50 radio 1
wmm edca-radio voice aifsn 1 cwmin 1 cwmax 3 txop 50 radio 1
no 11acsupport enable radio 1
no 11acsupport enable radio 2
802.11n mcs support 15 radio 1
802.11n mcs support 15 radio 2
antenna receive 3 radio 1
antenna receive 3 radio 2
antenna transmit 3 radio 1
antenna transmit 3 radio 2
radio-type 1 802.11b
radio-type 2 802.11a
beacon period 300 radio 1
beacon period 100 radio 2
ap-mac 001a.a9c5.3f49
no enable-radio 1
no enable-radio 2
!
```

常见错误

无。

1.5.7 配置允许接入信号强度

配置效果

- 通过控制 AP 广播 Beacon 帧的范围，减少远距离的无线用户接入；通过限制无线用户的 RSSI（接收信号强度指示）的最小值，当接收到无线用户的请求帧的 RSSI 小于这个值，则不允许该无线用户接入。

注意事项

- 无线用户接入最小 RSSI 不能太大，否则可能导致大量无线用户无法接入。
- 管理帧发送功率不能太大，否则可能导致大量距离较远无线用户无法发现网络。

配置方法

↘ 配置无线用户接入最小 RSSI

- 可选配置，使用 **response-rssi** 命令可以配置无线用户接入最小 RSSI。

- 若无特殊要求，应在 AC 设备的 AP 配置模式下配置。
- 无线用户接入最小 RSSI 越小，可以允许接入的无线用户的 RSSI 就越小，往往表示允许接入的无线用户距离 FAT-AP 的距离就越远。

【命令格式】 **response-rssi** *rssi* **radio** *radio-id*
【参数说明】 *rssi*：指定无线用户接入最小 RSSI，单位：dB，范围：0~100。
radio-id：指定要配置的 radio 的 id，范围为 1~16。
【缺省配置】 最小 RSSI 为 0，即不管无线用户的 RSSI 大小都允许接入
【命令模式】 AP 配置模式
【使用指导】 -

配置管理帧发送功率

- 可选配置，使用 **coverage-area-control** 命令可以配置管理帧发送功率。
- 若无特殊要求，应在 AC 设备的 AP 配置模式下配置。
- 管理帧发送功率越大(0 除外),FAT-AP 的无线用户范围越大 ,往往表示允许接入的无线用户距离 FAT-AP 的距离就越远。

【命令格式】 **coverage-area-control** *power*
【参数说明】 *power*：指定管理帧发送功率，单位：dBm，范围：0~32。
【缺省配置】 0
【命令模式】 AP 配置模式
【使用指导】 -

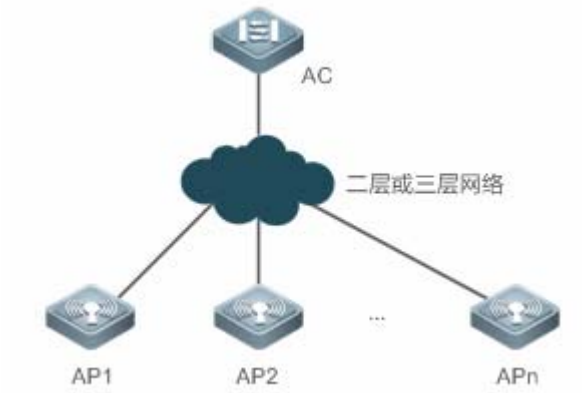
检验方法

- 通过 **show ap-config running** 命令可以查看允许接入信号强度的配置信息。

配置举例

配置允许接入信号强度

【网络环境】
图 1-9



【配置方法】
- 在 AC 设备上配置 AP1 Radio1 的无线用户接入最小 RSSI 为 20dB；
- 在 AC 设备上配置 AP1 Radio1 的管理帧发送功率为 30dBm。

AC

```
Ruijie#configure terminal
Ruijie(config)#ap-config AP1
Ruijie(config-ap)#response-rssi 20 radio 1
Ruijie(config-ap)#coverage-area-control 30
```

【检验方法】 用户配置允许接入信号强度后，通过显示允许接入信号强度配置信息进行检验。

- 通过 **show ap-config running** 命令可以查看允许接入信号强度的配置信息。

```
Ruijie#show ap-config running AP1
!
ap-config AP1
 ap-based per-user-limit up-streams average-data-rate 256 burst-data-rate 1024
 no 11acsupport enable radio 1
 no 11acsupport enable radio 2
 802.11n mcs support 15 radio 1
 802.11n mcs support 15 radio 2
 rts-threshold 800 radio 1
 coverage-area-control 30
 response-rssi 20 radio 1
 antenna receive 3 radio 1
 antenna receive 3 radio 2
 antenna transmit 3 radio 1
 antenna transmit 3 radio 2
 radio-type 1 802.11b
 radio-type 2 802.11a
 beacon period 300 radio 1
 beacon period 100 radio 2
 ap-mac 001a.a9c5.3f49
 no enable-radio 1
 no enable-radio 2
!
```

常见错误

无。

1.5.8 配置AP允许接入用户数

配置效果

- 通过限制 AP 下的 STA 接入数目，可以起到一定的负载分担功能，避免 AP 接入用户分配不均。。

注意事项

- 无。

配置方法

配置基于 AP 的 STA 数量限制

- 可选配置，使用 **sta-limit** 命令可以配置基于 AP 的 STA 数量限制。
- 若无特殊要求，应在 AC 设备的 AP 配置模式下配置。
- 基于 AP 的 STA 数量限制越大，可以接入的 STA 越多。

【命令格式】 **sta-limit** *max-num*
【参数说明】 *max-num*：指定基于 AP 的 STA 数量限制，范围 1~32
【缺省配置】 *32*
【命令模式】 AP 配置模式
【使用指导】 -

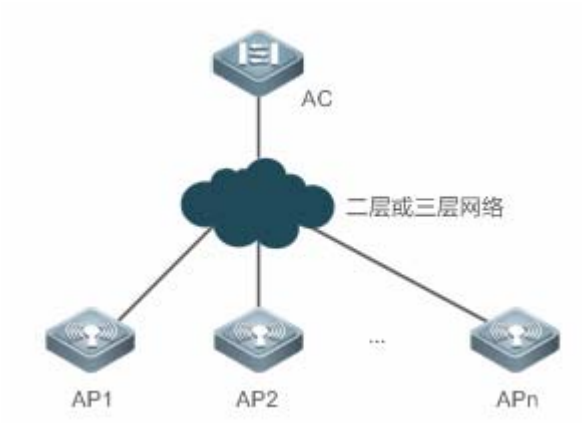
检验方法

- 通过 **show ap-config running** 命令可以查看基于 AP 的 STA 数量限制的配置信息。

配置举例

配置基于 AP 的 STA 数量限制

【网络环境】
图 1-10



【配置方法】
- 在 AC 设备上配置 AP1 的允许接入用户数为 12。

AC

```
Ruijie#configure terminal
```

```
Ruijie(config)#ap-config AP1
Ruijie(config-ap)#sta-limit 12
```

【检验方法】 用户配置 AP 允许接入用户数后，通过显示 AP 允许接入用户数配置信息进行检验。

- 通过 **show ap-config running** 命令可以查看 AP 允许接入用户数的配置信息。

```
Ruijie#show ap-config running AP1
!
ap-config AP1
 ap-based per-user-limit up-streams average-data-rate 256 burst-data-rate 1024
 no 11acsupport enable radio 1
 no 11acsupport enable radio 2
 802.11n mcs support 15 radio 1
 802.11n mcs support 15 radio 2
 rts-threshold 800 radio 1
 coverage-area-control 30
 response-rssi 20 radio 1
 antenna receive 3 radio 1
 antenna receive 3 radio 2
 antenna transmit 3 radio 1
 antenna transmit 3 radio 2
 radio-type 1 802.11b
 radio-type 2 802.11a
 sta-limit 12
 beacon period 300 radio 1
 beacon period 100 radio 2
 ap-mac 001a.a9c5.3f49
 no enable-radio 1
 no enable-radio 2
!
```

常见错误

无。

1.5.9 配置纯 11n网络

配置效果

- 通过配置纯 11n 网络，禁止非 11n 设备接入，使网络的 11n 设备均采用纯 HT 头部传输，减小报文头部尺寸，无线用户可用的信道带宽增加。

注意事项

- 纯 11n 网络，非 11n 设备无法接入。

配置方法

配置是否支持 11a

- 可选配置，使用 **11asupport enable** 命令可以配置是否支持 11a。
- 该配置仅在 AP 的 Radio 工作于 5G 下生效。
- 如果支持 11a，11a 的 STA 可以接入，否则不允许 11a 的 STA 接入。

【命令格式】 **11asupport enable radio** *radio-id*
【参数说明】 *radio-id*：指定要配置的 radio 的 id，范围为 1~16。
【缺省配置】 支持 11a 的 STA 接入
【命令模式】 AP 配置模式
【使用指导】 配置仅在 AP 的 Radio 工作在 5G 下生效。
不支持对所有 AP 进行配置。

配置是否支持 11b

- 可选配置，使用 **11bsupport enable** 命令可以配置是否支持 11b。
- 该配置仅在 AP 的 Radio 工作于 2.4G 下生效。
- 如果支持 11b，11b 的 STA 可以接入，否则不允许 11b 的 STA 接入。

【命令格式】 **11bsupport enable radio** *radio-id*
【参数说明】 *radio-id*：指定要配置的 radio 的 id，范围为 1~16。
【缺省配置】 支持 11b 用户接入
【命令模式】 AP 配置模式
【使用指导】 配置仅在 AP 的 Radio 工作在 2.4G 下生效。
不支持对所有 AP 进行配置。

配置是否支持 11g

- 可选配置，使用 **11gsupport enable** 命令可以配置是否支持 11g。
- 该配置仅在 AP 的 Radio 工作于 2.4G 下生效。
- 如果支持 11g，11g 的 STA 可以接入，否则不允许 11g 的 STA 接入。

【命令格式】 **11gsupport enable radio** *radio-id*
【参数说明】 *radio-id*：指定要配置的 radio 的 id，范围为 1~16。
【缺省配置】 支持 11g 用户接入
【命令模式】 AP 配置模式
【使用指导】 配置仅在 AP 的 Radio 工作在 2.4G 下生效。

不支持对所有 AP 进行配置。

配置是否支持 11na

- 可选配置，使用 **11nasupport enable** 命令可以配置 5GHz 下是否支持 11n。
- 该配置仅在 AP 的 Radio 工作于 5G 下生效。
- 如果 5GHz 下支持 11n，11n 的 STA 可以接入，否则不允许 11n 的 STA 接入。

【命令格式】 **11nasupport enable radio** *radio-id*
【参数说明】 *radio-id*：指定要配置的 radio 的 id，范围为 1~16。
【缺省配置】 在 5G 下支持 11n 用户接入
【命令模式】 AP 配置模式
【使用指导】 配置仅在 AP 的 Radio 工作在 5G 下生效。
不支持对所有 AP 进行配置。

配置是否支持 11ng

- 可选配置，使用 **11ngsupport enable** 命令可以配置 2.4GHz 下是否支持 11n。
- 该配置仅在 AP 的 Radio 工作于 2.4G 下生效。
- 如果 2.4GHz 下支持 11n，11n 的 STA 可以接入，否则不允许 11n 的 STA 接入。

【命令格式】 **11ngsupport enable radio** *radio-id*
【参数说明】 *radio-id*：指定要配置的 radio 的 id，范围为 1~16。
【缺省配置】 在 2.4G 下支持 11n 用户接入
【命令模式】 AP 配置模式
【使用指导】 配置仅在 AP 的 Radio 工作在 2.4G 下生效。
不支持对所有 AP 进行配置。

检验方法

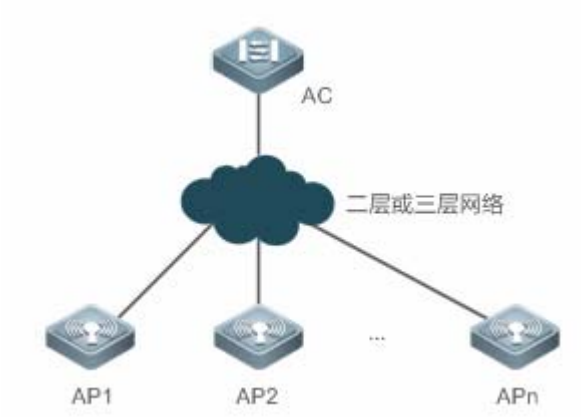
- 通过 **show ap-config radio** 命令可以查看纯 11n 网络的配置信息。

配置举例

配置纯 11n 网络

【网络环境】

图 1-11



- AP1 Radio1 工作在 2.4G。
- AP1 Radio2 工作在 5.8G。

【配置方法】

- 在 AC 设备上配置 AP1 Radio1 为纯 11n 网络；
- 在 AC 设备上配置 AP1 Radio2 为纯 11n 网络。

AC

```
Ruijie#configure terminal
Ruijie(config)#ap-config AP1
Ruijie(config-ap)#no 11bsupport enable radio 1
Ruijie(config-ap)#no 11gsupport enable radio 1
Ruijie(config-ap)#11ngsupport enable radio 1
Ruijie(config-ap)#no 11asupport enable radio 2
Ruijie(config-ap)#11nasupport enable radio 2
```

【检验方法】 用户配置纯 11n 网络后，通过显示纯 11n 网络配置信息进行检验。

- 通过 **show ap-config running** 命令可以查看纯 11n 网络的配置信息。

```
Ruijie#show ap-config running AP1
!
ap-config AP1
 ap-based per-user-limit up-streams average-data-rate 256 burst-data-rate 1024
 no 11asupport enable radio 2
 no 11bsupport enable radio 1
 no 11gsupport enable radio 1
 no 11acsupport enable radio 1
 no 11acsupport enable radio 2
 802.11n mcs support 15 radio 1
 802.11n mcs support 15 radio 2
 rts-threshold 800 radio 1
 coverage-area-control 30
 response-rssi 20 radio 1
 antenna receive 3 radio 1
```

```
antenna receive 3 radio 2
antenna transmit 3 radio 1
antenna transmit 3 radio 2
radio-type 1 802.11b
radio-type 2 802.11a
sta-limit 12
beacon period 300 radio 1
beacon period 100 radio 2
ap-mac 001a.a9c5.3f49
no enable-radio 1
no enable-radio 2
!
```

常见错误

无。

1.5.10 配置频谱导航

配置效果

- 开启 WLAN 的频谱导航功能，引导双频 STA 接入 5G 频段

注意事项

- 无。

配置方法

↘ 开启 WLAN 的频谱导航功能

- 必须配置。
- 若无特殊要求，在 AC 或者胖 AP 上打开。

【命令格式】 **band-select enable**
【参数说明】 **-**
【缺省配置】 关闭频谱导航功能
【命令模式】 WLAN 配置模式
【使用指导】 -

↘ 配置频谱导航可以接受的 STA 信号强度下限

- 可选配置，在需要调整频谱导航覆盖范围时进行配置。使用 **band-select acceptable-rssi** 命令可以配置频谱导航可以接受的 STA 信号强度下限，取值范围 [-100，-50]。
- 若无特殊要求，在 AC 或者胖 AP 上打开。
- 该限值越高，频谱导航的覆盖范围越小；该限值越低，频谱导航的覆盖范围越大；但是，如果超过了可以正常使用的限制，会导致接入的 STA 信号过弱，拖慢整网的连接速率。

【命令格式】 **band-select acceptable-rssi** *value*
【参数说明】 *value*：频谱导航可以接受的 STA RSSI 下限，范围[-100，-50]，单位 dBm。
【缺省配置】 频谱导航可以接受的 STA 信号强度下限为-80 dBm
【命令模式】 全局模式
【使用指导】 -

配置拒绝双频 STA 接入 2.4G 频段的次数

- 可选配置，在需要拒绝双频 STA 接入 2.4G 频段时配置；如果配置后出现较多双频 STA 接入时间过长或无法接入，要配置较小的值或去掉配置。
- 若无特殊要求，在 AC 或者胖 AP 上打开。

【命令格式】 **band-select access-denial** *value*
【参数说明】 *value*：拒绝双频 STA 接入 2.4G 频段的次数，范围[0，10]。
【缺省配置】 0
【命令模式】 全局模式
【使用指导】 -

配置 STA 信息的老化时间

- 可选配置，如果环境中没有双频 STA 切换成单频 2.4G STA 的情况，可以配置较大的老化周期，反之，配置较小的老化周期；如果不确定，使用默认配置即可。
- 若无特殊要求，在 AC 或者胖 AP 上打开。
- 使用 **band-select age-out** 命令可以调整 STA 信息的老化时间。双频 STA 信息老化时间取值范围为 [20，120] 秒；抑制 STA 信息老化时间取值范围为 [10，60] 秒。
- STA 信息老化时间越大，STA 的信息生命周期越长，AP 对 STA 的频段切换越不敏感。STA 信息老化时间越小，STA 的信息生命周期越短，AP 对 STA 的频段切换越敏感。

【命令格式】 **band-select age-out** { **dual-band** *value* **| suppression** *value* }
【参数说明】 **dual-band** *value*：双频 STA 信息的老化时间，范围[20，120]，单位秒。
suppression *value*：抑制 STA 信息的老化时间，范围[10，60]，单位秒。
【缺省配置】 双频 STA 信息老化时间为 60 秒；抑制 STA 信息老化时间为 20 秒
【命令模式】 全局模式
【使用指导】 推荐双频 STA 的信息老化时间配置为抑制 STA 的信息老化时间的两倍到三倍。

配置抑制 STA 的探测周期计数值

- 可选配置，如果出现单频 2.4G STA 长时间发现不了 WLAN 的情况，那么应该减小该配置。

- 若无特殊要求，在 AC 或者胖 AP 上打开。

【命令格式】 **band-select probe-count** *value*
【参数说明】 *value*：抑制 STA 的探测周期计数值，范围[1，10]。
【缺省配置】 2
【命令模式】 全局模式
【使用指导】 -

配置 STA 探测扫描周期门限

- 可选配置，如果出现单频 2.4G STA 长时间发现不了 WLAN 的情况，那么应该减小该配置；如果不确定，使用默认配置即可。
- 若无特殊要求，在 AC 或者胖 AP 上打开。

【命令格式】 **band-select scan-cycle** *value*
【参数说明】 *value*：STA 探测扫描周期门限，范围[1，1000]，单位毫秒。
【缺省配置】 200
【命令模式】 全局模式
【使用指导】 -

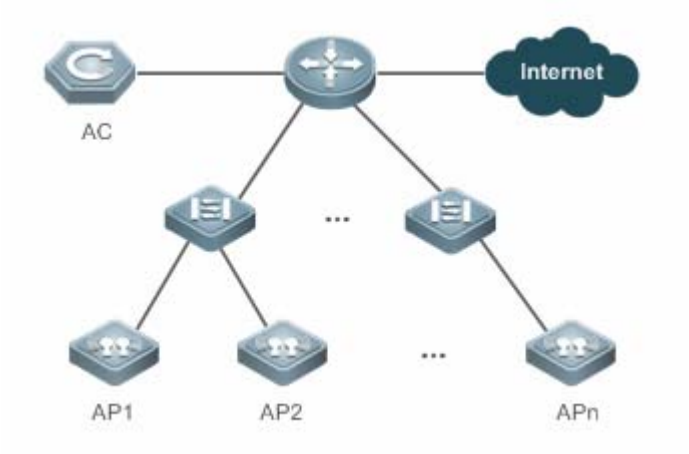
检验方法

- 使用 **show band-select configuration** 命令查看设备上的频谱导航参数配置。
- 使用 **show running-config** 命令查看 WLAN 配置是否打开了频谱导航功能。
- 运行一段时间后，使用 **show band-select statistics** 命令查看设备上的运行统计值。
- 抓包确认频谱导航是否控制了主动探测过程。

配置举例

瘦 AP 架构，配置 WLAN 的频谱导航

【网络环境】
图 1-12



如上图，典型瘦 AP 架构无线网络。

- AC 为无线接入控制器。
- AP1、AP2、.....、APn 都是双频 AP。
- AC 和 AP 通过二层交换设备和三层路由设备连接。
- 要开启频谱导航的 WLAN 为 WLAN 99，SSID“wlan-bandselect”，映射到所有双频 AP 的两个射频接口上。

【配置方法】

- 在 AC 上配置频谱导航运行参数（可选）。
- 在 AC 上开启 WLAN 99 的频谱导航功能。

AC

```
AC# configure terminal
AC(config)# wlan-config 99
AC(config-wlan)# band-select enable
```

【检验方法】 使用双频 STA 接入 WLAN“wlan-bandselect”。

- STA 接入 5G 频段。（也有可能出现导航失败，STA 接入 2.4G 频段）
- 检查 AC 上频谱导航运行统计值，应该出现计数增加。

AC

```
A# show band-select statistics
Band Select Statistics
  Number of dual band client.............................. 1
  Number of dual band client added........................ 1
  Number of dual band client expired...................... 0
  Number of suppressed client............................. 0
  Number of suppressed client added....................... 0
  Number of suppressed client expired..................... 0
```

常见错误

- 频谱导航运行参数配置不合适。
- 频谱导航功能没有打开。
- 双频 AP 的两个射频接口被关闭了一个。

1.5.11 配置一键网优

配置效果

- 提升网络性能

注意事项

- 无。

配置方法

配置网优选择优化项

- 可选配置。
- 若无特殊要求，在 AC 上打开。
- 使用 **wopt choose** 命令可以配置网优选择优化项，至少选择一项，也可多选。
- 网优选择优化项通过优化网络配置以提升网络性能。用户可根据建议配置和实际网络情况，来选择优化项。网优不支持 no 命令来还原优化前的配置，若是配置错了，可到相应模式下修订配置。

【命令格式】 **wopt choose** { **band-select-disable** | **band-select-enable** | **low-rate-disable** | **multicast-speed** | **rrm-disable** | **rrm-enable** | **session-limit** | **speed-limit** }

【参数说明】 **band-select-disable**：关闭 5G 优先（环境中只有少数 5G 终端时，建议关闭 5G 优先）
band-select-enable：开启 5G 优先（环境中有较多 5G 终端时，建议开启 5G 优先）
low-rate-disable：禁用低速（禁用小于 11Mbps 的速率）
multicast-speed：恢复默认组播速率（使用默认的组播速率 24Mbps）
rrm-disable：关闭 RRM（环境中无同频、邻频干扰时，建议关闭 RRM）
rrm-enable：开启 RRM（环境中有同频、邻频干扰时，建议开启 RRM，进行一次信道、功率调整）
session-limit：恢复默认会话数（会话数影响 iportal 推送认证界面，建议使用默认会话数（单个 STA 255，单个 port 1000））
speed-limit：限速(基于 WLAN 对所有用户限速，上/下行平均速率 256KB，突发速率 300KB)

【缺省配置】 -

【命令模式】 全局配置模式

【使用指导】 根据实际环境需要，选择网优项。
由于不支持还原网优前的配置，请慎重选择网优项。若优化错了配置，可手动在相关配置模式下，修改配置。

配置一键网优

- 可选配置。
- 若无特殊要求，在 AC 上打开。
- 使用 **wopt enable** 命令可以配置一键网优。
- 一键网优通过优化网络配置以提升网络性能。网优不支持 no 命令来还原优化前的配置，若是配置错了，可到相应模式下修订配置。

【命令格式】 **wopt enable**

【参数说明】 -

【缺省配置】 -

【命令模式】 全局配置模式

【使用指导】 若是实际环境需要优化禁用低速、恢复各 WLAN 的组播速率、恢复默认会话数、对各 WLAN 进行限速[上下行平均 256KB，突发 300KB]，则可配置一键网优。

~ 注意 由于不支持还原网优前的配置，请慎重使用。若优化错了配置，可手动在相关配置模式下，修改配置。

检验方法

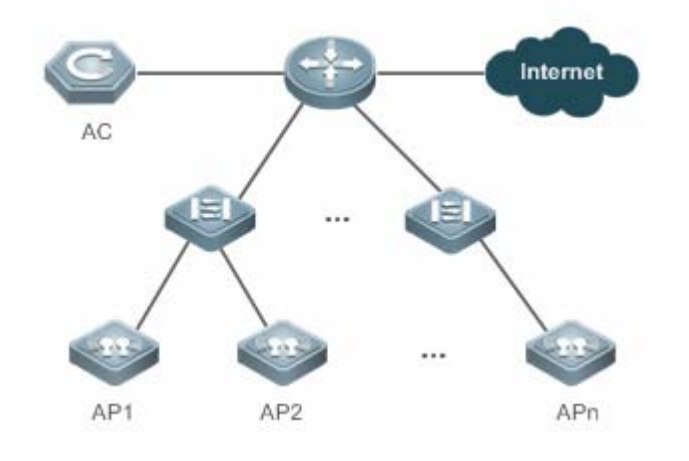
- 使用 **show wopt** 命令网优信息。

配置举例

↘ 瘦 AP 架构，配置网优选择优化项

【网络环境】

图 1-13



如上图，典型瘦 AP 架构无线网络。

- AC 为无线接入控制器。
- AP1、AP2、.....、APn 都是双频 AP。
- AC 和 AP 通过二层交换设备和三层路由设备连接。
- 环境中有较多 5G 终端时，建议开启 5G 优先，即开启频谱导航。
- 禁用低速率

【配置方法】

- 在 AC 上配置网优选择优化项。

AC

```
AC# configure terminal
AC(config)# wopt choose band-select-enable low-rate-disable
```

【检验方法】

用户配置网优选择优化项后，通过显示网优信息进行检验。

- 通过 **show wopt** 命令可以显示网优信息。

AC

```
AC# show wopt

Low rate status:
 802.11b rate:
    1 Mbps: Disable
```

```
    2 Mbps: Disable
  5.5 Mbps: Disable
   11 Mbps: Enable
 802.11g rate:
    1 Mbps: Disable
    2 Mbps: Disable
  5.5 Mbps: Disable
    6 Mbps: Disable
    9 Mbps: Disable
   11 Mbps: Enable
 802.11a rate:
    6 Mbps: Disable
    9 Mbps: Disable

Multicast rate:
1    24  Mbps
2    24  Mbps
3    24  Mbps
4    24  Mbps
5    24  Mbps
6    24  Mbps
7    24  Mbps
8    24  Mbps
11   24  Mbps
12   24  Mbps
13   24  Mbps
14   24  Mbps
15   24  Mbps
16   24  Mbps
17   24  Mbps
18   24  Mbps
19   24  Mbps
100  24  Mbps
1000 24  Mbps
1048 24  Mbps

Session limit:
 Session limit : 255

wlan 1, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.
```

```
wlan 2, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 3, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 4, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 5, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 6, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 7, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 8, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 11, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 12, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 13, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 14, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 15, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 16, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 17, Band select: enable
```

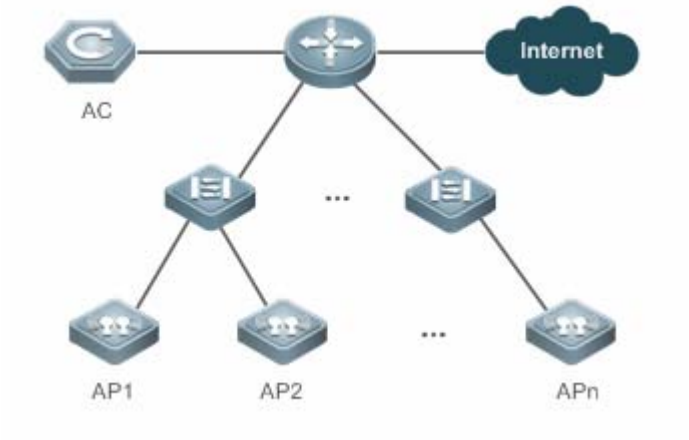
```
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 18, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 19, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 100, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 1000, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 1048, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

RRM status:
RRM 11a status: dca[disable] mode[NA]
                tpc[disable] mode[NA]
RRM 11b status: dca[disable] mode[NA]
                tpc[disable] mode[NA]
 -----> If there are co-channel and adjacent channel interference, suggest to enable RRM.

Speed limit:
 wlan[1   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300
Kbps]
 wlan[2   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300
Kbps]
 wlan[3   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300
Kbps]
 wlan[4   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300
Kbps]
 wlan[5   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300
Kbps]
 wlan[6   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300
Kbps]
 wlan[7   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300
Kbps]
 wlan[8   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300
Kbps]
```

```
 wlan[11  ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300
Kbps]
 wlan[12  ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300
Kbps]
 wlan[13  ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300
Kbps]
 wlan[14  ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300
Kbps]
 wlan[15  ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300
Kbps]
 wlan[16  ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300
Kbps]
 wlan[17  ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300
Kbps]
 wlan[18  ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300
Kbps]
 wlan[19  ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300
Kbps]
 wlan[100 ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300
Kbps]
 wlan[1000] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300
Kbps]
 wlan[1048] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300
Kbps]
```

↘ 瘦 AP 架构，配置一键网优

【网络环境】

图 1-14



如上图，典型瘦 AP 架构无线网络。

- AC 为无线接入控制器。
- AP1、AP2、……、APn 都是双频 AP。

- AC 和 AP 通过二层交换设备和三层路由设备连接。
- 配置一键网优。

【配置方法】
- 在 AC 上配置一键网优。

AC

```
AC# configure terminal
AC(config)# wopt choose band-select-enable low-rate-disable
```

【检验方法】 用户配置一键网优项后，通过显示网优信息进行检验。
- 通过 **show wopt** 命令可以显示网优信息。

AC

```
AC# show wopt

Low rate status:
 802.11b rate:
    1 Mbps: Disable
    2 Mbps: Disable
  5.5 Mbps: Disable
   11 Mbps: Enable
 802.11g rate:
    1 Mbps: Disable
    2 Mbps: Disable
  5.5 Mbps: Disable
    6 Mbps: Disable
    9 Mbps: Disable
   11 Mbps: Enable
 802.11a rate:
    6 Mbps: Disable
    9 Mbps: Disable

Multicast rate:
1    24  Mbps
2    24  Mbps
3    24  Mbps
4    24  Mbps
5    24  Mbps
6    24  Mbps
7    24  Mbps
8    24  Mbps
11   24  Mbps
12   24  Mbps
13   24  Mbps
14   24  Mbps
```

```
15   24  Mbps
16   24  Mbps
17   24  Mbps
18   24  Mbps
19   24  Mbps
100  24  Mbps
1000 24  Mbps
1048 24  Mbps

Session limit:
 Session limit : 255

wlan 1, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 2, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 3, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 4, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 5, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 6, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 7, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 8, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 11, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 12, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.
```

```
wlan 13, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 14, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 15, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 16, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 17, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 18, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 19, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 100, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 1000, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 1048, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

RRM status:
RRM 11a status: dca[disable] mode[NA]
                tpc[disable] mode[NA]
RRM 11b status: dca[disable] mode[NA]
                tpc[disable] mode[NA]
 -----> If there are co-channel and adjacent channel interference, suggest to enable RRM.

Speed limit:
 wlan[1    ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300
Kbps]
```

```
 wlan[2   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300
Kbps]
 wlan[3   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300
Kbps]
 wlan[4   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300
Kbps]
 wlan[5   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300
Kbps]
 wlan[6   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300
Kbps]
 wlan[7   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300
Kbps]
 wlan[8   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300
Kbps]
 wlan[11  ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300
Kbps]
 wlan[12  ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300
Kbps]
 wlan[13  ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300
Kbps]
 wlan[14  ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300
Kbps]
 wlan[15  ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300
Kbps]
 wlan[16  ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300
Kbps]
 wlan[17  ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300
Kbps]
 wlan[18  ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300
Kbps]
 wlan[19  ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300
Kbps]
 wlan[100 ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300
Kbps]
 wlan[1000] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300
Kbps]
 wlan[1048] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300
Kbps]
```

常见错误

- 无。

1.5.12 智能网优配置

配置效果

- 配置完此命令，可以根据网络情况，进行智能网优。

注意事项

- 无。

配置方法

- 在 config 配置模式下配置 wis enable 命令

【命令格式】 **wis enable**
【参数说明】 -
【缺省配置】 缺省不配置
【命令模式】 AC 的全局配置模式
【使用指导】 在运行网络中配置此命令后，可以实现对网络进行智能优化，一般用于网络管理人员。

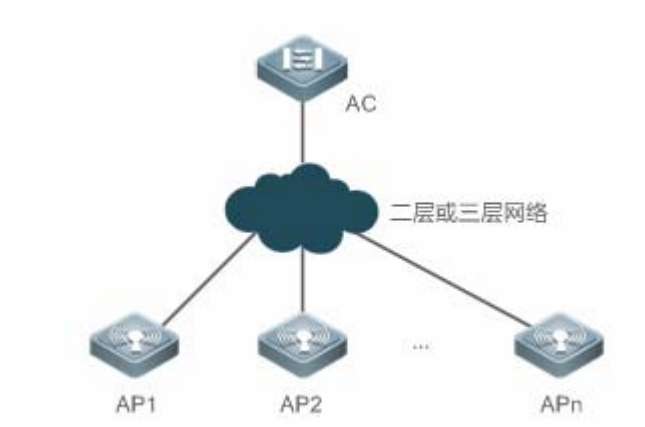
检验方法

- 通过 **show running** 命令可以查看配置。

配置举例

↘ 配置智能网优

【网络环境】
图 1-15



【配置方法】 ● 在 AC 设备上配置使能智能网优；

AC

```
Ruijie#configure terminal
Ruijie(config-ac)#wis enable
```

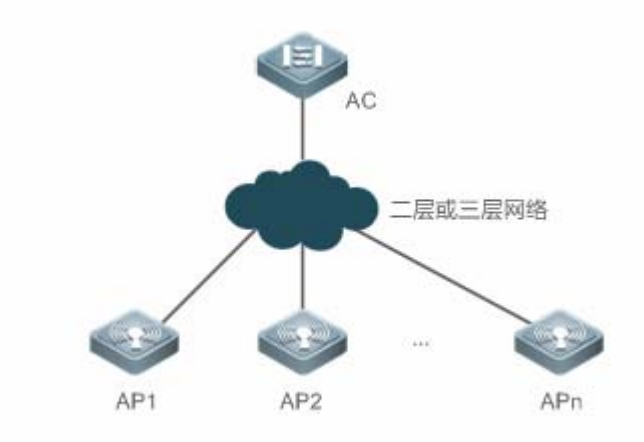
【检验方法】 用户配置智能网优后，通过显示进行校验。

● 通过 **show running** 命令可以查看速率集的配置信息。

```
Ruijie#show running
!
wis enable
!
```

常见错误

无。



1.5.13 mcell配置

配置效果

● 配置完此命令，使能密集部署优化。

注意事项

● 无。

配置方法

- 在 ap 配置模式下配置 mcell 命令

【命令格式】 Mcell enable **radio** *radio-id*
【参数说明】 *radio-id*：指定射频口索引，范围为 1~16
【缺省配置】 mcell 关闭
【命令模式】 AP 配置模式
【使用指导】 无

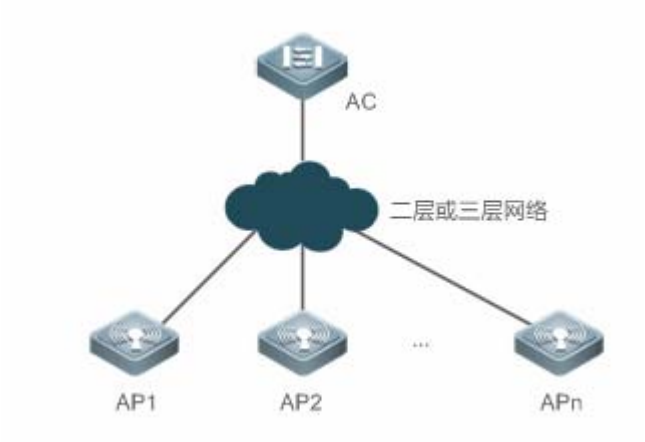
检验方法

- 通过 **show running** 命令可以查看配置。

配置举例

配置智能网优

【网络环境】
图 1-16



【配置方法】 - 在 AC 设备上配置使能智能网优；

AC

```
Ruijie#configure terminal
Ruijie(config)#ap-config AP1
Ruijie(config-ap)# mcell enable radio 1
```

【检验方法】 用户配置智能网优后，通过显示进行校验。

- 通过 **show running** 命令可以查看速率集的配置信息。

```
Ruijie#show ap-config running
ap-config AP1
 mcell enable radio 1
```

常见错误

无

1.5.14 配置漫游粘滞

配置效果

- 配置完此命令，开启漫游粘滞监控/导航。

注意事项

- 需要先开启 wis enable。

配置方法

- 在 ap-config all/ap-group 配置模式下配置漫游粘滞命令

【命令格式】 **sticky-steering** { **monitor-only** | **enable** }

【参数说明】 monitor-only：监控模式，只监控告警漫游粘滞，不做漫游粘滞导航

enable: 导航模式，一旦发现漫游粘滞，发起漫游粘滞导航

【缺省配置】 漫游粘滞关闭

【命令模式】 ap-config all 模式下配置到所有 AP 组，ap-group 模式下配置到单个 AP 组

【使用指导】 无

检验方法

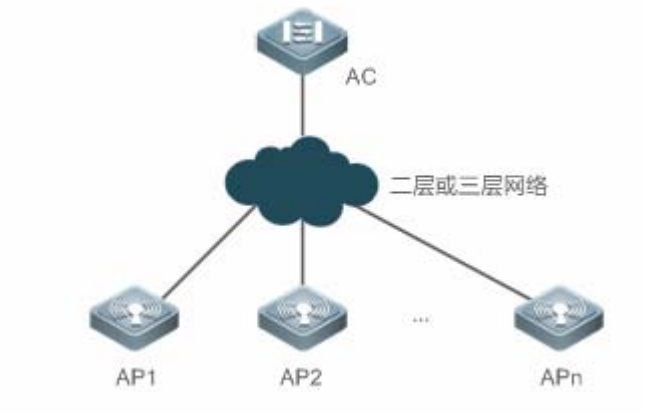
- 通过 **show running** 命令可以查看配置。

配置举例

↘ 配置智能网优

【网络环境】

图 1-17



【配置方法】
- 在 AC 设备上配置漫游粘滞监控；
- 在 AC 设备上配置漫游粘滞导航；

AC

```
Ruijie#configure terminal
Ruijie(config)#ap-config all
Ruijie(config-ap)# sticky-steering monitor-only
Ruijie(config-ap)# ap-group test1
Ruijie(config-group)#sticky-steering enable
```

【检验方法】 用户配置漫游粘滞后，通过显示进行校验。
- 通过 **show running** 命令可以查看漫游粘滞的配置信息。

```
Ruijie#show running-config
ap-group test1
 sticky-steering enable
!
ap-group test2
 sticky-steering monitor-only
!
ap-group test3
 sticky-steering monitor-only
!
```

常见错误

无

1.5.15 配置远端关联

配置效果

- 配置完此命令，使能远端信息采集，由 WIS 客户端提供远端关联优化方案。

注意事项

- 需要先开启 wis enable。

配置方法

- 在 ap-config all/ap-group 配置模式下配置远端关联使能命令

【命令格式】 **farpoint-steering enable**

【参数说明】 enable：使能远端关联信息采集

【缺省配置】 远端关联使能关闭

【命令模式】 ap-config all 模式下配置到所有 AP 组，ap-group 模式下配置到单个 AP 组

【使用指导】 无

检验方法

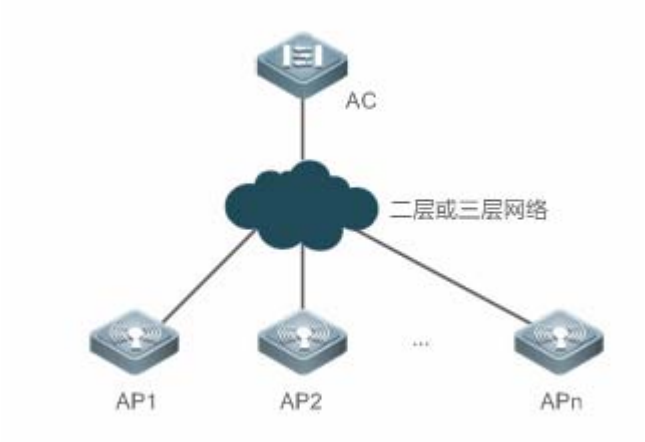
- 通过 **show running** 命令可以查看配置。

配置举例

配置智能网优

【网络环境】

图 1-18



【配置方法】

- 在 AC 设备上配置远端关联使能；

AC

```
Ruijie#configure terminal
Ruijie(config)#ap-config all
Ruijie(config-ap)# farpoint-steering enable
Ruijie(config-ap)# ap-group test1
Ruijie(config-group)#no farpoint-steering enable
```

【检验方法】 用户配置智能网优后，通过显示进行校验。

- 通过 **show running** 命令可以查看速率集的配置信息。

```
Ruijie#show running-config
ap-group test1
!
ap-group test2
 farpoint-steering enable
!
ap-group test3
```

```
farpoint-steering enable
!
```

常见错误

1.5.16 无配置设备信息自动上传功能

配置效果

- 配置完此命令，AC 和 AP 设备的软件版本信息，硬件版本信息都会自动上传到 WIS 云端

注意事项

- 在 WIS 功能没有开启时，配置该命令，也会自动上传。信息上传优先级如下：
- 如果有配置 WIS 客户端地址，则信息上传到 WIS 客户端
- 如果没有 WIS 客户端，但是设备可以通 WIS 公有云，则信息会上传到 WIS 公有云。
- 如果即没有配置 WIS 客户端，设备又通不了 WIS 公有云，则不上传设备信息

配置方法

- 在 config 配置模式下配置。

【命令格式】 **wis devinfo enable**
【参数说明】 enable：使能设备信息自动采集
【缺省配置】 使能设备信息自动采集
【命令模式】 全局配置模式
【使用指导】 无

检验方法

- 通过 **show running** 命令可以查看配置。

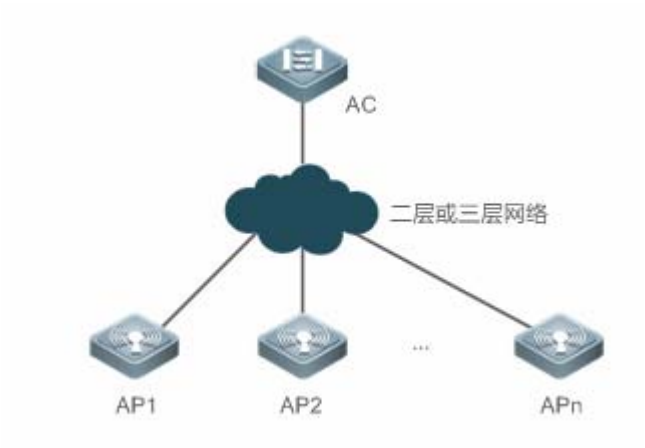
配置举例

无

↘ **配置智能网优**

【网络环境】

图 1-19



【配置方法】 ● 在 AC 设备上配置不自动上传设备信息；

AC

```
Ruijie#configure terminal
Ruijie(config)# no wis devinfo enable
```

【检验方法】 用户配置智能网优后，通过显示进行校验。

● 通过 **show running** 命令可以查看速率集的配置信息。

```
Ruijie#show running-config
no wis devinfo enable!
 !
```

常见错误

无

1.6 监视与维护

清除各类信息

无。

查看运行情况

作用	命令
查看全部配置信息。	**show running**
查看指定 AP 的配置信息	**show ap-config running** *ap-name*
查看所有 AP 的 radio 信息	**show ap-config radio**
查看指定 AP 指定 radio 的配置信息	**show ap-config radio** *radio-id* **config** *ap-name*
查看 AP 指定 radio 的详细状态信息	**show ap-config radio** *radio-id* **status** *ap-name*

显示 AP 的 radio 列表	**show ap-config radio status** *ap-name*
查看 Band Select 运行统计值。	**show band-select statistics**
查看网优信息	**show wopt**

查看调试信息

无。

2 频谱导航

2.1 概述

频谱导航（Band Select）是一种 WLAN 优化无线用户接入频段分配的技术。

频谱导航使用技术手段，引导使用双频 STA 的无线用户接入容量更高的 5G 频段，从而减轻 2.4G 频段的压力，提升用户体验。

频谱导航，适用于使用双频 AP 做覆盖，AP 两个射频接口分别工作在 2.4G 和 5G 频段；并且 WLAN 映射在 AP 的两个射频接口上，同时在两个频段提供接入服务的场景。

协议规范

- IEEE 802.11

2.2 典型应用

典型应用	场景描述
瘦 AP 架构 WLAN 频谱导航	瘦 AP 架构，由多台双频 AP 组建的 WLAN 开启频谱导航功能

2.2.1 瘦AP架构WLAN频谱导航

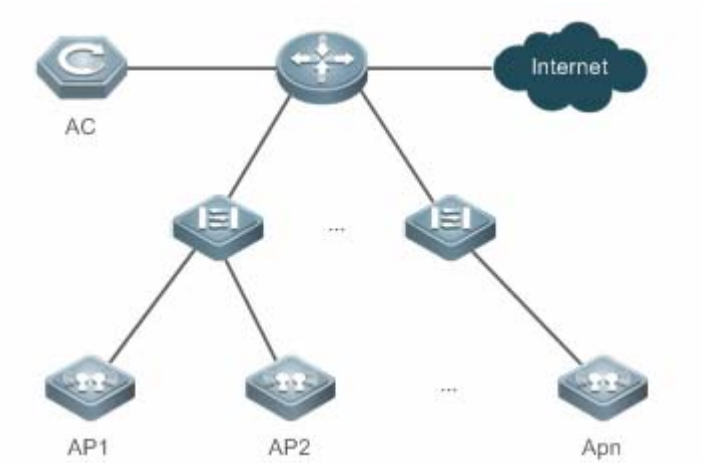
应用场景

瘦 AP 架构，由多台双频 AP 组建的 WLAN 开启频谱导航功能。

以下图为例，

- 一台 AC 下关联很多双频 AP，AC 和 AP 通过二层交换设备和三层路由设备连接。
- WLAN 映射到所有双频 AP 的两个射频接口上。

图 2-1



【注释】 AC 为无线接入控制器。
AP1、AP2、.....、APn 都是双频 AP。

功能部属

- AC 设备上管理频谱导航功能的工作参数。
- AP 设备上运行频谱导航功能，识别 STA 类型并引导 STA 接入。

2.3 功能详解

基本概念

IEEE802.11 通讯频段

IEEE802.11 的主要通讯频段分成两段：

- 2.4GHz (2.4 to 2.4835 GHz)，802.11b/g/n 所在频段
- 5GHz (5.15 to 5.35 and 5.725 to 5.825 GHz)，802.11a/n 所在频段

随着 WLAN 的普及，无线用户也越来越多，其中很多的用户使用能同时支持 2.4G 频段和 5G 频段的双频无线客户端（STA）。但是，802.11b/g 比 802.11a 的应用更为广泛，很多双频 STA 都使用 2.4G 频段，会造成 2.4G 频段的拥挤和 5G 频段的浪费。实际上，5G 频段拥有更高的接入容量：2.4G 频段最多只能有 3 个不重叠的通讯信道；而 5G 频段却能提供更多不重叠的通讯信道。

STA 发现 WLAN 的方式

有两种发现方式：被动扫描和主动扫描。

- 被动扫描：STA 在其支持的所有频段的所有信道上监听附近 AP 上发出的信标（Beacon）帧，信标帧包含了提供接入服务的 WLAN 以及附属信息。STA 解析这些信息就能了解周围存在哪些可以接入的 WLAN。

- 主动扫描：STA 首先在其支持的所有频段的所有信道上广播发送探测请求（Probe Request）帧，提供 WLAN 接入服务的 AP 收到探测请求帧，就会发出探测回应（Probe Response）帧，将自己提供的 WLAN 的一些信息发给 STA。

STA 一般会把发现的所有 WLAN 的 SSID 进行汇总，以可接入的 WLAN 列表的方式呈现给用户，供用户选择接入某个 WLAN。

↘ 双频 STA

无线用户用来连接 WLAN 的无线网卡，其功能规格描述中会有 a、b、g、n 等，它们表明无线网卡支持的 802.11 协议类型。802.11a 工作在 5G 频段；802.11b/g 工作在 2.4G 频段；802.11n 既可以工作在 5G 频段，也可以工作在 2.4G 频段。

所以，如果网卡功能规格描述中既包含 a，也包含 b 或者 g，那么就说明该网卡同时支持这两个频段，即为双频 STA。双频 STA 既可以接入 5G 频段，也可以接入 2.4G 频段。

↘ 双频 AP

双频 AP 即同时具有两个频段接入能力的 AP，所以双频 AP 至少需要两个射频接口，一个工作在 5G，另一个工作在 2.4G。

需要开启频谱导航的 WLAN，必须同时映射到双频 AP 的两个射频接口上，同时提供两个频段的接入服务。

功能特性

功能特性	作用
识别 STA 类型信息	识别 STA 是否双频 STA。
控制主动扫描过程	控制双频 STA 的主动扫描，防止其发现 2.4G 频段的 WLAN。
拒绝双频 STA 接入 2.4G 频段	拒绝双频 STA 接入 2.4G 频段，提高其接入 5G 频段的几率。

2.3.1 识别STA类型信息

要做到引导双频 STA 接入 5G 频段，第一步要识别 STA 是否双频 STA，就是识别 STA 的频段支持情况。

工作原理

主动扫描是 STA 发现 WLAN 的方式之一，STA 使用主动扫描时，会在 STA 支持的每个信道上发出探测请求帧，如果能得知 STA 发出的探测请求帧的信道信息，那么就能识别 STA 的频段支持情况。

比如，如果 AP 在 1～13 信道上接收到 STA 的探测请求帧，那么该 AP 就能知道该 STA 支持 2.4G 频段；如果 AP 在 149～165 信道上接收到 STA 的探测请求帧，那么该 AP 就能知道该 STA 支持 5G 频段。

因为单频 AP 只能从一个频段接收到探测请求帧，所以只有双频 AP 才能正确识别出 STA 类型。这就是频谱导航要求使用双频 AP 的原因。

↘ STA 分类标准

双频 AP 通过下面的标准将 STA 分类：

- 如果既能从 2.4G 频段收到该 STA 的探测请求，又能从 5G 频段收到该 STA 的探测请求，那么这是一个双频 STA；
- 如果只能从 5G 频段收到该 STA 的探测请求，那么该 AP 为 5G 的 STA；

- 如果只能从 2.4G 频段收到该 STA 的探测请求，那么该 AP 为 2.4G 的 STA；

因为需要等待一段时间以确认不会从另一个频段收到探测请求，识别单频的 STA 比较耗时一些，不过不会影响用户的正常使用。这三种 STA，前两种 STA 在频谱导航功能中称为双频类 STA，简称双频 STA；后面一种称为抑制类 STA，简称抑制 STA。

⚠ 对双频 STA 的识别，只能依赖等待一段时间（固定两秒）来确认其是否能在 5G 频段发出探测请求，因为 STA 驱动差别，这个时间不可能适用于所有的双频 STA，所以有几率出现刚开始不能正确识别 STA 类型的现象。只要以后双频 STA 能在 5G 频段发出探测请求，识别的 STA 类型就能恢复正确。

↘ STA 信息保存

双频 AP 识别到的 STA 的信息需要保存起来，给后续的回应策略提供依据。

因为 STA 的探测请求是广播报文，一般情况下，AP 都会收到大量的探测请求，把它们都保存起来是没有必要的，因为有些 STA 的距离太远，没有接入到本 AP 的可能。所以频谱导航只保存那些有可能接入的 STA 的信息，选择标准就是 STA 的 RSSI（Received Signal Strength Indication），RSSI 超过一个门限值的才是有可能接入的 STA，识别信息才需要保存。

↘ STA 信息老化

因为某些 STA 的频段支持情况是用户可以配置的，所以会出现在使用过程中，STA 的类型转换的情况。

比如一款支持 802.11agn 的无线网卡，开始使用时是双频 STA。后来用户手动禁用了它的 802.11a 模式或者 5G 频段信道的支持，那么该无线网卡就变成了单频 2.4G 的 STA 了。

针对这种情况，识别的 STA 信息要引入老化机制，一定时间后，丢弃先前识别的 STA 信息，然后重新识别。

2.3.2 控制主动扫描过程

识别了 STA 的频段支持情况后，双频 AP 就能根据 STA 信息，对 STA 的主动扫描过程进行控制，防止双频 STA 发现 2.4G 频段的 WLAN，从而达到引导双频 STA 接入 5G 频段的目的。

工作原理

STA 的主动扫描过程，正常情况下，STA 广播探测请求帧，AP 收到后会马上回应探测响应帧，告诉 STA 本 AP 上可以提供接入服务的 WLAN 信息等。双频 STA 在主动扫描时，在两个频段上都会发送探测请求并等待探测响应。打开频谱导航功能后，AP 要控制主动扫描的回应过程，针对不同的情况采用不同的回应方式。

↘ 频谱导航识别 STA 类型前的主动扫描

如果 WLAN 上开启了频谱导航功能，对 STA 的主动扫描回应有所变化。在识别 STA 类型信息之前：

- 2.4G 频段的探测请求不响应。
- 5G 频段的探测请求正常响应。

收到 2.4G 频段的探测请求，不能确定该 STA 是否支持 5G 频段，为了避免其发现 WLAN 在 2.4G 频段提供接入服务，需要等待识别过程结束才能回应。

收到 5G 频段的探测请求，就说明该 STA 支持 5G 频段，所以可以立刻回应探测响应，告诉该 WLAN 在 5G 频段提供接入服务。

频谱导航识别 STA 类型后的主动扫描

识别 STA 类型信息后，再收到 STA 的探测请求报文，可以根据探测请求报文中的源 MAC 地址找到 AP 上保存的 STA 的类型信息：

- 2.4G 频段的探测请求，如果 STA 类型是双频 STA，那么不回应探测响应；如果 STA 类型是抑制 STA，那么进行消极响应。
- 5G 频段的探测请求正常响应。

对双频 STA 在 2.4G 频段发出的探测请求 ,不回应探测响应可以避免双频 STA 发现 WLAN 在 2.4G 提供接入服务 ,让双频 STA 只能发现 WLAN 在 5G 频段提供接入服务，那么用户选择该 WLAN 接入时，双频 STA 就只能选择 5G 频段了。这就起到了引导双频 STA 接入 5G 频段的目的。

抑制 STA 在 2.4G 频段发出的探测请求，则必须进行回应。因为抑制 STA 只能支持 2.4G 频段，如果在 2.4G 频段不回应，那么它就无法发现 WLAN 了。不过回应方式上，可以对抑制 STA 进行抑制，也就是消极的回应。

5G 频段的探测请求，只有双频 STA 才能发出来，这时立刻回应探测响应，告诉该 WLAN 在 5G 频段提供接入服务。

频谱导航对抑制 STA 的消极回应

频谱导航对 5G 频段的探测请求都是积极回应的 ,对双频 STA 在 2.4G 频段探测请求都是不回应的 ,而对抑制 STA 的探测请求则是消极回应的。

消极回应，形象一点说，就是打了折扣的回应。比如连续收到多个探测请求，只回应一个探测响应。

频谱导航对抑制 STA 的消极回应程度，取决于两个参数：STA 探测扫描周期门限和抑制 STA 的探测周期计数值。

STA 探测扫描周期指的是 STA 主动扫描时，扫描完所有支持信道所花费的时间，这个时间取决于 STA 的驱动程序，每种 STA 可能均不相同。STA 探测扫描周期门限是一个用户可配置的值，可以理解成用户限制的 STA 探测扫描周期的最小值，如果某种 STA 的扫描周期小于这个值，那么连续的两个扫描周期会被 AP 认为是一个是扫描周期，这个参数可以正确处理某些 STA 在一个扫描周期内发送多个探测请求报文的情况。

举例说明：假设某 STA 每 150 毫秒扫描完所有信道，在每个信道上连续发送两个探测请求帧；如果 AP 上没有指定 STA 探测扫描周期的最小值 ,那么 AP 收到两个探测报文后 ,就无法判断是 STA 在一个扫描周期内发出来的两个还是连续两个扫描周期各发出来一个；如果 AP 上指定 STA 探测扫描周期的最小值为 200 毫秒，那么，因为两个报文的间隔不到 200 毫秒，就被认为是一个扫描周期内发出来的，AP 上该 STA 的探测周期计数就是 1。就例子中的 STA 而言，因为指定的 STA 探测扫描周期的最小值为 200 毫秒和实际扫描周期 150 毫秒不一致，也存在计数上的不一致问题：假设该 STA 连续扫描 3 个周期，那么 AP 上只能计数成 2 个周期，其中前两个周期被认为是同一个周期。不过这问题不会造成用户使用上的不便。

STA 的探测周期计数反映了频谱导航对抑制 STA 的消极回应的程度，这个参数的意思是：抑制 STA 主动扫描多个周期，AP 上才回应一次。比如，这个参数默认值为 2，表示 STA 连续两个扫描周期，AP 上的 WLAN 才回应一个探测响应帧。

2.3.3 拒绝双频STA接入 2.4G频段

⚠ 频谱导航功能只是控制了 STA 的主动扫描过程，还无法防止 STA 通过被动扫描发现 2.4G 频段的 WLAN。所以部分双频 STA 还是能发现 2.4G 频段的 WLAN 并尝试接入。这时频段导航功能就可能失效。

频谱导航可以拒绝双频 STA 在 2.4G 频段的接入请求，以提高双频 STA 接入 5G 频段的几率。

拒绝双频 STA 在 2.4G 频段的接入请求，可以提高频谱导航成功的几率，但是不可能达到 100%，频谱导航还是有可能失效的。

工作原理

STA 发现 WLAN 后，用户选择接入时，STA 首先发送链路认证请求帧（Authentication Request）给 AP，然后 AP 回应链路认证响应帧（Authentication Response）允许或拒绝 STA 的认证请求。

频谱导航功能可以处理链路认证请求帧，如果是双频 STA 在 2.4G 频段发出的认证请求，可以选择拒绝其认证请求，直到双频 STA 在 5G 频段发出认证请求才允许接入。这样也能起到引导双频 STA 接入 5G 频段的目的。

一般的双频 STA 接入时，会先在某个频段上发出一个或多个认证请求并等待回应，如果没有回应或者没有成功，就会转而在另一个频段发出认证请求并等待回应。但是也不排除有双频 STA 始终只在 2.4G 频段发出认证请求的情况，为了高可用性，频谱导航可以配置拒绝双频 STA 接入的次数。

假设某款双频 STA 接入时转换一次频段前会连续发送认证请求 M 次，而频谱导航功能的拒绝双频 STA 接入的次数配置成 N 次；那么，如果该双频 STA 首先尝试 5G 频段，那么就能马上接入；反之，如果该双频 STA 首先尝试 2.4G 频段，那么如果 N 大于等于 M，那么 STA 就能接入 5G 频段；反之，STA 将接入 2.4G 频段。不管接入哪个频段，如果双频 STA 首先尝试 2.4G 频段，那么总会有 min（M，N）（M，N 的较小的那个）个链路认证请求被拒绝或忽略，后果就是 STA 接入时间延长，延长的具体时间取决于 STA 的驱动，比如 STA 发送认证请求的间隔是 100 毫秒，有 4 个认证请求被忽略，那么该 STA 的正常接入会延长 400 毫秒。

频谱导航决定拒绝双频 STA 的接入请求时，如果其他的接入控制功能模块，比如负载均衡，决定接受该 STA 的接入请求，那么该 STA 是可以接入的。这是因为频谱导航功能只是在 STA 接入过程中起到“引导”作用，相对优先级比较低，当与其他功能相冲突时，以其他功能为优先。

2.4 产品说明

NBR800G、NBR950G、NBR1500G、NBR2000G 不支持无线集成 AC 功能；NBR108G-P、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持无线集成 AC 功能。

2.5 配置详解

配置项	配置建议 & 相关命令	
配置频谱导航	必须配置。用于开启 WLAN 的频谱导航功能。	
	band-select enable	开启频谱导航功能
	可选配置。用于配置频谱导航功能的工作参数。	
	band-select acceptable-rssi	配置频谱导航可以接受的STA信号强度下限。
	band-select access-denial	配置拒绝双频 STA 接入 2.4G 频段的次数。

	band-select age-out	配置 STA 信息的老化时间。
	band-select probe-count	配置抑制 STA 的探测周期计数值。
	band-select scan-cycle	配置 STA 探测扫描周期门限。

2.5.1 配置频谱导航

配置效果

- 开启 WLAN 的频谱导航功能，引导双频 STA 接入 5G 频段

注意事项

- 无。

配置方法

↘ 开启 WLAN 的频谱导航功能

- 必须配置。
- 若无特殊要求，在 AC 或者胖 AP 上打开。

【命令格式】 **band-select enable**
【参数说明】 **-**
【缺省配置】 关闭频谱导航功能
【命令模式】 WLAN 配置模式
【使用指导】 -

↘ 配置频谱导航可以接受的 STA 信号强度下限

- 可选配置，在需要调整频谱导航覆盖范围时进行配置。
- 若无特殊要求，在 AC 或者胖 AP 上打开。
- 该限值越高，频谱导航的覆盖范围越小；该限值越低，频谱导航的覆盖范围越大；但是，如果超过了可以正常使用的限制，会导致接入的 STA 信号过弱，拖慢整网的连接速率。

【命令格式】 **band-select acceptable-rssi** *value*
【参数说明】 *value*：频谱导航可以接受的 STA RSSI 下限，范围[-100，-50]，单位 dBm。
【缺省配置】 -80 dBm
【命令模式】 全局模式
【使用指导】 -

↘ 配置拒绝双频 STA 接入 2.4G 频段的次数

- 可选配置，在需要拒绝双频 STA 接入 2.4G 频段时配置；如果配置后出现较多双频 STA 接入时间过长或无法接入，要配置较小的值或配置为 0。
- 若无特殊要求，在 AC 或者胖 AP 上打开。
- 拒绝双频 STA 接入 2.4G 频段的次数越大，双频 STA 接入 2.4G 频段越困难，接入 2.4G 频段花费的时间也越长；拒绝双频 STA 接入 2.4G 频段的次数越小，双频 STA 接入 2.4G 频段越容易，接入 2.4G 频段花费的时间也越短。

【命令格式】 **band-select access-denial** *value*
【参数说明】 *value*：拒绝双频 STA 接入 2.4G 频段的次数，范围[0，10]。
【缺省配置】 2
【命令模式】 全局模式
【使用指导】 -

配置 STA 信息的老化时间

- 可选配置，如果环境中没有双频 STA 切换成单频 2.4G STA 的情况，可以配置较大的老化周期，反之，配置较小的老化周期；如果不确定，使用默认配置即可。
- 若无特殊要求，在 AC 或者胖 AP 上打开。
- STA 信息老化时间越大，STA 的信息生命周期越长，AP 对 STA 的频段切换越不敏感。STA 信息老化时间越小，STA 的信息生命周期越短，AP 对 STA 的频段切换越敏感。

【命令格式】 **band-select age-out** { **dual-band** *value* **| suppression** *value* }
【参数说明】 **dual-band** *value*：双频 STA 信息的老化时间，范围[20，120]，单位秒。
suppression *value*：抑制 STA 信息的老化时间，范围[10，60]，单位秒。
【缺省配置】 双频 STA 信息老化时间为 60 秒；抑制 STA 信息老化时间为 20 秒
【命令模式】 全局模式
【使用指导】 推荐双频 STA 的信息老化时间配置为抑制 STA 的信息老化时间的两倍到三倍。

配置抑制 STA 的探测周期计数值

- 可选配置，如果出现单频 2.4G STA 长时间发现不了 WLAN 的情况，那么应该减小该配置。
- 若无特殊要求，在 AC 或者胖 AP 上打开。
- STA 的探测周期计数值越大，频谱导航对抑制 STA 的抑制越大，抑制 STA 越不容易发现 WLAN；STA 的探测周期计数值越小，频谱导航对抑制 STA 的抑制越小，抑制 STA 越容易发现 WLAN。

【命令格式】 **band-select probe-count** *value*
【参数说明】 *value*：抑制 STA 的探测周期计数值，范围[1，10]。
【缺省配置】 2
【命令模式】 全局模式
【使用指导】 -

配置 STA 探测扫描周期门限

- 可选配置，如果出现单频 2.4G STA 长时间发现不了 WLAN 的情况，那么应该减小该配置；如果不确定，使用默认配置即可。

- 若无特殊要求，在 AC 或者胖 AP 上打开。
- STA 探测扫描周期门限值越大，STA 的探测周期计数增加越慢，STA 越不容易发现 WLAN；STA 探测扫描周期门限值越小，STA 的探测周期计数增加越快，STA 越容易发现 WLAN。

【命令格式】 **band-select scan-cycle** *value*
【参数说明】 *value*：STA 探测扫描周期门限，范围[1，1000]，单位毫秒。
【缺省配置】 200 毫秒
【命令模式】 全局模式
【使用指导】 -

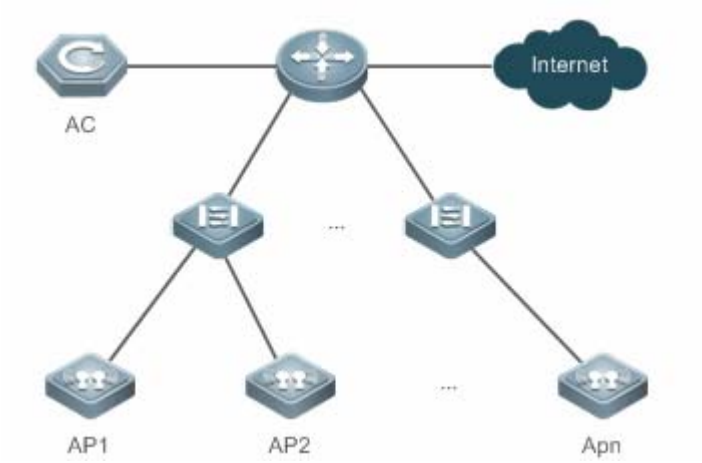
检验方法

- 使用 **show band-select configuration** 命令查看设备上的频谱导航参数配置。
- 使用 **show running-config** 命令查看 WLAN 配置是否打开了频谱导航功能。
- 运行一段时间后，使用 **show band-select statistics** 命令查看设备上的运行统计值。
- 抓包确认频谱导航是否控制了主动探测过程。

配置举例

↘ 瘦 AP 架构，配置 WLAN 的频谱导航

【网络环境】
图 2-2



如上图，典型瘦 AP 架构无线网络。

- AC 为无线接入控制器。
- AP1、AP2、.....、APn 都是双频 AP。
- AC 和 AP 通过二层交换设备和三层路由设备连接。
- 要开启频谱导航的 WLAN 为 WLAN 99，SSID “wlan-bandselect”，映射到所有双频 AP 的两个射频接口上。

【配置方法】
- 在 AC 上配置频谱导航运行参数（可选）。

- 在 AC 上开启 WLAN 99 的频谱导航功能。

AC

```
AC# configure terminal
AC(config)# wlan-config 99
AC(config-wlan)# band-select enable
```

【检验方法】 使用双频 STA 接入 WLAN“wlan-bandselect”。

- STA 接入 5G 频段。（也有可能出现导航失败，STA 接入 2.4G 频段）
- 检查 AC 上频谱导航运行统计值，应该出现计数增加。

AC

```
A# show band-select statistics
Band Select Statistics
  Number of dual band client.............................. 1
  Number of dual band client added........................ 1
  Number of dual band client expired...................... 0
  Number of suppressed client............................. 0
  Number of suppressed client added....................... 0
  Number of suppressed client expired..................... 0
```

常见错误

- 频谱导航运行参数配置不合适。
- 频谱导航功能没有打开。
- 双频 AP 的两个射频接口被关闭了一个。

2.6 监视与维护

清除各类信息

无。

查看运行情况

作用	命令
查看频谱导航运行配置。	**show band-select configuration**
查看频谱导航运行统计值。	**show band-select statistics**

查看调试信息

无。

WLAN 安全

本分册介绍 WLAN 安全相关内容，包括以下章节：

1. RSNA
2. WIDS
3. WAPI

1 RSNA

1.1 概述

RSNA（Robust Security Network Architecture，强健安全网络架构）功能实现无线网络安全机制。

由于无线网络使用的是开放性媒介采用公共电磁波作为载体来传输数据信号，通信双方没有线缆连接。如果传输链路未采取适当的加密保护，数据传输的风险就会大大增加。因此，安全机制在 WLAN 中显得尤为重要。

为了增强无线网络安全性，至少需要提供认证和加密两个安全机制：

- 认证机制：认证机制用来对用户的身份进行验证，以限定特定的用户（授权的用户）可以使用网络资源。
- 加密机制：加密机制用来对无线链路的数据进行加密，以保证无线网络数据只被所期望的用户接收和理解。

下文仅介绍 RSNA 的相关内容。

协议规范

- IEEE Standard for Information technology— Telecommunications and information exchange between systems— Local and metropolitan area networks— Specific requirements -2007
- WI-FI Protected Access – Enhanced Security Implementation Based On IEEE P802.11i Standard-Aug 2004
- 802.11i IEEE S tandard for Information techno logy—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements

1.2 典型应用

典型应用	场景描述
WEP 加密	在较为小型且对安全性要求不高的 WLAN 中 ,使用静态 WEP 加密模式保护无线数据通信。
PSK 接入认证	对于一些中小型的企业网络或者家庭用户 ,使用基于预共享密钥的接入认证方式加强无线网络安全。

1.2.1 WEP加密

应用场景

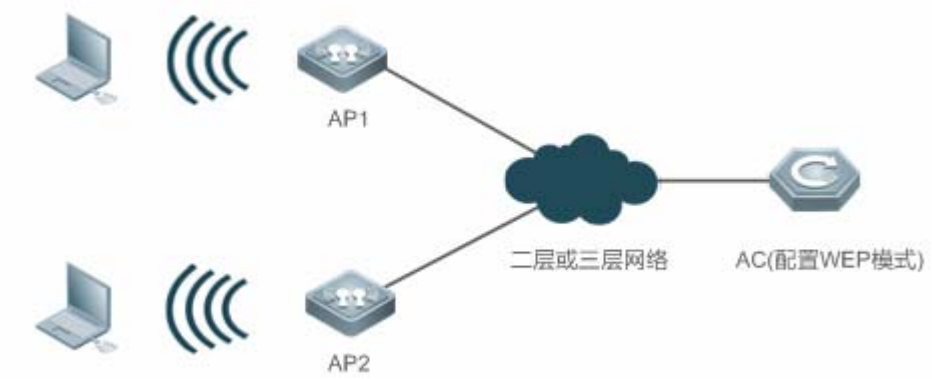
在较为小型且对安全性要求不高的 WLAN 中，可使用 WEP 加密模式。

WEP 加密模式可以分别采用 open-system 或者 shared-key 链路验证方式，两者的主要区别在于：

- 采用 open-system，此时 wep 密钥只用于数据加密，即使密钥配的不一致，用户也是可以上线，但上线后传输的数据会因为密钥不一致被接收端丢弃；
- 采用 shared-key，此时 wep 密钥做链路认证和数据加密，如果密钥不一致，客户端链路验证失败，无法上线。

静态 WEP 加密模式的应用场景如下图所示。

图 1-1



功能部属

- 在 AC 上配置 WLAN。
- 在 WLAN 安全模式下配置 WEP 加密模式。
- 将 WLAN 下发到 AP。

1.2.2 PSK接入认证

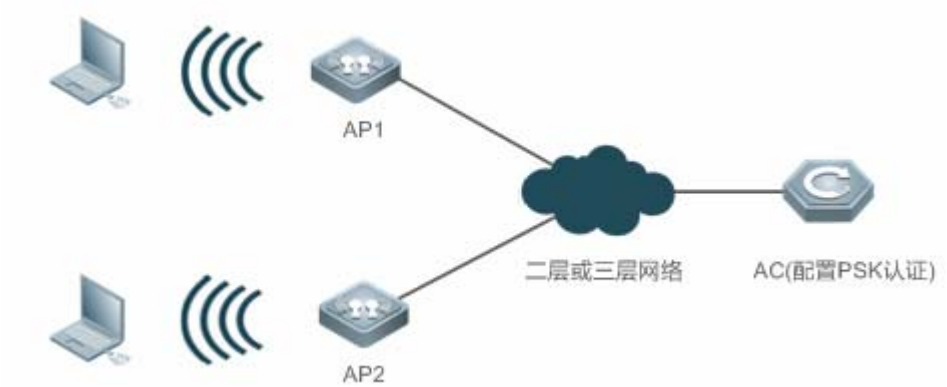
应用场景

对于一些中小型的企业网络或者家庭用户，使用 WPA 或 WPA2 标准加强无线网络安全，最简单的方法就是使用预共享密钥认证(分别称为 WPA-PSK 和 WPA2-PSK)。在这种情况下，WPA 的使用方法同 WEP 相似，但是能够得到 WPA 和 802.11i 带来的更高安全性，包括更强壮的认证和更好的加密算法。

PSK 认证只需为 STA 和接入设备配置相同的预共享密钥即可建立连接和通信，无需额外的认证服务器。

PSK 认证模式的应用场景如下图所示。

图 1-2



功能部属

- 在 AC 上配置 WLAN。
- 在 WLAN 安全模式下配置 PSK 认证模式。
- 将 WLAN 下发到 AP。
- 可配合 WEB 认证一起使用，以支持网络认证及计费功能。

1.3 功能详解

基本概念

WPA

Wi-Fi Protected Access，WPA 是 Wi-Fi 联盟定义的无线安全草案，IEEE802.11i 标准兼容该草案。

RSN

Robust Security Network，鲁棒性安全网络。IEEE802.11i 标准定义了 RSN 的概念，针对 WEP 加密机制的各种缺陷做了多方面的改进，功能上完全等同于 Wi-Fi 联盟推出的 WPA2。

TKIP

Temporal Key Integrity Protocol，临时密钥完整性协议，是对 WEP 安全性的增强。TKIP 提供每一数据包密钥混合、消息完整性核实和重新生成密钥机制，从而消除 WEP 的隐患。

AES

Advanced Encryption Standard，高级加密算法。AES 是 1997 年 1 月美国国家标准和技术研究所（NIST）发布征集的新加密算法。2000 年 10 月 2 日，由比利时设计者 Joan Daemen 和 Vincent Rijmen 设计的 Rijndael 算法以其优秀的性能和抗攻击能力，最终赢得了胜利，成为新一代的加密标准 AES。

CCMP

Counter CBC-MAC Protocol， 计数器模式密码块链消息完整码协议。CCMP 采用了比 TKIP 更安全的 AES 加密算法。

AKM

Authentication and Key Management，认证与密钥管理，即用户连接 WLAN 的接入认证方式。

功能特性

功能特性	作用
链路验证	STA 关联 WLAN 之前进行的无线链路安全验证。
接入认证	对接入 WLAN 的 STA 进行身份认证。
无线数据加密	实现对加入 WLAN 之后的 STA 通信数据的安全保护。

1.3.1 链路验证

链路验证即 802.11 身份验证，是一种低级的身份验证机制。在 STA 同 AP 进行 802.11 关联时发生，该行为早于接入认证。任何一个 STA 试图连接网络之前，都必须进行 802.11 的身份验证进行身份确认。可以把 802.11 身份验证看作是 STA 连接到网络时的握手过程的起点，是网络连接过程中的第一步。

IEEE 802.11 标准定义了两种链路层的认证：

- 开放系统链路验证
- 共享密钥链路验证

工作原理

开放系统链路验证

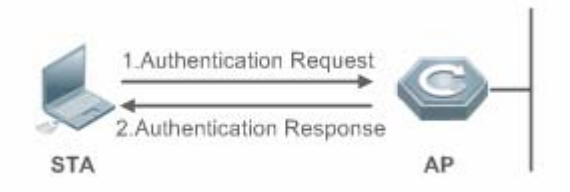
开放系统链路验证允许任何用户接入到无线网络中来。从这个意义上来说，实际上并没有提供对数据的保护，即不认证。也就是说，如果认证类型设置为开放系统认证，则所有请求认证的 STA 都会通过认证。

开放系统链路验证包括两个步骤：

第一步，STA 请求认证。STA 发出认证请求，请求中包含 STA 的 ID（通常为 MAC 地址）。

第二步，AP 返回认证结果。AP 发出认证响应，响应报文中包含表明认证是成功还是失败的消息。如果认证结果为“成功”，那么 STA 和 AP 就通过双向认证。

图 1-3



共享密钥链路验证

共享密钥链路验证是除开放系统链路验证以外的另外一种认证机制。共享密钥认证需要 STA 和 AP 配置相同的共享密钥。仅静态 WEP 加密模式下可配置共享密钥链路验证方式，其他模式均使用开放系统链路验证方式。

共享密钥链路验证的过程如下：

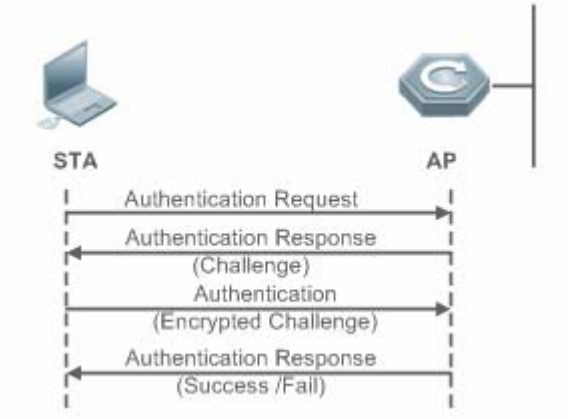
第一步，STA 先向 AP 发送认证请求；

第二步，AP 会随机产生一个 Challenge 包（即一个字符串）发送给 STA；

第三步，STA 会将接收到字符串拷贝到新的消息中，用密钥加密后再发送给 AP；

第四步，AP 接收到该消息后，用密钥将该消息解密，然后对解密后的字符串和最初给 STA 的字符串进行比较。如果相同，则说明 STA 拥有无线设备端相同的共享密钥，即通过了共享密钥认证；否则共享密钥认证失败。

图 1-4



1.3.2 接入认证

接入认证是一种增强 WLAN 安全性的解决方案。

当 STA 同 AP 关联后，是否可以使用无线接入点的服务要取决于接入认证的结果。如果认证通过，则无线接入点为 STA 打开这个逻辑端口，否则不允许用户连接网络。

IEEE 802.11 标准定义了如下接入认证方式：

- PSK 接入认证

工作原理

PSK 接入认证

PSK（Pre-shared key，预共享密钥）是一种 802.11i 身份验证方式，以预先设定好的静态密钥进行身份验证。该认证方式需要在无线用户端和无线接入设备端配置相同的预共享密钥。如果密钥相同， PSK 接入认证成功；如果密钥不同，PSK 接入认证失败。

1.3.3 无线数据加密

相对于有线网络，无线网络存在着更大的数据安全隐患。在一个区域内的所有的 WLAN 设备共享一个传输媒介，任何一个设备可以接收到其他所有设备的数据，这个特性直接威胁到 WLAN 接入数据的安全。

IEEE 802.11i 协议定义了以下三种无线数据加密算法：

- WEP 加密
- TKIP 加密
- AES 加密

工作原理

↘ WEP 加密

WEP（Wired Equivalent Privacy，有线等效加密）是原始 IEEE 802.11 标准中指定的数据加密方法，是 WLAN 安全认证和加密的基础，用来保护无线局域网中授权用户所交换的数据的私密性，防止这些数据被窃取。

WEP 使用 RC4 算法来保证数据的保密性，通过共享密钥来实现认证。WEP 没有规定密钥的管理方案，一般手动进行密钥的配置与维护。通常把这种不具密钥分配机制的 WEP 称为手动 WEP 或者静态 WEP。

WEP 加密密钥的长度一般有 64 位和 128 位两种。其中有 24Bit 的 IV（Initialization Vector，初始化向量）是由系统产生的。因此需要在 AP 和 STA 上配置的共享密钥就只有 40 位或 104 位。在实际中，已经广泛使用 104 位密钥的 WEP 来代替 40 位密钥的 WEP，104 位密钥的 WEP 称为 WEP-104。虽然 WEP-104 在一定程度上提高了 WEP 加密的安全性，但是受到 RC4 加密算法以及静态配置密钥的限制，WEP 加密还是存在比较大的安全隐患，无法保证数据的机密性、完整性和对接入用户实现身份认证。

↘ TKIP 加密

TKIP（Temporal Key Integrity Protocol，暂时密钥集成协议） 是 IEEE 802.11 组织为修补 WEP 加密机制而创建的一种临时的过渡方案。TKIP 也和 WEP 加密机制一样使用的是 RC4 算法，但是相比 WEP 加密机制，TKIP 加密机制可以为 WLAN 服务提供更加安全的保护。主要体现在以下几点：

–静态 WEP 的密钥为手工配置，且一个服务区内的所有用户都共享同一把密钥。而 TKIP 的密钥为动态协商生成，每个传输的数据包都有一个与众不同的密钥。

– TKIP 将密钥的长度由 WEP 的 40 位加长到 128 位，初始化向量 IV 的长度由 24 位加长到 48 位，提高了 WEP 加密的安全性。

– TKIP 支持 MIC 认证（Message Integrity Check，信息完整性校验）和防止重放攻击功能。

↘ AES 加密

AES-CCMP（Counter mode with CBC-MAC Protocol，计数器模式搭配 CBC-MAC 协议）是目前为止面向大众的最高级无线安全协议。

IEEE 802.11i要求使用CCMP来提供全部四种安全服务 认证、机密性、完整性和重发保护。CCMP使用128位AES（Advanced Encryption Standard，高级加密标准）加密算法实现机密性，使用CBC-MAC（区块密码锁链 - 信息真实性检查码协议）来保证数据的完整性和认证。

作为一种全新的高级加密标准，AES 加密算法采用对称的块加密技术，提供比 WEP/TKIP 中 RC4 算法更高的加密性能，成为取代 WEP 的新一代的加密技术，为无线网络带来更强大的安全防护。

1.4 产品说明

NBR800G、NBR950G、NBR1500G、NBR2000G 不支持无线集成 AC 功能，NBR108G-P、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持无线集成 AC 功能。

1.5 配置详解

配置项	配置建议 & 相关命令	
配置静态 WEP 模式	必须配置。用于启用静态 WEP 加密模式。	
	security static-wep-key encryption	配置 WLAN 启用静态 WEP 模式，同时配置静态 WEP 密钥。
	可选配置。用于配置链路验证方式。	
	security static-wep-key authentication	配置静态 WEP 模式的链路验证方式。
配置 WPA 认证	必须配置。用于启用 WPA 认证模式。	
	security wpa	配置 WLAN 的认证模式为 WPA 认证模式。
	security wpa ciphers	配置 WPA 认证模式的加密方式。
	security wpa akm	配置 WPA 认证模式的接入认证方式。
	可选配置。用于配置 WPA PSK 认证方式的共享密码。	
	security wpa akm psk set-key	配置 WPA PSK 认证方式的共享密码。
配置 RSN 认证	必须配置。用于启用 RSN 认证模式。	
	security rsn	配置 WLAN 的认证模式为 RSN 认证模式。
	security rsn ciphers	配置 RSN 认证模式的加密方式。
	security rsn akm	配置 RSN 认证模式的接入认证方式。
	可选配置。用于配置 RSN PSK 认证方式的共享密码。	
	security rsn akm psk set-key	配置 RSN PSK 认证方式的共享密码。
配置认证参数	可选配置。用于配置密钥交互相关参数及 WEB 认证模式下的防抖时间参数。	

	authtimeout forbidcount	配置四次握手 key 交互失败后 ,禁止关联的次数。
	authtimeout forbidtime	配置四次握手 key 交互失败后，禁止关联的时间间隔。
	authtimeout groupcount	配置组播密钥协商报文重传次数。
	authtimeout grouptime	配置组播密钥协商报文超时时间。
	authtimeout paircount	配置单播密钥协商报文重传次数。
	authtimeout pairtime	配置单播密钥协商报文超时时间。
	webauth prevent-jitter	配置 WEB 认证防抖时间。

1.5.1 配置静态WEP模式

配置效果

- 启用静态 WEP 加密模式，对 WLAN 中的数据提供 WEP 加密保护。
- 可配置链路验证方式。

注意事项

- 链路验证方式必须在启用静态 WEP 加密模式之后才可以配置。
- 在同一个 WLAN 安全模式下，静态 WEP 加密不可与其他认证加密同时配置。
- 只有 1 个 WLAN 可配置静态 WEP 加密模式。

配置方法

↘ 启用静态 WEP 模式

- 必须配置。
- 在 AC 设备上要启用静态 WEP 加密模式的 WLAN 对应的安全配置模式下配置。

【命令格式】 **security static-wep-key encryption** *key-length* { **ascii** | **hex** } *key-index key*

【参数说明】 *key-length*：密码长度，单位是比特，可以为 40 或 104。

ascii：密码形式为 ASCII 码。

hex：密码形式为 16 进制字符。

key-index：密钥索引号，配置范围是：1--4。

key：密码数据。

【缺省配置】 未启用静态 WEP 模式。

【命令模式】 WLAN 安全配置模式

【使用指导】 这条命令在配置静态 WEP 密钥，同时启用静态 WEP 模式。

这条命令可以重复配置，最后一次配置的命令生效。

密钥数据长度必须与命令中指定的 *key-length* 参数一致。

配置链路验证方式

- 可选配置。默认链路验证方式为开放系统链路验证，可使用该命令配置为共享密钥链路验证方式。
- 在 AC 设备上启用静态 WEP 加密模式的安全配置模式下配置。
- 必须在启用静态 WEP 模式之后才可以配置链路验证方式。配置共享密钥链路验证方式之后，STA 端也应该将链路验证方式选择为共享式，否则无法加入 WLAN。

【命令格式】 **security static-wep-key authentication** { **open** | **share-key** }

【参数说明】 **open**：配置开放系统链路验证方式。

share-key：配置共享密钥链路验证方式。

【缺省配置】 STA 加入 WLAN 采用开放系统链路验证方式

【命令模式】 WLAN 安全配置模式

【使用指导】 先配置完静态 WEP 密钥后才能配置链路验证方式。

除了静态 WEP 模式之外的其它安全配置模式，无法配置链路验证方式。

检验方法

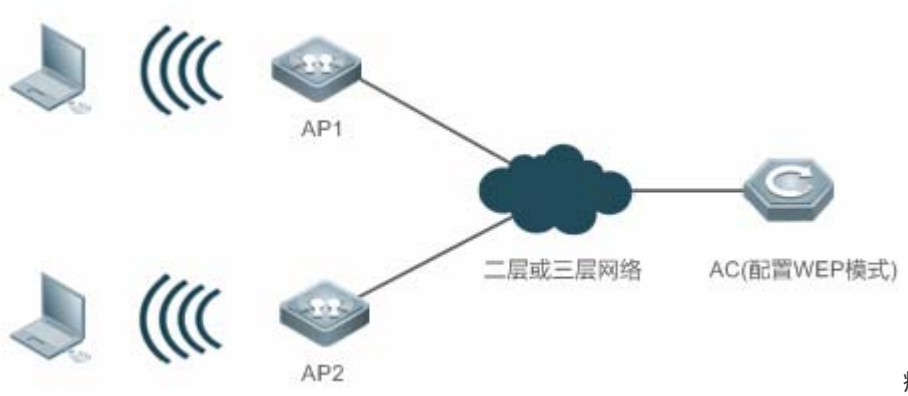
使用 **show running-config** | **begin wlansec** *wlan_id* 命令，可以查看配置是否生效。

配置举例

配置 WLAN 1 为静态 WEP 加密模式，且使用共享密钥链路验证方式

【网络环境】

图 1-5



瘦 AP 环境中，在 AC 设备上配置 WLAN 1，并配置 WLAN 1 的安全策略为：

1、静态 WEP 加密模式；

2、使用共享密钥链路验证方式。

【配置方法】

- 进入 WLAN 1 的安全配置模式。
- 配置启用静态 WEP 加密模式及 WEP 密钥。
- 配置链路验证方式为共享密钥链路验证。

AC

```
Ruijie(config)#wlansec 1
Ruijie(config-wlansec)#security static-wep-key encryption 40 ascii 1 12345
```

```
Ruijie(config-wlansec)#security static-wep-key authentication share-key
```

【检验方法】 使用 **show running-config | begin wlansec** *wlan_id* 命令，可以查看配置是否生效。

AC

```
Ruijie#show running-config | begin wlansec 1
wlansec 1
 security static-wep-key encryption 40 ascii 1 12345
 security static-wep-key authentication share-key
!
```

常见错误

- 配置的密码字符数与指定的密码长度不一致。
- 配置多个 WLAN 为静态 WEP 模式。
- 未配置启用静态 WEP 模式就配置链路验证方式。

1.5.2 配置WPA认证

配置效果

- WLAN 启用 WPA 认证模式。
- 指定 WPA 认证模式下的接入认证方式和数据加密方式。

注意事项

- 使用 WPA 认证时，需要配合配置数据加密方式和接入认证方式。
- 如果配置接入认证方式为 PSK，需配置 PSK 密码。
- 在同一个 WLAN 安全模式下，WPA 认证模式不能与 WEP 模式同时配置。

配置方法

↘ 配置 WPA 认证模式

- 必须配置。
- 在 AC 设备上要启用 WPA 认证模式的 WLAN 对应的安全配置模式下配置。

【命令格式】 **security wpa** { **enable** | **disable** }

【参数说明】 **enable**：启用 WPA 认证模式。

disable：关闭 WPA 认证模式。

【缺省配置】 关闭 WPA 认证模式。

【命令模式】 WLAN 安全配置模式

【使用指导】 只有启用了 WPA 认证模式才能在 WPA 模式下对加密方式和接入认证方式的配置，否则是配置是无效。

使用 WPA 认证时，需要配合配置加密方式和接入认证方式。如果只配置了加密方式，或者只配置了接入认证方式，或者两者都未配置，那么无线客户端将无法关联到无线网络。

配置 WPA 认证模式的数据加密方式

- 必须配置。
- 在 AC 设备上启用 WPA 认证模式的安全配置模式下配置。
- 必须在启用 WPA 认证模式之后才可以配置 WPA 认证模式下的数据加密方式。一个 WLAN 安全配置模式下可同时开启 AES 和 TKIP 两种加密方式。配置 WLAN 的数据加密方式之后，STA 加入 WLAN 之后的通信数据将使用相应的数据加密方式进行保护。

【命令格式】 **security wpa ciphers** { **aes** | **tkip** } { **enable** | **disable** }

【参数说明】 **aes**：配置加密方式为 AES。

tkip：配置加密方式为 TKIP。

enable：开启 WPA 认证模式的加密方式。

disable：关闭 WPA 认证模式的加密方式。

【缺省配置】 未配置数据加密方式

【命令模式】 WLAN 安全配置模式

【使用指导】 这个命令是用来启用 WPA 认证模式下的加密方式，有 AES 和 TKIP 两种加密方式。

一个 WLAN 安全配置模式下可同时开启 AES 和 TKIP 两种加密方式。

配置 WPA 认证模式的接入认证方式

- 必须配置。
- 在 AC 设备上启用 WPA 认证模式的安全配置模式下配置。
- 必须在启用 WPA 认证模式之后才可以配置 WPA 认证模式下的接入认证方式。一个 WLAN 安全配置模式下只能开启一种接入认证方式。启用接入认证方式的 WLAN，STA 必须通过相应的接入认证才可以加入 WLAN。

【命令格式】 **security wpa akm psk** { **enable** | **disable** }

【参数说明】 **psk**：配置接入认证方式为预共享密钥认证。

enable：开启 WPA 认证模式的接入认证方式。

disable：关闭 WPA 认证模式的接入认证方式。

【缺省配置】 未配置接入认证方式。

【命令模式】 WLAN 安全配置模式

【使用指导】 只有启用了 WPA 认证模式才能进行接入认证方式的配置。

一个 WLAN 安全配置模式下只能开启一种接入认证方式。

配置 WPA 认证模式的共享密码

- 可选配置，启用 WPA PSK 认证方式时必须配置。
- 在 AC 设备上启用 WPA PSK 认证模式的安全配置模式下配置。

【命令格式】 **security wpa akm psk set-key** { **ascii** *ascii-key* | **hex** *hex-key* }

【参数说明】 **ascii**：指定 PSK 密码形式为 ASCII 码。

ascii-key：ASCII 码形式的密码，长度限制为 8--63 个 ASCII 码字符。

hex：指定 PSK 密码形式为十六进制字符。

hex-key：十六进制形式的密码，长度必须为 64 个十六进制字符。

【缺省配置】 无

【命令模式】 WLAN 安全配置模式

【使用指导】 只有开启了 PSK 认证方式时，这个共享密码才有意义。

ASCII 码形式的密码，长度限制为 8--63 个 ASCII 码字符。

十六进制形式的密码，长度必须为 64 个十六进制字符。

检验方法

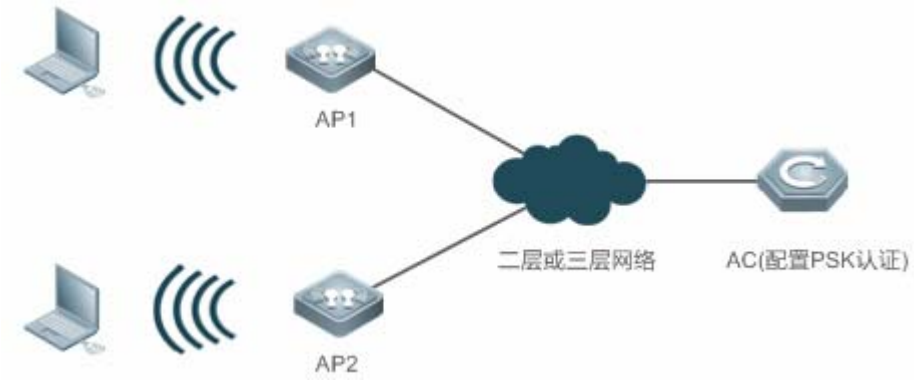
使用 **show running-config** | **begin wlansec** *wlan_id* 命令，可以查看配置是否生效。

配置举例

↘ 配置 WLAN 1 为 WPA PSK 认证模式，数据加密方式为 AES，密码为 12345678。

【网络环境】

图 1-6



瘦 AP 环境中，在 AC 设备上配置 WLAN 1 的安全策略为：

1、配置为 WPA PSK 认证方式；

2、配置数据加密方式为 AES；

3、配置共享密码为 12345678。

【配置方法】

- 进入 WLAN 1 的安全配置模式。
- 配置启用 WPA 认证模式。
- 配置 WPA 认证模式的数据加密方式为 AES。
- 配置 WPA 认证模式的接入认证方式为 PSK。
- 配置 PSK 密码为 12345678。

AC

```
Ruijie(config)#wlansec 1
Ruijie(config-wlansec)#security wpa enable
Ruijie(config-wlansec)#security wpa ciphers aes enable
```

```
Ruijie(config-wlansec)#security wpa akm psk enable
Ruijie(config-wlansec)#security wpa akm psk set-key ascii 12345678
```

【检验方法】 使用 **show running-config | begin wlansec** *wlan_id* 命令，可以查看配置是否生效。

AC

```
Ruijie#show running-config | begin wlansec 1
wlansec 1
 security wpa enable
 security wpa ciphers aes enable
 security wpa akm psk enable
 security wpa akm psk set-key ascii 12345678
!
```

常见配置错误

- WLAN 已经启用了其他的加密认证方式（如 WEP）。
- WLAN 安全配置模式下未启用 WPA 认证就配置 WPA 加密方式。
- WLAN 安全配置模式下未启用 WPA 认证就配置接入认证方式。
- WLAN 安全配置模式下已经开启了一种接入认证方式，则无法配置另一种接入认证方式。
- 未启用 WPA 认证，就配置 WPA PSK 密码。
- ASCII 码形式的密码长度不足 8 个字符或超过 63 个字符。
- 十六进制形式的密码长度不是 64 个十六进制字符。

1.5.3 配置RSN认证

配置效果

- WLAN 启用 RSN 认证模式。
- 指定 RSN 认证模式下的接入认证方式和数据加密方式。

注意事项

- 使用 RSN 认证时，需要配合配置数据加密方式和接入认证方式。
- 如果配置接入认证方式为 PSK，需配置 PSK 密码。
- 在同一个 WLAN 安全模式下，RSN 认证模式不能与 WEP 模式同时配置。

配置方法

配置 RSN 认证模式

- 必须配置。
- 在 AC 设备上要启用 RSN 认证模式的 WLAN 对应的安全配置模式下配置。

【命令格式】 **security rsn** { **enable** | **disable** }

【参数说明】 **enable**：启用 RSN 认证模式。

disable：关闭 RSN 认证模式。

【缺省配置】 关闭 RSN 认证模式。

【命令模式】 WLAN 安全配置模式

【使用指导】 只有启用了 RSN 认证模式才能在 RSN 模式下对加密方式和接入认证方式的配置，否则是配置是无效。

使用 RSN 认证时，需要配合配置加密方式和接入认证方式。如果只配置了加密方式，或者只配置了接入认证方式，或者两者都未配置，那么无线客户端将无法关联到无线网络。

配置 RSN 认证模式的数据加密方式

- 必须配置。
- 在 AC 设备上启用 RSN 认证模式的安全配置模式下配置。
- 必须在启用 RSN 认证模式之后才可以配置 RSN 认证模式下的数据加密方式。一个 WLAN 安全配置模式下可同时开启 AES 和 TKIP 两种加密方式。配置 WLAN 的数据加密方式之后，STA 加入 WLAN 之后的通信数据将使用相应的数据加密方式进行保护。

【命令格式】 **security rsn ciphers** { **aes** | **tkip** } { **enable** | **disable** }

【参数说明】 **aes**：配置加密方式为 AES。

tkip：配置加密方式为 TKIP。

enable：开启 RSN 认证模式的加密方式。

disable：关闭 RSN 认证模式的加密方式。

【缺省配置】 未配置数据加密方式

【命令模式】 WLAN 安全配置模式

【使用指导】 这个命令是用来启用 RSN 认证模式下的加密方式，有 AES 和 TKIP 两种加密方式。

一个 WLAN 安全配置模式下可同时开启 AES 和 TKIP 两种加密方式。

配置 RSN 认证模式的接入认证方式

- 必须配置。
- 在 AC 设备上启用 RSN 认证模式的安全配置模式下配置。
- 必须在启用 RSN 认证模式之后才可以配置 RSN 认证模式下的接入认证方式。一个 WLAN 安全配置模式下只能开启一种接入认证方式。启用接入认证方式的 WLAN，STA 必须通过相应的接入认证才可以加入 WLAN。

【命令格式】 **security rsn akm psk** { **enable | disable** }

【参数说明】 **psk**：配置接入认证方式为预共享密钥认证。

enable：开启 RSN 认证模式的接入认证方式。

disable：关闭 RSN 认证模式的接入认证方式。

【缺省配置】 未配置接入认证方式

【命令模式】 WLAN 安全配置模式

【使用指导】 只有启用了 RSN 认证模式才能进行接入认证方式的配置。

一个 WLAN 安全配置模式下只能开启一种接入认证方式。

↘ 配置 RSN 认证模式的共享密码

- 可选配置，启用 RSN PSK 认证方式时必须配置。
- 在 AC 设备上启用 RSN PSK 认证模式的安全配置模式下配置。

【命令格式】 **security rsn akm psk set-key** { **ascii** *ascii-key* | **hex** *hex-key* }

【参数说明】 **ascii**：指定 PSK 密码形式为 ASCII 码。

ascii-key：ASCII 码形式的密码，长度限制为 8--63 个 ASCII 码字符。

hex：指定 PSK 密码形式为十六进制字符。

hex-key：十六进制形式的密码，长度必须为 64 个十六进制字符。

【缺省配置】 无

【命令模式】 WLAN 安全配置模式

【使用指导】 只有开启了 PSK 认证方式时，这个共享密码才有意义。

ASCII 码形式的密码，长度限制为 8--63 个 ASCII 码字符。

十六进制形式的密码，长度必须为 64 个十六进制字符。

检验方法

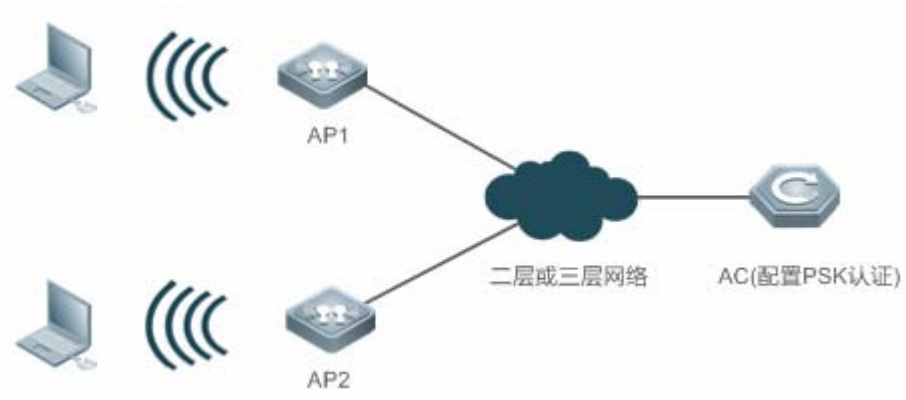
使用 **show running-config** | **begin wlansec** *wlan_id* 命令，可以查看配置是否生效。

配置举例

↘ 配置 WLAN 1 为 RSN PSK 认证模式，数据加密方式为 AES，密码为 12345678。

【网络环境】

图 1-7



瘦 AP 环境中，在 AC 设备上配置 WLAN 1 的安全策略为：

1、配置为 RSN PSK 认证方式；

2、配置数据加密方式为 AES；

3、配置共享密码为 12345678。

【配置方法】
- 进入 WLAN 1 的安全配置模式。
- 配置启用 RSN 认证模式。
- 配置 RSN 认证模式的数据加密方式为 AES。
- 配置 RSN 认证模式的接入认证方式为 PSK。
- 配置 PSK 密码为 12345678。

AC

```
Ruijie(config)#wlansec 1
Ruijie(config-wlansec)#security rsn enable
Ruijie(config-wlansec)#security rsn ciphers aes enable
Ruijie(config-wlansec)#security rsn akm psk enable
Ruijie(config-wlansec)#security rsn akm psk set-key ascii 12345678
```

【检验方法】 使用 **show running-config | begin wlansec** *wlan_id* 命令，可以查看配置是否生效。

AC

```
Ruijie#show running-config | begin wlansec 1
wlansec 1
 security rsn enable
 security rsn ciphers aes enable
 security rsn akm psk enable
 security rsn akm psk set-key ascii 12345678
!
```

常见配置错误

- WLAN 已经启用了其他的加密认证方式（如 WEP）。
- WLAN 安全配置模式下未启用 RSN 认证就配置 RSN 加密方式。
- WLAN 安全配置模式下未启用 RSN 认证就配置接入认证方式。
- WLAN 安全配置模式下已经开启了一种接入认证方式，则无法配置另一种接入认证方式。
- 未启用 RSN 认证，就配置 RSN PSK 密码。
- ASCII 码形式的密码长度不足 8 个字符或超过 63 个字符。
- 十六进制形式的密码长度不是 64 个十六进制字符。

1.5.4 配置认证参数

配置效果

- 配置密钥交互相关参数。
- 配置 WEB 认证模式下的防抖时间参数。

注意事项

- 必须先启用 WEB 认证，才可以配置 WEB 认证防抖时间参数。

配置方法

配置密钥交互相关参数

- 可选配置。一般不需要配置，无线网络环境较差的情况下可配置较大的报文重传次数及超时时间。
- 在 AC 设备上启用 PSK 认证方式的安全配置模式下配置。

【命令格式】 **authtimeout** { **forbidcount** *count* | **forbidtime** *time* | **groupcount** *count* | **grouptime** *timeout* | **paircount** *count* | **pairtime** *timeout* }

【参数说明】 **forbidcount** *count*：配置四次握手 key 交互失败后，禁止关联的次数。
forbidtime *time*：配置四次握手 key 交互失败后，禁止关联的时间间隔。
groupcount *count*：配置组播密钥协商报文重传次数。
grouptime *timeout*：配置组播密钥协商报文超时时间。
paircount *count*：配置单播密钥协商报文重传次数。
pairtime *timeout*：配置单播密钥协商报文超时时间。

【缺省配置】 四次握手 key 交互失败后，禁止关联的次数为 10 次
四次握手 key 交互失败后，禁止关联的时间间隔为 5 秒
组播密钥协商报文重传次数缺省为 7 次
组播密钥协商报文超时时间缺省为 1200ms
单播密钥协商报文重传次数缺省为 7 次
单播密钥协商报文超时时间缺省为 1200ms

【命令模式】 WLAN 安全配置模式

【使用指导】 密钥交互相关参数在 PSK 认证方式下才生效。

配置 WEB 认证防抖时间参数

- 可选配置。WEB 认证防抖时间默认为 300 秒，用户可根据实际需求配置防抖时间。或者通过配置 WEB 认证防抖时间为 0 秒关闭 WEB 认证防抖功能。
- 在 AC 设备上启用 WEB 认证的安全配置模式下配置。

【命令格式】 **webauth prevent-jitter** *timeout*

【参数说明】 *timeout*：配置 WEB 认证防抖时间，以秒为单位。*timeout* 的取值范围是 0s---86400s（*timeout* 为 0 表示关闭 WEB 认证防抖功能)。

【缺省配置】 WEB 认证防抖时间，缺省值为 300 秒。

【命令模式】 WLAN 安全配置模式

【使用指导】 必须先启用 WEB 认证，才可以配置 WEB 认证防抖时间。

检验方法

使用 **show running-config** | **begin wlansec** *wlan_id* 命令，可以查看配置是否生效。

配置举例

↘ 配置 WLAN 1 为 RSN-PSK + WEB 认证模式，配置单播密钥协商报文重传次数为 5 次，配置 WEB 认证防抖时间为 900 秒。

【网络环境】

图 1-8



瘦 AP 环境中，在 AC 设备上配置 WLAN 1 的安全策略为：

1、配置为 RSN PSK 认证方式；

2、启用 WEB 认证。

【配置方法】

- 进入 WLAN 1 的安全配置模式。
- 配置启用 RSN 认证模式。
- 配置 RSN 认证模式的数据加密方式为 AES。
- 配置 RSN 认证模式的接入认证方式为 PSK。
- 配置 PSK 密码为 12345678。
- 配置单播密钥协商报文重传次数为 5 次。
- 配置 WEB 认证。
- 配置 WEB 认证防抖时间为 900 秒。

AC

```
Ruijie(config)#wlansec 1
Ruijie(config-wlansec)#security rsn enable
Ruijie(config-wlansec)#security rsn ciphers aes enable
Ruijie(config-wlansec)#security rsn akm psk enable
Ruijie(config-wlansec)#security rsn akm psk set-key ascii 12345678
Ruijie(config-wlansec)#authtimeout paircount 5
Ruijie(config-wlansec)#webauth
Ruijie(config-wlansec)#webauth prevent-jitter 900
```

【检验方法】 使用 **show running-config | begin wlansec** *wlan_id* 命令，可以查看配置是否生效。

AC

```
Ruijie#show running-config | begin wlansec 1
wlansec 1
 security rsn enable
 security rsn ciphers aes enable
```

```
security rsn akm psk enable
security rsn akm psk set-key ascii 12345678
webauth prevent-jitter 900
webauth
authtimeout paircount 5
```

常见配置错误

- 未启用 WEB 认证就配置 WEB 认证防抖时间参数。

1.6 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
-	-

查看运行情况

作用	命令
显示 WLAN 的安全配置信息。	**show wlan security** *wlan-id*
查看 STA 的安全配置信息。	**show wclient security** *mac-address*

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
-	-

2 WIDS

2.1 概述

WLAN 具有安装便捷、使用灵活、经济节约和易于扩展等有线网络无法比拟的优点，因此得到越来越广泛的使用。但由于 WLAN 信道开放的特点，使得无线网络很容易受到各种网络威胁的影响，如冒牌的 AP 设备、Ad-hoc 网络、各种针对无线网络的协议攻击等等，因此安全性成为阻碍 WLAN 发展的重要因素。

WIDS（Wireless Intrusion Detection System，无线入侵检测系统）可以对恶意的用户攻击和入侵行为进行早期检测，帮助网络管理者主动发现网络中的隐患，在第一时间对无线攻击者进行主动防御和预警。

下文仅介绍 WIDS 的相关内容。

协议规范

无。

2.2 典型应用

典型应用	场景描述
帧过滤	无线网络中存在意图接入网络的非法用户，WIDS 需要通过帧过滤功能来控制用户的接入
用户隔离	无线网络中存在意图访问其他用户的用户，WIDS 需要通过用户隔离功能来隔离这些用户的直接通讯
IDS 攻击检测	无线网络中存在各种入侵攻击，WIDS 通过 IDS 攻击检测来检测无线入侵攻击
Rogue 设备检测与反制	无线网络中存在一些非法设备，这些非法设备通过提供仿冒的服务来危害用户以及正常服务，WIDS 需要通过 Rogue 设备检测与反制功能来监测和反制非法设备

2.2.1 帧过滤

应用场景

在一个无线网络中提供无线用户接入控制服务，包括允许指定用户接入网络、允许指定用户接入指定网络、禁止用户接入网络、禁止无线用户接入指定网络、禁止低速用户接入网络以及动态控制用户接入网络。

以下图为例，假设网络中存在如下部署要求：

1、 指定用户 Client1 可以接入无线网络，指定用户 Client2 可以接入指定无线网络服务 ssid1。

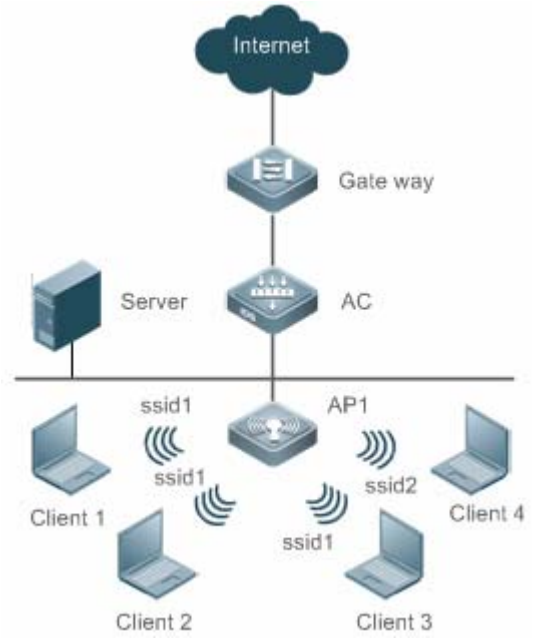
2、 指定用户 Client3 不可以接入无线网络，指定用户 Client4 不可以接入指定无线网络服务 ssid2。

3、 过滤低速用户，剔除低速用户。

4、 动态控制用户接入无线网络。

组网环境如下所示：

图 2-1 无线用户接入控制组网图



功能部属

设备端的配置要点如下：

1. 配置白名单列表表项 Client1，无线用户 Client1 可以接入 AC 下所有 AP 设备提供的无线网络服务，其他未配置到白名单表项的无线用户不能接入 AC 下所有 AP 设备提供的网络服务。
2. 配置基于 ssid1 网络的白名单列表表项 Client2，无线用户 Client2 可以接入 AC 下所有 AP 设备提供的 ssid1 网络，其他未配置在 ssid1 网络的白名单表项的无线用户不能接入 AC 下所有 AP 设备提供的 ssid1 网络。
3. 配置静态黑名单列表表项 Client3，无线用户 Client3 不能接入 AC 下所有 AP 设备提供的无线网络服务。
4. 配置基于 ssid1 网络的黑名单列表表项 Client4，无线用户 Client4 不能接入 AC 下所有 AP 设备提供的 ssid1 网络。
5. 配置低速用户过滤阈值 Rt，所有关联在 AC 下所有 AP 设备的用户的速率阈值低于 Rt，该用户将会被剔除出去
6. 配置动态黑名单功能 ,该功能与入侵攻击检测功能配套使用。开启了动态黑名单功能后 ,如果入侵攻击检测到入侵攻击后，将会添加到动态黑名单列表里面。动态黑名单表项在老化超时时限之内，符合动态黑名单表项的用户将会被禁止继续在当前 AP 设备通信以及接入。

2.2.2 用户隔离

应用场景

无线网络中提供用户二层用户隔离服务，包括：基于 AP 的二层用户隔离、基于 AP-SSID 的二层用户隔离、基于 AC 的二层用户隔离、基于 AC-SSID 的二层用户隔离和基于 SSID 的二层用户隔离。

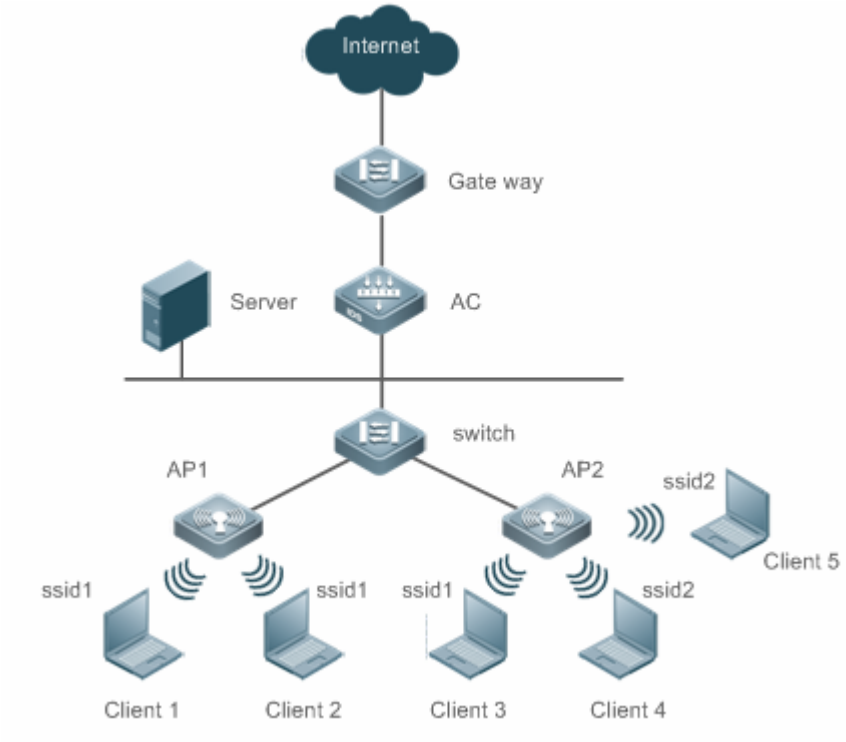
假设网络中存在如下部署要求：

Client1~Client 3 关联在 SSID1 的无线网络中，Client4 和 Client5 关联在 SSID2 的无线网络中，SSID1 与 SSID2 服务映射同一个 VLAN，即 Client1~Client 5 是二层用户。

1. Client1 与 Client 2 不能直接通讯，Client 3 ~ Client5 之间不能直接通信，其他用户间可以直接通信。
2. Client1 与 Client 2 不能直接通讯，Client4 和 Client5 不能直接通信，其他用户间可以直接通信。
3. Client1 不能和 Client3~Client5 直接通信，Client2 不能和 Client3~Client5 间直接通信，其他用户间可以直接通信。
4. Client3 和 Client1、Client2 间不能直接通信，其他用户间可以直接通信。
5. Client1~Client3 之间不能直接通信，其他用户间可以直接通信。

组网环境如下所示：

图 2-2 无线用户隔离场景



功能部属

设备端的配置要点如下：

6. 配置基于 AP 用户隔离，可以实现隔离 Client1 与 Client2 间的直接通信，Client3~Client5 间的直接通信。
7. 配置基于 AP-SSID 用户隔离，可以实现隔离 Client1 与 Client 2 间的直接通信，Client4 与 Client5 间的直接通信。
8. 配置基于 AC 用户隔离，可以实现 Client1 与 Client2 分别不能和 Client3~Client5 间的直接通信。
9. 配置基于 AC-SSID 用户隔离，可以实现 Client3 与 Client1、Client2 间的直接通信。
10. 配置互通基于 SSID1 的用户隔离，Client1~Client3 三者间不能直接进行通信。

2.2.3 IDS攻击检测

应用场景

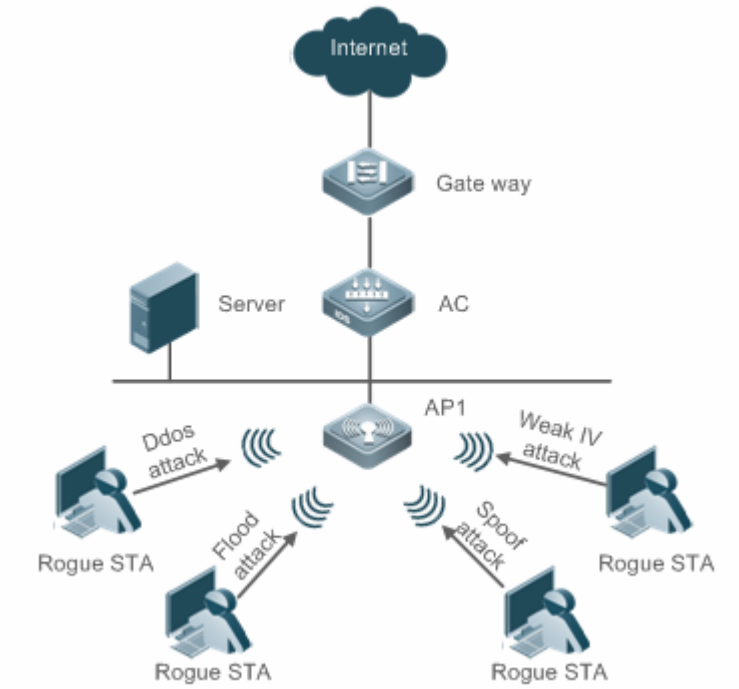
网络中存在无线入侵攻击，包括：DDOS 攻击、Spoof 攻击、Flooding 攻击以及 Weak IV 攻击。AP 设备需要能够检测检到这些攻击以及做相应的应对措施。

假设网络中存在如下部署要求：

11. 网络中存在 DDOS 攻击，需要进行检测防御。
12. 网络中存在 Spoof 攻击，需要进行检测防御。
13. 网络中存在 Flooding 攻击，需要进行检测防御。
14. 网络中存在 Weak IV 攻击，需要进行检测防御。

组网环境如下所示：

图 2-3 入侵攻击检测组网图



功能部属

设备端的配置要点如下：

15. 配置开启 DDOS 攻击检测功能和相关阈值，统计用户的 ARP、SYN、ICMP 攻击报文数量，如果超出阈值，检测结果将记录到日志中，同时动态黑名单开启的情况下，该用户将被添加到动态黑名单列表中。
16. 配置开启 Spoof 攻击检测功能和相关阈值，对用户的广播解认证、解关联报文进行检测，如果超出阈值，检测结果将记录到日志中，同时动态黑名单开启的情况下，该用户将被添加到动态黑名单列表中。。
17. 配置开启 Flooding 攻击检测功能和相关阈值，对用户的认证、关联、重关联、解认证、解关联、探查、空数据和 ACTION 报文进行检测，如果超出阈值，检测结果将记录到日志中，同时动态黑名单开启的情况下，该用户将被添加到动态黑名单列表中。
18. 配置开启 Weak IV 攻击检测功能和相关阈值，对用户的 WEB 报文的 IV 值进行检测，如果连续攻击超过阈值，检测结果将记录到日志中，同时动态黑名单开启的情况下，该用户将被添加到动态黑名单列表中。

2.2.4 Rogue设备检测与反制

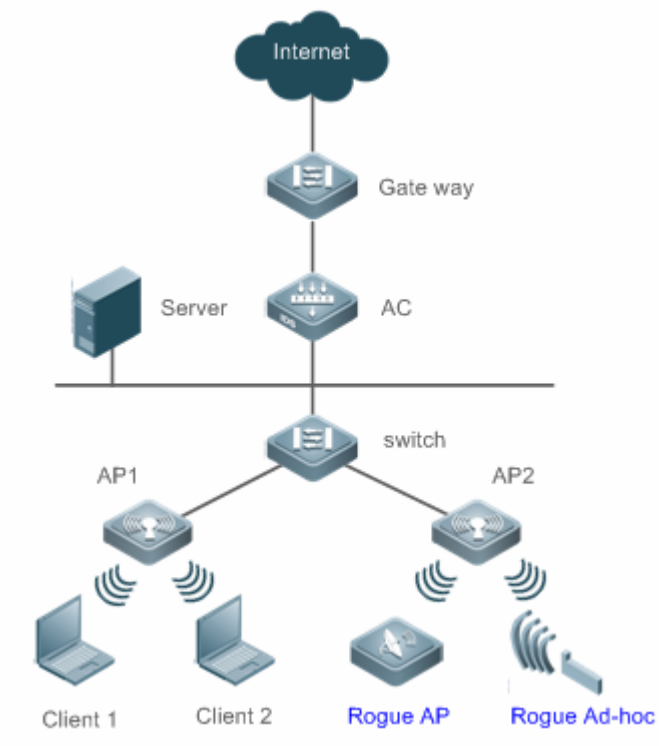
应用场景

假设网络中存在如下部署要求：

1、 网络中存在 Rogue AP 和 Rogue Ad-hoc 设备，需要进行检测和反制。

组网环境如下所示：

图 2-4 Rogue 设备检测与反制组网图



功能部属

设备端的配置要点如下：

19. 配置指定 AP 工作模式为 monitor 或者 hybrid，AP 设备将开启扫描定时器，在每个扫描周期结束后，将会获取扫描数据。
20. 配置开启设备反制功能以及模式相关配置。
21. 根据设备反制模式和扫描数据，定期反制 Rogue AP 和 Rogue Ad-hoc 设备，防止用户关联到假冒的服务上。
22. 配置 AP 反制功能生效之前，需要确认 AP 已经有了 WLAN 服务，这样反制功能才能生效。

2.3 功能详解

基本概念

↘ 工作模式的分类

工作模式可以分为如下三种：

- normal 模式，仅提供接入服务
- monitor 模式，仅提供监测服务

- hybrid 模式，提供监测服务和接入服务

IDS 攻击检测类型

IDS 攻击检测类型有如下五种：

- DDOS 攻击检测，包含检测 ARP、ICMP 以及 SYN 报文的拒绝服务攻击。
- Flooding 攻击检测，包含检测单用户或者多用户的管理报文泛洪攻击。
- Spoof 攻击检测，表示检测广播解除关联和解除认证攻击。
- Weak IV 攻击检测，表示检测弱向量攻击。
- 互通防 DOS 攻击检测

用户隔离模式

用户隔离模式有如下五种：

- 基于 AC 二层用户隔离，同 AC 下不同 AP 间的二层用户通讯隔离。
- 基于 AP 二层用户隔离，同 AP 下的二层用户通讯隔离。
- 基于 AC-SSID 二层用户隔离，同 AC 下不同 AP 间相同 WLAN 下的二层用户隔离。
- 基于 AP-SSID 二层用户隔离，同 AP 下相同 WLAN 下的二层用户隔离。
- 互通二层用户隔离，指定 WLAN 下二层用户隔离。

Rogue 设备反制模式

Rogue 设备反制模式有如下四种：

- Adhoc 反制模式，反制 Rogue Ad-hoc 设备。
- Rogue 反制模式，反制信号强度超过阈值的 Rogue 设备。
- SSID 反制模式，反制 SSID 一样的非法设备。
- Config 反制模式，反制与静态攻击列表或者 SSID 黑名单中一样的非法设备。

Rogue 设备检测分类

Rogue 设备检测分类如下：

- AP 设备
- Ad-hoc 设备
- 未知名 STA 设备

功能特性

功能特性	作用
帧过滤	通过一定的帧过滤规则判定是否允许指定无线客户端的报文通过，实现了对无线终端用户的接入控制

IDS 攻击检测	及时发现并防御 WLAN 网络中恶意或者无意的攻击
用户隔离	控制在无线网络覆盖区域中，无线终端之间的不安全访问，避免私人信息遭到他人窃取。
Rogue 设备检测与反制	Rogue 设备检测功能，可以对整个 WLAN 网络中的异常设备进行监视，帮助网络管理者发现网络中的隐患。 Rogue 设备反制是使用攻击列表中的 Rogue 设备的地址发送假的解除认证帧来对 Rogue 设备进行反制。

2.3.1 帧过滤

用于对无线终端用户的接入控制，主要包括：低速用户过滤、白名单列表、静态黑名单列表、动态黑名单列表、基于 SSID 的白名单和基于 SSID 的黑名单。

工作原理

↘ 低速用户过滤

低速用户过滤主要通过低速用户过滤阈值，当阈值大于 0 的时候，表示低速用户过滤功能开启。如果用户的速率低于该阈值，用户的报文将被丢弃，同时用户将被剔除出设备。

↘ 白名单列表

白名单列表中包含了允许接入的无线客户端的 MAC 地址，如果启用了白名单功能，则只有白名单中指定的无线用户可以接入到 WLAN 网络中，其他的无线用户的所有报文都将被 AP 直接丢弃，从而减少非法报文对无线网络的冲击。

↘ 静态黑名单列表

静态黑名单列表中包含了拒绝接入的无线客户端的 MAC 地址，如果启用了静态黑名单功能，则黑名单中指定的无线用户的所有报文都将被 AP 丢弃。

↘ 动态黑名单列表

动态黑名检单列表中包含了拒绝接入的无线客户端的 MAC 地址，可以在 WIDS 检测到 IDS 攻击时动态添加以及手动配置动态黑名单。当 WLAN 测到来自某一终端设备的无线入侵攻击时，可以选择将该设备的 MAC 地址动态加入到黑名单中，禁止接收任何来自于该设备的报文，实现 WLAN 网络的安全保护。

↘ 基于 SSID 的白名单列表

基于 SSID 白名单列表包含了指定 SSID 允许接入的无线客户端的 MAC 地址，用户可以通过命令行进行配置。如果启用了基于 SSID 白名单功能，则在该 SSID 子集内，只有白名单中指定的无线用户可以接入，其他无线用户的所有报文都将被 AP 直接丢弃，从而减少非法报文对无线网络的冲击。

↘ 基于 SSID 的黑名单列表

基于 SSID 黑名单列表包含了指定 SSID 拒绝接入的无线客户端的 MAC 地址，用户可以通过命令行进行配置。如果启用了基于 SSID 黑名单功能，则在该 SSID 子集内，黑名单中指定的无线用户的所有报文都将被 AP 丢弃。

2.3.2 IDS攻击检测

为了及时发现并防御 WLAN 网络中恶意或者无意的攻击，WIDS 支持对多种攻击行为进行检测。当 WIDS 检测到攻击后，会产生告警或者日志信息，提醒网络管理者进行相应处理。根据检测的结果，网络管理员可以及时调整网络的配置，清除 WLAN 网络的不安全因素。

目前设备支持的 IDS 攻击检测有以下五种：

- DDOS 攻击检测（分布式拒绝服务攻击检测）
- Flooding 攻击检测（泛洪攻击检测）
- Spoof 攻击检测（欺骗攻击检测）
- Weak IV 检测（弱初始化向量检测）
- 互通防 DOS 攻击检测

工作原理

DDOS 攻击检测

DDOS 攻击是指攻击者在短时间内向目标设备发送大量的攻击报文(目前识别 ARP 报文、ICMP 报文、SYN 报文)，从而影响合法用户关联到被攻击设备。

WIDS 的 DDOS 检测功能通过对攻击者的报文进行统计，通过判断报文的 PPS（每秒报文数）是否超出配置阈值，如果超出会将这个检测结果记录到日志中。如果开启动态黑名单功能，则将攻击者加入动态黑名单链表中。

Flooding 攻击检测

Flooding（泛洪）攻击是指攻击者在短时间内发送大量的同种类型的报文，导致 WLAN 设备被攻击者发送的泛洪报文淹没而无法处理真正正当的用户请求。

WIDS 攻击检测通过持续地监控每台设备的流量大小来预防这种泛洪攻击。在规定时间内，当流量超出网络管理者设置的上限时，该设备被认为正在进行网络泛洪攻击从而被锁定。Flooding 攻击检测可以和动态黑名单功能配合使用，当 WIDS 检测到 Flooding 攻击时，此时如果开启了动态黑名单功能，则发起攻击的无线客户端将被添加到动态黑名单中，从而保证 WLAN 系统不会再次被该设备攻击，保障网络安全。

Spoof 攻击检测

Spoof（欺骗）攻击是指攻击者以其他设备的名义发送仿冒报文。例如：一个仿冒的解除认证报文会导致无线客户端下线。

WIDS 通过对广播解除认证和广播解除关联报文进行检测，当接收到这类报文时将立刻被定义为欺骗攻击并被记录到日志中。

Weak IV 攻击检测

Weak IV（Weak Initialization Vector，弱初始化向量）攻击是指在 WLAN 使用 WEP 加密的过程中，攻击者通过截获带有弱初始化向量的报文，破解出共享密钥并最终窃取加密信息的一种攻击行为。

WLAN 使用 WEP 进行加密的时候，对于每一个报文都会产生一个 IV，IV 和共享密钥一起作为输入来生成密钥串。密钥串同明文加密，最终生成密文。当一个 WEP 报文被发送时，用于加密报文的 IV 也作为报文头的一部分被发送。如果使用不安全

的方法生成 IV，例如频繁生成重复的 IV 甚至是始终生成相同的 IV，就会轻易暴露共享密钥。如果潜在的攻击者获得了共享的密钥，攻击者将能够控制网络资源，对网络安全造成威胁。

WIDS 通过识别每个 WEP 报文的 IV 来预防这种攻击，当一个带有弱初始化向量的报文被检测到时，WIDS 即判定这是个攻击漏洞，将立刻将这个检测结果记录到日志中。

↘ 互通防 DOS 攻击检测

互通的防 DOS 攻击检测指的是对于每个接入或尝试加入的 STA，如果在指定时间内发现接收到的 Action、Association、Authentication、Deauthentication、Disassociation、Reassociation、Probe Request、Null data 报文数大于设定的阈值，就认为存在攻击。

2.3.3 用户隔离

由于无线用户的流动性和不确定性，在某些场合（特别是在公共场合），用户信息的私密性显得尤为重要，需要限制用户之间直接访问。用户隔离技术可以控制在无线网络覆盖区域中，无线终端之间的不安全访问（例如无线上网用户之间通过网上邻居访问），避免私人信息遭到他人窃取。

用户隔离功能在不影响用户正常上网的情况下对用户进行隔离，使之不能互访，保证了用户业务的安全。用户隔离功能分成以下五种：

- 基于 AP 的二层用户隔离
- 基于 AP-SSID 的二层用户隔离
- 互通二层用户隔离

工作原理

↘ 基于 AP 的二层用户隔离

关联到同一个 AP 上的所有二层用户之间不能直接进行通讯。

↘ 基于 AP-SSID 的二层用户隔离

关联到同一 AP 上的同一个 WLAN 下的用户之间不能直接进行通讯。

↘ 基于 AC 的二层用户隔离

关联到同一 AC 不同 AP 上的所有二层用户之间不能直接进行通讯，仅在集中转发模式下有效。

↘ 基于 AC-SSID 的二层用户隔离

关联到同一 AC 不同 AP 上的同一个 WLAN 下的用户之间不能直接进行通讯，仅在集中转发模式下有效。

↘ 互通二层用户隔离

互通的二层隔离功能指的是基于 SSID 的二层隔离功能要求，本地转发模式下在 AP 端生效。

2.3.4 Rogue设备检测与反制

一般可以把网络中的设备分为两种类型：非法设备（Rogue 设备）和合法设备。Rogue 设备可能存在安全漏洞或被攻击者操纵，因此会对用户网络的安全造成严重威胁或危害。WIDS 的 Rogue 设备检测功能，可以对整个 WLAN 网络中的异常设备进行监视，帮助网络管理者发现网络中的隐患。

Rogue 设备检测可以检测 WLAN 中多种 Rogue 设备：Rogue AP，Rogue Client，Rogue 无线网桥，Ad-hoc 网络等。目前，仅支持对 Rogue AP 和 Ad-hoc 网络的检测以及未知名 STA 的检测。

Rogue 设备反制是使用 Rogue 设备的地址发送假的解除认证帧来对 Rogue 设备进行反制，防止用户接入非法的服务或者非法的用户接入设备。

工作原理

Rogue 设备检测

Rogue 设备检测功能是由工作在监听模式或者混合模式下的 AP 进行检测的。WIDS 通过在无线网络中部署一些 AP 并设置它们工作在监听或者混合模式，捕捉空气介质中的无线报文。通过对监听到的无线报文进行分析统计，AP 就可以获取到 Rogue 设备的信息。同时，网络管理员还可以通过制定非法设备的检测规则，对整个 WLAN 网络中的异常设备进行监视。

未知名 STA 检测

未知名 STA 检测功能是对网络中非已接入用户的探测请求报文进行监测，同时网络管理员还可以通过配置来指定未知名 STA 信息。

Rogue 设备反制

Rogue 设备反制指的是通过模拟假的广播解除认证报文来反制符合反制模式规则的 Rogue 设备，反制正常用户接入 Rogue 设备的服务。

未知名 STA 反制

未知名 STA 反制指的是直接构造解除认证报文来防止未知名的 STA 的接入。

互通非法 AP 检测

互通的非法 AP 检测功能目的是为了防止非法 AP 对合法 AP 的信号传输产生干扰，甚至欺骗合法用户骗取用户的注册信息。互通非法 AP 检测功能应该具有非法 AP 检测的功能，并能在有条件的情况下，通过与后台系统配合，切断非法 AP 的网络连接。

2.4 产品说明



NBR800G、NBR950G、NBR1500G、NBR2000G 不支持无线集成 AC 功能，NBR108G-P、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持无线集成 AC 功能。

2.5 配置详解

配置项	配置建议&相关命令	
配置帧过滤功能	可选配置，用于设置帧过滤功能的配置	
	kickout threshold	配置低速用户过滤阈值
	whitelist mac-address	配置白名单列表表项
	whitelist max	配置白名单列表长度
	static-blacklist mac-address	配置静态黑名单列表表项
	static-blacklist max	配置静态黑名单列表长度
	dynamic-blacklist enable	配置动态黑名单功能
	dynamic-blacklist lifetime	配置动态黑名单表项生存时间
	dynamic-blacklist ac-max	配置动态黑名单列表 AC 端长度
	dynamic-blacklist ap-max	配置动态黑名单列表 AP 端长度
	dynamic-blacklist mac-address	配置动态黑名单列表表项
	ssid-filter max	配置基于 SSID 的黑、白名单和 SSID 列表长度
	ssid-filter blacklist mac-address	配置基于 SSID 的黑名单列表表项
	ssid-filter blacklist max	配置基于 SSID 的黑名单列表长度，默认 256
	ssid-filter whitelist mac-address	配置基于 SSID 的白名单列表表项
	ssid-filter whitelist max	配置基于 SSID 的白名单列表长度，默认 256
配置 IDS 攻击检测功能	可选配置，用于配置 IDS 攻击检测配置	
	attack-detection enable	配置 IDS 攻击检测功能的检测类型
	attack-detection ddos	配置 ddos 攻击检测周期时长和指定类型报文的报文检测阈值
	attack-detection flood multi-mac	配置 flood 攻击检测的多用户攻击检测阈值和周期检测时长
	attack-detection flood single-mac	配置 flood 攻击检测的单用户攻击检测阈值和周期检测时长
	attack-detection spoof	配置 spoof 攻击检测报文阈值和检测周期时长
	attack-detection weak-iv	配置 weak-iv 攻击检测报文阈值和检测周期时长

	attack-detection statistics ac-max	配置 IDS 攻击检测统计列表 AC 端长度
	attack-detection statistics ap-max	配置 IDS 攻击检测统计列表 AP 端长度
	dos-detection	配置开启互通防 dos 攻击检测功能或者互通防 dos 攻击相关阈值信息
配置用户隔离功能	⚠ 可选配置，用于设置用户隔离功能功能	
	user-isolation enable	配置使能基于 ap、基于 ap-ssid 和互通二层用户隔离功能模式
	user-isolation permit-mac	配置隔离允许 MAC 列表表项
	user-isolation permit-mac max	配置隔离允许 MAC 列表长度
配置 Rogue 设备检测与反制	⚠ 可选择配置，用于设置设备检测与反制功能	
	countermeasures enable	配置使能设备反制功能
	countermeasures ap-max	配置单次反制的设备数量
	countermeasures channel-match	配置使能基于信道反制
	countermeasures interval	配置反制周期时长
	countermeasures mode	配置反制模式
	countermeasures rssi-min	配置反制的信号强度下限
	device aging duration	配置检测到的设备生存时间
	device attack mac-address	配置静态攻击列表表项
	device attack max	配置静态攻击列表长度
	device black-ssid	配置 SSID 黑名单列表表项
	device max-black-ssid	配置 SSID 黑名单列表长度
	device friendly-flags	配置设备友好标识
	device permit mac-address	配置允许 MAC 列表表项
	device permit mac-address max	配置允许 MAC 列表长度
	device permit ssid	配置允许 SSID 列表表项
	device permit max-ssid	配置允许 SSID 列表长度
	device permit vendor bssid	配置允许产商列表表项
	device permit vendor bssid max	配置允许产商列表长度
	device unknown-sta dynamic-enable	配置使能未知名 STA 功能
	device unknown-sta mac-address	配置未知名 STA 列表表项
	device unknown-sta mac-address max	配置未知名 STA 列表长度
	device channel-bind radio	配置指定 radio 扫描信道信息
	device scan-para	配置互通非法 AP 检测扫描参数
	device detected-ap-max	配置扫描 AP 检测名单最大个数
	hybrid-scan radio	配置指定 radio 的扫描状态
	scan-channels { 802.11a | 802.11b } channels	配置指定 AP 的扫描信道
	rogue-ap countermeasures enable	配置互通非法 AP 反制功能

配置 AP 工作模式	可选配置，用于设置 AP 工作模式	
	device mode	配置 AP 工作模式

2.5.1 配置帧过滤功能

配置效果

- 配置帧过滤规则，提供报文过滤服务。

注意事项

- 同一个配置信息不能同时在静态黑名单列表和白名单列表中存在。
- 同一个配置信息不能同时在同一个 SSID 的黑名单列表和白名单列表中存在。

配置方法

配置低速用户过滤功能

- 可选配置，使用 **kickout threshold** 命令在 WIDS 配置模式下配置低速用户过滤阈值。配置了低速用户过滤阈值（阈值>0）后，低速用户过滤功能才能够有效运行。
- 若无特殊要求，该功能仅在需要支持低速用户过滤功能的 AC 设备上启动。

【命令格式】 **kickout threshold** *rate*
【参数说明】 *rate*：低速用户过滤阈值，可配置范围 0~130Mbps
【缺省配置】 默认情况下不过滤低速用户，速率阈值为 0
【命令模式】 WIDS 配置模式
【使用指导】 用户可以根据需要选择不同低速用户过滤阈值。

配置白名单功能

- 可选配置。
- 若无特殊要求，该功能仅在需要白名单功能的 AC 设备上启动。
- 配置白名单列表表项，同上。
- 配置白名单列表长度，同上。
- 使用 **whitelist mac-address** 命令在 WIDS 配置模式下配置白名单列表的单个表项信息。配置了有效的白名单表项后，白名单列表过滤功能才能够有效运行。
- 使用 **whitelist max** 命令在 WIDS 配置模式下配置白名单列表的表项个数上限 ,表示设备上允许配置的白名单表项个数上限。

【命令格式】 **whitelist** { **mac-address** *H.H.H* | **max** *num* }

【参数说明】 **mac-address** *H.H.H*：白名单列表表项 mac 地址

max *num*：白名单列表长度，可配置范围 1~2048。

【缺省配置】 缺省情况下白名单列表为空，白名单列表长度默认为 1024

【命令模式】 WIDS 配置模式

【使用指导】 白名单列表中存在表项时，白名单功能才生效。

配置静态黑名单功能

- 可选配置。
- 若无特殊要求，该功能仅在需要静态黑名单功能的 AC 设备上启动。
- 配置静态黑名单列表表项，同上。
- 配置静态黑名单列表长度，同上。
- 使用 **static-blacklist mac-address** 命令在 WIDS 配置模式下配置静态黑名单列表的单个表项信息。配置了有效的静态黑名单表项后，静态黑名单列表过滤功能才能够有效运行。
- 使用 **static-blacklist max** 命令在 WIDS 配置模式下配置静态名单列表的表项个数上限，表项设备上允许的静态黑名单最多配置个数上限。

【命令格式】 **static-blacklist** { **mac-address** *H.H.H* | **max** *num* }

【参数说明】 **mac-address** *H.H.H*：静态黑名单列表表项 mac 地址

max *num*：静态黑名单列表长度，可配置范围 1~2048。

【缺省配置】 缺省情况下静态黑名单列表为空，静态黑名单列表长度默认为 1024

【命令模式】 WIDS 配置模式

【使用指导】 静态黑名单列表中存在表项时，静态黑名单功能才生效。

配置动态黑名单功能

- 可选配置。
- 若无特殊要求，该功能仅在需要动态黑名单功能的 AC 设备上启动。
- 使用 **dynamic-blacklist enable** 命令在 WIDS 配置模式下配置开启动态态黑名单列表过滤功能。开启了动态黑名单过滤功能后，动态黑名单的表项才会随着 IDS 攻击检测动态生成，同时动态黑名单列表过滤功能才会运行。
- 使用 **dynamic-blacklist lifetime** 命令在 WIDS 配置模式下配置动态态名单列表的生存时长，表示动态生成的动态黑名单表项信息可以在设备在存在多长时间。
- 使用 **dynamic-blacklist** { **ac-max** | **ap-max** }命令在 WIDS 配置模式下配置动态黑名单在 AC 端和 AP 端的表项个数上限，表项 AC 端设备或者 AP 端设备最多允许的表项个数上限。
- 使用 **dynamic-blacklist mac-adress** 命令在 WIDS 配置模式下配置动态黑名单表项名单。

【命令格式】 **dynamic-blacklist** { **enable** | **lifetime** *time* | **ac-max** *num* | **ap-max** *num* | **mac-address** *H.H.H* }

【参数说明】 **enable**：使能动态黑名单功能

lifetime *time*：动态黑名单列表生存时间，配置范围 60~86400s。

ac-max *num*：动态黑名单列表 AC 端长度

ap-max *num*：动态黑名单列表 AP 端长度

mac-address *H.H.H*：动态黑名单列表表项 mac 地址

【缺省配置】 缺省情况动态黑名单功能关闭，动态黑名单列表端长度黑认为 2048，AP 端长度默认为 2048，动态黑名单生存时间 300s

【命令模式】 WIDS 配置模式

【使用指导】 动态黑名单列表表项在 IDS 攻击检测功能中生成。

配置基于 SSID 的黑名单功能

- 可选配置。
- 若无特殊要求，该功能仅在需要基于 SSID 的黑名单功能的 AC 设备上启动。
- 配置基于 SSID 的黑名单列表，同上。
- 配置基于 SSID 的黑名单列表长度，同上。
- 配置 SSID 列表长度，同上。
- 使用 **ssid-filter blacklist mac-address** 命令在 WIDS 配置模式下配置基于 ssid 的静态黑名单列表的单个表项信息。配置了有效的静态黑名单表项后，静态黑名单列表过滤功能才能够有效运行。
- 使用 **ssid-filter blacklist max** 命令在 WIDS 配置模式下配置基于 ssid 的静态名单列表的表项个数上限 ,表项设备上允许的静态黑名单最多配置个数上限。

【命令格式】 **ssid-filter** { **max** *num* | **blacklist mac-address** *H.H.H* **in-ssid** *string* | **blacklist max** *num* }

【参数说明】 **max** *num*：SSID 列表的最大长度，可配置范围 1 ~ 128

blacklist mac-address *H.H.H* **in-ssid** *string*：配置指定 SSID 的黑名单列表表项

blacklist max *num*：配置基于 SSID 的黑名单列长度，可配置范围 1~256

【缺省配置】 基于 SSID 的黑名单列表为空

【命令模式】 WIDS 配置模式

【使用指导】 基于 SSID 的黑名单列表中存在表项时，功能才生效

配置基于 SSID 的白名单功能

- 可选配置。
- 若无特殊要求，该功能仅在需要基于 SSID 的白名单功能的 AC 设备上启动。
- 配置基于 SSID 的白名单列表，同上。
- 配置基于 SSID 的白名单列表长度，同上。
- 使用 **ssid-filter whitelist mac-address** 命令在 WIDS 配置模式下配置基于 ssid 的白名单列表的单个表项信息。配置了有效的白名单表项后，白名单列表过滤功能才能够有效运行。
- 使用 **ssid-filter whitelist max** 命令在 WIDS 配置模式下配置基于 ssid 的白名单列表的表项个数上限 ,表示设备上允许配置的白名单表项个数上限。

【命令格式】 **ssid-filter** { **whitelist mac-address** *H.H.H* **in-ssid** *string* | **whitelist max** *num* }

【参数说明】 **whitelist mac-address** *H.H.H* **in-ssid** *string*：配置指定 SSID 的白名单列表表项

whitelist max *num*：配置基于 SSID 的白名单列长度，可配置范围 1~256

【缺省配置】 基于 SSID 的白名单列表为空

【命令模式】 WIDS 配置模式

【使用指导】 基于 SSID 的白名单列表中存在表项时，功能才生效

检验方法

根据相应的帧过滤规则，进行相关的功能验证。

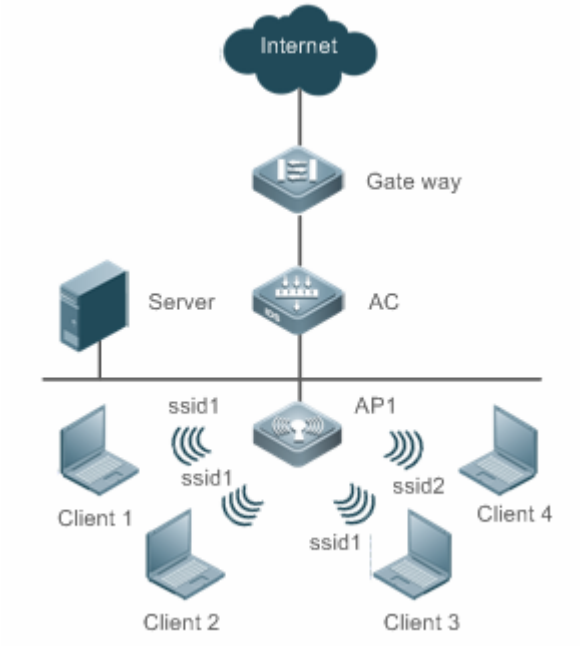
- 检测低速用户过滤功能，报文丢弃，低速用户成功被剔除。
- 检测白名单功能，白名单列表中存在配置时，非白名单列表中的用户无法加入 AP。
- 检测静态黑名单功能，静态黑名单中存在配置时，静态黑名单列表中的用户无法加入 AP。
- 检测动态黑名单功能，动态黑名单功能开启时，动态黑名单列表中的表项能够随着 IDS 攻击检测动态生成，在动态黑名单中的用户不能再次加入 AP。
- 检测基于 SSID 的黑名单功能，基于 SSID 的黑名单存在配置时，基于 SSID 的黑名单列表中的用户无法加入该 SSID 服务。
- 检测基于 SSID 的白名单功能，基于 SSID 的白名单存在配置时，非基于 SSID 的白名单列表中的用户无法加入该 SSID 服务。

配置举例

↘ 配置白名单表项

【网络环境】

图 2-5



【配置方法】

- 在 AC 设备上面配置白名单表项

```
Ruijie# configure terminal
```

```
Ruijie(config)# wids
Ruijie(config-wids)# whitelist mac-address 0000.0000.0001
```

【检验方法】 用户配置了白名单表项后，可以通过以下方式来难是否已经配置成功。

- 通过 show wids whitelist 命令可以查看用户配置的相关参数信息。
- 通过设备验证功能是否已经生效。

```
Ruijie#show wids whitelist
------------------     Whitelist Information     ------------------
num      Mac-address
1        0000.0000.0001
```

常见错误

无。

2.5.2 配置IDS攻击检测功能

配置效果

- 通过 IDS 攻击检测功能，可以及时发现并防御 WLAN 网络中恶意或者无意的攻击。

注意事项

- IDS 攻击检测功能需要和动态黑名单功能配置使用，这样可以更有效防止 WLAN 网络的攻击。

配置方法

↘ 配置使能 IDS 攻击检测类型

- 可选配置，缺省情况下 IDS 攻击检测类型未开启。
- 若无特殊要求，在需要 IDS 攻击检测功能的 AC 设备上配置该功能。
- 配置 IDS 攻击检测类型，同上。

【命令格式】 **attack-detection enable** { **all** | **ddos** | **flood** | **spoof** | **weak-iv** }

【参数说明】 **ddos**：配置 DDOS 攻击检测功能，默认关闭

flood：配置 Flooding 攻击检测功能，默认关闭

spoof：配置 Spoof 攻击检测功能，默认关闭

weak-iv：配置 Weak IV 攻击检测功能，默认关闭

all：配置开启所有 IDS 攻击检测类型，默认关闭

【缺省配置】 IDS 攻击检测的四种检测类型默认关闭

【命令模式】 WIDS 配置模式

【使用指导】 -

配置 DDOS 攻击检测

- 可选配置。
- 若无特殊要求，在需要 DDOS 攻击检测功能的 AC 设备上配置该功能。
- 配置 DDOS 攻击检测指定类型报文阈值和周期时长，同上。

【命令格式】 **attack-detection ddos** { **arp-threshold** *num* | **icmp-threshold** *num* | **syn-threshold** *num* | **interval** *time* }

【参数说明】 **arp-threshold** *num*：arp 报文阈值，可配置范围 1 ~ 10000pps

icmp-threshold *num*：icmp 报文阈值，可配置范围 1 ~ 10000pps

syn-threshold *num*：syn 报文阈值，可配置范围 1 ~ 10000pps

interval *time*：ddos 攻击检测周期，可配置范围 10~60s

【缺省配置】 缺省情况下，DDOS 攻击检测周期为 30s，对应的三种 DDOS 攻击检测阈值分别：arp 报文为 5pps，icmp 报文为 100pps，syn 报文为 5pps

【命令模式】 WIDS 配置模式

【使用指导】 -

配置 Flooding 攻击检测

- 可选配置，缺省情况下 Flooding 攻击检测功能未开启。
- 若无特殊要求，在需要 Flooding 攻击检测功能的 AC 设备上配置该功能。
- 配置 Flooding 攻击检测指定类型报文阈值和周期时长，同上。
- 使用 **attack-detection flood single-mac** { **total** | **assoc** | **reassoc** | **disassoc** | **probe** | **action** | **auth** | **deauth** | **null-data** } **threshold** *num* **interval** *time* 命令在 WIDS 配置模式下配置单用户的 flood 攻击的指定类型报文阈值和周期时长。
- 使用 **attack-detection flood multi-mac** { **assoc** | **reassoc** | **disassoc** | **probe** | **action** | **auth** | **deauth** | **null-data** } **threshold** *num* **interval** *time* 命令在 WIDS 配置模式下配置多用户的 flood 攻击的指定类型报文阈值和周期时长。

【命令格式】 **attack-detection flood single-mac** { **total** | **assoc** | **reassoc** | **disassoc** | **probe** | **action** | **auth** | **deauth** | **null-data** } **threshold** *num* **interval** *time*

【参数说明】 **single-mac**：单用户检测

total：全部报文

assoc：关联报文

reassoc：重关联报文

disassoc：解关联报文

probe：探测报文

action：action 报文

auth：认证报文

deauth：解认证报文
null-data：空数据报文
num：报文攻击检测阈值，可配置范围 1~5000
time：报文攻击检测周期，可配置范围 10~60s

【缺省配置】 所有 flood 攻击检测的报文阈值，单用户时默认 300，多用户默认 500，统计周期默认 10s
【命令模式】 WIDS 配置模式
【使用指导】 -

【命令格式】 **attack-detection flood multi-mac** { **assoc** | **reassoc** | **disassoc** | **probe** | **action** | **auth** | **deauth** | **null-data** } **threshold** *num* **interval** *time*
【参数说明】 **multi-mac**：多用户检测
assoc：关联报文
reassoc：重关联报文
disassoc：解关联报文
probe：探测报文
action：action 报文
auth：认证报文
deauth：解认证报文
null-data：空数据报文
num：报文攻击检测阈值，可配置范围 1~5000
time：报文攻击检测周期，可配置范围 10~60s
【缺省配置】 所有 flood 攻击检测的报文阈值，单用户时默认 300，多用户默认 500 统计周期默认 10s。
【命令模式】 WIDS 配置模式
【使用指导】 -

配置 Spoof 攻击检测

- 可选配置，缺省情况下 Spoof 攻击检测功能未开启。
- 若无特殊要求，在需要 Spoof 攻击检测功能的 AC 设备上配置该功能。
- 配置 Spoof 攻击检测指定类型报文阈值和周期时长，同上。

【命令格式】 **attack-detection spoof** { **threshold** *num* **| interval** *time* }
【参数说明】 **threshold** *num*：Spoof 攻击检测报文阈值可配置范围 1~1000
interval *time*：Spoof 攻击检测报文周期，可配置范围 10~60s
【缺省配置】 默认报文阈值为 1，默认检测周期为 50s
【命令模式】 WIDS 配置模式
【使用指导】 -

配置 Weak IV 攻击检测

- 可选配置，缺省情况下 Weak IV 攻击检测功能未开启。
- 若无特殊要求，在需要 Weak IV 攻击检测功能的 AC 设备上配置该功能。

- 配置 Weak IV 攻击检测指定类型报文阈值和周期时长，同上。

【命令格式】 **attack-detection weak-iv** { **threshold** *num* | **interval** *time* }
【参数说明】 **threshold** *num*：Weak IV 攻击检测报文阈值，可配置范围 1～10000
interval *time*：Weak IV 攻击检测周期，可配置范围 1～60s
【缺省配置】 Weak IV 的默认检测周期时长为 15s，默认检测阈值为 10
【命令模式】 WIDS 配置模式
【使用指导】 -

配置互通防 Dos 攻击检测

- 可选配置，缺省情况下互通防 Dos 攻击检测功能未开启。
- 若无特殊要求，在需要 Weak IV 攻击检测功能的 AC 设备上配置该功能。
- 配置互通防 Dos 攻击检测指定类型报文阈值和周期时长，同上。

【命令格式】 **dos-detection** { **enable** | **threshold** *num* | **interval** *time* }
【参数说明】 **enable**：使能互通防 Dos 攻击检测
threshold *num*：互通防 Dos 攻击检测报文阈值，可配置范围 1～5000
interval *time*：互通防 Dos 攻击检测周期，可配置范围 1000～60000ms
【缺省配置】 互通防 DOS 攻击检测周期时长为 1000ms，默认检测阈值为 30
【命令模式】 WIDS 配置模式
【使用指导】 -

检验方法

根据相应的 IDS 攻击检测类型。

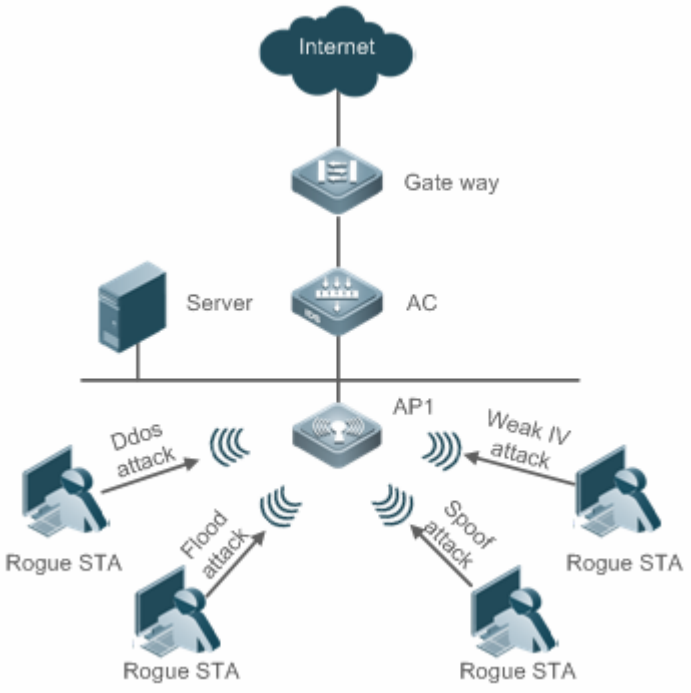
- DDOS 攻击检测功能，检测 arp 报文攻击、icmp 报文攻击和 syn 报文攻击。
- Flooding 攻击检测功能，检测多用户泛洪攻击和单用户泛洪攻击。
- Spoof 攻击检测功能，检测广播解关联和解认证报文攻击。
- Weak IV 攻击检测功能，检测弱初始化向量报文攻击。
- 互通防 Dos 攻击检测功能，检测 Dos 攻击。

配置举例

配置 DDOS 攻击检测功能

【网络环境】

图 2-6



【配置方法】

- 在 AC 设备上面配置 DDOS 攻击检测类型和相关阈值

```
Ruijie# configure terminal
Ruijie(config)# wids
Ruijie(config-wids)# attack-detection enable flood
Ruijie(config-wids)# attack-detection ddos interval 10
```

【检验方法】

- 如果存在 DDOS 攻击，那 AC 设备上将打印相关的 syslog 信息。

```
*Feb  7 13:37:03: %WIDS-6-ATTACK: Client(0025.64b8.2ffa): ARP DDOS attack to Ap (1414.0902.0016).
Feb  7 13:37:03: %WIDS-6-ATTACK: Client(0025.64b8.2ffa): ICMP DDOS attack to Ap (1414.0902.0016).
Feb  7 13:37:03: %WIDS-6-ATTACK: Client(0025.64b8.2ffa): SYN DDOS attack to Ap (1414.0902.0016).
```

常见错误

无。

2.5.3 配置用户隔离功能

配置效果

- 配置用户隔离功能后，符合用户隔离规则的用户将不能直接通信。

注意事项

- 用户隔离功能仅针对二层用户进行隔离

配置方法

配置隔离模式

- 可选配置。
- 若无特殊要求，在需要隔离功能的 AC 设备配置该功能。

【命令格式】 **user-isolation** { **ap** | **ssid-ap** | **wlan-id** *num* } **enable**

【参数说明】 **ap** :基于 AP 二层用户隔离

ssid-ap :基于 AP-SSID 二层用户隔离

wlan-id *num* :互通二层用户隔离，使能指定 wlan-id（ssid）互通的二层用户隔离功能

【缺省配置】 默认关闭

【命令模式】 WIDS 配置模式

【使用指导】 基于 AC 二层用户隔离和基于 AC-SSID 二层用户隔离仅在集中转发模式下有效。

配置隔离允许 MAC 列表

- 可选配置。
- 若无特殊要求，在需要隔离允许 MAC 列表的 AC 设备上配置该信息。
- 配置隔离列表长度，同上。

【命令格式】 **user-isolation permit-mac** { *H.H.H* | **max** *num* }

【参数说明】 *H.H.H*：隔离允许 MAC 列表表项信息

max *num*：隔离允许 MAC 列表长度，可配置范围 1 ~ 1024

【缺省配置】 用户隔离允许 MAC 列表为空，默认隔离允许 MAC 列表长度为 1024

【命令模式】 WIDS 配置模式

【使用指导】 -

检验方法

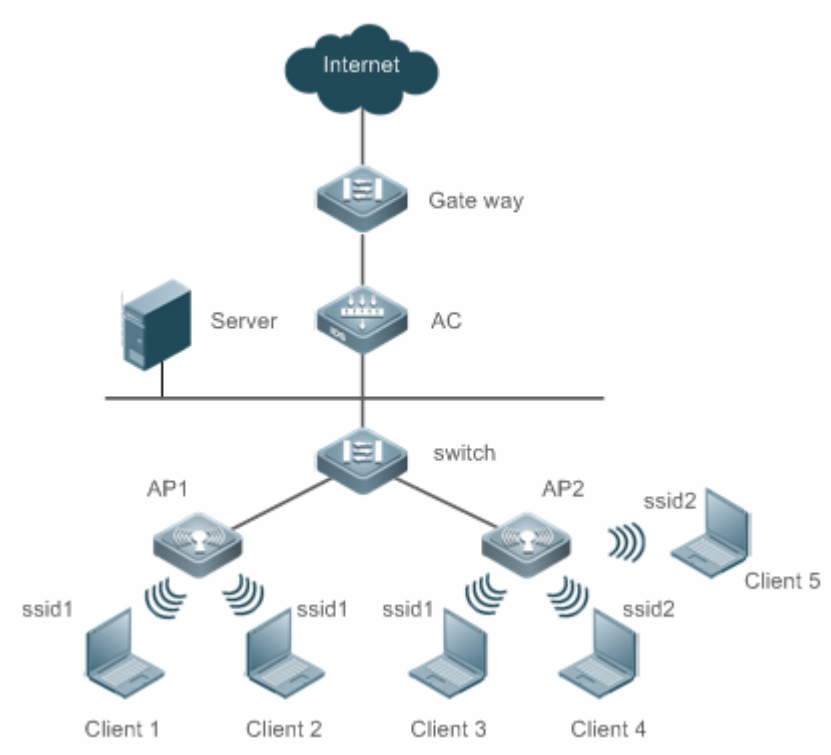
- 根据隔离模式进行相关验证。

配置举例

配置系统日志输出到监视终端

【网络环境】

图 2-7



【配置方法】

- 在 AC 设备上面配置基于 AP 二层用户隔离

```
Ruijie# configure terminal
Ruijie(config)# wids
Ruijie(config-wids)# user-isolation ap enable
```

【检验方法】

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

```
Ruijie#show running-config
…
!
wids
 user-isolation ap enable
!
```

常见错误

无

2.5.4 配置Rogue设备检测与反制

配置效果

配置 Rogue 设备检测与反制，设备能够提供对非法设备的抑制，维护无线网络的安全。

注意事项

Rogue 设备检测与反制功能需要 AP 工作模式为 hybrid 或者 monitor 才生效。

配置方法

配置 Rogue 设备反制功能

- 可选配置，使用 **countermeasures enable** 命令在 WIDS 配置模式下配置 Rogue 设备反制功能。
- 若无特殊要求，在需要配置 Rogue 设备反制功能的的 AC 设备上面配置该功能。

【命令格式】 **countermeasures enable**
【参数说明】 -
【缺省配置】 默认关闭
【命令模式】 WIDS 配置模式
【使用指导】 AP 工作在 normal 模式时，反制功能无效

配置 Rogue 设备反制周期

- 可选配置，使用 **countermeasures interval** *time* 命令在 WIDS 配置模式下配置 Rogue 设备的反制周期。
- 若无特殊要求，在需要配置 Rogue 设备反制周期的 AC 设备上配置反制周期。

【命令格式】 **countermeasures interval** *time*
【参数说明】 *time*：配置 Rogue 设备反制周期，默认为 1000ms，可配置范围为 100~10000ms
【缺省配置】 默认反制功能的时长为 1000ms
【命令模式】 WIDS 配置模式
【使用指导】 AP 工作在 normal 模式时，反制功能无效

配置 Rogue 设备检测、反制规则

- 可选配置，使用 **countermeasures mode** { **all** | **adhoc** | **config** | **rogue** | **ssid** }命令在 WIDS 配置模式下配置 Rogue 设备的检测、反制规则模式。
- 若无特殊要求，在需要配置 Rogue 设备检测、反制规则的 AC 设备上配置。

【命令格式】 **countermeasures mode** { **all** | **adhoc** | **config** | **rogue** | **ssid** }
【参数说明】 **adhoc**：配置 adhoc 反制模式，反制对象为 adhoc 检测设备。
config：配置 config 反制模式，反制对象为符合 SSID 黑名单以及静态攻击列表中表项的检测设备。
rogue：配置 rogue 反制模式，反制对象为信号强度大于阈值的检测设备。

ssid：配置 ssid 反制模式，反制对象为不在同一 AC 上的相同 SSID 检测设备。

all：配置 all 反制模式，表示 adhoc、config、rogue 和 ssid 四种模式。

【缺省配置】 Rogue 设备的检测、反制规则为空

【命令模式】 WIDS 配置模式

【使用指导】 AP 工作在 normal 模式时，反制功能无效

配置静态攻击列表

- 可选配置，使用 **device attack mac-address** *H.H.H* 命令在 WIDS 配置模式下配置静态攻击统计列表信息。
- 若无特殊要求，在需要配置静态攻击列表的 AC 设备上配置。

【命令格式】 **device attack** { **mac-address** *H.H.H* | **max** *num* }

【参数说明】 **mac-address** *H.H.H*：配置静态攻击列表表项信息，默认为空

max *num*：配置静态攻击列表长度，可配置范围为 1~1024

【缺省配置】 静态攻击列表为空，静态攻击列表长度缺省为 512

【命令模式】 WIDS 配置模式

【使用指导】 AP 工作在 normal 模式时，反制功能无效

配置 SSID 黑名单

- 可选配置，使用 **device black-ssid** *ssid* 命令在 WIDS 配置模式下配置 SSID 黑名单列表信息。
- 若无特殊要求，在需要配置 SSID 黑名单的 AC 设备上配置。

【命令格式】 **device { black-ssid** *ssid* | **max-black-ssid** *num* }

【参数说明】 **black-ssid** *ssid*：配置 SSID 黑名单列表表项，默认为空

max-black-ssid *num*：配置 SSID 黑名单列表长度，可配置范围 1~1024

【缺省配置】 SSID 黑名单列表为空，SSID 黑名单列表长度缺省为 512

【命令模式】 WIDS 配置模式

【使用指导】 AP 工作在 normal 模式时，反制功能无效

配置允许 MAC、允许 SSID 和允许产商列表

- 可选配置。
- 若无特殊要求，在需要配置允许 MAC、允许 SSID 和允许产商列表的 AC 设备上配置。
- 使用 **device permit mac-address** *H.H.H* 命令在 WIDS 配置模式下配置允许 MAC 列表表项信息。
- 使用 **device permit ssid** *ssid* 命令在 WIDS 配置模式下配置允许 SSID 列表表项信息。
- 使用 **device permit vendor bssid** *H.H.H* 命令在 WIDS 配置模式下配置允许产商列表表项信息。

【命令格式】 **device permit** { **mac-address** *H.H.H* | **mac-address max** *num* | **ssid** *ssid* | **max-ssid** *num* | **vendor bssid** *H.H.H* | **vendor bssid max** *num* }

【参数说明】 **mac-address** *H.H.H*：配置允许 MAC 列表表项，默认为空

mac-address max *num*：配置允许 MAC 列表长度，默认为 1024，可配置范围 1~2048

ssid *ssid*：配置允许 SSID 列表表项，默认为空

max-ssid *num*：配置允许 SSID 列表长度，默认为 512，可配置范围 1~1024

vendor bssid *H.H.H*：配置允许产商列表表项，默认为空

vendor bssid max *num*：配置允许产商列表长度，默认为 512，可配置范围 1~1024

【缺省配置】 见参数说明

【命令模式】 WIDS 配置模式

【使用指导】 AP 工作在 normal 模式时，反制功能无效

配置 Rogue 设备反制数量

- 可选配置，使用 **countermeasures ap-max** *ap-num* 命令在 WIDS 配置模式下配置 Rogue 设备反制数量。
- 若无特殊要求，在需要配置 Rogue 设备反制数量的 AC 设备上面配置。

【命令格式】 **countermeasures ap-max** *ap-num*

【参数说明】 *ap-num*：配置每次反制周期反制的设备最大数量，可配置范围 1~256

【缺省配置】 30

【命令模式】 WIDS 配置模式

【使用指导】 AP 工作在 normal 模式时，反制功能无效

配置设备超时时间

- 可选配置，使用 **device aging duration** *time* 命令在 WIDS 配置模式下配置设备超时时间。
- 若无特殊要求，在需要设备超时时间的 AC 设备上面配置。

【命令格式】 **device aging duration** *time*

【参数说明】 *time*：配置检测设备超时时间，可配置范围 500~5000s

【缺省配置】 1200s

【命令模式】 WIDS 配置模式

【使用指导】 AP 工作在 normal 模式时，反制功能无效

配置设备友好标识

- 可选配置，使用 **device friendly-flags** *value* 命令在 WIDS 配置模式下配置设备友好标识，通过设备友好标志位，AP 设备可以识别同 AC 上的设备。
- 若无特殊要求，在需要配置设备友好标识的 AC 设备上面配置。

【命令格式】 **device friendly-flags** *value*

【参数说明】 *value*：配置设备友好标识，可配置范围 1 ~ 4294967295

【缺省配置】 默认值为 0

【命令模式】 WIDS 配置模式

【使用指导】 AP 工作在 normal 模式时，反制功能无效

配置 Rogue 设备反制信号强度

- 可选配置，使用 **countermeasures rssi-min** *num* 命令在 WIDS 配置模式下配置 Rogue 设备反制信号强度。超过该信号强度的 Rogue 设备将被反制。
- 若无特殊要求，在需要设置日志写入内存缓冲区级别的 AC 设备上面配置。

【命令格式】 **countermeasures rssi-min** *num*

【参数说明】 *num*：配置 Rogue 设备反制信号强度，可配置范围 0~75(-95~-20)

【缺省配置】 默认反制功能的反制信号强度下限值为 25(-70)
【命令模式】 WIDS 配置模式
【使用指导】 AP 工作在 normal 模式时，反制功能无效

配置基于信道反制

- 可选配置，使用 **countermeasures channel-match** 命令在 WIDS 配置模式下配置基于信道反制功能。基于信道反制可以根据检测的 Rogue 设备所在的信道进行反制。
- 若无特殊要求，在需要配置基于信道反制功能的 AC 设备上面配置。

【命令格式】 **countermeasures channel-match**
【参数说明】 **channel-match**：配置基于信道反制功能
【缺省配置】 默认关闭
【命令模式】 WIDS 配置模式
【使用指导】 AP 工作在 normal 模式时，反制功能无效

配置未知名 STA 检测与反制

- 可选配置。
- 若无特殊要求，在需要未知名 STA 检测与反制功能的 AC 设备上面配置。
- 使用 device unknown-sta dynamic-enable 命令在 WIDS 配置模式下配置未知名 STA 检测与反制功能。
- 使 **device unknown-sta mac-address** *H.H.H* 命令在 WIDS 配置模式下配置未知名 STA 列表表项信息。

【命令格式】 **device unknown-sta** { **dynamic-enable** | **mac-address** *H.H.H* | **mac-address max** *num* }
【参数说明】 **dynamic-enable**：配置未知名 STA 检测与反制，默认关闭
mac-address *H.H.H*：配置未知名 STA 列表表项，默认为空
mac-address max *num*：配置未知名 STA 列表长度，可配置范围 1～256
【缺省配置】 默认关闭
【命令模式】 WIDS 配置模式
【使用指导】 AP 工作在 normal 模式时，反制功能无效

配置互通非法 AP 检测功能

- 可选配置。
- 若无特殊要求，在需要互通非法 AP 检测功能的 AC 设备上面配置。
- 使用 **device channel-bind radio** *radio-id* { **channel** *num* | **max-cycles** *value* }命令在 ap 配置模式下配置互通非法 AP 检测扫描参数。
- 使用 **device scan-para** { **radio** *radio-id* **scan-type** { **active** | **passive** } **device-detect** { **enable** | **disable** } | **ap-mode** { **normal** | **monitor** } | **detect-rpt-time** *time* }命令在 ap 配置模式下配置互通非法 AP 检测扫描参数。
- 使用 **rogue-ap countermeasures enable** 命令在 wids 模式下配置互通非法 AP 反制功能。
- 配置互通非法 AP 扫描信道信息

【命令格式】 **device channel-bind radio** *radio-id* { **channel** *num* | **max-cycles** *value* }
【参数说明】 *radio-id*：指定 AP 的 radio id 值

channel *num*：指定信道值，默认中国信道

max-cycles *value*：表示扫描次数，默认值 10 次，可配置范围 0~255

【缺省配置】 详见参数说明

【命令模式】 AP 配置模式

【使用指导】 -

【命令格式】 **device scan-para** { **radio** *radio-id* **scan-type** { **active** | **passive** } **device-detect** { **enable** | **disable** } | **ap-mode** { **normal** | **monitor** } | **detect-rpt-time** *time* }

【参数说明】 **radio** *radio-id*：配置 radio 值

scan-type active：表示扫描类型，主动扫描，默认被动扫描

scan-type passive：表示扫描类型，被动扫描

device-detect enable：表示检测开启，默认关闭

device-detect disable：表示检测关闭

ap-mode normal：表示 ap 操作模式：普通模式

ap-mode monitor：表示 ap 操作模式：监测模式

detect-rpt-time *time*：表示检测上报周期，默认 60s，可配置范围 60~120s

【缺省配置】 缺省见参数说明

【命令模式】 AP 配置模式

【使用指导】 -

【命令格式】 **rogue-ap countermeasures enable**

【参数说明】 -

【缺省配置】 默认关闭

【命令模式】 WIDS 配置模式

【使用指导】 -

配置扫描 AP 检测名单最大个数

- 可选配置，使用 **device detected-ap-max** *num* 命令在 WIDS 配置模式下配置扫描 AP 检测链表最大个数，配置值越小会导致 AP 上检测的数据过少，设备反制功能可能会由于检测数据太少，反制效果不明显，配置值越大，需要占用更多的内存。
- 若无特殊要求，在需要配置扫描检测名单最大个数的 AC 设备上面配置。

【命令格式】 **device detected-ap-max** *num*

【参数说明】 *num*: 表示扫描 AP 检测名单的最大个数，可配置范围 1~4096

【缺省配置】 2048

【命令模式】 WIDS 配置模式

【使用指导】 -

配置指定 radio 扫描状态

- 可选配置，使用 **hybrid-scan radio** *num* **{ disable | enable }**命令在 AP 配置模式下配置指定 radio 的扫描状态，如果配置关闭会导致 AP 工作在非 normal 模式时，无设备检测数据。
- 若无特殊要求，在需要配置 radio 扫描状态的 AC 设备上配置。

【命令格式】 **hybrid-scan radio** *num* **{ enable | disable }**
【参数说明】 *num*：表示指定 radio
【缺省配置】 所有 radio 扫描默认开启
【命令模式】 AP 配置模式
【使用指导】 -

配置 AP 的扫描信道

- 可选配置，使用 **scan-channels { 802.11a | 802.11b } channels** *num1 num2…num13* 命令在 AP 配置模式下配置扫描信道，如果没有配置扫描信道，结果会导致 AP 工作在非法 normal 时，无设备检测数据。
- 若无特殊要求，在需要配置指定 AP 扫描信道的 AC 设备上面配置。

【命令格式】 **scan-channels { 802.11a | 802.11b } channels** *num1 num2…num13*
【参数说明】 *num*：表示 AP 的扫描信道
【缺省配置】 扫描信道为空
【命令模式】 AP 配置模式
【使用指导】 -

检验方法

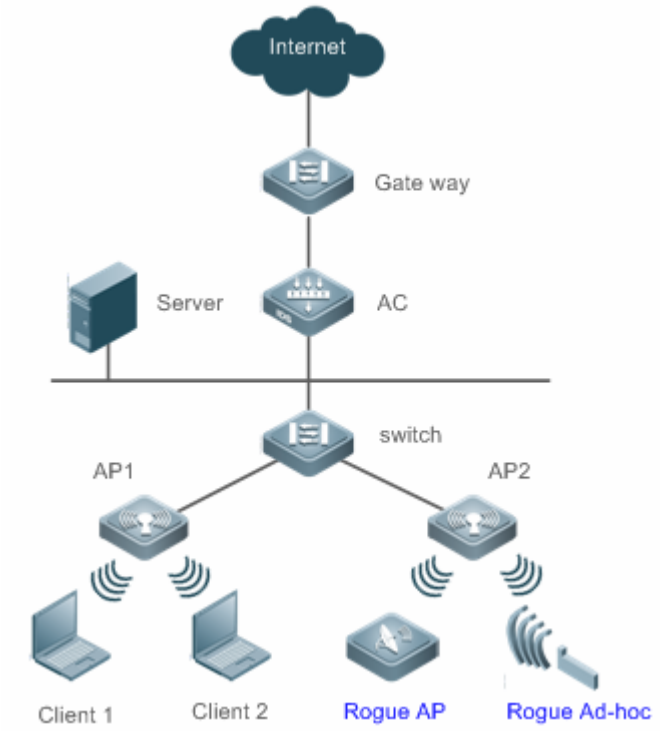
- 通过 **show wids detected** 命令查看检测结果

配置举例

配置 Rogue 设备反制功能

【网络环境】

图 2-8



【配置方法】

- 在 AC 设备上面配置 Rogue 设备反制信息，在配置反制之前，要先确认反制 AP 已经配置了 wlan 服务，这样反制才能生效。

假如反制 AP 已经加入到 default 组，在 AC 上查看 default 组是否绑定了 wlan

```
Ruijie#show ap-group intf-wlan-map default
```

如果 defaut 组没有绑定 wlan 服务，需要配置 wlan 服务。

```
Ruijie# configure terminal
Ruijie(config)# wlan-config 15 wids-monitor
Ruijie(config-wlan)# no enable-broad-ssid
Ruijie(config-wlan)# ap-group default
Ruijie(config-group)#interface-mapping 15 1
```

配置了 wlan 服务之后，wids 的功能开启之后才能生效：

```
Ruijie# configure terminal
Ruijie(config)# wids
Ruijie(config-wids)# countermeasures enable
Ruijie(config-wids)# countermeasures mode ssid
```

【检验方法】

- 通过 **show running-config** 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 running-config
```

```
Ruijie#show running-config
…
!
wids
 countermeasures enable
 countermeasures mode SSID
!
…
```

常见错误

无。

2.5.5 配置AP工作模式

配置效果

- 根据配置的工作模式，AP 能够提供不同的服务

注意事项

无。

配置方法

↘ 配置 AP 工作模式

- 可选配置。
- 若无特殊要求，应在每台 AP 设备上面配置。

【命令格式】 **device mode** { **hybrid** | **monitor** | **normal** }

【参数说明】 **hybrid**：混合模式，设备提供接入服务和监测服务

monitor：监测模式，设备仅提供监测服务

normal：普通模式，设备仅提供接入服务

【缺省配置】 AP 的工作模式为 normal

【命令模式】 AP 配置模式

【使用指导】 -

检验方法

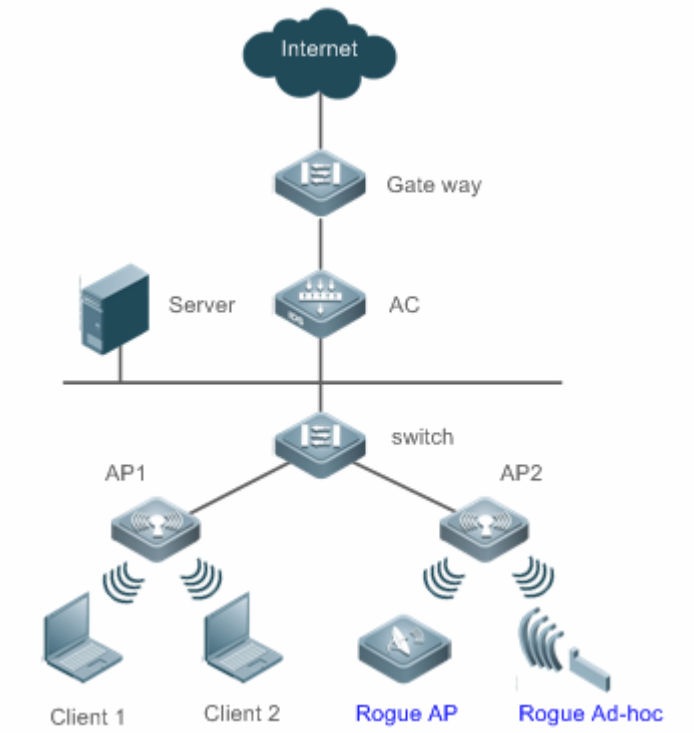
- 通过 **show ap-config running** *ap-name* 命令可以查看该 AP 的当前工作模式

配置举例

配置 AP 工作模式

【网络环境】

图 2-9



【配置方法】

- 在 AC 设备上面配置指定 AP 的工作模式

```
Ruijie# configure terminal
Ruijie(config)# ap-config ap220
Ruijie (config-ap)#device mode hybrid
```

【检验方法】

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

```
Ruijie#show ap-config running ap220
!
ap-config ap220
 device mode hybrid
 11acsupport enable radio 1
 11acsupport enable radio 2
 802.11n mcs support 23 radio 1
 802.11n mcs support 23 radio 2
 802.11ac mcs support 29 radio 1
 802.11ac mcs support 29 radio 2
```

```
antenna receive 7 radio 1
antenna receive 7 radio 2
antenna transmit 7 radio 1
antenna transmit 7 radio 2
!
```

常见错误

无。

2.6 监视与维护

清除各类信息

无。

查看运行情况

作用	命令
查看攻击列表配置信息	**show wids attack-list**
查看动态和静态黑名单列表配置信息	**show wids blacklist** { **dynamic** | **static** }
查看 SSID 黑名单列表配置信息	**show wids black-ssid**
查看检测到的指定类型设备信息	**show wids detected** { **adhoc** | **all** | **friendly ap** | **interfering ap** | **rogue** { **adhoc-ap** | **ap** | **client** | **config-ap** | **ssid-ap** } | **mac-address** *H.H.H* }
查看基于 SSID 的黑白名单列表表项配置信息	**show wids ssid-filter** { **blacklist all** [**in-ssid** *string*] | **ssid all** | **whitelist all** [**in-ssid string**] }
查看允许 MAC、允许 SSID 和允许产商列表表项配置信息	**show wids permitted** { **mac-address** | **ssid** | **vendor** }
查看 IDS 攻击检测信息	**show wids statistics**
查看未知名 STA 列表配置信息	**show wids unknown-sta**
查看用户隔离允许列表表项信息	**show wids user-isolation permit-mac**
查看白名单列表表项信息	**show wids whitelist**
查看 WIDS 其他配置信息	**show running-config**
查看互通的防 dos 攻击检测信息	**show wids dos-detected**
查看互通的非法 AP 检测信息	**show wids rogue-ap detected**

查看调试信息

无。

3 WAPI

3.1 概述

WAPI（WLAN Authentication and Privacy Infrastructure，无线局域网鉴别与保密基础结构）是中国具有自主知识产权的无线网络安全标准。

WAPI 协议由以下两部分构成：

- WAI（WLAN Authentication Infrastructure，无线局域网鉴别基础结构）：用于无线局域网中身份鉴别和密钥管理的安全方案。WAPI 标准提供两种用户身份鉴别方式：WAPI 预共享密钥鉴别和 WAPI 证书鉴别。
- WPI（WLAN Privacy Infrastructure，无线局域网保密基础结构）：用于无线局域网中数据传输保护的安全方案，包括数据加密、数据鉴别和重放保护等功能。

WAPI 既可以应用到小型无线网络，也应用于大规模部署的无线网络。预共享密钥认证方式，提供一种简单的不需要专门认证服务器的认证机制；WAPI 证书认证机制，借助专门的认证服务器，可以为大规模部署的无线网络提供安全且易于管理的接入方案。

下文仅介绍 WAPI 的相关内容。

协议规范

- GB 15629.11-2003/XG1-2006：信息技术 系统间远程通信和信息交换局域网和城域网特定要求 第 11 部分：无线局域网媒体访问控制和物理层规范 第 1 号修改单
- RFC 3280：Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- RFC 4492：Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)
- 《WAPI 多信任证书实施技术》，多证书认证技术指导性文件

3.2 典型应用

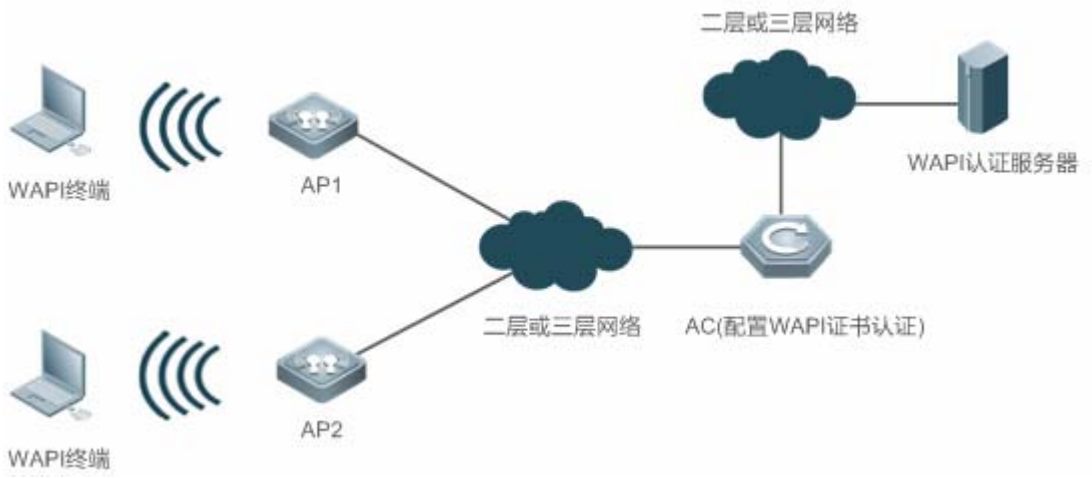
典型应用	场景描述
WAPI 证书认证	在大规模部署的无线网络中，建议配置 WAPI 证书认证模式。
WAPI 预共享密钥认证	在规模较小或者无管理需求的无线网络中，可配置 WAPI 预共享密钥模式。

3.2.1 WAPI证书认证

应用场景

在大规模部署的无线网络中，建议配置 WAPI 证书认证模式。典型应用场景如下图所示：

图 3-1



功能部属

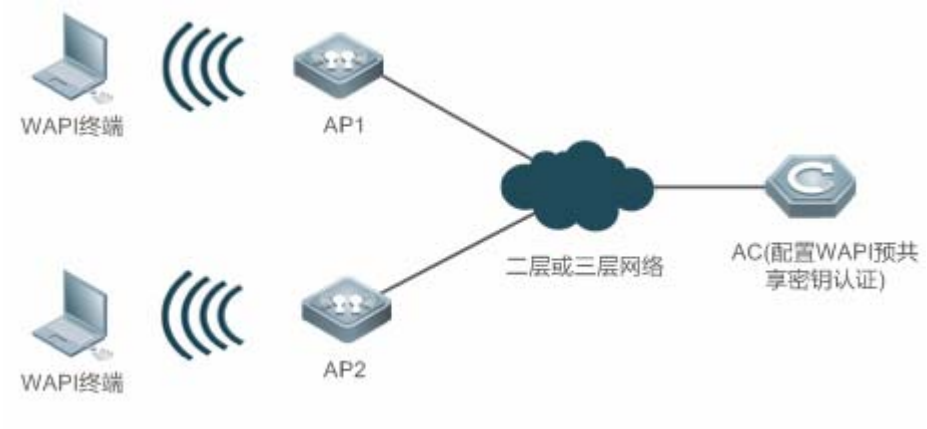
- 在 AC 上配置 WLAN。
- 配置 WAPI 证书认证服务器。
- 在 WLAN 安全模式下配置 WAPI 证书认证模式。
- 将 WLAN 下发到 AP。

3.2.2 WAPI预共享密钥认证

应用场景

在规模较小或者无管理需求的无线网络中，可配置 WAPI 预共享密钥模式。典型应用场景如下图所示：

图 3-2



功能部属

- 在 AC 上配置 WLAN。
- 在 WLAN 安全模式下配置 PSK 认证模式。
- 将 WLAN 下发到 AP。
- 可配合 WEB 认证一起使用，以支持网络认证及计费功能。

3.3 功能详解

基本概念

AE

Authenticator Entity，鉴别器实体。为鉴别请求者实体在接入服务之前提供鉴别操作的实体，该实体驻留在 AP 或 AC 中。

AS

Authentication Server，鉴别服务器。提供 WAPI 证书鉴别服务。

ASU

Authentication Service Unit，鉴别服务单元。为鉴别器实体和鉴别请求者实体提供相互鉴别服务的实体，该实体驻留在 AS 中。

ASUE

Authentication SUpplicant Entity，鉴别请求者实体。在接入服务之前请求进行鉴别操作的实体，该实体驻留在 STA 中。

BK

Base Key，基密钥。用于导出单播会话密钥的密钥。基密钥由证书鉴别过程协商得到或由预共享密钥导出。

CA

Certification Authority，证书颁发者。CA 是第三方机构，被信任，由它保证证书的确发给了应该得到该证书的人。

功能特性

功能特性	作用
WAPI 鉴别方式	对加入 WLAN 的 STA 进行身份认证。
WAPI 密钥管理	单播密钥协商与组播密钥通告。

3.3.1 WAPI鉴别方式

WAPI 协议标准定义了 2 种用户身份鉴别方式：

- 证书鉴别方式
- 预共享密钥鉴别方式

工作原理

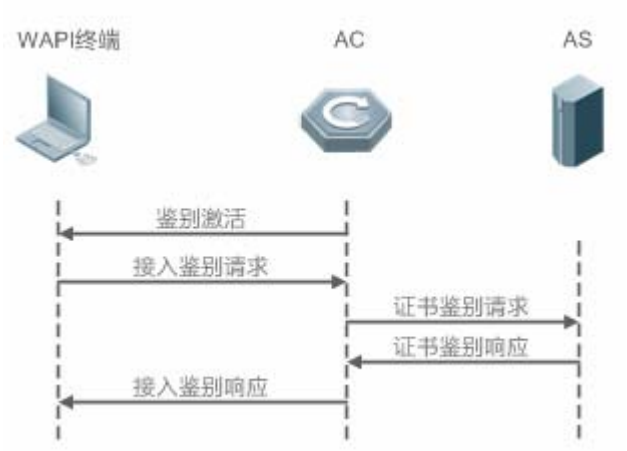
证书鉴别方式

证书鉴别是基于 STA 和 AE 双方的证书所进行的鉴别。鉴别前 STA 和 AE 必须预先拥有各自的证书，然后通过 AS 对双方的身份进行鉴别，根据双方产生的临时公钥和临时私钥生成 BK，并为随后的单播密钥协商和组播密钥通告做好准备。

当 WAPI 功能应用于大规模运营时，证书颁发系统和证书鉴别系统分离。ASUE 和 AE 安装证书时需要安装三张证书，一张为用户证书或设备证书，一张为颁发者证书，第三张为信任的 ASU 证书，其中 ASU 证书为强制信任证书（ASUE 和 AE 安装完证书后即信任颁发者和 ASU）。因此，我们将这种模式称为 WAPI 三证书认证模式；而证书颁发系统和证书鉴别系统为同一实体的模式，则称为 WAPI 二证书模式。

证书鉴别的过程如下图所示。

图 3-3



【注释】 AC 即为 AE 设备。

预共享密钥鉴别方式

预共享密钥鉴别是基于 STA 和 AE 双方的密钥所进行的鉴别。鉴别前 STA 和 AE 必须预先配置有相同的密钥，即预共享密钥。鉴别时直接将预共享密钥转换为 BK，然后进行单播密钥协商和组播密钥通告。

3.3.2 WAPI密钥管理

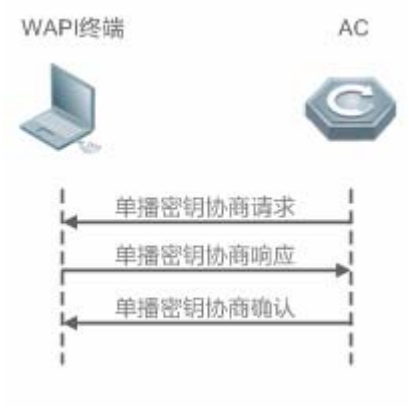
STA 与 AE 之间交互的单播数据利用单播密钥协商过程所协商出的单播加密密钥和单播完整性校验密钥进行保护；AE 利用自己通告的、由组播主密钥导出的组播加密密钥和组播完整性校验密钥对其发送的广播/组播数据进行保护，而 STA 则采用 AE 通告的、由组播主密钥导出的组播加密密钥和组播完整性校验密钥对收到的广播/组播数据进行解密。

工作原理

单播密钥协商

首先要进行单播密钥的协商，其过程如下图所示。

图 3-4



证书鉴别成功后，AE 向 ASUE 发送密钥协商请求，其中包含密钥协商请求数据。

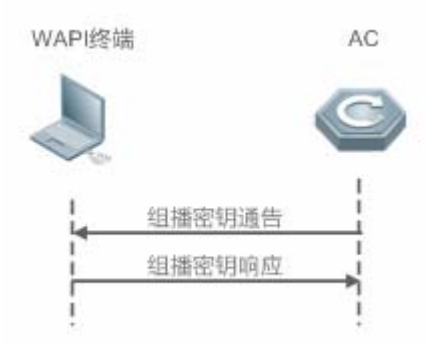
ASUE 接收到单播密钥协商请求并验证对其有效性后，生成密钥协商响应数据，构造单播密钥协商响应发送给 AE。双方利用密钥协商数据生成单播会话密钥。

AE 收到单播密钥协商响应并验证其有效性后，向 ASUE 返回单播密钥协商确认。双方建立了单播密钥安全关联。

组播密钥通告

当单播密钥协商完成后，再使用单播密钥协商过程所协商出的密钥进行组播密钥的通告，其过程如下图所示。

图 3-5



单播密钥协商成功即单播密钥安全关联建立后，AE 向 ASUE 发送组播密钥通告，通知 AE 发送的组播数据信息加密所使用的密钥。

ASUE 验证 AE 发送的组播密钥通告的有效性后，向 AE 返回组播密钥响应。双方建立了组播密钥安全关联。

⚠ 无论是 WAPI 证书认证还是预共享密钥认证方式，STA 加入 WLAN 都需要进行密钥交互过程。

3.4 产品说明

NBR800G、NBR950G、NBR1500G、NBR2000G 不支持无线集成 AC 功能，NBR108G-P、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持无线集成 AC 功能。

3.5 配置详解

配置项	配置建议 & 相关命令	
配置 WAPI 证书认证	必须配置。用于启用 WAPI 证书认证模式。	
	security wapi	配置启用 WAPI 安全模式。
	security wapi ae cert	配置 AE 设备的 WAPI 证书。
	security wapi asu address	配置认证服务器 IP 地址。
	security wapi ca cert	配置颁发者证书。
	可选配置。用于启用 WAPI 二证书认证方式或三证书认证方式。 启用 WAPI 证书认证模式之后，必须指定二证书认证或三证书认证其中一种认证方式。	
	security wapi 2-cert	配置二证书认证方式。
	security wapi 3-cert	配置三证书认证方式。
	security wapi asu cert	配置认证服务器 WAPI 证书。
配置 WAPI 预共享密钥认证	必须配置。用于启用 WAPI 预共享密钥认证模式。	
	security wapi	配置启用 WAPI 安全模式。
	security wapi psk	配置启用 WAPI 预共享密钥认证方式
	security wapi psk set-key	配置 WAPI 预共享密钥。

3.5.1 配置WAPI证书认证

配置效果

- 启用 WAPI 证书认证模式，使用证书鉴别方式对加入 WLAN 的 STA 进行身份认证。
- 可配置二证书认证方式或三证书认证方式。

注意事项

- 在同一个 WLAN 安全配置模式下，二证书认证方式和三证书认证模式不可同时启用。
- 需要与 WAPI 认证服务器配合。

配置方法

配置启用 WAPI 安全模式

- 必须配置。
- 在 AC 设备上要配置 WAPI 的 WLAN 对应安全配置模式下配置。

【命令格式】 **security wapi** { **enable** | **disable** }
【参数说明】 **enable**：启用 WAPI 安全模式。
disable：关闭 WAPI 安全模式。
【缺省配置】 关闭
【命令模式】 WLAN 安全配置模式
【使用指导】 在同一个 WLAN 安全配置模式下，WAPI 安全模式不能与其他加密认证模式同时启用。

配置二证书认证方式

- 可选配置。启用 WAPI 二证书认证模式时配置。使用 security wapi 2-cert { enable | disable }命令可以启用或关闭 WAPI 二证书认证方式。
- 在 AC 设备上启用 WAPI 的安全配置模式下配置。
- 配置二证书认证方式前应先启用 WAPI 安全模式。在同一个 WLAN 安全配置模式下，二证书认证方式和三证书认证模式不可同时启用。配置 WAPI 二证书认证方式之后，STA 和 AE 安装证书时需要安装两张证书，STA 接入 WLAN 将采用二证书鉴别方式。

【命令格式】 **security wapi 2-cert** { **enable** | **disable** }
【参数说明】 **enable**：启用 WAPI 二证书认证。
disable：关闭 WAPI 二证书认证。
【缺省配置】 关闭
【命令模式】 WLAN 安全配置模式
【使用指导】 配置二证书认证方式前应先启用 WAPI 安全模式。
在同一个 WLAN 安全配置模式下，二证书认证方式和三证书认证方式不可同时启用。

配置三证书认证方式

- 可选配置。启用 WAPI 三证书认证模式时配置。使用 security wapi 3-cert { enable | disable }命令可以启用或关闭 WAPI 三证书认证方式。
- 在 AC 设备上启用 WAPI 的安全配置模式下配置。
- 配置三证书认证方式前应先启用 WAPI 安全模式。在同一个 WLAN 安全配置模式下，三证书认证方式和二证书认证模式不可同时启用。配置 WAPI 三证书认证方式之后，STA 和 AE 安装证书时需要安装三张证书，STA 接入 WLAN 将采用三证书鉴别方式。

【命令格式】 **security wapi 3-cert** { **enable** | **disable** }
【参数说明】 **enable**：启用 WAPI 三证书认证。
disable：关闭 WAPI 三证书认证。
【缺省配置】 关闭

【命令模式】 WLAN 安全配置模式

【使用指导】 配置三证书认证方式前应先启用 WAPI 安全模式。

在同一个 WLAN 安全配置模式下，三证书认证方式和二证书认证方式不可同时启用。

配置 AE 设备的 WAPI 证书

- 必须配置。
- 在 AC 设备上启用 WAPI 的安全配置模式下配置。

【命令格式】 **security wapi ae cert** *ae_certfile*

【参数说明】 *ae_certfile*：AE 设备的 WAPI 证书文件名。

【缺省配置】 无

【命令模式】 WLAN 安全配置模式

【使用指导】 配置 AE 证书前应先启用 WAPI 安全模式。

配置前，应确保证书文件已导入到设备中。

配置认证服务器 IP 地址

- 必须配置。
- 在 AC 设备上启用 WAPI 的安全配置模式下配置。

【命令格式】 **security wapi asu address** *ip_address*

【参数说明】 *ip_address*：认证服务器的 IP 地址。

【缺省配置】 无

【命令模式】 WLAN 安全配置模式

【使用指导】 配置认证服务器 IP 地址之前应先启用 WAPI 安全模式。

配置认证服务器 WAPI 证书

- 可选配置。三证书认证方式下，需要配置 ASU 证书。
- 在 AC 设备上启用 WAPI 的安全配置模式下配置。

【命令格式】 **security wapi asu cert** *asu_certfile*

【参数说明】 *asu_certfile*：ASU 证书文件名。

【缺省配置】 无

【命令模式】 WLAN 安全配置模式

【使用指导】 配置 ASU 证书前应先启用 WAPI 安全模式。

配置前，应确保证书文件已导入到设备中。

三证书认证方式下，需要配置 ASU 证书。

二证书认证方式下，不需配置 ASU 证书。

配置颁发者证书

- 必须配置。
- 在 AC 设备上启用 WAPI 的安全配置模式下配置。

【命令格式】 **security wapi ca cert** *ca_certfile*

【参数说明】 *ca _certfile*：颁发者证书文件名。

【缺省配置】 无

【命令模式】 WLAN 安全配置模式

【使用指导】 配置 CA 证书前应先启用 WAPI 安全模式。

配置前，应确保证书文件已导入到设备中。

检验方法

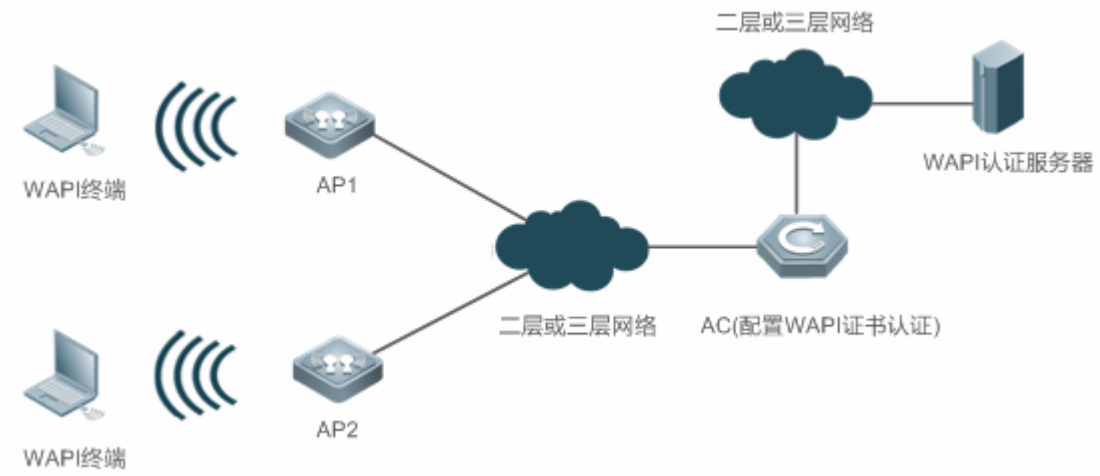
使用 **show running-config** | **begin wlansec** *wlan_id* 命令，可以查看配置是否生效。

配置举例

配置 WLAN 1 为 WAPI 二证书认证模式

【网络环境】

图 3-6



认证服务器 IP 地址为 192.168.1.123。

【配置方法】

- 进入 WLAN 1 的安全配置模式。
- 配置启用 WAPI 安全模式。
- 配置启用二证书认证方式。
- 配置颁发者证书。
- 配置 AE 设备的 WAPI 证书。
- 配置认证服务器 IP 地址。

AC

```
Ruijie(config)#wlansec 1
Ruijie(config-wlansec)#security wapi enable
Ruijie(config-wlansec)#security wapi 2-cert enable
Ruijie(config-wlansec)#security wapi ca cert CA.cer
Ruijie(config-wlansec)#security wapi ae cert AE.cer
Ruijie(config-wlansec)#security wapi asu address 192.168.1.123
```

【检验方法】 使用 **show running-config | begin wlansec** *wlan_id* 命令，可以查看配置是否生效。

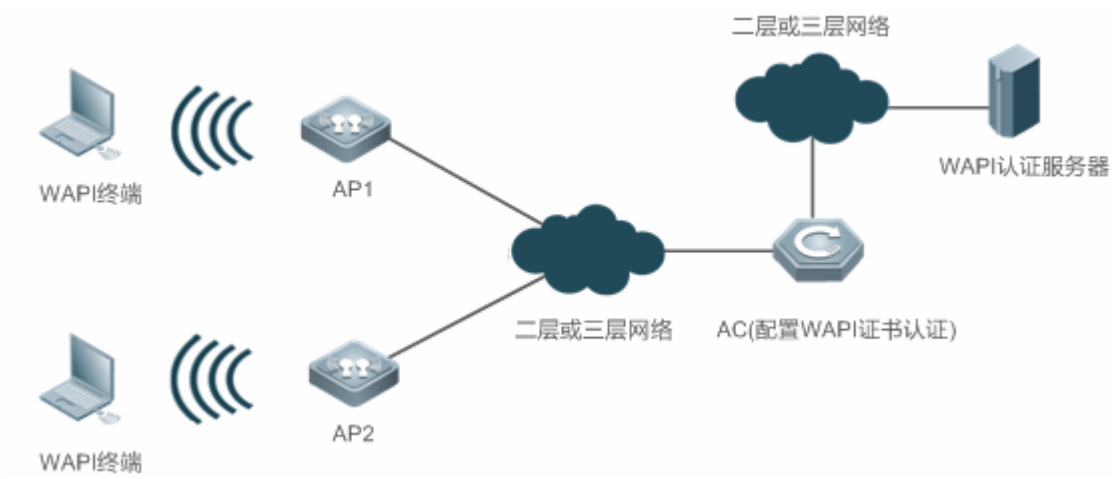
AC

```
Ruijie#show running-config | begin wlansec 1
wlansec 1
 security wapi enable
 security wapi asu address 192.168.1.123
 security wapi ca cert CA.cer
 security wapi ae cert AE.cer
 security wapi 2-cert enable
!
```

配置 WLAN 1 为 WAPI 三证书认证模式

【网络环境】

图 3-7



认证服务器 IP 地址为 192.168.1.123。

【配置方法】

- 进入 WLAN 1 的安全配置模式。
- 配置启用 WAPI 安全模式。
- 配置启用三证书认证方式。
- 配置颁发者证书。
- 配置 AE 设备的 WAPI 证书。
- 配置认证服务器 WAPI 证书
- 配置认证服务器 IP 地址。

AC

```
Ruijie(config)#wlansec 1
Ruijie(config-wlansec)#security wapi enable
Ruijie(config-wlansec)#security wapi 3-cert enable
Ruijie(config-wlansec)#security wapi ca cert CA.cer
Ruijie(config-wlansec)#security wapi ae cert AE.cer
Ruijie(config-wlansec)#security wapi asu cert ASU.cer
Ruijie(config-wlansec)#security wapi asu address 192.168.1.123
```

【检验方法】 使用 **show running-config | begin wlansec** *wlan_id* 命令，可以查看配置是否生效。

AC

```
Ruijie#show running-config | begin wlansec 1
wlansec 1
 security wapi enable
 security wapi asu address 192.168.1.123
 security wapi asu cert ASU.cer
 security wapi ca cert CA.cer
 security wapi ae cert AE.cer
 security wapi 3-cert enable
!
```

常见错误

- WLAN 已经启用了其他的加密认证方式（如 WEP/RSN/WPA）。
- WLAN 未启用 WAPI 安全模式就配置三证书认证方式。
- WAPI 证书未导入到设备中。

3.5.2 配置WAPI预共享密钥认证

配置效果

- 启用 WAPI 预共享密钥认证，STA 和 AE 必须预先配置相同的密钥。

注意事项

- 启用 WAPI 预共享密钥认证方式之后，需配置预共享密钥。

配置方法

↘ 配置启用 WAPI 安全模式

- 必须配置。
- 在 AC 设备上要配置 WAPI 的 WLAN 对应安全配置模式下配置。

【命令格式】 **security wapi** { **enable** | **disable** }

【参数说明】 **enable**：启用 WAPI 安全模式。

disable：关闭 WAPI 安全模式。

【缺省配置】 关闭

【命令模式】 WLAN 安全配置模式

【使用指导】 在同一个 WLAN 安全配置模式下，WAPI 安全模式不能与其他加密认证模式同时启用。

配置启用 WAPI 预共享密钥认证方式

- 必须配置。使用 security wapi psk { enable | disable }命令可以启用或关闭 WAPI 预共享密钥认证方式。
- 在 AC 设备上启用 WAPI 的安全配置模式下配置。
- 必配置 WAPI 预共享密钥认证方式前应先启用 WAPI 安全模式。STA 需要输入与 AE 设备相同的共享密钥才能接入配置 WAPI 预共享密钥认证的 WLAN。

【命令格式】 **security wapi psk** { **enable** | **disable** }

【参数说明】 **enable**：启用 WAPI 预共享密钥认证方式。

disable：关闭 WAPI 预共享密钥认证方式。

【缺省配置】 关闭

【命令模式】 WLAN 安全配置模式

【使用指导】 配置 WAPI 预共享密钥认证方式前应先启用 WAPI 安全模式。

配置 WAPI 预共享密钥

- 必须配置。
- 在 AC 设备上启用 WAPI 的安全配置模式下配置。

【命令格式】 **security wapi psk set-key** { **ascii** *ascii-key* | **hex** *hex-key* }

【参数说明】 **ascii**：指定预共享密钥形式为 ASCII 码。

ascii-key：ASCII 码形式的密码，长度限制为 8--32 个 ASCII 码字符。

hex：指定预共享密钥形式为十六进制字符。

hex-key：十六进制形式的密码，长度为 16--64 个十六进制字符，长度必须是偶数。

【缺省配置】 无

【命令模式】 WLAN 安全配置模式

【使用指导】 配置 WAPI 预共享密钥前应先启用 WAPI 安全模式。

密钥长度限定为 8--32 个 ASCII 码字符。

检验方法

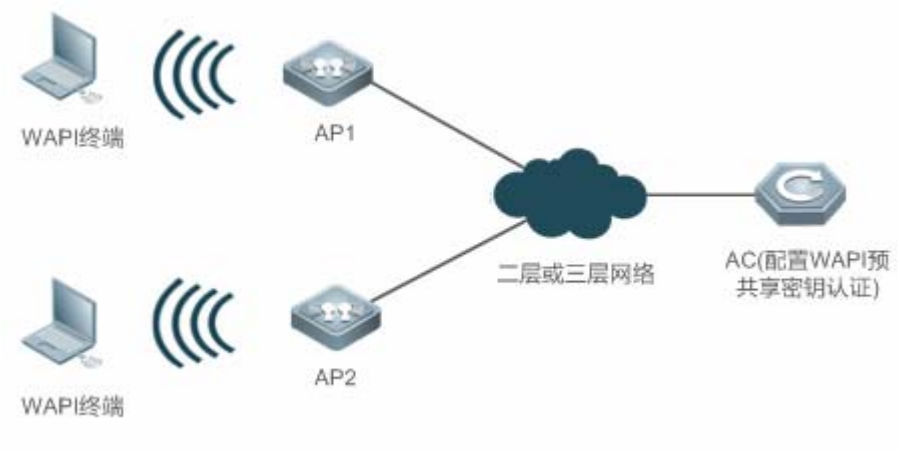
使用 **show running-config** | **begin wlansec** *wlan_id* 命令，可以查看配置是否生效。

配置举例

配置 WLAN 1 为 WAPI 预共享密钥认证模式，密码为 12345678。

【网络环境】

图 3-8



【配置方法】

- 进入 WLAN 1 的安全配置模式。
- 配置启用 WAPI 安全模式。
- 配置启用 WAPI 预共享密钥认证方式。
- 配置 WAPI 预共享密钥为 12345678。

AC

```
Ruijie(config)#wlansec 1
Ruijie(config-wlansec)#security wapi enable
Ruijie(config-wlansec)#security wapi psk enable
Ruijie(config-wlansec)#security wapi psk set-key ascii 12345678
```

【检验方法】 使用 **show running-config | begin wlansec** *wlan_id* 命令，可以查看配置是否生效。

AC

```
Ruijie#show running-config | begin wlansec 1
wlansec 1
 security wapi enable
 security wapi psk set-key ascii 12345678
 security wapi psk enable
!
```

常见配置错误

- WLAN 已经启用了其他的加密认证方式（如 WEP/RSN/WPA）。
- WAPI 预共享密钥长度不足 8 个或超过 32 个 ASCII 码字符。

3.6 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
-	-

查看运行情况

作用	命令
查看 WAPI 用户状态信息。	**show wapi-sta 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
-	-

WLAN QOS

本分册介绍 WLAN QOS 相关内容，包括以下章节：

1. WQOS
2. WMM

1 WQOS

1.1 概述

WQOS（WLAN QoS，无线带宽控制）是一种无线的带宽控制功能，它包括流量限速，公平调度，以及防内网代理。

流量限速，是用来对 AP、WLAN、STA 的数据流量进行限制，避免流量超过一定范围。流量限速适用于某些 STA 占用过多带宽挤占其它 STA 带宽的场景。

公平调度通过将时间均分，解决不同设备占用空口时间不一样，导致低速节点可能长期占用空口时间。公平调度适用于所有无线网络。

防内网代理用来解决无线网络中一个 STA 给其它 STA 作为代理使用，导致某些 STA 未经许可就能连接网络的问题。防内网代理适用于内网需要杜绝非法代理服务器的场景。

协议规范

- IEEE 802.11e-2005：Amendment 8：Medium Access Control (MAC) QualityofServiceEnhancements, IEEE Computer Society
- Wi-Fi：WMM Specification version 1.1

1.2 典型应用

典型应用	场景描述
瘦 AP 组网带宽控制	使用瘦 AP 组网，至少包括一台 AC、一台 AP

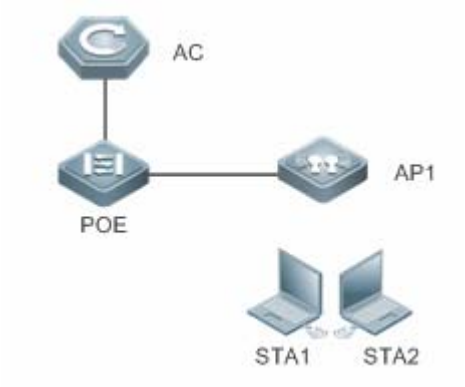
1.2.1 瘦AP组网带宽控制

应用场景

在无线网络中，部署一台 AC 设备，在 AC 上对 AP、WLAN、STA 进行流量限速，对 AP 开启公平调度和防内网代理。

以下图为例，在 AC 设备上对 AP、WLAN、STA 进行流量限速，对 AP 开启公平调度和防内网代理。

图 1-1



【注释】 AC：无线控制器设备。
POE：交换机设备，作为 AP 的网关。
AP：无线接入设备。
STA1、STA2：用户设备，作为 STA 来使用。

功能部属

- 在 AC 设备上开启 WQOS 功能。

1.3 功能详解

基本概念

流量限速

为了使有限的网络资源能够更好地发挥效用，更好地为更多的用户服务，设备需要支持流量限速功能。当数据流量符合承诺速率时，允许数据包通过；数据流量不符合承诺速率时，丢弃数据包。

评估流量的参数如下：

- 平均速率（average-data-rate），即允许的流的平均速度，也叫承诺信息速率。
- 突发速率（burst-data-rate），即每次突发所允许的最大的流量，也叫承诺突发尺寸。设置的突发尺寸必须大于最大报文长度这里指单个周期 10ms 里允许发送的最大速率（计算时，通过单个周期的最大流量除以 10ms 计算出速率值 KBps）。

公平调度

公平调度功能允许关联到同一个 AP 上同一个频段的 STA 共享 AP 提供的无线网络资源，公平的分享无线网络的带宽。使用公平调度功能可以防止低速 STA 拖慢整个无线网络的吞吐量，而且能够为 STA 提供更加平滑的网速体验。另外，公平调度功能还能够智能地监控每个 STA 的网络流量的变化，动态地调整每个 STA 的所占用的无线带宽比例，为用户带来更好的无线网络体验。在 10.4(1T19)p1 版本之后，允许在公平调度中，对 STA 设置不同的优先级，达到让特定用户能够优先占用无线带宽的目的。

防内网代理检测

在 10.4(1T19)p1 版本之后，防内网代理检测是为了检测无线内网中 STA 作为其他 STA 的代理服务器，从而达到对 STA 数量和网络流量的准确监控。

功能特性

功能特性	作用
流量限速	针对 AP、WLAN、STA 进行流量限速，使得流量不会超过限速值。
公平调度	对关联到同一 AP 上同一个频段的 STA 共享 AP 提供的无线网络资源，公平的分享无线网络的带宽。
防内网代理	检测无线内网中 STA 作为其他 STA 的代理服务器，对 STA 数量和网络流量的准确监控。

1.3.1 流量限速

流量限速是用来对某个 AP、某个 WLAN、或者某台 STA 的流量进行限制，保证流量不能超过一定的范围。

工作原理

流量限速是根据令牌桶算法来实现的。

- 记录这个时刻可以通过的报文字节数，通常称为令牌桶。
- 在每个单位周期内，会根据配置的平均速率和突发速率，算出每个单位周期内可以通过的报文字节数，来增加令牌桶的大小。
- 当有报文到达时，会判断报文字节数与令牌桶的大小。如果报文字节数小于令牌桶大小，则允许报文通过，并将令牌桶减少；当报文字节数大于令牌桶大小时，有两种处理方式：缓存报文，等到令牌桶允许通告之后，再继续发送，通常称为流量整形；丢弃报文，直接将报文丢弃，通常称为流量监控。流量整形算法，使得流量比较平稳，波动小；流量监控算法，使得流量波动比较大。
- 目前 AP 上，AP、STA、WLAN 的限速使用流量整形进行处理；AC 上，WLAN 的限速使用流量监控来处理。

1.3.2 公平调度

公平调度是通过将时间均分，解决不同设备占用空口时间不一样，导致低速节点可能长期占用空口时间。

工作原理

由于无线网络的特殊性，在同一个网络的 STA（包括 AP）共享空口资源，而由于无线和有线网络性能上的差异，空口资源往往成为 STA 性能的瓶颈。传统的报文调度采用 FIFO 的方式，同一个无线网络中，每个需要传输的 STA 都希望尽可能的占用空口资源。大量的低速报文的传送造成空口被长时间占用，从而队列长时间被占用，导致报文被丢，使得整体性能低下。

然而在实际无线应用场景中，STA 之间存在差别（类型不一样、能力不一样等）是十分常见的，这时往往导致了某些 STA 总是得不到空口资源，获取网络资源响应慢，极端情况下甚至关联不到网络，严重影响用户的体验。

为了解决这个问题，保证每一个 STA 都能够得到空口资源，就需要让 STA 公平地获得资源，这里的公平指的是每个需要传输的 STA 占用空口的时间是公平的。通过获取 STA 相关信息（协商速率、聚合类型等）、对应报文有效字节数来预测每个 STA 流量，并转换成单个 STA 可发送的报文个数，通过调整 STA 可发送报文数对 STA 空口带宽分配以及流量整形，从而实现无线链路的公平占用。在公平调度的协调下，STA 占用空口的时间较为平均，有效避免了出现某个 STA 性能特别差的情况，提升用户体验。

1.3.3 防内网代理

防内网代理用来解决无线网络中一个 STA 给其它 STA 作为代理使用，导致某些 STA 未经许可就能连接网络的问题。

工作原理

防内网代理功能，主要是通过检测 STA 发来的报文是否符合代理服务器的报文要求来判断是否是代理服务器，并进行反制。目前支持的策略有，ttl 检测策略和 tcp 源端口检测策略。

- ttl 检测策略：是通过在 AP 上检测 STA 发来的 IP 报文中的 TTL 字段是否在合理的范围。如果超出范围，则认为是代理服务器。
- tcp 源端口检测策略：是通过在 AP 上记录 STA 发来的 TCP 报文中使用的端口个数是否在合理范围内。如果超出范围，则认为是代理服务器。

1.4 产品说明



NBR800G、NBR950G、NBR1500G、NBR2000G 不支持无线集成 AC 功能，NBR108G-P、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持无线集成 AC 功能。

1.5 配置详解

配置项	配置建议&相关命令	
配置流量限速	⚠ 必须配置。用来开启流量限速。	
	ap-based	AC 上，配置基于 AP 的流量限速
	netuser	AC 上，配置基于 STA 的流量限速
	wlan-based	AC 上，配置基于 WLAN 的流量限速
	wlan-qos ap-based	AP 上，配置基于 AP 的流量限速
	wlan-qos netuser	AP 上，配置基于 STA 的流量限速
	wlan-qos wlan-based	AP 上，配置基于 WLAN 的流量限速
配置公平调度	⚠ 必须配置。用来开启公平调度功能。	

	fair-schedule	开启公平调度功能
	可选配置。用来调整公平调度过程中 STA 的优先级。	
	sta-fair	设置 STA 的公平调度优先级
配置防内网代理	必须配置。用来配置防内网代理的策略，并开启防内网检测功能。	
	illegal-sta-check ip ttl	开发防内网代理功能，使用 ttl 检测策略。
	illegal-sta-check tcp source-ports	开启防内网代理功能 ,使用 tcp 源端口检测策略。

1.5.1 配置流量限速

配置效果

- 用户可根据实际网络情况，限制某个流只能得到承诺分配给它的那部分资源，防止由于过分突发流量所引发的网络拥塞。

注意事项

- 胖 AP 上的 CLI 命令是在全局模式下配置的，在相关的命令前增加 **wlan-qos** 前缀。
- AC 上的 **wlan-based per-ap-limit** 限速的效果等同于在所有 AP 上配置 **wlan-qos wlan-based total-user-limit** 限速。
- wlan-based per-user-limit，wlan-based per-ap-limit intelligent，ap-based per-user-limit，ap-based total-limit intelligent ，netuser 这 5 种限速都是要作用到 sta 上的，但是 sta 的限速在一个时间内只能有一种在工作，从优先级选择上：netuser 高于 wlan-based per-ap-limit intelligent 高于 wlan-based per-user-limit 高于 ap-based total-limit intelligent 高于 ap-based per-user-limit。
- wlan-based total-limit，wlan-based per-ap-limit，ap-based total-limit 和 sta 限速由于作用的对象不同，可以同时工作，没有优先级之分。

配置方法

配置基于 AP 的流量限速

- 必须配置。
- 胖 AP 下，在全局配置模式下，使用 **wlan-qos ap-based** 命令进行配置。
- AC 下，在 AP 配置模式下，使用 ap-based 命令进行配置。

【命令格式】 **ap-based** { **per-user-limit** | **total-user-limit** [**intelligent**] } { **down-streams** | **up-streams** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*

【参数说明】 **per-user-limit**：对 AP 上的每个用户进行限速。

total-user-limit：对整个 AP 进行限速。

intelligent：表示是否对 total 进行智能限速。

down-streams：表示设置 AP 的下行流量限速。

up-streams：表示设置 AP 的上行流量限速。

average-data-rate：表示设置平均速率限制，单位为 8Kbps，范围为 8-261120。

burst-data-rate：表示设置突发速率限制，单位为 8Kbps，范围为 8-261120。

【缺省配置】 缺省为无流量限速。配置了 total-user-limit 缺省不开启智能限速

【命令模式】 AC：AP 配置模式，胖 AP：全局配置模式。

【使用指导】 -

配置基于 STA 的流量限速

- 必须配置。
- 胖 AP 下，在全局配置模式下，使用 **wlan-qosnetuser** 命令进行配置。
- AC 下，在 AC 配置模式下，使用 **netuser** 命令进行配置。

【命令格式】 **netuser** *mac-address* { **inbound** | **outbound** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*

【参数说明】 *mac-address*：表示需要设置的用户 MAC 地址。

inbound：表示设置用户的上行流量限速。

outbound：表示设置用户的下行流量限速。

average-data-rate：表示设置平均速率限制，单位为 8Kbps，范围为 8-261120。

burst-data-rate：表示设置突发速率限制，单位为 8Kbps，范围为 8-261120。

【缺省配置】 缺省为无流量限速

【命令模式】 AC:AC 配置模式，胖 AP：全局配置模式。

【使用指导】 -

配置基于 WLAN 的流量限速

- 必须配置。
- 胖 AP 下，在全局配置模式下，使用 **wlan-qos wlan-based** 命令进行配置。
- AC 下，在 WLAN 配置模式下，使用 **wlan-based** 命令进行配置。

【命令格式】 **wlan-based** { **per-user-limit** | **total-user-limit** [**intelligent**] | **per-ap-limit** } { **down-streams** | **up-streams** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*

【参数说明】 **per-user-limit**：对 WLAN 上的每个用户进行限速。

total-user-limit：对整个 WLAN 进行限速。

intelligent：表示是否对 total 进行智能限速。

per-ap-limit：对每个 AP 各自做 WLAN TOTAL 限速。

down-streams：表示设置 WLAN 的下行流量限速参数。

up-streams：表示设置 WLAN 的上行流量限速参数。

average-data-rate：表示设置平均速率限制，单位为 8Kbps，范围为 8-261120。

burst-data-rate：表示设置突发速率限制，单位为 8Kbps，范围为 8-261120。

【缺省配置】 缺省为无流量限速。

【命令模式】 AC:WLAN 配置模式，胖 AP:全局配置模式

【使用指导】 -

检验方法

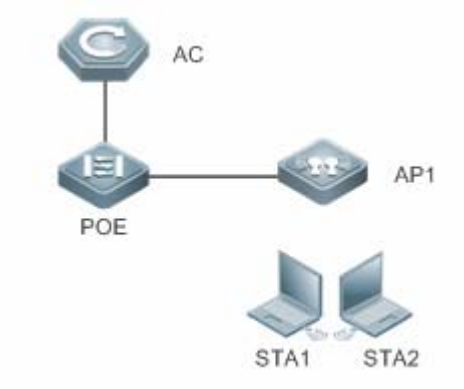
- 使用 **show dot11 ratelimit ap** 查看基于 AP 的流量限速信息。
- 使用 **show dot11 ratelimit user** 查看基于 STA 的流量限速信息。
- 使用 **show dot11 ratelimit wlan** 查看基于 WLAN 的流量限速信息。

配置举例

配置基于 AP 的流量限速

【网络环境】

图 1-2



【配置方法】

AC

- AP 配置模式下，配置基于 AP 的 per-user 下行流量限速。

```
Ruijie#configure terminal
Ruijie(config)# ap-config ap1
Ruijie(config-ap)#ap-based per-user-limit down-streams average-data-rate 100000 burst-data-rate 120000
Ruijie(config-ap)# exit
```

【检验方法】

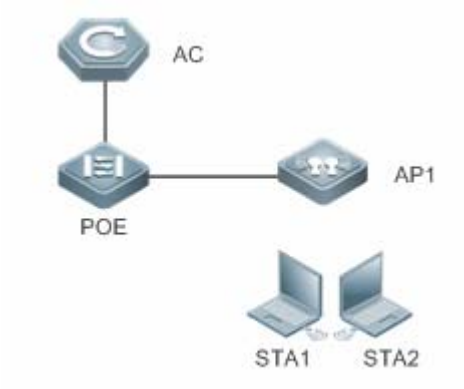
AC

通过 **show dot11 ratelimit ap** 显示配置信息。

```
AC_20_3F#show dot11 ratelimitap
AP name :test, ratelimit info(unit :8kbps):
Per-user-limit:
    Upstream   : average rate - 0 , burst rate - 0
    Downstream : average rate - 100000, burst rate - 120000
Total-user-limit:
    Upstream   : average rate - 0 , burst rate - 0
```

【网络环境】

图 1-2



【配置方法】

AC

- AP 配置模式下，配置基于 AP 的 per-user 下行流量限速。

```
Ruijie#configure terminal
Ruijie(config)# ap-config ap1
Ruijie(config-ap)#ap-based per-user-limit down-streams average-data-rate 100000 burst-data-rate 120000
Ruijie(config-ap)# exit
```

【检验方法】 通过 **show dot11 ratelimit ap** 显示配置信息。

```
    Downstream : average rate - 0 , burst rate - 0
```

常见错误

- 无。

1.5.2 配置公平调度

配置效果

- 用公平调度功能可以防止低速 STA 拖慢整个无线网络的吞吐量，而且能够为 STA 提供更加平滑的网速体验。

注意事项

- 在胖 AP 上，配置公平调度的命令位于全局配置模式下，使用 **show running-config** 查看配置。
- 当 AP 工作在瘦 AP 模式时，公平调度功能只能在 AC 上进行配置。

配置方法

开启公平调度功能

- 必须配置。
- AC 上，在 AP 配置模式下通过 **fair-schedule** 命令配置。
- 胖 AP 上，在全局配置模式下通过 **fair-schedule** 配置。
- 开启公平调度功能，使得可以时间公平的给 STA 分配时间。

【命令格式】 **fair-schedule**
【参数说明】 -
【缺省配置】 公平调度功能开启
【命令模式】 AP 配置模式，或者全局配置模式
【使用指导】 -

配置公平调度优先级

- 可选配置。如果需要提高某一 STA 的优先级的话，必须配置。
- AC 上，在 AC 配置模式下通过 **sta-fair** 命令配置。
- 胖 AP 上，在全局配置模式下通过 **sta-fair** 命令配置。

【命令格式】 **sta-fair** *mac-address* **priority** *priority*
【参数说明】 *mac-address*：表示需要设置的用户 MAC 地址。
priority：优先级别，范围：1 到 6
【缺省配置】 缺省所有的 STA 优先级为 1。数值越大代表优先级越高，优先级越高，分配给 STA 的空口时间越多。
【命令模式】 AC 配置模式，或者全局配置模式
【使用指导】 -

检验方法

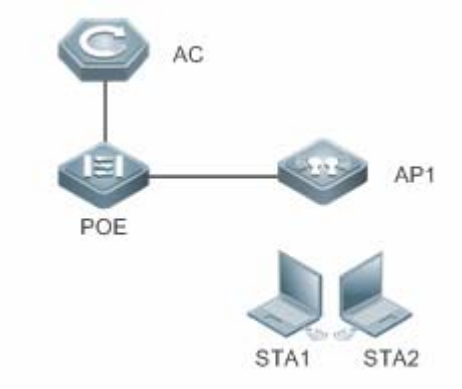
- 使用 **show ap-config run** 查看配置信息

配置举例

开启公平调度功能，并设置优先级

【网络环境】

图 1-3



【配置方法】

- AP 配置模式下，开启公平调度功能。
- AC 配置模式下，配置 STA 优先级。

AC

```
Ruijie#configure terminal
Ruijie(config)# ap-config ap1
Ruijie(config-ap)#fair-schedule
Ruijie(config-ap)# exit
Ruijie(config)#ac-controller
Ruijie(config-ac)#sta-fair 1111.1111.1111 priority 6
Ruijie(config-ac)# end
```

【检验方法】 通过 **show ap-config running** 和 **show running-config** 显示配置信息。

AC

```
Ruijie# show ap-config running
!
ap-configap1
!
Ruijie# show running-config
!
ac-controller
sta-fair 1111.1111.1111 priority 6
!
```

常见错误

- 无。

1.5.3 配置防内网代理

配置效果

- 检测无线内网中 STA 作为其他 STA 的代理服务器，从而达到对 STA 数量和网络流量的准确监控。

注意事项

- 无。

配置方法

↘ 开启防内网代理功能

- 必须配置。可以选择 ttl 检测策略，或者 tcp 源端口检测策略。
- AC 上，在 AP 配置模式下开启。在 AP 配置模式下，使用 **illegal-sta-check** 命令可以开启防内网代理功能。
- 开启防内网代理功能，可以检测一台 STA 给另一台 STA 提供代理服务器服务的情况，并进行反制。
- 开启防内网代理功能，使用 ttl 检测策略

【命令格式】 **illegal-sta-check ip ttl**
【参数说明】 -
【缺省配置】 缺省关闭
【命令模式】 AP 配置模式
【使用指导】 -

- 开启防内网代理功能，使用 tcp 源端口检测策略

【命令格式】 **illegal-sta-check tcp source-ports** [*port-num*]
【参数说明】 *port-num*：设置端口检测数量的上限，范围在 1 到 512 之间
【缺省配置】 缺省关闭
【命令模式】 AP 配置模式
【使用指导】 -

检验方法

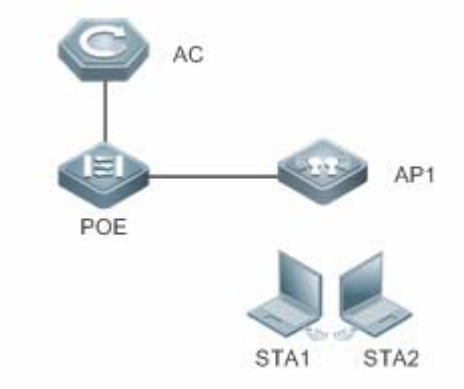
- 通过 **show running-config** 查看相应的配置。

配置举例

↘ 开启防内网代理功能

【网络环境】

图 1-4



【配置方法】

- AP 配置模式下，开启防内网代理功能

AC

```
Ruijie#configure terminal
Ruijie(config)# ap-config ap1
Ruijie(config-ap)# illegal-sta-check ip ttl
Ruijie(config-ap)# illegal-sta-check tcp source-ports
Ruijie(config-ap)# end
```

【检验方法】

通过 **showap-config running** 显示配置信息。

AC

```
Ruijie# show ap-config running ap1
!
ap-configap1
 illegal-sta-check ip ttl
 illegal-sta-check tcp source-ports
!
```

常见错误

- 无。

1.6 监视与维护

清除各类信息

无。

查看运行情况

作用	命令
显示 WQOS 限速信息	**show dot11 ratelimit** {**wlan** | **ap** | **user** }

查看调试信息

无。

2 WMM

2.1 概述

WMM 是一种无线 QoS 协议，是 802.11e 协议的一个子集。

用于保证高优先级的报文有优先的发送权利，从而保证语音、视频等应用在无线网络中有更好的质量。

本文分为两部分内容：WMM 服务和 QoS 报文优先级映射。

- WMM 服务：区分不同优先级的接入信道的能力，从而保障了信道资源依据数据流优先级分配。用户可以根据实际需求，调整客户端或 AP 使用的 EDCA 参数值，使高优先级的 AC 在竞争中可以更早地进行退避过程，从而优先接入信道。
- QoS 报文优先级映射：无线 QoS 到有线 QoS 以及有线 QoS 到无线 QoS 的映射关系，进而实现了全网的端到端 QoS，保证高优先级业务流的质量。

下文仅介绍 WMM 的相关内容。

协议规范

- IEEE 802.11e-2005：Amendment 8：Medium Access Control (MAC) Quality of Service Enhancements, IEEE Computer Society
- RFC5416：Control and Provisioning of Wireless Access Points(CAPWAP) Protocol Binding for IEEE802.11

2.2 典型应用

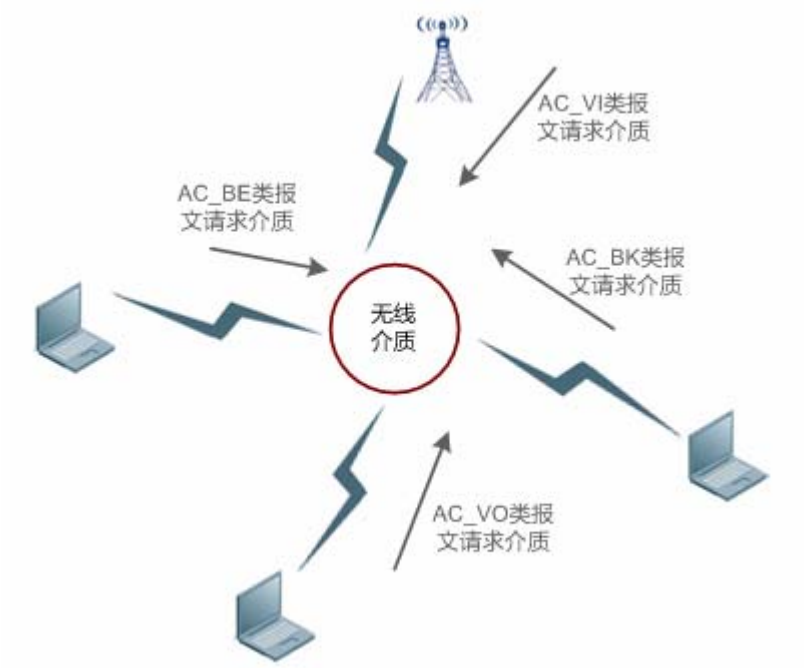
典型应用	场景描述
WMM 服务场景	不同优先级的信道竞争过程。
无线到有线优先级映射场景	无线到有线 QoS 报文优先级映射过程。
有线到无线优先级映射场景	有线到无线 QoS 报文优先级映射过程。

2.2.1 WMM服务场景

应用场景

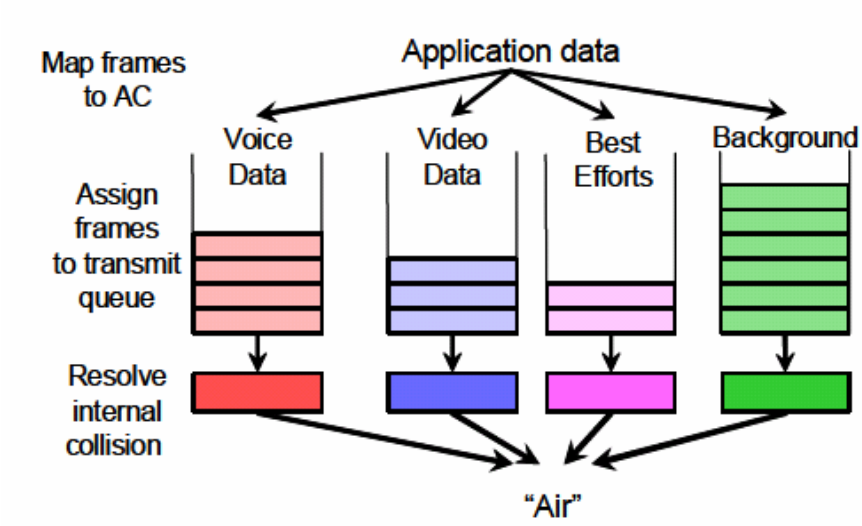
无线通信依靠的介质是无线电，在特定的频段，信道是共享的，即无线网络通信是共享信道的，在同一个射频环境中，各个站点的上下行流量就会产生冲突，因此，无线 QoS 需要解决在共享信道中，通信的参与者之间如何竞争信道的问题。如下图所示，在同一无线网络环境下有 4 种不同优级类型报文(优先级从高到低分别为 AC_VO，AC_VI，AC_BE 和 AC_BK)需要请求介质发送报文，竞争信道情况下将通过竞争协调机制决定哪一个请求者的报文可以获取介质的访问权，使用高优先级的报文应该有较大的机率取得信道的访问权。

图 2-1 竞争信道情况



在无线网络中，由于介质的特殊性，在网络传输过程中产生的丢包和信号干扰导致包损坏的现象是比较严重的，需要重传机制不同的无线传输参数来保证报文能顺利到达，但是对所有的报文都采用较好的参数是不现实的，在这样的情况下，为了保证一些对可靠性实时性要求高的业务的顺利进行，采用对报文分类的方法。简单地说，就是针对各种不同需求，提供不同的网络服务质量，对实时性强，重要的数据报文提供更好的服务质量，优先处理；而对于实时性不强，一般的普通数据报文，则提供较低的处理优先级。若要在网络上承载各种不同的业务，就要求网络不仅能提供单一的尽力而为的服务，而且能为不同业务提供不同的 QoS。因此无线 AP 的 QoS 需要报文的分类/标识，区分不同的数据流并且提供不同质量的服务。

图 2-2 无线 QoS 多优先级队列



功能部属

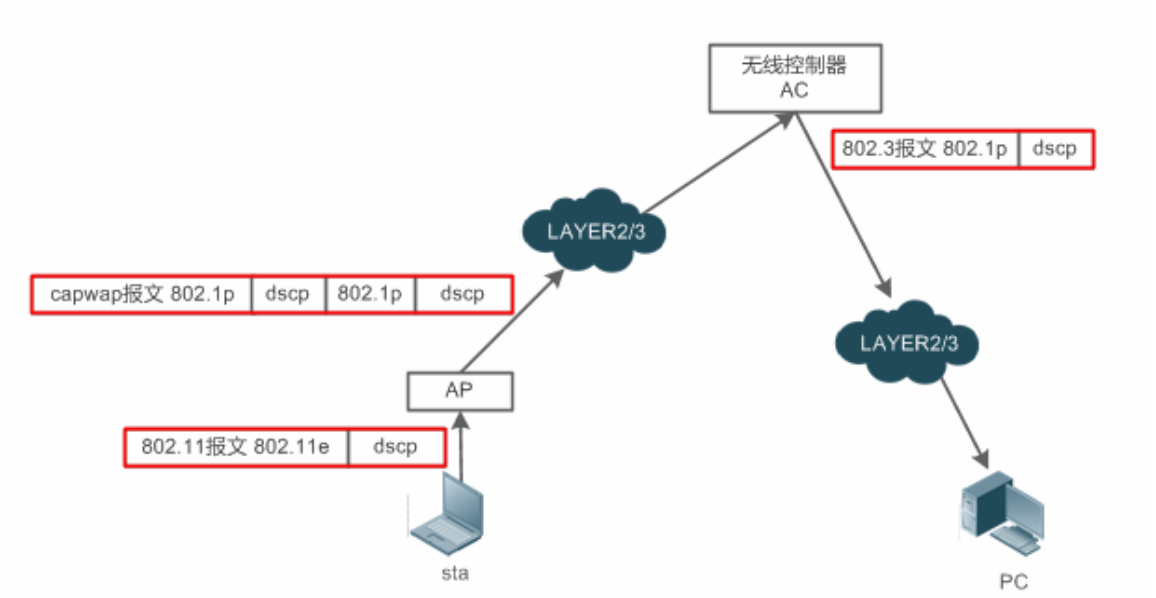
设备端的配置要点如下：

- 设置 WMM 使能。
- 设置 WMM EDCA 竞争参数，一般采用默认值。

2.2.2 无线到有线优先级映射场景

应用场景

图 2-3 无线到有线报文的优先级映射



STA TO PC 情况下的优先级映射过程：

- 无线用户 STA 发送带 802.11e 和 dscp 信息的 802.11 报文到 AP；
- AP 根据无线端口（基于 BSSID、在 AC 的 ESS 上配置）的信任模式设置报文的内部优先级；如果信任报文为 802.11e 优先级，则根据入报文的 802.11e 设置转换成有线报文的 802.1p 和 dscp 优先级和经过 CAPWAP 封装过的 CAPWAP 报文的 802.1p 和 dscp 优先级。如果信任模式为 dscp 优先级，则根据传入无线报文的 dscp 优先级进行上述设置。目前 ETH 信任默认为 dscp，无线端固定映射到 dot11e。
- CAPWAP 报文在经过 LAYER 2/3 网络时按照有线的 QoS 方法进行处理。
- 无线控制器收到 CAPWAP 报文后进行解封装，然后转发解封装后的有线报文到 LAYER 2/3 网络。
- 有线报文在经过 LAYER 2/3 网络时按照有线的 QoS 方法进行处理。

功能部属

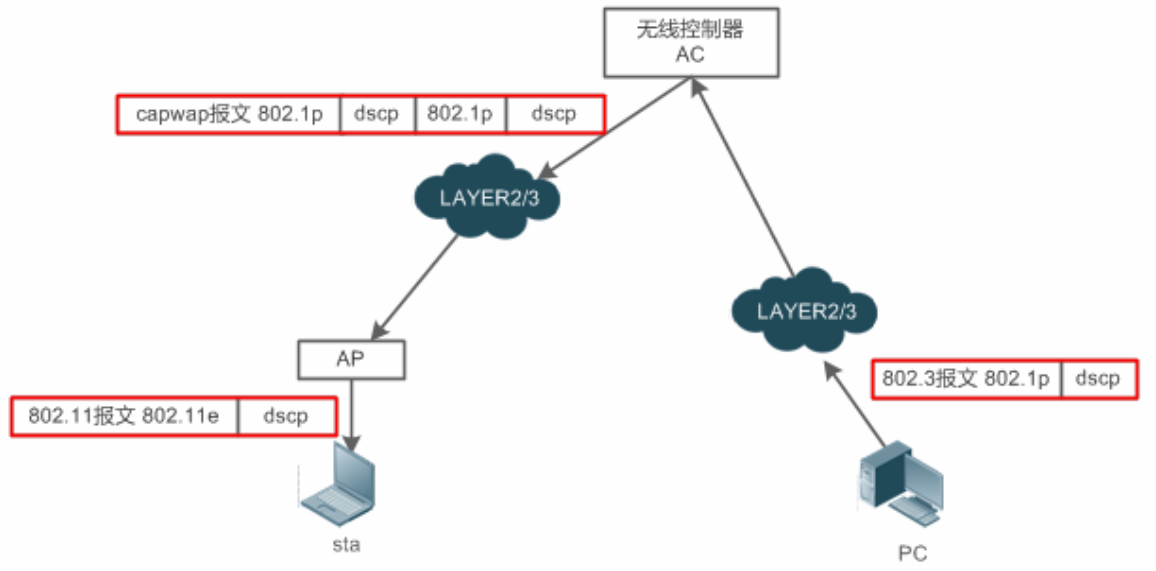
设备端的配置要点如下：

- 设置 WMM 使能。
- 设置无线到有线优先级映射表，一般采用默认值。

2.2.3 有线到无线优先级映射场景

应用场景

图 2-4 有线到无线报文的优先级映射



PC TO STATION 情况下的 QoS 映射过程

- AC 收到 PC 发送过来的 802.3Mac 报文；
- 根据物理端口的信任模式设置报文的内部优先级 COS。如果信任报文的 802.1p 优先级且报文带 TAG 则取报文，则根据入报文的 802.1p 设置报文的内部优先级 COS，否则，根据端口的缺省优先级设置报文的缺省优先级；如信任模式是 dscp 则根据传入报文的 dscp 优先级进行上述设置。目前 ETH 信任默认为 dscp，无线端固定映射到 dot11e。
- AC 对 802.3 报文进行 capwap 封装。
- AP 收到 CAPWAP 报文并进行解封装，根据 QoS 优先级信任模式对解封装后有线将到无线报文进行 QoS 优先级映射。如果信任模式是 DSCP，则根据 802.3 报文的 dscp 字段值设置无线报文的 802.11e 和 dscp 字段时行映射；如果信任模式是 802.1p 则根据有线 802.3 报文的 cos 字段进行相应设置。
- AP 根据无线报文的 802.11e 优先级参与无线信道的竞争并将无线报文发送到 STA。

功能部属

设备端的配置要点如下：

- 设置 WMM 使能。
- 设置有线到无线优先级映射表，一般采用默认值。

2.3 功能详解

基本概念

接入类

WMM 标准将接入的数据流分为四个优先级，每一个优先级作为一个分类，优先级从低到高分别是：背景（AC_BK，Background）、尽力而为（AC_BE，Best Efforts）、视频（AC_VI，Video Data）、语音（AC_VO，Voice Data）。

EDCA 竞争机制

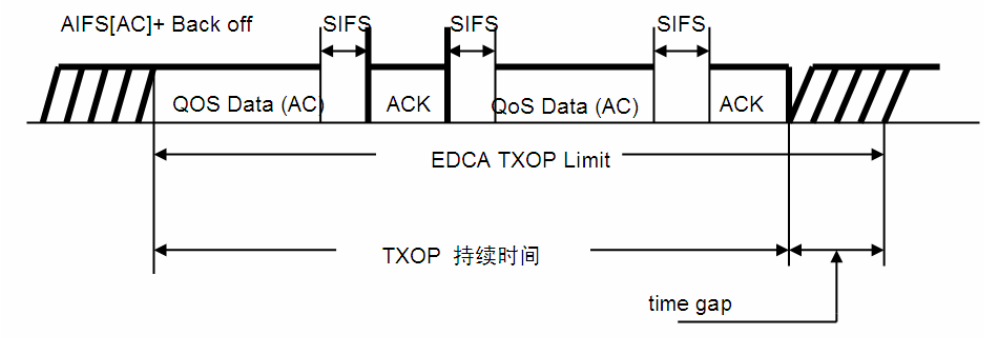
EDCA 竞争机制是 IEEE 802.11e 的核心，EDCA 区分了不同优先级的 AC 接入信道的能力，从而保障了空口资源依据数据流优先级分配。EDCA，增强的分布式信道接入，在保留 AP/STA 间的分布式信道竞争外，引入了 QAP/QSTA 内部四个优先级分类的内部竞争，从而在无线空口引入不同 QAP/QSTA 间区分优先级分类的信道竞争机制。EDCA 通过配置不同优先级类的竞争参数来实现信道的竞争，QAP 为 QSTA 下发竞争参数，控制 QSTA 的接入能力，竞争参数包含：AIFS、TXOP Limit、CWmin、CWmax。

EDCA 参数

EDCA 竞争参数含义如下：

- AIFSN（Arbitration Inter Frame Spacing Number，仲裁帧间隙数），在 802.11 协议中，空闲等待时长（DIFS）为固定值，而 WMM 针对不同 AC 可以设置不同的空闲等待时长，AIFSN 数值越大，用户的空闲等待时间越长。等待时间越短则获取信道的机会更大；
- ECWmin（Exponent form of CWmin，最小竞争窗口指数形式）和 ECWmax（Exponent form of CWmax，最大竞争窗口指数形式)，决定了平均退避时间值，这两个数值越大，用户的平均退避时间越长；
- TXOP（Transmission Opportunity，传输机会），用户一次竞争成功后，可占用信道的最大时长。数值越大，用户一次能占用信道的时长越大，如果为 0，则每次占用信道后只能发送一个报文。如果一个帧太大导致不能在一个 TXOP 内发送完毕，则必须分片。

图 2-5 TXOP 连续帧传送示意图



ACK 策略

ACK 策略有两种：Normal ACK 和 No ACK。

- Normal ACK：对每个发送的单播报文，接收者在成功接收后都发送一个 ACK 回应。
- No ACK：在通信质量较好，环境干扰较少的情况下，可以设置某一个优先级的流不需要 ACK 报文回复进行确认，以节省回复的 ACK 帧占用的信道资源。无线报文交互时可以不使用 ACK 报文进行确认。No ACK 策略能有效提高传输效率，但也有可能造成丢包问题。

IEEE 802.11 标准规定组播、广播帧不回复 ACK。

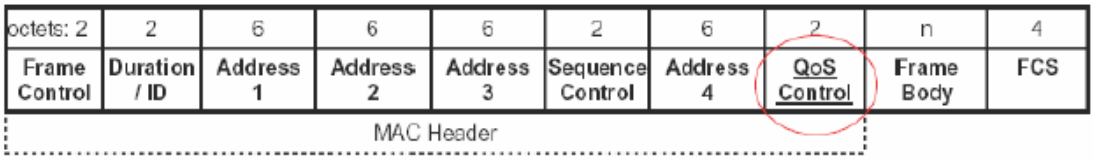
AC 队列深度

不同优先级队列的深度，如果大于设定的 AC 队列深度值，则丢弃报文。否则按正常的逻辑入队处理。

802.11e 优先级

802.11e 扩展了 802.11 的 MAC 头，新增了 QoS Control 域，如下图所示：

图 2-6 802.11e MAC Header



QoS Control 域有 2 个字节，其中，前 3 个 Bit 是 TID 字段，表示数据形态识别码。TID 值 0-7 用于具有优先权的 QoS，表示使用者的优先顺序（UP），值 8-15 用于参数化的 QoS，表示数据流 ID（TSID）。

WMM 将 UP 对应相应的 AC。802.11e 优先级同 AC 映射表如下表所示：

Priority	UP（User Priority）	AC（Access Category）
Lowest ↓ **Highest**	1	Back-ground
	2	Back-ground
	0	Best-effort
	3	Best-effort
	4	Video
	5	Video
	6	Voice
	7	Voice

优先级映射表

报文在进入设备以后，设备首先需要判断当前接口的报文信任模式，即接收的报文中哪个部分的优先级信息有效，以及当前 AP 的工作模式（胖 AP 瘦 AP）；然后根据设定信息选择映射关系表，进行优先级的映射操作。

设备提供了优先级映射表，分别对应相应的优先级映射关系。

功能特性

功能特性	作用
WMM 服务	用于配置 WMM 服务相关内容，包括 EDCA 竞争参数，AC 队列深度和 ACK 策略。
QoS 报文优先级映射	用于配置 QoS 报文优先级映射相关内容，包括 QoS 报文优先级映射表以及优先级映射策略。

2.3.1 WMM服务

用于配置 WMM 服务相关内容，包括 EDCA 竞争参数，AC 队列深度和 ACK 策略。

工作原理

针对各种不同需求，提供不同的网络服务质量，对实时性强，重要的数据报文提供更好的服务质量，优先处理；而对于实时性不强，一般的普通数据报文，则提供较低的处理优先级。WMM 标准将接入的数据流分为四个优先级，每一个优先级作为一个分类，EDCA 区分了不同优先级的 AC 接入信道的能力，从而保障了空口资源依据数据流优先级分配。

↘ WMM 使能

设置开启/关闭 WMM 服务。开启 WMM 服务，使用四级优先级队列接收与映射。关闭 WMM 服务，采用默认的优先级队列接收与映射。

↘ EDCA 竞争机制、AC 队列深度，NO ACK 策略

- EDCA 竞争机制：

EDCA 参数区分了不同优先级的接入信道的能力，每个接 AC 均有独立的 EDCA 信道竞争参数。用户可以根据实际需求，调整客户端或 AP 的 EDCA 参数值，使高优先级的 AC 在竞争中可以更早地进行退避过程，从而优先接入信道。信道的竞争完全由硬件自动完成，软件上只需要设置好各硬件队列的 CWmin，CWmax，AIFSN，TXOP 这几个参数，硬件将根据设置的参数参与信道的竞争。

实际配置中可根据应用需求选择配置 client 端或者 AP 端的 EDCA 参数。配置 edca-client 主要影响 sta 的 wmm 竞争参数，配置 edca-radio 主要影响 AP 的 wmm 竞争参数。

QSTA 的信道竞争参数由 QAP 统一管理和下发。QAP 和 QSTA 的信道竞争参数完全独立。一般可以稍稍提高 QAP 的信道竞争参数，保障 QAP 有足够高的信道控制能力。QAP 通过 beacon 或 Probe Response 帧中的 EDCA Parameter S et IE 通告 QAP 的 EDCA 参数设置，通过(Re)Association Response 帧中的 EDCA Parameter Set IE 将经过协商的 EDCA 参数设置下发给 QSTA。

- AC 队列深度：

设置 AC 队列深度值，根据当前 AC 硬件队列的长度（里面的报文个数）作为判断条件，如果大于设定的 AC 队列深度值，则丢弃报文。否则按正常的逻辑入队处理。

- NO ACK 策略：

设置 NO ACK（No Acknowledgment）策略开启/关闭。NO ACK 策略包括发送方和接收发同时支持，对于 NO ACK 策略帧发送芯片不支持把把某个硬件发送队列设置为 NO ACK，而只能对发送的每一帧报文分别设置 NO ACK 策略，在发送帧的 DMA 描述符中进行设置。

NO ACK 策略，是针对通信质量较好，干扰较小的情况下，在无线报文交互过程中，不使用 ACK 报文进行接收确认的一种策略。NO ACK 策略能有效提高传输效率，但在不使用 ACK 确认的情况下，如果通信质量较差，即使接收端没有收到发送包，发送端也不会重发，所以会造成丢包率增大的问题。

2.3.2 QoS报文优先级映射

用于配置 QoS 报文优先级映射相关内容，包括 QoS 报文优先级映射表以及优先级映射策略。

工作原理

设备提供了优先级映射表，分别对应相应的优先级映射关系。然后根据设定信息选择映射关系表，进行优先级的映射操作，进而实现了全网的端到端 QoS。

↘ 报文优先级映射

在 IP 网络中，IPv4 报文中有三种承载 QoS 优先级标签的方式，分别为基于二层的 CoS 字段（IEEE802.1p）的优先级、基于 IP 层的 IP 优先级字段 ToS 优先级和基于 IP 层的 DSCP（Differentiated Services Codepoint，差分服务代码点）字段优先级。

对于有线报文三种 QoS 优先级标签的方式，DSCP 兼容 ToS 因此只要支持 DSCP 和 dot1P 两种 QoS 即可。无线报文除上述三种外又多一种 dot11e 的 QoS 优先级标签方式。

报文优先级映射操作的判断执行部分，首先需要判断当前接口的报文信任模式或标签策略，即接收的报文中哪个部分的优先级信息有效，以及当前 AP 的工作模式（集中转发或本地转发），然后即可根据设定信息选择映射关系表，进行优先级的映射操作。

2.4 产品说明

NBR800G、NBR950G、NBR1500G、NBR2000G 不支持无线集成 AC 功能，NBR108G-P、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR2500D-E、NBR3000D-E、NBR3000D-UE、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持无线集成 AC 功能。

2.5 配置详解

配置项	配置建议 & 相关命令	
配置 WMM 服务	⚠ 必须配置。用于启用 WMM 服务。	
	wmm enable	启用 WMM 服务
	⚠ 可选配置。用于配置竞争参数。	
	wmm edca-client	配置客户端的 EDCA 参数
	wmm edca-radio	配置 AP 使用的 EDCA 参数
配置 QoS 报文优先级映射	⚠ 可选配置。用于配置优先级映射。非互通版本映射命令。	

	wlan-qos map-table	配置当前 WLAN 的报文优先级映射关系
	可选配置。用于配置 802.11p QoS 策略映射机制。互通版本映射命令。	
	wmm dot1p enable	开启 802.11p QoS 映射策略机制
	wmm dot1p policy 1q	配置 AP 如何应用 802.11p QoS 映射策略机制
	wmm dot1p tag	配置 802.1p 优先级
	可选配置。用于配置 dscp QoS 策略映射机制。互通版本映射命令。	
	wmm dscp enable	开启 dscp QoS 映射策略机制
	wmm dscp policy outer-tunnel inner-tunnel	配置 AP 如何应用 dscp QoS 映射策略机制
	wmm dscp tag	配置 dscp 标识

2.5.1 配置WMM服务

配置效果

- 配置客户端 EDCA 竞争参数。
- 配置 AP 使用的 EDCA 竞争参数。
- 配置 ACK 策略。
- 配置优先级队列长度

注意事项

- 开启 WMM 服务后配置的参数才能生效。
- 开启 WMM 服务且 BE 队列是默认配置值时，Xspeed 功能会动态调整 BE 队列的参数。

配置方法

↘ 启动 WMM 服务

- 必须配置。
- 使用 **wmm enable radio** *radio-id* 命令瘦 AP 在 AP 配置模式下，胖 AP 在接口配置模式下配置 WMM 使能开关。
- 开启 WMM 服务，使用四级优先级队列接收与映射。关闭 WMM 服务，采用默认的优先级队列接收与映射。

【命令格式】 **wmm enable radio** *radio-id*

【参数说明】 **radio** *radio-id*：表示选择开启/关闭 WMM 服务的 radio，范围为 1-48。胖 AP 上无此参数，仅 AC 支持该参数的配置。

【缺省配置】 WMM 使能开启

【命令模式】 瘦 AP 下在 AP 配置模式，胖 AP 下在接口配置模式。

【使用指导】 WMM 服务关闭，采用默认的优先级队列接收与映射。

配置客户端 EDCA 参数

- 可选配置。
- 缺省情况下，client 端 EDCA 参数值如下表所示：

AC	aifs	cwmin	cwmax	txop
back-ground	7	4	10	0
best-effort	3	4	10	0
video	2	3	4 94	
voice	2	2	3 47	

- 配置 client 端的 EDCA 参数，AC 队列深度为非默认后会按照配置的值进行处理，否则按默认值进行处理。

【命令格式】 **wmm edca-client** { **back-ground** | **best-effort** | **video** | **voice** } { **aifsn** [*aifsn-value*] **cwmin** [*cwmin-value*] **cwmax** [*cwmax-value*] **txop** [*txop-value*] | **length** [*queue-length*] } **radio** *radio-id*

【参数说明】 **back-ground**：表示将设置 back-ground 队列。

best-effort：表示将设置 best-effort 队列。

video：表示将设置 video 队列。

voice：表示将设置 voice 队列。

aifsn *aifsn-value*：表示设置 aifsn 值，范围为 1-15。

cwmin *cwmin-value*：表示设置 cwmin 值，范围为 0-15。

cwmax *cwmax-value*：表示设置 cwmax 值，范围为 0-15。

txop *txop-value*：表示设置 txop 值，范围为 0-255，单位为 32 微秒。

length *queue-length*：表示设置 AC 队列长度，范围为 1-255。默认为最大值。

radio *radio-id*：表示选择设置客户端 EDCA 参数的 radio，范围为 1-48。胖 AP 上无此参数，仅 AC 支持该参数的配置。

no：no 表示恢复默认配置。

【缺省配置】 见上述缺省表

【命令模式】 瘦 AP 下在 AP 配置模式，胖 AP 下在接口配置模式。

【使用指导】 wmm 服务开启时，配置的参数才能生效。

cwmax 值必须大于 cwmin 值。否则提示配置失败。

配置 AP 使用的 EDCA 参数

- 可选配置。
- 缺省情况下，AP 端 EDCA 参数值如下表所示：

AC	aifs	cwmin	cwmax	txop
back-ground	7	4	10	0
best-effort	3	4	6 0	
video	1	3	4 94	

voice	1	2	3 47	

- 配置 AP 端的 EDCA 参数，NO ACK 策略为非默认后会按照配置的值进行处理，否则按默认值进行处理。
- 高优先级的 AC AIFS 时间越短，可以更早的进行退避过程。而由 CWmin 和 CWmax 决定的 Backoff 时间，同样值越小 Backoff 的时间越短。TXOP limit 允许 AC 在竞争到传输机会后 ,在 SIFS 间隔时间内连续传输本 AC 下的多帧报文 ,TXOP limit 越大则在一定程度上降低了报文冲突率和空口资源浪费。

【命令格式】 **wmm edca-radio** { **back-ground** | **best-effort** | **video** | **voice** } { **aifsn** [*aifsn-value*] **cwmin** [*cwmin-value*] **cwmax** [*cwmax-value*] **txop** [*txop-value*] | **noack** } **radio** *radio-id*

【参数说明】 **back-ground**：表示将设置 back-ground 队列。
best-effort：表示将设置 best-effort 队列。
video：表示将设置 video 队列。
voice：表示将设置 voice 队列。
aifsn *aifsn-value*：表示设置 aifsn 值，范围为 1-15。
cwmin *cwmin-value*：表示设置 cwmin 值，范围为 0-15。
cwmax *cwmax-value*：表示设置 cwmax 值，范围为 0-15。
txop *txop-value*：表示设置 txop 值，范围为 0-255，单位为 32 微秒。
noack：表示开启 no ack 策略。默认不开启 no ack 策略。
radio *radio-id*：表示选择设置客户端 EDCA 参数的 radio，范围为 1-48。胖 AP 上无此参数，仅 AC 支持该参数的配置。
no：no 表示恢复默认配置。

【缺省配置】 见上述缺省表

【命令模式】 瘦 AP 下在 AP 配置模式，胖 AP 下在接口配置模式。

【使用指导】 wmm 服务开启时，配置的参数才能生效。
cwmax 值必须大于 cwmin 值。否则提示配置失败。

检验方法

- 瘦 AP 下使用 **show run** 与 **show ap-config run** 命令，胖 AP 下使用 **show run** 命令，可以查看 WMM 服务状态，当前生效的客户端的 EDCA 参数与 AP 使用的 EDCA 参数，默认配置时不显示。
- 抓包查看客户端的 EDCA 参数。

配置举例

以下配置举例，仅介绍与 WMM 服务相关的配置。

配置 WMM 服务参数

【配置方法】
- 配置 AP 上开启/关闭 WMM 服务。
- 配置客户端的 EDCA 参数。
- 配置 AP 使用的 EDCA 参数。

```
Ruijie # configure terminal
Ruijie(config)# ap-config AP001
```

```
Ruijie(config-ap)# wmm enable radio 1
Ruijie(config-ap)# wmm edca-client voice aifsn 2 cwmin 2 cwmax 3 txop 50 radio 1
Ruijie(config-ap)# wmm edca-radio voice aifsn 1 cwmin 1 cwmax 3 txop 50 radio 1
```

【检验方法】 瘦 AP 下使用 **show run** 与 **show ap-config run** 命令,胖 AP 下使用 **show run** 命令，查看当前生效的客户端的 EDCA 参数与 AP 使用的 EDCA 参数，默认配置时不显示。

常见错误

- 如果 radio 不存在，则提示错误。
- EDCA 参数配置不合理时，影响性能。例如：低优先级的配置参数比高优先级的配置参数值优，影响高优先级的性能。

2.5.2 配置QoS报文优先级映射

配置效果

- 配置当前 WLAN 的报文优先级映射关系。
- 配置 802.11p QoS 映射策略机制。
- 配置 dscp QoS 映射策略机制。

注意事项

- 开启 WMM 服务后 QoS 报文优先级映射才能生效。

配置方法

缺省情况下，dscp 到 802.11e 映射表如下表所示:

dscp	802.11e
0~7	0
16~23	1
24~31	2
8~15	3
32~39	4
40~47	5
48~55	6
56~63	7

映射表缺省情况下，802.11e 到 DSCP 映射表如下表所示:

802.11e	dscp
0	0

3	8
1	16
2	24
4	32
5	40
6	48
7	56

配置当前 WLAN 的报文优先级映射关系

- 可选配置。
- 配置当前 WLAN 的报文优先级映射关系：若无特殊要求，应在每台 AP 上配置当前 WLAN 的报文优先级映射关系。

配置优先级映射，映射表对应值为非默认会按照配置的值进行处理，否则按默认值进行处理。

【命令格式】 **wlan-qos map-table** { **dot11e-inner-dscp** | **dot11e-tunnel-dscp** | **dscp-dot11e** } **import** *import-tag-value* **export** *export-tag-value*

【参数说明】 **dot11e-inner-dscp**：表示设置 dot11e 到内部 dscp 的优先级映射。

dot11e-tunnel-dscp：表示设置 dot11e 到 CAPWAP dscp 的优先级映射。

dscp-dot11e：表示设置 dscp 到 dot11e 的优先级映射。

import *import-tag-value*：表示设置进入的原始报文优先级。

export *export-tag-value*：表示设置输出的报文优先级。

no：表示还原报文映射关系为默认值。

【缺省配置】 见上述表格

【命令模式】 WLAN 配置模式

【使用指导】 此命令为非互通版本映射命令。

wmm 服务开启时，配置才能生效。

胖 AP 不支持 dot11e-tunnel-dscp，dot11e-inner-dscp 为 dot11e-dscp。

802.11p QoS 映射策略机制

- 可选配置。
- 若无特殊要求，应在每台 AP 上关闭 802.11p QoS 映射策略机制。

开启 802.11p QoS 策略机制，使用 802.11p QoS 相关映射表。关闭 802.11p QoS 策略机制，采用默认方式映射。

【命令格式】 **wmm dot1p enable radio** *radio-id*

【参数说明】 **radio** *radio-id*：表示选择开启/关闭 802.11p QoS 映射策略机制的 radio，范围为 1-48。胖 AP 上无此参数，仅 AC 支持该参数的配置。

no：no 表示恢复默认配置。

【缺省配置】 关闭 802.11p QoS 映射策略机制

【配置模式】 瘦 AP 下在 AP 配置模式，胖 AP 下在接口配置模式。

【使用指导】 此命令为互通版本映射命令。

wmm 服务开启时，配置才能生效。

配置 AP 如何应用 802.11p QoS 映射策略机制

- 可选配置。
- 配置 AP 如何应用 802.11p QoS 映射策略机制：若无特殊要求，应在每台 AP 上配置 AP 如何应用 802.11p QoS 映射策略机制。

根据配置的 AP 如何应用 802.11p QoS 映射策略机制决定 802.1Q 的优先级从哪里获取。

【命令格式】 **wmm dot1p policy 1q** [*1q-policy-value*] **radio** *radio-id*

【参数说明】 **1q** *1q-policy-value*：表示设置应用 802.11p QoS 映射策略机制，范围为 0-1。默认值为 0。

radio *radio-id*：表示 AP 如何应用 802.11p QoS 映射策略机制的 radio，范围为 1-48。胖 AP 上无此参数，仅 AC 支持该参数的配置。

no：no 表示恢复默认配置。

【缺省配置】 默认配置为 0

【配置模式】 瘦 AP 下在 AP 配置模式，胖 AP 下在接口配置模式。

【使用指导】 此命令为互通版本映射命令。

wmm 服务开启时，配置才能生效。

开启 802.11p QoS 机制时，配置应用 802.11p QoS 映射策略机制才有效。

配置 802.1p 优先级

- 可选配置。
- 配置 802.1p 优先级：若无特殊要求，应在每台 AP 上配置 802.1p 优先级。

根据配置的 802.1p 优先级决定 802.1p 的优先级。

【命令格式】 **wmm dot1p tag** [*tag-value*] { **back-ground** | **best-effort** | **video** | **voice** } **radio** *radio-id*

【参数说明】 **tag** *tag-value*：表示设置 802.1p 优先级，范围为 0-7，best-effort 默认值为 0，back-ground 默认值为 2，video 默认值为 4，voice 默认值为 6。

back-ground：表示将设置 back-ground 队列。

best-effort：表示将设置 best-effort 队列。

video：表示将设置 video 队列。

voice：表示将设置 voice 队列。

radio *radio-id*：表示选择开启/关闭 802.11p QoS 映射策略机制的 radio，范围为 1-48。胖 AP 上无此参数，仅 AC 支持该参数的配置。

no：no 表示恢复默认配置。

【缺省配置】 best-effort 默认值为 0，back-ground 默认值为 2，video 默认值为 4，voice 默认值为 6

【配置模式】 瘦 AP 下在 AP 配置模式，胖 AP 下在接口配置模式。

【使用指导】 此命令为互通版本映射命令。

wmm 服务开启时，配置才能生效。

开启 802.11p QoS 机制时，802.1p 优先级才有效。

DSCP QoS 映射策略机制

- 可选配置。

- 若无特殊要求，应在每台 AP 上关闭 dscpQoS 映射策略机制。

开启 dscp QoS 策略机制，使用 dscp QoS 相关映射表。关闭 dscp QoS 策略机制，采用默认方式映射。

【命令格式】 **wmm dscp enable radio** *radio-id*

【参数说明】 **radio** *radio-id*：表示选择开启/关闭 dscp QoS 映射策略机制的 radio，范围为 1-48。胖 AP 上无此参数，仅 AC 支持该参数的配置。

no：no 表示恢复默认配置。

【缺省配置】 关闭 dscp QoS 策略机制

【配置模式】 瘦 AP 下在 AP 配置模式，胖 AP 下在接口配置模式。

【使用指导】 此命令为互通版本映射命令。

wmm 服务开启时，配置才能生效。

配置 AP 如何应用 DSCP QoS 映射策略机制

- 可选配置。
- 配置 AP 如何应用 dscp QoS 映射策略机制：若无特殊要求，应在每台 AP 上配置 AP 如何应用 dscp QoS 映射策略机制。

根据配置的 AP 如何应用 dscp QoS 映射策略机制决定 DSCP 域优先级从哪里获取。

【命令格式】 **wmm dscp policy outer-tunnel** [*outer-tunnel-value*] **inner-tunnel** [*inner-tunnel-value*] **radio** *radio-id*

【参数说明】 **outer-tunnel** *outer-tunnel-value*：表示设置 outer tunnel 头如何应用 dscp QoS 映射策略机制，范围为 0-1。默认值为 0。

inner-tunnel *inner-tunnel-value*：表示设置 inner tunnel 头如何应用 dscp QoS 映射策略机制，范围为 0-1。默认值为 0。

radio *radio-id*：表示 AP 如何应用 dscp QoS 映射策略机制的 radio，范围为 1-48。胖 AP 上无此参数，仅 AC 支持该参数的配置。

no：no 表示恢复默认配置。

【缺省配置】 默认配置为 0

【配置模式】 瘦 AP 下在 AP 配置模式，胖 AP 下在接口配置模式。

【使用指导】 此命令为互通版本映射命令。

wmm 服务开启时，配置才能生效。

开启 dscp QoS 机制时，配置应用 dscp QoS 映射策略机制才有效。

配置 dscp 标识

- 可选配置。
- 配置 dscp 标识：若无特殊要求，应在每台 AP 上配置 dscp 标识。

根据配置的 dscp 标识决定 dscp 优先级。

【命令格式】 **wmm dscp tag** [*tag-value*] { **back-ground** | **best-effort** | **video** | **voice** } **radio** *radio-id*

【参数说明】 **tag** *tag-value* :表示设置 dscp 优先级，范围为 0-63，best-effort 默认值为 0，back-ground 默认值为 16，video 默认值为 32，voice 默认值为 48。

back-ground：表示将设置 back-ground 队列。

best-effort：表示将设置 best-effort 队列。

video：表示将设置 video 队列。

voice：表示将设置 voice 队列。

radio *radio-id*：表示选择设置 dscp 标识的 radio，范围为 1-48。胖 AP 上无此参数，仅 AC 支持该参数的配置。

no：no 表示恢复默认配置。

【缺省配置】 best-effort 默认值为 0，back-ground 默认值为 16，video 默认值为 32，voice 默认值为 48

【配置模式】 瘦 AP 下在 AP 配置模式，胖 AP 下在接口配置模式。

【使用指导】 此命令为互通版本映射命令。

wmm 服务开启时，配置才能生效。

开启 dscp 机制时，dscp 标识才有效。

检验方法

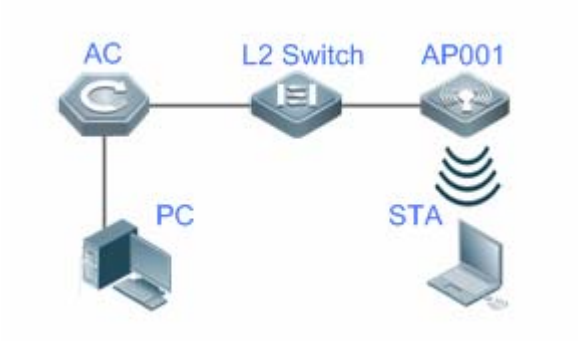
- 瘦 AP 下使用 **show run** 与 **show ap-config run** 命令，胖 AP 下使用 **show run**，可以查看映射配置信息，默认配置时不显示。
- 抓包查看优先级是否映射正确。

配置举例

↘ 配置 QoS 报文优先级映射

【网络环境】

图 2-7



AC 与二层交换机 L2 Switch 相连，AP001 通过 L2 Switch 与 AC 相连；AP001 上配置 wlan1。STA 通过对无线接入 AP001，PC 通过有线连接 AC。

【配置方法】 在 AC 上进行以下配置：

- 进入指定 WLAN 配置模式。
- 配置报文优先级映射。

```
Ruijie# configure terminal
Ruijie(config)# wlan-config 1
Ruijie(config-wlan)#wlan-qos map-table dot11e-tunnel-dscp import 7 export 50
Ruijie(config-wlan)# end
```

【检验方法】 用 IxChariot 打入 STA 到 PC 方向的 AC_VO 优先级流量，并抓空口报文查看无线端优先级；再通过抓包工具，抓 AC 到 PC 的报文查看有线端的优先级。

常见错误

- WMM 服务未开启。

2.6 监视与维护

清除各类信息

无。

查看运行情况

无。

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 wmm vsp 的调试开关。	**debug wlan-qos-vsp**
打开 wmm cli 的调试开关	**debug wlan-qos-cli**
打开 wmm 映射的调试开关	**debug wlan-qos-map**